The Hitchhiker's Guide to the Galaxy

Atticus Wang

Draft: December 26, 2023

“My God, it’s full of stars!”
2001: A Space Odyssey

Contents

CHAPTER 1

Fields and Galois Theory

CHAPTER 2

Lie Groups and Lie Algebras

1. Finite-dimensional Lie algebras

1.1. Basic definitions.

1.1.1. Definition. Let F be a field. A *Lie algebra* over F is a F-vector space L, together with a skew-symmetric bilinear map $[\,,\,] : L \times L \to L$, satisfying Jacobi's identity.

For this section, Lie algebras will be assumed to be finite-dimensional.

1.1.2. Definition. A *Lie subalgebra* $M \subset L$ is a subspace closed under the Lie bracket. An *ideal* $I \subset L$ is a subspace satisfying that for every $x \in I$, $y \in L$, $[x, y] \in I$.

1.1.3. Example. Here are some standard constructions:

- There is a homomorphism of Lie algebras $\mathrm{ad} : L \to \mathfrak{gl}(L)$ called the *adjoint representation*, given by $x \mapsto (y \mapsto [x, y])$.
- For any Lie algebra L, $[L, L] \subset L$ is an ideal.
- The *center* $Z = \{x \in L : [x, L] = 0\} \subset L$ is an ideal. It is the kernel of the adjoint representation.
- Let $M \subset L$ be a subalgebra. Its *normalizer* $N_L(M) = \{x \in L : [x, M] \subset M\}$ is a subalgebra containing M.
- Let $S \subset L$ be a subset. Its *centralizer* $C_L(S) = \{x \in L : [x, S] = 0\}$ is a subalgebra. It is an ideal if S is.
- The *Killing form* $K : L \times L \to F$ is a bilinear form, defined as $K(x, y) = \mathrm{Tr}(\mathrm{ad}\, x\, \mathrm{ad}\, y)$. It is *invariant*, meaning that $K(x, [y, z]) = K([x, y], z)$.
- The *universal enveloping algebra* $U = U(L)$ is a filtered algebra, defined by
$$U(L) = T(L)/(x \otimes y - y \otimes x - [x, y]).$$
The filtration $F_\bullet U$ is given by $F_j U = \mathrm{im}(T^j L)$. Since $[F_i U, F_j U] \subset F_{i+j-1} U$ (here the bracket is in the sense of algebras, $[v, w] = v \otimes w - w \otimes v$), $\mathrm{gr}\, U(L)$ is commutative.

1.1.4. Remark (Motivation for the universal enveloping algebra)**.** We want to write $[x, y] = xy - yx$, which does't make sense a priori, and $U(L)$ is the smallest construction which makes sense of it. Also, we want to view L-reps as actual modules over some ring, and $U(L)$ is the natural such ring.

1.1.5. Theorem (PBW)**.** *The natural map of commutative algebras $S(L) \to \mathrm{gr}\, U(L)$ is an isomorphism.*

In other words, if we fix an F-basis $x_1, \dots, x_n$ of L, then $U(L)$ has an F-basis given by $x_1^{e_1} \otimes \cdots \otimes x_n^{e_n}$. In particular, this means that the map $L \to U(L)$ is injective.

Proof. It suffices to show that these "ordered" elements $x_1^{e_1} \otimes \cdots \otimes x_n^{e_n}$ are linearly independent in $U(L)$. To do that, it suffices to construct a linear map $\Phi : T(L) \to S(L)$ that maps $x_1^{e_1} \otimes \cdots \otimes x_n^{e_n}$ to themselves, and that kills the two-sided ideal $(x \otimes y - y \otimes x - [x, y])$, so that it factors through $U(L)$. This is done inductively on the degree d. For example, $x_2 x_1$ should be mapped to $x_1 x_2 - [x_1, x_2]$, and $x_3 x_1 x_2 \mapsto x_1 x_2 x_3 - x_1[x_2, x_3] - [x_1, x_3]x_2$. In general, for a permutation $t = t_{m_r} \dots t_{m_2} t_{m_1}$ on d elements (where t_m is the transposition $(m, m+1)$), suppose $X = x_{i_1} x_{i_2} \dots x_{i_d}$ is an ordered monomial, then let $t(X) = x_{i_{t(1)}} \dots x_{i_{t(d)}}$, and define
$$\Phi(t(X)) = X - \sum_{i=0}^{r-1} \Phi(u_{m_{i+1}}(t_{m_i} \dots t_{m_1}(X)))$$
where $u_m(x_{i_1} \dots x_{i_d}) = x_{i_1} \dots x_{i_{m-1}} [x_{i_m}, x_{i_{m+1}}] x_{i_{m+2}} \dots x_{i_d}$. One can show that this does not depend on the way t is written as the product of neighboring transpositions. □

1.1.6. Definition. Let L be a Lie algebra. Its *lower central series* is the sequence of subalgebras

$$L^0 \supset L^1 \supset L^2 \supset \cdots$$

where $L^0 = L$, $L^n = [L, L^{n-1}]$. It is *nilpotent* if its lower central series terminates ($L^n = 0$ for some n).

1.1.7. Definition. Let L be a Lie algebra. Its *derived series* is the sequence of subalgebras

$$L^{(0)} \supset L^{(1)} \supset L^{(2)} \supset \cdots$$

where $L^{(0)} = L$, $L^{(n)} = [L^{(n-1)}, L^{(n-1)}]$. It is *solvable* if its derived series terminates ($L^{(n)} = 0$ for some n).

We also recall the Jordan–Chevalley decomposition theorem in linear algebra. Let V be a finite-dimensional vector space over an algebraically closed field F (not necessarily of characteristic 0). Call an element $x \in \operatorname{End} V$ *semisimple* if its minimal polynomial over F has distinct roots (equivalently, it is diagonalizable).

1.1.8. Theorem (Jordan–Chevalley)**.** *Let $x \in \operatorname{End} V$.*

(1) There exists unique $x_s, x_n \in \operatorname{End} V$, such that $x = x_s + x_n$, x_s is semisimple, x_n is nilpotent, and x_s, x_n commute.
(2) x_s, x_n are polynomials in x (with coefficients in F).
(3) If $A \subset B \subset V$ and $x(B) \subset A$, then $x_s(B), x_n(B) \subset A$ too.

1.2. Nilpotent and solvable Lie algebras.

1.2.1. Theorem (Engel's theorem)**.** *Let L be a Lie algbera whose every element is ad-nilpotent. Then L is a nilpotent Lie algebra.*

In the rest of subsections 1.2, 1.3, and 1.4, let F be an algebraically closed field of characteristic 0.

1.2.2. Theorem (Lie's theorem)**.** *Let $L \subset \mathfrak{gl}(V)$ be a solvable Lie algebra over F, where V is a finite-dimensional vector space. Then L stabilizes some flag of V, i.e. there is a basis of V for which every element in L is upper-triangular.*

1.2.3. Proposition (Cartan's criterion for solvability)**.** *Let L be a finite dimensional Lie algebra over F. Then L is solvable iff the Killing form $K(x, y) = \operatorname{Tr}((\operatorname{ad} x) \circ (\operatorname{ad} y))$ satisfies that $K(x, y) = 0$ for $x \in L$, $y \in [L, L]$.*

1.3. Semisimple Lie algebras.

1.3.1. Proposition (Cartan's criterion for semisimplicity)**.** *Let L be a finite dimensional Lie algebra over F. Then L is semisimple iff the Killing form is nondegenerate.*

1.3.2. Theorem. *Let L be semisimple, then there exist simple ideals (unique up to permutation) $L_1, \ldots, L_t \subset L$, such that $L = L_1 \oplus \cdots \oplus L_t$.*

1.3.3. Proposition. *Let L be semisimple, then* $\operatorname{ad} L = \operatorname{Der} L$.

1.3.4. Theorem (Weyl's theorem)**.** *Let $\phi : L \to \mathfrak{gl}(V)$ be a finite dimensional representation of a semisimple Lie algebra L. Then ϕ is completely reducible.*

1.3.5. Definition (Abstract Jordan–Chevalley decomposition)**.** Let L be semisimple, so that $\operatorname{ad} L = \operatorname{Der} L$. Let $x \in L$. Since $\operatorname{Der} L$ contains the semisimple and nilpotent parts of all its elements, there exist $s, n \in L$ such that $\operatorname{ad} x = \operatorname{ad} s + \operatorname{ad} n$, so $x = s + n$.

1.3.6. Proposition (Actually useful criterion for semisimplicity)**.** *Suppose L is a Lie algebra over an algebraically closed field F of characteristic 0, and $\phi : L \subset \mathfrak{gl}(V)$ is a finite-dimensional faithful irrep. Then L is reductive and* $\dim Z(L) \leq 1$. *If $L \subset \mathfrak{sl}(V)$ then L is semisimple.*

Proof. Let $S = \operatorname{Rad}(L)$. By Lie's theorem 1.2.2, there exists a basis of V for which S is upper-triangular. In particular there is a simultaneous eigenvector v for S, say $sv = \lambda(s)v$. Then since S is an ideal, for any $x \in L$,

$$sxv = \lambda(s)xv + \lambda([s, x])v. \tag{1.3.7}$$

Now, since V is irreducible, all vectors in V can be written as linear combinations of $x_1 x_2 \ldots x_n v$ for some $x_1, \ldots, x_n \in L$. Repeatedly using eq. (1.3.7) shows that $sx_1 \ldots x_n v - \lambda(s)x_1 \ldots x_n v$ can be written as linear combinations of vectors that result from strictly less than n applications of elements of L to v. So, we can choose a basis of V, such that every $s \in S$ is an upper-triangular matrix whose diagonal entries are all $\lambda(s)$. However, the elements $[s, x]$ all have trace 0, so their diagonal entries are 0. By eq. (1.3.7) again, $s \in S$ acts as the scalar $\lambda(s)$ on V, so $S \subset Z(L)$, so L is reductive and $\dim Z(L) \leq 1$. If $L \subset \mathfrak{sl}(V)$ then $S = 0$, so L is semisimple. □

1.3.8. Corollary. *The classical Lie algebras $\mathfrak{sl}_n, \mathfrak{sp}_{2n}, \mathfrak{o}_n$ are all semisimple.*

1.4. Root space decomposition.

Let L be a semisimple Lie algebra over F.

1.4.1. Definition. A subalgebra $H \subset L$ is *toral* if all its elements are (ad-)semisimple.

1.4.2. Exercise. Toral subalgebras are abelian.

The following definition is only true when L is semisimple. There is a general notion of Cartan subalgebras, defined later.

1.4.3. Definition. A toral subalgebra $H \subset L$ is called a *Cartan subalgebra* if it satisfies any of the following equivalent conditions:

(1) H is maximal among all toral subalgebras;
(2) $H = C_L(H)$.

1.4.4. Definition.

1.5. Root systems and abstract weights.

1.5.1. Definition. Let $V = F^n$. A *root system* $\Phi \subset V$ is a subset satisfying:

(1) Φ is finite, $0 \notin \Phi$, and Φ spans V.
(2) For any $\alpha \in \Phi$, the only other scalar multiple of α in Φ is $-\alpha$.
(3) For any $\alpha, \beta \in \Phi$, $\langle \alpha, \beta \rangle := \frac{2(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$.
(4) For any $\alpha, \beta \in \Phi$, $\alpha - \langle \alpha, \beta \rangle \beta \in \Phi$.

1.5.2. Definition. Let $\Phi \subset V$ be a root system. Let $\alpha \in \Phi$ be any element, then denote $\sigma_\alpha \in \mathrm{Aut}(\Phi)$ by the automorphism $\kappa \mapsto \kappa - \langle \kappa, \alpha \rangle \alpha$, which is reflection across the hyperplane normal to α. The *Weyl group* W is the group generated by these σ_α's (for $\alpha \in \Phi$).

In fact, the Weyl group of any Φ is a Coxeter group: $\sigma_\alpha \sigma_\beta$ is a rotation with angle 2θ, where $(\alpha, \beta) = |\alpha||\beta| \cos \theta$. Since $\theta \in \{0, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}\}\pi$, the order of $\sigma_\alpha \sigma_\beta$ must be in $\{1, 2, 3, 4, 6\}$.

1.5.3. Definition. For $\alpha \in \Phi$, let P_α denote the hyperplane normal to α. The connected components of $V - \bigcup_\alpha P_\alpha$ are called the *Weyl chambers* of Φ.

1.5.4. Definition. Let $\Phi \subset V$ be a root system. A subset $\Delta \subset \Phi$ is a *base* if it is a basis of V, and every root $\alpha \in \Phi$ is expressed as the linear combination of elements in Δ with either *all non-negative or all non-positive integer* coefficients. Say a root is *positive* or *negative* accordingly.

Let $\gamma \in V - \bigcup_\alpha P_\alpha$. Denote by $\Phi_+(\gamma) = \{\alpha \in \Phi : (\alpha, \gamma) > 0\}$. An element $\alpha \in \Phi_+(\gamma)$ is *indecomposable* if there does not exist $x, y \in \Phi_+(\gamma)$ with $x + y = \alpha$. Denote by $\Delta(\gamma)$ the set of all indecomposable roots in $\Phi_+(\gamma)$.

1.5.5. Proposition. *$\Phi_+(\gamma)$ is a base, and all bases are of this form. So bases are in 1-to-1 correspondence with Weyl chambers.*

1.5.6. Proposition. *Fix a base Δ.*

(1) For any positive root $\alpha \notin \Delta$, $\alpha - \beta$ is a positive root for some $\beta \in \Delta$.
(2) Let $\alpha \in \Delta$, then σ_α permutes $\Delta \backslash \{\alpha\}$.

1.5.7. Proposition. *The Weyl group W acts simply transitively on bases, and it is generated by σ_α, $\alpha \in \Delta$.*

1.5.8. Remark. The Weyl group also naturally acts on Weyl chambers, and these two actions are compatible via the correspondence between Weyl chambers and bases.

1.5.9. Definition. The *length* of an element $\sigma \in W$ is the smallest $n \in \mathbb{Z}_{\geq 0}$ such that $\sigma = \sigma_{\alpha_1} \dots \sigma_{\alpha_n}$ for some $\alpha_1, \dots, \alpha_n \in \Delta$.

1.5.10. Proposition. *Let $\sigma \in W$, then its length is equal to the number of positive roots α such that $\sigma(\alpha)$ is negative.*

1.5.11. Proposition. *The closure of the Weyl chamber $C(\Delta)$ corresponding to Δ is a fundamental domain for the action of W on V.*

1.5.12. Definition. Let Φ be a root system. A *weight* $\lambda \in V$ is an element such that $\langle \lambda, \alpha \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$. Equivalently, if we fix a base $\Delta = \{\alpha_1, \dots, \alpha_n\}$, it is an element such that $\langle \lambda, \alpha_i \rangle \in \mathbb{Z}$ for all i.

1.5.13. Definition. A weight λ is *dominant* (resp. *strongly dominant*) if $\lambda \in \overline{C(\Delta)}$ (resp. $\lambda \in C(\Delta)$). Equivalently, $\langle \lambda, \alpha_i \rangle \geq 0$ (resp. $\langle \lambda, \alpha_i \rangle > 0$).

1.5.14. Remark. It could very well happen that $\lambda \prec \mu$, λ is (strongly) dominant, and μ is not dominant.

1.5.15. Example. Let $\lambda_i \in V$ such that $\langle \lambda_i, \alpha_j \rangle = \delta_{ij}$. Then the set of weights Λ is just the lattice $\bigoplus_i \mathbb{Z}\lambda_i$. Inside Λ, there is a sublattice Λ_r, the *root lattice*, generated by Φ, whose index is equal to the determinant of the Cartan matrix of Φ. There is an element $\delta \in \Lambda$, $\delta = \sum_i \lambda_i = \frac{1}{2}\sum_{\alpha \in \Phi} \alpha$.

1.5.16. Definition. A set $\Pi \subset \Lambda$ is *saturated* if for any $\lambda \in \Pi$, $\lambda - i\alpha \in \Pi$ for every $\alpha \in \Phi$, $0 \leq i \leq \langle \lambda, \alpha \rangle$.

1.5.17. Proposition. *Let Π be saturated, and suppose there exists $\lambda \in \Pi$ such that every $\mu \in \Pi$ has $\mu \prec \lambda$. Then for any dominant μ with $\mu \prec \lambda$, $\mu \in \Pi$.*

1.6. Representations of semisimple Lie algebras. Let L be a semisimple Lie algebra over an algebraically closed field F of characteristic 0. Fix a Cartan subalgebra H of L, let Φ be the set of roots, and fix a base Δ. Let $B = H \bigoplus_{\alpha \succ 0} L_\alpha$ be a Borel subalgebra.

1.6.1. Theorem (Theorem of the highest weight)**.** *There is a bijection*

$$\{\textit{finite-dimensional irreps of } L\} \longleftrightarrow \{\textit{dominant integral weights of } \Delta\}.$$

First we develop some theory about maximal vectors and weights.

1.6.2. Definition. Let V be a (possibly infinite-dim) representation of L, and let V_λ be the weight spaces, $\lambda \in H^*$. A *maximal vector* $v \in V_\lambda$ with *weight* λ is a common eigenvector of H killed by all L_α, $\alpha \succ 0$.

1.6.3. Example. For the adjoint representation of a simple Lie algebra, there is a unique maximal root β, and the maximal vector is the vector in L_β (and its weight is β). For a finite-dimensional representation, by Lie's theorem there exists a common eigenvector v of B, which must be a maximal weight: for any $x \in L_\alpha$, $\alpha \succ 0$, there exists $h \in H$ such that $\alpha(h) \neq 0$, and we have $0 = hxv - xhv = [h,x]v = \alpha(h)xv$ so $xv = 0$. For infinite-dimensional representations, maximal weights do not necessarily exist.

1.6.4. Definition. If $V = U(L)v$ for some maximal vector $v \in V_\lambda$, call V a *highest weight module* (of weight λ).

1.6.5. Proposition (Structure of highest weight modules)**.** *Let $V = U(L)v$ be a highest weight module of weight λ, where v is a maximal vector. Then:*

1. *V is spanned by $(\prod y_\alpha)v$ for $\alpha \succ 0$. In particular V is the direct sum of weight spaces V_μ.*
2. *The possible weights μ which appear are all of the form $\lambda - \sum c_i\alpha_i$, where $\alpha_i \succ 0$, $c_i \in \mathbb{Z}_{\geq 0}$, and they appear with finite multiplicity, and λ appears with multiplicity one.*
3. *Any proper submodule is the direct sum of weight spaces not including V_λ.*
4. *V is indecomposable, with a unique maximal submodule, and their quotient is an irreducible highest weight module of weight λ.*

1.6.6. Proposition. *Suppose V is an irreducible highest weight module. Then there exists a unique maximal vector up to scalar multiplication.*

1.6.7. Proposition. *For any $\lambda \in H^*$, there exists a unique (up to isomorphism) irreducible highest weight representation $V(\lambda)$ of weight λ.*

Proof. Existence: One can take the 1-dimensional rep W of B given by λ, and define $M(\lambda) = U(L) \otimes_{U(B)} W$, or equivalently take $M(\lambda) = U(L)/(x_\alpha, h - \lambda(h)1 : \alpha \succ 0, h \in H)$. ($M$ is called a *Verma module.*) Then quotient out the highest weight $M(\lambda)$ by its unique maximal proper subrepresentation to get $V(\lambda)$. □

Now we are ready to prove the theorem: we now know that in one direction, a irrep V corresponds to its maximal weight λ, and in the other direction one associates λ with $V(\lambda)$.

Proof of theorem 1.6.1. One direction is easy: if $V(\lambda)$ is finite-dimensional, then the $\mathfrak{sl}_2$-triples $(x_\alpha, y_\alpha, h_\alpha)$ in L all act on $V(\lambda)$, and we know that these have integral weights, and the maximal one is clearly dominant. Conversely, suppose λ is dominant integral. We have to show that $V(\lambda)$ is finite-dimensional. Suppose $\Delta = \{\alpha_1, \dots, \alpha_\ell\}$, and let $x_i = x_{\alpha_i}$, $y_i = y_{\alpha_i}$, $h_i = h_{\alpha_i}$. Denote the $\mathfrak{sl}_2$-triple (x_i, y_i, h_i) by $\mathfrak{sl}_2^{(i)}$.

First, we show that the action of x_i, y_i need to be locally (pointwise) nilpotent. For the maximal vector v, one can verify that that $y_i^{\lambda(h_i)+1}v$ is killed by all x_j, hence must be zero, since it has weight $\lambda - (\lambda(h_i)+1)\alpha_i \prec \lambda$. So the subspace generated by $v, y_i v, \dots, y_i^{\lambda(h_i)}v$ is a $\mathfrak{sl}_2^{(i)}$-module. Consider the sum of all finite-dimensional $\mathfrak{sl}_2^{(i)}$-submodules of $V(\lambda)$, then it is nonempty and stable under L (for any finite-dimensioonal $\mathfrak{sl}_2^{(i)}$-submodule W, the sum $\sum_{\alpha\in\Phi} x_\alpha W$ is L-stable), hence must be equal to $V(\lambda)$. So any $w \in V(\lambda)$ lies in such a finite-dimensional $\mathfrak{sl}_2^{(i)}$-submodule, therefore x_i, y_i are locally nilpotent.

Thus, we can define automorphisms $\exp(x_i), \exp(y_i)$ of $V(\lambda)$. The automorphism $s_i = \exp(x_i)\exp(-y_i)\exp(x_i)$ satisfies $s_i V_\mu = V_{\sigma_i \mu}$. In particular, the Weyl group permutes the weights that appear. But then the set of weights that appear must be finite (since they are bounded by λ). So $\dim V$ must be finite as well. □

1.6.8. Corollary. *The set of weights in $V(\lambda)$ form a saturated set (definition 1.5.16). In particular, μ appears iff all W-conjugates of μ are smaller than λ.*

1.6.9. Proposition. *For a dominant integral λ, so that $\lambda(h_i) = m_i \in \mathbb{Z}_{\geq 0}$,*

$$V(\lambda) \simeq U(L)/(x_\alpha, h - \lambda(h)1, y_i^{m_i+1} : \alpha \succ 0, h \in H, 1 \leq i \leq \ell).$$

1.6.10. Theorem (Freudenthal's formula). *Let V be an irreducible L-module with highest weight $\lambda \in \Lambda^+$. Then for any weight $\mu \in \Lambda$, its multiplicity* $\operatorname{mult}(\mu) = \dim V_\mu$ *satisfies the recursion*

$$\operatorname{mult}(\mu) = \frac{2\sum_{\alpha\succ 0}\sum_{i\geq 1} \operatorname{mult}(\mu + i\alpha)\cdot(\mu + i\alpha, \alpha)}{(\lambda+\delta, \lambda+\delta) - (\mu+\delta, \mu+\delta)}.$$

CHAPTER 3

Commutative Algebra

These notes contain solutions to selected problems in Atiyah and MacDonald's *Introduction to Commutative Algebra*. All mistakes are my own.

1. Rings and ideals

1.2. Problem. iv) For a polynomial $f = a_0 + a_1x + \cdots + a_nx^n$, we use $I(f)$ to denote the ideal $(a_0, \ldots, a_n)$. It suffices to show the more general relation

$$I(fg) \subset I(f)I(g) \subset \operatorname{rad}(I(fg)).$$

The first inclusion is obvious. Suppose $g = b_0 + \cdots + b_mx^m$. To prove the second inclusion, we will show $a_ib_j \in \operatorname{rad}(I(fg))$ by induction on i. For the induction basis $i = n$, we can easily show $a_n^{r+1}b_{m-r} \in I(fg)$ for all r, so obviously $a_nb_j \in \operatorname{rad}(I(fg))$. For the induction step from $k+1$ to k, since we can assume $a_ib_j \in \operatorname{rad}(I(fg))$ for all $i > k$, we have then $\sum_j a_jb_{l-j} \in \operatorname{rad}(I(fg))$ for each $l \leq m + k$. Repeating the argument above, we can show that $a_k^{r+1}b_{m-r} \in \operatorname{rad}(I(fg))$ for all r, so $a_kb_j \in \operatorname{rad}(I(fg))$ for all j, concluding the induction.

1.7. Problem. Suppose $\mathfrak{p}$ is a prime ideal, and $x \notin \mathfrak{p}$. Choose $n \geq 2$ such that $x^n = x$. Since $A/\mathfrak{p}$ is an integral domain, $0 = x^n - x = x(x^{n-1} - 1)$ implies that $x^{n-1} = 1$ modulo $\mathfrak{p}$, i.e. x is invertible in $A/\mathfrak{p}$. Therefore, $A/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal.

1.14. Problem. Clearly Σ has a maximal element $\mathfrak{a}$ by Zorn's lemma. Suppose $\mathfrak{a}$ is not prime, that is, there exists $xy \in \mathfrak{a}$ such that $x, y \notin \mathfrak{a}$. Then $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ each contain a non-zero-divisor, say $m + xn$ and $s + yt$. Then $(m + xn)(s + yt) \in \mathfrak{a}$ is a non-zero-divisor, a contradiction.

1.16. Problem. Because $\mathbb{Z}$ is a PID, the points of $\operatorname{Spec}(\mathbb{Z})$ are just 0 and (p), p prime, and the closed sets are any set not containing 0, as well as $\operatorname{Spec}(\mathbb{Z})$.

Because $\mathbb{R}$ is a field, $\operatorname{Spec}(\mathbb{R})$ is the trivial 1-point space.

Because $\mathbb{C}[x]$ is a PID, the points of $\operatorname{Spec}(\mathbb{C}[x])$ are 0 and $(x - z)$, $z \in \mathbb{C}$. The closed sets are any set not containing 0, as well as the whole $\operatorname{Spec}(\mathbb{C}[x])$.

Because $\mathbb{R}[x]$ is a PID, the points of $\operatorname{Spec}(\mathbb{C}[x])$ are 0, $(x - r)$, and $(x^2 + ax + b)$ where $a^2 - 4b < 0$. The closed sets are any set not containing 0, as well as the whole $\operatorname{Spec}(\mathbb{R}[x])$.

Finally, we wish to characterize prime ideals $\mathfrak{p} \subset \mathbb{Z}[x]$. The set $\mathfrak{p} \cap \mathbb{Z}$ must be a prime ideal in $\mathbb{Z}$. Case 1: $\mathfrak{p} \cap \mathbb{Z} = \{0\}$. Assume $\mathfrak{p}$ is nonzero. Let $f(x) \in \mathfrak{p}$ such that it has lowest degree and smallest leading coefficient. Then it is unique and irreducible. For any element $g_0(x) \in \mathfrak{p}$, we can repeat the following modified Euclidean algorithm: there exists nonzero $m_0 \in \mathbb{Z}$ and $a_0(x) \in \mathbb{Z}[x]$ such that $g_1(x) = m_0g_0(x) - f(x)a_0(x)$ has strictly smaller degree than $g_0(x)$, and we substitute $g_1(x)$ for $g_0(x)$. In the end, $\deg g_k(x) < \deg f(x)$, which means $g_k(x) = 0$ for some k. Then we see that $f(x) \mid m_0m_1 \ldots m_{k-1}g_0(x)$. Since f is primitive, $f(x) \mid g_0(x)$. This means $\mathfrak{p} = (f(x))$ where f is irreducible.

Case 2: $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime p. Consider the image of $\mathfrak{p}$ in $\mathbb{Z}[x]/p = \mathbb{F}_p[x]$, which is a prime ideal since the map is surjective. Since $\mathbb{F}_p[x]$ is a PID, the image is $(f(x))$ for some monic irreducible f in $\mathbb{F}_p[x]$ (or else it is 0, in which case $\mathfrak{p} = (p)$). Pick a monic $\tilde{f}(x) \in \mathbb{Z}[x]$ above f, then it is clear $\mathfrak{p} = (p, \tilde{f}(x))$.

In conclusion, prime ideals in $\mathbb{Z}[x]$ are either 0, (p), $(f(x))$, or $(p, f(x))$. Closed sets of $\operatorname{Spec}(\mathbb{Z}[x])$ are characterized by a choice of primes (p), a choice of polynomials $f(x)$, and all $(p, f(x))$ with either p or $f(x)$ among the chosen ones (as well as, of course, the whole $\operatorname{Spec}(\mathbb{Z}[x])$).

1.20. Problem. iv) Let Y be a irreducible component of $X = \operatorname{Spec}(A)$. Since the closure of a irreducible subspace is again irreducible, we can assume Y is closed. Then $Y = V(\mathfrak{a})$ for some radical ideal $\mathfrak{a}$. If $\mathfrak{a}$ is not prime, then there exists $xy \in \mathfrak{a}$ and $x, y \notin \mathfrak{a}$. Then $V(\mathfrak{a}, x) \cup V(\mathfrak{a}, y) = V(\mathfrak{a})$ while neither is equal to $V(\mathfrak{a})$, contradiction. Therefore $\mathfrak{a}$ is prime. By maximality, $\mathfrak{a}$ must be a minimal prime, as desired.

1.22. Problem. We will prove ii) $\implies$ i) $\implies$ iii) $\implies$ ii).

ii) $\implies$ i): In general, it is easy to show that any prime ideal in $A = A_1 \times \cdots \times A_n$ must be of the form $A_1 \times \cdots \times A_{i-1} \times \mathfrak{p} \times A_{i+1} \times \ldots A_n$, where i is some index and $\mathfrak{p} \subset A_i$ is a prime ideal. This easily implies that $\operatorname{Spec} A = \operatorname{Spec} A_1 \sqcup \cdots \sqcup \operatorname{Spec} A_n$.

iii) $\implies$ ii): Say $e^2 = e$ where $e \neq 0, 1$. Let $A_1 = eA$ and $A_2 = \ker(A \twoheadrightarrow eA) = \operatorname{Ann}(e)$. Then e is a unit in A_1 while $1 - e$ is a unit in A_2, so both A_1 and A_2 are nonzero rings. Furthermore, any element $a \in A$ can be uniquely written as $ea + (1-e)a \in A_1 \times A_2$. This shows $A \cong A_1 \times A_2$.

i) $\implies$ iii): Suppose $\operatorname{Spec} A = V(\mathfrak{a}) \sqcup V(\mathfrak{b})$. Then any prime ideal either contains $\mathfrak{a}$ or contains $\mathfrak{b}$, but not both. This means that $\mathfrak{a} + \mathfrak{b} = (1)$ and $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \operatorname{rad}(A)$. So there exists $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ where $a + b = 1$, and $(ab)^n = 0$. Let $e = (1 - a^n)^n$. Then $e(1-e)$ is a multiple of $(ab)^n$, so $e = e^2$. If $e = 0$, then $1 - a^n \in \operatorname{rad}(A)$, which means that a^n, hence a, is a unit (Problem 1.1), a contradiction. If $e = 1$, then $1 - a^n$ is a unit, then so is $b = 1 - a$, a contradiction. Therefore, e is an idempotent $\neq 0, 1$.

1.28. Problem. Injectivity is clear. For surjectivity, fix a homomorphism $f : P(Y) \to P(X)$. Let $\phi = (\phi_1, \ldots, \phi_m)$ where $\phi_i = f(y_i)$ (here $y_i \in P(Y)$ is the ith coordinate of k^m). Then ϕ induces the homomorphism f.

2. Modules

For convenience, we also record some important results in each chapter.

2.1. Proposition (Cayley-Hamilton). *Let M be a finitely generated A-module, and $\phi : M \to M$ a homomorphism. Suppose $\mathfrak{a} \subset A$ is an ideal such that $\phi(M) \subset \mathfrak{a}M$. Then there exists a polynomial*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where $a_i \in \mathfrak{a}$.

Proof. Suppose $x_1, \ldots, x_m$ generate M, and $\phi(x_i) = \sum_{j=1}^m a_{ij}x_j$ where $a_{ij} \in \mathfrak{a}$. Let C_{ij} be the matrix defined by $C_{ij} = a_{ij}$ when $i \neq j$, and $C_{ii} = a_{ii} - \phi$. (In other words, we treat a_{ij} as elements of $\operatorname{End}(M)$.) Then C annihilates all of $x_1, \ldots, x_m$, so $\det C$ does as well (multiply by the adjugate matrix). But $\det C$ is a polynomial in ϕ of the required form. □

2.2. Proposition. *Let M be a finitely generated A-module. If $\mathfrak{a}M = M$ for some ideal $\mathfrak{a} \in A$, then there exists $a \in \mathfrak{a}$ with $am = m$ for every $m \in M$.*

Proof. Take $\phi = \mathrm{id}$ in the above proposition. □

2.3. Corollary (Nakayama's lemma). *Let M be a finitely generated A-module. If $\mathfrak{a}M = M$ for some ideal $\mathfrak{a} \in A$, $\mathfrak{a} \subset J(A)$, then $M = 0$.*

First proof. Since any $1 - x$ ($x \in J(A)$) is a unit, this follows from Proposition 2.2. □

Second proof. Suppose $x_1, \ldots, x_n$ is a *minimal* set of generators of M. We have $x_n = \sum_{i=1}^n a_i x_i$, so $(1 - a_n)x_n = \sum_{i=1}^{n-1} a_i x_i$. But $1 - a_n$ is a unit, so x_n is generated by $x_1, \ldots, x_{n-1}$, a contradiction. □

2.4. Corollary. *Let M be a finitely generated A-module, $N \subset M$ a submodule, $\mathfrak{a} \in J(A)$ an ideal. If $M = \mathfrak{a}M + N$, then $M = N$.*

Proof. Apply Corollary 2.3 to M/N. □

2.5. Corollary. *Let $(A, \mathfrak{m}, k)$ be a local ring, M a finitely generated A-module. Let $x_1, \ldots, x_n \in M$ whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then $x_1, \ldots, x_n$ is a set of minimal generators of M.*

Proof. Let $N = (x_1, \ldots, x_n)$. Then $M = N + \mathfrak{m}M$, so $M = N$ by Corollary 2.4. □

○

2.11. Problem. Suppose $A^m \cong A^n$. Let $\mathfrak{m}$ be a maximal ideal of A, then $(A/\mathfrak{m}) \otimes A^m \cong (A/\mathfrak{m}) \otimes A^m$, and both sides are now vector spaces over $k = A/\mathfrak{m}$, so $m = n$.

If $\phi : A^m \to A^n$ is surjective, then so is the induced map $(A/\mathfrak{m})^m \to (A/\mathfrak{m})^n$, hence $m \geq n$.

Suppose $\phi : A^m \to A^n$ is injective, and $m > n$. We may view ϕ as an injective map $\phi : A^m \to A^m$ satisfying $\phi(A^m) \subset \mathfrak{a}(A^m)$, where $\mathfrak{a}$ is the ideal generated by $(1, \dots, 1, 0, \dots, 0)$, with n ones. By (2.4) of the book, ϕ satisfies an equation $\phi^k + a_1\phi^{k-1} + \dots + a_k = 0$, so $\phi^k(0, \dots, 0, 1) = 0$, a contradiction to injectivity. Therefore, $m \leq n$.

2.13. Problem. Define $p : N_B \to N$ by $b \otimes n \mapsto bn$. Then $p \circ g$ is the identity on N, so g is injective. In addition, the sequence

$$0 \to \ker p \to N_B \xrightarrow{p} N \to 0$$

splits by the existence of $g : N \to N_B$, so $N_B \cong N \oplus \ker p$.

2.19. Problem (Direct limits are exact)**.** Let $\mu_{ij}, \nu_{ij}, \pi_{ij}$ be the maps inside the direct systems M, N, P respectively. Let f_i, g_i be the individual maps between the direct systems, and let $f : M \to N$, $g : N \to P$ be the induced maps. Suppose $n \in N$ such that $g(n) = 0$, then there exists $n_i \in N_i$ such that $\nu_i(n_i) = n$ and $\pi_i(g_i(n_i)) = 0$, in other words, some $g_j(\nu_{ij}(n_i)) = \pi_{ij}(g_i(n_i)) = 0$. By exactness, there exists $m_j \in M_j$ such that $f_j(m_j) = \nu_{ij}(n_i)$. Then if we let $m = \mu_j(m_j)$, then $f(m) = \nu_j(f_j(m_j)) = n$. Consequently, $\ker g \subset \operatorname{im} f$.

Suppose now that $n = f(m)$ for $m \in M, n \in N$. Then there is $m_i \in M_i$ such that $\mu_i(m_i) = m$. Denote $n_i = f_i(m_i)$, then $\nu_i(n_i) = n$. By exactness, $g_i(n_i) = 0$, so $g(n) = 0$. This means that $\operatorname{im} f \subset \ker g$, so $M \to N \to P$ is exact.

2.25. Problem. For any A-module M, the Tor long exact sequence gives

$$\dots \to \operatorname{Tor}_2(M, N'') \to \operatorname{Tor}_1(M, N') \to \operatorname{Tor}_1(M, N) \to \operatorname{Tor}_1(M, N'') \to \dots$$

By Problem 2.24, the first and last terms are both zero, so N' is flat iff N is flat.

2.26. Problem. This exercise demonstrates the power of direct limits. The nontrivial part is to show that $\operatorname{Tor}_1(A/\mathfrak{a}, N) = 0$ for all f.g. ideal $\mathfrak{a}$ implies N flat.

First, let $\mathfrak{a} \subset A$ be *any* ideal. Let $\mathfrak{a}_i$ be the directed system of finitely generated ideals such that $\mathfrak{a}_i \subset \mathfrak{a}$, ordered by inclusion. Taking the direct limit of the exact sequences $0 \to \mathfrak{a}_i \to A \to A/\mathfrak{a}_i \to 0$ gives the exact sequence $0 \to \mathfrak{a} \to A \to \varinjlim A/\mathfrak{a}_i \to 0$, so we conclude that $A/\mathfrak{a} \cong \varinjlim A/\mathfrak{a}_i$. Now, $\operatorname{Tor}_1(A/\mathfrak{a}, N)$ is the first homology of

$$\dots \to P_2 \otimes (A/\mathfrak{a}) \to P_1 \otimes (A/\mathfrak{a}) \to P_0 \otimes (A/\mathfrak{a}) \to 0$$

for a fixed projective resolution $P_i \to N$. Since this becomes exact when we replace $\mathfrak{a}$ by each $\mathfrak{a}_i$, and direct limits commute with tensor products, we conclude that $\operatorname{Tor}_1(A/\mathfrak{a}, N) = 0$.

Next, let M be any *finitely generated* A-module. Then there is a filtration

$$0 = M_0 \subset M_1 \subset \dots \subset M_n = M$$

such that each M_i/M_{i-1} is generated by one element, i.e. is isomorphic to $A/\mathfrak{a}$ for some ideal $\mathfrak{a}$. We now know that $\operatorname{Tor}_1(M_i/M_{i-1}, N) = 0$. Using induction and Problem 2.25, we conclude that $\operatorname{Tor}_1(M, N) = 0$.

Finally, let M be any A-module. Then $M = \varinjlim M_i$ where M_i are finitely generated submodules of M, so we conclude that $\operatorname{Tor}_1(M, N) = 0$. This implies that N is flat, as desired.

2.27. Problem. i) $\Longrightarrow$ ii): Let $(x) \subset A$ be a principal ideal. Then $A/(x)$ is flat, so the map $(x) \otimes (A/(x)) \hookrightarrow A \otimes (A/(x))$ is injective. In other words, $(x) \otimes (A/(x)) = 0$. Let $\mathfrak{a} \subset A$ be the ideal generated by x and $\operatorname{Ann}(x)$. Define a map $(x) \times (A/(x)) \to A/\mathfrak{a}$ by $(ax, b + (x)) \mapsto ab + \mathfrak{a}$. This is well-defined and bilinear, so it induces a well-defined surjective linear map $(x) \otimes (A/(x)) \to A/\mathfrak{a}$. Therefore, $\mathfrak{a} = A$. So there exists $a, y \in A$ such that $ax + y = 1$ and $xy = 0$, in other words, $x(1 - ax) = 0$. So (x) is idempotent.

ii) $\Longrightarrow$ iii): Every finitely generated ideal is generated by idempotents, so it must be principal (use $(e, f) = (e + f - ef)$). So it is a direct summand of A.

iii) $\Longrightarrow$ i): Since the direct summand of a free module is free, for any finitely generated ideal $\mathfrak{a} \in A$, $A/\mathfrak{a}$ is free. So for any A-module M, $\operatorname{Tor}_1^A(A/\mathfrak{a}, M) = 0$, so by the previous problem M is flat.

3. Rings and modules of fractions

Here's a brief summary of how the operations we've learned so far interact with each other:

- Tensor products are right exact;
- Direct limits are exact;
- Tensor products commute with direct limits;
- Localization is exact;
- $S^{-1}A$ is a flat A-module;
- Localization commutes with tensor products ($S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N)$);
- Exactness is a local property (in fact it can be checked at *maximal* ideals);
- Flatness is a local property.

○

3.7. Problem. i) Suppose S is saturated, and let $x \in A \backslash S$. Then its image in $S^{-1}A$ is non-unit, since otherwise there exists $b \in A$ such that $ab \in S$, which would mean $a \in S$, contradiction. In addition, WLOG $0 \notin S$. So there exists a maximal ideal $\mathfrak{m} \subset S^{-1}A$ containing $\frac{x}{1}$. Then $\mathfrak{m} \cap A$ is a prime ideal in A containing x and disjoint from S. This means that $A - S$ is a union of prime ideals. The converse is obvious.

ii) Since the intersection of a family of saturated sets is again saturated, $\overline{S}$ exists. Any prime ideal in $A \backslash \overline{S}$ is necessarily in $A \backslash S$, so $\overline{S}$ is the complement of the union of prime ideals not intersecting S.

Suppose that $S = 1 + \mathfrak{a}$. Any prime ideal $\mathfrak{p}$ not intersecting S corresponds one-to-one with a prime $S^{-1}\mathfrak{p} \subset S^{-1}A$. The union of all prime ideals in $S^{-1}A$ is clearly the set of all non-units in $S^{-1}A$, so the union of all prime ideals not intersecting S is the set

$$\{x \in A : \nexists y \in A \text{ such that } xy \in S\}.$$

But this is precisely the set of elements $x \in A$ whose image in $A/\mathfrak{a}$ is a nonunit. So $\overline{S}$ is the set of elements $x \in A$ whose image in $A/\mathfrak{a}$ is a unit.

3.8. Problem. i) $\Longrightarrow$ ii): Since $t/1$ is a unit in $T^{-1}A$, it should be a unit in $S^{-1}A$ too.

ii) $\Longrightarrow$ iii): This is by definition.

iii) $\Longrightarrow$ i): To show injectivity, suppose $at = 0$ for some $t \in T$. Then there exists $x \in A$ with $xt \in S$, so there exists $s = xt$, $s \in S$, such that $as = 0$. To show surjectivity, suppose $a/t \in T^{-1}A$. Take $s = xt \in S$. Then $a/t = ax/xt = ax/s$ is in $\phi(S^{-1}A)$.

iii) $\Longleftrightarrow$ iv): By the reasoning in the above problem, the saturation $\overline{S}$ consists of all elements that divide some element of S.

iv) $\Longleftrightarrow$ v): Follows from the above problem.

3.10. Problem. ii) If A is absolutely flat, then so is $A_{\mathfrak{m}}$, but since it is a local ring it must be a field. Conversely, suppose $A_{\mathfrak{m}}$ is a field for all maximal $\mathfrak{m}$. It suffices to show that for any A-module M and any injection of A-modules $N \to P$, $M \otimes N \to M \otimes P$ is injective. Since exactness is a local property, it suffices to show that $M_{\mathfrak{m}} \otimes N_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes P_{\mathfrak{m}}$ is injective. But since $A_{\mathfrak{m}}$ is a field, the map is automatically injective.

3.11. Problem. i) $\Longrightarrow$ ii): If $A/\operatorname{rad} A$ is absolutely flat, then for any $a \in A$, there exists $x \in A$ such that $a(1 - ax) \in \operatorname{rad}(A)$, i.e. $a(1 - ax)$ is nilpotent. Let $\mathfrak{p} \subset A$ be a prime ideal, then for any a, either $a \in \mathfrak{p}$ or $1 - ax \in \mathfrak{p}$. Consequently, $A/\mathfrak{p}$ is a field, and $\mathfrak{p}$ is maximal.

ii) $\Longleftrightarrow$ iii): The closure of $\{x\} \in X = \operatorname{Spec} A$ is $\overline{\{x\}} = V(\mathfrak{p}_x) = \{x\}$, iff $\mathfrak{p}_x$ is maximal. (Remark: $\operatorname{Spec} A$ is always T_0 for any ring A.)

ii) $\Longrightarrow$ iv): Let $\mathfrak{p}_1, \mathfrak{p}_2$ be distinct points in $X = \operatorname{Spec} A$. Choose $f_1 \notin \mathfrak{p}_1$, $f_1 \in \mathfrak{p}_2$. We wish to find $f_2 \notin \mathfrak{p}_2$ such that $f_1 f_2$ is nilpotent (which guarantees that $X_{f_1} \cap X_{f_2} = \varnothing$). Consider the image of f_1 in $A_{\mathfrak{p}_2}$. Because every prime ideal in A is maximal, $A_{\mathfrak{p}_2}$ is a local ring whose only prime ideal is $\mathfrak{p}_2 A_{\mathfrak{p}_2}$. Therefore, f_1 is nilpotent in $A_{\mathfrak{p}_2}$, so there exists $f_2 \in A \backslash \mathfrak{p}_2$ such that $f_1 f_2$ is nilpotent in A. Then X_{f_1}, X_{f_2} are disjoint neighborhoods of $\mathfrak{p}_1, \mathfrak{p}_2$ respectively.

iv) $\Longrightarrow$ iii) is obvious.

ii), iv) $\Longrightarrow$ i): By the last problem, it suffices to show that $(A/\operatorname{rad} A)_{\mathfrak{m}}$ is a field for any maximal ideal $\mathfrak{m} \subset A/\operatorname{rad} A$. Because the preimage $\mathfrak{m}^c$ of $\mathfrak{m}$ is a prime ideal, it is maximal in A. Let $(a + \operatorname{rad} A)/(s + \operatorname{rad} A) \in A_{\mathfrak{m}}$ such that $a \in \mathfrak{m}^c$. Copying the proof of ii) $\Longrightarrow$ iv), we can find $t \in A \backslash \mathfrak{m}^c$ such that at is nilpotent in A, i.e. $(a + \operatorname{rad} A)/(s + \operatorname{rad} A)$ is zero. So $(A/\operatorname{rad} A)_{\mathfrak{m}}$ is indeed a field and we are done.

Finally, we need to show that $X = \operatorname{Spec} A$ is totally disconnected. Because $A/\operatorname{rad} A$ is absolutely flat, for any $a \in A$, there exists $x \in A$ such that $a(1-ax)$ is nilpotent. Therefore, X_a and X_{1-ax} partition X. As a result, if a subset $S \subset X$ is connected, either $X_a \subset S$ or $X_a \cap S = \varnothing$. If S contains at least two points, then since X is Hausdorff, S cannot be connected. So S must be a single point.

3.12. Problem. iv) Because $K \otimes_A M \cong S^{-1}M$ where $S = A\backslash\{0\}$, the kernel of the map $M \to K \otimes_A M \cong S^{-1}M$ is precisely $T(M)$ by definition of localization.

3.15. Problem. It suffices to show that if $\phi : A^n \to A^n$ is surjective, then it is bijective. By localizing at each prime ideal, we can assume WLOG A is local. Let $\mathfrak{m}$ be its maximal ideal and k be its residue field. Tensoring the split exact sequence $0 \to \ker\phi \to A^n \to A^n \to 0$ with k, we obtain that $\ker\phi = \mathfrak{m}\ker\phi$. Also $\ker\phi$ is finitely generated since it is a direct summand of A^n, so by Nakayama's lemma $\ker\phi = 0$, as desired. (Aside: If ϕ is injective, there is no reason for it to be surjective. For example, consider $\mathbb{Z} \to \mathbb{Z}$ with multiplication by 2. The dual argument breaks down since $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ is not split.)

3.19. Problem. viii) Let $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p} = \mathfrak{q}^c \in \operatorname{Spec} A$. We have

$$(B \otimes_A M)_{\mathfrak{q}} = B_{\mathfrak{q}} \otimes_B (B \otimes_A M) = (B_{\mathfrak{q}} \otimes_B B) \otimes_A M = B_{\mathfrak{q}} \otimes_A M = B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$$

using the homomorphisms $A \to A_{\mathfrak{p}} \to B_{\mathfrak{q}}$. Therefore, if $M_{\mathfrak{p}} = 0$, then $(M_B)_{\mathfrak{q}} = 0$. Conversely, by problem 2.13 the map $M_{\mathfrak{p}} \to B_{\mathfrak{q}} \otimes M_{\mathfrak{p}}$ is an injection, so $(M_B)_{\mathfrak{q}} = 0$ implies $M_{\mathfrak{p}} = 0$. This is enough to imply $\operatorname{Supp} M_B = (f^*)^{-1}(\operatorname{Supp} M)$.

3.21. Problem. iv) (Fiber over a point) Let $\mathfrak{p} \in \operatorname{Spec}(A)$. We have the following commutative diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "f"'] & A_{\mathfrak{p}} \arrow[r] \arrow[d] & A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \arrow[d] \\
B \arrow[r] & B_{\mathfrak{p}} \arrow[r] & B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}
\end{tikzcd}$$

where $B_{\mathfrak{p}} = f(A\backslash\mathfrak{p})^{-1}B$ and $\mathfrak{p}B_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^e$. In terms of the spectra, we then have

$$\begin{tikzcd}
\operatorname{Spec} B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \arrow[r] \arrow[d] & \operatorname{Spec} B_{\mathfrak{p}} \arrow[r] \arrow[d] & \operatorname{Spec} B \arrow[d, "f^*"] \\
\operatorname{Spec} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \arrow[r] & \operatorname{Spec} A_{\mathfrak{p}} \arrow[r] & \operatorname{Spec} A.
\end{tikzcd}$$

Hence $\operatorname{Spec} B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} = \operatorname{Spec} B \otimes_A (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$ is canonically homeomorphic to the fiber $(f^*)^{-1}(\mathfrak{p})$.

(Aside: we can use this to give a better proof of problem 1.16. To find the prime ideals of $\mathbb{Z}[x]$, it is enough to find the fibers over each $\mathfrak{p} \subset \mathbb{Z}$. The fiber over $\mathfrak{p} = 0$ is $\operatorname{Spec} \mathbb{Z}[x] \otimes \mathbb{Q} = \operatorname{Spec} \mathbb{Q}[x]$. These are the polynomials in $\mathbb{Z}[x]$ that are irreducible in $\mathbb{Q}[x]$, and by Gauss's lemma they must be irreducible in $\mathbb{Z}[x]$. The fiber over $\mathfrak{p} = (p)$ is $\operatorname{Spec} \mathbb{Z}[x] \otimes \mathbb{F}_p = \mathbb{F}_p[x]$. These are the polynomials in $\mathbb{Z}[x]$ that are irreducible mod p.)

3.24. Problem. By compactness WLOG suppose $X_{f_1}, \ldots, X_{f_n}$ cover $\operatorname{Spec} A$.

Existence: suppose elements $a_i/f_i^{e_i} \in A_{f_i}$ satisfy that $a_i f_j^{e_j}/f_i^{e_i} f_j^{e_j} = a_j f_i^{e_i}/f_i^{e_i} f_j^{e_j}$ in $A_{f_i f_j}$, that is, $a_i f_j^{e_j} - a_j f_i^{e_i}$ is killed by some power of $f_i f_j$.

Let $g_i = f_i^{e_i}$, and suppose $a_i g_j - a_j g_i$ is killed by $(g_i g_j)^N$ for some large enough N, for all pairs i, j. Then $X_{g_1^{N+1}}, \ldots, X_{g_n^{N+1}}$ cover $\operatorname{Spec} A$, so there exist $m_i \in A$ such that

$$1 = \sum_i m_i g_i^{N+1} = \sum_i (m_i g_i^N) g_i.$$

(This is like a "partition of unity" that allows one to go from local to global.)

Let $a = \sum_i m_i g_i^N a_i$. It suffices to show that for any i, $a g_i - a_i$ is killed by a power of g_i. We expand

$$\begin{aligned} a g_i - a_i &= (\sum_j m_j g_j^N a_j) g_i - a_i (\sum_j m_j g_j^{N+1}) \\ &= \sum_j m_j g_j^N (a_j g_i - a_i g_j) \end{aligned}$$

which is killed by g_i^N.

Uniqueness: it suffices to show that if the image of $x \in A$ in each A_{f_i} is zero, then $x = 0$. Suppose x is killed by $f_i^{e_i}$ for each i. Since $X_{f_i^{e_i}}$ cover X, there are $m_i \in A$ such that $\sum_i m_i f_i^{e_i} = 1$. Then 1 kills x, so $x = 0$.

3.27. Problem. iv) Suppose X is covered by a collection of open sets defined by $f_\alpha : A \to B_\alpha$. Then $\operatorname{Spec}(\bigotimes_\alpha B_\alpha) = \varnothing$, so $\bigotimes_\alpha B_\alpha = 0$. Since this is a direct limit, one of the terms $\bigotimes_i B_i$ in the direct system must be zero, and this tensor product is over a finite index set.

3.30. Problem. If $A/\operatorname{rad} A$ is absolutely flat, then X_a is both open and closed, so X and X_C agree. Conversely, suppose the complement of X_a is X_b, then $A = (a) + (b)$, so there exist x, y with $1 = xa + yb$. In addition, ab must belong to all prime ideals, so $ab \in \operatorname{rad} A$, so $a(1 - xa)$ is nilpotent, so $A/\operatorname{rad} A$ is absolutely flat.

4. Primary decomposition

Suppose $\mathfrak{a} \subset A$ is a decomposable ideal.

4.1. Theorem. *Let $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ be a minimal primary decomposition. Then $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$ are precisely prime ideals of the form $\operatorname{rad}(\mathfrak{a} : x)$ as x ranges over A. In particular, the set of $\mathfrak{p}_i$'s are only dependent on $\mathfrak{a}$ (these are the primes* associated with *$\mathfrak{a}$).*

Proof. The proof is surprisingly easy. We expand

$$\operatorname{rad}(\mathfrak{a} : x) = \operatorname{rad}(\bigcap_i \mathfrak{q}_i : x) = \bigcap_i \operatorname{rad}(\mathfrak{q}_i : x) = \bigcap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i.$$

Picking $x \notin \mathfrak{q}_i$, $x \in \bigcap_{j \neq i} \mathfrak{q}_j$ by minimality, we have $\operatorname{rad}(\mathfrak{a} : x) = \mathfrak{p}_i$. Conversely, if $\operatorname{rad}(\mathfrak{a} : x)$ is prime, then it must equal one of the $\mathfrak{p}_i$'s. □

4.2. Proposition. *The isolated (mimimal) prime ideals associated with $\mathfrak{a}$ are precisely the minimal prime ideals containing $\mathfrak{a}$.* □

4.3. Proposition. $\bigcup_i \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}$.

Proof. Reducing to $A/\mathfrak{a}$, it suffices to show that if 0 is decomposable with associated prime ideals $\mathfrak{p}_i$, then $\bigcup_i \mathfrak{p}_i$ is precisely the set of zero divisors, $\bigcup_{x \neq 0} \operatorname{rad}(0 : x)$. If $x \neq 0$ then there must exist i such that $x \notin \mathfrak{q}_i$, so $\operatorname{rad}(0 : x) \subset \mathfrak{p}_i$ by Theorem 4.1. Conversely, for each $\mathfrak{p}_i$, there exists x such that $\operatorname{rad}(0 : x) = \mathfrak{p}_i$, also by Theorem 4.1. □

Primary ideals interact nicely with localizations. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, $\mathfrak{p} \cap S = \varnothing$, then $S^{-1}\mathfrak{q}$ is a $S^{-1}\mathfrak{p}$-primary ideal that contracts back to $\mathfrak{q}$. If $\mathfrak{p} \cap S \neq \varnothing$, then $S^{-1}\mathfrak{q} = S^{-1}A$.

We say a subset Σ of prime ideals associated to $\mathfrak{a}$ is *isolated* if is closed downwards under inclusion. Then, localizing at $A \backslash (\bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p})$ kills off precisely the associated primes not in Σ.

4.4. Theorem. *Let $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ be a minimal primary decomposition. Let $\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_m}$ be an isolated set of associated primes. Then $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is dependent only on $\mathfrak{a}$. In particular, if $\mathfrak{p}_i$ is isolated, then $\mathfrak{q}_i$ is dependent only on $\mathfrak{a}$.*

Proof. Localize at $S = A \backslash (\mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_m})$. Then $S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_{i_1} \cap \cdots \cap S^{-1}\mathfrak{q}_{i_m}$ is a minimal primary decomposition of $S^{-1}\mathfrak{a}$, and $S^{-1}\mathfrak{a} \cap A = \mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is a minimal primary decomposition of $S^{-1}\mathfrak{a} \cap A$, which is only dependent on $\mathfrak{a}$ since S is only dependent on $\mathfrak{a}$. □

Some (counter)examples to keep in mind:

- In $k[x, y]$, $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$. These are both minimal primary decompositions, and the set of associated primes are (x) and (x, y). Furthermore, the primary ideal corresponding to isolated primes (x) is the same, whereas the other primary ideal is different.
- A prime power is not necessarily primary (whereas this becomes true if "prime" is replaced by "maximal"). An example is $\mathfrak{p}^2$ in $k[x, y, z]/(xy - z^2)$, where $\mathfrak{p} = (x, z)$.
- A $\mathfrak{p}$-primary ideal is not necessarily a power of $\mathfrak{p}$. An example is (x, y^2) in $k[x, y]$.

Finally, we summarize the theory of primary decomposition for modules. Fix a ring A and an A-module M. An element $x \in A$ is a zero-divisor in M if $xm = 0$ for some $m \neq 0$. It is nilpotent in M if some power of it kills M.

For a submodule $N \subset M$, define its radical $r_M(N) = \operatorname{rad}(N : M)$. It is *primary* in M if $N \neq M$ and every zero divisor in M/N is nilpotent. Equivalently, $N \subset M$ is primary iff $(N : M) = \operatorname{Ann}(M/N)$ is $r_M(N)$-primary. A minimal *primary decomposition* of $N \subset M$ is

$$N = \bigcap_{i=1}^{n} Q_i$$

where each Q_i is primary in M, $r_M(Q_i)$ are all distinct, and none of Q_i is redundant.

4.5. Proposition. *The primes $\mathfrak{p}_i = r_M(Q_i)$ are only dependent on N. They are the prime ideals of the form* $\operatorname{rad}(N : x)$ *where $x \in M$.*

4.6. Proposition. *The minimal prime ideals associated with N are precisely the minimal primes containing $r_M(N)$.*

4.7. Proposition. $\bigcup_i \mathfrak{p}_i = \{x \in A : (N : x) \neq N\}$.

4.8. Proposition. *Let $\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_m}$ be an isolated set of associated primes. Then $Q_{i_1} \cap \cdots \cap Q_{i_m}$ is dependent only on N. In particular, if $\mathfrak{p}_i$ is isolated, then Q_i is dependent only on N.*

The proofs of these propositions are completely standard.

○

4.3. Problem. Suppose A is absolutely flat, and $\mathfrak{q} \subset A$ is primary. Then $A/\mathfrak{q}$ is absolutely flat (problem 2.28). Suppose $a \in A/\mathfrak{q}$ is a nonunit, then there exists $x \in A/\mathfrak{q}$ such that $a(1-ax) = 0$, so a is a zero-divisor. Since $\mathfrak{q}$ is primary, a is nilpotent. Then $a^n = 0$ for some n, so $a = x^{n-1}a^n = 0$. In other words, $A/\mathfrak{q}$ is a field, so $\mathfrak{q}$ is maximal.

4.6. Problem. We claim that the zero ideal is not decomposable. Suppose otherwise, then the set of zero divisors in $C(X)$ is equal to the union of the (finitely many) prime ideals associated with (0). Find maximal ideals $\mathfrak{m}_{x_1}, \dots, \mathfrak{m}_{x_n}$ containing each associated prime ideal (these can only be of the form $\mathfrak{m}_x = \{f \in C(X) : f(x) = 0\}$). It suffices to find a zero divisor g that does not vanish at all of $x_1, \dots, x_n$.

Since X is compact Hausdorff, X is a normal space. Urysohn's lemma then says that if $A, B \subset X$ are two disjoint nonempty closed sets, then they are separated by a continuous function.

We choose $x \neq x_1, \dots, x_n$ since X is infinite. Since X is Hausdorff, there exist disjoint open sets $U, V \subset X$ such that $x \in U$ and $x_1, \dots, x_n \in V$. Choose a function $g \in C(X)$ that equals 1 on $x_1, \dots, x_n$ and 0 on $X \backslash V$. Then $\operatorname{Supp} g = \overline{\{x \in X : g(x) \neq 0\}} \subset X \backslash U$. Then we can find $h \neq 0$ that vanishes on $\operatorname{Supp} g$ and equals 1 at x, so that $gh = 0$.

4.7. Problem. iii) If $f(x)$ is a zero-divisor in $(A/\mathfrak{q})[x] \cong A[x]/\mathfrak{q}[x]$, then there exists a nonzero element $a \in A/\mathfrak{q}$ such that $af(x) = 0$, so every coefficient of f is a zero-divisor in $A/\mathfrak{q}$. Because $\mathfrak{q}$ is primary, this implies that every coefficient of f is nilpotent, so f is nilpotent. This shows that $\mathfrak{q}[x]$ is primary, and clearly it must be $\mathfrak{p}[x]$-primary.

4.9. Problem. Suppose $\mathfrak{p}$ is a minimal prime ideal containing $(0 : a)$ for some element a. Then the image of $\mathfrak{p}$ in $A/(0 : a)$ is a minimal prime, so every element inside is a zero-divisor. Therefore, if $x \in \mathfrak{p}$, then there exists $y \in A, y \notin (0 : a)$ such that $xy \in (0 : a)$. So $x \in (0 : ay)$ and $ay \neq 0$, as desired.

If 0 is decomposable, then the primes in $\operatorname{Ass}(0)$ are precisely primes of the form $\operatorname{rad}(0 : x)$, which is a subset of $D(A)$. Conversely, if $\mathfrak{q} \in D(A)$, then by the above paragraph $\mathfrak{q} \subset \bigcup_{x \neq 0} \operatorname{rad}(0 : x) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(0)} \mathfrak{p}$, so by prime avoidance we have $\mathfrak{q} \in \operatorname{Ass}(0)$.

4.13. Problem (nth symbolic powers)**.** i) Since $\mathfrak{p}A_\mathfrak{p}$ is a maximal ideal, $\mathfrak{p}^n A_\mathfrak{p}$ is $\mathfrak{p}A_\mathfrak{p}$-primary, so $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

ii) The only isolated prime of $\mathfrak{p}^n$ is $\mathfrak{p}$, because $\operatorname{rad}(\mathfrak{p}^n) = \mathfrak{p}$. The proof of theorem 4.4 then tells us that $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component.

iii) It is easy to show that $S_\mathfrak{p}(\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}) = S_\mathfrak{p}(\mathfrak{p}^{m+n})$, so they have the same $\mathfrak{p}$-primary components.

iv) This is obvious by ii).

4.14. Problem. It suffices to show that $\mathfrak{p} = (\mathfrak{a} : x)$ is prime. Suppose $yz \in \mathfrak{p}$, then $xyz \in \mathfrak{a}$. If $y \notin \mathfrak{p}$, then $xy \notin \mathfrak{a}$, so $(\mathfrak{a} : xy) \supset (\mathfrak{a} : x)$ implies $(\mathfrak{a} : xy) = (\mathfrak{a} : x)$. Since $z \in (\mathfrak{a} : xy)$, $z \in \mathfrak{p}$ as well.

4.17. Problem. We first show the following claim: let $\mathfrak{a}$ be an ideal, $\mathfrak{p}$ a minimal prime ideal containing $\mathfrak{a}$, then $\mathfrak{q} = S_{\mathfrak{p}}(\mathfrak{a})$ is $\mathfrak{p}$-primary, and if $\mathfrak{q} = (\mathfrak{a} : x)$ then $\mathfrak{a} = \mathfrak{q} \cap (\mathfrak{a}, x)$. The first clause of the claim follows from problem 4.11 by reducing mod $\mathfrak{a}$. For the second clause, suppose $bx \in \mathfrak{q}$ for some $b \in A$, then since $x \notin \mathfrak{p}$, $b \in \mathfrak{q}$, so $bx \in \mathfrak{a}$. This proves the claim.

Now, fix an ideal $\mathfrak{a}_0$. From the claim, we may choose $\mathfrak{a}_0 = \mathfrak{q}_1 \cap (\mathfrak{a}_0, x_0)$ for some $\mathfrak{q}_1 = S_{\mathfrak{p}_1}(\mathfrak{a}_0) = (\mathfrak{a}_0 : x_0)$ and $x_0 \notin \mathfrak{p}_1$. Choose $\mathfrak{a}_1$ maximal such that $\mathfrak{a}_0 = \mathfrak{a}_1 \cap \mathfrak{q}_1$ and $x_0 \in \mathfrak{a}_1$. Repeating the above procedure, we may choose $\mathfrak{a}_1 = \mathfrak{q}_2 \cap (\mathfrak{a}_1, x_1)$ where $\mathfrak{q}_2 = S_{\mathfrak{p}_2}(\mathfrak{a}_1) = (\mathfrak{a}_1 : x_1)$ and $x_1 \notin \mathfrak{p}_2$. Choose $\mathfrak{a}_2$ maximal such that $\mathfrak{a}_2 \cap \mathfrak{q}_2 = \mathfrak{a}_1$ and $x_1 \in \mathfrak{a}_2$. Repeating this again, at each stage we have $\mathfrak{a}_0 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{a}_n$, $\mathfrak{a}_n \not\subset \mathfrak{q}_1, \ldots, \mathfrak{q}_n$, and $\mathfrak{a}_{n-1} \subsetneq \mathfrak{a}_n$.

Even though this does not necessarily terminate in finitely many steps, we can use transfinite induction. The successor step is the same as the one described above. For the limit step, we just take $\mathfrak{a}_\alpha$ to be the union of the $\mathfrak{a}_\beta$'s where $\beta < \alpha$. Then in fact at each stage we have

$$\mathfrak{a}_0 = \text{pr} \bigcap_{\beta \leq \alpha} \mathfrak{q}_\beta \cap \mathfrak{a}_\alpha.$$

Then consider an ordinal α such that $\alpha > |A|$, where we well-order A a priori. We must then have $\mathfrak{a}_\alpha = (1)$, at which point $\mathfrak{a}_0$ is expressed as the intersection of primary ideals $\mathfrak{q}_\beta$, $\beta < \alpha$.

4.18. Problem. i) $\implies$ ii): Suppose $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$, then we know that $S_{\mathfrak{p}}(\mathfrak{a}) = \bigcap_{\mathfrak{p}_i \subset \mathfrak{p}} \mathfrak{q}_i$. Clearly, we may choose $x \in A$ such that $x \notin \mathfrak{p}_i$ iff $\mathfrak{p}_i \subset \mathfrak{p}$. Then $S_{\mathfrak{p}}(\mathfrak{a}) = (\mathfrak{a} : x^n)$ for a sufficiently large power of x, by problem 4.15, so this verifies (L1). Problem 4.12 directly implies (L2) since $S_1(\mathfrak{a}) \supset S_2(\mathfrak{a}) \supset \ldots$.

ii) $\implies$ i): By problem 4.17 we express $\mathfrak{a} = \bigcap_\alpha \mathfrak{q}_\alpha$. Let $S_n = S_{\mathfrak{p}_1} \cap \cdots \cap S_{\mathfrak{p}_n}$. Then $S_n(\mathfrak{a}) = S_n(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{a}_n) = S_n(\mathfrak{q}_1) \cap \cdots \cap S_n(\mathfrak{q}_n) \cap S_n(\mathfrak{a}_n) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ since $\mathfrak{a}_n \notin \bigcup_{i=1}^n \mathfrak{p}_i$ by construction. Since $S_n(\mathfrak{a})$ stabilizes, we can use transfinite induction to show that $\mathfrak{q}_\alpha \supset \bigcap_{i=1}^n \mathfrak{q}_i$ for every ordinal $\alpha > n$, which then implies $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$.

4.19. Problem. Induct on n where the induction basis is obvious. For the inductive step, suppose WLOG $\mathfrak{p}_n$ is *minimal* among $\mathfrak{p}_i$. By inductive hypothesis there is a minimal primary decomposition $\mathfrak{a}' = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{n-1}$ where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. It suffices to find a $\mathfrak{p}_n$-primary ideal $\mathfrak{q}_n$ such that $\mathfrak{q}_n \not\supset \mathfrak{a}'$. Suppose otherwise, then $\mathfrak{a}' \subset S_{\mathfrak{p}_n}(0)$. In other words, $\bigcap_{i=1}^{n-1} S_{\mathfrak{p}_n}^{-1}(\mathfrak{q}_i) = 0$. But for every $\mathfrak{p}_i$, $\mathfrak{p}_i \not\subset \mathfrak{p}_n$ by minimality, so $S_{\mathfrak{p}_n}^{-1}(\mathfrak{q}_i) = S_{\mathfrak{p}_n}^{-1}(A)$, which is not the zero ring, so we get a contradiction.

5. Integral dependence and valuations

5.1. Proposition. *Let $A \subset B$ be a ring extension. The following are equivalent:*

(i) $x \in B$ is integral over A;
(ii) $A[x]$ is a finitely generated module over A.
(iii) $A[x]$ is contained in a subring $C \subset B$ that is f.g. as an A-module.
(iv) There is a faithful $A[x]$-module M such that M is f.g. over A.

Proof. The nontrivial part is iv) $\implies$ i). Consider M as an f.g. A-module, and consider the map $\phi : M \to M$ given by $m \mapsto xm$. By Cayley-Hamilton, ϕ satisfies a monic polynomial equation over A. Since M is faithful as an $A[x]$-module, x satisfies a monic polynomial equation over A. □

5.2. Corollary. *The elements in B integral over A forms a subring of B, called the integral closure of A in B.*

5.3. Corollary. *If B is integral over A and C is integral over B, then C is integral over A.*

In addition, integral dependence is preserved by passing to quotient rings and localizations. Even better, if C is the integral closure of A in B, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$, S being any multiplicatively closed subset of A.

5.4. Proposition. *Let $A \subset B$ be an integral extension of integral domains. Then A is a field iff B is a field.*

5.5. Corollary. *Let $A \subset B$ be an integral extension. Let $\mathfrak{q} \subset B$ be a prime ideal, and let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal in B iff $\mathfrak{p}$ is maximal in A.*

5.6. Corollary. *Let $A \subset B$ be an integral extension. Then no two distinct prime ideals lying over prime $\mathfrak{p} \in A$ can have a containment relation.*

PROOF. Localize at $S = A - \mathfrak{p}$, and use corollary 5.5. □

5.7. Theorem (Lying-over)**.** *Let $A \subset B$ be an integral extension, and $\mathfrak{p} \subset A$ a prime. Then there exists a prime $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

PROOF. Consider the contraction of a maximal ideal in $S^{-1}B$, $S = A - \mathfrak{p}$. □

5.8. Theorem (Going-up)**.** *Let $A \subset B$ be an integral extension. Suppose $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ is a chain of prime ideals. Then for any $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ respectively, it can be extended to a chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$, each lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.* □

An integral domain is said to be integrally closed if it is so as a subring of its field of fractions. Clearly, any UFD is integrally closed. Being integrally closed is a local property.

Define, for $\mathfrak{a} \subset A$ an ideal, the integral closure of $\mathfrak{a}$ in B to be the set of elements in B satisfying a monic polynomial equation with coefficients in $\mathfrak{a}$.

5.9. Proposition. *Let C be the integral closure of A in B, and let $\mathfrak{a} \subset A$ be an ideal. Then its integral closure in B is $\operatorname{rad}(\mathfrak{a}^e)$ where $\mathfrak{a}^e$ is the extension of the ideal in C.*

5.10. Corollary. *Let $A \subset B$ be integral domains, A integrally closed, $x \in B$ integral over an ideal $\mathfrak{a} \subset A$. Then x is algebraic over the quotient field K of A, and its minimal polynomial $t^n + a_1 t^{n-1} + \cdots + a_n$ satisfies $a_1, \ldots, a_n \in \operatorname{rad}(\mathfrak{a})$.*

PROOF. The conjugates of x are all integral over $\mathfrak{a}$ since they all satisfy the same integral equation over $\mathfrak{a}$. Since the a_i's are polynomials in the conjugates of x, they all belong to $\operatorname{rad}(\mathfrak{a}^e) = \operatorname{rad}(\mathfrak{a})$ since A is integrally closed. □

5.11. Theorem (Going-down)**.** *Let $A \subset B$ be an integral extension, such that A is integrally closed. Suppose $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ is a chain of prime ideals. Then for any $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ respectively, it can be extended to a chain $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$, each lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.*

PROOF. It suffices to show that given $\mathfrak{p}_1 \supset \mathfrak{p}_2$, with $\mathfrak{q}_1$ lying over $\mathfrak{p}_1$, there exists $\mathfrak{q}_2 \subset \mathfrak{q}_1$ lying over $\mathfrak{p}_2$. It then suffices to show that $\mathfrak{p}_2^{ec} = \mathfrak{p}_2$, where the extension and contraction are through $A \to B \to B_{\mathfrak{q}_1}$. To this end, suppose $x \in A$, $s \in B - \mathfrak{q}_1$, $y \in \mathfrak{p}_2 B$ such that $\frac{x}{1} = \frac{y}{s}$. Then $yt = xst$ for some $t \in B - \mathfrak{q}_1$. Replacing y with yt, and s with st, we may assume WLOG $t = 1$.

Since $y \in \mathfrak{p}_2 B$, y is integral over $\mathfrak{p}_2$, so it satisfies an equation $y^r + u_1 y^{r-1} + \cdots + u_r = 0$ where $u_i \in \mathfrak{p}_2$. Working in K, the quotient field of A, we have $s = yx^{-1}$, so

$$s^r + \frac{u_1}{x} s^{r-1} + \frac{u_2}{x^2} s^{r-2} + \cdots + \frac{u_r}{x^r} = 0.$$

But $s \in B$, so each $u_i/x^i = v_i \in A$. If $x \notin \mathfrak{p}_2$, then $v_i \in \mathfrak{p}_2$ for every i, so $s \in \mathfrak{p}_2 B \subset \mathfrak{p}_1 B \subset \mathfrak{q}_1$, a contradiction. Therefore, $x \in \mathfrak{p}_2$ as desired. □

5.12. Proposition. *Let A be an integrally closed domain, K its field of fractions, L/K a separable finite extension, B the integral closure of A in L. Then there exists a basis v_i of L/K such that $B \subseteq \sum A v_i$.*

PROOF. Consider an arbitrary basis of L/K, then each basis element can be multiplied by some element in A such that they lie in B. Call this basis $u_1, \ldots, u_n$. Consider the trace form $\operatorname{Tr}_{L/K} : L \times L \to K$, given by $(x, y) \mapsto \operatorname{Tr}_{L/K}(xy)$. This is nondegenerate by separability. So there exists a dual basis $v_1, \ldots, v_n \in L$ such that $\operatorname{Tr}(v_i u_j) = \delta_{ij}$. We claim this is the desired basis. Indeed, consider $x \in B$, and express $x = \sum_i x_i v_i$, then because $u_i \in B$, $x_i = \operatorname{Tr}(x u_i) \in A$. □

For an integral domain B and its field of fractions K, we say B is a valuation ring of K if for any nonzero $x \in K$, either $x \in B$ or $x^{-1} \in B$. Then B must be a local ring that is integrally closed (in K).

Let K be any field, Ω an algebraically closed field. Consider the set of pairs (A, f) where $A \subset K$ is a ring and $f : A \to \Omega$ is a homomorphism. Partially order this set so that $(A, f) \leq (A', f')$ iff $A \subset A'$ and $f = f'|_A$. Let (B, g) be a maximal element of this set.

5.13. Proposition. *B is a local ring with maximal ideal $\mathfrak{m} = \ker g$.*

5.14. Proposition. *Let $x \in K$, $x \neq 0$. Then either $\mathfrak{m}[x] \neq B[x]$ or $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.*

5.15. Theorem. *B is a valuation ring of K.*

Proof. Let nonzero $x \in K$, it suffices to show either $x \in B$ or $x^{-1} \in B$. By proposition 5.14 WLOG $\mathfrak{m}[x] \neq B[x]$. Then it is contained in some maximal ideal $\mathfrak{m}' \subset B' = B[x]$. We must have $\mathfrak{m}' \cap B = \mathfrak{m}$ since $\mathfrak{m}$ is maximal, so the inclusion $B \hookrightarrow B[x]$ induces a field extension $k = B/\mathfrak{m}$ to $k' = B'/\mathfrak{m}'$. Because $k' = k[x]$, it is a finite extension, so the induced embedding $\overline{g} : k \to \Omega$ (recall $\mathfrak{m} = \ker g$) extends to an embedding $k' \to \Omega$ since Ω is algebraically closed. This extends to a map $B' \to \Omega$, so by maximality, $B = B'$. Since $x \in B'$, $x \in B$, as desired. □

5.16. Corollary. *Let A be a subring of a field K. Then its integral closure is the intersection of all valuation rings of K containing A.*

5.17. Proposition. *Let $A \subset B$ be integral domains, B a finitely generated algebra over A. Let $v \in B$ nonzero. Then there exists $u \in A$ nonzero such that any map $f : A \to \Omega$, where Ω is algebraically closed and $f(u) \neq 0$, can be extended to a map $g : B \to \Omega$ where $g(v) \neq 0$.*

Proof. Inducting on the number of generators, we may suppose B is generated over A by one element x.

If x is transcendental, suppose $v = a_n x^n + \cdots + a_0$. Let $u = a_n$. Then for any $f : A \to \Omega$ where $f(a) \neq 0$, there must exist $\omega \in \Omega$ such that $f(a_n)\omega^n + \cdots + f(a_0) \neq 0$. Extend f to $g : B \to \Omega$ by mapping x to ω.

If x is algebraic, then so is v^{-1} (over $K = \mathrm{Frac}(A)$). So we have equations

$$a_0 x^m + \cdots + a_m = 0, \quad a_0' v^{-n} + \cdots + a_n' = 0$$

of least degrees, for $a_i, a_i' \in A$. Let $u = a_0 a_0'$, and consider $f : A \to \Omega$ such that $f(u) \neq 0$. We easily extend this to $f_1 : A[u^{-1}] \to \Omega$, and now both x and v^{-1} are integral over $A[u^{-1}]$. Extend f_1 to $h : C \to \Omega$, C being a valuation ring containing $A[u^{-1}]$, then $x, v^{-1} \in C$. But since $x \in C$, C contains B, so $v \in B \subset C$ too. So $h(v) \neq 0$ since v is a unit, and taking $g : B \hookrightarrow C \xrightarrow{h} \Omega$ finishes the proof. □

5.18. Corollary (Hilbert's nullstellensatz)**.** *Let k be a field, B a finitely generated k-algebra that is a field. Then B is a finite extension of k.*

○

5.1. Problem. Let $\mathfrak{b} \in B$ be an ideal, $\mathfrak{q} \in V(\mathfrak{b})$ in $\operatorname{Spec} B$. Then $f^*(\mathfrak{q}) = \mathfrak{q}^c \supseteq \mathfrak{b}^c =: \mathfrak{a}$, so $f^*(\mathfrak{q}) \in V(a)$ in $\operatorname{Spec} A$. Conversely, suppose $\mathfrak{p} \supseteq \mathfrak{a}$. Because $f : A \to B$ is integral, so is $\overline{f} : A/\mathfrak{a} \to B/\mathfrak{b}$. So there exists a prime $\overline{\mathfrak{q}} \in B/\mathfrak{b}$ above $\overline{\mathfrak{p}} \in A/\mathfrak{a}$. Pull $\overline{\mathfrak{q}}$ back to $\mathfrak{q} \in B$, which is a prime ideal lying above $\mathfrak{p}$ that lies inside $V(\mathfrak{b})$.

5.2. Problem. Zorn's lemma.

5.8. Problem. ii) Let $B_1 = B[x_0]/fg(x_0)$. Then $fg(x_1)$ factors as $fg(x_1) = (x_1 - x_0)p_1(x_1)$ in $B_1[x_1]$, and $\deg p_1 = \deg(fg) - 1$. Let $B_2 = B_1[x_1]/p_1(x_1)$, and so on. We end up with a ring $B' \supset B$ such that $fg(x)$ splits into linear factors in $B'[x]$. The roots of fg are all integral over C, therefore so are the coefficients of f and g. But they also lie in B, so they must lie in C since C is integrally closed in B. (Note that this problem implies that for a ring extension $A \subset B$, for elements $a, b \in B$, if both $a + b$ and ab are integral over A, then so are a, b themselves.)

5.13. Problem. Suppose $\mathfrak{q}_1, \mathfrak{q}_2 \in P$. Let $x \in \mathfrak{q}_2$, then $\prod_{g \in G} gx \in A^G \subset \mathfrak{q}_1$, so there exists $g \in G$ such that $gx \in \mathfrak{q}_1$. Therefore, $\mathfrak{q}_2 \subset \bigcup_{g \in G} g\mathfrak{q}_1$, so there exists $g \in G$ such that $\mathfrak{q}_2 = g\mathfrak{q}_1$.

5.15. Problem. Any finite extension can be split into a separable extension followed by a purely inseparable one, so it suffices to prove the two cases separately.

If L/K is separable: consider a set of generators of L over K, and take the splitting field M of the minimal polynomials of these elements. Then M/K is a finite Galois extension since it is the splitting field of a separable polynomial. By problem 5.14, $A = B^{\mathrm{Gal}(M/K)}$. By problem 5.13, $\operatorname{Spec} B \to \operatorname{Spec} A$ has finite fibers.

If L/K is purely inseparable: let $p = \operatorname{char} K$. Then for any $x \in B$, there exists $n > 0$ such that $x^{p^n} \in K$, so $x^{p^n} \in A$ since A is integrally closed. Suppose prime ideal $\mathfrak{q} \in B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then $x \in \mathfrak{q}$

implies $x^{p^n} \in A \cap \mathfrak{q} = \mathfrak{p}$. Conversely, if $x^{p^n} \in \mathfrak{p} \subset \mathfrak{q}$, then $x \in \mathfrak{q}$ since $\mathfrak{q}$ is prime. Therefore, $\mathfrak{q}$ is uniquely characterized as the set of elements whose some p^nth power lies in $\mathfrak{p}$.

5.16. Problem (Noether's normalization lemma)**.** We only show the second part of the problem (geometric interpretation). Namely, if $k[y_1, \dots, y_r] \hookrightarrow A = k[x_1, \dots, x_n]/I$ is injective, the induced map of affine algebraic varieties $X \to k^r$ is surjective. A point in k^r corresponds to a morphism of algebras $k[y_1, \dots, y_r] \to k$. Since k is algebraically closed and A is integral over $k[y_1, \dots, y_r]$, this can be extended to a morphism $A \to k$, which corresponds to a point in X.

5.17. Problem (Hilbert's nullstellensatz)**.** We state several theorems that are associated with the name. Let k be an algebraically closed field.

A formulation of nullstellensatz: the map $k^n \to \operatorname{Spm} k[x_1, \dots, x_n]$ given by $(a_1, \dots, a_n) \mapsto (x_1 - a_1, \dots, x_n - a_n)$ is bijective. (Proof: using problem 5.18, suppose $\mathfrak{m} \subset k[x_1, \dots, x_n]$ is a maximal ideal. Then $k[x_1, \dots, x_n]/\mathfrak{m}$ is a finitely generated algebra over k that is a field, so it is a finite extension of k, so it is equal to k since k is algebraically closed. Suppose $a_1, \dots, a_n$ are the images of $x_1, \dots, x_n$ in k, then $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$.)

Weak nullstellensatz: if $\mathfrak{a} \neq (1)$ is an ideal in $k[x_1, \dots, x_n]$, then its associated variety $V(\mathfrak{a})$ is nonempty. (This is easily equivalent to the above statement.)

(Strong) nullstellensatz: if $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ is an ideal, then $I(V(\mathfrak{a})) = \operatorname{rad} \mathfrak{a}$.

5.18. Problem (Zariski's lemma)**.** There is an integral extension $k[y_1, \dots, y_r] \hookrightarrow B$. Since B is a field, so is $k[y_1, \dots, y_r]$. This implies $r = 0$.

5.22. Problem. Let $v \neq 0$ be an element of B. Since $A \subset B_v$ are integral domains and B_v is finitely generated over A, there exists an $s \neq 0$ in A such that, given any map $f : A \to \Omega$ where $f(s) \neq 0$ and Ω is algebraically closed, f can be extended to a map $g : B_v \to \Omega$.

Since $J(A) = 0$, there is a maximal ideal $\mathfrak{m} \subset A$ not containing s. Taking Ω to be the algebraic completion of $A/\mathfrak{m}$, we obtain a map $g : B_v \to \Omega$. In particular, $g(v) \neq 0$, so $\mathfrak{n} = \ker g \cap B$ does not contain v. It suffices then to show that $\mathfrak{n}$ is maximal in B. Observe that the integral extension $A \hookrightarrow B$ induces a map $A/\mathfrak{m} \to B/\mathfrak{n}$ that is also integral. Since the left side is a field, so is the right side.

5.23. Problem. iii) $\implies$ i): Suppose for contradiction that $\mathfrak{p} \subset A$ is not the intersection of maximal ideals. Replacing A with $A/\mathfrak{p}$, we have $J(A) \neq 0$ and it suffices to find a non-maximal prime $\mathfrak{q} \subset A$ that is not the intersection of primes strictly containing $\mathfrak{q}$. Choose $x \in J(A)$, pick $\mathfrak{q}$ to be the pullback of a maximal ideal in A_x. Then $\mathfrak{q}$ is a prime ideal such that $x \notin \mathfrak{q}$. Since x belongs to all maximal ideals in A, $\mathfrak{q}$ is not maximal. Furthermore, any prime ideal strictly containing $\mathfrak{q}$ must contain x, so we are done.

5.24. Problem. (i) If B is integral over A, consider a prime $\mathfrak{q} \subset B$. Then $\mathfrak{p} = \mathfrak{q}^c$ is a prime in A. Since A is Jacobson, $\mathfrak{p} = \bigcap_i \mathfrak{m}_i$ for maximal ideals $\mathfrak{m}_i \subset A$. By going-up, there exist maximal $\mathfrak{n}_i$ containing $\mathfrak{q}$ such that $\mathfrak{n}_i^c = \mathfrak{m}_i$. Then $(\bigcap_i \mathfrak{n}_i)^c = \bigcap_i \mathfrak{n}_i^c = a\mathfrak{p}$. Since $\mathfrak{q} \subseteq \bigcap_i \mathfrak{n}_i$ and both pull back to $\mathfrak{p}$, $\mathfrak{q} = \bigcap_i \mathfrak{n}_i$. Thus B is Jacobson.

(ii) If B is a finitely generated A-algebra, consider a prime $\mathfrak{q} \subset B$ and its pre-image $\mathfrak{p} = \mathfrak{q}^c \subset C$. Then $A/\mathfrak{p} \to B/\mathfrak{q}$ is an inclusion of integral domains, and $J(A/\mathfrak{p}) = 0$ because $\mathfrak{p}$ is the intersection of maximal ideals. By 5.22, $J(B/\mathfrak{q}) = 0$ as well, so $\mathfrak{q}$ is the intersection of maximal ideals. Thus B is Jacobson.

In particular, every finitely generated ring and every finitely generated algebra over a field is Jacobson.

6. Chain conditions

Example of a $\mathbb{Z}$-module satisfying dcc but not acc: take $G \subset \mathbb{Q}/\mathbb{Z}$ be elements whose order is a power of p. Then $G_0 \subset G_1 \subset G_2 \subset \dots$, where G_i consists of elements $x \in G$ such that $p^i x = 0$.

For any partially ordered set: acc $\iff$ every nonempty subset has a maximal element; dcc $\iff$ every nonempty subset has a minimal element.

6.1. Proposition. *Suppose* $0 \to M' \to M \to M'' \to 0$ *is exact. Then* M *is Noetherian (resp. Artinian) iff* M' *and* M'' *are both Noetherian (resp. Artinian).*

6.2. Proposition. *If* M *is a finitely generated module over a Noetherian (resp. Artinian) ring, then* M *is a Noetherian (resp. Artinian) module.*

A *composition series* for a module M is a chain

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

such that M_i/M_{i+1} is simple (has no nontrivial proper submodules).

6.3. Proposition. *If M has a composition series with finite length n, then every composition series of M has length n. Furthermore, every chain in M can be extended to a composition series.*

Proof. Let $l(M)$ be the *least* length of a composition series of M of finite length.

Suppose $N \subset M$, $N \neq M$. Consider a composition series $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ of length $n = l(M)$. Then $N = M_0 \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq M_n \cap N = 0$ is a composition series of N, so $l(N) \leq n$. If equality is achieved, then each $(M_i \cap N)/(M_{i+1} \cap N)$ is nontrivial. Since it is a submodule of M_i/M_{i+1}, it must be equal to M_i/M_{i+1}. We then see inductively that $M = N$, a contradiction. Therefore, $l(N) < l(M)$.

Now, consider any composition series $M = M_0 \supset \cdots \supset M_m = 0$. Then $l(M) > l(M_1) > \cdots > l(M_m) = 0$, so $l(M) \geq m$. But $l(M) \leq m$ by definition, so $l(M) = m$. □

6.4. Proposition. *M has finite length iff M is both Noetherian and Artinian.*

6.5. Theorem (Jordan-Hölder)**.** *Any two composition series of M have the same length, and the multiset of successive quotients M_i/M_{i+1} do not depend on the particular composition series chosen.*

6.6. Proposition. *Suppose $0 \to M' \to M \to M'' \to 0$ is exact, then $l(M) = l(M') + l(M'')$.*

6.7. Proposition. *Suppose $(0) = \mathfrak{m}_1 \ldots \mathfrak{m}_n$ for maximal ideals $\mathfrak{m}_i$ (not necessarily distinct), then A is Noetherian iff A is Artinian.*

Proof. $A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_n = 0$. Each successive quotient is a vector space over a field, so acc $\Longleftrightarrow$ dcc for each quotient. By induction, acc $\Longleftrightarrow$ dcc for A. □

7. Noetherian rings

7.1. Proposition. *Suppose A is a Noetherian ring.*

- *Let $B = A/\mathfrak{a}$ for some ideal $\mathfrak{a} \subset A$, then B is a Noetherian ring.*
- *Let B be a ring, $A \subset B$, such that B is f.g. as A-module. Then B is a Noetherian ring.*
- *Let $S \subset A$ be a multiplicative closed subset, then $S^{-1}A$ is a Noetherian ring.*
- *(Hilbert Basis Theorem) $A[x]$ is Noetherian. Corollary: let B be an associative algebra over A of finite type. Then B is Noetherian.*

7.2. Proposition. *Let $A \subseteq B \subseteq C$ be rings, A Noetherian, C f.g. as A-algebra. If C is either f.g. as B-module or integral over B (these two equivalent), then B is f.g. as A-algebra.*

We say an ideal $\mathfrak{a}$ is *irreducible* if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ implies $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

7.3. Proposition. *In a Noetherian ring, every ideal is a finite intersection of irreducible ideals.*

7.4. Proposition. *In a Noetherian ring, every irreducible ideal is primary.*

Proof. Passing to the quotient we assume WLOG 0 is irreducible. Suppose $xy = 0$, $x \neq 0$. Consider the chain $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \ldots$, then $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^{n+1})$ for some n. Then if $a \in (x) \cap (y^n)$, suppose $a = by^n$, then $by^{n+1} = ay = 0$, so $b \in \mathrm{Ann}(y^{n+1}) = \mathrm{Ann}(y^n)$, so $a = 0$. Therefore $(x) \cap (y^n) = 0$, so $y^n = 0$. We have shown that (0) is primary. □

Consequently, all results in section 4 applies to Noetherian rings.

7.5. Proposition. *In a Noetherian ring A, any ideal contains a power of its radical. In particular,* $\mathrm{rad}(A)$ *is nilpotent.*

7.6. Proposition. *Let $\mathfrak{a} \neq (1)$ be an ideal in a Noetherian ring. Then the prime ideals associated with $\mathfrak{a}$ are precisely prime ideals of the form $(\mathfrak{a} : x)$.*

Proof. Passing to the quotient, assume WLOG $\mathfrak{a} = 0$. Suppose $0 = \bigcup_j \mathfrak{q}_j$ is a minimal primary decomposition, with $\operatorname{rad}(\mathfrak{q}_j) = \mathfrak{p}_j$. Let $\mathfrak{a}_i = \bigcap_{j \neq i} \mathfrak{q}_j \neq 0$.

Take nonzero $x \in \mathfrak{a}_i$, then $(0 : x) = \bigcap_j (\mathfrak{q}_j : x) = (\mathfrak{q}_i : x) \subseteq \mathfrak{p}_i$. On the other hand, there exists n such that $\mathfrak{p}_i^n \subseteq \mathfrak{q}_i$, so $\mathfrak{a}_i \mathfrak{p}_i^n \subseteq \mathfrak{a} \cap \mathfrak{q}_i = 0$. Take the smallest such n, then there exists nonzero $x \in \mathfrak{a}_i \mathfrak{p}_i^{n-1}$, and $\mathfrak{p}_i x = 0$, so $\mathfrak{p}_i \subseteq (0 : x)$. So $(0 : x) = \mathfrak{p}_i$.

Conversely, if $(0 : x)$ is prime, then so is $\operatorname{rad}(0 : x)$, which is associated with a by Theorem 4.1. □

8. Artin rings

In what follows, the terms "Artin" and "Artinian" are used interchangeably.

8.1. Proposition. *Any prime ideal in an Artin ring is maximal.*

8.2. Proposition. *An Artinian ring has finitely many maximal ideals.*

8.3. Proposition. *Let A be Artinian, then $J(A) = \operatorname{rad}(A)$ is nilpotent.*

Proof. Suppose $\operatorname{rad}(A)^n = \operatorname{rad} A^{n+1} = \cdots = \mathfrak{a}$ is nonzero. Look at the minimal ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} \neq 0$. By minimality, $\mathfrak{b}$ is principal, and its generator x must satisfy $x\mathfrak{a} = (x)$. Thus there exists nonzero $y \in \mathfrak{a}$ such that $xy = x$, so $x = xy = \cdots = xy^N = 0$ since $y \in \operatorname{rad}(A)$ is nilpotent, so $\mathfrak{b} = 0$, contradiction! □

8.4. Theorem. *A is Artinian if and only if A is both Noetherian and* $\dim A = 0$.

8.5. Proposition. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then exactly one of the following is true: either $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all n, or $\mathfrak{m}^n = 0$ for some n and A is Artinian.*

8.6. Theorem. *An Artinian ring A is uniquely a finite product of Artin local rings.*

8.7. Proposition. *Let A be an Artinian local ring. Then the following are equivalent:*

- *Every ideal is principal;*
- *The maximal ideal is principal;*
- $\dim(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

In fact, if any of the above is true, then any ideal is a power of the maximal ideal.

9. Discrete valuation rings and Dedekind domains

9.1. Proposition. *Let A be a Noetherian domain of dimension 1. Then any ideal is uniquely written as a product of primary idelas whose radicals are all distinct.*

Proof. By primary decomposition, any ideal is the intersection of primary ideals. Since their radicals are all isolated, the primary ideals are unique. Since $\mathfrak{p}_i + \mathfrak{p}_j = (1)$, $\mathfrak{q}_i$ and $\mathfrak{q}_j$ are also pairwise coprime, so $\bigcap q_i = \prod \mathfrak{q}_i$. □

Let K be a field. A discrete valuation $v : K^* \to \mathbb{Z}$ is a surjective group homomorphism satisfying $v(x + y) \geq \min(v(x), v(y))$. The set $A = \{x \in K : v(x) \geq 0\}$ is then a valuation ring of K. By results in chapter 5, A is local and its maximal ideal is $\mathfrak{m} = \{x : v(x) > 0\}$. It is easy to see that $\mathfrak{m}$ is principal, and if we pick a generator $(x) = \mathfrak{m}$, then every nonzero ideal in A is of the form (x^n) for some $n \geq 0$. As such, A is a Noetherian local domain with dimension 1. Conversely, these are also characteristic of discrete valuation rings:

9.2. Proposition. *Let A be a Noetherian local domain of dimension 1. The following are equivalent:*

(i) *A is a DVR;*
(ii) *A is integrally closed (in K = field of fractions);*
(iii) $\mathfrak{m}$ *is principal;*
(iv) $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$*;*
(v) *Every nonzero ideal is a power of* $\mathfrak{m}$*;*
(vi) *There exists $x \in A$ such that very nonzero ideal is (x^n) for $n \geq 0$.*

Proof. (i) $\Longrightarrow$ (ii): suppose $x \in K$ satisfies $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for $a_i \in A$, then $nv(x) = v(x^n) \geq v(a_n) \geq 0$, so $v(x) \geq 0$.

(ii) $\Longrightarrow$ (iii): Pick any nonzero $a \in \mathfrak{m}$, then since A has dimension 1, (a) is $\mathfrak{m}$-primary. Since $\mathfrak{m}$ is finitely generated, there exists n such that $\mathfrak{m}^n \subseteq (a)$ and $\mathfrak{m}^{n-1} \not\subseteq (a)$. Pick $b \in \mathfrak{m}^{n-1}$ that does not belong in (a), and consider $a^{-1}b$. It is clear that $a^{-1}b \notin A$, since otherwise $b \in (a)$. On the other hand, $a^{-1}b\mathfrak{m} \subseteq A$ is an ideal. If $a^{-1}b\mathfrak{m} = A$, then $\mathfrak{m} = (ab^{-1})$ is principal, which is what we wanted. Otherwise, $a^{-1}b\mathfrak{m} \subseteq \mathfrak{m}$, so $\mathfrak{m}$ is a faithful $A[a^{-1}b]$-module that is finitely generated as an A-module, so $a^{-1}b$ is integral over A, hence belongs to A, which is a contradiction.

(iii) $\Longrightarrow$ (iv) is clear.

(iv) $\Longrightarrow$ (v): Suppose $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$. Consider an ideal $\mathfrak{a}$, then there exists n such that $\mathfrak{m}^n \subseteq \mathfrak{a}$. Consider the image $\overline{\mathfrak{a}}$ of $\mathfrak{a}$ in $A/\mathfrak{m}^n$, which is an Artinian local ring by proposition 8.5. In this ring, the image of $\overline{\mathfrak{m}}$ is nilpotent, so there exists m with $\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{m}}^m$ and $\overline{\mathfrak{a}} \not\subseteq \overline{\mathfrak{m}}^{m+1}$. Since $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$, $\overline{\mathfrak{m}}$ is principal, say $\overline{\mathfrak{m}} = (x)$. Then $yx^m \notin (x^{m+1})$ for some $y \in A/\mathfrak{m}^n$, so $y \notin (x) = \mathfrak{m}$, so y is a unit, so $x^m \in \overline{\mathfrak{a}}$, so $\overline{\mathfrak{a}} = \overline{\mathfrak{m}}^m$, so $\mathfrak{a}$ is a power of $\mathfrak{m}$.

(v) $\Longrightarrow$ (vi): since A is not Artinian, $\mathfrak{m}^n \neq \mathfrak{m}^{n-1}$ for any n. Pick $x \in \mathfrak{m}$, $x \notin \mathfrak{m}^2$. Suppose $(x) = \mathfrak{m}^n$, then $n = 1$, as desired.

(vi) $\Longrightarrow$ (i): since $(x^n) \neq (x^{n+1})$ for any n, we see that for any $a \in A$, there is a unique n such that $(a) = (x^n)$. Define $v : A \to \mathbb{Z}$ by mapping a to n, and extend this to K^* by $v(a/b) = v(a) - v(b)$. □

A Noetherian domain A with dimension one is a *Dedekind domain* if it is integrally closed. Equivalently, each $A_{\mathfrak{p}}$ is integrally closed, i.e. $A_{\mathfrak{p}}$ is a DVR. By proposition 9.2, this is also equivalent to saying that any primary ideal is a power of its radical. By proposition 9.1, this is also equivalent to saying that any ideal is uniquely factorized into the product of prime ideals.

Examples of Dedekind domains: any PID is a Dedekind domain, for A is a Noetherian domain with dimension one such that every localization $A_{\mathfrak{p}}$ is a PID (hence DVR by proposition 9.2). An important class of examples arise as rings of integers $\mathcal{O}_K$ of finite extensions $K/\mathbb{Q}$ (algebraic number fields). This is because $\mathcal{O}_K$ is a submodule of some $\mathbb{Z}^n$, and therefore is a Noetherian $\mathbb{Z}$-module and an integrally closed domain (as the integral closure of $\mathbb{Z}$ in K). To show it has dimension 1, consider any nonzero prime $\mathfrak{p} \subset \mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} \neq 0$, so it is maximal, so $\mathfrak{p}$ is maximal as well. In particular, in $\mathcal{O}_K$, ideals can be uniquely factorized into prime ideals.

A *fractional* ideal in an integral domain A is an A-submodule M of $K = \mathrm{Frac}(A)$ such that there exists nonzero $x \in A$ satisfying that $xM \subseteq A$. The set of $x \in K$ such that $xM \subseteq A$ is denoted $(A : M)$.

A submodule M of K is said to be *invertible* if there exists a submodule N of K such that $MN = A$. If M is invertible then its inverse N is necessarily equal to $(A : M)$, since $N \subseteq (A : M) = (A : M)(MN) \subseteq AN = N$. Then $M(A : M) = A$, so there exist $x_i \in M$, $y_i \in (A : M)$ such that $\sum x_i y_i = 1$, which implies that the x_i generate M as an A-module. Since M is finitely generated, it is a fractional ideal. The invertible ideals form a group with respect to multiplication.

9.3. Proposition. *Invertibility is a local property: for a fractional ideal M, the following are equivalent:*

(i) M is invertible;
(ii) M is finitely generated and each $M_{\mathfrak{p}}$ is invertible;
(iii) M is finitely generated and each $M_{\mathfrak{m}}$ is invertible.

Proof. (i) $\Longrightarrow$ (ii): $A_{\mathfrak{p}} = (M(A : M))_{\mathfrak{p}} = M_{\mathfrak{p}}(A : M)_{\mathfrak{p}}$. Since M is clearly finitely generated, $(A : M)_{\mathfrak{p}} = (A_{\mathfrak{p}} : M_{\mathfrak{p}})$, so $M_{\mathfrak{p}}(A_{\mathfrak{p}} : M_{\mathfrak{p}}) = A_{\mathfrak{p}}$, so $M_{\mathfrak{p}}$ is invertible.

(iii) $\Longrightarrow$ (i): Let $\mathfrak{a} = M(A : M) \subseteq A$. The inclusion $f : \mathfrak{a} \to A$, localized at each $\mathfrak{m}$, is bijective, so f is a bijection too. □

9.4. Proposition. *Let A be a local domain, then A is a DVR iff every nonzero fractional ideal is invertible.*

Proof. A is clearly Noetherian, so it suffices to show any ideal $\mathfrak{a}$ is a power of the maximal ideal $\mathfrak{m}$. Suppose $\mathfrak{m}\mathfrak{n} = 1$ for a fractional ideal $\mathfrak{n}$. Consider the maximal $\mathfrak{a}$ that is not a power of $\mathfrak{m}$. Then $\mathfrak{a} \subseteq \mathfrak{n}\mathfrak{a} \subseteq A$, and furthermore $\mathfrak{a} \neq \mathfrak{n}\mathfrak{a}$, since otherwise $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ and $\mathfrak{a} = 0$ by Nakayama. Therefore, by maximality, $\mathfrak{n}\mathfrak{a} = \mathfrak{m}^k$, so $\mathfrak{a} = \mathfrak{m}^{k+1}$, contradiction! □

The corresponding global result is:

9.5. Proposition. *Let A be an integral domain. Then A is a Dedekind domain iff every nonzero fractional ideal is invertible.*

Therefore, for a Dedekind domain A, the set of nonzero fractional ideals forms a group I, and I is free abelian with the nonzero prime ideals as generators.

There is an exact sequence of abelian groups

$$1 \to U \to K^* \xrightarrow{x \mapsto (x)} I \to H \to 1,$$

where U is the group of units in A, and $H = I/P$ is the ideal class group (fractional ideals quotient principal fractional ideals). For $A = \mathcal{O}_K$ rings of integers in algebraic number fields, H is finite and U is finitely generated. The torsion part of U is the subgroup W of roots of unities in K, and U/W is freely generated by r_1+r_2-1 elements, where r_1 is the number of real embeddings and $2r_2$ is the number of complex embeddings of K.

10. Completions

10.1. Proposition. *Suppose G is a topological group, and H is the intersection of all open neighborhoods of 0. Then $H = \overline{\{0\}}$ is a subgroup of G, and $H = 0$ if and only if G is Hausdorff.*

Define the completion $\widehat{G}$ using Cauchy sequences: a sequence (x_n) is Cauchy if for any open neighborhood U of 0, there exists N (dependent on U) such that $x_m - x_n \in U$ for all $m, n \geq N$. Then $\widehat{G}$ is the set of Cauchy sequences modulo equivalence. The natural map $\phi : G \to \widehat{G}$ has kernel precisely $H = \overline{\{0\}}$. The construction is functorial: for a continuous homomorphism $f : G \to H$, there is induced a natural continuous homomorphism $\widehat{f} : \widehat{G} \to \widehat{H}$. ($\widehat{G}$ is naturally a group, and it inherits a topology as an inverse limit as described below.)

Suppose G has a neighborhood basis $G = G_0 \supset G_1 \supset G_2 \supset \cdots$ given by *subgroups*. Then by looking at cosets, each G_i is both open and closed. Furthermore, $\widehat{G} = \varprojlim G/G_i$ since an equivalence class of Cauchy sequences corresponds exactly to a coherent system of elements of G/G_i. So $\widehat{G}$ inherits a topology as a subset of the infinite product of G/G_i as discrete spaces. This is the same topology as the one induced by the sequence of subgroups $\widehat{G} \supset \widehat{G_1} \supset \widehat{G_2} \supset \cdots$. Under this topology, the image of $f : G \to \widehat{G}$ is dense.

10.2. Proposition. *Let $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ be an exact sequence of inverse systems, then $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$ is exact. Moreover, if the inverse system A_n is surjective (the maps $A_{n+1} \to A_n$ are surjective), then $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$ is exact.*

(In general, $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to \varprojlim^1 A_n$ is exact, where $\varprojlim^1 A_n = \operatorname{coker} d$, where $d : \prod A_n \to \prod A_n$ by $a_n \mapsto a_n - \theta_{n+1}(a_{n+1})$, where $\theta_n : A_n \to A_{n-1}$.)

10.3. Corollary. *Let $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ be an exact sequence of groups. Let $\{G_n\}$ be a sequence of subgroups that define the topology on G. Let $G'_n = f^{-1}(G_n)$, $G''_n = g(G_n)$, then $0 \to \widehat{G'} \to \widehat{G} \to \widehat{G''} \to 0$ is exact.*

10.4. Corollary. *$\widehat{G_n}$ is a subgroup of $\widehat{G}$, and $\widehat{G}/\widehat{G_n} \cong G/G_n$.*

Proof. Take $G' = G_n$, $G'' = G/G_n$ in the above, then $\widehat{G''} = G''$ since it has the discrete topology. □

10.5. Corollary. *$\widehat{\widehat{G}} = \widehat{G}$.*

We say G is *complete* if $\phi : G \to \widehat{G}$ is an isomorphism; then the completion of G is complete. Complete implies Hausdorff. Given a commutative ring A and an ideal $\mathfrak{a}$, consider the $\mathfrak{a}$-*adic topology* generated by the neighborhood basis $\mathfrak{a}^n$. This is Hausdorff iff $\bigcap \mathfrak{a}^n = 0$. Similarly, for an A-module M, define the $\mathfrak{a}$-adic topology as generated by the neighborhood basis $\mathfrak{a}^n M$. Now, the completion $\widehat{M}$ is a topological $\widehat{A}$-module, and for any A-module homomorphism $f : M \to N$, induced is a continuous homomorphism $\widehat{f} : \widehat{M} \to \widehat{N}$.

Example. Let $A = k[x]$, $\mathfrak{a} = (x)$. Then $\widehat{A} = k[[x]]$.

Example. Let $A = \mathbb{Z}$, $\mathfrak{a} = (p)$. Then $\widehat{A} = \mathbb{Z}_p$, the p-adic integers.

For a filtration $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$, it is called an $\mathfrak{a}$-filtration if $\mathfrak{a} M_i \subseteq M_{i+1}$ for all i. It is called a stable $\mathfrak{a}$-filtration if $\mathfrak{a} M_i = M_{i+1}$ for all i large enough.

10.6. Lemma. *For any two stable $\mathfrak{a}$-filtrations M_i, M_i', there exist N such that $M_{i+N} \subseteq M_i'$ and $M_{i+N}' \subseteq M_i$.*

10.7. Proposition. *Let $A = \bigoplus_{n\geq 0} A_n$ be a graded ring. Then A is Noetherian iff A_0 is Noetherian and A is a f.g. algebra over A_0.*

Proof. $\Longleftarrow$ follows from Hilbert's basis theorem.

$\Longrightarrow$: Let $A_+ = \bigoplus_{n>0} A_n$, then A_+ is an ideal and $A/A_+ = A_0$. Therefore, A_0 is a Noetherian ring. Because A_+ is finitely generated as an ideal, it is finitely generated as an A_0-module, hence Noetherian as an A_0-module. Therefore, the A_n's, as A_0-submodules, are finitely generated. Line up the generators in ascending order of n, and consider the ideal (in A) generated by the first k generators. This ascending chain is eventually constant, which means that the ideal A_+ is finitely generated by homogeneous elements. Call them $x_1, \dots, x_s$, with degrees $k_1, \dots, k_s$.

Let A' be the A_0-algebra generated by x_i. We show by induction that $A_n \subseteq A'$. The induction basis is trivial. Suppose $A_0, \dots, A_n \subseteq A'$. Let $x \in A_{n+1} \subset A_+$, so that $x = \sum a_i x_i$ where $\deg a_i = n + 1 - k_i$. Since $n + 1 - k_i \leq n$, $a_i \in A'$, so $x \in A'$ as well. This finishes the proof. □

Let A be *any* ring, $\mathfrak{a}$ an ideal, then $A^* = \bigoplus_{n\geq 0} \mathfrak{a}^n$ is a graded ring. Let M be an A-module, M_n be an $\mathfrak{a}$-filtration, then $M^* = \bigoplus_{n\geq 0} M_n$ is a graded A^*-module. If A is Noetherian, then so is A^*, by the proposition above.

10.8. Proposition. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$, M f.g. A-module, and (M_n) an $\mathfrak{a}$-filtration of M. Then M^* is f.g. as A^*-module iff (M_n) is stable.*

Proof. Let $M_n^* = M_0 \oplus M_1 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots$ be the A^*-submodule generated by $\bigoplus_{i=0}^n M_i$. Since M is f.g. over a Noetherian ring, it is Noetherian, so each M_i is a finitely generated A-module. Therefore, M_n^* is a finitely generated A^*-module.

If M^* is finitely generated, then it is a Noetherian A^*-module, so the M_n^* is eventually constant, i.e. M_n is a stable filtration. Conversely, if M_n^* is eventually constant, since $M^* = \bigcup_n M_n^*$, it is finitely generated as an A^*-module. □

10.9. Corollary. *Let A be Noetherian, $\mathfrak{a} \subset A$, M f.g. A-module, (M_n) $\mathfrak{a}$-stable filtration. Suppose $M' \subseteq M$ is a submodule, then $(M' \cap M_n)$ is a $\mathfrak{a}$-stable filtration of M'.*

10.10. Corollary (Artin-Rees)**.** *Let A be Noetherian, M f.g. A-module, M' submodule, then there exists k such that for all $n \geq k$, $a^n M \cap M' = a^{n-k}(a^k M \cap M')$.*

10.11. Corollary. *Let A be Noetherian, M f.g. A-module, M' submodule, then the $\mathfrak{a}$-stable filtrations $\mathfrak{a}^n M'$ and $\mathfrak{a}^n M \cap M'$ have bounded difference, and therefore determine the same $\mathfrak{a}$-adic topology on M'.*

10.12. Proposition (Completion is exact for finitely generated over Noetherian)**.** *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of f.g. modules over an Noetherian ring A. Let $\mathfrak{a} \subset A$ be an ideal, then the sequence of $\mathfrak{a}$-adic completions $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$ is exact.*

Proof. This follows from corollary 10.3 and 10.11. □

10.13. Proposition. *Let A be a ring, M a finitely generated A-module, then the natural linear map $\phi : \widehat{A} \otimes_A M \to \widehat{M}$ is surjective. Furthermore, if A is Noetherian, then ϕ is bijective.*

Proof. First, clearly $\widehat{A^n} \cong \widehat{A}^n$, so we take an exact sequence $0 \to N \to F \to M \to 0$ where F is a f.g. free A-module. Then $\widehat{A} \otimes_A N \to \widehat{A} \otimes_A F \to \widehat{A} \otimes_A M \to 0$ is exact. Furthermore we get a (not necessarily exact) sequence $0 \to \widehat{N} \to \widehat{F} \to \widehat{M} \to 0$. Since $\widehat{F} \to \widehat{M}$ is surjective and $\widehat{F} \cong \widehat{A} \otimes_A F$, we conclude that ϕ is surjective.

If A is Noetherian, then $0 \to \widehat{N} \to \widehat{F} \to \widehat{M} \to 0$ is exact, and in addition N is finitely generated, so $\widehat{A} \otimes_A N \to \widehat{N}$ is surjective. This is enough to show that ϕ is injective. □

Recall that to show an A-module K is flat, it is enough to have $K \otimes_A M \to K \otimes_A N$ for injective maps $M \to N$ for *finitely generated* M, N. Consequently, if A is Noetherian, $\widehat{A}$ is a flat A-algebra.

10.14. Proposition. *Let A be a Noetherian ring, $\widehat{A}$ its $\mathfrak{a}$-adic completion, then:*

(i) $\widehat{\mathfrak{a}} = \widehat{A}\mathfrak{a} = \widehat{A} \otimes_A \mathfrak{a}$. *($\widehat{A}\mathfrak{a}$ is the ideal in $\widehat{A}$ generated by the image of $\mathfrak{a}$.)*

(ii) $\widehat{\mathfrak{a}}^n = \widehat{\mathfrak{a}^n}$.
(iii) $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \widehat{\mathfrak{a}}^n/\widehat{\mathfrak{a}}^{n+1}$.
(iv) $\widehat{\mathfrak{a}} \subseteq J(\widehat{A})$.

Proof. (i) $\widehat{A} \otimes_A \mathfrak{a} \to \widehat{\mathfrak{a}}$ is an isomorphism, and its image is $\widehat{A}\mathfrak{a}$.

(ii) $\widehat{\mathfrak{a}}^n = (\widehat{A}\mathfrak{a})^n = \widehat{A}\mathfrak{a}^n = \widehat{\mathfrak{a}^n}$.

(iii) Take the completion of the exact sequence $0 \to \mathfrak{a}^{n+1} \to \mathfrak{a}^n \to \mathfrak{a}^n/\mathfrak{a}^{n+1} \to 0$.

(iv) Since $\widehat{\mathfrak{a}}^n = \widehat{\mathfrak{a}^n}$, $\widehat{A}$ is complete under the $\widehat{\mathfrak{a}}$-adic topology. Therefore, for any $x \in \widehat{\mathfrak{a}}$, $(1-x)^{-1} = 1 + x + x^2 + \dots$ converges in $\widehat{A}$. □

10.15. Corollary. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Then $\widehat{A}$ is a local ring with $\widehat{\mathfrak{m}}$ its maximal ideal.*

Proof. Because $\widehat{A}/\widehat{\mathfrak{m}} \cong A/\mathfrak{m}$ is a field, $\widehat{\mathfrak{m}}$ is a maximal ideal. Because it is contained in $J(\widehat{A})$, it is the unique maximal ideal. □

10.16. Theorem (Krull's intersection theorem)**.** *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal, M a finitely generated A-module. Then*

$$E = \bigcap_{n \geq 1} \mathfrak{a}^n M = \{x \in M : \exists y \in \mathfrak{a}, x(1-y) = 0\}.$$

Proof. We know E is finitely generated. By Artin-Rees lemma, there exists k such that $E = \mathfrak{a}^{k+1}M \cap E = \mathfrak{a}(\mathfrak{a}^k M \cap E) = \mathfrak{a}E$, so by Nakayama there exists $a \in \mathfrak{a}$ such that $1-a$ annihilates all elements of E. The converse is trivial. □

This means that $A \to \widehat{A}$ and $A \to S^{-1}A$ have the same kernel, where $S = 1 + \mathfrak{a}$. Furthermore, $\phi : A \to \widehat{A}$ maps every element of S to a unit (proposition 10.14). Therefore, there is a uniquely induced *injective* map $S^{-1}A \to \widehat{A}$.

10.17. Corollary. *Let A be a Noetherian domain, $\mathfrak{a} \neq (1)$ an ideal, then $\bigcap_{n\geq 1} \mathfrak{a}^n = 0$.*

Counterexample for A not Noetherian: let A be the ring of C^∞ functions on $\mathbb{R}$, $\mathfrak{a}$ the maximal ideal of functions vanishing at 0. Then $\bigcap_{n\geq 1} \mathfrak{a}^n$ consists of $f \in A$ such that $f(0), f'(0), f''(0), \dots$ all equal 0. On the other hand, x is annihilated by an element in $1 + \mathfrak{a}$ iff $x = 0$ in some open neighborhood of 0. These two sets are clearly not the same (e^{-1/x^2}).

10.18. Corollary. *Let A be a Noetherian ring, $\mathfrak{a} \subseteq J(A)$, and M finitely generated A-module. Then the $\mathfrak{a}$-adic topology on M is Hausdorff.*

10.19. Corollary. *Let A be a Noetherian ring, $\mathfrak{p}$ a prime ideal of A, then the intersection of all $\mathfrak{p}$-primary ideals of A is* $\ker(A \to A_{\mathfrak{p}})$.

Given a ring A and an ideal $\mathfrak{a}$, define its associated graded ring

$$\mathrm{gr}_{\mathfrak{a}}(A) = G(A) = \bigoplus_{n\geq 0} \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

Given an A-module M and a $\mathfrak{a}$-filtration M_n, define

$$\mathrm{gr}(M) = G(M) = \bigoplus_{n\geq 0} M_n/M_{n+1}.$$

It is a graded $G(A)$-ring.

10.20. Proposition. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$ an ideal. Then*

(i) $G_{\mathfrak{a}}(A)$ *is Noetherian.*
(ii) $G_{\widehat{\mathfrak{a}}}(\widehat{A}) \cong G_{\mathfrak{a}}(A)$ *as graded rings.*
(iii) If (M_n) is a stable $\mathfrak{a}$-filtration of a finitely generated A-module M, then $G(M)$ is a finitely generated graded $G_{\mathfrak{a}}(A)$-module.

We work towards proving that the $\mathfrak{a}$-adic completion of a Noetherian ring is Noetherian.

10.21. Proposition. *Let $\phi : (A_n) \to (B_n)$ be a homomorphism of filtered groups. Let $G(\phi) : G(A) \to G(B)$, $\widehat{\phi} : \widehat{A} \to \widehat{B}$ be the induced maps. Then if $G(\phi)$ is injective (resp. surjective), so is $\widehat{\phi}$.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_n/A_{n+1} \arrow[r] \arrow[d, "\alpha"] & A/A_{n+1} \arrow[r] \arrow[d, "\beta"] & A/A_n \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & B_n/B_{n+1} \arrow[r] & B/B_{n+1} \arrow[r] & B/B_n \arrow[r] & 0
\end{tikzcd}$$

Because the rows are exact, we can apply snake lemma to obtain an exact sequence

$$0 \to \ker \alpha \to \ker \beta \to \ker \gamma \to \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma \to 0.$$

If $G(\phi)$ is injective, then by injection so is β for all n, so since inverse limits preserve injectivity, $\widehat{\phi}$ is injective as well. Similarly for surjectivity. □

10.22. Proposition. *Let A be a complete ring in the $\mathfrak{a}$-adic topology, M an A-module, (M_n) an $\mathfrak{a}$-filtration such that $\bigcap_n M_n = 0$. If $G(M)$ is a finitely generated $G(A)$-module, then M is a finitely generated A-module.*

Proof. Pick a finite set of (WLOG homogeneous) generators of $G(M)$ over $G(A)$, say $\overline{x_i} \in M_{n_i}/M_{n_i+1}$. For each i, construct a filtered A-module $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots$ where $A_0 = \cdots = A_{n_i} = A$ and $A_{n_i+k} = \mathfrak{a}^k$. Direct sum these together, we obtain a map of filtered A-modules $\phi : F \to M$ where F is free. This induces $G(\phi) : G(F) \to G(M)$, which is surjective by construction. By the above proposition, $\widehat{\phi} : \widehat{F} \to \widehat{M}$ is surjective as well. Consider the diagram

$$\begin{tikzcd}
F \arrow[r] \arrow[d] & M \arrow[d] \\
\widehat{F} \arrow[r] & \widehat{M}
\end{tikzcd}$$

The bottom map is surjective, the vertical map on the right is injective, and the vertical map on the left is an isomorphism. Therefore, $F \to M$ is surjective, and M is finitely generated as an A-module. □

10.23. Corollary. *Let A be a complete ring in the $\mathfrak{a}$-adic topology, M an A-module, (M_n) an $\mathfrak{a}$-filtration such that $\bigcap_n M_n = 0$. If $G(M)$ is a Noetherian $G(A)$-module, then M is a Noetherian A-module.*

Proof. Let $M' \subset M$ be a submodule. Then $(M' \cap M_n)$ is an $\mathfrak{a}$-filtration such that $\bigcap_n (M' \cap M_n) = 0$. Since $G(M') \subset G(M)$ is a submodule of a Noetherian module, it is finitely generated, so M' is a finitely generated A-module. □

10.24. Theorem. *Let A be a Noetherian ring, $\mathfrak{a} \subset A$ an ideal, then the $\mathfrak{a}$-adic completion $\widehat{A}$ is Noetherian.*

Proof. Since A is Noetherian, so is $G_{\mathfrak{a}}(A) = G_{\widehat{\mathfrak{a}}}(\widehat{A})$. Viewing $\widehat{A}$ as a module over itself, and applying the above corollary ($\widehat{A}$ is complete), implies that $\widehat{A}$ is Noetherian. □

For example, $A[[x_1, \dots, x_n]]$ is Noetherian whenever A is Noetherian.

11. Dimension theory

Our first notion of dimension applies to finitely generated graded modules $M = \bigoplus_n M_n$ over Noetherian graded rings $A = \bigoplus_n A_n$. We know A can be viewed as a finitely generated algebra over A_0, say generated by homogeneous elements $x_1, \dots, x_s$ of degrees $k_1, \dots, k_s$. In addition, it is clear that each M_n is finitely generated as an A_0-module.

Let λ be a $\mathbb{Z}$-valued additive function on the class of all finitely generated A_0-modules. Define the Poincaré series

$$P(M, t) = \sum_{n \geq 0} \lambda(M_n) t^n \in \mathbb{Z}[[t]].$$

11.1. Theorem. *There exists $f(t) \in \mathbb{Z}[t]$ such that*

$$P(M, t) = \frac{f(t)}{(1 - t^{k_1})(1 - t^{k_2}) \dots (1 - t^{k_s})}.$$

Proof. Induct on s by considering the "multiplication by x_s" map on M. □

Denote by $d(M)$ the order of the pole of $P(M,t)$ at 1. In particular, taking $M = A$, we arrive at the first notion of "dimension" of A.

11.2. Corollary. *If all $k_i = 1$, then $\lambda(M_n)$ is a polynomial in n of degree $d(M) - 1$ for all n large enough. (This is the Hilbert polynomial of M.)*

11.3. Proposition. *If $x \in A$ is not a zero divisor in M, then $d(M/xM) = d(M) - 1$.*

When A_0 is Artinian, any f.g. module M over A_0 has finite length, so we could take λ to be ℓ, the length function. For example, when $A = k[x_1, \ldots, x_s]$, $\ell(A_n) = \binom{n+s-1}{s-1}$, so $P(A,t) = (1-t)^{-s}$, so $d(A) = s$ (as expected).

Using this, we may define the dimension of a Noetherian local ring.

11.4. Proposition. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal, M a finitely generated A-module, and (M_n) a stable $\mathfrak{q}$-filtration of M. Then:*

(i) M/M_n is of finite length;

(ii) For all sufficiently large n, $\ell(M/M_n)$ is a polynomial $g(n)$ in n of degree at most the number of generators of $\mathfrak{q}$;

(iii) The degree and leading coefficient of g depends only on M and $\mathfrak{q}$ and not on the filtration chosen.

Proof. □

CHAPTER 4

Homological Algebra

CHAPTER 5

Algebraic Number Theory

These notes loosely follow what was covered in the one-year graduate number theory sequence at MIT. 18.785 was taught in fall 2022 by Bjorn Poonen; 18.786 in spring 2023 by Andrew Sutherland. I have included additional topics in the canon, such as Tate's thesis and modular forms. All mistakes are the author's own.

1. Algebra preliminaries

1.1. Absolute values.

1.1.1. Definition. A (real-valued) *absolute value* on a field k is a map $|\ |: k \to \mathbb{R}_{\geq 0}$ such that:

- $|x| = 0 \iff x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$ (triangle inequality).

If the stronger condition that $|x+y| \leq \max(|x|, |y|)$ is satisfied, the absolute value is called *nonarchimedean*; otherwise it is *archimedean*. Note the spelling of the word *archimedean*.

1.1.2. Example. Examples of absolute values:

- The usual absolute value $|\ |$ on $\mathbb{C}$, and the inherited absolute values on $\mathbb{R}$, $\mathbb{Q}$.
- The trivial absolute value on any field: $|x| = 1$ for $x \neq 0$. This is often implicitly excluded from consideration, to little detriment.
- The p-adic absolute value on $\mathbb{Q}$: $|x|_p = p^{-v_p(x)}$.

An absolute value induces a metric on k by $d(x, y) = |x - y|$, which then induces a topology (generated by the open balls). Under this topology, it is easy to verify that k is a topological field.

1.1.3. Definition. Two absolute values on k are *equivalent* if they induce the same topology.

1.1.4. Proposition. *Two absolute values $|\ |_1$ and $|\ |_2$ are equivalent if and only if $|\ |_2 = |\ |_1^s$ for some real $s > 0$.*

Proof. Consider the image of the homomorphism $f : k^* \to \mathbb{R}^2$ by $x \mapsto (\log |x|_1, \log |x|_2)$.

Case 1: the image does not intersect the second quadrant. Then it must be a subset of a line with positive slope, and therefore $|\ |_2 = |\ |_1^s$ for some positive s. Since these induce the same open balls, they have the same topology as well. So in this case both statements are true.

Case 2: the image intersects the second quadrant. Then there exists $x \in k$ such that $|x|_1 < 1$ and $|x|_2 > 1$ (without loss of generality, both absolute values are nontrivial). In this case, the sequence $x, x^2, x^3, \ldots$ converges in the first topology but diverges in the second, so the two absolute values induce different topologies. So in this case both statements are false. □

1.1.5. Corollary. *If two absolute values $|\ |_1$ and $|\ |_2$ on k are inequivalent, then there exists $x \in k$ such that $|x|_1 < 1$ and $|x|_2 > 1$.*

1.1.6. Proposition. *An absolute value $|\ |$ is nonarchimedean iff there exists a constant C such that $|n| \leq C$ for all positive integers n. In fact, this C is then easily seen to be 1.*

Proof. ($\Longrightarrow$) is easy. ($\Longleftarrow$): say $x, y \in k$, $|x| \leq |y|$. Then

$$|x + y|^n = |(x + y)^n| = \left|\sum_i \binom{n}{i} x^i y^{n-i}\right| \leq C(|x|^n + |x|^{n-1}|y| + \cdots + |y|^n) \leq Cn|y|^n.$$

Taking $n \to \infty$, we obtain $|x + y| \leq |y| = \max(|x|, |y|)$. □

1.1.7. Corollary. *In a field of positive characteristic, every absolute value is nonarchimedean.*

1.1.8. Theorem (weak approximation theorem)**.** *Let k be a field, and let $| \ |_1, \dots, | \ |_n$ be pairwise inequivalent nontrivial absolute values on k. Let $a_1, \dots, a_n \in k$, and $\varepsilon > 0$. Then there exists $x \in k$ such that $|x - a_i|_i < \varepsilon$ for each $i = 1, \dots, n$.*

Proof. First, we find z such that $|z|_1 > 1$ and $|z|_2, \dots, |z|_n < 1$. The induction basis $n = 2$ follows from [1.1.5]. Suppose we have found z such that $|z|_1 > 1$ and $|z|_2, \dots, |z|_n < 1$. If $|z|_{n+1} \leq 1$ we are already done, so suppose $|z|_{n+1} > 1$. Then as $m \to \infty$, $\left|\frac{z^m}{1+z^m}\right|_1, \left|\frac{z^m}{1+z^m}\right|_{n+1} \to 1$, whereas $\left|\frac{z^m}{1+z^m}\right|_2, \dots, \left|\frac{z^m}{1+z^m}\right|_n \to 0$. Take y such that $|y|_1 > 1$ and $|y|_{n+1} < 1$, then $\frac{yz^m}{1+z^m}$ satisfies the induction step for sufficiently large m.

Next, we solve the case $a_1 \neq 0$, $a_2, \dots, a_n = 0$. This amounts to finding y such that $|y-1|_1, |y|_2, \dots, |y|_n$ are all arbitrarily small. Take z as above, and consider $y = \frac{z^m}{1+z^m}$ once again.

Finally, we find y_i replacing a_1 with each nonzero a_i, and add them all together. This element satisfies the desired approximation. □

1.1.9. Theorem (Ostrowski)**.** *The only nontrivial absolute values on $\mathbb{Q}$ are either $| \ |_\infty^e$ for $0 < e \leq 1$, or $| \ |_p^e$ for some prime p and $e > 0$.*

Proof. Divide into the archimedean and nonarchimedean cases.

Case 1: there exists a positive integer b with $|b| > 1$. Say $|b| = b^\alpha$. For any positive integer n, write $n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_0$, where $a_0, \dots, a_k \in \{0, \dots, b-1\}$. Let $C = \max_{1 \leq m \leq b-1} |m|/m^\alpha$. Then $|n| \leq |a_k| b^{\alpha k} + |a_{k-1}| b^{\alpha(k-1)} + \dots + |a_0| \leq C(a_k^\alpha b^{\alpha k} + \dots + a_0^\alpha) \leq C(a_k b^k + \dots + a_0)^\alpha = Cn^\alpha$. Then $|n|^m = |n^m| \leq Cn^{m\alpha}$, so taking $m \to \infty$ we obtain $|n| \leq n^\alpha$. On the other hand, for any positive integer n, take k such that $b^k \leq n \leq b^{k+1}$. Then $|n| \geq b^{\alpha(k+1)} - (b^{k+1} - n)^\alpha \geq b^{\alpha k}(b^\alpha - (b-1)^\alpha) = Cn^\alpha$ for a fixed C not depending on n, so similar to above we obtain $|n| \geq n^\alpha$. This means $|n| = n^\alpha$, so $|x| = x^\alpha$ for all $x \in \mathbb{Q}^\times$, so the absolute value is equivalent to $| \ |_\infty$. In order for the triangle inequality to hold, it must be $| \ |_\infty^e$ for $0 < e \leq 1$.

Case 2: $|n| \leq 1$ for all integers n. Then by [1.1.6], $| \ |$ is nonarchimedean. Consider

$$\mathfrak{p} = \{n \in \mathbb{Z} : |n| < 1\}.$$

Then $x, y \in \mathfrak{p} \implies |x+y| \leq \max(|x|, |y|) < 1$, so $\mathfrak{p}$ is an ideal. Furthermore it is a prime ideal, since $|xy| < 1 \implies$ either $|x| < 1$ or $|y| < 1$, and $1 \notin \mathfrak{p}$. Therefore, there exists a prime p such that $|n| = 1$ for any integer n coprime to p, and $|p| = p^{-e} < 1$ for some $e > 0$. Since $| \ |$ is multiplicative, it has to be $| \ |_p^e$. □

1.1.10. Theorem (Ostrowski's theorem for function fields)**.** *Let k be any field. The only nontrivial absolute values on $k(t)$ that restrict to the trivial absolute value on k are either $| \ |_{\infty,c}$ or $| \ |_{\pi,c}$, where π is a monic irreducible polynomial in $k[t]$.*

Here, as usual, $|f|_{\infty,c} = c^{-\deg f}$ and $|f|_{\pi,c} = c^{v_\pi(f)}$.

Proof. (TODO) □

1.2. Valuations.

1.2.1. Definition. A (real-valued) *valuation* on a field k is a homomorphism $v : k^* \to \mathbb{R}$ such that

$$v(x+y) \geq \min(v(x), v(y)).$$

We usually extend this to a map on the whole k by the convention $v(0) = \infty$.

If v is a valuation, $c \in (0,1)$, then $|x| = c^{v(x)}$ is a nonarchimedean absolute value. The image of v is called the *value group*. Let $A = \{x \in k : v(x) \geq 0\}$, then A is called a *valuation ring*. If the valuation group is discrete (which can then be scaled to $\mathbb{Z}$), then v is called a *discrete valuation* and A is a *discrete valuation ring*. Note that by definition, a discrete valuation will surject onto $\mathbb{Z}$.

More generally, in the same way, one could define a valuation with values in any totally ordered abelian group $(\Gamma, +, \leq)$, and extend this to $\Gamma \cup \{\infty\}$ with the usual addition and size convention for ∞.

1.2.2. Definition. Let A be an integral domain, and K its field of fractions. It is a *valuation ring* (of K) if any of the following equivalent conditions hold:

(1) For any $x \in K$, either $x \in A$ or $x^{-1} \in A$ (or both).

(2) There exists a totally ordered abelian group $(\Gamma, +, \leq)$, and a Γ-valued valuation $v : K^\times \to \Gamma$, such that $A = \{x \in K : v(x) \geq 0\}$.

Proof. (1) $\implies$ (2): Let $\Gamma = K^\times/A^\times$. Consider the projection $v : K^\times \to \Gamma$. Multiplicatively, Γ is a totally ordered abelian group under the relation $v(x) \geq v(y) \iff xy^{-1} \in A$. Then v is a valuation, and $A = \{x \in K : v(x) \geq v(1)\}$.

The converse is easy. □

1.2.3. Proposition. *Let A be a valuation ring of $K = \operatorname{Frac}(A)$. Then:*

- *A is a local ring, with the set of nonunits as its maximal ideal;*
- *A is an integrally closed domain.*

Proof. Atiyah–MacDonald, Proposition 5.18. □

1.2.4. Proposition. *Let A be a subring of a field K. Then its integral closure in K is the intersubsection of all valuation rings of K containing A.*

Proof. Atiyah–MacDonald, Corollary 5.22. □

1.2.5. Proposition. *Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation, and let A be its valuation ring. Suppose $x_1, \ldots, x_n \in K$ and $v(x_1) < v(x_i)$ for all $i \geq 2$. Then $v(x_1 + \cdots + x_n) = v(x_1)$.*

Proof. $v(x_1 + \cdots + x_n) \geq \min(v(x_1), \ldots, v(x_n)) = v(x_1)$, and $v(x_1) \geq \min(v(x_1 + \cdots + x_n), v(x_2), \ldots, v(x_n))$. Since $v(x_1)$ is strictly the smallest, this minimum must be equal to $v(x_1 + \cdots + x_n)$. So we conclude $v(x_1 + \cdots + x_n) = v(x_1)$. □

1.3. Discrete valuation rings.

1.3.1. Definition. Let A be an integral domain. It is a *discrete valuation ring* (or *DVR* for short) if any of the following equivalent conditions hold:

(1) A is the valuation ring of a (unique) discrete valuation of $K = \operatorname{Frac} A$;
(2) A is a local, dimension-1 PID;
(3) A is a local, dimension-1, Noetherian, integrally closed domain.

Proof. (1) $\implies$ (2): For any ideal $\mathfrak{a} \subset A$, consider $n = v(\mathfrak{a}) := \inf_{x \in \mathfrak{a}} v(x)$. Let $\pi \in A$ be an element such that $v(\pi) = 1$, and suppose $x \in \mathfrak{a}$ satisfies $v(x) = n$. Then $x/\pi^n \in K$ has valuation 0, hence is a unit in A. So $\pi^n \in \mathfrak{a}$. Similarly, we can show $\mathfrak{a} \subset (\pi^n)$, so $\mathfrak{a} = (\pi^n)$. So any ideal is principal, and the only prime ideal is (π).

(2) $\implies$ (3): Every PID is noetherian and UFD, hence integrally closed.

(3) $\implies$ (1): We first claim that for any fractional ideal I of A, the fractional ideal $A(I) := \{x \in K : xI \subset I\}$ is equal to A. Clearly $A(I)$ is a subring of K containing A, so for any $x \in A(I)$, $A[x] \subset A(I)$. Since $A(I)$ is a fractional ideal of a Noetherian ring A, it is finitely generated over A. By [1.4.1], x is integral over A, hence inside A. This shows $A(I) = A$.

Now, let $\mathfrak{p}$ be maximal among the nonzero ideals $I \subset A$ with $I^{-1} = \{x \in K : xI \subset A\} \supsetneq A$. (Such an ideal clearly exists, because any principal ideal generated by a non-unit satisfies this.) We claim that $\mathfrak{p}$ is prime (hence is the unique nonzero prime ideal). Let $x, y \in A$, $xy \in \mathfrak{p}$, $x \notin \mathfrak{p}$, and take $z \in \mathfrak{p}^{-1} \backslash A$. Then $zy(\mathfrak{p} + (x)) \subset A$, and since $x \notin \mathfrak{p}$, $\mathfrak{p} \subsetneq \mathfrak{p} + (x)$, so by maximality, we conclude $zy \in A$. Therefore, $z(\mathfrak{p} + (y)) \subset A$, and so we conclude that $y \in \mathfrak{p}$.

So we have $A \supset \mathfrak{p}\mathfrak{p}^{-1} \supset \mathfrak{p}$. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, then $\mathfrak{p}^{-1} \subset A(\mathfrak{p}) = A$, a contradiction. So since $\mathfrak{p}$ is a maximal ideal, $\mathfrak{p}\mathfrak{p}^{-1} = A$. In addition, since $\mathfrak{p}^{-1} \subset A(\bigcap \mathfrak{p}^n)$, we must have $\bigcap \mathfrak{p}^n = 0$. So we can choose some element $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$, then $\pi\mathfrak{p}^{-1} \subset A$ but $\pi\mathfrak{p}^{-1} \not\subset \mathfrak{p}$, so $\pi\mathfrak{p}^{-1} = A$, i.e. $(\pi) = \mathfrak{p}$. Then for any element $x \in A$, there exists a unique $n \geq 0$ such that $x \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$, so that $x/\pi^n \in A \backslash \mathfrak{p}$, i.e. x/π^n is a unit. This then defines a unique discrete valuation on K, whose valuation ring is A. □

1.3.2. Proposition. *Let $(A, \mathfrak{m}, k)$ be a DVR, $n \geq 0$.*

(i) $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong k$ *non-canonically (as k-vector spaces);*
(ii) Let $U_n = 1 + \mathfrak{m}^n$ be subgroups of $A^\times$ for $n \geq 1$, and define $U_0 = A^\times$. Then $U_n/U_{n+1} \cong \mathfrak{m}^n/\mathfrak{m}^{n+1}$ for $n \geq 1$, and $U_0/U_1 \cong k^\times$, both canonically.

Proof. (i) $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an $(A/\mathfrak{m})$-module, i.e. a k-vector space. Since $\mathfrak{m}^n = (\pi^n)$ is a principal ideal, the image of π^n in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is nonzero and generates the vector space. So $\dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1} = 1$.

(ii) It is clear that $v(\frac{1}{1+a\pi^n} - 1) \geq n$, so inverses exist in U_n, i.e. is a subgroup of $A^\times$. Map $U_n/U_{n+1} \to \mathfrak{m}^n/\mathfrak{m}^{n+1}$ by $1 + u \mapsto \overline{u}$. It is easy to check that this is a group isomorphism. Also, the map $A \to k$ induces $U_0/U_1 \cong k^\times$. □

1.3.3. Proposition. *Let A be a DVR with fraction field K and residue field k. Let $n \geq 1$.*

(i) If k has characteristic $p > 0$, then $U_n^p \subset U_{n+1}$;
(ii) If K is complete and $\operatorname{char} k$ *does not divide m, then $u \mapsto u^m$ is an automorphism on U_n.*

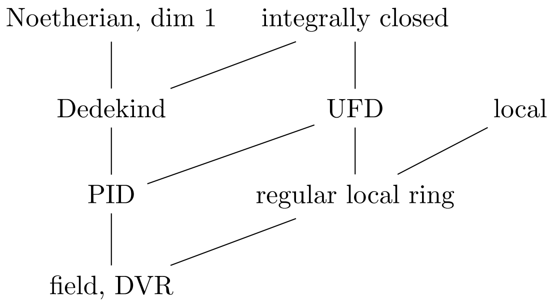
Proof. (i) follows from the previous proposition.

(ii) Injectivity is because $u \mapsto u^m$ is an isomorphism on each U_q/U_{q+1}, for $q \geq n$. To show surjectivity, let $v_n \in U_n$. Then some $u_n \in U_n$ satisfies $u_n^m v_{n+1} = v_n$ where $v_{n+1} \in U_{n+1}$. Similarly, we can find $u_{n+1} \in U_{n+1}$ such that $u_{n+1}^m v_{n+2} = v_{n+1}$ where $v_{n+2} \in U_{n+2}$. Keep going like this, then $u_n u_{n+1} u_{n+2} \dots$ converges to an element $u \in U_n$ by completeness, and $u^m = v_n$. □

1.3.4. Example. Examples of DVRs:

- Consider $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, then its valuation ring is $A = \mathbb{Z}_{(p)}$ ($\mathbb{Z}$ localized at (p)).
- Consider $v : k((t)) \to \mathbb{Z} \cup \{\infty\}$ mapping each formal Laurent series to the lowest degree whose coefficient is nonzero. Then $A = k[[t]]$.
- For a connected open $U \subseteq \mathbb{C}$, let $\mathscr{M}(U)$ be the field of meromorphic functions on U. For $V \subset U$ open, there is a restriction map $\mathscr{M}(U) \to \mathscr{M}(V)$ that is injective (because of analytic continuation). Let
$$\mathscr{M} = \varinjlim_{U \ni 0} \mathscr{M}(U).$$
This is the field of germs of meromorphic functions at 0. Consider $v : \mathscr{M} \to \mathbb{Z} \cup \{\infty\}$ mapping f to the order of vanishing of f at 0. Then A is the ring of germs of holomorphic functions at 0.

1.3.5. Remark. DVRs are the simplest commutative rings after fields. There is the following tower of inclusions:



Furthermore, the following reverse implications hold:

- Noetherian, dim 1 + integrally closed $\Longrightarrow$ Dedekind;
- Dedekind + UFD $\Longrightarrow$ PID;
- Dedekind + local $\Longrightarrow$ field or DVR.

DVRs are an example of what's regular local rings.

1.3.6. Definition. For a Noetherian local ring A with maximal ideal $\mathfrak{m}$ and residue field k, it is called a *regular local ring* if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$ (in general $\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \dim A$).

Geometrically, a regular local ring corresponds to a curve being nonsingular at a point.

1.3.7. Example. Consider the Noetherian local ring $A = \mathbb{C}[[x, y]]/(y^2 - x^3)$. The curve $y^2 - x^3$ has a singularity at the origin. Correspondingly, A is not a regular local ring for any of the following reasons:

- $\mathfrak{m} = (x, y)$ is not principal;
- $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 2$, while $\dim A = 1$;
- A is not integrally closed: consider the injection $A \hookrightarrow \mathbb{C}[[t]]$ by $x \mapsto t^2$, $y \mapsto t^3$. Then A maps isomorphically to the subring of $\mathbb{C}[[t]]$ consisting of power series in which the coefficient of t is 0. This ring is not integrally closed since $t = t^3/t^2 \in \operatorname{Frac}(A)$ is integral over A but not in A.

1.4. Integral extensions.

1.4.1. Proposition. *Let $A \subset B$ be a ring extension. The following are equivalent:*

(i) *$x \in B$ is integral over A;*
(ii) *$A[x]$ is a finitely generated module over A.*
(iii) *$A[x]$ is contained in a subring $C \subset B$ that is f.g. as an A-module.*
(iv) *There is a faithful $A[x]$-module M such that M is f.g. over A.*

1.4.2. Proposition. *Let A be an integrally closed domain, $K = \mathrm{Frac}(A)$, L/K a finite extension. Then $\alpha \in L$ is integral over A if and only if its minimal polynomial in K has coefficients in A.*

Proof. Suppose $\alpha \in L$ is integral over A. Let $g \in A[x]$ be monic such that $g(\alpha) = 0$, and let $f \in K[x]$ be the minimal polynomial of α in K. Consider an algebraic closure $\overline{K} \supset L \supset K$, then in $\overline{K}[x]$, f factors into linear factors $f(x) = \prod(x - \alpha_i)$. Then each α_i is also a root of g, hence integral over A. Therefore, the coefficients of f, being symmetric polynomials in α_i, are elements in K integral over A, so they are in A themselves. □

1.4.3. Example (Integral closure resolves codimension-1 singularities)**.** Let $A = k[x,y]/(y^2 - x^3)$. We saw in the previous subsection that A is not integrally closed by embedding $A \cong k[t^2, t^3] \hookrightarrow k[t]$. The integral closure of A (in its fraction field) is $k[t]$. The map $A \hookrightarrow k[t]$ corresponds to the map between varieties from the affine line to the curve $y^2 - x^3 = 0$.

1.5. Localization. The following properties are preserved by localization (by a set not containing 0):

- Noetherian
- Integrally closed
- Integral domain
- PID
- UFD
- Exactness.

1.5.1. Proposition. $\dim A = \sup\{\dim A_{\mathfrak{p}} : \mathfrak{p} \in \operatorname{Spec} A\}$. *(easy)*

1.5.2. Proposition. *Let $A \subset K$ where K is a field, let M be an A-module such that M injects into the vector space $V = M \otimes_A K$. Then*

$$M = \bigcap_{\mathfrak{p} \subset A \text{ prime}} M_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \subset A \text{ maximal}} M_{\mathfrak{m}}.$$

Proof. It suffices to show that if $x \in M_{\mathfrak{m}}$ for every $\mathfrak{m}$, then $x \in M$. Define the ideal

$$I = \{a \in A : ax \in M\}.$$

Since $x \in M_{\mathfrak{m}}$, there exists $s \notin \mathfrak{m}$ such that $s \in I$. Therefore, I is not contained in any maximal ideal, so $I = A$, so $x \in M$. □

Remarks: 1) We require $M \hookrightarrow V$ to be injective because otherwise we cannot view M as a submodule of $M_{\mathfrak{m}}$. 2) This proposition allows us to go from local to global.

1.6. Dedekind domains.

1.6.1. Definition. Let A be an integral domain, $K = \mathrm{Frac}(A)$. A *fractional ideal* of A is an A-submodule I of K, such that $aI \subset A$ for some $a \in K$. When A is Noetherian, this is equivalent to imposing that I is finitely generated as an A-module. A fractional ideal is *invertible* if $II^{-1} = A$, where I^{-1} is the fractional ideal $\{x \in K : xI \subset A\}$.

1.6.2. Definition. Let A be an integral domain. It is a *Dedekind domain* if it satisfies any of the following equivalent conditions:

(i) A is Noetherian, and each $A_{\mathfrak{p}}$ ($\mathfrak{p} \neq 0$) is a DVR;
(ii) A is Noetherian, $\dim A \leq 1$, and A is integrally closed;
(iii) All fractional ideals of A are invertible.

Proof. (i) $\Longrightarrow$ (ii): If $\mathfrak{p} \neq 0$, then $A_{\mathfrak{p}}$ is a DVR. If $\mathfrak{p} = 0$ then $A_{\mathfrak{p}} = \mathrm{Frac}(A)$ is a field. Therefore by Proposition 5.1, $\dim A \leq 1$. Also, each $A_{\mathfrak{p}}$ is integrally closed, so by Proposition 5.2, $A = \bigcap A_{\mathfrak{p}}$, so it is integrally closed as well.

(ii) $\Longrightarrow$ (i): easy. □

1.6.3. Example. Examples of Dedekind domains:

- Every PID is a Dedekind domain. In particular, $\mathbb{Z}$ and $k[x]$ are Dedekind domains.
- The ring of integers $\mathcal{O}_K$ of any algebraic number field is a Dedekind domain.
- The coordinate ring of a nonsingular affine algebraic curve C is a Dedekind domain.

The set of invertible fractional ideals forms an abelian group under multiplication. It is the *ideal group* $\mathrm{Div}(A)$ of A. The set of principal fractional ideals forms a subgroup, and the quotient is called the *class group* $\mathrm{Cl}(A)$.

Invertibility is a local property:

1.6.4. Proposition. *For a fractional ideal M, the following are equivalent:*

(i) M is invertible;
(ii) Each $M_{\mathfrak{p}}$ is invertible;
(iii) Each $M_{\mathfrak{m}}$ is invertible.

1.6.5. Corollary. *In a Dedekind domain A, every nonzero fractional ideal is invertible.*

(Reduce to the local case, where everything is easy because it's DVR.)

1.6.6. Proposition. *Let A be a Dedekind domain, then every nonzero $x \in A$ belongs to finitely many prime ideals.*

Proof. The map $I \mapsto (x)I^{-1}$ gives an order-reversing involution on the set of ideals between (x) and A. Therefore, $A/(x)$ is an Artinian ring, so it has dimension 0 and has finitely many maximal ideals. Since every prime is maximal, it has finitely many prime ideals. □

In what follows, assume A is a Dedekind domain, and K its field of fractions. We study prime factorization in Dedekind domains.

Let I be a fractional ideal of A, then $I_{\mathfrak{p}}$ is a fractional ideal of $A_{\mathfrak{p}}$, so it is equal to $(\mathfrak{p}A_{\mathfrak{p}})^n$ for some unique $n \in \mathbb{Z}$. Define then $v_{\mathfrak{p}}(I) = n$.

1.6.7. Proposition. *(i) The map $v_{\mathfrak{p}} : \mathrm{Div}(A) \to \mathbb{Z}$ mapping $I \mapsto v_{\mathfrak{p}}(I)$ is a group homomorphism. (ii) Suppose I is generated by $x_1, \dots, x_m$, thn $v_{\mathfrak{p}}(I) = \min v_{\mathfrak{p}}(x_i)$.*

1.6.8. Corollary. *For each $x \in K^\times$, there only exist finitely many $\mathfrak{p} \leq 0$ such that $v_{\mathfrak{p}}(x) \neq 0$.*

Proof. For any $x \in A$, it belongs to only finitely many primes, so for all other primes $\mathfrak{p}$, x is invertible in $A_{\mathfrak{p}}$, so $v_{\mathfrak{p}}(x) = 0$. In general $r/s \in K^\times$, where $r, s \in A$. □

1.6.9. Corollary. *For any fractional ideal I of A, there only exist finitely many $\mathfrak{p} \leq 0$ such that $v_{\mathfrak{p}}(I) \neq 0$.*

1.6.10. Theorem. *There is an isomorphism of abelian groups:*

$$\begin{aligned} \mathrm{Div}(A) &\cong \bigoplus_{\textit{primes } \mathfrak{p} \neq 0} \mathbb{Z} \\ I &\mapsto (\dots, v_{\mathfrak{p}}(I), \dots) \\ \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}} &\leftarrow\!\shortmid (e_{\mathfrak{p}})_{\mathfrak{p}} \end{aligned}$$

1.6.11. Proposition. *Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, $J = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$. Then*

- *$I \supset J \Longleftrightarrow e_{\mathfrak{p}} \leq f_{\mathfrak{p}}$ (to contain is to divide)*
- *$I + J = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(e_{\mathfrak{p}}, f_{\mathfrak{p}})}$*
- *$I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(e_{\mathfrak{p}}, f_{\mathfrak{p}})}$*
- *$IJ = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}} + f_{\mathfrak{p}}}$*
- *$(I : J) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}} - f_{\mathfrak{p}}}$*

1.6.12. Theorem. *For a Dedekind domain A, the following are all equivalent:*

- $\mathrm{Cl}(A)$ *is trivial.*
- *A is a PID;*
- *A is a UFD;*

Proof. (iii) $\Longrightarrow$ (i): Let I be any fractional ideal. Because it factors into the product of prime powers, it suffices to show that any nonzero prime ideal $\mathfrak{p}$ is principal. Pick $a \neq 0$ in $\mathfrak{p}$, then we can uniquely factorize $a = \prod_p p$ where each p is irreducible. Since $\mathfrak{p} \supseteq (a)$, $\mathfrak{p} \mid (a)$, so $\mathfrak{p} \mid \prod_p (p)$. Since $\mathfrak{p}$ is prime, $\mathfrak{p}$ must divide some (p), but since (p) is a prime ideal, $\mathfrak{p} = (p)$ is principal. □

More concepts: Let A be the coordinate ring of a regular affine curve X over an algebraically closed field k. (Then $X = \operatorname{Spec} A$, and A is a Dedekind domain.)

algebra	geometry
$K = \mathrm{Frac}(A)$	function field on X
nonzero primes $\mathfrak{p} \subset A$	closed points P of X
nonzero fractional ideal $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ of A	divisor $\sum_P e_{\mathfrak{p}} P$ on X
integral ideal $I \subseteq A$	effective divisor on X
principal fractional ideal (f)	principal divisor (f) on X

1.6.13. Theorem (Strong approximation theorem)**.** *Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$. Suppose we have distinct nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$, integers $e_1, \dots, e_n$, and elements $a_1, \dots, a_n \in K$. Then there exists $x \in K$, such that:*

- *$v_{\mathfrak{p}_i}(x - a_i) \geq e_i$ (this is the "weak" part);*
- *$v_{\mathfrak{q}}(x) \geq 0$ for all prime ideals $\mathfrak{q} \neq 0$, $\mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.*

Proof. Without loss of generality, assume all $e_i \geq 0$.

Case I: Suppose $a_1 \in A$, $a_2, \dots, a_n = 0$. Because $\mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n} = A$, there exists $y \in \mathfrak{p}_1^{e_1}$, $x \in \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$ such that $x + y = a_1$. Then $v_{\mathfrak{p}_1}(x - a_1) = v_{\mathfrak{p}_1}(-y) = v_{\mathfrak{p}_1}(y) \geq e_1$, and $v_{\mathfrak{p}_i}(x - a_i) = v_{\mathfrak{p}_i}(x) \geq e_i$ for every $i \neq 1$. Also, since $x \in A$, $v_{\mathfrak{q}}(x) \geq 0$ for all $\mathfrak{q}$.

Case II: Suppose $a_1, \dots, a_n \in A$. Then using Case I, we can choose x_i satisfying that $v_{\mathfrak{p}_i}(x_i - a_i) \geq e_i$ and $v_{\mathfrak{p}_j}(x_i) \geq 0$ for $i \neq j$. Let $x = x_1 + \cdots + x_n$, then $v_{\mathfrak{p}_i}(x - a_i) \geq v_{\mathfrak{p}_i}(x_i - a_i) \geq e_i$, and $v_{\mathfrak{q}}(x) \geq 0$.

Case III: Suppose $a_1, \dots, a_n \in K$ in general. Take nonzero $t \in A$ such that $ta_1, \dots, ta_n \in A$. Then by Case II, there exists $x \in A$ such that $v_{\mathfrak{p}_i}(x - ta_i) \geq e_i + v_{\mathfrak{p}_i}(t)$, $v_{\mathfrak{q}}(x) \geq v_{\mathfrak{q}}(t)$ for those $\mathfrak{q}$ with $v_{\mathfrak{q}(t) \geq 0}$, and $v_{\mathfrak{q}}(x) \geq 0$ for all others. Then $x/t \in K$ satisfies the conditions. □

Remark: we can in fact force $v_{\mathfrak{p}_i}(x) = f_i$ for any collection of f_i: just take a_i such that $v_{\mathfrak{p}_i}(a_i) = f_i$ and $e_i > f_i$, then any x such that $v_{\mathfrak{p}_i}(x - a_i) \geq e_i$ satisfies $v_{\mathfrak{p}_i}(x) = f_i$.

1.6.14. Corollary. *A semilocal Dedekind ring A must be a PID.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the nonzero primes. Any ideal I is $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$. By SA, there exists $x \in K = \mathrm{Frac}(A)$ such that $v_{\mathfrak{p}_i}(x) = e_i$, so in fact $I = (x)$. □

1.7. Separability. Next, we review some field theory related to separability. Let K be a field and $\overline{K}$ be an algebraic closure of K.

1.7.1. Lemma. *Let $\alpha \in \overline{K}$, $L = K(\alpha)$. Then $[L : K] \geq |\mathrm{Hom}_K(L, \overline{K})|$ with equality iff α is separable, iff L/K is separable.*

Proof. We have $L \cong K[x]/(f(x))$ for some irreducible $f(x) \in K[x]$. Any homomorphism $\sigma : L \to \overline{K}$ fixing K must send x to another root of f in $\overline{K}$, so there are at most $\deg f$ choices, and there are exactly $\deg f$ choices if and only if all roots of f are distinct.

Let $\beta \in L$ be any element, then $K(\beta) \subset K(\alpha)$. Since α is separable over both K and $K(\beta)$, we then have $[K(\beta) : K] = \frac{[K(\alpha):K]}{[K(\alpha):K(\beta)]} = \frac{\mathrm{Hom}_K(K(\alpha),\overline{K})}{\mathrm{Hom}_{K(\beta)}(K(\alpha),\overline{K})} = \mathrm{Hom}_K(K(\beta), \overline{K})$, which shows that β is separable over K as well. Therefore L/K is separable. □

1.7.2. Proposition. *For a finite extension L/K, the following are equivalent:*

- *L is separable over K;*

- *$L = K(\alpha_1, \dots, \alpha_n)$ for some α_i separable over K;*
- *$L = K(\alpha)$ for some α separable over K;*
- *$[L : K] = |\operatorname{Hom}_K(L, \overline{K})|$.*

1.7.3. Corollary. *Let M/L, L/K be finite separable extensions, then M/K is separable as well.*

1.7.4. Lemma. *Let L/K be a field extension, and let F be the set of elements in L separable over K. Then F is a field between L and K.*

Proof. It suffces to show that if $\alpha, \beta \in L$ are separable over K, then so are $\alpha + \beta, \alpha\beta$. Consider the tower of extensions $K(\alpha, \beta) \supset K(\alpha) \supset K$. By the above lemma, $[K(\alpha) : K] = |\operatorname{Hom}_K(K(\alpha), \overline{K})|$ and $[K(\alpha, \beta) : K(\alpha)] = |\operatorname{Hom}_{K(\alpha)}(K(\alpha, \beta), \overline{K})|$. So

$$[K(\alpha, \beta) : K] = |\operatorname{Hom}_K(K(\alpha), \overline{K})| \cdot |\operatorname{Hom}_{K(\alpha)}(K(\alpha, \beta), \overline{K})| = |\operatorname{Hom}_K(K(\alpha, \beta), \overline{K})|.$$

By the primitive element theorem, there exists $\gamma \in K(\alpha, \beta)$ with $K(\gamma) = K(\alpha, \beta)$, then we conclude that γ is separable over K. Thus $\alpha + \beta, \alpha\beta \in L$ are both separable. □

Then we call $[F : K] = [L : K]_s$ the *separable degree* of L/K, and call $[L : F] = [L : K]_i$ the *inseparable degree* of L/K. Call L/K *separable* if $F = L$, and *purely inseparable* if $F = K$.

1.7.5. Theorem (Primitive element theorem)**.** *Let L/K be a finite separable extension. Then $L = K(\alpha)$ for some element $\alpha \in L$.*

1.7.6. Theorem (Normal basis theorem)**.** *Let L/K be a finite Galois extension, with G its Galois group. Then there exists $\beta \in L$, such that $\{\sigma\beta : \sigma \in G\}$ forms a K-basis of L.*

1.7.7. Theorem (Purely inseparable extensions)**.** *Let K be a field of characteristic p.*

- *A extension L/K of degree p is purely inseparable iff $L = K(\alpha^{1/p})$ where $\alpha \in K$ is not a p-th power.*
- *Any purely inseparable extension is a tower of purely inseparable degree-p extensions.*

1.7.8. Proposition. *The separable degree $[L : K]_s$ is equal to $|\operatorname{Hom}_K(L, \overline{K})|$.*

Proof. By definition, $[L : K]_s = |\operatorname{Hom}_K(F, \overline{K})|$ where F is the separable closure of K in L. But $\operatorname{Hom}_K(F, \overline{K})$ corresponds one-to-one with $|\operatorname{Hom}_K(L, \overline{K})|$ (use the above theorem and the fact that pth roots are unique in characteristic p). □

So the separable degree is multiplicative: for field extensions $M/L/K$, $[M : L]_s[L : K]_s = [M : K]_s$, and so does the inseparable degree.

1.7.9. Definition. A field K is called *perfect* if any finite extension of K is separable. Equivalently, either $\operatorname{char} K = 0$, or $\operatorname{char} K = p$ and the Frobenius endomorphism $x \mapsto x^p$ is an automorphism.

For example, any finite field $\mathbb{F}_q$ is perfect, but $\mathbb{F}_q(t)$ is not.

1.7.10. Definition. A field K is called *separably closed* if its only separable extension is K itself.

1.8. Étale algebras.

1.8.1. Definition. Let K be a field. An *étale algebra* L over K is a finite product of finite separable extensions of K.

Apparently, a K-algebra A is étale if and only if the map $\operatorname{Spec} A \to \operatorname{Spec} K$ is an étale morphism.

1.8.2. Proposition. *Let L be a commutative K-algebra with finite dimension, such that $\dim_K L < |K|$. TFAE:*

- *L is a fintie étale K-algebra;*
- *Every element of L is separable over K;*
- *$L \otimes_K K'$ is reduced for every extension K'/K;*
- *$L \otimes_K K'$ is semisimple for every extension K'/K;*
- *$L = K[x]/(f)$ for some separable $f \in K[x]$.*

The advantage of working with étale algebras instead of separable field extensions is that they are preserved by extension of coefficients. In other words, let K'/K be a field extension, and L/K a finite separable extension, then $L \otimes_K K'$ is not necessarily a field. However:

1.8.3. Proposition. *Let K'/K be a field extension, L is an étale K-algebra, then $L \otimes_K K'$ is an étale K'-algebra.*

Proof. Because tensor products commute with finite products, WLOG assume L/K is a finite separable extension. By the primitive element theorem, $L = K[x]/(f(x))$ for some irreducible separable polynomial f. Then $L \otimes_K K' = K'[x]/(f(x))$.

In $K'[x]$, $f(x)$ factors into the product of irreducible separable polynomials $f_1(x) \cdots f_n(x)$. By the Chinese Remainder Theorem, $K'[x]/(f(x)) \cong \prod_{i=1}^n K'[x]/(f_i(x))$ is a product of finite separable extensions over K'. □

1.8.4. Proposition. *Let L/K be an étale algebra, Ω a separably closed field containing K. Then*

$$L \otimes_K \Omega \to \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \Omega$$
$$\ell \otimes 1 \mapsto (\dots, \sigma(\ell), \dots)$$

is an isomorphism.

Proof. Because $\mathrm{Hom}_K(\prod L_i, \Omega) = \coprod \mathrm{Hom}_K(L_i, \Omega)$, we may again assume L/K is a finite separable extension, i.e. $L \cong K[x]/(f(x))$ for an irreducible separable polynomial f. Then $f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ in $\Omega[x]$, so any $\sigma \in \mathrm{Hom}_K(L,\Omega)$ must send x to one of α_i. The map is therefore given by

$$L \xrightarrow{\ell \mapsto \ell \otimes 1} L \otimes_K \Omega = \frac{\Omega[x]}{(f(x))} = \prod_{i=1}^n \frac{\Omega[x]}{x - \alpha_i} \cong \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \Omega.$$

□

1.9. Norm and trace.

1.9.1. Definition. Let $A \subset B$ be commutative rings, such that B is a free A-module of rank n. For $b \in B$, the map $B \xrightarrow{\times b} B$ is an A-linear map, so we may define

$$\mathrm{N}_{B/A}(b) = \det(B \xrightarrow{\times b} B),$$
$$\mathrm{Tr}_{B/A}(b) = \mathrm{tr}(B \xrightarrow{\times b} B).$$

1.9.2. Proposition. *Let $A \to A'$ be any ring homomorphism, $A \subset B$ such that B is a free A-module of rank n, and let $B' = B \otimes_A A'$ be a ring that is a free A'-module of rank n. Then*

$$\mathrm{N}_{B/A}(b) = \mathrm{N}_{B'/A'}(b \otimes 1),$$
$$\mathrm{Tr}_{B/A}(b) = \mathrm{Tr}_{B'/A'}(b \otimes 1).$$

1.9.3. Theorem. *Let L be an étale K-algebra, Ω/K separably closed, and $\Sigma = \mathrm{Hom}_K(L, \Omega)$. Then*

$$\mathrm{N}_{L/K}(b) = \prod_{\sigma \in \Sigma} \sigma(b),$$
$$\mathrm{Tr}_{L/K}(b) = \sum_{\sigma \in \Sigma} \sigma(b).$$

Proof. We have $\mathrm{N}_{L/K}(b) = \mathrm{N}_{L \otimes_K \Omega/\Omega}(b \otimes 1) = \mathrm{N}_{\Omega \times \dots \times \Omega/\Omega}(\dots, \sigma(b), \dots)$, by propositions 1.8.4 and 1.9.2. But this is just the diagonal matrix with entries $\sigma(b)$, so the norm is $\prod_{\sigma \in \Sigma} \sigma(b)$. The situation is identical for the trace. □

1.9.4. Proposition (Norm and trace for finite extensions)**.** *Let L/K be a finite extension, and fix an embedding $L \subset \overline{K}$. Let $\alpha \in L^\times$ have minimal polynomial $f(x) \in K[x]$. Suppose $f(x) = \prod_i (x - \alpha_i)$ in $\overline{K}[x]$, and let $e = [L : K(\alpha)]$. Then*

$$\mathrm{N}_{L/K}(\alpha) = \prod_i \alpha_i^e, \quad \mathrm{Tr}_{L/K}(\alpha) = e \sum_i \alpha_i.$$

1.9.5. Theorem. *Suppose $A \subseteq B \subseteq C$ are rings, such that B is a free A-module of rank n, and C is a free B-module of rank m. Then*

$$\begin{aligned} \mathrm{N}_{C/A}(c) &= \mathrm{N}_{B/A}(\mathrm{N}_{C/B}(c)), \\ \mathrm{Tr}_{C/A}(c) &= \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(c)). \end{aligned}$$

Proof. We refer to https://stacks.math.columbia.edu/tag/0BIJ. □

1.10. Bilinear pairings. Let k be a field, V a finite dimensional k-vector space. Let $\langle -, - \rangle : V \times V \to k$ be a symmetric bilinear pairing. This induces a map $V \to V^*$ by

$$v \longmapsto (w \mapsto \langle v, w \rangle).$$

The left kernel (which is equal to the right kernel since the form is symmetric) is the set of $v \in V$ such that $\langle v, w \rangle = 0$ for all $w \in V$.

Fixing a basis $e_1, \dots, e_n$ of V allows the definition of the *discriminant*

$$\mathrm{disc}(\langle -, - \rangle, e_1, \dots, e_n) = \det(\langle e_i, e_j \rangle).$$

Applying a change-of-basis matrix T multiplies the discriminant by a factor of $(\det T)^2$.

The symmetric bilinear form is called *nondegenerate* (or a *perfect pairing*) if the following equivalent conditions are met:

- the induced $V \to V^*$ is an isomorphism;
- the left kernel is 0;
- the discriminant under any basis is nonzero.

Given a basis $e_1, \dots, e_n$ of V, there is a *dual basis* $f_1, \dots, f_n$ of V^* defined by $f_i(e_j) = \delta_{ij}$. If the pairing is perfect, then f_i correspond to a dual basis e_i' of V, satisfying $\langle e_i, e_j \rangle = \delta_{ij}$.

2. The AKLB setup

2.1. Dedekind extensions. We work in the following setup. Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, L/K a finite separable extension, and B the integral closure of A in L. The main goal of this subsection is to show that B is also a Dedekind domain.

2.1.1. Proposition. *For any element $\ell \in L$, there exists $s \in A$ such that $s\ell \in B$.*

Consequently, $L = \mathrm{Frac}(B)$.

2.1.2. Proposition. *If $b \in B$, then $\mathrm{Tr}_{L/K}(b) \in A$.*

We define the *trace pairing*:

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \mathrm{Tr}_{L/K}(xy). \end{aligned}$$

2.1.3. Proposition. *The trace pairing is nondegenerate.*

Proof. Let $\Sigma = \mathrm{Hom}_K(L, \Omega) = \{\sigma_1, \dots, \sigma_m\}$ where Ω is some separably closed extension of K. Pick a basis $\beta_1, \dots, \beta_m$ of L/K. Then the discriminant is equal to

$$\det(\mathrm{Tr}(\beta_i \beta_j)) = \det \mathrm{pr} \sum_{\sigma_k} \sigma_k(\beta_i)\sigma_k(\beta_j) = \det(\sigma_k(\beta_i)) \det(\sigma_k(\beta_j)) = \det(\sigma_k(\beta_i))^2.$$

So it suffices to show that $\sigma_k(\beta_i)$ are linearly independent over Ω. But this is just the linear independence of characters (on the group $L^\times$). □

Given an A-module $M \subseteq L$, define its *dual* $M^* = \{x \in L : \mathrm{Tr}(xm) \in A \ \forall m \in M\}$. This is order-reversing.

2.1.4. Proposition. *B is a finitely generated module over A.*

Proof. Consider an arbitrary basis of L/K, then each basis element can be multiplied by some element in A such that they lie in B. Call this basis $u_1, \dots, u_n$ and let $M \subseteq B$ be the A-module generated by these elements. Consider its dual, M^*, which is freely generated by the dual basis v_i of u_i, $\mathrm{Tr}(v_i u_j) = \delta_{ij}$. So $B \subseteq B^* \subseteq M^*$, and B is finitely generated (since A is Noetherian). □

2.1.5. Theorem. *B is also a Dedekind domain.*

Proof. Because B is a Noetherian A-module, it is a Noetherian ring. By definition, B is integrally closed. Because B/A is integral, $\dim B = \dim A \leq 1$. So B is a integrally closed Noetherian domain with dimension at most 1, hence a Dedekind domain. □

2.1.6. Corollary. *$\mathcal{O}_K$ is Dedekind.*

Actually we don't need L/K to be separable.

2.1.7. Theorem (Krull-Akizuki theorem)**.** *Let A be a Noetherian integral domain with dimension 1, with $K = \operatorname{Frac} A$. Let L/K be a finite extension, and B a ring with $A \subset B \subset L$. Then B is Noetherian with dimension at most 1, and for any nonzero ideal $J \subset B$, B/J is an A-module of finite length.*

2.1.8. Corollary. *Let A be a Dedekind domain, $K = \operatorname{Frac} A$, L/K finite, and B the integral closure of A in L. Then B is a Dedekind domain.*

Finally, we mention the following notations:

- $\mathfrak{q} \mid \mathfrak{p}$ (lying over) for primes $\mathfrak{q} \subset B$, $\mathfrak{p} \subset A$ means that $\mathfrak{q} \cap A = \mathfrak{p}$;
- Given nonzero prime $\mathfrak{p} \subset A$, we can uniquely factor
$$\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}.$$
Call e_i the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$;
- For $\mathfrak{q} \mid \mathfrak{p}$, $f_\mathfrak{q} = [B/\mathfrak{q} : A/\mathfrak{p}]$ is called the *residue field degree.*

2.2. Prime factorization in Dedekind extensions. We continue to work in the AKLB setup. Let $\mathfrak{p} \subset A$ be a prime ideal, then $\mathfrak{p}B = \prod \mathfrak{q}^{e_\mathfrak{q}}$ factors as a product of primes in B. For a prime $\mathfrak{q} \in B$, $\mathfrak{q} \mid \mathfrak{p} \iff \mathfrak{q} \cap A = \mathfrak{p} \iff \mathfrak{q} \supseteq \mathfrak{p}B \iff \mathfrak{q}$ appears in the factorization of $\mathfrak{p}B$.

2.2.1. Proposition. $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K] =: n$.

Proof. Let $S = A - \mathfrak{p}$. Because $A/\mathfrak{p} \cong S^{-1}A/\mathfrak{p}(S^{-1}A)$ and $B/\mathfrak{p}B \cong S^{-1}B/\mathfrak{p}(S^{-1}B)$, we may WLOG replace A with $S^{-1}A$ and B by $S^{-1}B$. (Here we implicitly use the fact that localization commutes with integral closure.) But now since $S^{-1}A = A_\mathfrak{p}$ is a DVR, it is a PID, so B is free over A with the same rank as $[L : K]$. Consequenly, $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K]$. □

2.2.2. Proposition. *Given $\mathfrak{p} \subset A$, $\sum_{\mathfrak{q}\mid\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q} = n$.*

Proof. We count the dimension of $B/\mathfrak{p}B$ as a $A/\mathfrak{p}$-vector space. By the above proposition, this dimension is equal to n. On the other hand, by CRT, $B/\mathfrak{p}B = \prod_{\mathfrak{q}\mid\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$. Consider the filtration of $B/\mathfrak{q}$-vector spaces:
$$B/\mathfrak{q}^{e_\mathfrak{q}} \supset \mathfrak{q}/\mathfrak{q}^{e_\mathfrak{q}} \supset \cdots \supset \mathfrak{q}^{e_\mathfrak{q}-1}/\mathfrak{q}^{e_\mathfrak{q}} \supset 0.$$
Every step is equal to $\mathfrak{q}^i/\mathfrak{q}^{i+1}$, which is a 1-dimensional $B/\mathfrak{q}$-vector space, so $B/\mathfrak{q}^{e_\mathfrak{q}}$ is $e_\mathfrak{q}$-dimensional over $B/\mathfrak{q}$, which is in turn $f_\mathfrak{q}$-dimensional over $A/\mathfrak{p}$. So $\dim_{A/\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}} = e_\mathfrak{p} f_\mathfrak{p}$, and we're done. □

2.2.3. Corollary. *There are at most n primes lying over $\mathfrak{p}$.*

2.2.4. Definition. The extension L/K is called:

- *totally ramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = n$, $f_\mathfrak{q} = 1$, and $\mathfrak{q}$ is the only prime lying over $\mathfrak{p}$.
- *unramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = 1$ and $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$.
- *unramified above* $\mathfrak{p}$ if it is unramified at every prime above $\mathfrak{p}$. Equivalently, iff $B/\mathfrak{p}B$ is an étale $A/\mathfrak{p}$-algebra.

2.2.5. Definition. A prime $\mathfrak{p} \subset A$:

- is *inert* if $\mathfrak{q} = \mathfrak{p}B$ is prime in B.
- *splits completely* if all $e_\mathfrak{q} = f_\mathfrak{q} = 1$.

2.2.6. Definition. A discrete valuation w on L is said to *extend* the discrete valuation v on K if $w|_K = e \cdot v$ for some $e \in \mathbb{Z}_+$.

2.2.7. Proposition. *Fix $\mathfrak{p} \subset A$. Then there is a bijection*

$$\{\text{primes } \mathfrak{q} \mid \mathfrak{p}\} \Longleftrightarrow \{\text{discrete valuations } w \text{ extending } v_{\mathfrak{p}}\}$$

given by $\mathfrak{q} \mapsto v_{\mathfrak{q}}$.

Proof. First, we show that $v_{\mathfrak{q}}$ indeed extends $v_{\mathfrak{p}}$. Because for distinct primes in A, the sets of primes $\mathfrak{q}$ lying above them are disjoint, it is clear that $v_{\mathfrak{q}}(x) = e_{\mathfrak{q}} v_{\mathfrak{p}}(x)$. The hard part is to show that all discrete valuations extending $v_{\mathfrak{p}}$ are of this form. Let w be such a discrete valuation, and let $W = \{x \in L : w(x) \geq 0\}$, which is a DVR. Let $\mathfrak{m}$ be the maximal ideal of W, and $\mathfrak{q} = \mathfrak{m} \cap B$. Since $\mathfrak{q} = \mathfrak{m} \cap B \supseteq \mathfrak{m} \cap A = \mathfrak{p}$, $\mathfrak{q} \mid \mathfrak{p}$. Because $L \neq W \supseteq B_{\mathfrak{q}}$, $W = B_{\mathfrak{q}}$ (since $B_{\mathfrak{q}}$ is a DVR), and $w = v_{\mathfrak{q}}$. □

2.3. Dedekind-Kummer theorem. We wish to give some intuition of the $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}}$'s. We continue to work in the AKLB setup.

2.3.1. Theorem (Dedekind-Kummer). *Suppose $B = A[\alpha]$ for some $\alpha \in L$. Let $f(x) \in A[x]$ be the minimal polynomial of α in K, and suppose that $f(x) \mod \mathfrak{p} = \prod (g_i(x) \mod \mathfrak{p})^{e_i}$. Then $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$, where $\mathfrak{q}_i = (\mathfrak{p}, g_i(\alpha)) \subset B$, $e_i = e_{\mathfrak{q}_i}$, and $f_i = f_{\mathfrak{q}_i} = [B/\mathfrak{q}_i : A/\mathfrak{p}] = \deg g_i(x)$.*

Proof. We have $B = A[x]/(f(x))$, so

$$\begin{aligned} B/\mathfrak{p}B &= (A/\mathfrak{p})[x]/(f(x) \mod \mathfrak{p}) \\ &= \prod (A/\mathfrak{p})[x]/(g_i(x) \mod \mathfrak{p})^{e_i} \\ &= \prod A[x]/(\mathfrak{p}, g_i(x))^{e_i} \\ &= \prod B/(\mathfrak{p}, g_i(\alpha))^{e_i}. \end{aligned}$$

By the uniqueness of factorizing an étale algebra into separable extensions, we conclude $\mathfrak{p}B = \prod (\mathfrak{p}, g_i(\alpha))^{e_i} = \prod \mathfrak{q}_i^{e_i}$. Furthermore, $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}] = [A[x]/(\mathfrak{p}, g_i(x)) : A/\mathfrak{p}] = [(A/\mathfrak{p})[x]/g_i(x) : A/\mathfrak{p}] = \deg g_i$. □

From this, counting the degree of f, we get a more intuitive epxlanation of $n = \sum_{\mathfrak{q} \mid \mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$.

Geometric example:

	algebra	geometry
Dedekind domain A	$\mathbb{Z}$	$\mathbb{C}[z]$
Field of fractions K	$\mathbb{Q}$	$\mathbb{C}(z)$
Degree two separable extension L	$\mathbb{Q}(\sqrt{-5})$	$\mathbb{C}(\sqrt{z})$
Integral closure B	$\mathbb{Z}[\sqrt{-5}]$	$\mathbb{C}[\sqrt{z}]$
Totally ramified ideal	(2)	(z)
Ideal that split completely	(3)	$(z - z_0)$, $z_0 \neq 0$

2.4. Index of A-lattices. We now change gears to the topic of A-lattices.

2.4.1. Definition. Let V be an r-dimensional vector space over K. An *A-lattice in V* is a finitely generated A-submodule of V such that $V = MK$.

Our goal in this subsection is to define the "index" of an A-lattice, which will be an ideal in A. This allows us to define the ideal norm.

First, consider a torsion module M over A of finite type. Since A is a Dedekind domain, the simple torsion modules over A are of the form $A/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Then given any composition series

$$M = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0,$$

with $M_i/M_{i-1} \cong A/\mathfrak{p}_i$, we define

$$\chi(M) = \mathfrak{p}_1 \ldots \mathfrak{p}_n.$$

By Jordan-Hölder theorem, $\chi(M)$ only depends on M, and not on the composition series chosen.

2.4.2. Proposition. *For fractional ideals $I \subseteq J$, $\chi(J/I) = IJ^{-1}$.*

Proof. Localize at each prime to assume A is a DVR, where everything is easy. □

2.4.3. Corollary. *If $I \subset A$ is an integral ideal, then $\chi(A/I) = I$.*

2.4.4. Definition. Let $M, N \subset V$ be A-lattices.

- If $M \supseteq N$, then M/N is torsion. Define $(M : N)_A = \chi(M/N)$, which is an integral ideal in A.
- In general, for any two A-lattices M, N, there exists an A-lattice P contained in M and N, so we can define $(M : N)_A = \frac{(M:P)_A}{(N:P)_A}$.

In particular, when $V = K$, for I, J fractional ideals, $(J : I)_A = IJ^{-1}$.

It is important that everything we do here commutes with localization: for example, $((M : N)_A)_{\mathfrak{p}} = (\chi(M/N))_{\mathfrak{p}} = \chi((M/N)_{\mathfrak{p}}) = \chi(M_{\mathfrak{p}}/N_{\mathfrak{p}}) = (M_{\mathfrak{p}} : N_{\mathfrak{p}})_{A_{\mathfrak{p}}}$. Many arguments we have for the general AKLB setup start by immediately reducing to the DVR case using localization.

2.4.5. Proposition. *Given $X \in \mathrm{GL}_n(K)$, $(A^n : X(A^n))_A = (\det X)$.*

Proof. Assume WLOG A is a DVR, hence a PID, so X has a Smith normal form, which is diagonal, so we just reduce to the case $n = 1$. But $(A : xA)_A = \chi(A/(x)) = (x)$. □

2.5. Inclusion and ideal norm. We continue to work in the AKLB setup.

2.5.1. Definition. Let $\mathcal{I}_A, \mathcal{I}_B$ be the ideal groups of A and B. Define

- $i : \mathcal{I}_A \to \mathcal{I}_B$ by $I \mapsto IB$, the *inclusion homomorphism*.
- $N : \mathcal{I}_B \to \mathcal{I}_A$ by $J \mapsto (B : J)_A$, the *ideal norm*.

2.5.2. Proposition. *The following two diagrams commute:*

$$\begin{tikzcd}
L^\times \arrow[r, "x\mapsto(x)"] & \mathcal{I}_B & L^\times \arrow[r, "x\mapsto(x)"] \arrow[d, "\mathrm{N}_{L/K}"] & \mathcal{I}_B \arrow[d, "N"] \\
K^\times \arrow[r, "x\mapsto(x)"] \arrow[u, hook] & \mathcal{I}_A, \arrow[u, "i"'] & K^\times \arrow[r, "x\mapsto(x)"] & \mathcal{I}_A.
\end{tikzcd}$$

Proof. The first one is trivial. For the second one, consider an element $x \in L^\times$, then $N((x)) = (B : (x))_A$. If A is a DVR, then it is a PID, so B is a free A-module, and by proposition 2.4.5, $(B : (x))_A = (\det(L \xrightarrow{x} L)) = (\mathrm{N}_{L/K}(x))$. In general, localize at each prime $\mathfrak{p}$, and because $((B : (x))_A)_{\mathfrak{p}} = (B_{\mathfrak{p}} : (x)_{\mathfrak{p}})_{A_{\mathfrak{p}}} = (\mathrm{N}_{L/K}(x))_{\mathfrak{p}}$ at each $\mathfrak{p}$, $(B : (x))_A = (\mathrm{N}_{L/K}(x))$. □

2.5.3. Proposition. *i and N are group homomorphisms.*

Proof. This is clear for i. If A is a DVR, hence a PID, B must be a semilocal Dedekind domain, so it is a PID (corollary 1.6.14). This means that the map $L^\times \to \mathcal{I}_B$ is surjective, so N is a homomorphism. In general, localize A at each prime $\mathfrak{p}$. Then because localization commutes with $(:)_A$, the diagrams

$$\begin{tikzcd}
\mathcal{I}_B \arrow[r] \arrow[d, "N"] & \mathcal{I}_{B_{\mathfrak{p}}} \arrow[d, "N_{\mathfrak{p}}"] \\
\mathcal{I}_A \arrow[r] & \mathcal{I}_{A_{\mathfrak{p}}}
\end{tikzcd}$$

commute. Because the $N_{\mathfrak{p}}$'s on the right are group homomorphisms for every $\mathfrak{p}$, we conclude that $N : \mathcal{I}_B \to \mathcal{I}_A$ is a homomorphism as well. □

2.5.4. Proposition. *Let $\mathfrak{p} \subset A$ satisfy that $\mathfrak{p}B = \prod \mathfrak{q}^{e_{\mathfrak{q}}}$. Then:*

- *$i(\mathfrak{p}) = \prod \mathfrak{q}^{e_{\mathfrak{q}}}$;*
- *For $\mathfrak{q} \mid \mathfrak{p}$, $N(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}}}$.*

Proof. For the second one, $N(\mathfrak{q}) = (B : \mathfrak{q})_A = \chi(B/\mathfrak{q}) = \chi((A/\mathfrak{p})^{\oplus f_{\mathfrak{q}}}) = \mathfrak{p}^{f_{\mathfrak{q}}}$. □

The geometric picture:

algebra	geometry
Ring A	Affine scheme $\operatorname{Spec} A$
Dedekind domain	Nonsingular curve
Inclusion of Dedekind domains $A \hookrightarrow B$	(possibly) Ramified cover $\operatorname{Spec} B \twoheadrightarrow \operatorname{Spec} A$
Ideal group $\mathcal{I}$	Divisor group Div
Inclusion homomorphism $i : \mathcal{I}_A \to \mathcal{I}_B$	Inverse image/pullback $f^* : \operatorname{Div} X \to \operatorname{Div} Y$
Ideal norm $N : \mathcal{I}_B \to \mathcal{I}_A$	Image/pushforward $f_* : \operatorname{Div} Y \to \operatorname{Div} X$

2.6. DVR extensions. We now consider the following setup. Let A be a DVR with maximal ideal $\mathfrak{p} = (\pi)$, $K = \operatorname{Frac} A$, $B = A[x]/(f(x))$ for some monic $f(x) \in A[x]$. In general, B need not even be integrally closed.

2.6.1. Lemma. *Any maximal ideal of B contains $\mathfrak{p}$.*

Proof. Let $\mathfrak{m} \subset B$ be maximal. Then if $\mathfrak{p} \not\subseteq \mathfrak{m}$, $\mathfrak{m} + \mathfrak{p}B = B$, so the image of $\mathfrak{m}$ generates $B/\mathfrak{p}B$. Applying Nakayama's lemma to the local ring A and finitely generated A-module B, we see that $\mathfrak{m}$ generates B, a contradiction. □

2.6.2. Corollary. *Maximal ideals of B are in bijection with maximal ideals of $B/\mathfrak{p}B = (A/\mathfrak{p})[x]/(f)$, which are in bijection with irreducible factors of $f(x)$ mod $\mathfrak{p}$.*

Armed with this information, we consider two conditions on f that would make B not only Dedekind, but actually a DVR.

Case 1: Suppose f is irreducible mod $\mathfrak{p}$. Then the only maximal ideal of B is $\mathfrak{p}B = (\pi)B$, which is principal. So B is a local Noetherian domain whose maximal ideal is principal, so B is a DVR. Here, the ramification index $e = 1$, $f = n$, $\mathfrak{p} \subset A$ is inert, and unramified if f mod $\mathfrak{p}$ is separable.

Case 2: Suppose f is Eisenstein; this means that $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_i \in \mathfrak{p}$ but $a_0 \notin \mathfrak{p}^2$. (This actually implies f is irreducible too.) In this case $f = x^n$ mod $\mathfrak{p}$, so there is also only one maximal ideal in B, corresponding to $(\mathfrak{p}, x) = (a_0, x)$. But since $a_0 = -(x^n + \cdots + a_1 x)$, $a_0 \in (x)$. So the unique maximal ideal is just (x), so B is also a DVR. Also, we check that $B/(x) = A/\mathfrak{p}$, so $f = 1$, $e = n$, and $\mathfrak{p}$ is totally ramified.

We now study the converse of the above. Suppose in the AKLB setup, $[L : K] = n$, and we assume in addition that A is a DVR. Then the following are true:

2.6.3. Proposition. *If B is a DVR, with maximal ideal $\mathfrak{m}$, such that $[B/\mathfrak{m} : A/\mathfrak{p}] = n$, then $B \cong A[x]/(f(x))$ for some monic $f \in A[x]$ irreducible mod $\mathfrak{p}$.*

Proof. By the primitive element theorem, there exists $\overline{b} \in B/\mathfrak{m}$ that generates it over $A/\mathfrak{p}$, which is represented by $b \in B$. Let $f(x) \in A[x]$ be the characteristic polynomial of b over K. We have $f(b) = 0$, so the image $\overline{f}$ of f in $(A/\mathfrak{p})[x]$ has $\overline{b}$ as a root. Since $\overline{b}$ is of degree n over $A/\mathfrak{p}$, $\overline{f}$ is irreducible of degree n. So by the discussion above: $A[x]/(f(x))$ is a DVR, and there is an inclusion $A[x]/(f(x)) \hookrightarrow B$ mapping $x \mapsto b$. Since $L = K(b)$, $L = \operatorname{Frac} A[x]/(f(x))$ as well, and because B is an intermediate ring between a DVR and its field of fractions, and $B \neq L$, it must be that $B = A[x]/(f(x))$. □

2.6.4. Proposition. *If B is a DVR, with the discrete valuation $w : L^\times \to \mathbb{Z}$, and w extends the valuation v on A with index n, then $B \cong A[x]/(f(x))$ for some Eisenstein polynomial $f \in A[x]$.*

Proof. Pick $\beta \in B$ such that $w(\beta) = 1$. Let $f \in A[x]$ be the characteristic polynomial of β in K. We wish to show that it is Eisenstein. Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (the fact that it has degree n follows from the same argument as follows). Then $\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = 0$ in B. Since $w(a_i\beta^i) \equiv i \pmod{n}$, and the two terms with smallest w have to have the same valuation, we conclude that $w(a_0) = w(\beta^n) = n$, so $v(a_0) = 1$ and $v(a_i) \geq 1$ for $i = 1, \ldots, n-1$. Also, $A[x]/(f(x))$ is a DVR that injects into B, so $A[x]/(f(x)) = B$. □

3. Galois extensions

3.1. Galois extensions. We now consider the following "AKLBG" setup: in addition to having the original AKLB, we require L/K to be a finite *Galois* extension with $G = \operatorname{Gal}(L/K)$.

3.1.1. Proposition. *Fix a nonzero prime $\mathfrak{p} \subset A$. Then the G-action on L induces a transitive G-action on $\{\mathfrak{q} \subset B : \mathfrak{q} \mid \mathfrak{p}\}$.*

Proof. Fix on $\mathfrak{q}$ above $\mathfrak{p}$. If $\mathfrak{q}'$ above $\mathfrak{p}$ is not in the orbit of $\mathfrak{q}$, then by prime avoidance, we may find $b \in \mathfrak{q}'$, such that $b \notin g\mathfrak{q}$ for all $g \in G$. This means that $gb \notin \mathfrak{q}$ for all $g \in G$. Consider the norm $\mathrm{N}_{L/K}(b) = \prod_{g \in G} gb \in A$, then $\mathrm{N}_{L/K}(b) \in \mathfrak{q}'$ but $\mathrm{N}_{L/K}(b) \notin \mathfrak{q}$. This is a contradiction to $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. □

Because of this, the $e_\mathfrak{q}$ and $f_\mathfrak{q}$ are the same for all $\mathfrak{q} \mid \mathfrak{p}$, for any fixed $\mathfrak{p}$, so we can just call them $e_\mathfrak{p}$ and $f_\mathfrak{p}$. Also, let $g_\mathfrak{p}$ denote the number of primes above $\mathfrak{p}$. Then:

3.1.2. Proposition. *$e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = n$.*

3.2. Decomposition group. Fix $\mathfrak{q}$ a prime upstairs. Define the *decomposition group* $D = D_{\mathfrak{q}} \leq G$ as the stabilizer of $\mathfrak{q}$ in G. Then $(G : D) = g_{\mathfrak{q}}$ by the orbit-stabilizer theorem, so $|D| = e_{\mathfrak{p}} f_{\mathfrak{p}}$.

The reason we define D is that while G preserves B and permutes the primes $\{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{p}\}$, D preserves both B and $\mathfrak{q}$, which means that it acts on $B/\mathfrak{q}$.

3.2.1. Proposition. *Suppose $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$. Then:*

- *$B/\mathfrak{q}$ is Galois over $A/\mathfrak{p}$;*
- *The natural map $D \to \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is surjective. (Here, $\mathbb{F}_{\mathfrak{q}} = B/\mathfrak{q}$, $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$.)*

PROOF. For the first bullet point, it suffices to show that $B/\mathfrak{q}$ is normal over $A/\mathfrak{p}$. Given $\overline{b} \in B/\mathfrak{q}$, represented by $b \in B$, we let $P(x) = \prod_{g \in G}(x - gb)$. This polynomial is G-invariant, hence is in $K[x]$, hence in $A[x]$. Reducing modulo $\mathfrak{q}$, we get $\overline{P}(x) = \prod_{g \in G}(x - g\overline{b}) \in (A/\mathfrak{p})[x]$. This shows that $\overline{b}$ is the root of a polynomial in $(A/\mathfrak{p})[x]$ that splits completely, so the extension is indeed normal.

For the second bullet point, by primitive element theorem, $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_{\mathfrak{p}}(\overline{b})$ for some nonzero $\overline{b} \in \mathbb{F}_{\mathfrak{q}}$. Strong approximation gives us $b \in B$ such that $b = \overline{b}$ mod $\mathfrak{q}$ and $b \in \mathfrak{q}'$ for all other $\mathfrak{q}' \mid \mathfrak{p}$. Then $gb \in \mathfrak{q}$ for all $g \in G \backslash D$. Let $P(x) = \prod_{g \in G}(x - gb) \in A[x]$, then reducing mod $\mathfrak{q}$, we get $\overline{P}(x) = \prod_{g \in G}(x - g\overline{b}) \in \mathbb{F}_{\mathfrak{p}}[x]$. But since $g\overline{b} = 0$ in $\mathbb{F}_{\mathfrak{p}}$, $\overline{P}(x) = \prod_{g \in D}(x - g\overline{b})x^{|G|-|D|}$. Since $\overline{P}(b) = 0$, every conjugate of $\overline{b}$ is a nonzero root of $\overline{P}(x)$, hence equals $g\overline{b}$ for some $g \in D$. This shows that $D \to \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is surjective. □

3.3. Inertia group.

3.3.1. Definition. The *inertia group* $I_{\mathfrak{q}}$ satisfies the short exact sequence

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \to \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \to 1.$$

In other words, $I_{\mathfrak{q}}$ consists of the elements of G that preserve B and $\mathfrak{q}$, and act as the identity on $B/\mathfrak{q} = \mathbb{F}_{\mathfrak{q}}$.

Because $|D| = ef$, $|\operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})| = [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}] = f$, we see that $|I| = e$. So the inertia group "detects" ramification in some sense.

By Galois theory, the sequence of subgroups $1 \leq I \leq D \leq G$ corresponds to a tower of fields $L \supseteq L^I \supseteq L^D \supset K$, where L^I is the *inertia field* and L^D is the *decomposition field*. Computing the group indices, we get $[L : L^I] = e$, $[L^I : L^D] = f$, $[L^D : K] = g$.

In addition, I and D behave well under sub- and quotient groups, as follows: fix AKLBG, and let H be a subgroup of G. Let $L^H \subset L$ be the fixed field of H. The corresponding $B^H \subset L^H$ is the integral closure of A in L^H, then B is the integral closure of L^H in K by transitivity of integrality. Fixing $\mathfrak{q} \subset B$, it pulls back to $\mathfrak{q}^H \subset B^H$ and $\mathfrak{p} \subset A$, and similarly we have a tower of fields $\mathbb{F}_{\mathfrak{q}} \supset \mathbb{F}_{\mathfrak{q}^H} \supset \mathbb{F}_{\mathfrak{p}}$. For the Galois extension L/L^H, we can similarly define the inertia and composition groups $I_H \leq D_H \leq H$.

3.3.2. Proposition. *$D_H = D \cap H$, $I_H = I \cap H$.* □

If, in addition, H is a *normal* subgroup, then L^H/K is Galois as well, with Galois group G/H. Then:

3.3.3. Proposition. *The following diagram commutes and has exact rows and columns:*

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & I_H \arrow[r] \arrow[d] & D_H \arrow[r] \arrow[d] & \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{q}^H}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I_{G/H} \arrow[r] \arrow[d] & D_{G/H} \arrow[r] \arrow[d] & \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}^H}/\mathbb{F}_{\mathfrak{p}}) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

3.4. Frobenius class. Now, we consider the case where $\mathbb{F}_\mathfrak{p}$ is a *finite field*. Then it is a well-known result that finite extensions of finite fields are always cyclic and generated by the Frobenius element

$$\mathrm{Frob}_\mathfrak{q} : x \mapsto x^{|\mathbb{F}_\mathfrak{p}|}.$$

Suppose L/K is unramified at $\mathfrak{q}$, then $D \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is a cyclic group, and we can view $\mathrm{Frob}_\mathfrak{q}$ as an element in D with order f.

For $\mathfrak{q}' \mid \mathfrak{p}$, $\mathfrak{q}' = \sigma\mathfrak{q}$ for some $\sigma \in G$, so $D_{\mathfrak{q}'} = \sigma D \sigma^{-1}$ are conjugate subgroups of G, and $\mathrm{Frob}_{\mathfrak{q}'} = \sigma \,\mathrm{Frob}_\mathfrak{q} \,\sigma^{-1}$. Therefore, $\mathfrak{p}$ determines a conjugacy class in G, called the *Frobenius class*. (So if G is abelian, the Frobenius class is actually an element in G.)

3.4.1. Definition. Assume AKLBG with finite residue fields. For $\mathfrak{q}$ unramified, define the Artin symbol

$$\mathrm{pr}\,\frac{L/K}{\mathfrak{q}} := \mathrm{Frob}_\mathfrak{q}\,.$$

When G is abelian, this only depends on $\mathfrak{p}$, so we may instead write $\mathrm{pr}\,\frac{L/K}{\mathfrak{p}}$.

3.4.2. Definition (Artin map)**.** Let A be Dedekind, $K = \mathrm{Frac}\, A$, L/K abelian extension. There is a homomorphism from the subgroup of the ideal group $\mathcal{I}_A$ generated by unramified primes to G, given by

$$\prod \mathfrak{p}_i^{e_i} \mapsto \prod \mathrm{pr}\,\frac{L/K}{\mathfrak{p}_i}^{e_i}.$$

3.4.3. Remark. Here's how to determine the splitting type of a prime in a separable but not necessarily Galois field extension. Assume AKLB, and let M be the Galois closure of L/K. (So M is the splitting field of the minimal polynomial of α, where $L = K(\alpha)$).

Let $G = \mathrm{Gal}(M/K)$, then G naturally embeds into S_n by permuting the n maps $\mathrm{Hom}_K(L, M)$. The subgroup of G corresponding to L is $H = G \cap S_{n-1}$, where S_{n-1} is the subgroup of all permutations fixing the identity embedding $L \hookrightarrow M$. Because the G-action on $\mathrm{Hom}_K(L, M)$ is transitive, this action is exactly the G-action on $H\backslash G$, the right cosets of H.

Fix a prime $\mathfrak{p} \subset A$ that we want to study. Suppose C is the integral closure of B in M, and fix an arbitrary prime $\mathfrak{P} \subset C$ above $\mathfrak{p}$. Let $I \subseteq D \subseteq G$ be the inertia and decomposition groups of $\mathfrak{P}$. Then the transitive G-action on $H\backslash G$ induces a D-action on $H\backslash G$.

The main claim here is that the orbits of this D-action corresponds precisely to the primes $\mathfrak{q} \subset B$ above $\mathfrak{p}$, and the size of the orbit corresponding to $\mathfrak{q}$ is $e_\mathfrak{q} f_\mathfrak{q}$. Proof of this claim: given some orbit $[Hg]$ of $H\backslash G$ under D, we map this to $g\mathfrak{P} \cap L$.

- Injectivity: suppose $g_1\mathfrak{P} \cap L = g_2\mathfrak{P} \cap L = \mathfrak{q}$, then $g_1 g_2^{-1}$ maps $g_2\mathfrak{P}$ to some prime that is also above $\mathfrak{q}$. Because L/M is Galois, there is an element $h \in H \subset G$ mapping $g_1\mathfrak{P}$ back to $g_2\mathfrak{P}$. Then $h g_1 g_2^{-1} \in D$, so $[Hg_1] = [Hg_1(g_2^{-1} g_2)] = [H(hg_1g_2^{-1})g_2] = [Hg_2]$.
- Surjectivity: follows because G is transitive on the primes in C above $\mathfrak{p}$.
- Size of the orbit: by orbit-stabilizer theorem, this is equal to $\frac{|D_{\mathfrak{P}/\mathfrak{p}}|}{|D_{\mathfrak{P}/\mathfrak{q}}|} = \frac{e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}}{e_{\mathfrak{P}/\mathfrak{q}} f_{\mathfrak{P}/\mathfrak{q}}} = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$.

Even better, we have that $I \trianglelefteq D$ is normal, so every I-orbit in a D-orbit corresponding to $\mathfrak{q}$ (of size $e_\mathfrak{q} f_\mathfrak{q}$) has the same size. By orbit-stabilizer theorem, this size is $\frac{|I_{\mathfrak{P}/\mathfrak{p}}|}{|I_{\mathfrak{P}/\mathfrak{q}}|} = e_{\mathfrak{q}/\mathfrak{p}}$. Notice that:

- When L/K is already Galois, $H = \{1\}$, and every orbit of the D-action on G (i.e. the D-cosets) have the same size.
- When $\mathfrak{p}$ is unramified and residue fields are finite (e.g. K, L are local fields), D is generated by the Frobenius element, so D-orbits are the same as the orbits of Frobenius.

Reference: Melanie Wood.

4. Completeness and local fields

4.1. Local fields.

4.1.1. Definition. A *local field* is a field K with a nontrivial absolute value that is locally compact.

Recall that

- An absolute value induces a metric, which induces a topology on K, under which K is a topological field;

- A locally compact space is one where each point x has a compact neighborhood, i.e. $x \in U \subset K$ where U is open and K is compact.

4.1.2. Proposition. *Suppose the absolute value on K is induced by a discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$. Then K is locally compact, iff K is complete and the residue field is finite.*

Proof. ($\Longrightarrow$) It is clear that K is Hausdorff. If K is locally compact, then each point of K has a local base of closed compact neighborhoods. Given any Cauchy sequence, we can find a descending, nested sequence of closed compact sets, so by Cantor intersubsection theorem there is a unique point inside all of them whence the sequence converges. Let A be the valuation ring and π a uniformizer. Also, since some $\pi^n A$ is compact, multiplying by π^{-n} shows that A is compact, so $A/\pi A$ is compact and discrete, hence finite.

($\Longleftarrow$) If $A/\pi A$ is finite, then $A/\pi^n A$ is also finite. Then $\widehat{A} = \varprojlim A/\pi^n A$ is a closed subset of $\prod_{n\geq 0} A/\pi^n A$, which is compact by Tychonoff. So $\widehat{A} = A$ is compact, so $\pi^n A$ is compact, and they form a basis of compact open neighborhoods of K. □

4.1.3. Proposition. *Let F be a global field, with a nontrivial absolute value $| \,|_v$. Then its completion F_v with respect to this absolute value is a local field.*

Proof. If the absolute value is archimedean, then F must be a finite extension of $K = \mathbb{Q}$, and the absolute value must restrict to the usual Euclidean one on $\mathbb{Q}$. So F_v is a finite extension of $\mathbb{R}$, which is either $\mathbb{R}$ or $\mathbb{C}$. These are local fields.

If the absolute value is nonarchimedean, I claim that it is induced by a discrete valuation. Let $C = B_{\leq 1}(0)$ and $\mathfrak{m} = B_{<1}(0)$, which are nonempty because $| \,|_v$ is nontrivial. Consider the absolute value $| \,|_v$ restricted to $K = \mathbb{Q}$ or $\mathbb{F}_p(t)$. By Ostrowski's theorem, this is induced by some discrete valuation v on $A = \mathbb{Z}$ or $\mathbb{F}_p[t]$. Then $A \subset C$, and since C is integrally closed, it contains B, the integral closure of A in F. Let $\mathfrak{q} = \mathfrak{m} \cap B$, then $B_{\mathfrak{q}} \subset C$. But since there are no intermediate rings between a DVR and its fraction field, $B_{\mathfrak{p}} = C$. Therefore, the absolute values $| \,|_v$ and the one induced by $v_{\mathfrak{q}}$ have the same valuation rings, hence equivalent.

Now, F_v evidently has finite residue field, so it is a local field. □

4.1.4. Lemma. *A locally compact topological vector space over a nondiscrete locally compact field has finite dimension.*

4.1.5. Theorem. *Any local field is either $\mathbb{R}, \mathbb{C}$, or a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.*

4.2. Hensel's lemma.

4.2.1. Lemma (Hensel's lemma)**.** *Let A be a complete DVR with residue field k, $F \in A[x]$, and $f \in k[x]$ be the image of F. Suppose $\alpha \in k$ is a simple root of f, then there exists a unique $a \in A$ lifting α, such that $F(a) = 0$.*

4.2.2. Lemma (Hensel's lemma, stronger)**.** *Let A, k, F, f as before. If $f(x) = g(x)h(x)$, where g, h are coprime monic polynomials in $k[x]$, then $F(x) = G(x)H(x)$, with $G, H \in A[x]$ lifting g, h.*

4.3. Extensions of complete DVRs.

4.3.1. Theorem. *In the AKLB setup, assume A is a* complete DVR *with prime ideal $\mathfrak{p}$. Then B is a DVR, i.e. there is only 1 prime above $\mathfrak{p}$.*

(In fact, this holds even when L/K is finite and not necessarily separable — see Serre's book.)

First proof. Suppose there are at least two primes $\mathfrak{q}_1, \mathfrak{q}_2$ above $\mathfrak{p}$. Pick $b \in \mathfrak{q}_1, b \notin \mathfrak{q}_2$, then $\mathfrak{q}_1 \cap A[b]$ and $\mathfrak{q}_2 \cap A[b]$ are distinct primes in $A[b]$, both containing $\mathfrak{p}$. So $A[b]/\mathfrak{p}A[b]$ has at least 2 primes as well. Now, let $F(x) \in A[x]$ be the minimal polynomial of b in K, so that

$$\frac{A[b]}{\mathfrak{p}A[b]} \cong \frac{A[x]}{(F(x), \mathfrak{p})} \cong \frac{k[x]}{(f(x))}$$

where f is the reduction of F mod $\mathfrak{p}$. Because $k[x]/(f(x))$ has at least 2 primes, f factors into coprime monic $g, h \in k[x]$, which we lift into a factorization of F by Hensel's lemma. But this contradicts the irreducibility of F. □

4.3.2. Lemma. *If $(K, |\cdot|)$ is complete and V is a f.d. vector space over K, then any two norms are equivalent.*

Second proof. Each prime $\mathfrak{q} \mid \mathfrak{p}$ defines an norm on L (as a f.d. K-vector space) extending the absolute value on K. It suffices then to find a way to characterize $\mathfrak{q}$ in terms of the topology it induces. In fact, for $x \in L$, x is in the valuation ring of $\mathfrak{q}$ iff the sequence $x^{-1}, x^{-2}, \dots$ does not converge to 0, so the topology uniquely characterizes the valuation ring of $\mathfrak{q}$, which uniquely characterizes $\mathfrak{q}$ as its maximal ideal. □

Some corollaries of the above theorem:

- B is a DVR and a free A-module of rank n.
- There exists a unique discrete valuation w on L extending v on K, with index e.
- B and L are complete with respect to w. (since it is equivalent to the sup norm, which is complete)
- If $x, y \in L$ are conjugate over K, then $w(x) = w(y)$. (suppose $y = \sigma x$, then w and $w \circ \sigma$ are two discrete valuations extending v, so they are the same)
- For $x \in L$, $w(x) = \frac{1}{f} v(\mathrm{N}_{L/K}(x))$. (use the ideal norm interpretation)

4.3.3. Corollary. *The valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ is the restriction of a unique valuation $\overline{K} \twoheadrightarrow \mathbb{Q} \cup \{\infty\}$.*

Proof. For each finite algebraic extension L/K, v can be uniquely extended to L. The map $\overline{K} \to \mathbb{Q} \cup \{\infty\}$ is surjective because $\overline{K}$ contains all nth roots. □

However, by taking the algebraic closure, $\overline{K}$ is no longer complete! For example, $\overline{\mathbb{Q}_p}$ has a valuation with value group $\mathbb{Q}$ and residue field $\overline{\mathbb{F}_p}$, but it is not complete anymore. So we can define $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$, which is complete, but it is not obvious that it is still algebraically closed. Fortunately:

4.3.4. Theorem. *Let K be a field complete with respect to a nontrivial non-archimedean absolute value. Then the completion of $\overline{K}$ is algebraically closed.*

Proof. See Brian Conrad's handout here. □

4.4. Newton polygons. Let K be a field with a valuation $v : K \to \mathbb{R} \cup \{\infty\}$ (not necessarily surjective). For a polynomial $f(x) = a_n x^n + \cdots + a_0 \in K[x]$, we may construct its *Newton polygon* as the lower convex hull of the points $(i, v(a_i))$. The main theorem is the follows:

4.4.1. Theorem. *The width of the slope s segment of the Newton polygon is at least the number of zeros of f with valuation $-s$, with equality when f splits completely into linear factors.*

Note that this provides additional motivation for Eisenstein's criterion.

Proof. WLOG pass to the case $K = \overline{K}$. First, notice that changing $f(x)$ to $f(ax)$ or $af(x)$ by any constant $a \in K^\times$ does not alter the content of the theorem. As such we can reduce to the case $s = 0$ and suppose f factors as

$$f(x) = \prod_{i=1}^{a}(x - r_i) \prod_{j=1}^{b}(x - t_j) \prod_{k=1}^{c}(1 - x/u_k) \in A[x]$$

where $v(r_i) > 0$, $v(t_j) = 0$, and $v(u_k) < 0$. Reducing modulo the maximal ideal of A, we get

$$\overline{f}(x) = x^a \prod_{j=1}^{b}(x - \overline{t_j}).$$

This means that the Newton polygon of f has a segment from $(a, 0)$ to $(a + b, 0)$, which has width b equal to the number of zeros of f with valuation 0. □

4.5. p-adic analysis. Let K be complete with respect to a nonarchimedean aboslute value, i.e. coming from some valuation. Because we have a notion of size, we can do "p-adic analysis" much like how we do real or complex analysis. But here, lots of small errors cannot add up to a big error because of the nonarchimedean triangle inequality, so very nice things hold.

For example, for a sequence $a_0, a_1, \dots \in K$, the series $\sum a_n$ converges if and only if $a_n \to 0$.

For another example, we have the Cauchy-Hadamard formula for the radius of convergence: given $f(x) = \sum a_n x^n \in K[[x]]$, its radius of convergence

$$R = \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}}.$$

4.5.1. Theorem (Strassmann's theorem). *Let A be the valuation ring of K, $f(x) = \sum a_n x^n \in A[[x]]$ a nonzero formal power series such that $a_n \to 0$. Then the number of zeros of $f(x)$ in A is at most N, where N is the largest such that $|a_N| = \max |a_n|$.*

We now specialize to the case $K = \mathbb{C}_p$. Here, we have the p-adic exponential function

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n} \in \mathbb{Q}_p[[x]].$$

Its radius of convergence is $R = p^{-\frac{1}{p-1}}$. Using the Newton polygon, we see that the truncated exp has no roots with valuation at least $\frac{1}{p-1}$.

Conversely, we may wish to find a p-adic logarithm. There is a natural one, called the Iwasawa logarithm.

4.5.2. Proposition. *There exists a unique homomorphism*

$$\log : \mathbb{C}_p^\times \to (\mathbb{C}_p, +)$$

satisfying:

1. *For $|x| < 1$, $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$;*
2. *$\log p = 0$.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of the valuation ring of $\mathbb{C}_p$. Construct the logarithm in stages:

- First, for $x \in \mathfrak{m}$, define $\log(1+x)$ according to the infinite series. Then
$$\log(1+x) + \log(1+y) = \log((1+x)(1+y))$$
holds as an identity on power series, so it holds as numbers in $\mathbb{C}_p$.
- Second, for $x \in G = p^{\mathbb{Z}}(1+\mathfrak{m})$, define $\log(p^n(1+x)) = \log(1+x)$.
- Third, we claim that $\mathbb{C}_p^\times/G$ is in fact torsion. This would allow us to uniquely extend log to the entire $\mathbb{C}_p^\times$. To show this is torsion, let $\mathcal{O} = \{x \in \mathbb{C}_p : v(x) = 0\}$ be the group of units in the valuation ring, and notice that
$$\mathcal{O}^\times/(1+\mathfrak{m}) \to \mathbb{C}_p^\times/G \xrightarrow{v_p} \mathbb{Q}/\mathbb{Z}$$
is exact. The left side is isomorphic to $\overline{\mathbb{F}_p}^\times$, which is torsion; the right side is also torsion. So the middle term must be torsion as well, which finishes the proof.

□

4.6. Completing a Dedekind extension. Let us start with an example. We wish to compute field extensions of $\mathbb{Q}_p$ such as $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_p$. This is clearly an étale algebra over $\mathbb{Q}_p$, and depending on how x^2+1 factors in $\mathbb{Q}_p[x]$ (read: in $\mathbb{F}_p[x]$, because of Hensel's lemma), it is either

- $\mathbb{Q}_p \times \mathbb{Q}_p$, in the case that x^2+1 factors into two distinct factors (e.g. $p = 5$). There are two primes above $p\mathbb{Z}_p$.
- a totally ramified extension over $\mathbb{Q}_p$, in the case that x^2+1 factors into the same factors (e.g. $p = 2$). There is one prime above $p\mathbb{Z}_p$ with $e = 2$, $f = 1$.
- an unramified extension over $\mathbb{Q}_p$, in the case that x^2+1 does not factor (e.g. $p = 7$). There is one prime above $p\mathbb{Z}_p$ with $e = 1$, $f = 2$.

The following theorem generalizes the previous example.

4.6.1. Theorem. *Assume AKLB, and fix a prime $\mathfrak{p} \subset A$ and the valuation $v = v_{\mathfrak{p}}$ on K. Let w_i be the distinct discrete valuations on L extending v, which are in bijection with primes $\mathfrak{q} \mid \mathfrak{p}$. Let $\widehat{K}$ be the completion of K wrt v, and let $\widehat{L}_i$ be the completions of L wrt w_i. Then:*

1. *$\widehat{L}_i/\widehat{K}$ is a field extension;*
2. *The induced $\widehat{w_i}$ on $\widehat{L}_i$ is the unique extension of $\widehat{v}$ on $\widehat{K}$.*

(3) $e(\widehat{w_i}/\widehat{v}) = e_i$, *and* $f(\widehat{w_i}/\widehat{v}) = f_i$.
(4) $[\widehat{L}_i : \widehat{K}] = e_i f_i$.
(5) $L \otimes_K \widehat{K} \to \prod_i \widehat{L}_i$ *is an isomorphism.*

Proof. (1) through (4) are easy. For (5), there is a natural K-bilinear $L \times \widehat{K} \to \prod_i \widehat{L}_i$ given by $(\ell, \alpha) \mapsto \ell\alpha$, which induces a linear map $L \otimes_K \widehat{K} \to \prod_i \widehat{L}_i$. To show this is an isomorphism, it suffices to show this is surjective, since both sides have the same $\widehat{K}$-dimension ($n = \sum_i e_i f_i$).

Choose a $\widehat{K}$-basis α_i ($i = 1, 2, \ldots, n$) for $\prod_i \widehat{L}_i$. For each α_i, using weak approximation, we could find $\ell_i \in L$ such that its diagonal embedding into $\prod_i L_i$ is close to α_i. Then these ℓ_i still forms a basis (because the change-of-basis matrix is close enough to id). This shows surjection, as desired. □

4.6.2. Proposition. *If, in addition, L/K is Galois, then each $\widehat{L}_i/\widehat{K}$ is Galois as well, with Galois group D_i.*

Proof. Each $\sigma \in D_i$ acts on L respecting w_i, so it acts on $\widehat{L}_i$ fixing $\widehat{K}$. This gives a homomorphism $\phi : D_i \to \operatorname{Aut}(\widehat{L}_i/\widehat{K})$. Conversely, there is a map $\psi : \operatorname{Aut}(\widehat{L}_i/\widehat{K}) \to D_i$ by restricting to L. Since $\psi \circ \phi = \mathrm{id}$, ϕ is injective. But

$$e_i f_i = |D_i| \le |\operatorname{Aut}(\widehat{L}_i/\widehat{K})| \le [\widehat{L}_i : \widehat{K}] = e_i f_i,$$

so all inequalities must be equal, and $\widehat{L}_i/\widehat{K}$ is Galois. □

4.6.3. Proposition. *Let B_i be the valuation of v_i on L. Then $B \otimes_A \widehat{A} \cong \prod_i \widehat{B_i}$.*

Proof. Both sides are free $\widehat{A}$-modules of rank n. So it suffices to check isomorphism after reducing mod $\widehat{p}$. The LHS reduces to $B/\mathfrak{p}B$, and the RHS reduces to $\prod_i B/\mathfrak{q}_i^{e_i} B$, and the two are equal by CRT. □

5. Ramification

5.1. The different. Setup: AKLB. Recall that an *A-lattice* M is a finitely generated A-submodule of L, such that $MK = L$. Then we can define its *dual* as

$$M^* = \{x \in L : \operatorname{Tr}(xm) \in A, \forall m \in M\}.$$

If M is free, then so is M^* (with the dual basis). If M is a B-module (i.e. a fractional B-ideal), then so is M^*.

5.1.1. Definition. The *different ideal* $\mathcal{D}_{B/A}$ is defined as the inverse of the dual of B as an A-lattice:

$$\mathcal{D}_{B/A} := (B^*)^{-1}.$$

This is in fact an actual ideal inside B, since $B \subseteq B^* \implies (B^*)^{-1} \subseteq B$.

5.1.2. Proposition. *For any prime $\mathfrak{p} \subset A$, $(\mathcal{D}_{B/A})_{\mathfrak{p}} = \mathcal{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$.*

5.1.3. Proposition. *For primes $\mathfrak{q} \mid \mathfrak{p}$, $\mathcal{D}_{B/A} \cdot \widehat{B_{\mathfrak{q}}} = \mathcal{D}_{\widehat{B_{\mathfrak{q}}}/\widehat{A_{\mathfrak{p}}}}$. (Both sides are ideals in $\widehat{B_{\mathfrak{q}}}$.)*

Proof. Assume WLOG A is a DVR with maximal ideal $\mathfrak{p}$, by localizing. Let $\widehat{L} = L \otimes_K \widehat{K} = \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{L_{\mathfrak{q}}}$, and $\widehat{B} = B \otimes_A \widehat{A} = \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B_{\mathfrak{q}}}$ (cf. previous subsection). Even though $\widehat{L}$ may not be a field, it is still an étale $\widehat{K}$-algebra, so the trace pairing is still nondegenerate. Consequently, we can form $\widehat{B}^* = B^* \otimes_A \widehat{A} = \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B_{\mathfrak{q}}}^*$. This shows that B^* generates each $\widehat{B_{\mathfrak{q}}}^*$ over $\widehat{A}$, so $\mathcal{D}_{B/A}$ generates $\mathcal{D}_{\widehat{B_{\mathfrak{q}}}/\widehat{A_{\mathfrak{p}}}}$ as desired. □

5.2. The discriminant. The different $\mathcal{D}_{B/A}$ is an ideal in B. We will define another ideal, the *discriminant* $D_{B/A}$, which is an ideal in A.

5.2.1. Definition. Given elements $e_1, \ldots, e_n \in L$, their *discriminant*

$$\operatorname{disc}(e_1, \ldots, e_n) = \det(\operatorname{Tr}(e_i e_j))_{i,j}.$$

This has the following properties:

- If $e_1, \ldots, e_n \in B$, $\operatorname{disc}(e_1, \ldots, e_n) \in A$.

- Suppose $\phi \in \operatorname{End}_K(L)$ mapping $e_1, \ldots, e_n$ to $e'_1, \ldots, e'_n$, then
$$\operatorname{disc}(e'_1, \ldots, e'_n) = (\det \phi)^2 \operatorname{disc}(e_1, \ldots, e_n).$$
- Let M be a free A-lattice. For two bases of M, their discriminants must differ by the square of a unit in A (which must be 1 when $A = \mathbb{Z}$!)

5.2.2. Definition. Assuming AKLB and given an A-lattice M:

- When $A = \mathbb{Z}$, M is necessarily free, and $\operatorname{disc} M \in \mathbb{Z}$ is an integer (given by the discriminant of any set of A-basis of M).
- When A is general and M is a free A-module, the discriminant $D(M)$ is the principal (fractional) ideal generated by the discriminant of any basis of M.
- When A, M are both general: the discriminant $D(M)$ is the A-module generated by $\operatorname{disc}(x_1, \ldots, x_n)$ for any n elements $x_1, \ldots, x_n \in M$.

5.2.3. Proposition. *The discriminant $D(M)$ is finitely generated over A, and therefore it is a fractional A-ideal.*

Proof. Choose independent elements $e_1, \ldots, e_n \in M$ generating L/K, and let N be the free A-lattice generated by them. Then $M \subseteq a^{-1}N$ for some $a \in A$, so $D(M) \subseteq D(a^{-1}N)$. The latter is generated by 1 element, so it is a Noetherian A-module, so $D(M)$ is finitely generated. □

5.2.4. Proposition. *For any prime $\mathfrak{p} \subset A$, $(D_{B/A})_{\mathfrak{p}} = D_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$.*

5.2.5. Proposition. *Let L/K be a finite separable extension with degree n, and suppose $\sigma_i : L \to \Omega$ are n distinct elements in* $\operatorname{Hom}_K(L, \Omega)$*. Then given $e_1, \ldots, e_n \in L$,*
$$\operatorname{disc}(e_1, \ldots, e_n) = \det(\sigma_i(e_j))^2_{i,j}.$$

Proof. $\operatorname{Tr}(e_i e_j)_{ij} = (\sum_k \sigma_k(e_i)\sigma_k(e_j))_{ij} = (\sigma_k(e_i))_{ik}(\sigma_j(e_k))_{jk}$. □

5.2.6. Proposition. *For $x \in L$,*
$$\operatorname{disc}(1, x, x^2, \ldots, x^{n-1}) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2.$$

Proof. This is the Vandermonde determinant. □

5.2.7. Definition. If $f = \prod(x - \alpha_i)$, then the *discriminant* of this polynomial
$$\operatorname{disc} f = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

5.2.8. Proposition. *If A is a Dedekind domain, $f \in A[x]$ a monic separable polynomial, then* $\operatorname{disc}(f) = \operatorname{disc}(1, x, x^2, \ldots, x^{n-1})$.

5.2.9. Definition. The *discriminant* ideal $D_{B/A} = D(B) \subseteq A$, which is an actual ideal in A.

5.2.10. Example. $D_{\mathbb{Z}[i]/\mathbb{Z}} = (-4) = (4)$.

5.3. Detecting ramification.

5.3.1. Theorem. *Assume AKLB, then $D_{B/A} = N(\mathcal{D}_{B/A})$, where N is the ideal norm.*

Proof. Since everything is compatible with localization, WLOG A is a DVR, so B is free, say with basis $e_1, \ldots, e_n$. Then B^* is free also, with the dual basis $e'_1, \ldots, e'_n$.

In general, if $m_1, \ldots, m_n$ is an A-basis for another free lattice M, then $(\operatorname{Tr}(m_i e_j))$ is the change-of-basis matrix sending $e'_1, \ldots, e'_n$ to $m_1, \ldots, m_n$. Setting $m_i = e_i$, we see that $(\operatorname{Tr}(e_i e_j))$ is the change-of-basis matrix sending $e'_1, \ldots, e'_n$ to $e_1, \ldots, e_n$. Taking the ideal generated by the determinant on both sides, we see that $D_{B/A}$ is equal to the index $(B^* : B)_A = (B : (B^*)^{-1})_A = N(\mathcal{D}_{B/A})$. □

5.3.2. Theorem. *Assume AKLB, $\mathfrak{p} \in A$, $\mathfrak{q} \mid \mathfrak{p}$. Then L/K is unramified at $\mathfrak{q}$ iff $\mathfrak{q} \nmid \mathcal{D}_{B/A}$.*

Proof. In the general case, first localize, then complete with respect to the unique discrete valuation to reduce to the case where A is a *complete* DVR. Then B is a DVR as well, with $\mathfrak{p}B = \mathfrak{q}^e$. The different is a power of $\mathfrak{q}$, $\mathcal{D}_{B/A} = \mathfrak{q}^m$, for some $m \geq 0$. Then $D_{B/A} = N(\mathcal{D}_{B/A}) = \mathfrak{p}^{fm}$. Pick an A-basis $b_1, \dots, b_n$ of B, and let $\overline{b_1}, \dots, \overline{b_n}$ be their images in $B/\mathfrak{p}B$. Then L/K is unramified at $\mathfrak{q}$ if and only if $B/\mathfrak{q}^e = B/\mathfrak{p}B$ is a separable field extension of $A/\mathfrak{p}$, iff $\det(\mathrm{Tr}(\overline{b_i b_j}))_{i,j} \neq 0$, iff $\overline{\det(\mathrm{Tr}(b_i b_j)_{i,j})} \neq 0 \bmod \mathfrak{p}$, iff $\mathfrak{p} \nmid D_{B/A}$, iff $\mathfrak{q} \nmid \mathcal{D}_{B/A}$. □

5.3.3. Corollary. *Assume AKLB, $\mathfrak{p} \in A$, then L/K is unramified at $\mathfrak{p}$ (i.e. unramified at all primes above $\mathfrak{p}$) iff $\mathfrak{p} \nmid D_{B/A}$.*

5.3.4. Corollary. *Only finitely many pimes of B ramify.*

5.3.5. Example. Take $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$ where α is a root of $x^3 - x - 1$. We wish to compute the ring of integers $\mathcal{O}_K$. Clearly, $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Suppose m is the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$. The discriminant $D(\mathbb{Z}[\alpha]) = \mathrm{disc}(1, \alpha, \alpha^2) = \mathrm{disc}(x^3 - x - 1) = -23$. But $\mathrm{disc}\, \mathcal{O}_K = -23/m^2$ is necessarily an integer, so $m = 1$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Moreover, Dedekind-Kummer theorem tells us that the factorization of a prime (p) in $\mathbb{Z}[\alpha]$ corresponds to factorization of $x^3 - x - 1$ modulo p. In the case $p = 23$, the fact that $(23) \mid D_{L/K}$ corresponds to the fact that $x^3 - x - 1 = (x - 10)^2(x - 3)$ is ramified.

5.4. More on the different. There is a neat formula for the different in the case where B is monogenic:

5.4.1. Proposition. *If $B = A[\alpha]$, and f is the minimal polynomial of α, then $\mathcal{D}_{B/A} = (f'(\alpha))$.*

5.4.2. Lemma. *Under the hypotheses above,*

$$\mathrm{Tr}(\alpha^i / f'(\alpha)) = \begin{cases} 0, & \textit{for } i = 0, 1, \dots, n-2 \\ 1, & \textit{for } i = n-1 \end{cases}$$

and for all i, $\mathrm{Tr}(\alpha^i / f'(\alpha)) \in A$.

Proof. Expand both sides of

$$\frac{1}{f(x)} = \sum_{f(\beta)=0} \frac{1}{(x - \beta) f'(\beta)}$$

at infinity, and compare the coefficients. □

Proof of 5.4.1. Let $I = (1/f'(\alpha)) \subseteq B^*$ be the fractional B-ideal, i.e. the A-span of $\alpha^i/f'(\alpha)$ for $i = 0, \dots, n-1$. We compute

$$(B^* : I) = (\det(\mathrm{Tr}(\alpha^{i+j}/f'(\alpha))_{i,j})) = (1)$$

by the lemma, so $B^* = I$, and $\mathcal{D}_{A/B} = (B^*)^{-1} = (f'(\alpha))$. □

5.4.3. Lemma. *Assume AKLB. Let $\mathfrak{a}$ be a fractional ideal of A, $\mathfrak{b}$ a fractional ideal of B. Then $\mathrm{Tr}(\mathfrak{b}) \subseteq \mathfrak{a}$ iff $\mathfrak{b} \subseteq \mathfrak{a}B^*$.*

Proof. Assume WLOG $\mathfrak{a} \neq 0$. Then $\mathrm{Tr}(\mathfrak{b}) \subseteq \mathfrak{a} \iff \mathfrak{a}^{-1}\,\mathrm{Tr}(\mathfrak{b}) \subseteq (1) \iff \mathrm{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq (1) \iff \mathfrak{a}^{-1}\mathfrak{b} \subseteq B^* \iff \mathfrak{b} \subseteq \mathfrak{a}B^*$. □

5.4.4. Proposition. *For a tower AKBLCM, we have that*

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}$$

as ideals of C, and

$$D_{C/A} = N_{L/K}(D_{C/B}) \cdot D_{B/A}^{[M:L]}$$

as ideals of A.

PROOF. For a fractional ideal $\mathfrak{c}$ of C, we have the following equivalence:

$$\begin{aligned}\mathfrak{c} \subseteq \mathcal{D}_{C/B}^{-1} &\iff \operatorname{Tr}_{M/L}(\mathfrak{c}) \subseteq B \\ &\iff \mathcal{D}_{B/A}^{-1} \operatorname{Tr}_{M/L}(\mathfrak{c}) \subseteq \mathcal{D}_{B/A}^{-1} \\ &\iff \operatorname{Tr}_{L/K}(\mathcal{D}_{B/A}^{-1} \operatorname{Tr}_{M/L}(\mathfrak{c})) \subseteq A \\ &\iff \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(\mathcal{D}_{B/A}^{-1}\mathfrak{c})) \subseteq A \\ &\iff \operatorname{Tr}_{M/K}(\mathcal{D}_{B/A}^{-1}\mathfrak{c})) \subseteq A \\ &\iff \mathcal{D}_{B/A}^{-1}\mathfrak{c} \subseteq \mathcal{D}_{C/A}^{-1} \\ &\iff \mathfrak{c} \subseteq \mathcal{D}_{B/A}\mathcal{D}_{C/A}^{-1}.\end{aligned}$$

This implies $\mathcal{D}_{C/B}^{-1} = \mathcal{D}_{B/A}\mathcal{D}_{C/A}^{-1}$, i.e. $\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}$. Taking the ideal norm $N_{M/K}$ of both sides, we get the formula for the discriminant. □

Geometrically, the different ideal corresponds to the *ramification divisor*. Fix an algebraically closed k, and let K be a finite type k-algebra of transcendental degree 1. Then K is a finite extension of $k(t)$, and there is an unique regular projective curve X over k whose function field $K(X) = K$. Here, X serves as the analog of Dedekind rings — the stalk at each non-generic point is a DVR. Moreover, any nonempty proper open subset of X is $\operatorname{Spec} A$ for some Dedekind A.

Now, suppose L/K is a finite separable extension of degree n, and L is the function field of another curve Y. Then there is a dominant morphism $\pi : Y \to X$, and for any nonempty proper open $\operatorname{Spec} A \subset X$, its preimage is $\operatorname{Spec} B \subset Y$. In this case, we return to our familiar AKLB setup, where an ideal of B corresponds to an effective divisor on $\operatorname{Spec} B$. In the case of the different, because the different is compatible with localization, the corresponding divisors on $\operatorname{Spec} B$'s glue together to give a divisor on Y. This is called the ramification divisor R if $\pi : Y \to X$, and the points that appear are exactly primes that ramify.

The ramification divisor appears in the Riemann-Hurwitz formula: $2g_Y - 2 = n(2g_X - 2) + \deg R$.

5.5. Unramified extensions of complete DVRs.

5.5.1. Theorem. *Let A be a complete DVR with residue field k. Let $K = \operatorname{Frac} A$. Then there is an equivalence of categories between the category of finite unramified extensions L/K and the category of finite separable extensions k'/k, given by the functor F mapping L to its residue field k'.*

PROOF. It suffices to show the functor F is essentially surjective and fully faithful.

Essentially surjective: consider a finite separable k'/k, say $k' = k[x]/(\overline{f}(x))$ with $\overline{f}(x)$ monic irreducible separable of degree n. Lift $\overline{f}$ to $f(x) \in K[x]$ (monic, irreducible and separable), and let $L = K[x]/(f(x))$. This is a finite separable extension of K, and suppose its Dedekind ring is B with maximal ideal $\mathfrak{q}$. Then because f is irreducible mod $\mathfrak{q}$, L/K is unramified, with residue field $B \cong A[x]/(f(x))$, so that $B/\mathfrak{q} = A[x]/(f(x), \mathfrak{q}) = k[x]/(\overline{f}(x)) = k'$.

Fully faithful: The map of Homs is given by

$$\operatorname{Hom}_K(L_1, L_2) \to \operatorname{Hom}_A(B_1, B_2) \to \operatorname{Hom}_k(k_1', k_2').$$

The first map is bijective, with inverse given by tensoring a map $B_1 \to B_2$ with K. So we focus on the second map. Write $k_1' = k[x]/(\overline{g}(x)) = k(\overline{\alpha})$, and lift $\overline{\alpha}$ to $\alpha \in B$. Then $L_1 = K(\alpha)$, because $[L_1 : K] = [k_1' : k] = \deg \overline{g}(x)$ is at most the degree of the (monic) minimal polynomial $g(x) \in A[x]$ of α. Then $B_1 = A[\alpha]$ as well, and $\operatorname{Hom}_A(B_1, B_2)$ then corresponds bijectively to the roots of g in B_2. Similarly, $\operatorname{Hom}_k(k_1', k_2')$ corresponds to the roots of $\overline{g}$ in k_2'. But every root of $\overline{g}$ in k_2' lifts uniquely to a root of g in B_2, by Hensel's lemma. This finishes the proof. (In fact, here only the fact that L_1/K is unramified is used, so L_2/K does not need to be unramified for this to hold.) □

5.6. Totally ramified extensions of complete DVRs. Suppose K is a local field, and fix a separable closure K^{sep}/K. The maximal unramified extension of K can be defined as

$$K^{\mathrm{unr}} = \bigcup_{K' \subseteq K^{\mathrm{sep}} : K'/K \text{ f. unram.}} K'.$$

5.6.1. Example. Consider the case $K = \mathbb{Q}_p$. Because $k = \mathbb{F}_p$, the only finite separable extensions of k are $\mathbb{F}_{p^n}$, one for each n. As such, there is one unramified extension of $\mathbb{Q}_p$ of degree n for each n. Therefore, $\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p$ is an infinite Galois extension, with Galois group the profinite integers

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell.$$

Note that $\mathbb{Q}_p^{\mathrm{unr}}$ has value group $\mathbb{Z}$ and residue field $\overline{\mathbb{F}_p}$.

Now, we show that any finite extension can be broken down into an unramified part and a totally ramified part. Let A be a complete DVR, $K = \operatorname{Frac} A$ with residue field k, L/K f. sep. and with residue field ℓ. Assuming that ℓ/k is separable (which is true e.g. for number fields), each unramified subextension of L/K corresponds to a separable subextension of ℓ/k, which is contained in ℓ. So the unramified subextension K'/K corresponding to ℓ/k contains all unramified subextensions of L/K. We have $[K' : K] = [\ell : k] = f$, so $[L : K'] = e$. Also, $f = 1$ for the extension L/K', so in fact it is totally ramified. Furthermore, if L/K is Galois, then $\mathrm{Gal}(L/K') = I_{L/K'} = I_{L/K}$ since everything has size e.

Next, we study totally ramified extensions. Assume AKLB with A, B complete DVRs, L/K totally ramified with residue field k, and let $p = \operatorname{char} k$.

5.6.2. Definition. Say L/K is *tamely ramified* if $p \nmid e$ (which is automatically true when k has characteristic 0). Otherwise, say L/K is *wildly ramified.*

For example, $L = K(\pi^{1/e}) = K[x]/(x^e - \pi)$ is a totally ramified extension of degree e (here π is a uniformizer in K). It turns out that all *tamely* ramified extensions must be of this form:

5.6.3. Theorem. *Assume AKLB as above, L/K totally tamely ramified of degree e. Then $L = K(\pi^{1/e})$ for some uniformizer π.*

Proof. Choose uniformizers π_K of K, π_L of L. Then $[L : K] \geq [K(\pi_L) : K] \geq e = [L : K]$, so $L = K(\pi_L)$. We have $\pi_L^e = u \cdot \pi_K$ for some unit u of B. We wish to get rid of that unit to conclude $L = K(\pi_K^{1/e})$. This requires us to use the tamely ramified condition.

Because A and B have the same residue field, we may assume WLOG $u \equiv 1 \pmod{\mathfrak{q}}$ by adjusting π_K by a unit in A. Now, the polynomial $x^e - u = 0$ has a simple root of 1 in k (since $e \neq 0$), so by Hensel's lemma it has a root in B. In other words, u has an e-th root in B, so we're done. □

5.7. Continuity of roots.

5.7.1. Lemma (Krasner's lemma)**.** *Let K be a field complete with respect to a nontrivial non-archimedean absolute value, and $\overline{K}$ a separable closure of K. Given an element $\alpha \in \overline{K}$, let its Galois conjugates be α_i. If an element $\beta \in \overline{K}$ is such that $|\alpha - \beta| < |\alpha - \alpha_i|$ for all i, then $K(\alpha) \subseteq K(\beta)$.*

Proof. Suppose for contradiction that $\alpha \notin K(\beta)$. Then there exists $\sigma \in \mathrm{Aut}(\overline{K}/K(\beta))$ sending α to $\sigma\alpha \neq \alpha$. Then $|\alpha - \beta| = |\sigma(\alpha - \beta)| = |\sigma\alpha - \beta| > |\alpha - \beta|$, which is a contradiction. □

We use Krasner's lemma to derive a result known as "continuity of roots".

5.7.2. Proposition (Continuity of roots)**.** *Let K be a field complete wrt a nontrivial nonarchimedean absolute value. Then we can uniquely extend the absolute value to $\overline{K}$. Let $f \in K[x]$ be a separable monic irreducible degree n polynomial. If $g \in K[x]$ of degree n has all coefficients sufficiently close to f's, then the following holds:*

- *Each root β of g belongs to a root α of f;*
- *$K(\beta) = K(\alpha)$;*
- *g is separable and irreducible.*

Proof. To start with, it is clear that when f and g are close enough, the roots of g have absolutely bounded size. This is because if $g(\beta) = 0$ where $g(x) = b_n x^n + \cdots + b_0$, then

$$|b_n||\beta|^n = |b_{n-1}\beta^{n-1} + \cdots + b_0| \leq \max(|b_{n-1}||\beta|^{n-1}, \ldots, |b_0|).$$

Now, since $|\beta|$ is bounded by an absolute constant, we have for f, g close enough, if $g(\beta) = 0$,

$$\prod_{i=1}^{n}(\beta - \alpha_i) = f(\beta) \approx g(\beta) = 0.$$

So one of the factors $|\beta - \alpha_i|$ must be small. When f, g are sufficiently close, we can force it to be smaller than all $|\alpha_i - \alpha_j|$ for $i \neq j$, so β belongs to some α_i. Then Krasner's lemma implies $K(\beta) \supseteq K(\alpha_i)$, but the former is of degree at most n over K and the latter is of degree n, so $K(\beta) = K(\alpha_i)$ and g is irreducible and separable. □

5.7.3. Corollary. *Let K be a degree n extension of $\mathbb{Q}_p$. Then there exists a degree n number field F contained in K, such that $F\mathbb{Q}_p = K$.*

Proof. Let $K = \mathbb{Q}_p(\alpha) = \mathbb{Q}_p[x]/(f(x))$ where f is the min. poly of α. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we may approximate f arbitrarily well by some $g \in \mathbb{Q}[x]$. By the continuity of roots, g is separable, irreducible, and has a root $\beta \in \overline{K}$ such that $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha) = K$. Let $F = \mathbb{Q}(\beta)$, then F is a degree n number field such that $F\mathbb{Q}_p = \mathbb{Q}_p(\beta) = K$. □

5.7.4. Corollary. *Choose an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ inside $\overline{\mathbb{Q}_p}$. Then $\overline{\mathbb{Q}}\mathbb{Q}_p = \overline{\mathbb{Q}_p}$.*

5.7.5. Corollary. *The map $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ given by $\sigma \mapsto \sigma|_{\overline{\mathbb{Q}}}$ is injective. (The image is called the decomposition subgroup.)*

Remark: $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is a pro-solvable group, while $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is very poorly understood.

6. Lattice methods

6.1. Lattices in $\mathbb{R}^n$.

We move on to lattice methods in studying number fields (finite extensions of $\mathbb{Q}$).

6.1.1. Definition. Let V be a n-dimensinoal $\mathbb{R}$-vector space. A *lattice* in V is a subgroup

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_m$$

for some linearly independent $e_1, \ldots, e_m$. It is *full* if $m = n$.

6.1.2. Proposition. *Let $\Lambda \subset V$ be a subgroup, then Λ is discrete iff Λ is a lattice.*

Equip V with the dot product in $\mathbb{R}^n$ so that we pin down the unit length. Then we get a unique Haar measure on V, such that V together with the measure is isomorphic to $\mathbb{R}^n$.

6.1.3. Definition. For a set X and a σ-algebra Σ on X, a map $\mu : \Sigma \to \mathbb{R} \cup \{\pm\infty\}$ is a *measure* if:

- $\mu(\varnothing) = 0$;
- $\mu(E) \geq 0$ for all $E \in \Sigma$;
- For a countable family of pairwise disjoint sets $E_i \in \Sigma$, $\mu(\bigcup_i E_i) = \sum_i \mu(E_i)$.

6.1.4. Theorem (Haar's theorem)**.** *Let G be a locally compact Hausdorff topological group. A* Borel set *is an element in the* Borel algebra*, i.e. the σ-algebra generated by open sets of G. There is a unique (up to scaling) nontrivial measure μ on the Borel algebra such that:*

- *$\mu(gS) = \mu(S)$ (left translation-invariant);*
- *$\mu(K) < \infty$ for K compact;*
- *$\mu(S) = \inf\{\mu(U) : S \subseteq U, U$ open$\}$;*
- *$\mu(U) = \sup\{\mu(K) : K \subseteq U, K$ compact$\}$ for U open.*

For a full lattice $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$, let

$$F = \{a_1e_1 + \cdots + a_ne_n : 0 \leq a_i < 1\}.$$

Then $\mathbb{R}^n = \coprod_{\lambda\in\Lambda}(F + \lambda)$. Also, $\mathrm{vol}(F) = |\det(e_1, \ldots, e_n)| = \sqrt{\det(\langle e_i, e_j\rangle)_{i,j}}$.

More generally:

6.1.5. Definition. A *fundamental domain* for $\Lambda \subset V$ is a measurable $F \subset V$ such that $V = \coprod_{\lambda\in\Lambda}(F + \lambda)$.

6.1.6. Proposition. *If F, G are two fundamental domains then they have the same volume.*

Proof. For each $\lambda \in \Lambda$, $(F + \lambda) \cap G$ is a translate of $F \cap (G - \lambda)$, so they have the same volume. Taking the sum over $\lambda \in \Lambda$, we get $\mathrm{vol}(G) = \mathrm{vol}(F)$. □

6.1.7. Definition. The *covolume* $\mathrm{covol}(\Lambda)$ of a full lattice Λ is defined to be the volume of any fundamental domain of Λ.

6.1.8. Proposition. *Suppose $\Lambda \supseteq \Lambda'$ are full lattices, then*

$$\operatorname{covol}(\Lambda') = (\Lambda : \Lambda') \operatorname{covol}(\Lambda).$$

6.2. Minkowski's lattice point theorem.

6.2.1. Lemma. *Let $S \subset \mathbb{R}^n$, $\operatorname{vol}(S) > 1$. Then there exist distinct $s, s' \in S$, such that $s - s' \in \mathbb{Z}^n$.*

Proof. Cut up $\mathbb{R}^n$ into unit cubes, and translate pieces of S into $[0,1)^n$. They must overlap. □

6.2.2. Theorem (Minkowski's lattice point theorem for $\mathbb{Z}^n$)**.** *Let $S \subset \mathbb{R}^n$ be a symmetric convex region such that $\operatorname{vol}(S) > 2^n$. Then S contains a nonzero lattice point.*

Proof. The dilation $\frac{1}{2}S$ must contain two distinct points $\frac{1}{2}s, \frac{1}{2}s'$ where $\frac{1}{2}(s - s') \in \mathbb{Z}^n$, which is the point we want. □

6.2.3. Theorem (Minkowski's lattice point theorem, full version)**.** *Let V be a finite dimensional $\mathbb{R}$-vector space, Λ a full lattice, $S \subset V$ a symmetric convex region with $\operatorname{vol}(S) > 2^n \operatorname{covol}(\Lambda)$, then it contains a nonzero lattice point.*

As an application, we prove the following classical result:

6.2.4. Theorem. *If $p \equiv 1 \pmod 4$ is a prime, then $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$.*

Proof. Because $(\frac{-1}{p}) = 1$, there exists $i \in \mathbb{F}_p$ with $i^2 + 1 \equiv 0 \pmod p$. Let $\Lambda \subset \mathbb{Z}^2$ be the lattice consisting of points $\lambda \pmod p$ that is a multiple of $(1, i) \bmod p$. Clearly, Λ has index p in $\mathbb{Z}^2$, so $\operatorname{covol}(\Lambda) = p$. Let $S = \{x \in \mathbb{R}^2 : |x| < \sqrt{2p}\}$. Then $|S| = 2p\pi > 4p = 2^2 \operatorname{covol}(\Lambda)$, so S contains a lattice point in Λ, which is necessarily a solution to $x^2 + y^2 = p$. □

7. Global fields

7.1. Global fields.

7.1.1. Definition. A *global field* is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$.

7.2. Places. We transition to a discussion of places, which are like primes but generalizes to the archimedean case as well.

7.2.1. Theorem. *The category of global function fields with field inclusions is equivalent to the category of smooth projective curves with dominant rational maps, via $X \mapsto K(X)$.*

Let K be a number field.

7.2.2. Definition. A *place* of K is an equivalence class of nontrivial absolute values on K. The set of all places is commonly denoted by M_K.

By Ostrowski's theorem, $M_{\mathbb{Q}}$ corresponds set-theoretically with $\operatorname{Spec}\mathbb{Z}$. Every place $v \in M_K$ is an extension of $|\,|_p$ for some $p \leq \infty$ (we write $v \mid p$ for this). We already know that places $v \mid p$ for finite p correspond bijectively to primes $\mathfrak{q} \mid (p)$.

7.2.3. Proposition. *v is archimedean if $v \mid \infty$, and nonarchimedean otherwise.*

Proof. Complete wrt v to get an extension $K_v/\mathbb{Q}_p$, and use theorem 15.1.4. □

7.2.4. Lemma. *Suppose $K = \mathbb{Q}(\alpha)$. If $v \mid p$ for $p \leq \infty$, then $K_v = \mathbb{Q}_p(\alpha)$.*

Proof. Consider $\mathbb{Q}_p(\alpha)$, which must be contained in K_v. The absolute value on $\mathbb{Q}_p$ then extends uniquely to an absolute value on $\mathbb{Q}_p(\alpha)$, under which $\mathbb{Q}_p(\alpha)$ is complete. Since this absolute value concides with that of K_v and $K \subset \mathbb{Q}_p(\alpha)$, we have $K_v = \mathbb{Q}_p(\alpha)$. □

The minimal polynomial of α in K_v is then an irreducible factor of the min. poly of α in K. Conversely, any irreducible factor gives a finite extension $F/\mathbb{Q}_p$, which is equipped with a complete absolute value, and there is a unique extension $K \hookrightarrow F$, which is the completion of K wrt that absolute value. Therefore we have

7.2.5. Theorem. *$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{v \mid p} K_v$, for $p \leq \infty$.*

7.2.6. Example. If $v \mid \infty$, then K_v is a finite extension of $\mathbb{R}$, so either $\mathbb{R}$ or $\mathbb{C}$. Suppose $K = \mathbb{Q}[x]/f(x)$, then $f(x)$ in $\mathbb{R}[x]$ factors as the product of r_1 linear factors and r_2 quadratic factors. The linear factors $(x-a)$ correspond to embeddings $K \hookrightarrow \mathbb{R}$ mapping $x \mapsto a$ (these are the "real places"), and the quadratic factors $(x-z)(x-\overline{z})$ correspond to pairs of embeddings $K \hookrightarrow \mathbb{C}$ mapping $x \mapsto z$ or $\overline{z}$ (these are the "complex places"). Then $r_1 + 2r_2 = [K : \mathbb{Q}]$ by counting degrees.

7.2.7. Corollary. *The places $v \mid p$ correspond bijectively to* $\operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}_p})/\operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

7.2.8. Definition. If $v \mid p$, the *normalized absolute value* on K_v is $|x|_v = |\operatorname{N}_{K_v/\mathbb{Q}_p}(x)|_p$.

7.2.9. Proposition. *Suppose p is finite, $v \mid p$, and let $\mathcal{O}_v$ be the DVR in K_v. If $x \in \mathcal{O}_v$, then*

$$|x|_v := (\#\mathcal{O}_v/x\mathcal{O}_v)^{-1}.$$

Proof. We have $(\operatorname{N}_{K_v/\mathbb{Q}_p}(x)) = N(x\mathcal{O}_v) = (\mathcal{O}_v : x\mathcal{O}_v)_{\mathbb{Z}_p} = \chi(\mathcal{O}_v/x\mathcal{O}_v) = (\#\mathcal{O}_v/x\mathcal{O}_v)$. Taking $|\,|_p$ on both sides gives us the formula. □

7.2.10. Example. If v is complex, then $|x|_v = |x|^2$, which is actually not an absolute value! In general, $|x|_v = |x|_p^{[K_v:\mathbb{Q}_p]}$ for $x \in \mathbb{Q}$. This normalization is "intrinsic", because given $x \in \mathcal{O}_K$, multiplication by x scales the Haar measure on K_v by a factor of $|x|_v$.

7.2.11. Theorem (Product formula). *If $x \in K^\times$, then $\prod_{v \in M_K} |x|_v$ makes sense and is equal to 1.*

Proof. $\operatorname{N}_{K/\mathbb{Q}}(x) = \operatorname{N}_{K \otimes_{\mathbb{Q}} \mathbb{Q}_p/\mathbb{Q}_p}(x) = \prod_{v|p} \operatorname{N}_{K_v/\mathbb{Q}_p}(x)$, so taking $|\,|_p$ on both sides gives us

$$|\operatorname{N}_{K/\mathbb{Q}}(x)|_p = \prod_{v|p} |x|_v.$$

Taking the product over all p an using the product formula for $\mathbb{Q}$, we get the desired formula. □

7.3. Orders. We are on our way to apply Minkowski's lattice point formula to say something nontrivial about the ideal class group.

7.3.1. Definition. An *order* in a number field K is a subring $\mathcal{O}$ of finite index in $\mathcal{O}_K$.

Equivalently, $\mathcal{O}$ is a $\mathbb{Z}$-lattice in K that is also a ring.

For an order $\mathcal{O}$, we have the following inclusions:

$$\mathcal{O} \hookrightarrow K \hookrightarrow K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow K_{\mathbb{C}} := K_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}.$$

Thus, $\mathcal{O}$ is a lattice in the $\mathbb{R}$-vector space $K_{\mathbb{R}}$. The canonical Hermitian inner product on $\mathbb{C}^n$ restricts to an inner product on $K_{\mathbb{R}} \cong \mathbb{R}^n$ (note that this inner product is not equal to the canonical one on $\mathbb{R}^n$: for example, $(x, y) = x + yi \in \mathbb{C}$ is embedded as $(x+yi, x-yi) \in \mathbb{C}^2$, so $(x+yi, x-yi)\cdot(z+wi, z-wi) = 2(xy+zw) = 2(x,y)\cdot(z,w)$. Consequently, the volume under this inner product is scaled by a factor of 2^{r_2}). For $x, y \in K$, we then get an inner product

$$\langle x, y\rangle = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \sigma x \cdot \overline{\sigma y}.$$

7.3.2. Proposition. $\operatorname{covol}(\mathcal{O}) = \sqrt{|\operatorname{disc}\mathcal{O}|}$.

Proof. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Let $A = (\sigma(e_j))_{\sigma,j} \in M_{n\times n}(\mathbb{C})$. Then $|\operatorname{disc}\mathcal{O}| = (\det A)^2$. But $\operatorname{covol}(\mathcal{O})^2 = \det\langle e_i, e_j\rangle = \det(\sum_\sigma \sigma e_i \cdot \sigma e_j) = |\det A|^2$. So $\operatorname{covol}(\mathcal{O}) = \sqrt{|\operatorname{disc}\mathcal{O}|}$. □

7.3.3. Corollary. *Suppose I is an invertible fractional $\mathcal{O}$-ideal, then* $\operatorname{covol}(I) = \sqrt{\operatorname{disc}\mathcal{O}} \cdot N(I)$.

7.4. Finiteness of the class group, and other applications. Now we are ready to apply Minkowski's lattice point theorem to show that every fractional ideal contains a relatively short vector. Use (r, s) to denote (r_1, r_2).

7.4.1. Theorem. *Let K be a number field, $\mathcal{O}$ an order. Let $m = \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|\operatorname{disc}\mathcal{O}|}$, then for any invertible fractional $\mathcal{O}$-ideal I, there exists a nonzero $a \in I$, such that $|N(a)| \leq m \cdot |N(I)|$.*

Proof. Let $S = \{z = (z_\sigma)_{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \in K_{\mathbb{R}} : \sum |z_\sigma| < t\}$, where t is a constant we fix later. Then it is not hard to show that $\mathrm{vol}(S) = 2^r \pi^s \frac{t^n}{n!}$. Choose t such that $\mathrm{vol}(S) > 2^n \operatorname{covol}(I)$. By Minkowski's lattice point theorem, there exists nonzero $a \in I$ lying in S, such that $t > \sum_\sigma |\sigma a| \geq n \sqrt[n]{\prod_\sigma |\sigma a|} = n \sqrt[n]{|\mathrm{N}_{K,\mathbb{Q}}(a)|}$. We know that t can be chosen to be arbitrarily close to $\sqrt[n]{(\frac{4}{\pi})^s n! \sqrt{\operatorname{disc} \mathcal{O}} \cdot |N(I)|}$ from above, so we see that

$$|N(a)| = |\mathrm{N}_{K,\mathbb{Q}}(a)| \leq \frac{n!}{n^n} \operatorname{pr} \frac{4}{\pi}^s \sqrt{|\operatorname{disc} \mathcal{O}|} \cdot |N(I)| = m \cdot |N(I)|,$$

as desired. □

7.4.2. Corollary. *Every ideal class contains an integral ideal of norm at most m.*

Proof. Let $[I]$ be the inverse of the target ideal class, then there exists $a \in I$, such that $|N(a)| \leq m \cdot |N(I)|$. This means that $(a)I^{-1}$ is an integral ideal in the target ideal class, whose norm is at most m. □

7.4.3. Lemma. *There are finitely many ideals of norm at most m.*

Proof. It suffices to show that $\mathbb{Z}^n$ has finitely many subgroups of a given index. This is because any subgroup of index q contains $(q\mathbb{Z})^n$, so there can only be finitely many. □

7.4.4. Theorem. *The class group of a number field is finite.*

7.4.5. Proposition. $\sqrt{\operatorname{disc} \mathcal{O}_K} \geq \frac{n^n}{n!}(\frac{\pi}{4})^s \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$.

Proof. Take I to be the unit ideal, so that its norm is 1. Because the norm of any nonzero element is at least 1, $m \geq 1$. □

7.4.6. Corollary. *If $K \neq \mathbb{Q}$, then $|\operatorname{disc} \mathcal{O}_K| > 1$. In other words, there are no everywhere unramified nontrivial extensions of $\mathbb{Q}$.*

7.4.7. Proposition. *There are finitely many number fields K with $|\operatorname{disc} \mathcal{O}_K| < B$, for any real B.*

Proof. By proposition 7.4.5, it suffices to show that there are finitely many such number fields of any fixed degree n.

Case 1: K is totally real. Let $S := \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_1| \leq 2B^{1/2}, |x_i| < 1 \text{ for all } i \neq 1\}$. Then $\mathrm{vol}(S) \approx 2^{n+1} B^{1/2} > 2^n |\operatorname{disc} \mathcal{O}_K|^{1/2} = 2^n \operatorname{covol}(\mathcal{O}_K)$. By Minkowski, there exists a nonzero $\alpha \in \mathcal{O}_K \subset \mathbb{R}^n$ in S. Then $\prod |\alpha_i| = |N(\alpha)| \geq 1$ while $|\alpha_2|, \dots, |\alpha_n| < 1$, which forces $|\alpha_1| > 1$. If $\mathbb{Q}(\alpha) \neq K$, then each α_i will be repeated $[K : \mathbb{Q}(\alpha)]$ times (by the norm formula), which is not the case because α_1 is the only one with absolute value larger than 1. The minimal polynomial of α, which is in $\mathbb{Z}[x]$, has finitely many possibilities, since its coefficients, as symmetric functions in its roots which have bounded sizes, have bounded sizes. So there are only finitely many possibilities for K also.

Case 2: The signature of K is (r, s), then $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$. Let $S := \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |z_1|^2 \leq cB^{1/2}, |x_i|, |z_j| < 1 \text{ for all } i \text{ and for all } j \neq 1\}$, where c is large enough that $\mathrm{vol}(S) > 2^n \operatorname{covol}(\mathcal{O}_K)$. The argument in Case 1 continues verbatim. □

7.4.8. Lemma. *Let K be a number field of degree n, then for any prime p, $v_p(D_K) \leq n \lfloor \log_p n \rfloor + n - 1$.*

Proof. We have $v_p(D_K) = v_p(N(\mathcal{D}_K)) = \sum_{\mathfrak{q}|p} f_{\mathfrak{q}} v_{\mathfrak{q}}(\mathcal{D}_K) \leq \sum_{\mathfrak{q}|p} f_{\mathfrak{q}}(e_{\mathfrak{q}} - 1 + v_p(e_{\mathfrak{q}})) \leq n - 1 + n \lfloor \log_p n \rfloor$ by trivial bounding. □

7.4.9. Theorem (Hermite). *Let S be a finite set of places of $\mathbb{Q}$, and let n be an integer. Then there are finitely many number fields K of degree n that are unramified outside S.*

Proof. Each valuation $v_p(D_K)$ is bounded, so D_K is bounded, so there are finitely many K's. □

7.5. Adèle ring. Let K be a global field, v a place, $\mathcal{O}_v$ the valuation ring of K_v (defined to be equal to K_v when v is archimedean). The normalized absolute value induces a topology on K_v, under which it is locally compact. Furthermore, if v is nonarchimedean, $\mathcal{O}_v$ is compact.

We now define the *adèle ring* of K, which will be a topological ring:

7.5.1. Definition. The adèle ring $\mathbb{A}_K$ of a global field K is the *restricted product*

$$\prod\nolimits'_v (K_v, \mathcal{O}_v),$$

which as a set is equal to

$$\{(a_v) \in \prod K_v : \text{all but finitely many } a_v \in \mathcal{O}_v\}.$$

It is easy to verify that this forms a ring. The topology on this is *finer than* the subset topology of the product topology; instead, a base is given by open sets of the form $\prod_v U_v$, where $U_v \subseteq K_v$ are open and all but finitely many $U_v = \mathcal{O}_v$. (In particular, $\prod_v \mathcal{O}_v$ is a locally compact open.)

7.5.2. Proposition. *$\mathbb{A} = \mathbb{A}_K$ is locally compact.*

PROOF. $\prod_v \mathcal{O}_v$ is a locally compact neighborhood of 0. □

Because any element of K has only finitely many absolute values where it is 1, K embeds into $\mathbb{A}_K$ naturally.

7.5.3. Proposition. *If L/K is a finite separable extension of global fields, $\mathbb{A}_L \cong L \otimes_K \mathbb{A}_K$ as topological rings.*

In fact, $K \hookrightarrow \mathbb{A}$ is very much like the embedding $\mathbb{Z} \hookrightarrow \mathbb{R}$:

7.5.4. Theorem. *K is a discrete subgroup of $\mathbb{A}$, and $\mathbb{A}/K$ is compact.*

PROOF. We only prove this for $K = \mathbb{Q}$, and the number field case then follows from proposition 7.5.3. The function field case follows from a similar argument, so we focus on $\mathbb{Q}$ form here.

Discreteness of $\mathbb{Q}$: $U = (-1, 1) \times \prod_p \mathbb{Z}_p$ is an open neighborhood of 0 that contains no points of $\mathbb{Q}$.

Compactness of $\mathbb{A}/\mathbb{Q}$: we claim that $\mathbb{A} = \mathbb{Q} + [0, 1] \times \prod_p \mathbb{Z}_p$. Given $x = (x_p)_{p \le \infty}$, expand x_p in powers of p, and let y_p be the decimal part of x_p (i.e. $x_p - y_p \in \mathbb{Z}_p$ and the denominator of y_p is a power of p). Almost all y_p are zero, so it makes sense to talk about $x - \sum_p y_p$, which belongs to every $\mathbb{Z}_p$. Now adjust by an integer to get in $[0, 1]$. □

7.6. Idèle group.

7.6.1. Definition. The *idèle group* is $\mathbb{A}^\times = \prod'_v (K_v^\times, \mathcal{O}_v^\times)$, with the restricted product topology.

Remark: This is finer than the topology inherited as a subspace of $\mathbb{A}$! For example, $\prod \mathcal{O}_v^\times$ is open in $\mathbb{A}^\times$ but not in $\mathbb{A}$. But the topology is induced from $\mathbb{A}$ via the map $\mathbb{A}^\times \hookrightarrow \mathbb{A} \times \mathbb{A}$, $x \mapsto (x, x^{-1})$.

7.6.2. Proposition. *$K^\times$ is discrete in $\mathbb{A}^\times$.*

PROOF. $K^\times = \mathbb{A}^\times \cap (K \times K)$ inside $\mathbb{A} \times \mathbb{A}$, so it is discrete. □

7.6.3. Definition. For an idèle $a = (a_v)_v \in \mathbb{A}^\times$, define $|a| = \prod_v |a_v|_v$.

This is also the correct notion of "size" in terms of scaling the Haar measure.

7.6.4. Definition. The group $\mathbb{A}_1^\times = \ker(\mathbb{A}^\times \xrightarrow{||} \mathbb{R}_{>0}^\times)$.

7.6.5. Proposition. *$K^\times$ embeds into $\mathbb{A}_1^\times$.*

Let K be a number field for now. We also have a natural map $\mathbb{A}^\times \to \mathcal{I}$ assembled from each $K_\mathfrak{p}^\times \xrightarrow{v_p} \mathbb{Z}$. This is surjective (in contrast to the case where $\mathbb{A}^\times$ is replaced with the group of principal fractional ideals, when there is a problem with the class group). Also, it is clear that $\ker(\mathbb{A}^\times \to \mathcal{I}) = \prod_v \mathcal{O}_v^\times$.

The ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ can be recast in adelic language:

$$\mathrm{Cl}(\mathcal{O}_K) = \mathcal{I}/K^\times = \frac{\mathbb{A}^\times}{K^\times \cdot \prod \mathcal{O}_v^\times}.$$

7.6.6. Definition. The *idèle class group* is $\mathbb{A}^\times / K^\times$.

7.6.7. Theorem. *$\mathbb{A}_1^\times / K^\times$ is compact.*

This is a hard theorem and directly implies finiteness of the class group.

7.6.8. Definition. For $d = (d_v)_v \in \mathbb{A}^\times$, define the adelic parallelotope (box)

$$\mathbb{L}(d) := \{(x_v) \in \mathbb{A} : |x_v|_v \leq |d_v|_v \text{ for all } v\},$$

and

$$L(d) = \mathbb{L}(d) \cap K$$

is the set of lattice points in the box.

Clearly $\mathbb{L}(d)$ is a compact neighborhood of 0. In the function field case, $L(d)$ is like "functions with prescribed orders of poles and zeroes", cf. Riemann-Roch. Since K is discrete in $\mathbb{A}$, $L(d)$ is discrete and compact, hence finite.

7.6.9. Theorem (Adelic Minkowski)**.** *There exists a constant c (depending on K), such that if $|d| > c$, then $L(d)$ contains a nonzero element.*

Proof. We only prove this for number fields. Then d maps to some ideal I. For $x \in K$, unwrapping the condition $|x|_v \leq |d_v|_v$ for archimedean and nonarchimedean v, we need $x \in I$ (which is a lattice in $K_\mathbb{R}$) and x belongs to a product of intervals and disks, a symmetric convex set in $K_\mathbb{R}$. When $|d|$ is big enough, Minkowski's theorem applies and we get a nonzero point in $L(d)$. □

7.7. Strong approximation. Let K be a global field. For any finite set of places S containing all archimedean places, the *S-integral adèles* are elements of the ring

$$\mathbb{A}_S := \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v.$$

This is equipped with the actual product topology. For $S \subseteq T$, there is a natrual $\mathbb{A}_S \hookrightarrow \mathbb{A}_T$. Then

$$\mathbb{A} = \varinjlim_{S} \mathbb{A}_S.$$

Here is a corollary of the adelic Minkowski theorem, about scaling a box by elements of $K^\times$ to fit in another box.

7.7.1. Corollary. *If $a, b \in \mathbb{A}^\times$ such that $|b| > c|a|$ (where) c is as in theorem 7.6.9. Then there exists $u \in K^\times$, such that $u\mathbb{L}(a) \subseteq \mathbb{L}(b)$.*

Proof. By adelic Minkowski, there exists $u \in K^\times$ such that $u \in \mathbb{L}(b/a)$. This is the same as $u\mathbb{L}(a) \subseteq \mathbb{L}(b)$. □

7.7.2. Lemma. *There exists $a \in \mathbb{A}^\times$, such that $\mathbb{A} = K + \mathbb{L}(a)$.*

Proof. Just for this problem, let $\mathbb{L}(d)'$ be the same as $\mathbb{L}(d)$, except it is open for archimedean v. These are open neighborhoods of 0 that cover $\mathbb{A}$, so their images in $\mathbb{A}/K$ cover $\mathbb{A}/K$. The image is open because its preimage is the union of all translations of $\mathbb{L}(d)'$ by elements of K. Since $\mathbb{A}/K$ is compact, we need only finitely many $\mathbb{L}(d)'$s whose images cover $\mathbb{A}/K$. So we can choose a big enough such that $\mathbb{L}(a)$ contains each of the finitely many $\mathbb{L}(d)'$s. □

7.7.3. Lemma. *If $b \in \mathbb{A}^\times$, $|b|$ sufficiently large, then $\mathbb{A} = K + \mathbb{L}(b)$.*

Proof. Combine the previous two claims. □

7.7.4. Theorem (Strong approximation)**.** *Let K be a global field, and suppose that the set of places of K are partitioned into $S \sqcup T \sqcup \{w\}$, where S is finite. For each $v \in S$, fix $a_v \in K_v$ and a real $\varepsilon_v > 0$. Then there exists $x \in K$ such that:*

- *$|x - a_v|_v \leq \varepsilon_v$ for all $v \in S$;*
- *$|x|_v \leq 1$ for all $v \in T$.*

Note that $|x|_w$ may behave wildly.

Proof. Define $a_v = 0$ for all $v \notin S$ to make an adèle $a = (a_v)_v$. For $v \in S$: we may shrink ε_v so that $\varepsilon_v = |b_v|_v$ for some $b_v \in K_v$. For $v \in T$: let $b_v = 1$. Let $b_w \in K_w$ be large enough that $|b| = \prod_v |b_v|_v$ is large enough, as in the previous lemma. Then there exists $x \in K$, $x - a \in \mathbb{L}(b)$, which is what we wanted. □

7.8. Compactness of $\mathbb{A}_1^\times/K^\times$.

7.8.1. Lemma. *$\mathbb{A}_1^\times$ is a closed subset of $\mathbb{A}$ and of $\mathbb{A}^\times$, and the two subspace topologies coincide.*

Proof. First of all, we remark that $\mathbb{A}_1^\times$ is closed because it is cut out by an equation. So it suffices to show that the two subspace topologies coincide.

We claim that for any idèle $a = (a_v)_v$, $\mathbb{A}_1^\times \cap \mathbb{L}(a) \subseteq \mathbb{A}_S^\times$ for some finite S. To show this claim, let S contain the places v such that $|a_v|_v \neq 1$ and the nonarchimedean places whose residue field has size at most $|a|$, as well as the archimedean ones. If $(x_v)_v \in \mathbb{A}_1^\times \cap \mathbb{L}(a)$, then at all $w \notin S$, $|x_w|_w \leq |a_w|_w = 1$, so $x_w \in \mathcal{O}_w$. If $|x_w|_w < 1$, then $|x_w|_w \leq \frac{1}{q}$ where q is the size of the residue field at w. Then $|x| \leq |a|/q < 1$, which is a contradiction to $x \in \mathbb{A}_1^\times$. So $x \in \mathbb{A}_S^\times$ and the lemma is proved.

Now, because the topology of $\mathbb{A}_S^\times$ is just the product topology, it is the same in both $\mathbb{A}$ and $\mathbb{A}^\times$. Because $\mathbb{A}_1^\times$ is covered by $\mathbb{A}_1^\times \cap \mathbb{L}(a)$'s, we are done. □

7.8.2. Theorem. *$\mathbb{A}_1^\times/K^\times$ is compact.*

Proof. Choose $d \in \mathbb{A}^\times$ large enough for the adelic Minkowski. By the above lemma, $\mathbb{A}_1^\times \cap \mathbb{L}(d)$ is closed inside $\mathbb{L}(d)$, which is compact. So $\mathbb{A}_1^\times \cap \mathbb{L}(d)$ is compact.

It remains to show that $\mathbb{A}_1^\times \cap \mathbb{L}(d)$ surjects onto $\mathbb{A}_1^\times/K^\times$. Given any $u \in \mathbb{A}_1^\times$, we have $|d/u| = |d|$, so there exists a nonzero element $x \in K^\times$ in $\mathbb{L}(d/u)$ by adelic Minkowski. This is equivalent to $ux \in \mathbb{L}(d)$, but $ux \in \mathbb{A}_1^\times$ also. So the above map is indeed a surjection, which tells us that $\mathbb{A}_1^\times/K^\times$ is compact. □

7.9. Finiteness of the class group, second proof.

We will use the compactness of $\mathbb{A}_1^\times/K^\times$ to show:

7.9.1. Theorem (finiteness of class group)**.** *We have:*

1. *If K is a number field, then $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*
2. *If K is a global function field, and X is the associated smooth projective curve, then $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\operatorname{im}(K^\times)$ is finite.*

Proof. (1) Consider the natural surjective map $\mathbb{A}^\times \twoheadrightarrow \mathcal{I}$. The induced $\mathbb{A}_1^\times \to \mathcal{I}$ is still surjective because we can always normalize at archimedean places. So we get a surjection $\mathbb{A}_1^\times/K^\times \twoheadrightarrow \mathcal{I}/\operatorname{im}(K^\times) = \mathrm{Cl}(\mathcal{O}_K)$. The kernel of this map is open, so the LHS quotient the kernel is compact and discrete, hence finite.

(2) Consider the natural surjective map $\mathbb{A}^\times \twoheadrightarrow \mathrm{Div}(X)$, which induces $\mathbb{A}_1^\times \twoheadrightarrow \mathrm{Div}^0(X)$. So we get a surjection $\mathbb{A}_1^\times/K^\times \twoheadrightarrow \mathrm{Pic}^0(X)$, and we can argue as in (1). □

7.10. Dirichlet's unit theorem.

7.10.1. Definition. Let S be a set of places containing all archimedean ones. Let

$$\mathcal{O}_S = \{x \in K : |x_v|_v \leq 1 \text{ for all } v \notin S\}.$$

Then $\mathcal{O}_S = \mathbb{A}_S \cap K$, and $\mathcal{O}_S^\times = \mathbb{A}_S^\times \cap K^\times$. Let $\mu = (\mathcal{O}_S^\times)_{\text{tors}} = (K^\times)_{\text{tors}}$ be the group of roots of unities.

Define a continuous homomorphism

$$\begin{aligned} \mathrm{Log} : \mathbb{A}_S^\times &\to \mathbb{R}^S \\ (a_v) &\mapsto (\log|a_v|_v)_{v \in S}. \end{aligned}$$

7.10.2. Lemma. *Let S be the set of archimedean places. Then the induced map $\mathrm{Log} : \mathbb{A}_{S,1}^\times \to \mathbb{R}_0^S$ is surjective.* □

7.10.3. Lemma. *The induced $\mathrm{Log} : \mathcal{O}_S^\times \to \mathbb{R}^S$ has finite kernel and discrete image.*

Proof. Let B be a compact neighborhood of 0. Then $\mathrm{Log}^{-1}(B)$ is contained in some $\mathbb{L}(d)$, so $\mathrm{Log}^{-1}(B) \cap K^\times$ is finite. In particular, Log has finite kernel, and 0 is an isolated point in the image, i.e. the image is discrete. □

7.10.4. Corollary. *$\ker(\mathrm{Log} : \mathcal{O}_S^\times \to \mathbb{R}^S) = \mu$, and $\mathrm{Log}(\mathcal{O}_S^\times)$ is a free abelian group of finite rank.*

Proof. Clearly, μ is in the kernel. Because the kernel is finite, it must be torsion. □

7.10.5. Theorem (Dirichlet's S-unit theorem)**.** *Let K be a number field, then $\mathcal{O}_S^\times$ is finitely genrated with rank $|S| - 1 = r_1 + r_2 - 1$.*

Proof. We only prove this in the case where S is the set of archimedean places. By the previous corollary, $\mathcal{O}_S^\times$ is finitely generated (μ is contained in some adelic parallelotope intersect $K^\times$, hence finite).

Consider the open and closed inclusion $\mathbb{A}_{S,q}^\times \hookrightarrow \mathbb{A}_1^\times$, which induces a map $\mathbb{A}_{S,1}^\times/\mathcal{O}_S^\times \to \mathbb{A}_1^\times/K^\times$. This is open and closed, and the RHS is compact, so the LHS is compact also. Under the log map, $\mathbb{A}_S^\times/\mathcal{O}_S^\times \to \mathbb{R}_0^S/\log(\mathcal{O}_S^\times)$ is surjective, so the RHS is compact as well. This means that the lattice is a full lattice, i.e. is of full rank $|S| - 1$. □

8. Cyclotomic fields

8.1. Cyclotomic fields. We transition to the next topic, cyclotomic fields. Let n be a natural number, K be a field whose characteristic does not divide n, and let L be the splitting field of the separable polynomial $x^n - 1$ in K, i.e. $L = K(\zeta_n)$. We get an injection $\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, which is not always surjective. However, this is surjective when $K = \mathbb{Q}$. This amounts to showing that $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$. Consider the discriminant $\mathrm{disc}(x^n - 1) = \pm n^n$. Let $f(x)$ be a factor of $x^n - 1$, and ζ a root of f. Let p be a prime coprime to n. Suppose ζ^p is not a root of f, then $f(\zeta^p) \neq 0$ is a product of differences of roots of unity, hence an algebraic integer dividing n^n. But $f(\zeta^p) \equiv f(\zeta)^p = 0 \bmod p$, so $p \mid f(\zeta^p)$, so $p \mid n^n$, a contradiction. So ζ^p is a root of f. By induction, ζ^m is a root of f for any m coprime to n, as desired.

Another way to write the proof is as follows:

8.1.1. Proposition. *If a prime p is coprime to n, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is unramified above p, and* Frob_p *acts by $\zeta_n \mapsto \zeta_n^p$.*

So all primes coprime to n lie in the image of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$, so it must be surjective.

8.1.2. Corollary. *If $p \nmid n$, then $f_p = [\mathbb{F}_\mathfrak{q} : \mathbb{F}_p]$ is equal to the order of* Frob_p *in G, which is equal to the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.*

8.1.3. Proposition. *The ring of integers in $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.*

Proof. Induct on the number of primes dividing n. Suppose $n = mp^r$, $p \nmid m$. We have a tower of extensions $K = \mathbb{Q}(\zeta_m)/\mathbb{Q}$, and $K(\zeta_{p^r})/K$. By induction we know that $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

We claim that $\mathcal{O}_K[\zeta_{p^r}]$ is integrally closed. This can be checked after localizing at each prime $\mathfrak{p}$ in K, i.e. $(\mathcal{O}_K)_\mathfrak{p}[\zeta_{p^r}]$ is integrally closed. Consider

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}.$$

If $\mathfrak{p}$ lies above p, then $\Phi_{p^r}(x+1)$ is Eisenstein at $\mathfrak{p}$ (this uses that $p \nmid m$, which implies $\mathfrak{p}$ is unramified), so $(\mathcal{O}_K)_\mathfrak{p}[\zeta_{p^r}]$ is a DVR (see §2.6). But there can be no nontrivial rings between a DVR and its field of fractions, so $(\mathcal{O}_K)_\mathfrak{p}[\zeta_{p^r}]$ is integrally closed.

If $\mathfrak{p} \mid \ell \neq p$, then $x^{p^r} - 1$ is separable mod ℓ, and so is $\Phi_{p^r}(x)$ mod $\mathfrak{p}$. So $(\mathcal{O}_k)_\mathfrak{p}[\zeta_{p^r}]$ is a DVR (?), and therefore integrally closed. □

9. Analytic number theory

9.1. Zeta functions. We transition to yet another topic: analytic number theory. A good reference is Davenport's *Multiplicative Number Theory.*

9.1.1. Definition (Riemann zeta function)**.** For $\mathrm{Re}(s) > 1$,

$$\zeta(s) := \prod_p \frac{1}{1 - p^{-s}} = \sum_{n \geq 1} n^{-s}.$$

9.1.2. Definition (Dedekind zeta function)**.** Let K be a number field,

$$\zeta_K(s) := \prod_{\text{nonzero } \mathfrak{p}} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}} = \prod_{\text{nonzero } \mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-s}.$$

where $\mathrm{N}(\mathfrak{p})$ is the absolute norm, i.e. $\mathrm{N}(\mathfrak{p}) = p^{[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]} = |\mathcal{O}_K/\mathfrak{p}|$.

9.1.3. Proposition. *There are infinitely many primes. Even better, $\sum \frac{1}{p}$ diverges.*

PROOF. Clearly, $\lim_{s\to 1^+}\zeta(s)=\infty$, so $\log\zeta(s)=\sum_p -\log(1-p^{-s})$ also tends to ∞. Expanding as a Taylor series, the main part is $\sum\frac{1}{p^s}$ and the rest is obviously bounded. □

9.1.4. Proposition. $\zeta(s)=\frac{1}{s-1}+\phi(s)$*, where* $\phi(s)$ *extends to a holomorphic function on* $\mathrm{Re}(s)>0$*.*

PROOF. For $\mathrm{Re}(s)>1$,

$$\begin{aligned}\zeta(s)&=\sum_{n\geq 1}n^{-s}\\&=\sum_{n\geq 1}n(n^{-s}-(n+1)^{-s})\\&=\sum_{n\geq 1}\mathrm{pr}\, n\int_n^{n+1} sx^{-s-1}dx\\&=s\int_1^\infty \lfloor x\rfloor\, x^{-s-1}dx\\&=\frac{1}{s-1}+\mathrm{pr}\,1-s\int_1^\infty \{x\}x^{-s-1}dx,\end{aligned}$$

where the latter term (which we call $\phi(s)$) converges absolutely for $\mathrm{Re}(s)>0$, and uniformly so on $\mathrm{Re}(s)\geq\varepsilon$ for any $\varepsilon>0$. □

9.1.5. Proposition. *The following are true about* $\zeta(s)$*:*

1. *memoromorphic on* $\mathbb{C}$*; has a simple pole at 1, and no other poles*
2. *functional equation*
3. *trivial zeros at negative even numbers*
4. *(infinitely many) all other zeros lie in the critical strip* $0<\mathrm{Re}(s)<1$*, conjectured to all lie on* $\mathrm{Re}(s)=1/2$*.*

9.2. Character theory of finite abelian groups.

9.2.1. Theorem (Dirichlet)**.** *If* $\gcd(a,m)=1$*, then there exist infinitely many primes congruent to a mod* m*.*

9.2.2. Definition. A mod m *Dirichlet character* is a character on $(\mathbb{Z}/m\mathbb{Z})^\times$, i.e. a homomorphism

$$\chi:(\mathbb{Z}/m\mathbb{Z})^\times\to\mathbb{C}^\times.$$

Extend to $\chi:\mathbb{Z}_{\geq 0}\to\mathbb{C}$ by mapping to zero the numbers a not coprime to n.

We review some character theory of finite abelian groups.

9.2.3. Proposition. *For a character* $\chi\in\widehat{G}$*,*

$$\sum_{g\in G}\chi(g)=\begin{cases}|G| & \text{if } \chi \text{ is trivial,}\\ 0 & \text{otherwise.}\end{cases}$$

PROOF. When χ is nontrivial, there exists $a\in G$, with $\chi(a)\neq 1$. Let s be the sum. Then

$$\chi(a)s=\sum_g\chi(ag)=\sum_g\chi(g)=s,$$

so $s=0$. □

9.2.4. Proposition. *For an element* $g\in G$*,*

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}|\widehat{G}|=|G| & \text{if } g=1,\\ 0 & \text{otherwise.}\end{cases}$$

The proof is similar.

9.2.5. Theorem (Fourier transform on finite abelian groups)**.** *Any function $f : G \to \mathbb{C}^\times$ is a linear combination of characters:*

$$f = \sum_\chi \widehat{f}(\chi)\chi$$

where

$$\widehat{f}(\chi) = \frac{1}{|G|}\sum_g \chi(g^{-1})f(g).$$

Proof. By linearity, it suffices to prove this for a basis of functions $G \to \mathbb{C}^\times$. Take f to be the indicator function for $a \in G$. Then

$$\widehat{f}(\chi) = \frac{1}{|G|}\chi(a^{-1}).$$

So $\sum_\chi \widehat{f}(\chi)\chi(g) = \frac{1}{|G|}\chi(a^{-1}g)$, which is 1 when $a^{-1}g = 1_G$ and 0 otherwise, i.e. the same as f. □

9.3. Proof of Dirichlet's theorem, minus two theorems.

9.3.1. Definition. Let χ be a Dirichlet character mod m. Define the *Dirichlet L-series*

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}} = \sum_{n\geq 1}\chi(n)n^{-s}.$$

This *a priori* converges absolutely for $\mathrm{Re}(s) > 1$.

9.3.2. Proposition. *If $\chi \neq \mathbf{1}$ (the trivial character), then $L(s,\chi)$ extends to a holomorphic function for* $\mathrm{Re}(s) > 0$.

Proof. Let $T(x) := \sum_{1\leq n<x}\chi(n)$ for $x \in \mathbb{R}$. This is periodic with period m, hence bounded. So

$$\begin{aligned}L(s,\chi) &= \sum_{n\geq 1}\chi(n)n^{-s} \\ &= \int_1^\infty x^{-s}dT(x) \\ &= x^{-s}T(x)|_1^\infty - \int_1^\infty -T(x)sx^{-s-1}dx \\ &= s\int_1^\infty T(x)x^{-s-1}dx\end{aligned}$$

where we've used the Riemann-Stieltjes integral. (Here it is just a fancy way to justify summation by parts.) This integral converges as long as $\mathrm{Re}(s) > 0$. Furthermore, it converges uniformly on $\mathrm{Re}(s) \geq \varepsilon$ for every ε, so L can be extended holomorphically to $\mathrm{Re}(s) > 0$. □

Proof of theorem 9.2.1, Dirichlet's theorem on arithmetic progressions. Writing the indicator function as the sum of characters,

$$\begin{aligned}\sum_{p\equiv a} p^{-s} &= \sum_p p^{-s}\,\mathrm{pr}\,\frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\chi(p) \\ &= \frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\,\mathrm{pr}\sum_p \chi(p)p^{-s} \\ &= \frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\,\mathrm{pr}\log L(s,\chi) + O(1) \\ &= \frac{1}{\phi(m)}\log L(s,\mathbf{1}) + \frac{1}{\phi(m)}\sum_{\chi\neq\mathbf{1}}\chi(a^{-1})\log L(s,\chi) + O(1).\end{aligned}$$

We have

$$\log L(s,\mathbf{1}) = \log\zeta(1) + O(1) \to \infty$$

as $s \to 1^+$. The goal now is to show that the other terms are in fact $O(1)$ as $s \to 1^+$. It is then sufficient to show that if $\chi \neq \mathbf{1}$, $L(1,\chi) \neq 0$. This would follow from the following two theorems, by analyzing the order of vanishing at $s = 1$. □

9.3.3. Theorem. *Up to Euler factors at primes dividing m,*

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod_{\chi:(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times} L(s,\chi).$$

9.3.4. Theorem. *For any number field K, $\zeta_K(s)$ has a simple pole at $s = 1$.*

We first remark that the proof above in fact shows that $\delta(\{p \equiv a \pmod m\}) = \frac{1}{\phi(m)}$.

Proof of theorem 9.3.3. We compare the two sides. Consider a prime $p \nmid m$ (so unramified), and consider primes $\mathfrak{p} \mid \mathfrak{p}$. So $e_p = 1$, f_p is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$, and $g_p = \phi(m)/f_p$. The corresponding term on the LHS is

$$\prod_{\mathfrak{p}|p}(1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1} = (1 - (p^{-s})^{f_p})^{-g_p}.$$

So it suffices to show that

$$\prod_{\chi}(1 - \chi(p)p^{-s}) = (1 - (p^{-s})^{f_p})^{g_p}.$$

Among the characters χ of $(\mathbb{Z}/m\mathbb{Z})^\times$, the values of $\chi(p)$ are $1, \mu_f, \mu_f^2, \dots, \mu^{f_p - 1}$, where μ_f is a primitive f-th root of unity, each with multiplicity g_p. This completes the proof. □

9.3.5. Theorem (analytic class number formula)**.** *Let K be a number field, then $\zeta_K(s)$ extends to a meromorphic function in a neighborhood of $s = 1$ with a simple pole at 1. Moreover,*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{\mathrm{vol}(\mathbb{A}_1^\times/K^\times)}{\mathrm{vol}(\mathbb{A}/K)} = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K / w_k}{\sqrt{|D_K|}},$$

where $h_K = \#\operatorname{Cl}_K$, $w_K = \#\mu_K$.

We will prove the latter equality and, in particular, define the volumes, so we will do a bit of review of measure theory. The former equality will be proven next semester in 18.786, using methods in Tate's thesis.

10. Analysis preliminaries

10.1. Measure theory.

10.1.1. Definition. Let X be a set, $\mathscr{M}$ a collection of subsets of X. If $\mathscr{M}$ is closed under countable unions and complements, call $\mathscr{M}$ a *σ-algebra.*

10.1.2. Example. Let X be a topological space. The set of *Borel sets* $\mathscr{B}$ is the σ-algebra generated by the open sets.

The sets in $\mathscr{M}$ are called *measurable sets.*

10.1.3. Definition. A function $f : X \to \mathbb{C}$ is called *measurable* if the inverse image of measurable subsets are measurable. (It suffices to check the inverse images of open disks.)

10.1.4. Definition. A *measure* on $(X, \mathscr{M})$ is a function $\mu : \mathscr{M} \to [0,\infty]$ such that $\mu(\bigcup A_i) = \sum \mu(A_i)$ for any countable collections of disjoint measurable sets. Call μ the *Borel measure* if $\mathscr{M} = \mathscr{B}$. A null set is a subset $N \subseteq X$ contained in a measure-0 set. It is easy to enlarge $\mathscr{M}$ so that all null sets are measurable. A function $f : X \to \mathbb{C}$ is a *null function* if $\{x \in X : f(x) = 0\}$ is a null set.

We now define in stages a notion of integrals. Fix $(X, \mathscr{M}, \mu)$.

- Given $S \in \mathscr{M}$ with $\mu(S) < \infty$, let 1_S be the function that is 1 on S and 0 on $X - S$. Then define $\int 1_S = \mu(S)$.
- A *step function* f is a finite $\mathbb{C}$-linear combination of 1_S's. Define $\int f$ linearly.
- Define the L^1 norm of f, $\|f\|_1 := \int |f| \in \mathbb{R}_{\geq 0}$. Call a function $f : X \to \mathbb{C}$ *integrable* if outside a null set, it is equal to the pointwise limit of some L^1-Cauchy sequence (f_i) of step functions. Then define $\int_X f d\mu = \int f = \lim_i \int f_i \in \mathbb{C}$. (The pointwise limit of measurable functions is measurable, so in particular integrable functions are measurable.)

10.2. Radon measures and integrals. There is an alternative definition of integration for all measurable functions $f : X \to [0, \infty]$, which agrees with the previous definition if f is integrable:

$$\int f := \sup\{\int g : g \text{ is a step function and } 0 \leq g \leq f\} \in [0, \infty].$$

Also, for a measurable function $f : X \to \mathbb{C}$, f is integrable iff $|f|$ is integrable, in which case we have $|\int f| \leq \int |f|$.

10.2.1. Theorem (Monotone convergence theorem)**.** *Suppose (f_n) is a sequence of measurable functions $X \to [0, \infty]$ such that $0 \leq f_1 \leq f_2 \leq \dots$, then the pointwise limit f satisfies $\int f = \lim \int f_n$.*

10.2.2. Theorem (Dominated convergence theorem)**.** *Suppose measurable functions $f_1, f_2, \cdots : X \to \mathbb{C}$ converge pointwise to $f : X \to \mathbb{C}$. If there is an integrable $g : X \to \mathbb{C}$ such that $|f_n| \leq |g|$ for all n, then f and f_n are all integrable and $\int f = \lim \int f_n$.*

10.2.3. Definition. Let X be a Hausdorff topological space. X is *locally compact* if every $x \in X$ has a compact neighborhood (i.e. $x \in U \subseteq K$ where U open and K compact).

10.2.4. Definition. An *outer Radon measure* is a Borel measure (a measure on $\mathscr{B}$) such that:

- (locally finite) Every $x \in X$ has an open neighborhood U such that $\mu(U) < \infty$;
- (outer regular) Every $S \in \mathscr{B}$ satisfies $\mu(S) = \inf\{\mu(U) : U \supseteq S \text{ open}\}$;
- (inner regular) Every open U satisfies $\mu(U) = \sup\{\mu(K) : K \subseteq U \text{ compact}\}$;

Let $C(X)$ be the $\mathbb{C}$-vector space of continuous functions $f : X \to \mathbb{C}$, and let $C_c(X)$ be the $\mathbb{C}$-vector space of continuous functions with compact support.

10.2.5. Definition. A *Radon integral* on X is a $\mathbb{C}$-linear map $I : C_c(X) \to \mathbb{C}$ such that $I(f) \geq 0$ if $f \geq 0$. (It is assumed that f is real-valued.)

Given an outer Radon measure μ, we can define an integral $I_\mu : f \mapsto \int_X f d\mu$. The converse is:

10.2.6. Theorem (Riesz–Markov–Kakutani representation theorem)**.** *Let X be a LCH space, then the map*

$$\{\textit{outer Radon measures } \mu\} \to \{\textit{Radon integrals on } X\}$$

by $\mu \mapsto I_\mu$, is a bijection.

10.2.7. Example. Let $X = \mathbb{R}^n$, the Riemann integral corresponds to the Lebesgue measure.

10.2.8. Example. Examples of LCH topological groups:

- $\mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \mathbb{Q}_p, \mathbb{A}$;
- The unit groups $A^\times$ of any of the above topological rings;
- $\mathrm{GL}_n(A)$ of any of the above;
- Any group equipped with the discrete topology.

10.3. Haar measures.

10.3.1. Definition. Let G be a LCH topological group. A *left Haar measure* on G is a nonzero left-invariant outer Radon measure.

Theorem 6.1.4 says that such a measure always exists and is unique up to multiplication by a positive constant.

10.3.2. Proposition. *G is compact iff $\mu(G) < \infty$. In this case, the* normalized Haar measure *is the unique Haar measure with $\mu(G) = 1$.*

10.3.3. Example. Examples of Haar measures:

- On $\mathbb{R}^n$, the Lebesgue measure is a Haar measure;
- On a discrete group, the counting measure is a Haar measure.

10.3.4. Definition. An *LCA group* is a locally compact abelian Hausdorff topological group. This forms a category, with morphisms being continuous homomorphisms.

For example, $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$ is the unit circle in the complex plane; it is an LCA group.

10.4. Duality of locally compact abelian groups.

10.5. Dec. 7.

10.6. Dec. 9.

10.7. Dec. 12.

10.8. Dec. 14.

11. Local class field theory: Setup

11.1. Kronecker–Weber theorem.

11.1.1. Theorem (global KW). *Any finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$.*

11.1.2. Theorem (local KW). *Any finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}_p(\zeta_m)$.*

11.1.3. Lemma (Galois group of compositum). *Let $L_1, L_2/K$ be finite Galois extensions that lie in some bigger extension Ω/K. Then L_1L_2 is Galois over K, with*

$$\mathrm{Gal}(L_1L_2/K) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) : \sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}\}.$$

11.1.4. Proposition. *Local KW implies global KW.*

Proof. Consider each prime $p \in \mathbb{Z}$ where a finite abelian extension $K/\mathbb{Q}$ is ramified. Fix $\mathfrak{p} \mid p$ to be a prime in K above p, and consider the extension $K_\mathfrak{p}/\mathbb{Q}_p$, which is finite abelian with $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) = D_\mathfrak{p}$. Assuming local KW, suppose $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p})$. Let $n_p = v_p(m_p)$ and $m = \prod p^{n_p}$, among all (finitely many) p that ramify. Let $L = K(\zeta_m)$. It suffices to show $L = \mathbb{Q}(\zeta_m)$.

Because $L = K \cdot \mathbb{Q}(\zeta_m)$, $L/\mathbb{Q}$ is abelian as well. Pick a prime $\mathfrak{q} \mid \mathfrak{p}$ in L/K, then $L_\mathfrak{q}$ is also finite abelian over $\mathbb{Q}_p$. Let $F_\mathfrak{q}$ be the maximal unramified extension of $\mathbb{Q}_p$ in $L_\mathfrak{q}$. Then $L_\mathfrak{q}/F_\mathfrak{q}$ is totally ramified with Galois group $I_\mathfrak{q} =: I_p$, which only depends on p (since the Galois group is abelian).

We claim that $I_p \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times$. To show this, notice that $\mathbb{Q}_p(\zeta_{m_p/p^{n_p}})$ is unramified over $\mathbb{Q}_p$, so $K_\mathfrak{p} \subset F_\mathfrak{q}(\zeta_{p^{n_p}})$. Now, since $L_\mathfrak{q} \supseteq K_\mathfrak{p}(\zeta_m)$ and $[L_\mathfrak{q} : K_\mathfrak{p}] = [L : K]$, $L_\mathfrak{q} = K_\mathfrak{p}(\zeta_m) \subseteq F_\mathfrak{q}(\zeta_{p^{n_p}})$, so in fact $L_\mathfrak{q} = F_\mathfrak{q}(\zeta_{p^{n_p}})$. So we have the following field inclusions

$$\begin{tikzcd}
 & L_\mathfrak{q} \arrow[dl, dash] \arrow[dr, dash] & \\
F_\mathfrak{q} \arrow[dr, dash] & & \mathbb{Q}_p(\zeta_{p^{n_p}}) \arrow[dl, dash] \\
 & \mathbb{Q}_p, &
\end{tikzcd}$$

where $\mathbb{Q}_p = F_\mathfrak{q} \cap \mathbb{Q}_p(\zeta_{p^{n_p}})$ since one is unramified and the other is totally ramified. So

$$I_p = \mathrm{Gal}(L_\mathfrak{q}/F_\mathfrak{q}) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_p}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times.$$

Now, let I be the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by I_p's. Then

$$|I| \leq \prod |I_p| = \prod \phi(p^{n_p}) = \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

Let L^I be the fixed field of I. Then $L^I/\mathbb{Q}$ is unramified, so $L^I = \mathbb{Q}$. This means

$$[L : \mathbb{Q}] = [L : L^I] = |I| \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \leq [L : \mathbb{Q}],$$

so $L = \mathbb{Q}(\zeta_m)$ as desired. □

11.1.5. Proposition. *It suffices to show local KW for cyclic extensions with Galois group $\mathbb{Z}/\ell^r\mathbb{Z}$.*

Proof. For an arbitrary abelian extension $K/\mathbb{Q}_p$, decompose its Galois group into the product of prime-power cyclic groups H_i, and let $K_i = K^{H_i}$. Then $K = \bigvee K_i$ (compositum), from which the proposition is clear. □

Now we begin the proof of local KW, with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/\ell^r\mathbb{Z}$. There are three cases:

- tamely ramified case, $\ell \neq p$;
- wildly ramified case with odd degree, $\ell = p \geq 3$;
- wildly ramified case with even degree, $\ell = p = 2$.

Proof of case 1. Let F be the maximal unramified extension of $\mathbb{Q}_p$ in K. Then $F/\mathbb{Q}_p$ is already equal to some cyclotomic extension (to see this, consider the corresponding finite separable extension of residue fields; the Galois group of finite field extensions is cyclic). Furthermore, $K = F(\pi^{1/e})$ for some uniformizer π in F (cf. 5.6.3). Assume that $\pi = -pu$, where $u \in \mathcal{O}_K^\times$. Then K lies in the compositum $F((-p)^{1/e}) \cdot F(u^{1/e})$, and it suffices to show both are included in some cyclotomic extension of F.

For $F(u^{1/e})/F$, it is unramified since the discriminant is $\operatorname{disc}(x^e - u)$, which is a unit in F. This implies that it is also equal to some cyclotomic extension.

Consider $K(u^{1/e})/\mathbb{Q}_p$, which is the compositum of K and $F(u^{1/e})$, so it is also an abelian extension. Therefore, since $F((-p)^{1/e}) \subseteq K(u^{1/e})$, $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is Galois as well, which implies $\zeta_e \in \mathbb{Q}_p((-p)^{1/e})$ because $\mathbb{Q}_p((-p)^{1/e})$ then must contain all e-th roots of $-p$. And it is totally ramified since the minimal polynomial of $(-p)^{1/e}$, $x^e + p$, is Eisenstein. Since $\mathbb{Q}_p(\zeta_e) \subset \mathbb{Q}_p((-p)^{1/e})$ is unramified over $\mathbb{Q}_p$, we conclude $\mathbb{Q}_p(\zeta_e) = \mathbb{Q}_p$. Because the residue field of $\mathbb{Q}_p$ contains only $(p-1)$-th roots of unity, $e \mid (p-1)$. Then

$$\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p),$$

by the lemma that follows. But from this we conclude that $F((-p)^{1/e})$ is also in some cyclotomic extension, so we are done. □

11.1.6. Lemma. $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.

Proof. Let $\alpha = (-p)^{1/(p-1)}$. Then $\alpha^{p-1} + p = 0$, which is an Eisenstein polynomial of degree $p-1$, so α is a uniformizer for $\mathbb{Q}_p(\alpha)$. Let $\pi = \zeta_p - 1$, whose minimal polynomial is also Eisenstein of degree $p-1$, so π is a uniformizer for $\mathbb{Q}_p(\zeta_p)$. The goal now is to show that $\alpha \in \mathbb{Q}_p(\zeta_p)$, from which the lemma will follow by a degree argument.

Let $u = -\pi^{p-1}/p \equiv 1 \pmod{\pi}$, so u is an unit in the valuation ring of $\mathbb{Q}_p(\zeta_p)$. Consider $g(x) = x^{p-1} - u$, which, mod π, has 1 as a simple root, so by Hensel's lemma we obtain a root β of $g(x)$. Then

$$(\pi/\beta)^{p-1} + p = \frac{\pi^{p-1} + p\beta^{p-1}}{\beta^{p-1}} = 0,$$

so $\alpha \mapsto \pi/\beta$ gives an injection. □

Proof of case 2. Suppose $K/\mathbb{Q}_p$ cyclic of degree p^r, $p \geq 3$. There are two obvious cyclotomic extensions of degree p^r; in the unramified case we have $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$, and in the totally ramified case we have the index-$(p-1)$ subfield of $\mathbb{Q}_p(\zeta_{p^{r+1}})$. Suppose for contradiction K does not lie in $\mathbb{Q}_p(\zeta_{p^{r+1}(p^{p^r}-1)})$. Then

$$\operatorname{Gal}(K(\zeta_{p^{r+1}(p^{p^r}-1)})/\mathbb{Q}_p) \subseteq \operatorname{Gal}(K/\mathbb{Q}_p) \times (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}$$

surjecting onto the last two factors, and nontrivial in the first. So the Galois group has a quotient group that is $(\mathbb{Z}/p\mathbb{Z})^3$, i.e. there exists an extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$. We are going to show that no such extensions exist. □

11.1.7. Definition (semidirect product)**.** Let G be a group, $N \lhd G$ a normal subgroup, and $H \leq G$ a subgroup. If $H \to G \to G/N$ is an isomorphism, then we say $G = N \rtimes H$.

More generally, let H, N be groups, with a homomorphism $\phi : H \to \operatorname{Aut}(N)$. Then $N \rtimes H$, as a set, is equal to $N \times H$, but the group operation is given by

$$(n_1, h_1)(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2).$$

This is the (outer) semidirect product.

11.1.8. Proposition (Schur-Zassenhaus lemma)**.** *Let $N \lhd G$ with $|N|$ and $|G/N|$ coprime, then there exists a subsection $G/N \to G$. Consequently $G = N \rtimes G/N$.*

11.1.9. Proposition. *Let p be an odd prime, then any totally wildly ramified Galois extension of $\mathbb{Q}_p$ is cyclic.*

Proof. See 18.786 pset 1. □

11.1.10. Theorem. *Let p be an odd prime, then no $(\mathbb{Z}/p\mathbb{Z})^3$-extension $K/\mathbb{Q}_p$ exists.*

PROOF. We first only assume $K/\mathbb{Q}_p$ is Galois. Let $G = \mathrm{Gal}(K/\mathbb{Q}_p)$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be the unique prime above p. Since $\mathcal{O}_K$ is a DVR, $G = D_{\mathfrak{p}}$. Let the *ramification groups* $G_i = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathfrak{p}^{i+1}}$ for any $x \in \mathcal{O}_K\}$, and let $\pi_{\mathfrak{p}} : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ be the natural map whose kernel is $I_{\mathfrak{p}} = G_0$.

Let $U_i = 1 + \mathfrak{p}^i$ be subgroups of $\mathcal{O}_K^\times$ for $i \geq 1$, and set $U_0 = \mathcal{O}_K^\times$. Then $U_0/U_1 \cong \mathbb{F}_{\mathfrak{p}}^\times$ and $U_i/U_{i+1} \cong \mathbb{F}_{\mathfrak{p}}$ as abelian groups. For each $i \geq 0$, there is an injection $G_i/G_{i+1} \hookrightarrow U_i/U_{i+1}$ given by $\sigma \mapsto \sigma(\pi)/\pi$ where $\mathfrak{p} = (\pi)$. Therefore, G_0/G_1 is cyclic with order coprime to p, and G_1 is a p-group. Consider the normal subgroups $G_1 \lhd G_0 \lhd G$ (which implies that G is solvable), then the corresponding subfield $K^{G_0} = K^I$ is the maximal unramified extension of $\mathbb{Q}_p$ in K, $K^{G_1}/\mathbb{Q}_p$ is the maximal tamely ramified extension, and K/K^{G_1} is totally wildly ramified.

By Proposition 11.1.8, $G_0 \cong G_1 \ltimes G_0/G_1$.

In the case $G = (\mathbb{Z}/p\mathbb{Z})^3$, since all nontrivial proper subgroups are $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z}$, so $G \cong I \times H$, where $H := \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is cyclic. Since $K^H/\mathbb{Q}_p$ is totally wildly ramified ($I = \mathrm{Gal}(K^H/\mathbb{Q}_p)$ is a p-group), it is cyclic. But G is not the product of two cyclic groups. □

11.1.11. Remark. If p is odd, then there are exactly p ramified extensions with degree p, namely

$$\mathbb{Q}_p[x]/(x^p + px^{p-1} + p(1 + ap))$$

for $0 \leq a \leq p - 1$.

PROOF OF CASE 3. In this case, $\mathbb{Q}_2(\zeta_{24})/\mathbb{Q}_2$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. But we can still follow a similar argument. Suppose $K/\mathbb{Q}_2$ is cyclic with order 2^r. As usual, the suspects are $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{2^r}-1})/\mathbb{Q}_2) \cong \mathbb{Z}/2^r\mathbb{Z}$ and $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{r+2}})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^{r+2}\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$. We claim that $K \subseteq \mathbb{Q}(\zeta_{2^{r+2}(2^{2^r}-1)})$. Suppose otherwise, then either

$$\mathrm{Gal}(K(\zeta_{2^{r+2}(2^{2^r}-1)})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^s\mathbb{Z}$$

for $s \geq 1$, or

$$\mathrm{Gal}(K(\zeta_{2^{r+2}(2^{2^r}-1)})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z}$$

for $s \geq 2$. So it has a quotient equal to either $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. In the first case, we can show that there are 7 quadratic extensions of $\mathbb{Q}_2$, but $(\mathbb{Z}/2\mathbb{Z})^4$ has 15 subgroups of index 2; in the second case, there are 12 cyclic quartic extensions of $\mathbb{Q}_2$, but $(\mathbb{Z}/4\mathbb{Z})^3$ has 28 subgroups whose quotient is $\mathbb{Z}/4\mathbb{Z}$ (see LMFDB). □

This finishes the proof of Kronecker–Weber theorem.

11.2. The Artin map.

Now fix L/K an abelian extension of global fields, so that we have the Artin symbol

$$\mathrm{pr}\,\frac{L/K}{\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{p}} =: \sigma_{\mathfrak{p}}$$

for unramified $\mathfrak{p}$. Let $\mathfrak{m}$ be an ideal divisible by all ramified primes. Then we have the Artin map

$$\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K).$$

The first major step in proving class field theory is the following:

11.2.1. Proposition. *Let K be a number field, L/K abelian. Then the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is surjective.*

11.2.2. Proposition. *The primes in* $\ker \psi_{L/K}$ *are the primes in K that split completely in L.* □

11.2.3. Proposition. *Let $K \subseteq L \subseteq M$ be a tower of abelian extensions of global fields. Then the Artin maps commute with the restriction map* $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$.

11.3. Ray class groups.

11.3.1. Proposition. *The Artin map is surjective for abelian extensions $L/\mathbb{Q}$.*

PROOF. By KW it suffices to show this for $L = \mathbb{Q}(\zeta_m)$. In this case, (p) hits the residue class of p in $(\mathbb{Z}/m\mathbb{Z})^\times$, so the Artin map is clearly surjective. □

For global field K, let M_K be the set of places of K. Finite places v are ones corresponding to prime ideals, and the rest are infinite places. (Infinite places can be nonarchimedean; for example, since function fields have characteristic p, all nontrivial places are nonarchimedean. Places of a function field correspond 1-to-1 with closed points of its associated smooth projective curve. For number fields, however, infinite places are all archimedean, and are either real or complex.)

11.3.2. Definition. Let K be a number field. A *modulus* for K is a function $\mathfrak{m} : M_K \to \mathbb{Z}_{\geq 0}$ with finite support, such that $\mathfrak{m}(v) \leq 1$ for infinite places, and $\mathfrak{m}(v) = 1$ only when v is real.

This should be thought of as a product of prime ideals and some set of real places.

11.3.3. Definition. A fractional ideal I of $\mathcal{I}_K$ is *coprime* to $\mathfrak{m}$ if $v_{\mathfrak{p}}(I) = 0$ for finite primes $\mathfrak{p} \mid \mathfrak{m}$. The subgroup of fractional ideals coprime to $\mathfrak{m}$ is denoted by $\mathcal{I}_K^{\mathfrak{m}}$. The subgroup of elements $a \in K^\times$ such that $(a) \in \mathcal{I}_K^{\mathfrak{m}}$ is denoted by $K^{\mathfrak{m}}$. Finally, $K^{\mathfrak{m},1}$ is the subgroup of elements a where $v_{\mathfrak{p}}(a-1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ for finite $\mathfrak{p} \mid \mathfrak{m}$, and $a_v > 0$ for all infinite $v \mid \mathfrak{m}$ where a_v is the image of the embedding $K \hookrightarrow K_v = \mathbb{R}$.

11.3.4. Definition. The *ray group* $\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ is the image of $K^{\mathfrak{m},1}$ in $\mathcal{I}_K^{\mathfrak{m}}$. The *ray class group* for $\mathfrak{m}$ is $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$.

11.3.5. Definition. A finite abelian extension L/K unramified at all primes that do not divide $\mathfrak{m}$, for which $\ker \psi_{L/K}^{\mathfrak{m}} = \mathcal{R}_K^{\mathfrak{m}}$ is called a *ray class field* for $\mathfrak{m}$. When $\mathfrak{m}$ is trivial, it is the *Hilbert class field*, i.e. the maximal unramified abelian extension (which we will show).

When $\mathfrak{m}$ has only all the real places, this is called the *narrow class group.*

11.3.6. Lemma. *Let A be a Dedekind domain, $\mathfrak{a}$ an A-ideal. Then every ideal class in* $\mathrm{Cl}(A)$ *contains an A-ideal coprime to $\mathfrak{a}$.*

Proof. Let I be a nonzero fractional ideal. For each $\mathfrak{p} \mid \mathfrak{a}$, pick $\pi_{\mathfrak{p}} \in \mathfrak{p}$ such that $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$ and $v_{\mathfrak{q}}(\pi_{\mathfrak{p}}) = 0$ for all other $\mathfrak{q} \mid \mathfrak{a}$ by strong approximation. Then $I' = (\prod_{\mathfrak{p} \mid \mathfrak{a}} \pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}(\mathfrak{a})})I$ is in the class of I and satisfies I' coprime to $\mathfrak{a}$. Then make it integral by multiplying by the appropriate elements again found by strong approximation. □

11.3.7. Proposition. *Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus for K. We have an exact sequence*

$$(*) \qquad 0 \to \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \to \mathcal{O}_K^\times \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 0.$$

and $K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$ canonically.

Proof. Consider the composition $K^{\mathfrak{m},1} \xrightarrow{f} K^{\mathfrak{m}} \xrightarrow{g} \mathcal{I}_K^{\mathfrak{m}}$. Then f is injective, $\ker(g) = \mathcal{O}_K^\times$, $\ker(g \circ f) = \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$, $\mathrm{coker}(g) = \mathcal{I}_K^{\mathfrak{m}}/\mathrm{im}(K^{\mathfrak{m}}) = \mathrm{Cl}_K$ by the previous lemma, and $\mathrm{coker}(g \circ f) = \mathrm{Cl}_K^{\mathfrak{m}}$. The kernel-cokernel exact sequence yields

$$0 \to \ker(f) \to \ker(g \circ f) \to \ker(g) \to \mathrm{coker}(f) \to \mathrm{coker}(g \circ f) \to \mathrm{coker}(g) \to 0,$$

which becomes $(*)$.

For the second statement, given $\alpha \in K^{\mathfrak{m}}$, write $\alpha = a/b \in K^{\mathfrak{m}}$ where $a, b \in \mathcal{O}_K$ are both coprime to $\mathfrak{m}$. Send

$$\phi : K^{\mathfrak{m}} \to \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$$

by α mapping to $(\mathrm{sgn}(\alpha_v), \overline{\alpha} = \overline{a}\overline{b}^{-1})$. This is surjective by strong approximation, and the kernel is precisely $K^{\mathfrak{m},1}$. This is canonical because $\overline{\alpha}$ does not depend on a, b. □

11.3.8. Corollary. *Let $h_K^{\mathfrak{m}} = |\,\mathrm{Cl}_K^{\mathfrak{m}}\,|$ be the ray class number. Then*

$$h_K^{\mathfrak{m}} = \frac{\phi(\mathfrak{m}) h_K}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}]}.$$

Here $\phi(\mathfrak{m}) = \phi(\mathfrak{m}_0)\phi(\mathfrak{m}_\infty) = |K^{\mathfrak{m}}/K^{\mathfrak{m},1}|$, where

$$\phi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty}, \quad \phi(\mathfrak{m}_0) = |(\mathcal{O}_K/\mathfrak{m}_0)^\times| = \prod_{\mathfrak{p} \mid \mathfrak{m}_0} |(\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times| = \mathrm{N}(\mathfrak{m}_0) \prod_{\mathfrak{p} \mid \mathfrak{m}_0} (1 - \mathrm{N}(\mathfrak{p})^{-1}).$$

11.4. Polar density.

11.4.1. Definition. Let S be a set of primes of a global field K. The *partial Dedekind zeta function*

$$\zeta_{K,S} := \prod_{\mathfrak{p}\in S} \frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}}.$$

This converges on $\mathrm{Re}(s) > 1$.

If S is finite then this is just holomorphic on a neighborhood of $s = 1$. If S is cofinite then this is ζ_K over a holomorphic function, hence meromorphic on a neighborhood of 1 with a simple pole at 1.

11.4.2. Definition. If $\zeta^n_{K,S}$ extends to a meromorphic function on a neighborhood of 1, the *polar density*

$$\rho(S) := \frac{m}{n},$$

where m is the order of the pole.

The *Dirichlet density* is

$$d(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}},$$

and the *natural density* is

$$\delta(S) = \lim_{n\to\infty} \frac{\#\{\mathfrak{p}\in S : \mathrm{N}(\mathfrak{p}) \le n\}}{\#\{\mathfrak{p} : \mathrm{N}(\mathfrak{p}) \le n\}}.$$

11.4.3. Proposition. *If S has a natural density, then it has a Dirichlet density, and the two densities agree.*

PROOF. 18.786 problem set 2. □

11.4.4. Proposition. *If S has a polar density, then it has a Dirichlet density, and the two densities agree.*

PROOF. Suppose $\rho(S) = m/n$, then the Laurent series for $\zeta^n_{K,S}$ is

$$a(s-1)^{-m} + \sum_{r>-m} a_r (s-1)^r.$$

Since $\zeta_{K,S}(s) > 0$ for real $s > 1$, $a > 0$. Taking logarithms on both sides,

$$n\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s} \sim m \log\frac{1}{s-1}$$

as $s \to 1^+$. This shows that $d(S) = m/n = \rho(S)$. □

11.4.5. Proposition. *Let S, T be sets of primes in a number field K. Let $\mathcal{P}$ be the set of all primes, and $\mathcal{P}_1$ the set of primes with $f = 1$. Then:*

(a) If S is finite, $\rho(S) = 0$. If $\mathcal{P}\backslash S$ is finite, then $\rho(S) = 1$.
(b) If $S \subseteq T$ then $\rho(S) \le \rho(T)$ if both exist.
(c) If $S \cap T$ is finite, then $\rho(S\cup T) = \rho(S) + \rho(T)$ whenever two of the three exist.
(d) $\rho(\mathcal{P}_1) = 1$, and $\rho(S\cap\mathcal{P}_1) = \rho(S)$ whenever S has polar density.

PROOF. (d) Let $\mathcal{P}_2$ be the other primes. The key fact here is that there are at most $n = [K : \mathbb{Q}]$ primes above p in $\mathcal{P}_2$, each with norm at least p^2. So $\zeta_{K,\mathcal{P}_2}(s) < \zeta^n(2s)$, so $\zeta_{K,\mathcal{P}_2}$ is holomorphic and vanishing around 1. □

11.5. Surjectivity of the Artin map. We begin by commenting that all this works for global functions as well, only the proofs will be sllightly different. Our goal in this subsection is to show the surjectivity of the Artin map.

11.5.1. Theorem. *Let L/K be Galois extensions of number fields of degree n. Let $\mathrm{Spl}(L/K)$ be the set of primes in K that split completely in L. Then $\rho(\mathrm{Spl}(L/K)) = 1/n$.*

Proof. Let S be the set of degree-1 primes that split completely, it suffices to show $\rho(S) = 1/n$. For these $\mathfrak{p}$, $e = f = 1$. Let $T = \{\mathfrak{q} \mid \mathfrak{p} : \mathfrak{p} \in S\}$, then $\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}$, and $\mathrm{N}(\mathfrak{q}) = \#(\mathcal{O}_L/\mathfrak{q}) = \mathrm{N}(\mathfrak{p})$, so $\mathfrak{q}$ is degree 1 as well. On the other hand, any unramified $\mathfrak{q}$ of degree 1 must lie above an unramified degree-1 prime $\mathfrak{p}$, which is in S; so all but finitely many (ramified) degree-1 primes $\mathfrak{q} \in T$. This means $\rho(T) = 1$.

Each prime $\mathfrak{p} \in S$ has n primes above it in T. So

$$\zeta_{L,T} = \prod_{\mathfrak{q} \in T} \frac{1}{1 - \mathrm{N}(\mathfrak{q})^{-s}} = \prod_{\mathfrak{p} \in S} \frac{1}{(1 - \mathrm{N}(\mathfrak{p})^{-s})^n} = \zeta_{K,S}^n.$$

This shows $\rho(S) = \frac{1}{n}\rho(T) = \frac{1}{n}$. □

11.5.2. Corollary. *Let L/K be a finite extension with Galois closure M/K of degree n. Then $\rho(\mathrm{Spl}(L/K)) = \rho(\mathrm{Spl}(M/K)) = \frac{1}{n}$.*

Proof. A prime $\mathfrak{p} \subset K$ splits completely in L iff it splits completely in every conjugate of L in M, iff it splits completely in M. □

11.5.3. Corollary. *Let L/K be finite Galois with Galois group G, and $H \lhd G$. Then $S = \{\mathfrak{p} \in K : \mathrm{Frob}_{\mathfrak{p}} \subseteq H\}$ has polar density $\rho(S) = \#H/\#G$.*

Proof. We have $\mathrm{Gal}(L^H/K) \cong G/H$, and $\mathrm{Frob}_{\mathfrak{p}} \subseteq H$ iff every $\mathrm{Frob}_{\mathfrak{q}}$ fixes L^H for $\mathfrak{q} \mid \mathfrak{p}$ in L, iff $\mathfrak{p}$ splits completely in L^H. □

Write $S \sim T$ if $S \triangle T$ is finite; $S \lesssim T$ if $S - T$ is finite.

11.5.4. Lemma. *Let $L/K, M/K$ be finite Galois extensions, and LM be their compositum. Then a prime in K splits completely (resp. is unramified) in LM iff it splits completely (resp. is unramified) in both L and M.*

Proof. Use the fact that for a tower of Galois extensions $M/N/K$, if $\mathfrak{p} \subset K$ and $\mathfrak{q} \subset M$ lies above $\mathfrak{p}$, then $D(\mathfrak{q})$ fixes N iff $e_{\mathfrak{p}}(N/K) = f_{\mathfrak{p}}(N/K) = 1$. Then since $\mathfrak{p}$ splits completely in both L and M, for any $\mathfrak{q}$ in LM above $\mathfrak{p}$, both $L, M \subseteq (LM)^{D_{\mathfrak{q}}}$, hence $LM \subseteq (LM)^{D_{\mathfrak{q}}}$, hence $|D_{\mathfrak{q}}| = 1$. □

11.5.5. Theorem. *If L/K, M/K are finite Galois, then*

$$L \subseteq M \iff \mathrm{Spl}(M) \subseteq \mathrm{Spl}(L) \iff \mathrm{Spl}(M) \lesssim \mathrm{Spl}(L).$$

Proof. The nontrivial direction is showing that $\mathrm{Spl}(M) \lesssim \mathrm{Spl}(L) \implies L \subseteq M$. Consider the compositum LM, then a prime $\mathfrak{p}$ in K splits completely in LM if and only if it splits completely in both L and M. So $\mathrm{Spl}(LM) \sim \mathrm{Spl}(M)$. This implies $\frac{1}{[M:K]} = \frac{1}{[LM:K]}$, so $LM = M$, so $L \subseteq M$. □

11.5.6. Theorem (the Artin map is surjective)**.** *Let L/K be finite abelian, $\mathfrak{m}$ a modulus divisible by all primes in K that ramify and all real places in K that ramify (that extend to a complex place). Then*

$$\psi_{L/K}^{m} : \mathcal{I}_{L/K}^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

is surjective.

Proof. Let H be the image, and $F := L^H$; we will show $F = K$.

For any $\mathfrak{p} \in \mathcal{I}_{L/K}^{\mathfrak{m}}$, $\psi_{L/K}^{\mathfrak{m}}(\mathfrak{p}) \in H$, so $\mathrm{Frob}_{\mathfrak{p}}$ acts trivially on F, so $\mathfrak{p}$ splits completely in F. But $\mathcal{I}_{L/K}^{\mathfrak{m}}$ contains all but finitely many primes, so $\rho(\mathrm{Spl}(F/K)) = 1$. But $\rho(\mathrm{Spl}(F/K)) = \frac{1}{[F:K]}$, so $F = K$ as desired. □

11.5.7. Theorem. *Let $\mathfrak{m}$ be a modulus for K, and $L/K, M/K$ finite abelian extensions unramified away from $\mathfrak{m}$. If $\ker \psi_{L/K}^{\mathfrak{m}} = \ker \psi_{M/K}^{\mathfrak{m}}$, then $L = M$. In particular, the ray class field is unique (only depends on $\mathfrak{m}$).*

Proof. Consider the set S of primes not dividing $\mathfrak{m}$. Then $\mathfrak{p} \in S$ splits completely in L iff it is in $\ker \psi_{L/K}^{\mathfrak{m}}$. So $\mathrm{Spl}(L/K) \sim S \cap \ker \psi_{L/K} = S \cap \ker \psi_{M/K} \sim \mathrm{Spl}(M/K)$, so $L = M$ by applying Theorem 11.5.5 twice. □

By surjectivity of the Artin map, if the ray group $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$, then $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Cl}_K^{\mathfrak{m}}$, with equality iff L is the ray class field, which we denote by $K(\mathfrak{m})$. In general, the intermediate fields between K and $K(\mathfrak{m})$ correspond 1-to-1 to subgroups between $\mathcal{R}_K^{\mathfrak{m}}$ and $\mathcal{I}_K^{\mathfrak{m}}$, by $L \mapsto \mathcal{C} = \ker \psi_{L/K}^{\mathfrak{m}}$ and $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C} \cong \mathrm{Gal}(L/K)$.

Given a finite abelian L/K, there may be many choices of $\mathfrak{m}$, and as we make $\mathfrak{m}$ smaller, the ray group $\mathcal{R}_K^{\mathfrak{m}}$ gets bigger so that it might not be contained inside $\ker \psi_{L/K}^{\mathfrak{m}}$. Fortunately there is a minimal modulus that works, called the *conductor*, for which $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$, which implies $\mathrm{Spl}(K(\mathfrak{m})) \subseteq \mathrm{Spl}(L)$, which implies $L \subseteq K(\mathfrak{m})$.

11.6. Conductors.

11.6.1. Definition. A *congruence subgroup* for a modulus $\mathfrak{m}$ in a global field K is a subgroup $\mathcal{C} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ that contains the ray group $R_K^{\mathfrak{m}}$.

11.6.2. Definition. For two congruence subgroups $\mathcal{C}_1$ for $\mathfrak{m}_1$ and $\mathcal{C}_2$ for $\mathfrak{m}_2$, say that

$$(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$$

iff $\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1$. This defines an equivalence relation, and if $\mathfrak{m}_1 = \mathfrak{m}_2$ then $\mathcal{C}_1 = \mathcal{C}_2$.

The reason we are interested in this equivalence relation, is that if $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$, then $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \cong \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ canonically, and the isomorphism preserves cosets of ideals coprime to $\mathfrak{m}_1\mathfrak{m}_2$. And these quotients are what we really care about.

If $\mathcal{C}$ is a congruence subgroup for two moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$, then $(\mathcal{C}, \mathfrak{m}_1) \sim (\mathcal{C}, \mathfrak{m}_2)$. So each subgroup $\mathcal{C} \subseteq \mathcal{I}_K$ lies in at most one equivalence class. So we can just write $\mathcal{C}_1 \sim \mathcal{C}_2$ without specifying the moduli. Also, within one equivalence class, there can be at most one congruence subgroup with a specified modulus.

11.6.3. Lemma. *Let $(\mathcal{C}_1, \mathfrak{m}_1)$ be a congruence subgroup, and $\mathfrak{m}_2 \mid \mathfrak{m}_1$. There exists $(\mathcal{C}_2, \mathfrak{m}_2)$ in the same equivalence class iff*

$$\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_1,$$

in which case $\mathcal{C}_2 = \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2}$.

11.6.4. Proposition. *If $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$, then there exists a congruence subgroup $\mathcal{C}$ in the same equivalence class, with modulus $\mathfrak{m} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$.*

11.6.5. Corollary. *If $(\mathcal{C}, \mathfrak{m})$ is a congruence subgroup, then there exists a unique $\mathcal{C}' \sim \mathcal{C}$ whose modulus divides that of any $\mathcal{C}'' \sim \mathcal{C}$.*

11.6.6. Definition. The unique modulus $\mathfrak{c} = \mathfrak{c}(\mathcal{C})$ given by the above corollary is called the *conductor* of $\mathcal{C}$. We say $\mathcal{C}$ is primitive if $\mathcal{R}_K^{\mathfrak{c}} \subseteq \mathcal{C}$.

11.6.7. Proposition. *If $\mathcal{C}$ is a primitive congruence subgroup of modulus $\mathfrak{m}$, then $\mathfrak{m}$ is the conductor of all $\mathcal{C}' \subset \mathcal{C}$ with modulus $\mathfrak{m}$. In particular, $\mathfrak{m}$ is the conductor of $\mathcal{R}_K^{\mathfrak{m}}$.*

Proof. Suppose $\mathcal{C}' \subseteq \mathcal{C}$ with modulus $\mathfrak{m}$, and let $(\mathcal{C}_0, \mathfrak{c})$ be its conductor. Obviously $\mathfrak{c} \mid \mathfrak{m}$. On the other hand,

$$\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{c}} \subseteq \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{C}_0 = \mathcal{I}_K^{\mathfrak{c}} \cap \mathcal{C}' \subseteq \mathcal{C}' \subseteq \mathcal{C},$$

so if we let $\mathcal{C}'' = \mathcal{C}\mathcal{R}_K^{\mathfrak{c}}$, then $\mathcal{C}''$ has modulus $\mathfrak{c}$ and

$$\mathcal{I}_K^{\mathfrak{c}} \cap \mathcal{C} = \mathcal{C} = \mathcal{C}(\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{c}}) = \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{C}\mathcal{R}_K^{\mathfrak{c}} = \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{C}'',$$

so $\mathcal{C} \sim \mathcal{C}''$. Because $\mathcal{C}$ is primitive, $\mathfrak{m} \mid \mathfrak{c}$. So $\mathfrak{c} = \mathfrak{m}$. □

11.6.8. Example. Let $K = \mathbb{Q}$, $\mathfrak{m} = (2)$. Then $\mathcal{R}_{\mathbb{Q}}^{(2)} = \mathcal{I}_{\mathbb{Q}}^{(2)}$ has conductor (1), since it is equivalent to $\mathcal{I}_{\mathbb{Q}}^{(1)}$. So (2) is not the conductor of any congruence subgroup of $\mathbb{Q}$.

11.6.9. Example. Let $K = \mathbb{Q}$, $L = K[x]/(x^3 - 3x - 1)$, $G = \mathrm{Gal}(L/K) = \mathbb{Z}/3\mathbb{Z}$. This is unramified away from (3), since it has discriminant 81. So the Artin map makes sense for any modulus divisible by 3. The ray class field for (3) is $\mathbb{Q}(\zeta_3)^+ = \mathbb{Q}$, and the ray class field for $(3)\infty$ is $\mathbb{Q}(\zeta_3)$. These both have degree at most 2, so cannot contain L; equivalently, $\mathcal{R}_K^{\mathfrak{m}}$ is not contained in $\ker \psi_{L/K}^{\mathfrak{m}}$. The correct modulus to use is $\mathfrak{m} = (9)$, and indeed $L = \mathbb{Q}(\zeta_9)^+$ is the ray class field for (9).

In general, the ray class field for (n) is $\mathbb{Q}(\zeta_n)^+$, and the ray class field for $(n)\infty$ is $\mathbb{Q}(\zeta_n)$.

11.7. Ray class characters.

11.7.1. Definition. A totally multiplicative function $\chi : \mathcal{I}_K \to \mathbb{C}$ with finite image for which $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker(\chi) := \chi^{-1}(1)$ and $\mathcal{I}_K^{\mathfrak{m}} = \chi^{-1}(U_1)$ (unit circle) is a *ray class character* of $\mathfrak{m}$. Equivalently, χ is the extension by zero of a character of the finite abelian group $\mathrm{Cl}_K^{\mathfrak{m}}$.

11.7.2. Example. When $K = \mathbb{Q}$, a ray class character of modulus $(m)\infty$ is just a Dirichlet character of modulus m, and its conductor divides (m) iff the character is *even*, i.e. $\chi(-1) = 1$.

11.7.3. Definition. Suppose χ_1, χ_2 are ray class characters of moduli $\mathfrak{m}_1 \mid \mathfrak{m}_2$. If $\chi_2(I) = \chi_1(I)$ for all ideals $I \in \mathcal{I}_K^{\mathfrak{m}_2}$, then we say χ_2 is *induced* by χ_1. A ray class character is *primitive* if it is not induced by any character other than itself.

11.7.4. Definition. The *conductor* of a ray class character is the conductor of its kernel (which is a congruence subgroup).

11.7.5. Proposition. *A ray class character is primitive iff its kernel is primitive, and every ray class character is induced by a primitive one.*

Proof. Let χ be a ray class character with (some) modulus $\mathfrak{m}$. Let κ be the corresponding group character on $\mathcal{I}_K^{\mathfrak{m}}/\ker\chi$. Let $\mathcal{C}$ be the primitive congruence subgroup equivalent to $\ker\chi$, with modulus $\mathfrak{c}$, the conductor, dividing $\mathfrak{m}$. We have a canonical isomorphism $\phi : \mathcal{I}_K^{\mathfrak{c}}/\mathcal{C} \to \mathcal{I}_K^{\mathfrak{m}}/\ker\chi$. Let $\widetilde{\chi}$ be the ray class character of $\mathfrak{c}$ that is the extension by zero of $\kappa \circ \phi$. By definition of ϕ, $\widetilde{\chi}(I) = \chi(I)$ for $I \in \mathcal{I}_K^{\mathfrak{m}}$, so χ is induced by $\widetilde{\chi}$ (whose kernel is primitive).

In general, if $(\chi_2, \mathfrak{m}_2)$ is induced by $(\chi_1, \mathfrak{m}_1)$, then $\ker\chi_1 \cap \mathcal{I}_K^{\mathfrak{m}_2} = \ker\chi_2 = \ker\chi_2 \cap \mathcal{I}_K^{\mathfrak{m}_1}$, so $\ker\chi_1$, $\ker\chi_2$ are equivalent. If, furthermore, $\chi_1 \neq \chi_2$, then $\mathcal{I}_K^{\mathfrak{m}_1} \neq \mathcal{I}_K^{\mathfrak{m}_2} \implies \mathfrak{m}_1 \neq \mathfrak{m}_2$. Applying this to the above situation of χ and $\widetilde{\chi}$: if $\widetilde{\chi}$ is induced by some other character with modulus $\mathfrak{c}'$, then $\mathfrak{c}$ cannot divide $\mathfrak{c}'$, a contradiction; so $\widetilde{\chi}$ is primitive. Moreover, χ is primitive iff $\chi = \widetilde{\chi}$ iff $\ker\chi = \ker\widetilde{\chi}$ is primitive. □

For a modulus $\mathfrak{m}$, ley $X(\mathfrak{m})$ denote the set of primitive ray class characters of conductor dividing $\mathfrak{m}$, which is in bijection with the character group of $\mathrm{Cl}_K^{\mathfrak{m}}$. For a congruence subgroup $\mathcal{C}$ of modulus $\mathfrak{m}$, let $X(\mathcal{C})$ denote the set of primitive ray class characters whose kernels contain $\mathcal{C}$, and $X(\mathcal{C})$ is in bijection with the character group of $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C}$, a subgroup of $X(\mathfrak{m})$. (Why?)

11.7.6. Definition. A ray class character is *principal* if $\ker\chi = \chi^{-1}(U_1)$. We use $\mathbf{1}$ to denote the unique primitive principal ray class group. (It is not the unique primitive character of conductor (1); when Cl_K is nontrivial, any character on Cl_K induces a primitive character of conductor (1), but only one is principal.)

11.8. Weber L-functions.

11.8.1. Definition (Weber L-function)**.** The *Weber L-function* $L(s, \chi)$ of ray class character χ is

$$L(s,\chi) = \prod_{\mathfrak{p}\in K} \frac{1}{1 - \chi(\mathfrak{p})\,\mathrm{N}(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a}} \chi(\mathfrak{a})\,\mathrm{N}(\mathfrak{a})^{-s},$$

which converges absolutely to a nonvanishing holomorphic function for $\mathrm{Re}(s) > 1$.

This generalizes Dirichlet L-functions ($K = \mathbb{Q}$) and Dedekind zeta functions ($\chi = \mathbf{1}$), both of which generalize the Riemann zeta function.

11.8.2. Proposition. *Let χ be a ray class character for a global field K. Then $L(s, \chi)$ extends to a meromorphic function on a neighborhood of $s = 1$, with a simple pole at $s = 1$ if $\chi = \mathbf{1}$ and holomorphic otherwise.*

Proof. Wait for Tate's thesis. □

11.8.3. Proposition. *Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for K. Let $n = [\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$, then $S = \{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density*

$$d(S) = \begin{cases} 1/n, & \textit{if } L(1,\chi) \neq 0 \textit{ for all } \chi \neq \mathbf{1} \textit{ in } X(\mathcal{C}); \\ 0, & \textit{otherwise.} \end{cases}$$

(Actually the second case never happens, but that will be shown later.)

Proof. By character theory,

$$\frac{1}{n}\sum_{\chi\in X(\mathcal{C})}\chi(\mathfrak{p})=\begin{cases}1, & \text{if } \mathfrak{p}\in\mathcal{C};\\ 0, & \text{otherwise.}\end{cases}$$

Because as $s\to 1^+$,

$$\log L(s,\chi)\sim\sum_{\mathfrak{p}}\chi(\mathfrak{p})\,\mathrm{N}(\mathfrak{p})^{-s},$$

we have

$$\begin{aligned}\sum_{\chi\in X(\mathcal{C})}\log L(s,\chi)&\sim\sum_{\chi\in X(\mathcal{C})}\sum_{\mathfrak{p}}\chi(\mathfrak{p})\,\mathrm{N}(\mathfrak{p})^{-s}\\ &=\sum_{\mathfrak{p}}\mathrm{N}(\mathfrak{p})^{-s}\sum_{\chi\in X(\mathcal{C})}\chi(\mathfrak{p})\\ &=n\sum_{\mathfrak{p}\in\mathcal{C}}\mathrm{N}(\mathfrak{p})^{-s}.\end{aligned}$$

By the above proposition, near $s=1$, $L(s,\chi)=(s-1)^{e(\chi)}g(s)$ where g is holomorphic and nonvanishing, and $e(\chi)=-1$ if $\chi=\mathbf{1}$ and $e(\chi)\geq 0$ otherwise. So

$$n\sum_{\mathfrak{p}\in\mathcal{C}}\mathrm{N}(\mathfrak{p})^{-s}\sim\log\frac{1}{s-1}-\sum_{\chi\neq\mathbf{1}}e(\chi)\log\frac{1}{s-1}$$

as $s\to 1^+$. This is equivalent to saying as $s\to 1^+$,

$$0\leq d(S)=\frac{\sum_{p\in\mathcal{C}}\mathrm{N}(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}}=\frac{1-\sum_{\chi\neq\mathbf{1}}e(\chi)}{n},$$

which is either 0 or $1/n$ depending on whether one of the $e(\chi)=1$. □

11.8.4. Proposition. *Let $\mathcal{C}$ be a congruent subgroup of modulus $\mathfrak{m}$, $n=[\mathcal{I}_K^{\mathfrak{m}}:\mathcal{C}]$. Then for any $I\in\mathcal{I}_K^{\mathfrak{m}}$, the coset $\{\mathfrak{p}\in I\mathcal{C}\}$ has Dirichlet density the same as the trivial coset.*

Proof. Same proof, just change the indicator function. □

11.8.5. Corollary. *The coset $\{p\in I\mathcal{C}\}$ has Dirichlet density $1/n$ (so the second possibility never occurs), and every non-primitive $\chi\in X(\mathcal{C})$ is nonvanishing at $s=1$.*

Proof. Summing over all cosets, the Dirichlet densities should add up to 1. □

11.8.6. Corollary. *Let L/K be a finite abelian extension, $\mathcal{C}$ a congruence subgroup of modulus $\mathfrak{m}$. If* $\mathrm{Spl}(L/K)\lesssim\{\mathfrak{p}\in\mathcal{C}\}$, *then $[I_K^{\mathfrak{m}}:\mathcal{C}]\leq[L:K]$.*

Proof. We know $\mathrm{Spl}(L/K)$ has polar density (hence also Dirichlet density) $1/[L:K]$, and $\{p\in\mathcal{C}\}$ has Dirichlet density $1/[I_K^{\mathfrak{m}}:\mathcal{C}]$. □

11.9. Second main inequality of CFT.

11.9.1. Definition. Let L/K be a finite abelian extension of *local* fields, then the *conductor*

$$\mathfrak{c}(L/K):=\begin{cases}1, & \text{if } L=\mathbb{C}, K=\mathbb{R}\\ 0, & \text{if } L=K \text{ archimedean}\\ \min\{n:1+\mathfrak{p}^n\subseteq\mathrm{N}_{L/K}(L^\times)\}, & \text{otherwise.}\end{cases}$$

For a finite abelian extension of *global* fields, $\mathfrak{c}(L/K)$ is a map from M_K (the set of places of K) to $\mathbb{Z}$, given by mapping $v\mapsto\mathfrak{c}(L_w/K_v)$, where w is any place above v. (Since L/K is Galois, this does not depend on the choice of w.)

11.9.2. Proposition. *Let L/K be a finite abelian extension of local or global fields. For each prime $\mathfrak{p}$ of K,*

$$v_{\mathfrak{p}}(L/K)=\begin{cases}0 & \textit{if } \mathfrak{p} \textit{ is unramified}\\ 1 & \textit{if } \mathfrak{p} \textit{ is tamely ramified}\\ \geq 2 & \textit{if } \mathfrak{p} \textit{ is wildly ramified.}\end{cases}$$

Proof. See 18.786 pset 2. □

11.9.3. Remark. The conductor and the discriminant are supported on the same primes (but the valuations can be very different).

11.9.4. Lemma. *Let L_1, L_2 be finite abelian extensions of local or global fields. Suppose $L_1 \subseteq L_2 \implies \mathfrak{c}(L_1/K) \mid \mathfrak{c}(L_2/K)$.*

Proof. In the local nonarchimedean case, $\mathrm{N}_{L_2/K}(L_2^\times) = \mathrm{N}_{L_1/K}(\mathrm{N}_{L_2/L_1}(L_2^\times)) \subseteq \mathrm{N}_{L_1/K}(L_1^\times)$. In the local archimedean case this is obvious. So this also holds for global fields. □

11.9.5. Definition. Let L/K be a finite abelian extension of global fields, $\mathfrak{m}$ a modulus divisible by $\mathfrak{c}(L/K)$. The *norm group* (also *Takagi group*) for $\mathfrak{m}$ is

$$T^{\mathfrak{m}}_{L/K} = \mathcal{R}^{\mathfrak{m}}_K \, \mathrm{N}_{L/K}(\mathcal{I}^{\mathfrak{m}}_L),$$

where $\mathcal{I}^{\mathfrak{m}}_L$ are the fractional $\mathcal{O}_L$-ideals coprime to $\mathfrak{m}_0\mathcal{O}_L$.

11.9.6. Proposition. *Let L/K be a finite abelian extension of global fields, $\mathfrak{m}$ a modulus divisible by $\mathfrak{c}(L/K)$, then $\mathrm{Spl}(L/K) \lesssim \{\mathfrak{p} \in T^{\mathfrak{m}}_{L/K}\}$.*

Proof. Suppose $\mathfrak{p}$ is coprime to $\mathfrak{m}$, and splits completely in L, so $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$. Pick $\mathfrak{q} \mid \mathfrak{p}$, then $\mathfrak{q} \in \mathcal{I}^{\mathfrak{m}}_K$ and $\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}$, so $\mathfrak{p}$ is in $T^{\mathfrak{m}}_{L/K}$. □

11.9.7. Theorem (second main inequality)**.** *Let L/K be a finite abelian extension of global fields, $\mathfrak{m}$ a modulus divisible by $\mathfrak{c}(L/K)$. Then*

$$[\mathcal{I}^{\mathfrak{m}}_K : T^{\mathfrak{m}}_{L/K}] \le [L : K].$$

Proof. Follows from corollary 11.8.6. □

The goal now is to show that this is actually an equality.

12. Global class field theory: Setup

12.1. Global CFT via ideals. What we are working towards is the following:

12.1.1. Theorem (global CFT, via ideals)**.** *The main theorems of ideal-theoretic CFT:*

- *The ray class field $K(\mathfrak{m})$ exists;*
- *For L/K finite abelian extension, $L \subseteq K(\mathfrak{m})$ iff $\mathfrak{c}(L/K) \mid \mathfrak{m}$.*
- *Artin reciprocity: If $L \subseteq K(\mathfrak{m})$, then $\ker \psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$, its conductor is $\mathfrak{c}(L/K) \mid \mathfrak{m}$, and $\mathcal{I}^{\mathfrak{m}}_K / T^{\mathfrak{m}}_{L/K} \cong \mathrm{Gal}(L/K)$ canonically.*

Artin reciprocity gives the following commutative diagram of canonical bijections:

$$\begin{tikzcd}
\{\text{finite abelian } L/K \text{ with } \mathfrak{c}(L/K) \mid \mathfrak{m}\} \arrow[r, "L \mapsto T^{\mathfrak{m}}_{L/K}"] \arrow[d, "L \mapsto \mathrm{Gal}(L/K)"'] & \{\text{congruence subgroups of modulus } \mathfrak{m}\} \arrow[d, "\mathcal{C} \mapsto I^{\mathfrak{m}}_K/\mathcal{C}"] \\
\{\text{quotients of } \mathrm{Gal}(K(\mathfrak{m})/K)\} & \{\text{quotients of } \mathrm{Cl}^{\mathfrak{m}}_K\} \arrow[l, "\psi^{\mathfrak{m}}_{L/K}"]
\end{tikzcd}$$

12.1.2. Definition. The *Hilbert class field* of a global field K is the maximal unramified abelian extension of K (in some fixed algebraic closure).

From class field theory, taking the trivial modulus, we see in particular that this is a finite extension, which is already not obvious.

12.2. Simple pole of ζ_K at $s = 1$. In this subsection we digress to show that $\zeta_K(s)$ can be meromorphically continued to have a simple pole at $s = 1$. We use the following fact without proof:

12.2.1. Proposition. *Let $a_1, a_2, \dots \in \mathbb{C}$ be a sequence of complex numbers, ρ a nonzero real, and $\sigma \in [0, 1)$, such that $\sum_{k=1}^{t} a_k = \rho t + O(t^\sigma)$, then $\sum a_n n^{-s}$ has a meromorphic continuation to $\operatorname{Re}(s) > \sigma$ with a simple pole at $s = 1$ with residue ρ.* □

So to show analytic continuation of $\zeta_K(s)$, it suffices to show that $\#(\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \le t) = \rho t + O(t^\sigma)$ for $\sigma \in [0, 1)$. The strategy is to first count the principal ideals, then count the ideals by partitioning into ideal classes: note that if we fix ideal class representatives $\mathfrak{a} \in \mathcal{I}_K$. Then

$$\begin{aligned}\{\text{integral ideals } \mathfrak{b} \in [\mathfrak{a}^{-1}] : \mathrm{N}(\mathfrak{b}) \le t\} &\xrightarrow{\cong} \{\text{nonzero principal integral } (\alpha) \subseteq \mathfrak{a} : \mathrm{N}(\alpha) \le t\,\mathrm{N}(\mathfrak{a})\} \\ &\xrightarrow{\cong} \{\text{nonzero integral } \alpha \in \mathfrak{a} : \mathrm{N}(\alpha) \le t\,\mathrm{N}(\mathfrak{a})\}/\mathcal{O}_K^\times.\end{aligned}$$

by multiplying by $\mathfrak{a}$.

Recall that for a number field K, $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R} = \prod_{v|\infty} K_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. We have an injection $K^\times \hookrightarrow K_\mathbb{R}^\times$ by embedding diagonally, and a map

$$\mathrm{Log} : K_\mathbb{R}^\times \to \mathbb{R}^{r_1 + r_2}$$

sending $(x_v) \mapsto \log \|x_v\|_v$, where $\|\|_v$ is the usual norm in $\mathbb{R}$ and the square of the absolute value in $\mathbb{C}$. By Dirichlet's unit theorem, $\mathcal{O}_K^\times = \mu_K \times U$, where Log maps $\mathcal{O}_K^\times$ into a full lattice Λ_K in $\mathbb{R}_0^{r_1+r_2}$, with kernel μ_K.

Define $\nu : K_\mathbb{R}^\times \to K_{\mathbb{R},1}^\times$ by $x\,\mathrm{N}(x)^{-1/n}$, where $n = r_1 + 2r_2$. Then $\mathrm{Log}(\nu(K_\mathbb{R}^\times)) = \mathbb{R}_0^{r_1+r_2}$. Let us fix a fundamental domain F for the lattice Λ_K (whose covolume is R_K, the *regulator*), and let $S := \nu^{-1}(\mathrm{Log}^{-1}(F))$. Then S is a set of coset representatives for $K_\mathbb{R}^\times / U$. Let $S_{\le t} = \{x \in S : \mathrm{N}(x) \le t\} \subseteq K_\mathbb{R} \cong \mathbb{R}^n$. It then suffices to estimate $\#(S_{\le t} \cap \mathcal{O}_K)$: the method only uses the fact that $\mathcal{O}_K$ is a lattice, so the same method will work for counting $\#(S_{\le t} \cap \mathfrak{a})$.

Since $t^{1/n} S_{\le 1} = S_{\le t}$ (where we work in $\mathbb{R}^n$), what we want is:

12.2.2. Proposition. *Let Λ be a lattice in $V \cong \mathbb{R}^n$, let S be a "nice" (Lebesgue) measurable set, then $\#(tS \cap \Lambda) = \frac{\mu(S)}{\mathrm{covol}(\Lambda)} t^n + O(t^{n-1})$.*

This would imply that $\#(S_{\le t} \cap \mathcal{O}_K) = \rho t + O(t^{1-\frac{1}{n}})$, which is the bound we want. We now need to say what it means to be "nice".

12.2.3. Definition. Let X, Y be metric spaces. A map $f : X \to Y$ is *Lipschitz continuous* if there exists $c > 0$, such that $d(f(u), f(v)) \le c d(u, v)$ for all $u, v \in X$.

This is a stronger condition than uniform continuity.

12.2.4. Definition. A set B in a metric space X is *d-Lipschitz parametrizable* if it is the union of finitely many images for Lipschitz-continuous functions $f : [0, 1]^d \to X$.

12.2.5. Lemma. *Let $S \subseteq \mathbb{R}^n$ be measurable with boundary $(n-1)$-Lipschitz parametrizable. Then $\#(tS \cap \mathbb{Z}^n) = \mu(S) t^n + O(t^{n-1})$.* □

So what we need to show is that $\partial S_{\le 1}$ is $(n-1)$-Lipschitz parametrizable. The kernel of Log is $(\pm 1)^{r_1} \times U(1)^{r_2}$. We thus have a continuous isomorphism of locally compact groups

$$K_\mathbb{R}^\times \to \mathbb{R}^{r_1 + r_2} \times \{\pm 1\}^{r_1} \times [0, 2\pi)^{r_2}$$

mapping $(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \mapsto (\mathrm{Log}\, x) \times (\mathrm{sgn}\, x_1, \dots, \mathrm{sgn}\, x_{r_1}) \times (\arg z_1, \dots, \arg z_{r_2})$.

Analyzing $S_{\le 1}$, it has 2^{r_1} connected components, each parametrized by n parameters:

- $r_1 + r_2 - 1$ parameters in $[0, 1)$ encoding a point in F as an $\mathbb{R}$-linear combination of Log applied to a basis of U;
- r_2 parameters in $[0, 1)$ encoding an element of $U(1)$;
- one parameter in $(0, 1]$ encoding the n-th root of the norm.

This gives a continuously differentiable bijection from $[0, 1)^{n-1} \times (0, 1]$ to a connected component of $S_{\le 1}$. So its boundary is clearly $(n-1)$-Lipschitz parametrizable, proving the theorem.

12.2.6. Remark. If we keep track of the coefficient of the linear term, we actually get the analytic class number formula.

12.3. Group cohomology.

12.3.1. Definition. Let G be *any* group, a *left G-module* is an abelian group A with a compatible G-action: $g(a+b) = ga + gb$. Equivalently, A is a left $\mathbb{Z}[G]$-module. A *morphism* of G-modules is a morphism of $\mathbb{Z}[G]$-modules. The category of G-modules is denoted Mod_G. Since it is just the category of modules over a ring $\mathbb{Z}[G]$, it is an abelian category.

12.3.2. Remark. When G is a topological group, we need to require the G-action to be continuous.

12.3.3. Example. Examples of G-modules:

- If A is any abelian group, A can be made into a *trivial G-module*, i.e. G acts trivially.
- For L/K Galois extension, the abelian groups $L, L^\times, \mathcal{O}_L, \mathcal{O}_L^\times$ are all $\mathrm{Gal}(L/K)$-modules.
- For $A, B \in \mathrm{Mod}_G$, the abelian group $\mathrm{Hom}_{\mathrm{Ab}}(A, B)$ has a natural G-module structure: $(g\phi)(a) = g\phi(g^{-1}a)$.

12.3.4. Definition. For $A \in \mathrm{Mod}_G$, the subgroup $A^G = \{a \in A : ga = a \text{ for all } g \in G\}$ is the subgroup of *G-invariants*.

12.3.5. Example. $\mathrm{Hom}_G(A, B) \cong \mathrm{Hom}_{\mathrm{Ab}}(A, B)^G$. In particular, $\mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G$.

Any morphism of G-modules $A \to B$ restricts to a morphism $A^G \to B^G$. We thus have a functor $\bullet^G : \mathrm{Mod}_G \to \mathrm{Mod}_G$ (in fact the subcategory of trivial G-modules, which is just Ab), which is left exact because it is $\mathrm{Hom}_G(\mathbb{Z}, \bullet)$. (Recall that this is exact iff $\mathbb{Z}$ is a projective $\mathbb{Z}[G]$-module, which is not true when G is nontrivial.)

The category Mod_G is in fact a Grothendieck category (in particular, has enough injectives). So we can define $H^n(G, A)$ to be the n-th right derived functors of the left exact $\bullet^G : \mathrm{Mod}_G \to \mathrm{Ab}$. In particular $H^0(G, A) = A^G$.

Now, we give another definition of group cohomology using cochains.

12.3.6. Definition. Let A be a left G-module, $n \geq 0$. The group $C^n(G, A)$ of *n-cochains* is the abelian group of maps of sets $f : G^n \to A$, under pointwise addition. The n-th *coboundary map* is a homomorphism $d^n : C^n(G, A) \to C^{n+1}(G, A)$ given by

$$d^n f(g_0, \dots, g_n) := g_0 f(g_1, \dots, g_n) + \sum_{i=1}^{n} (-1)^i f(\dots, g_{i-2}, g_{i-1}g_i, g_{i+1}, \dots) + (-1)^{n+1} f(g_0, \dots, g_{n-1}).$$

Define the n-cocycles and n-coboundaries $Z^n(G, A) = \ker d^n$ and $B^n(G, A) = \operatorname{im} d^{n-1}$. Since $d^{n+1}d^n = 0$, $B^n(G, A) \subseteq Z^n(G, A)$. In other words, we get a cochain complex

$$0 \to C^0(G, A) \to C^1(G, A) \to C^2(G, A) \to \dots,$$

and the *n-th cohomology group of G with coefficients in A* is

$$H^n(G, A) = \frac{Z^n(G, A)}{B^n(G, A)}.$$

12.3.7. Example. Low-degree cohomologies:

- $C^0(G, A) \cong A$;
- $d^0 : C^0(G, A) \to C^1(G, A)$ sends $a \mapsto (g \mapsto ga - a)$;
- $H^0(G, A) = \ker d^0 = A^G$;
- $B^1(G, A)$ is the group of *principal crossed homomorphisms*;
- $d^1 : C^1(G, A) \to C^2(G, A)$ sends $f \mapsto ((g, h) \mapsto gf(h) - f(gh) + f(g))$.
- $Z^1(G, A) = \ker d^1$ consists of $f : G \to A$ such that $f(gh) = f(g) + gf(h)$. This is the group of *crossed homomorphisms.*
- $H^1(G, A) = Z^1(G, A)/B^1(G, A)$ are the crossed homomorphisms modulo the principal ones.
- If $A = A^G$, then $H^1(G, A) = \mathrm{Hom}_{\mathrm{Grp}}(G, A) = \mathrm{Hom}_{\mathrm{Ab}}(G^{\mathrm{ab}}, A)$.

We give a useful interpretation of $H^2(G, A)$.

12.3.8. Definition. Let $A \in \mathrm{Mod}_G$, a group extension E of G by A is a short exact sequence of groups:

$$0 \to A \to E \to G \to 0,$$

such that for any set-theoretic subsection $s : G \to E$, we have $s(g)as(g)^{-1} = ga$.

In other words, A has a G-action because it is a G-module, and $G \cong E/A$ also acts on A by conjugation, and we require these two actions to be the same.

Two extensions E, E' are *isomorphic* if there is an isomorphism $\theta : E \to E'$ such that

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\theta"] & G \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r] & E' \arrow[r] & G \arrow[r] & 0
\end{tikzcd}$$

commutes.

12.3.9. Proposition. *$H^2(G, A)$ is canonically the abelian group of isomorphism classes of extensions of G by A, which sends $f : G^2 \to A$ to $E_f = A \times G$ (as a set) with the group law*

$$(a, g) \cdot (b, h) = (a + gb + f(g, h), gh).$$

By definition, the image of $0 \in H^2(G, A)$ is $A \rtimes G$.

12.3.10. Lemma. *Given a map of G-modules $\alpha : A \to B$, there is an induced map of cochain complexes $C^\bullet(G, A) \to C^\bullet(G, B)$ (which in turn induces maps $\alpha^n : H^n(G, A) \to H^n(G, B)$).*

Proof. It suffices to show that $\alpha^n : C^n(G, A) \to C^n(G, B)$ commutes with d^n. For $f \in C^n(G, A)$,

$$\begin{aligned}
\alpha^{n+1} d^n f(g_0, \dots, g_n) &= \alpha(g_0 f(g_1, \dots, g_n) + \sum_{i=1}^{n} (-1)^n f(\dots, g_{i-1}g_i, \dots) + f(g_0, \dots, g_{n-1})) \\
&= g_0 \alpha f(g_0, \dots, g_n) + \sum_{i=1}^{n} (-1)^n \alpha f(\dots, g_{i-1}g_i, \dots) + \alpha f(g_0, \dots, g_{n-1}) \\
&= d^n \alpha^n f(g_0, \dots, g_n).
\end{aligned}$$

That a map of cochain complexes induces a map of cohomologies is clear. □

12.3.11. Lemma. *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a exact sequence of G-modules, then $0 \to C^i(G, A) \to C^i(G, B) \to C^i(G, C) \to 0$ is exact for all $i \geq 0$, hence an exact sequence $0 \to C^\bullet(G, A) \to C^\bullet(G, B) \to C^\bullet(G, C) \to 0$.* □

12.3.12. Theorem. *Every short exact sequence $0 \to A \to B \to C \to 0$ induces a long exact sequence*

$$\begin{aligned}
0 &\to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \\
&\to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \\
&\to H^2(G, A) \to \dots
\end{aligned}$$

and this is functorial.

Proof. Apply the snake lemma to

$$\begin{tikzcd}
 & \operatorname{coker} d_A^{n-1} \arrow[r] \arrow[d, "d_A^n"] & \operatorname{coker} d_B^{n-1} \arrow[r] \arrow[d, "d_B^n"] & \operatorname{coker} d_C^{n-1} \arrow[r] \arrow[d, "d_C^n"] & 0 \\
0 \arrow[r] & \ker d_A^{n+1} \arrow[r] & \ker d_B^{n+1} \arrow[r] & \ker d_C^{n+1} &
\end{tikzcd}$$

where the resulting connecting homomorphism $\delta : H^i(G, C) \to H^{i+1}(G, A)$ is explicitly given by sending $[f]$ to $[\alpha^{-1} \circ d_B^n(\overline{f})]$, where we lift f along β to $\overline{f} \in H^i(G, B)$. □

12.3.13. Definition (cohomological δ-functors)**.** Let $\mathscr{C}$ be abelian, $\mathscr{C}'$ additive. A (covariant) cohomological δ-functor $\mathscr{C} \to \mathscr{C}'$ is:

- a system of additive functors $T^i : \mathscr{C} \to \mathscr{C}'$ $(i \geq 0)$, and
- connecting morphisms $\delta : T^i(A'') \to T^{i+1}(A')$, for every $i \geq 0$ and each short exact $0 \to A' \to A \to A'' \to 0$ in $\mathscr{C}$,

satisfying:

- Given a map of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & A' \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B' \arrow[r] & B \arrow[r] & B'' \arrow[r] & 0,
\end{tikzcd}$$

the diagram

$$\begin{tikzcd}
T^i(A'') \arrow[r, "\delta"] \arrow[d] & T^{i+1}(A') \arrow[d] \\
T^i(B'') \arrow[r, "\delta"] & T^{i+1}(B')
\end{tikzcd}$$

commutes;
- Given an exact sequence $0 \to A' \to A \to A'' \to 0$, the sequence

$$0 \to T^0(A') \to T^0(A) \to T^0(A'') \xrightarrow{\delta} T^1(A') \to \dots$$

is a chain complex.

When $\mathscr{C}'$ is abelian as well, the δ-functor is called *exact* if the above chain complex is exact.

In this context, $H^i(G, \bullet)$ is the unique universal exact cohomological δ-functor extending $\bullet^G$. We will give yet another equivalent definition of group cohomology.

12.3.14. Definition. The *standard resolution* of $\mathbb{Z}$ by G-modules is

$$\dots \to \mathbb{Z}[G^{n+1}] \xrightarrow{d_n} \mathbb{Z}[G^n] \xrightarrow{d_{n-1}} \dots \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \to 0,$$

where $\mathbb{Z}[G^n]$ is the free $\mathbb{Z}$-algebra generated by the direct product G^n, with left diagonal action $g \cdot (g_1, \dots, g_n) = (gg_1, \dots, gg_n)$, and

$$d_n(g_0, \dots, g_n) := \sum_{i=0}^{n} (-1)^i (g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n).$$

Note that $d_0 : \mathbb{Z}[G] \to \mathbb{Z}$ is the augmentation map $\sum n_g g \mapsto \sum n_g \in \mathbb{Z}$.

12.3.15. Lemma. *The standard resolution is exact, so that it is a free resolution of $\mathbb{Z}$ as a (trivial) $\mathbb{Z}[G]$-module.*

12.3.16. Definition (Ext groups)**.** Let A, B be R-modules. Take $P_\bullet \to B$ to be a projective resolution of B. Applying the contravariant left exact functor $\operatorname{Hom}_R(\bullet, A)$ to $P_\bullet \to 0$ and deleting the $\operatorname{Hom}(B, A)$-term, we get a cochain complex

$$0 \to \operatorname{Hom}(P_0, A) \to \operatorname{Hom}(P_1, A) \to \dots,$$

then $\operatorname{Ext}^n_R(B, A)$ is defined as its n-th cohomology.

12.3.17. Lemma. *The groups $\operatorname{Ext}^n_R(B, A)$ do not depend on the projective resolution.*

Applying this for $B = \mathbb{Z}$, $R = \mathbb{Z}[G]$, we can use the standard resolution to compute $\operatorname{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, as the n-th cohomology of

$$0 \to \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{d_1^*} \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], A) \xrightarrow{d_2^*} \dots.$$

12.3.18. Proposition. *We have isomorphisms of abelian groups ($n \geq 0$):*

$$\Phi^n : \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{n+1}], A) \to C^n(G, A)$$

by

$$\phi \mapsto [(g_1, \dots, g_n) \mapsto \phi(1, g_1, g_1 g_2, \dots, g_1 g_2 \cdots g_n)].$$

Furthermore, this commutes with the coboundary maps, so that it defines a chain isomorphism.

Proof. Φ^n is clearly a homomorphism.

Injectivity: let $\phi \in \ker \Phi^n$. For any $g_0, \dots, g_n \in G$, define $h_i = g_{i-1}^{-1} g_i$. Then

$$\phi(g_0, \dots, g_n) = g_0 \phi(1, h_1, h_1 h_2, \dots, h_1 h_2 \cdots h_n) = 0,$$

so $\phi = 0$.

Surjectivity: for $f \in C^n(G, A)$, define $\phi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{n+1}], A)$ by

$$(g_0, \dots, g_n) \mapsto g_0 f(g_0^{-1} g_1, \dots, g_{n-1}^{-1} g_n).$$

This gets sent to f by Φ^n.

Finally, we show that Φ^n commutes with coboundary maps, i.e. $\Phi^{n+1} d_{n+1}^* = d^n \Phi^n$. We compute:

$$\begin{aligned}
\Phi^{n+1}(d_{n+1}^*(\phi))(g_1, \dots, g_{n+1}) &= d_{n+1}^*(\phi)(1, g_1, \dots, g_1 \cdots g_{n+1}) \\
&= \phi(d_{n+1}(1, g_1, \dots, g_1 \cdots g_{n+1})) \\
&= \phi(g_1, \dots, g_1 \cdots g_{n+1}) - \sum_{i=1}^{n} (-1)^i \phi(\dots, g_1 \cdots g_{i-1}, g_1 \cdots g_{i+1}, \dots) \\
&\quad + (-1)^{n+1} \phi(1, g_1, \dots, g_1 \cdots g_n) \\
&= g_1 \Phi^n(\phi)(g_2, \dots, g_{n+1}) - \sum_{i=1}^{n} (-1)^i \Phi^n(\phi)(\dots, g_{i-1}, g_i g_{i+1}, \dots) \\
&\quad + (-1)^{n+1} \Phi^n(\phi)(g_1, \dots, g_n) \\
&= d^n \Phi^n(\phi)(g_1, \dots, g_{n+1}),
\end{aligned}$$

as desired. □

12.3.19. Corollary. $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

We remark that Ext^n are also the right derived functors of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \bullet) = \bullet^G$, and right derived functors of any left-exact functor F is the unique universal exact cohomological δ-functor extending F. This shows the equivalence of the four definitions of group cohomology we gave:

- via injective resolutions, i.e. as right derived functors of $\bullet^G$;
- as the unique universal exact cohomological δ-functor extending $\bullet^G$;
- via cochains;
- via the standard resolution.

12.3.20. Corollary. $H^n(G, A \oplus B) = H^n(G, A) \oplus H^n(G, B)$.

Proof. This is because in general,

$$\mathrm{Ext}^i_R(\bigoplus M_\alpha, N) = \prod \mathrm{Ext}^i_R(M_\alpha, N) \quad \text{and} \quad \mathrm{Ext}^i_R(M, \prod N_\alpha) = \bigoplus \mathrm{Ext}^i_R(M, N_\alpha)$$

for any R-modules M and N. □

12.3.21. Definition. Let $H \leq G$ be a subgroup, A and H-module. The *induced* G-module

$$\mathrm{Ind}_H^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A,$$

and the *coinduced* G-module

$$\mathrm{CoInd}_H^G(A) := \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A).$$

12.3.22. Theorem. *If H has finite index in G, then* $\mathrm{Ind}_H^G(A) \cong \mathrm{CoInd}_H^G(A)$.

When $H = \{1\}$ we just write Ind^G and CoInd^G.

12.3.23. Lemma. *Group cohomology of coinduced modules from the trivial group:*

$$H^n(G, \mathrm{CoInd}^G(A)) = \begin{cases} A, & \textit{if } n = 0; \\ 0, & \textit{otherwise.} \end{cases}$$

PROOF. For $n \geq 1$ we have isomorphisms of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^n], \mathrm{CoInd}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G^n], A),$$

given by

$$\phi \mapsto [z \mapsto \phi(z)(1)]$$
$$[z \mapsto [y \mapsto \phi(yz)]] \leftarrow\!\shortmid \phi.$$

so $H^n(G, \mathrm{CoInd}^G(A)) = H^n(\{1\}, A)$ for $n \geq 0$. Just use the stupid resolution $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$. □

12.4. Group homology. A minor point concerning tensor products over noncommutative rings: for $M \otimes_R N$, it only makes sense when M is a right R-module and N is a left R-module, and the resulting $M \otimes_R N$ is a priori only an abelian group. So, in the definition of $\mathrm{Ind}_H^G(A)$, we really think of $\mathbb{Z}[G]$ as a *right* $\mathbb{Z}[H]$-module, and then "manually" define the extra structure of $\mathrm{Ind}_H^G(A)$ as a $\mathbb{Z}[G]$-module, by $g(\alpha \otimes a) = (g\alpha) \otimes a$. Similarly, the $\mathbb{Z}[G]$-module structure on $\mathrm{CoInd}_H^G(A)$ is given by $(g\phi)(\alpha) = \phi(\alpha g)$.

12.4.1. Lemma. *When G is finite, there is a canonical isomorphism* $\mathrm{CoInd}^G(A) \cong \mathrm{Ind}^G(A)$ *given by*

$$\phi \mapsto \sum_{g \in G} g^{-1} \otimes \phi(g)$$
$$(g^{-1} \mapsto a) \leftarrow\!\shortmid g \otimes a.$$

where $(g^{-1} \mapsto \alpha)$ maps g' to 0 for $g' \neq g^{-1}$.

12.4.2. Definition (group homology)**.** The n-th group homology with coefficients in A is

$$H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A) = L_n(\mathbb{Z} \otimes_{\mathbb{Z}[G]} \bullet)(A) = L_n(\bullet \otimes_{\mathbb{Z}[G]} A)(\mathbb{Z}).$$

In practice, we use the last expression, with the standard resolution of $\mathbb{Z}$ by right $\mathbb{Z}[G]$-modules (the same as the standard resolution by left $\mathbb{Z}[G]$-modules, except G acts diagonally on the right). This is the (unique) universal exact homological δ-functor extending $\bullet \otimes_{\mathbb{Z}[G]} A$.

12.4.3. Lemma. *$H_n(G, A \oplus B) \cong H_n(G, A) \oplus H_n(G, B)$.*

PROOF. This is just because Tor commutes with arbitrary direct sums and filtered colimits in each variable. □

12.4.4. Definition (coinvariants)**.** Let A be a left G-module. The *G-coinvariants A_G* of A is the G-module $A/I_G A$, where I_G is the *augmentation ideal*

$$I_G = \ker(\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}) = \mathbb{Z}[g - 1 : g \in G].$$

In other words, A_G is the largest quotient of A which is a trivial G-module. Observe that naturally $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong A_G$, so that $H_0(G, A) = A_G$ (just like $H^0(G, A) = A^G$).

Similar to group cohomology, we have:

12.4.5. Lemma. *Group homology of induced modules from the trivial group:*

$$H_n(G, \mathrm{Ind}^G(A)) = \begin{cases} A, & \text{if } n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

12.5. Tate cohomology.

12.5.1. Lemma. *Let G be finite, and let $N_G = \sum_{g \in G} g$ be the* norm element*. Let $N_G : A \to A$ be the multiplication-by-N_G map. Then $I_G A \subseteq \ker N_G$ and $\mathrm{im}\, N_G \subseteq A^G$. Consequently, we get an induced map $\hat{N}_G : A_G \to A^G$.* □

12.5.2. Definition (Tate (co)homology)**.** Define $\hat{H}^n(G, A) = H^n(G, A)$ for $n > 0$, and $\hat{H}^0(G, A) = \operatorname{coker} \hat{N}_G$. Define $\hat{H}_n(G, A) = H_n(G, A)$ for $n > 0$, and $\hat{H}_0(G, A) = \ker \hat{N}_G$. Define $\hat{H}^{-n}(G, A) = \hat{H}_{n-1}(G, A)$ and $\hat{H}_{-n}(G, A) = \hat{H}^{n-1}(G, A)$ for $n > 0$.

Then, it is easy to check that a morphism of G-modules induces natural morphisms of Tate (co)homology groups in all degrees. The key theorem is the following:

12.5.3. Theorem. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then we get a long exact sequence of abelian groups*

$$\begin{aligned} \ldots \to \hat{H}_1(G,A) &\to \hat{H}_1(G,B) \to \hat{H}_1(G,C) \\ &\to \hat{H}_0(G,A) \to \hat{H}_0(G,B) \to \hat{H}_0(G,C) \\ &\to \hat{H}^0(G,A) \to \hat{H}^0(G,B) \to \hat{H}^0(G,C) \\ &\to \hat{H}^1(G,A) \to \hat{H}^1(G,B) \to \hat{H}^1(G,C) \to \ldots \end{aligned}$$

Furthermore, this is functorial.

Proof. Apply the snake lemma to the commutative diagram

$$\begin{tikzcd}
H_1(G,C) \arrow[r] & A_G \arrow[r] \arrow[d, "\hat{H}_G"] & B_G \arrow[r] \arrow[d, "\hat{H}_G"] & C_G \arrow[r] \arrow[d, "\hat{H}_G"] & 0 \\
0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & H^1(G,A).
\end{tikzcd}$$

Furthermore, by diagram chasing, the image of $H_1(G,C)$ lies in $\hat{H}_0(G,A)$, and $C^G \to H^1(G,A)$ factors through $\hat{H}^0(G,A)$. Finally, it is not hard to verify exactness at these two terms, and to check that a commutative diagram of short exact sequences induces a commutative diagram of long exact sequences. □

12.5.4. Lemma. *$\hat{H}^n(G, A \oplus B) \cong \hat{H}^n(G,A) \oplus \hat{H}^n(G,B)$, and $\hat{H}_n(G, A \oplus B) \cong \hat{H}_n(G,A) \oplus \hat{H}_n(G,B)$.*

12.5.5. Theorem. *Let G be finite, and $B = \mathrm{Ind}^G(A) \cong \mathrm{CoInd}^G(A)$. Then the Tate (co)homology groups of G with coefficients in B all vanish.*

Proof. It suffices to show that for $B = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$, $\ker(N_G : B \to B) = I_G B$ and $\mathrm{im}(N_G) = B^G$. Since G acts on B only on its $\mathbb{Z}[G]$-component, it suffices to show this for $\mathbb{Z}[G]$, in which case it is easily verified. □

12.5.6. Corollary. *Let A be a free $\mathbb{Z}[G]$-module, then it has trivial Tate (co)homology.*

Proof. Let B be the free $\mathbb{Z}$-module generated by a $\mathbb{Z}[G]$-basis of A. Then $A \cong \mathrm{Ind}^G(B)$. □

Finally, we specialize to the case where $G = \langle g \rangle$ is a finite cyclic group. Then, instead of using the standard resolution, we can use instead

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0. \tag{$*$}$$

Since G is abelian, we may view $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$ as a $\mathbb{Z}[G]$-module by $(g\phi)(h) := \phi(gh)$, and $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$ as a $\mathbb{Z}[G]$-module by $g(h \otimes a) := (gh) \otimes a = h \otimes (ga)$. Of course, both of these are canonically isomorphic to A as G-modules.

12.5.7. Theorem. *Let $G = \langle g \rangle$ be a finite cyclic group, then the even-indexed Tate cohomologies (i.e. odd-indexed Tate homologies) of any G-module A are all equal to $\hat{H}^0(G,A)$, and the odd-indexed Tate cohomologies (i.e. even-indexed Tate homologies) are all equal to $\hat{H}_0(G,A)$.*

Proof. Apply the tensor and hom functors on $(*)$. □

12.6. Herbrand quotient.

12.6.1. Definition. Let G be a finite cyclic group, A a G-module. Let $h^0(A) = h^0(G,A) = \#\hat{H}^0(G,A)$, and $h_0(A) = h_0(G,A) = \#\hat{H}_0(G,A)$. When both of these are finite, the *Herbrand quotient* is defined as

$$h(A) = h^0(A)/h_0(A) \in \mathbb{Q}.$$

12.6.2. Proposition. *Let G be a finite cyclic group, $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then there is an exact hexagon*

$$\begin{tikzcd}
& \hat{H}^0(A) \arrow[r, "\alpha^0"] & \hat{H}^0(B) \arrow[dr, "\beta^0"] & \\
\hat{H}_0(C) \arrow[ur, "\delta_0"] & & & \hat{H}^0(C) \arrow[dl, "\delta^0"] \\
& \hat{H}_0(B) \arrow[ul, "\beta_0"] & \hat{H}_0(A) \arrow[l, "\alpha_0"'] &
\end{tikzcd}$$

where the map δ^0 is given by $\hat{H}^0(C) \cong \hat{H}^{-2}(C) = \hat{H}_1(C) \to \hat{H}_0(A)$. □

12.6.3. Corollary. *In $0 \to A \to B \to C \to 0$, if two of $h(A), h(B), h(C)$ are defined then so is the third, and $h(B) = h(A)h(C)$.*

Proof. We have $h^0(A) = \#\hat{H}^0(A) = \#\ker\alpha^0 \#\operatorname{im}\alpha^0 = \#\ker\alpha^0\#\ker\beta^0$. Similarly, we obtain

$$h^0(A)h^0(C)h_0(B) = \#\ker\alpha^0\#\ker\beta^0\#\ker\delta^0\#\ker\alpha_0\#\ker\beta_0\#\ker\delta_0 = h_0(A)h_0(C)h^0(B),$$

as desired. □

12.6.4. Corollary. *If A is either (a) induced or coinduced, or (b) finite, then $h(A) = 1$.*

Proof. If A is induced or coinduced, then both $h^0(A)$ and $h_0(A)$ are 1.

If A is finite: consider the exact sequence $0 \to A^G \to A \xrightarrow{g-1} A \to A_G \to 0$, which implies

$$\#A^G = \#\ker(g-1) = \#\operatorname{coker}(g-1) = \#A_G,$$

so $h_0(A) = \#\ker(\hat{N}_G) = \#\operatorname{coker}(\hat{N}_G) = h^0(A)$. □

12.6.5. Corollary. *Let A be a finitely generated abelian group, then $h(A) = h(A/A_{\text{tors}})$. Moreover, if A is a trivial G-module, then $h(A) = \#(G)^{\operatorname{rk} A}$.* □

12.6.6. Lemma. *Let $\alpha : A \to B$ have finite kernel and cokernel. Then $h(A) = h(B)$.*

Proof. Use the exact sequences $0 \to \ker\alpha \to A \to \operatorname{im}\alpha \to 0$ and $0 \to \operatorname{im}\alpha \to B \to \operatorname{coker}\alpha \to 0$ □

12.6.7. Corollary. *Let $A \subseteq B$ be a submodule with finite index, then $h(A) = h(B)$.*

12.7. Herbrand unit theorem. We now apply all this to the class field theory setting. Let L/K be a finite Galois extension of local or global fields. Then the abelian groups L, $L^\times$, $\mathcal{O}_L$, $\mathcal{O}_L^\times$, $\mathcal{I}_L$, $\mathcal{P}_L$ (principal) are all (nontrivial) G-modules, where $G = \operatorname{Gal}(L/K)$.

In the case $G = \langle\sigma\rangle$ is cyclic, we can compute the Herbrand quotient for all of the above (recall, again, that $\hat{H}_0(A) = \ker\hat{N}_G = \ker(N_G)/\operatorname{im}(\sigma-1)$ and $\hat{H}^0(A) = \operatorname{coker}\hat{N}_G = \ker(\sigma-1)/\operatorname{im}(N_G)$). Also, in the case for $L^\times, \mathcal{O}_L^\times, \mathcal{I}_L, \mathcal{P}_L$, the norm map corresponds to the element norm and the ideal norm; in the case L and $\mathcal{O}_L$, the norm map corresponds to the trace.

12.7.1. Lemma (linear independence of automorphisms)**.** *Let L/K be finite Galois, then the set $\operatorname{Aut}_K(L)$ is linearly independent in the L-vector space $f : L \to L$.*

Proof. Suppose otherwise, then suppose n is smallest such that there exists distinct $f_1, \ldots, f_n \in \operatorname{Aut}_K(L)$ and $a_1, \ldots, a_n \in L^\times$ with $\sum a_i f_i \equiv 0$. Since $f_1 \neq f_2$, there exists $x_0 \in L$ such that $f_1(x_0) \neq f_2(x_0)$. Then $\sum a_i f_i(x_0 x) = \sum a_i f_i(x_0) f_i(x) = 0$ for all $x \in L$. Canceling out the two equations gives us a linear dependence among $n-1$ automorphisms, a contradiction. □

12.7.2. Lemma. *Let L/K finite Galois, $G = \operatorname{Gal}(L/K)$. Then:*

(i) $\hat{H}^0(G, L) = \hat{H}^1(G, L) = 0$*;*

(ii) $\hat{H}^0(G, L^\times) \cong K^\times/\operatorname{N}(L^\times)$*, and* $\hat{H}^1(G, L^\times)$ *is trivial.*

PROOF. For (i): first, since $\ker(\sigma - 1 : L \to L) = L^G = K$, and $\operatorname{im}(N_G) = \operatorname{im}(\operatorname{Tr}_{L/K}) = K$ (L/K Galois hence separable hence trace form nondegerate), we have $\hat{H}^0(G, L) = 0$. To find $H^1(G, L)$, we use its description as the crossed homomorphisms $f : G \to L$ modulo the principal ones. Let $f : G \to L$ be any crossed homomorphism, then let $\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha) \in L$, where $\alpha \in L$ is a fixed element with trace 1. Then for any $\sigma \in G$,

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} (f(\sigma\tau) - f(\sigma))(\sigma\tau(a)) = \beta - f(\sigma),$$

so $f(\sigma) = \beta - \sigma(\beta)$, so f is in fact principal.

For (ii), $(L^\times)^G = K^\times$, and $\operatorname{im}(N_G) = \mathrm{N}(L^\times)$. To find $H^1(G, L^\times)$, let $f : G \to L^\times$ be any crossed homomorphism. Let $\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha)$ where α is chosen so that $\beta \in L^\times$ (by linear independence of automorphisms). Then

$$\tau(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} f(\sigma\tau)f(\sigma)^{-1}(\sigma\tau(\alpha)) = f(\sigma)^{-1}\beta,$$

so $f(\sigma) = \beta/\tau(\beta)$ is principal. □

Let L/K be a Galois extension of global fields. Then $\operatorname{Gal}(L/K)$ acts on the set of places M_L, via $\|\alpha\|_{\sigma w} = \|\sigma\alpha\|_w$. Also, for a fixed place v of K, it permutes the places $w \mid v$.

12.7.3. Definition. The *decomposition group* D_w of a place $w \in M_L$ is the stabilizer

$$D_w := \{\sigma \in \operatorname{Gal}(L/K) : \sigma(w) = w\}.$$

We know $\operatorname{Gal}(L/K)$ acts transitively on $\{w \mid v\}$, so the D_w's are conjugate.

12.7.4. Remark. For archimedean places for number fields, $w \mid v$, D_w is trivial unless w is complex and v is real, in which case $\#D_w = 2$. Also, in the archimedean case, we define $I_w = D_w$. So $f_w = 1$ always, and $e_w = 2$ iff w is a complex place that extends a real place.

With these definitions, $[L : K] = e_v f_v g_v$ for *all* places $v \in M_K$.

12.7.5. Definition. Let L/K be an extension of number field. Let $e_0 = \prod_{v \nmid \infty} e_v$ and $e_\infty = \prod_{v \mid \infty} e_v$, $e(L/K) = e_0 e_\infty$.

12.7.6. Theorem (Herbrand unit theorem)**.** *Let L/K be a Galois extension of number fields, and let $w_1, \ldots, w_{r+s}$ be the archimedean places of L. Then there exist $\varepsilon_1, \ldots, \varepsilon_{r+s} \in \mathcal{O}_L^\times$, such that:*

- *$\sigma(\varepsilon_i) = \varepsilon_j \iff \sigma(w_i) = w_j$, for $\sigma \in G$;*
- *$\varepsilon_1, \ldots, \varepsilon_{r+s}$ generate a finite index subgroup of $\mathcal{O}_L^\times$;*
- *$\varepsilon_1\varepsilon_2 \ldots \varepsilon_{r+s} = 1$, and all other multiplicative relations are multiples of this.*

PROOF. Pick $v_1, \ldots, v_{r+s} \in \mathcal{O}_L^\times$ (i.e. 1 at all finite places) such that $|v_i|_{w_j} < 1$ when $i \neq j$ and $|v_i|_{w_i} > 1$ (which is then automatic). These can be picked as follows (say $i = 1$): we use the adelic Minkowski theorem. Choose the idèle d as follows: $|d_w|_w = 1$ for nonarchimedean w, $|d_{w_i}|_{w_i} = \frac{1}{M}$ for $i \neq 1$ (M a large number chosen afterwards), and $|d_{w_1}|_{w_1}$ large enough such that $|d| = c$ (the bound in adelic Minkowski), so that $L(d)$ contains a nonzero point $x \in L$. In fact, by construction, $x \in \mathcal{O}_L$, and $\mathrm{N}(x) = \prod_i |x|_{w_i} = c$. To modify x so that it lies in $\mathcal{O}_L^\times$, choose a generator γ for all (finitely many) principal ideals of norm at most c. Then dividing x by the previously fixed generator of (x) gives a number in $\mathcal{O}_L^\times$. To control its absolute value under w_i ($i \neq 1$), let

$$M = \max_{\gamma : i \neq 1} \frac{1}{|\gamma|_i},$$

so that $|x/\gamma|_i < 1$ for $i \neq 1$. This concludes the process of choosing $v_1 = x/\gamma$.

Let $\alpha_i = \prod_{\sigma \in D_{w_i}} \sigma(v_i) \in \mathcal{O}_L^\times$. Then it is easy to compute $|\alpha_i|_{w_i} > 1$ and $|\alpha_i|_{w_j} < 1$ for $j \neq i$, and furthermore the stabilizer of α_i in G is D_{w_i}.

Now, the Galois group partitions w_i into m orbits, where m is the number of archimedean places of K. Reindex w_i and a_i such that $w_1, \ldots, w_m$ lie in distinct orbits. For $i = 1, \ldots, r+s$, let $r(i) = \min\{j : \sigma(w_j) = w_i \text{ for some } \sigma\}$, and call the corresponding σ_i (which is unique up to $D_{w_{r(i)}}$).

Now, let $\beta_i = \sigma_i(\alpha_{r(i)})$, which does not depend on the choice of σ_i since $\alpha_{r(i)}$ is fixed by $D_{w_{r(i)}}$. Then it is not hard to verify that β_i satisfy the first bullet point. Furthermore,

$$|\beta_i|_{w_j} = \left|\sigma_i(\alpha_{r(i)})\right|_{w_j} = \left|\alpha_{r(i)}\right|_{\sigma_i(w_j)},$$

so $|\beta_i|_{\sigma_i^{-1}w_{r(i)}} > 1$ and for all other places of L, $|\beta_i| < 1$. Furthermore, it is clear that $\sigma_i^{-1}w_{r(i)}$ are simply a permutation of w_i: if $\sigma_{i_1}^{-1}w_{r(i_1)} = \sigma_{i_2}^{-1}w_{r(i_2)}$, then $r(i_1) = r(i_2)$ and $\sigma_{i_1}\sigma_{i_2}^{-1} \in D_{w_{r(i_1)}}$, so $\beta_{i_1} = \beta_{i_2}$, which implies $w_{i_1} = w_{i_2}$, so $i_1 = i_2$. Thus, to show that β_i's generate a finite index subgroup of $\mathcal{O}_L^\times$, we observe that in fact any $r+s$ units satisfying the condition ε_i has this property (essentially because a $(r+s-1)\times(r+s-1)$ matrix with positive row sums, where only diagonal elements are positive and the rest are negative, is necessarily invertible).

Finally, because β_i's must have one relation, suppose $\prod_i \beta_i^{n_i}$ is one with coprime exponents. By a rank argument, these cannot have other relations. Then, we claim that taking $\varepsilon_i = \beta_i^{n_i}$ finishes the problem. Indeed, (iii) and (ii) are easy to verify. To show (i), we need $n_i = n_j$ whenever w_i and w_j are in the same G-orbit. But this is true, since applying $\sigma \in G$ should not give any additional relations between β_i. □

12.8. The ambiguous class number formula.

12.8.1. Lemma (Noether)**.** *For L/K finite cyclic with $G = \mathrm{Gal}(L/K)$, $\hat{H}_0(G,L) = \hat{H}_0(G,L^\times) = 0$.*

Proof. Let σ be a generator of G. By normal basis theorem (theorem 1.7.6), there exists $\beta \in L^\times$ such that $\{\sigma^i\beta\}$ is a basis of L/K. Under this basis, σ acts by translating the coordinates. So for $\alpha \in \ker(N_G) \subseteq L$, $\alpha = \sum_i \alpha_i(\sigma^i\beta)$, let us define $\gamma = \sum_i \gamma_i(\sigma^i\beta)$ where $\gamma_i = -\sum_{j=1}^i \alpha_i$. Since $\sum_i \alpha_i = 0$, we have $\alpha = \sigma\gamma - \gamma$, i.e. $\alpha \in \mathrm{im}(\sigma - 1)$. This shows $\hat{H}_0(G,L) = 0$. A similar proof works for $\hat{H}_0(G,L^\times)$. □

12.8.2. Remark. This also follows from the vanishing of $\hat{H}^1(G,L)$ and $\hat{H}^1(G,L^\times)$ in general, and that for G cyclic, $\hat{H}^1 = \hat{H}_0$.

12.8.3. Corollary (Hilbert 90, original form)**.** *Let L/K be a finite cyclic extension, with* $\mathrm{Gal}(L/K)$ *generated by σ. Then for $\alpha \in L^\times$, $\mathrm{N}(\alpha) = 1$ iff $\alpha = \beta/\sigma(\beta)$ for some $\beta \in L^\times$.*

12.8.4. Theorem. *Let L/K finite cyclic, then*

$$h(\mathcal{O}_L^\times) = \frac{e_\infty(L/K)}{[L:K]}.$$

Proof. Let $\varepsilon_1, \ldots, \varepsilon_{r+s}$ be as in the Herbrand unit theorem, and let A be the finite-index subgroup of $\mathcal{O}_L^\times$ they generate. Then A is also a G-module. For an embedding $\phi : K \hookrightarrow \mathbb{C}$, let E_ϕ be the free Z-module with basis $\varphi : L \hookrightarrow \mathbb{C}$ extending ϕ. Then E_ϕ are also G-modules; in fact, G acts on $\{\varphi \mid \phi\}$ freely and transitively, so $E_\phi \cong \mathbb{Z}[G] \cong \mathrm{Ind}^G(\mathbb{Z})$. Let v_ϕ be the place of K corresponding to ϕ. Let A_v be the free G-module with basis w (places above v). Consider the G-module morphism $\pi : E_\phi \to A_v$, sending $\varphi \mapsto w_\varphi$. We have an exact sequence

$$0 \to \ker\pi \to E_\phi \xrightarrow{\pi} A_v \to 0,$$

where $\ker\pi = (\sigma^m - 1)E_\phi$, where σ is a generator for G and $m = \#\{w \mid v\}$. If ϕ is unramified, then $\ker\pi = 0$ and $h(A_v) = h(E_\phi) = 1$. If G is ramified, then a more careful analysis gives $h(\ker\phi) = 1/2$, so $h(A_v) = 2$. In any case, $h(A_v) = e_v$.

Now, consider the exact sequence of G-modules

$$0 \to \mathbb{Z} \to \bigoplus_{v\mid\infty} A_v \xrightarrow{\phi} A \to 0,$$

where ψ sends $w_i \mapsto \varepsilon_i$. We are done because $h(\mathbb{Z}) = \#G = [L:K]$. □

12.8.5. Lemma. *Let L/K be a cyclic extension of global fields. Then $h_0(\mathcal{I}_L) = 1$ and $h(\mathcal{I}_L) = h^0(\mathcal{I}_L) = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$.*

Proof. Suppose $I \in \ker N_G$, i.e. $I \in \mathcal{I}_L$ satisfies $N(I) = \mathcal{O}_K$. By using the explicit description $N(\mathfrak{q}) = p^{f_\mathfrak{q}}$, we can conclude that for each $\mathfrak{p}$ in K, $\sum_{\mathfrak{q}\mid\mathfrak{p}} v_\mathfrak{q}(I) = 0$. Since $G = \mathrm{Gal}(L/K)$ is cyclic, we can order $\{\mathfrak{q} \mid \mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$ such that $\sigma\mathfrak{q}_i = \mathfrak{q}_{i+1}$ where σ is a fixed generator of G (of course, $\sigma\mathfrak{q}_g = \mathfrak{q}_1$).

Let $n_i = v_{\mathfrak{q}_i}(I)$ and $m_i = -\sum_{j=1}^{i} n_j$, and let $J_\mathfrak{p} = \sum \mathfrak{q}_i^{\mathfrak{m}_i}$. Then $\sigma(J_\mathfrak{p})/J_\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{v_q(I)}$. The conclusion is that $I = \sigma(J)/J$, i.e. $I \in \operatorname{im}(\sigma - 1)$. This shows $h_0(I_L) = 1$.

Now, we compute $h^0(\mathcal{I}_L)$. Suppose $I \in \ker(\sigma - 1) = \mathcal{I}_L^G$, then this is equivalent to $v_\mathfrak{q}(I)$ being constant for $\mathfrak{q}$ over a fixed $\mathfrak{p}$. Then I is a product of ideals of form $(\mathfrak{p}\mathcal{O}_L)^{1/e_\mathfrak{p}}$. So $[\mathcal{I}_L^G : \mathcal{I}_K] = e_0(L/K)$, so $h^0(\mathcal{I}_L) = [\mathcal{I}_L^G : N(\mathcal{I}_L)] = [\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : N(\mathcal{I}_L)] = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$. □

12.8.6. Theorem (ambiguous class number formula)**.** *Let L/K be a finite cyclic extension of number fields. Then*

$$\#\operatorname{Cl}_L^G = \frac{e(L/K)\#\operatorname{Cl}_K}{n(L/K)[L:K]},$$

where $n(L/K) = [\mathcal{O}_K^\times : \mathrm{N}(L^\times) \cap \mathcal{O}_K^\times] \in \mathbb{Z}_{\geq 1}$.

Proof. Consider the long exact sequence in cohomology

$$0 \to \mathcal{P}_L^G \to \mathcal{I}_L^G \to \operatorname{Cl}_L^G \to H^1(\mathcal{P}_L) \to 0,$$

since $H^1(\mathcal{I}_L) \cong \hat{H}_0(\mathcal{I}_L) = 0$. Therefore, $\#\operatorname{Cl}_L^G = h_0(\mathcal{P}_L) \cdot [\mathcal{I}_L^G : \mathcal{P}_L^G]$.

Consider the inclusions $\mathcal{P}_K \subseteq \mathcal{P}_L^G \subseteq \mathcal{P}_L$, so

$$[\mathcal{I}_L^G : \mathcal{P}_L^G] = \frac{[\mathcal{I}_L^G : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{[\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{e_0(L/K)\#\operatorname{Cl}_K}{[\mathcal{P}_L^G : \mathcal{P}_K]}.$$

Now, consider another long exact sequence in cohomology

$$0 \to (\mathcal{O}_L^\times)^G \to (L^\times)^G \to \mathcal{P}_L \to H^1(\mathcal{O}_L^\times) \to H^1(L^\times) \to H^1(\mathcal{P}_L^G) \to H^2(\mathcal{O}_L^\times) \to H^2(L^\times),$$

which can be simplified into

$$0 \to \mathcal{O}_K^\times \to K^\times \to \mathcal{P}_L^G \to \hat{H}_0(\mathcal{O}_L^\times) \to 0 \to \hat{H}_0(\mathcal{P}_L) \to \hat{H}^0(\mathcal{O}_L^\times) \xrightarrow{f} K^\times/\mathrm{N}(L^\times).$$

Since $K^\times/\mathcal{O}_K^\times \cong \mathcal{P}_K$, we get

$$[\mathcal{P}_L^G : \mathcal{P}_K] = h_0(\mathcal{O}_L^\times) = \frac{h^0(\mathcal{O}_L^\times)[L:K]}{e_\infty(L/K)}.$$

The last three terms of the above long exact sequence also gives

$$\frac{h^0(\mathcal{O}_L^\times)}{h_0(\mathcal{P}_L)} = \#\operatorname{im} f = [\mathcal{O}_K^\times : \mathrm{N}(L^\times) \cap \mathcal{O}_K^\times].$$

Therefore,

$$\#\operatorname{Cl}_L^G = \frac{h_0(\mathcal{P}_L)e(L/K)\#\operatorname{Cl}_K}{h_0(\mathcal{O}_L^\times)[L:K]} = \frac{e(L/K)\#\operatorname{Cl}_K}{n(L/K)[L:K]},$$

as desired. □

Some remarks on the ambiguous class number formula. First, if L/K is quadratic, then $G = \{1, \sigma\}$ has order 2. In this case, for any $I \in \mathcal{I}_L$, $N(I) = I \cdot \sigma I$, so passing to Cl_L gives $[1] = [I][\sigma I]$. This means that $[I]$ is a 2-torsion element in Cl_L iff $[I]$ is G-invariant. In particular, when L/K is an imaginary quadratic extension with discriminant D, $e_\infty(L/K) = [L:K] = 2$ and $n(L/K) = 2$, so the ambiguous class number formula gives $\#\operatorname{Cl}_L[2] = \frac{e_0(L/K)}{2}$, i.e. its $\mathbb{Z}/2\mathbb{Z}$-rank is $\#\{p \mid D\} - 1$. This has applications in factoring integers.

12.9. First main inequality of CFT.

12.9.1. Lemma. *Let $f : A \to C$ be a map of abelian groups, such that* $\ker f \subseteq B \subseteq A$*, then $A/B \cong f(A)/f(B)$.*

Proof. Use snake lemma. □

And now the payoff:

12.9.2. Theorem (first main inequality)**.** *Let L/K be a totally unramified cyclic extension of number fields (i.e. $e(L/K) = 1$). Then*

$$[\mathcal{I}_K : T_{L/K}] \geq [L:K],$$

where $T_{L/K} = \mathcal{P}_K N(\mathcal{I}_L)$ is the norm group (Takagi group) for the trivial modulus.

Proof. Let us rewrite

$$\begin{aligned}[\mathcal{I}_K : \mathcal{P}_K N(\mathcal{I}_L)] &= \frac{[\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_K N(\mathcal{I}_L) : \mathcal{P}_K]}\\ &= \frac{\#\operatorname{Cl}_K}{[N(\mathcal{I}_L) : N(\mathcal{I}_L)\cap \mathcal{P}_K]}\\ &= \frac{\#\operatorname{Cl}_K}{[\mathcal{I}_L : N^{-1}(\mathcal{P}_K)]}\\ &= \frac{\#\operatorname{Cl}_K}{[\mathcal{I}_L/\mathcal{P}_L : N^{-1}(\mathcal{P}_K)/\mathcal{P}_L]}\\ &= \frac{\#\operatorname{Cl}_K}{[\operatorname{Cl}_L : \operatorname{Cl}_L[N_G]]}\\ &= \frac{\#\operatorname{Cl}_K}{\#N_G(\operatorname{Cl}_L)}.\end{aligned}$$

Now, $h^0(\operatorname{Cl}_L) = [\operatorname{Cl}_L^G : N_G(\operatorname{Cl}_L)]$, so by the ambiguous class number formula:

$$[\mathcal{I}_K : T_{L/K}] = \frac{\#\operatorname{Cl}_K h^0(\operatorname{Cl}_L)}{\#\operatorname{Cl}_L^G} = \frac{h^0(\operatorname{Cl}_L)n(L/K)[L:K]}{e(L:K)} = h^0(\operatorname{Cl}_L)n(L/K)[L:K] \geq [L:K],$$

as desired. □

12.9.3. Corollary (norm index equality, etc.). *Let L/K be a totally unramified cyclic extension of number fields, then:*

- $[\mathcal{I}_K : T_{L/K}] = [L:K]$;
- $\#\operatorname{Cl}_L^G = \#\operatorname{Cl}_K/[L:K]$;
- *the Tate cohomologies of* Cl_L *all vanish;*
- *every unit in* $\mathcal{O}_K^\times$ *is the norm of an element in* L.

Proof. Equality follows from theorems 11.9.7, 12.9.2. In fact, because equality holds, the proof of the first main inequality tells us more things: $\hat{H}^0(\operatorname{Cl}_L) = 0$ and $\mathcal{O}_K^\times \subset \mathrm{N}(L^\times)$ (every unit is a norm). The ambiguous class number formula then says $\#\operatorname{Cl}_L^G = \#\operatorname{Cl}_K/[L:K]$. In addition, $h(\operatorname{Cl}_L) = 1$ since Cl_L is finite, and since we know $h^0(\operatorname{Cl}_L) = 1$, $h_0(\operatorname{Cl}_L) = 1$ as well. □

In the homework, it will be shown that this implies $\ker \psi_{L/K} = T_{L/K}$, and a similar equality holds in the ramified case where there is a nontrivial modulus. This then immediately implies that $\mathcal{I}_K^{\mathfrak{m}}/T_{L/K} \cong \operatorname{Gal}(L/K)$ is an isomorphism, i.e. Artin reciprocity.

12.10. Local CFT. In this subsection we will focus on local class field theory. Since what we've shown points to the importance of the images of norm maps, and norms can be computed locally, it makes sense for us to start locally.

Let K be a local field, with a fixed separable closure K^{sep}, and let

$$K^{\text{ab}} = \bigcup_{L\subseteq K^{\text{sep}}: L/K \text{ finite abelian}} L$$

$$K^{\text{unr}} = \bigcup_{L\subseteq K^{\text{sep}}: L/K \text{ finite unramified}} L$$

be the maximal abelian and unramified extensions of K (inside K^{sep}), so $K \subseteq K^{\text{unr}} \subseteq K^{\text{ab}} \subseteq K^{\text{sep}}$. The middle inclusion is true because any finite unramified extension of K is cyclic. Infinite Galois theory tells us that there is a one-to-one correspondence

$$\{\text{extensions } L/K \text{ in } K^{\text{ab}}\} \longleftrightarrow \{\text{closed subgroups of } \operatorname{Gal}(K^{\text{ab}}/K)\}$$

$$\{\text{Galois extensions}\} \longleftrightarrow \{\text{closed normal subgroups}\}$$

$$\{\text{finite extensions}\} \longleftrightarrow \{\text{open subgroups}\}.$$

The archimedean case is not very interesting, so let us assume K is nonarchimedean. Then the discrete valuation ring $\mathcal{O}_K$ is a DVR, with prime $\mathfrak{p}$, and let $\mathbb{F}_{\mathfrak{p}}$ be the residue field.

Let L/K be unramified, then the Galois group $\mathrm{Gal}(L/K)$ is generated by the Frobenius element $\mathrm{Frob}_{L/K}$. The Artin map $\psi_{L/K} : \mathcal{I}_K \to \mathrm{Gal}(L/K)$ sends $\mathfrak{p} \mapsto \mathrm{Frob}_{L/K}$. Since $\mathcal{O}_K$ is a PID, we can extend $\psi_{L/K}$ multiplicatively to a map $\psi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$.

12.10.1. Theorem (local Artin reciprocity)**.** *Let K be a local field. There is a unique continuous homomorphism $\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, such that for any finite abelian L/K in K^{ab}, we have an induced map $\theta_{L/K} : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$, which satisfies:*

- *If K is nonarchimedean and L is unramified, then $\theta_{L/K}(\pi) = \mathrm{Frob}_{L/K}$, where π is any uniformizer of K;*
- *$\theta_{L/K}$ is surjective with kernel $\mathrm{N}_{L/K}(L^\times)$, hence induces an isomorphism $K^\times/\,\mathrm{N}_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$.*

12.10.2. Remark. Mentally compare this to the more complicated global CFT: there is no modulus since K^{ab} covers everything, and $\mathcal{I}_K^{\mathfrak{m}}/T_{L/K}$ is replaced with $K^\times/\,\mathrm{N}(L^\times)$. The analogue in global CFT is by considering the *idèle* class group, which contains everything and hides the moduli.

12.10.3. Definition. A *norm group* of a local field K is any subgroup of $K^\times$ of the form $\mathrm{N}_{L/K}(L^\times)$, L finite ab. extension.

12.10.4. Remark. The word "abelian" can be removed without changing anything. If L/K is any finite extension, not even necessarily Galois, then the *norm limitation theorem* implies that $\mathrm{N}(L^\times) = \mathrm{N}(M^\times)$, where M is the maximal abelian extension of K in L.

12.10.5. Corollary. *The map $L \mapsto \mathrm{N}(L^\times)$ induces an inclusion-reversing bijection between finite abelian extensions L/K and norm groups of K, satisfying:*

- $\mathrm{N}((L_1L_2)^\times) = \mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times)$*;*
- $\mathrm{N}((L_1 \cap L_2)^\times) = \mathrm{N}(L_1^\times)\,\mathrm{N}(L_2^\times)$*.*

Proof. The inclusion-reversal follows from transitivity of norms. We use Artin reciprocity to prove the two bullet points.

To show $\mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times) \subseteq \mathrm{N}((L_1L_2)^\times)$: because $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ is injective, we can conclude by Artin reciprocity. The other direction is clear.

To show the map $L \mapsto \mathrm{N}(L^\times)$ is a bijection: surjectivity follows by definition. Suppose L_1, L_2 give rise to the same norm group, then L_1L_2 also gives rise to the same norm group. By Artin reciprocity, $\mathrm{Gal}(L_1L_2/K) = \mathrm{Gal}(L_1/K) = \mathrm{Gal}(L_2/K)$, so $L_1 = L_2$. This shows injectivity.

Finally, to show the second bullet point, note that $\mathrm{N}(L_1^\times)\,\mathrm{N}(L_2^\times)$ is the smallest subgroup of $K^\times$ containing both norm groups, and $L_1 \cap L_2$ is the largest extension of K contained in both L_1 and L_2. So $\mathrm{N}((L_1 \cap L_2)^\times) = \mathrm{N}(L_1^\times)\,\mathrm{N}(L_2^\times)$ by the bijection described above. □

12.10.6. Corollary. *Every norm group has finite index in $K^\times$, and every group that contains a norm group is a norm group.*

Proof. By Artin reciprocity, $K^\times/\,\mathrm{N}(L^\times) \cong \mathrm{Gal}(L/K)$ is a finite group, so every norm group has finite index.

Suppose $\mathrm{N}(L^\times) \leq H \leq K^\times$. Consider $F = L^{H/\,\mathrm{N}(L^\times)}$, where $H/\,\mathrm{N}(L^\times)$ is viewed as a subgroup of $K^\times/\,\mathrm{N}(L^\times) \cong \mathrm{Gal}(L/K)$. Then Artin reciprocity shows that $\mathrm{N}(F^\times) \cong H$. □

12.10.7. Lemma. *Let L/K be any extension of local fields. If $\mathrm{N}(L^\times)$ has finite index in $K^\times$, then it is open.*

Proof. The archimedean case is not interesting, so WLOG K is nonarchimedean. Since $\mathcal{O}_L^\times$ is compact, its image $\mathrm{N}(\mathcal{O}_L^\times)$ must also be compact, hence closed ($K^\times$ is Hausdorff). Because for $\alpha \in L^\times$,

$$\alpha \in \mathcal{O}_L^\times \iff |\alpha| = 1 \iff \left|\mathrm{N}_{L/K}(\alpha)\right| = 1 \iff \mathrm{N}_{L/K}(\alpha) \in \mathcal{O}_K^\times,$$

we have $\mathrm{N}(\mathcal{O}_L^\times) = \mathrm{N}(L^\times) \cap \mathcal{O}_K^\times$, so it is the kernel of the map $\mathcal{O}_K^\times \hookrightarrow K^\times \twoheadrightarrow K^\times/\,\mathrm{N}(L^\times)$. This shows $\mathcal{O}_K^\times/\,\mathrm{N}(\mathcal{O}_L^\times)$ is finite, and thus $\mathrm{N}(\mathcal{O}_L^\times)$ is closed and of finite index in $\mathcal{O}_K^\times$, hence open. But $\mathcal{O}_K^\times$ is open in $K^\times$, so $\mathrm{N}(\mathcal{O}_L^\times)$ is open in $K^\times$, so $\mathrm{N}(L^\times)$ is open as well, being the union of cosets of $\mathrm{N}(\mathcal{O}_L^\times)$. □

The two other main statements of local CFT are the following:

- Existence: for any open $H \subseteq K^\times$ of finite index, there exists a unique L/K in K^{ab} such that $H = \mathrm{N}(L^\times)$. By virtue of Lemma 12.10.7, this means that for subgroups of $K^\times$, finite index open $\iff$ is a norm group.
- Main Theorem: θ_K induces a canonical homeomorphism of profinite groups

$$\widehat{\theta}_K : \widehat{K^\times} \xrightarrow{\cong} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Proof of the Main Theorem. By Artin reciprocity and the existence theorem,

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim_{L/K \text{ f. ab.}} \mathrm{Gal}(L/K) \cong \varprojlim_{H \text{ norm group}} \frac{K^\times}{H} = \varprojlim_{H \text{ finite index open}} \frac{K^\times}{H} \cong \widehat{K^\times},$$

as desired. □

When K is archimedean, $\widehat{K^\times}$ is either trivial ($K = \mathbb{C}$) or has order 2 ($K = \mathbb{R}$). So we focus on the nonarchimedean case. By picking a uniformizer π, we get a non-canonical isomorphism $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$. So $\widehat{K^\times} \cong \widehat{\mathcal{O}_K^\times} \times \widehat{\mathbb{Z}} = \mathcal{O}_K \times \widehat{\mathbb{Z}}$, where $\mathcal{O}_K^\times$ is already profinite because it is compact, Hausdorff, and totally disconnected. More canonically, we have the commutative diagram of split exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\cong"] & K^\times \arrow[r, "v"] \arrow[d, "\theta_K"] & \mathbb{Z} \arrow[r] \arrow[d, hook, "\phi"] & 1 \\
1 \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}}) \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r] & \mathrm{Gal}(K^{\mathrm{unr}}/K) \arrow[r] & 1
\end{tikzcd}$$

where ϕ becomes the inclusion $\phi : \mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$ under the identification $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(\overline{\mathbb{F}_\mathfrak{p}}/\mathbb{F}_\mathfrak{p}) \cong \widehat{\mathbb{Z}}$, and sends 1 to the element $(\mathrm{Frob}_{L/K})_L$, called the *arithmetic Frobenius*. (Aside: $\phi(-1)$ is called the *geometric Frobenius*.) Taking the profinite completion of the top row yields the bottom row. The arithmetic/geometric Frobenius is a topological generator (generates a dense subgroup) of $\mathrm{Gal}(K^{\mathrm{unr}}/K)$.

Now consider $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Because the top sequence splits, the bottom does as well (also non-canonically): $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$. The fixed field of $\mathcal{O}_K \cong \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}})$ is K^{unr}, and let K_π be the fixed field of $\theta_K(\pi)$. Then $K^{\mathrm{ab}} = K^{\mathrm{unr}} K_\pi$. The fact that K_π is not canonical reflects the fact that one cannot say the "maximal totally ramified extension". But what we can say is that K_π is the compositum of all finite, totally ramified L/K in K^{ab} such that $\pi \in \mathrm{N}(L^\times)$.

12.10.8. Example. Let $K = \mathbb{Q}_p$, and pick $\pi = p$ (of course, we could have picked any valuation-1 element). Then the picture looks like this:

$$\begin{tikzcd}
 & \mathbb{Q}_p^{\mathrm{ab}} \arrow[dl, dash, "\mathbb{Z}_p^\times"'] \arrow[dr, dash, "\widehat{\mathbb{Z}}"] & \\
\mathbb{Q}_p^{\mathrm{unr}} \cong \bigcup_n \mathbb{Q}_p(\zeta_{p^n}) \arrow[dr, dash, "\widehat{\mathbb{Z}}"'] & & (\mathbb{Q}_p)_p = \bigcup_{\gcd(m,p)=1} \mathbb{Q}_p(\zeta_m) \arrow[dl, dash, "\mathbb{Z}_p^\times"] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

12.11. Global CFT via idèles. Let K be a global field. Recall the group of idèles

$$\mathbb{I}_K = \mathbb{A}_K^\times := \prod\nolimits_v' (K_v^\times, \mathcal{O}_v^\times).$$

Standard caveat is that in the first equality, the topology of $\mathbb{I}_K$ is finer than the one inherited as a subset of $\mathbb{A}_K$. We have a natural map

$$\begin{aligned} \varphi : \mathbb{I}_K &\to \mathcal{I}_K \\ a &\mapsto \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}. \end{aligned}$$

This ignores the infinite places. There is a natural commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r] \arrow[d, two heads, "x\mapsto(x)"'] & \mathbb{I}_K \arrow[r] \arrow[d, two heads, "\varphi"] & C_K \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & \mathcal{P}_K \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

where C_K is the idèle class group.

12.11.1. Definition. Given finite separable L/K, define the norm map

$$\mathrm{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$$

mapping

$$(a_w)_w \mapsto \left.\mathrm{pr}\prod_{w|v} \mathrm{N}_{L_v/K_w}(a_w)\ \right._v .$$

This behaves well with the other norm maps:

$$\begin{tikzcd}
L^\times \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathbb{I}_L \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathcal{I}_L \arrow[d, "N"] \\
K^\times \arrow[r] & \mathbb{I}_K \arrow[r] & \mathcal{I}_K,
\end{tikzcd}$$

so this induces a map

$$\begin{tikzcd}
C_L \arrow[r, two heads] \arrow[d, "\mathrm{N}_{L/K}"'] & \mathrm{Cl}_L \arrow[d, "\mathrm{N}_{L/K}"] \\
C_K \arrow[r, two heads] & \mathrm{Cl}_K.
\end{tikzcd}$$

We wish to glue together the local Artin homomorphisms to get a global Artin homomorphism.

Define $\varphi_w : \mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$ by restricting $\sigma \mapsto \sigma|_L$. Then the image of φ_w is just D_w. Because L/K is abelian, D_w only depends on v. Furthermore, $\varphi_w \circ \theta_{L_w/K_v} : K^\times \to \mathrm{Gal}(L/K)$ does not depend on w. This is easy to see in the unramified nonarchimedean case.

Define $i_v : K_v^\times \hookrightarrow \mathbb{I}_K$ sending $\alpha \mapsto (1, \dots, \alpha, \dots, 1)$ at the entry corresponding to v. The image intersects the principal idèles trivially. In addition, i_v commutes with the norm maps $L_w \to K_v$ and $\mathbb{I}_L \to \mathbb{I}_K$.

Now, for a finite abelian extension L/K, define a map

$$\theta_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

mapping

$$(a_v)_v \mapsto \prod_v \phi_w(\theta_{L_w/K_v}(a_v))$$

where we fix a place $w \mid v$ for each v; this does not depend on which w we pick. This product is well-defined, because for unramified (all but finitely many) v, $\phi_w(\theta_{L_w/K_v}(a_v)) = \mathrm{Frob}_v^{v(a_v)}$, which is 1 for all but finitely many a_v.

It is clear that $\theta_{L/K}$ is a group homomorphism. It is also continuous, because its kernel is the union of open sets. In addition, if $L_1 \subseteq L_2$ are two finite abelian extensions of K, then $\theta_{L_1/K}$ is the same as $\theta_{L_2/K}$ composed with $\mathrm{Gal}(L_2/K) \twoheadrightarrow \mathrm{Gal}(L_1/K)$. So we get a unique induced continuous homomorphism

$$\theta_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

12.11.2. Definition. This is called the *global Artin homomorphism*.

12.11.3. Proposition. *The global Artin homomorphism is the unique continuous homomorphism characterized by the property that for any finite abelian L/K, and any place w of L extending v of K, the diagram*

$$\begin{tikzcd}
K_w^\times \arrow[r, "\theta_{L_w/K_v}"] \arrow[d, "i_v"] & \mathrm{Gal}(L_w/K_v) \arrow[d, "\phi_w"] \\
\mathbb{I}_K \arrow[r, "\theta_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

commutes. □

Now we are ready to state the main theorems of the idèle-theoretic formulation of global CFT.

12.11.4. Theorem (global CFT, via idèles)**.** *The global Artin homomorphism θ_K satisfies:*

- *(Artin reciprocity)* $\ker\theta_K$ *contains* $K^\times$*, and the induced map* $\theta_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ *satisfies that for any L/K finite abelian, the induced* $\theta_{L/K} : C_K \to \mathrm{Gal}(L/K)$ *is surjective, with kernel* $\mathrm{N}_{L/K}(C_L)$*.*
- *(Existence theorem) For any finite index open $H \leq C_K$, there exists a unique finite abelian L/K in* K^{ab} *such that* $\mathrm{N}_{L/K}(C_L) = H$*.*
- *(Main theorem) θ_K induces an isomorphism*
$$\widehat{\theta}_K : \widehat{C_K} \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$
- *(Functoriality) For any finite separable L/K, the diagram*
$$\begin{tikzcd} C_L \arrow[r, "\theta_L"] \arrow[d, "\mathrm{N}_{L/K}"] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[d, "\mathrm{res}"] \\ C_K \arrow[r, "\theta_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{tikzcd}$$
commutes.

12.11.5. Remark. There is then an inclusion-reversing bijection

$$\{\text{finite index open subgroups } H \leq C_K\} \longleftrightarrow \{\text{finite abelian extensions } L/K \text{ in } K^{\mathrm{ab}}\}$$

$$H \mapsto (K^{\mathrm{ab}})^{\theta_K(H)}$$
$$\mathrm{N}_{L/K}(C_L) \leftarrow\!\shortmid L.$$

12.11.6. Remark. When K is a number field, θ_K is surjective with kernel he connected component of the identity in $\mathbb{I}_K$. When K is a global function field, θ_K is injective with dense image.

Finally, we state the connection to ideal-theoretic CFT (Theorem 12.1.1). Let $\mathfrak{m} = \prod_v v^{e_v}$ be a modulus for K. Define the group

$$U_K^{\mathfrak{m}}(v) := \begin{cases} \mathcal{O}_v^\times, & \text{for } v \nmid \mathfrak{m} \\ \mathbb{R}_{>0}, & \text{for } v \text{ real, } v \mid \mathfrak{m} \\ 1 + \mathfrak{p}^{e_v}, & \text{for } v \text{ finite, } v \mid \mathfrak{m}, \text{ where } \mathfrak{p} = \{x \in \mathcal{O}_v : |x|_v < 1\}. \end{cases}$$

Let $U_K^{\mathfrak{m}} = \prod_v U_K^{\mathfrak{m}}(v)$, then this is an open subgroup of $\mathbb{I}_K$. Its image $\overline{U}_K^{\mathfrak{m}}$ in C_K is a finite index open subgroup. Define
$$C_K^{\mathfrak{m}} = \mathbb{I}_K/(K^\times U_K^{\mathfrak{m}}) = C_K/\overline{U}_K^{\mathfrak{m}},$$
then it turns out that
$$C_K^{\mathfrak{m}} \cong \mathrm{Cl}_K^{\mathfrak{m}} \cong \mathrm{Gal}(K(\mathfrak{m})/K).$$
The existence of ray class fields $K(\mathfrak{m})$ is then the reincarnation of the existence of a field L such that $\mathrm{N}(C_L) = \overline{U}_K^{\mathfrak{m}}$.

Finally, for a finite abelian L/K, $\mathrm{N}(C_L)$ contains $\overline{U}_K^{\mathfrak{m}}$ for some $\mathfrak{m}$; in fact, the $\overline{U}_K^{\mathfrak{m}}$ forms a neighborhood basis of 1 in C_K, and the smallest $\mathfrak{m}$ for which $\overline{U}_K^{\mathfrak{m}} \subseteq \mathrm{N}(C_L)$ is true is the conductor $\mathfrak{c}(L/K)$. This then shows that L is contained in some ray class field.

13. Cohomological tools

13.1. Dimension shifting. In the next few subsections we develop more cohomological tools to prove local CFT.

To see the connection with cohomology: $\hat{H}^0(G, A) = A^G/N_G(A)$, so taking $A = L^\times$ and $G = \mathrm{Gal}(L/K)$ gives precisely that $\hat{H}^0(\mathrm{Gal}(L/K), L^\times) = K^\times/\,\mathrm{N}(L^\times)$ for any Galois L/K. We will use a theorem of Tate to construct an explicit isomorphism $\mathrm{Gal}(L/K) \cong \hat{H}^0(\mathrm{Gal}(L/K), L^\times)$.

13.1.1. Definition. Let A be a G-module. Define another G-action on $\mathrm{Ind}^G(A)$ and $\mathrm{CoInd}^G(A)$:

$$g(z \otimes a) = gz \otimes ga$$
$$g\varphi = [z \mapsto g\varphi(g^{-1}z)].$$

This only makes sense when A is a G-module (while the usual Ind and CoInd make sense for any abelian group A).

13.1.2. Lemma. *Let A be a G-module, A° the corresponding abelian group by forgetting its G-module structure. Then the maps*

$$\Phi : \mathrm{Ind}^G(A) \to \mathrm{Ind}^G(A^\circ)$$
$$g \otimes a \mapsto g \otimes g^{-1}a$$

and

$$\Psi : \mathrm{CoInd}^G(A) \to \mathrm{CoInd}^G(A^\circ)$$
$$\phi \mapsto [g \mapsto g\phi(g^{-1})]$$

are G-module isomorphisms.

Proof. It is straightforward to check these are G-module homomorphisms. The inverse of the first one is $g \otimes a \mapsto g \otimes ga$, and the second one is its own inverse. □

Recall the augmentation ideal I_G satisfies an exact sequence of G-modules

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

where $\varepsilon : \sum n_g g \mapsto \sum n_g$. As $\mathbb{Z}$-modules, this sequence obviously splits. But the splitting is not a map of G-modules: $\mathbb{Z} \cong \mathbb{Z}1_G$ is not a G-submodule of $\mathbb{Z}[G]$.

13.1.3. Lemma. *Let A be a G-module, then the map*

$$\pi : \mathrm{Ind}^G(A) \to A$$
$$z \otimes a \mapsto \varepsilon(z)a$$

is surjective with kernel $I_G \otimes_{\mathbb{Z}} A$, and the map

$$\iota : A \to \mathrm{CoInd}^G(A)$$
$$a \mapsto [z \mapsto \varepsilon(z)a]$$

is injective with cokernel $\mathrm{Hom}_{\mathbb{Z}}(I_G, A)$*.* □

So we get two short exact sequences of G-modules

$$0 \to I_G \otimes_{\mathbb{Z}} A \to \mathrm{Ind}^G(A) \xrightarrow{\pi} A \to 0$$

and

$$0 \to A \xrightarrow{\iota} \mathrm{CoInd}^G(A) \to \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \to 0.$$

Recall that Ind^G and CoInd^G have trivial (co)homology at $n > 0$, and when G is finite, their Tate cohomologies all vanish (even as H-modules where $H \leq G$ finite index). So we have:

13.1.4. Theorem (dimension shifting)**.** *Let A be a G-module, $H \leq G$ a subgroup of finite index. If G is finite, then for any $n \in \mathbb{Z}$,*

$$\hat{H}^{n+1}(H, A) = \hat{H}^n(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A))$$

and

$$\hat{H}^{n-1}(H, A) = \hat{H}^n(H, I_G \otimes_{\mathbb{Z}} A).$$

When G is any (not necessarily finite) group, this holds for H^n and H_n for $n > 0$.

Using this theorem, one could alternatively *define* Tate (co)homology using only the zeroth Tate cohomology. Dimension shifting gives us theorems about all cohomologies provided we have proven it *in general* for the zeroth.

13.1.5. Proposition. *When G is finite, A any G-module, then $\hat{H}^n(G, A)$ is torsion with exponent dividing $\#G$.*

Proof. By dimension shifting, it suffices to show this for $n = 0$, where $\hat{H}^0(G, A) = A^G/N_G(A)$. But for $a \in A^G$, $N_G a = (\#G)a$, so $\#G$ kills $\hat{H}^0$. □

13.1.6. Corollary. *Let G be finite, A any G-module. If multiplication by $\#G$ is an isomorphism $A \to A$, then A has trivial Tate cohomology.*

In particular, this holds when A is the additive group of a ring and $\#G$ is a unit in it.

Proof. $[\#G]$ then induces isomorphisms on all $\hat{H}^n(G, A)$, but they are all killed by $\#G$, hence trivial. □

13.1.7. Corollary. *Let G be finite, A any finitely generated G-module. Then $\hat{H}^n(G, A)$ is finite for all $n \in \mathbb{Z}$. In particular, the Herbrand quuotient will be defined.*

Proof. It is a finitely generated torsion abelian group, hence finite. □

13.2. Restriction. Recall the functoriality of group (co)homology: a map of G-modules $\phi : A \to B$ induces maps

$$\phi_n : H_n(G, A) \to H_n(G, B), \quad \phi^n : H^n(G, A) \to H^n(G, B).$$

In the other input, if $\varphi : H \to G$ is a group homomorphism, we get a homomorphism from the standard resolution of $\mathbb{Z}$ by H-modules to the standard resolution of $\mathbb{Z}$ by G-modules. This induces maps

$$\varphi_n : H_n(H, \mathrm{Res}^G_H(A)) \to H_n(G, A), \quad \varphi^n : H^n(G, A) \to H^n(H, \mathrm{Res}^G_H(A)).$$

13.2.1. Definition. Let $\varphi : H \to G$ be a group homomorphism, A an H-module, and B a G-module. Suppose $\phi : A \to B$ or $\phi : B \to A$ is a map of H-modules, then we say ϕ is *compatible* with φ.

If $\phi : A \to B$ is compatible with $\varphi : H \to G$, we get homomorphisms

$$H_n(H, A) \xrightarrow{\phi_n} H_n(H, B) \xrightarrow{\varphi_n} H_n(G, B)$$

and if $\phi : B \to A$ then we get

$$H^n(G, B) \xrightarrow{\varphi^n} H^n(H, B) \xrightarrow{\phi^n} H^n(H, A).$$

13.2.2. Definition. Let A be a G-module, $H \leq G$. The morphisms

$$\mathrm{Res} : H^n(G, A) \to H^n(H, A)$$
$$\mathrm{CoRes} : H_n(H, A) \to H_n(G, A)$$

are the above maps induced by $\varphi : H \to G$ and $\phi : A \xrightarrow{\mathrm{id}} A$.

13.2.3. Example. When $n = 0$, $\mathrm{Res} : A^G \to A^H$ is the natural inclusion, and $\mathrm{CoRes} : A_H \to A_G$ is the natural quotient.

13.2.4. Definition. Let A be a G-module, $H \leq G$ of finite index. Fix $S \subseteq G$ a set of left coset representatives for H. Define

$$N_{G/H} := \sum_{s \in S} s \in \mathbb{Z}[G], \quad N^{-1}_{G/H} := \sum_{s \in S} s^{-1} \in \mathbb{Z}[G].$$

Define a restriction map on homology by

$$\mathrm{Res} : H_0(G, A) \to H_0(H, A)$$
$$a + I_G A \mapsto N^{-1}_{G/H} a + I_H A$$

It is easy to check that this does not depend on the set of representatives we choose, and for $\alpha : A \to B$ a map of G-modules, the diagram

$$\begin{tikzcd} H_0(G, A) \arrow[r, "\alpha_0"] \arrow[d, "\mathrm{Res}"] & H_0(G, B) \arrow[d, "\mathrm{Res}"] \\ H_0(H, A) \arrow[r, "\alpha_0"] & H_0(H, B) \end{tikzcd}$$

commutes.

If G is finite, then $\operatorname{Res}(\ker \hat{N}_G) \subseteq \ker \hat{N}_H$, so we have an induced map

$$\hat{H}_0(G,A) \to \hat{H}_0(H,A).$$

Similarly, define the corestriction for cohomology

$$\begin{aligned} \operatorname{CoRes}: H^0(H,A) &\to H^0(G,A) \\ a &\mapsto N_{G/H}a \end{aligned}$$

and it is also functorial and does not depend on the coset representatives S.

Now, we extend Res to higher homologies. From the long exact sequence for $0 \to I_G \otimes_{\mathbb{Z}} A \to \operatorname{Ind}^G(A) \to A \to 0$, we can uniquely extend

$$\begin{tikzcd} 0 \arrow[r] & H_1(G,A) \arrow[r] \arrow[d, dashed, "\exists!"] & H_0(G, I_G \otimes_{\mathbb{Z}} A) \arrow[r] \arrow[d, "\operatorname{Res}"] & H_0(G, \operatorname{Ind}^G(A)) \arrow[r] \arrow[d, "\operatorname{Res}"] & 0 \\ 0 \arrow[r] & H_1(H,A) \arrow[r] & H_0(H, I_G \otimes_{\mathbb{Z}} A) \arrow[r] & H_0(H, \operatorname{Ind}^G(A)) \arrow[r] & 0 \end{tikzcd}$$

and similarly dimension shifting gives maps $\operatorname{Res}: H_n(G,A) \to H_n(H,A)$.

Similarly, we get $\operatorname{CoRes}: H^n(H,A) \to H^n(G,A)$. Restriction and corestriction are transitive and δ-functorial.

13.2.5. Proposition. *Let A be a G-module, $H \leq G$ fintie index, then* $\operatorname{CoRes} \circ \operatorname{Res}$ *is multiplication by $[G:H]$ on $H_n(G,A)$ and $H^n(G,A)$ (and all $\hat{H}^n(G,A)$ when G is finite).*

PROOF. Prove this for $n=0$, and use dimension shifting. □

13.3. Inflation.

13.3.1. Definition. Let A be a G-module, $H \lhd G$. Then A^H, A_H are trivial H-modules, hence G/H-modules. Then the map induced by $\varphi: G \to G/H$ and $\phi: A^H \to A$ is the *inflation*

$$\operatorname{Inf}: H^n(G/H, A^H) \to H^n(G,A)$$

and the map induced by $\varphi: G \to G/H$ and $\phi: A \to A_H$ is the *coinflation*

$$\operatorname{CoInf}: H_n(G,A) \to H_n(G/H, A_H).$$

These are also δ-functorial.

13.3.2. Example. In degree $n=0$, Inf and CoInf are just the identity maps on A_G and A^G.

13.3.3. Example. Let $f: G^n \to A$ be a n-cochain representing $\gamma \in H^n(G,A)$. Then $\operatorname{Res}(\gamma) \in H^n(H,A)$ is represented by the restriction of f to H^n.

Let $f: (G/H)^n \to A$ be a n-cochain representing $\gamma \in H^n(G/H,A)$. Then $\operatorname{Inf}(\gamma) \in H^n(G,A)$ is given by composing f with the projection $G^n \to (G/H)^n$.

13.3.4. Theorem (inflation-restriction theorem)**.** *Let A be a G-module, $H \lhd G$, $n \geq 1$. If $H^i(H,A) = 0$ for $1 \leq i \leq n-1$, then*

$$0 \to H^n(G/H, A^H) \xrightarrow{\operatorname{Inf}} H^n(G,A) \xrightarrow{\operatorname{Res}} H^n(H,A)$$

is exact.

PROOF. Use induction on n.

In the base case $n=1$, everything can be written down explicitly. Let $f: G/H \to A^H$ be a 1-cochain representing $\gamma \in \ker \operatorname{Inf}$. Since f composed with $G \to G/H$ must be of form $[g \mapsto ga - a]$ for some $a \in A^H$, f itself must be given by $[\overline{g} \mapsto \overline{g}a - a]$, so it is a coboundary, so $\gamma = 0$. Next, since $H \to G \to G/H$ is trivial, $\operatorname{im} \operatorname{Inf} \subseteq \ker \operatorname{Res}$. To show equality, let $f: G \to A$ be a 1-cochain representing $\gamma \in \ker \operatorname{Res}$. Then on H, f must act as $[h \mapsto ha - a]$ for some $a \in A$. Define $\overline{f}: G \to A$ by $g \mapsto f(g) - ga + a$, then $\overline{f}$ vanishes on H, so

$$\overline{f}(gh) = g\overline{f}(h) + \overline{f}(g) = \overline{f}(g)$$

and

$$\overline{f}(hg) = h\overline{f}(g) + \overline{f}(h) = h\overline{f}(g).$$

The first equation tells us that $\overline{f}$ factors through G/H, and the second tells us that the image of $\overline{f}$ is H-invariant. So $\overline{f}$ gives an element in $H^1(G/H, A^H)$ whose inflation is f. This shows the case $n = 1$.

Now the induction step. Assume this holds for n (for all G, H, A), and we show this for $n+1$. By dimension shifting, if A satisfies the hypothesis for $n+1$, then $\mathrm{Hom}_{\mathbb{Z}}(I_G, A)$ satisfies the hypothesis for n. By inductive hypothesis,

$$0 \to H^n(G/H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H) \xrightarrow{\mathrm{Inf}} H^n(G, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \xrightarrow{\mathrm{Res}} H^n(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A))$$

is exact. By dimension shifting again,

$$0 \to H^{n+1}(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^{n+1}(G, A) \xrightarrow{\mathrm{Res}} H^{n+1}(H, A)$$

is exact. □

13.3.5. Remark. There is an analogous theorem for CoRes and CoInf:

$$H_n(H, A) \xrightarrow{\mathrm{CoRes}} H_n(G, A) \xrightarrow{\mathrm{CoInf}} H_n(G/H, A_H) \to 0$$

is exact, if $H_i(H, A) = 0$ for $1 \le i \le n-1$.

13.4. Tate's theorem.

13.4.1. Theorem. *Let A be a G-module, where G is finite. Suppose for all $H \le G$, we have $H^1(H, A) = H^2(H, A) = 0$. Then $\hat{H}^n(G, A) = 0$ for all $n \in \mathbb{Z}$.*

Proof. For G cyclic, this is clear since Tate cohomology is periodic with period 2.

For G solvable, let $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_m = G$ be the shortest possible subnormal series, such that all consecutive quotients are cyclic. Proceed by induction on m, with the base case clear. Let $H \neq G$ be a normal subgroup of G such that G/H is cyclic, then by induction hypothesis, $\hat{H}^n(H, A) = 0$ for all $n \in \mathbb{Z}$.

By the inflation-restriction theorem, we have $H^n(G/H, A^H) \cong H^n(G, A)$ for $n \ge 1$ (since $H^n(H, A) = \hat{H}^n(H, A) = 0$). So $H^1(G/H, A^H) = H^2(G/H, A^H) = 0$, and consequently for all $n \in \mathbb{Z}$, $\hat{H}^n(G/H, A^H) = 0$. This implies that $H^n(G, A) = 0$ for all $n \ge 1$, and also

$$0 = \hat{H}^0(G/H, A^H) = (A^H)^{G/H}/N_{G/H}(A^H).$$

Combine this with $0 = \hat{H}^0(H, A) = A^H/N_H(A)$, we have

$$A^G = (A^H)^{G/H} = N_{G/H}(A^H) = N_{G/H}(N_H(A)) = N_G(A),$$

so $\hat{H}^0(G, A) = 0$. Since this holds for general A, we may use dimension shifting to address $n < 0$: since $\hat{H}^{n-1}(H, A) = \hat{H}^n(H, I_G \otimes_{\mathbb{Z}} A)$, the hypothesis $H^1(H, I_G \otimes_{\mathbb{Z}} A) = H^2(H, I_G \otimes_{\mathbb{Z}} A) = 0$ holds, so $\hat{H}^{-1}(G, A) = \hat{H}^0(G, I_G \otimes_{\mathbb{Z}} A) = 0$, and repeating this proves that $\hat{H}^n(G, A) = 0$ for all $n \in \mathbb{Z}$.

In general, suppose G is not necessarily solvable. Let H be a Sylow p-subgroup of G, then H is solvable. Consider the composition

$$H^n(G, A) \xrightarrow{\mathrm{Res}} H^n(H, A) \xrightarrow{\mathrm{CoRes}} H^n(G, A)$$

which is multiplication by $(G : H)$, a number coprime to p. But for $n \ge 1$, this is also the zero map since the middle group is zero. So $H^n(G, A)$ has no elements of order p. Since this is for any p, we conclude $\hat{H}^n(G, A) = 0$ for $n \ge 1$. For $n = 0$, since $\hat{H}^0(H, A) = 0$, the map $N_H : A \to A^H$ is surjective, so for any $a \in A^G \subset A^H$, there exists $a' \in A$ such that $a = \sum_{h \in H} ha'$, so $N_G(a') = [G : H]a$. This shows that multiplication by $[G : H]$ kills $\hat{H}^0(G, A)$ as well, so it has no elements of order p, and since this is for any p we conclude $\hat{H}^0(G, A) = 0$. Finally, for $n < 0$, again use the same dimension shifting argument as in the solvable case. □

13.4.2. Theorem (Tate's theorem)**.** *Let A be a G-module where G finite, and suppose for every $H \le G$, $H^1(H, A) = 0$ and $H^2(H, A)$ is cyclic with order equal to $\#H$. For any generator γ of $H^2(G, A)$ and all $n \in \mathbb{Z}$, there is a uniquely determined isomorphism*

$$\Phi_\gamma : \hat{H}^n(G, \mathbb{Z}) \to \hat{H}^{n+2}(G, A)$$

compatible with Res *and* CoRes*.*

Tate's theorem is the keystone of the proof of local Artin reciprocity, so we will walk through the proof carefully.

Proof of Tate's theorem 13.4.2. Let φ be a 2-cocycle in $C^2(G,A)$ representing $\gamma \in H^2(G,A)$. Let $A(\varphi)$ be the G-module

$$A(\varphi) = A \bigoplus_{g \in G - \{1\}} \mathbb{Z}g,$$

where G acts on A as usual and $gx_h := x_{gh} - x_g + \varphi(g,h)$, where x_g is the generator for the $\mathbb{Z}g$ component for $g \neq 1$, and $x_1 := \varphi(1,1) \in A$. It is easy to check that this is a G-action:

$$\begin{aligned} g_1(g_2x_h) - (g_1g_2)x_h &= g_1(x_{g_2h} - x_{g_2} + \varphi(g_2,h)) - x_{g_1g_2h} + x_{g_1g_2} - \varphi(g_1g_2,h) \\ &= g_1\varphi(g_2,h) - \varphi(g_1g_2,h) + \varphi(g_1,g_2h) - \varphi(g_1,g_2) \\ &= (d\varphi)(g_1,g_2,h) = 0, \end{aligned}$$

since φ is a cocycle.

Now, by definition, the 2-cocycle $\varphi : G^2 \to A \xrightarrow{i} A(\varphi)$ is the coboundary of the 1-cochain

$$\psi = [g \mapsto x_g] \in C^1(G, A(\varphi)),$$

since

$$(d\psi)(g,h) = gx_h - x_{gh} + x_g = \varphi(g,h).$$

So γ lies in the kernel of the map

$$i^2 : H^2(G,A) \to H^2(G,A(\varphi)).$$

But since γ generates $H^2(G,A)$, we conclude that i^2 is the zero map.

Now define a morphism of G-modules $\phi : A(\varphi) \to \mathbb{Z}[G]$ sending $a \mapsto 0$ for $a \in A$ and sending $x_g \mapsto g - 1$ (it is easy to check this is G-equivariant). Note that $\ker \phi = A$ and $\operatorname{im} \phi = I_G$, so we have a short exact sequence of G-modules

$$(*) \qquad 0 \to A \xrightarrow{i} A(\varphi) \to I_G \to 0.$$

In particular, for each $H \leq G$, this is a short exact sequence of H-modules. We also have our usual short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

Consider its long exact sequence of Tate cohomology. Because $\hat{H}^n(H,\mathbb{Z}[G]) = 0$ for all n, we have $\hat{H}^n(H,\mathbb{Z}) \cong \hat{H}^{n+1}(H,I_G)$. In particular:

- $H^2(H,I_G) = H^1(H,\mathbb{Z}) = \mathrm{Hom}_{\mathrm{Ab}}(H,\mathbb{Z})$ (this can be seen using cochains and the fact that $\mathbb{Z}$ is a trivial H-module), but this is zero because H is finite;
- $H^1(H,I_G) = \hat{H}^0(H,\mathbb{Z}) = \mathbb{Z}^H/N_H\mathbb{Z} = \mathbb{Z}/(\#H)$.

Now, we can write down the long exact sequence of Tate cohomology of $(*)$:

$$H^1(H,A) \xrightarrow{i^1} H^1(H,A(\varphi)) \xrightarrow{\phi^1} H^1(H,I_G) \xrightarrow{\delta^1} H^2(H,A) \xrightarrow{i^2} H^2(H,A(\varphi)) \xrightarrow{\phi^2} H^2(H,I_G)$$

which, given our current information, is

$$0 \xrightarrow{i^1} H^1(H,A(\varphi)) \xrightarrow{\phi^1} H^1(H,I_G) \xrightarrow{\delta^1} \mathbb{Z}/(\#H) \xrightarrow{i^2} H^2(H,A(\varphi)) \xrightarrow{\phi^2} 0.$$

Now, since i^2 is the zero map, $H^2(H,A(\varphi)) = 0$, so δ^1 is surjective. But since $H^1(H,I_G) \cong \mathbb{Z}/(\#H)$, we conclude that δ^1 is an isomorphism, and $H^1(H,A(\varphi)) = 0$.

By theorem 13.4.1, we conclude that $\hat{H}^n(G,A(\varphi)) = 0$ for all $n \in \mathbb{Z}$. Therefore, we have isomorphisms $\hat{H}^n(G,I_G) \cong \hat{H}^{n+1}(G,A)$. So we have isomorphisms

$$\Phi_\gamma : \hat{H}^n(H,\mathbb{Z}) \cong \hat{H}^{n+1}(G,I_G) \cong \hat{H}^{n+2}(G,A).$$

Furthermore, the first map is canonical, and the second map only depends on γ (choosing a different φ does not change any of the maps in cohomology). Since Res and CoRes are both morphisms of δ-functors, they commute with both maps. This concludes the proof. □

13.5. Continuous cohomology. Let us switch gears to developing more cohomology theory, this time for profinite (more generally, topological) groups, taking the topology into account.

13.5.1. Definition. Let G be a topological group. A *topological G-module* (or *continuous G-module*) is an abelian topological group A on which G acts continuously, i.e. $G \times A \to A$ is continuous. A *discrete G-module* A is a topological G-module such that A carries the discrete topology. A *morphism of topological G-modules* is a map of topological abelian groups compatible with the G-action.

In general, there are several inequivalent ways to define cohomology for topological G-modules. But we are only interested in the case where G is profinite and A is discrete, and in this case there is a natural choice, namely *continuous cohomology.*

Consider the *continuous* n-cochains $C^n(G, A)$, consisting of continuous maps $G^n \to A$. This forms an abelian group. Consider the continuous cochain complex, and it is easy to see that the coboundary of a continuous cochain is necessarily continuous as well. So we may define $H^n(G, A)$ to be the cohomology groups of the continuous cochain complex. Note that $H^0(G, A) = A^G$. To distinguish this from usual group cohomology, this is also denoted $H^n_c(G, A)$ or $H^n_{\text{cts}}(G, A)$.

Let $A \to B$ be a morphism of topological G-modules. We then get induced maps $C^n(G, A) \to C^n(G, B)$, hence $H^n(G, A) \to H^n(G, B)$. But warning! This is not necessarily a cohomological δ-functor. But it is, in the case we are interested in (G profinite and A discrete). This also makes sense, because the more connected G is, the harder it is for a cochain to be continuous, and profinite groups are totally disconnected.

13.5.2. Lemma. *Let G be a compact group, A a G-module, then the following are equivalent:*

(i) A is a discrete G-module;
(ii) For every $a \in A$, $\operatorname{Stab}(a)$ is open;
(iii) $A = \bigcup A^H$, where H ranges among open normal subgroups of G.

Proof. (i) $\implies$ (ii) is clear.

(ii) $\implies$ (iii): Let $a \in A$, then $\operatorname{Stab}(a)$ is open. Since G is compact, $\operatorname{Stab}(a)$ has finite index, hence finitely many conjugates; their intersubsection is an open normal subgroup H that fixes a.

(iii) $\implies$ (i): For each $a \in A$, it is fixed by some open normal $H \lhd G$. Then for $\pi : G \times A \to A$, $\pi^{-1}(a)$ is the union of open sets $Ng \times \{b\}$ where $gb = a$, hence open. □

In general, (i) and (ii) are equivalent even when G is not compact.

13.5.3. Lemma. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of discrete G-modules, then the induced*

$$0 \to C^n(G, A) \to C^n(G, B) \to C^n(G, C) \to 0$$

is exact for all n.

Warning: this does not hold for *topological* G-modules in general (right-exactness may fail)!

13.5.4. Theorem. *Every short exact sequence of discrete G-modules $0 \to A \to B \to C \to 0$ induces a long exact sequence in continuous cohomology*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to \dots$$

and commutative diagrams induce commutative diagrams.

13.6. Cohomology of profinite groups.

13.6.1. Definition. Let G be a group, and $H \lhd K$ be two subgroups normal in G. We can view K/H as a normal subgroup of G/H, and so we get an inflation map

$$\operatorname{Inf} : H^n(G/K, A^K) \to H^n(G/H, A^H).$$

This is compatible with towers of inclusions $H \lhd K \lhd L$, all normal in G.

For any profinite group

$$G = \varprojlim_{N \lhd G \text{ open}} G/N,$$

the inflation maps give us a direct system of $H^n(G/N, A^N)$.

13.6.2. Theorem. *Let G be a profinite group, then for every discrete G-module A and $n \geq 0$,*

$$H^n(G,A) \cong \varinjlim_{N \lhd G \text{ open}} H^n(G/N, A^N).$$

Proof. Direct limits are exact in the category of modules over a ring, in particular in Ab. So it suffices for us to show that the natural map

$$\varphi : \varinjlim_{N \lhd G \text{ open}} C^n(G/N, A^N) \to C^n(G,A)$$

is a bijection, where for $H \lhd K$, $C^n(G/K, A^K) \to C^n(G/H, A^H)$ is given by composing a continuous cochain $(G/K)^n \to A^K$ with the quotient map $(G/H)^n \to (G/K)^n$ and the map $A^K \hookrightarrow A^H$.

It is clear that φ is injective. To show it is surjective, let $f : G^n \to A$ be a continuous cochain. Then since G is compact, so is $\operatorname{im} f$. Since it is also discrete, it is finite. So the stabilizer of $\operatorname{im} f$ is open, and intersecting it with its conjugates gives an open normal subgroup $N_1 \lhd G$, such that $\operatorname{im} f \subseteq A^{N_1}$. For any $a \in \operatorname{im} f$, $f^{-1}(a)$ is open in G^n, so it contains a product of n open sets in G, each of which contains some open normal subgroup, and intersecting them gives an open normal N_a, so that $f(N_a^n) = a$. Finally, let $N = N_1 \bigcap_{a \in \operatorname{im} f} N_a$, then f induces a continuous cochain $(G/N)^n \to A^N$. □

13.6.3. Corollary. *For every profinite G and discrete G-module A, $H^n(G,A)$ is torsion for all $n \geq 0$.*

Proof. By proposition 13.1.5, each $H^n(G/N, A^N)$ is torsion. The direct limit of torsion abelian groups is torsion as well. □

13.6.4. Corollary (Hilbert 90 for infinite extension)**.** *Let L/K be any (not necessarily finite) Galois extension, then $H^1(\mathrm{Gal}(L/K), L^\times)$ is trivial.*

Proof. Follows from lemma 12.7.2. □

13.6.5. Theorem. *Let G be profinite, and suppose A is a direct limit of discrete G modules A_i. Then A is a discrete G-module, and*

$$H^n(G,A) \cong \varinjlim_i H^n(G, A_i)$$

for all $n \geq 0$.

Proof. Every $a \in A$ is represented by some $a_i \in A_i$, so its stabilizer is open. This shows that A is a discrete G-module. As before, since direct limits are exact in Ab, it suffices to show the natural map

$$\varphi : \varinjlim_i C^n(G, A_i) \to C^n(G,A)$$

is an isomorphism. It is clearly injective. To show surjectivity, let $f : G^n \to A$ be a continuous cochain. It has finite image since the image is compact and discrete. So there exists i such that $\operatorname{im} f \subseteq A_i$ (recall that in the definition of directed limits, i ranges in a directed set I, so upper bounds always exist). Then f induces a continuous cochain $G^n \to A_i$. This shows surjectivity. □

13.6.6. Definition. Let $\varphi : G \to G'$ be a continuous homomorphism of profinite groups, A a continuous G-module, A' a continuous G'-module. Then a continuous map $\phi : A \to A'$ or $\phi : A' \to A$ is *compatible* with φ if it commutes with the G-action.

We can similarly define Res and Inf for profinite groups G and discrete G-modules; equivalently, one could define them as direct limits of the maps defined for finite quotients of G. Because direct limits are exact, we get:

13.6.7. Theorem (inflation-restriction for profinite groups)**.** *Let H be a closed normal subgroup of a profinite group G. Let A be a discrete G-module, and let $n \geq 1$. If $H^i(H,A) = 0$ for $1 \leq i \leq n-1$, then*

$$0 \to H^n(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^n(G,A) \xrightarrow{\mathrm{Res}} H^n(H,A)$$

is exact.

13.6.8. Remark. As in infinite Galois theory, we need H to be closed because we require it to be profinite; a subgroup of a profinite group is profinite iff it is closed. This follows immediately from the fact that a topological group is profinite iff it is totally disconnected, compact and Hausdorff. Every subset of a totally disconnected space is totally disconnected, but a subset of a compact Hausdorff space is compact Hausdorff iff it is closed.

13.6.9. Remark. What cannot be extended to the discrete G-module case? When G is infinite, $\mathbb{Z}[G]$ will not be a discrete G-module! This makes it hard to define homology and Tate cohomology directly, but one can work around this by taking an inverse limit of quotients of G by open normal subgroups.

14. Local class field theory: Proof

14.1. The invariant map: unramified case. With our cohomological tools in place, let us return to local CFT. Let K be a nonarchimedean local field, L/K Galois (not necessarily finite). Then $G = \mathrm{Gal}(L/K)$ is profinite and $L^\times$ and $\mathcal{O}_L^\times$ are discrete G-modules (any $\alpha \in L^\times$ generates a finite extension $K(\alpha)/K$ that is the fixed field of a finite index closed subgroup, which is open).

We first do the finite unramified case:

14.1.1. Theorem. *Let L/K be finite unramified, then $\hat{H}^n(G, \mathcal{O}_L^\times) = 0$ for all $n \in \mathbb{Z}$. Moreover, for any subgroup $H \leq G$, $\hat{H}^n(H, \mathcal{O}_L^\times) = 0$ for all $n \in \mathbb{Z}$.*

Proof. Since G is then cyclic, it suffices to prove this for $n = 0, 1$. For any uniformizer π for $\mathcal{O}_L$, $L^\times \cong \mathcal{O}_L^\times \times \mathbb{Z}$ by $x \mapsto (\frac{x}{\pi^{v_L(x)}}, v_L(x))$. Since L/K is unramified, v_L extends v_K with index 1, so we can pick π to be a uniformizer of $\mathcal{O}_K$. Then G acts trivially on the $\mathbb{Z}$ component in $\mathcal{O}_L$. Then for every n,

$$\hat{H}^n(G, L^\times) \cong \hat{H}^n(G, \mathcal{O}_L^\times) \oplus \hat{H}^n(G, \mathbb{Z}).$$

By Hilbert 90, $H^1(G, L^\times) = 0$, so $\hat{H}^1(G, \mathcal{O}_L^\times) = 0$. So we focus on the degree 0 case, where $\hat{H}^0(G, \mathcal{O}_L^\times) = \mathcal{O}_K^\times / \mathrm{N}(\mathcal{O}_L^\times)$. So it suffices to show that the norm hits every element in $\mathcal{O}_K^\times$.

Let $\mathfrak{p}, \mathfrak{q}, k, \ell$ be the maximal ideals and the residue fields of K, L. Let $U_K^r = 1 + \mathfrak{p}^r$ and $U_L^r = 1 + \mathfrak{q}^r$ be subgroups of $\mathcal{O}_K^\times$ and $\mathcal{O}_L^\times$, so that $U_L^0/U_L^1 \cong \ell^\times$ and $U_L^i/U_L^{i+1} \cong \ell$ for $i \geq 1$. Now, since $G = \mathrm{Gal}(\ell/k)$, by Hilbert 90, $H^1(G, \ell^\times) = 0$. Since $\ell^\times$ is finite, its Herbrand quotient $h^0(\ell^\times)/h_0(\ell^\times) = 1$ (cf. Corollary 12.6.4). Consequently, $k^\times / \mathrm{N}(\ell^\times) = \hat{H}^0(G, \ell^\times) = 0$, so the norm map on residue fields is surjective. By Lemma 12.7.2, $k/\mathrm{Tr}(\ell) = \hat{H}^0(G, \ell) = 0$, so the trace map on residue fields is surjective as well.

I claim that these are sufficient to imply that $\mathrm{N}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$. Suppose we are given $u \in \mathcal{O}_K^\times$. By the commutative diagram

$$\begin{tikzcd}
\mathcal{O}_L^\times \arrow[r, "\bmod \mathfrak{q}"] \arrow[d, "\mathrm{N}"] & \mathcal{O}_L^\times/U_L^1 \cong \ell^\times \arrow[d, "\mathrm{N}"] \\
\mathcal{O}_K^\times \arrow[r, "\bmod \mathfrak{p}"] & \mathcal{O}_K^\times/U_K^1 \cong k^\times,
\end{tikzcd}$$

we may pick $v_1 \in \mathcal{O}_L^\times$ such that the norm of the image of v_1 in $\ell^\times$ is the image of u in $k^\times$. This implies that $u/\mathrm{N}(v_1) \in U_K^1$. By the commutative diagram

$$\begin{tikzcd}
U_L^1 \arrow[r] \arrow[d, "\mathrm{N}"] & U_L^1/U_L^2 \cong \ell \arrow[d, "\mathrm{Tr}"] \\
U_K^1 \arrow[r] & U_K^1/U_K^2 \cong k,
\end{tikzcd}$$

we may pick $w_2 \in U_L^1$ such that $\mathrm{N}(w_2) \equiv u/N(v_1)$ modulo U_K^2. Taking $v_2 = w_2 v_1$, we see that $u/\mathrm{N}(v_2) \in U_K^2$. We may repeat this process with $U_L^2, U_L^3, \ldots$, and since these form a Cauchy sequence in $\mathcal{O}_L^\times$, they approach a limit v (because L is complete). Then $u/\mathrm{N}(v)$ lies in every U_K^i, hence equals 1. This concludes the proof that $\hat{H}^n(G, \mathcal{O}_L^\times) = 0$ for all $n \in \mathbb{Z}$.

For any subgroup $H \leq G$, $H = \mathrm{Gal}(L/L^H)$. So we may just apply the above to the extension L/L^H. □

In the proof, we have shown the following:

14.1.2. Corollary. *Let L/K be finite unramified, then the norm map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.* □

14.1.3. Corollary. *Let L/K be unramified (not necessarily finite). Then $H^n(G, \mathcal{O}_L^\times) = 0$ for $n > 0$.*

Proof. For any open normal subgroup $N \lhd G$, the fixed field L^N is a finite unramified extension, with $\mathrm{Gal}(L^N/K) \cong G/N$, and $\hat{H}^n(G/N, (\mathcal{O}_L)^N) = 0$. For $n > 0$, taking the direct limit gives $H^n(G, \mathcal{O}_L^\times) = 0$ (theorem 13.6.2). □

Now for L/K unramified, consider the exact sequence of discrete G-modules

$$0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0,$$

then by what we proved above, $H^2(G, L^\times) \cong H^2(G, \mathbb{Z})$. Now consider the exact sequence of trivial G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Since $\#(G/N)$ is a unit in $\mathbb{Q}$ for every open normal $N \lhd G$, $H^n(G, \mathbb{Q}) = \varinjlim H^n(G/N, \mathbb{Q}) = 0$ for $n > 0$ (corollary 13.1.6). So

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z}).$$

Since $\mathbb{Q}/\mathbb{Z}$ is a trivial G-module, $H^1(G, \mathbb{Q}/\mathbb{Z})$ just consists of continuous homomorphisms of abelian groups $G \to \mathbb{Q}/\mathbb{Z}$.

Now, consider the Frobenius element $\sigma \in G$ that restricts to the Frobenius element $\mathrm{Frob}_{M/K}$ in any finite extension M/K in L.

14.1.4. Definition. The *invariant map* is defined by the composition

$$\mathrm{inv}_{L/K} : H^2(G, L^\times) \to H^2(G, \mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}.$$

Note that this is very canonical. In particular, it is functorial in L in the sense that for $K \subseteq M \subseteq L$ unramified,

$$\begin{tikzcd} H^2(\mathrm{Gal}(M/K), M^\times) \arrow[rr, "\mathrm{Inf}"] \arrow[dr, "\mathrm{inv}_{M/K}"'] & & H^2(\mathrm{Gal}(L/K), L^\times) \arrow[dl, "\mathrm{inv}_{L/K}"] \\ & \mathbb{Q}/\mathbb{Z} & \end{tikzcd}$$

commutes.

14.1.5. Theorem. *The invariant map $\mathrm{inv}_K := \mathrm{inv}_{K^{\mathrm{unr}}/K}$ is the unique isomorphism*

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z},$$

such that for any finite unramified L/K in K^{unr}, composing with the inflation map gives isomorphisms

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

Proof. For any unramified L/K (not necessarily finite), σ is a topological generator, so $\mathrm{inv}_{L/K}$ is always injective.

For any finite unramified L/K, $G = \mathrm{Gal}(L/K)$, we have a cochain $f \in H^1(G, \mathbb{Q}/\mathbb{Z})$ mapping $\mathrm{Frob}_{L/K} \mapsto \frac{1}{[L:K]}$, so the image of inv contains $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. But this must be an equality, since $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z}) \cong \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/(\#G)$. So $\mathrm{inv}_{L/K}$ is an isomorphism onto $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. Now, since K^{unr} contains unramified extensions of every degree, $\mathrm{inv}_{K^{\mathrm{unr}}/K}$ is surjective. So it is an isomorphism. It remains to show that $\mathrm{inv}_K := \mathrm{inv}_{K^{\mathrm{unr}}/K}$ is unique. This is just because

$$H^2(G, K^{\mathrm{unr}\,\times}) \cong \varinjlim_{H \lhd G \text{ open}} H^2(G/H, (K^{\mathrm{unr}\,\times})^H),$$

where $G = \mathrm{Gal}(K^{\mathrm{unr}}/K)$, and knowing that inv_K restricts to $\mathrm{inv}_{L/K}$ already determines inv_K. □

14.2. The invariant map: general case. Now we have to figure out how to deal with ramification.

14.2.1. Proposition. *Let L/K be a finite extension, not necessarily unramified and not necessarily Galois. There is a canonical homomorphism ϕ that makes*

$$\begin{tikzcd}
H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) \arrow[r, "\phi"] \arrow[d, "\mathrm{inv}_K"'] & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commute. When L/K is Galois, we may identify $\ker\phi$ with a subgroup of $H^2(\mathrm{Gal}(L/K), L^\times)$ isomorphic to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Proof. Note that L^{unr} is just the compositum $L\cdot K^{\mathrm{unr}}$ since finite unramified extensions are constructed by adjoining appropriate roots of unity.

By Hilbert 90, $H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}) = 0$. Suppose L/K is Galois, then by inflation-restriction, there is an exact sequence

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\mathrm{Inf}} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/K), L^{\mathrm{unr}\,\times}) \xrightarrow{\mathrm{Res}} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}).$$

Similarly, since $H^1(\mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}}), L^{\mathrm{unr}\,\times}) = 0$, there is an exact sequence

$$0 \to H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) \xrightarrow{\mathrm{Inf}'} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/K), L^{\mathrm{unr}\,\times}) \xrightarrow{\mathrm{Res}'} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}}), L^{\mathrm{unr}\,\times}).$$

Now, define $\phi : \mathrm{Res}\circ\mathrm{Inf}'$. Note that this is defined even when L/K is not Galois. But when it is, there exists an induced injection $\ker\phi \to H^2(\mathrm{Gal}(L/K), L^\times)$.

Now we drop the condition that L/K is Galois. Then the discrete valuation v_L extends v_K with index $e = e_{L/K}$. Let σ_K, σ_L be the arithmetic Frobenii of K and L, and $f = f_{L/K}$ be the inertia degree, so that $[L:K] = ef$. Writing out the maps defining inv_K and inv_L:

$$\begin{tikzcd}
H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) \arrow[r] \arrow[d, "\phi"] & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Z}) \arrow[r] \arrow[d] & H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "{[e]\circ\phi}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}) \arrow[r] & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Z}) \arrow[r] & H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Q}/\mathbb{Z}) \arrow[r] & \mathbb{Q}/\mathbb{Z},
\end{tikzcd}$$

where the leftmost square is induced by

$$\begin{tikzcd}
K^{\mathrm{unr}\,\times} \arrow[r, "v_K"] \arrow[d, hook] & \mathbb{Z} \arrow[d, "{[e]}"] \\
L^{\mathrm{unr}\,\times} \arrow[r, "v_L"] & \mathbb{Z},
\end{tikzcd}$$

the middle square is just a pair of isomorphisms, and the right square is commutative because given any cochain $g : \mathrm{Gal}(L^{\mathrm{unr}}/L) \to \mathbb{Q}/\mathbb{Z}$ (homomorphism of abelian groups), $g(\sigma_L) = g(\sigma_K^f) = f \cdot g(\sigma_K)$. Finally, having argued that the diagram is commutative, it is then clear that $\ker\phi$ is isomorphic to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, the kernel of the rightmost map. □

To extend the invariant map to arbitrary separable extensions, we first prove what Neukirch calls the *class field axiom*:

14.2.2. Theorem (class field axiom)**.** *Let L/K be a cyclic extension of nonarchimedean local fields, and $G = \mathrm{Gal}(L/K)$ has order n. Then $\#\hat{H}^k(G, L^\times) = n$ when k is even, and 1 when k is odd.*

Proof. Since G is cyclic, it suffices to show this for $k = 0, 1$. By Hilbert 90, $\hat{H}^1(G, L^\times)$ is trivial. So it remains to show $\hat{H}^0(G, L^\times)$ has cardinality n. Consider the exact sequence

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0.$$

Then $h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z})$. By corollary 12.6.5, $h(\mathbb{Z}) = n$. Since $\#\hat{H}_0(L^\times) = \#\hat{H}^1(L^\times) = 0$, it suffices to show that $h(\mathcal{O}_L^\times) = 1$. By corollary 12.6.7 it suffices to find a finite-index G-submodule $A \subset \mathcal{O}_L^\times$ with trivial Tate cohomology groups.

Let $\mathfrak{p}, \mathfrak{q}$ be the maximal ideals of $\mathcal{O}_K, \mathcal{O}_L$, with uniformizers π, ϖ. Let σ generate G. By normal basis theorem 1.7.6, choose $\alpha \in L^\times$ such that $\{\sigma^i\alpha\}$ forms a K-basis of L. Write $\alpha = \beta/\gamma$ where $\beta, \gamma \in \mathcal{O}_L$, then $v_i = \mathrm{N}_{L/K}(\gamma)\sigma^i\alpha \in \mathcal{O}_L$. Take $z_j \in L^\times$ to be the dual basis of v_i, so that $\mathrm{Tr}_{L/K}(z_j v_i) = \delta_{ij}$. Then one can easily see $z_j = \sigma^j z_0$. Again, scale z_0 by an element of $\mathcal{O}_K$ so that z_j lie in $\mathcal{O}_L$; we may also assume they have arbitrarily small absolute value, by scaling by a big power of ϖ, say ϖ^m. Let

$$M = \bigoplus_i z_i \mathcal{O}_K \subset \mathcal{O}_L.$$

This is a G-submodule of $\mathcal{O}_L$ isomorphic to $\mathcal{O}_K[G]$. Also by, say, Atiyah–MacDonald proposition 5.17, a multiple of $\mathcal{O}_L$ sits inside M, so M has finite index in $\mathcal{O}_L$.

Now, to construct A, there are two ways. The easy way is to take $A = \exp(M)$, where

$$\exp(x) = 1 + x + \frac{x^2}{2} + \dots$$

is the exponential function (see section 4.5), whose radius of convergence is $p^{-\frac{1}{p-1}}$. The drawback is that this only works in characteristic zero. The hard way is to take $A = 1 + \pi^m M$, which is an open subgroup of the compact group $\mathcal{O}_L^\times$, hence finite index; and take a filtration $A_i = 1 + \pi^{m+i}M$. These are all normal subgroups of $\mathcal{O}_L^\times$. Then

$$A/A_i \cong M/\pi^i M \cong (\mathcal{O}_K/\mathfrak{p}^i)[G] \cong \mathrm{Ind}^G(\mathcal{O}_K/\mathfrak{p}^i)$$

as G-modules, which has trivial Tate cohomology (theorem 12.5.5). In fact, they are *cohomologically trivial*, i.e. for any $H \leq G$ their Tate cohomology groups also vanish. Then, since

$$A \cong \varprojlim_i A/A_i,$$

it suffices to prove that an inverse limit of cohomologically trivial G-modules is cohomologically trivial. By 18.786 pset (add reference)... □

14.2.3. Corollary. *For L/K finite Galois extension of nonarchimedean local fields, $H^2(\mathrm{Gal}(L/K), L^\times)$ is cyclic of order $n = [L : K]$.*

Proof. We show this by induction on n. If L/K is cyclic, we are already done. □

14.2.4. Theorem. *Let K be a nonarchimedean local field. There is a unique isomorphism*

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

which descends through Inf *to isomorphisms*

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for every finite Galois extension L/K, that coincides with the previously defined $\mathrm{inv}_{L/K}$ *in the unramified case.*

Moreover, for any finite separable extension L/K, then the diagram

$$\begin{tikzcd}
H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"'] & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/L), K^{\mathrm{sep}\,\times}) \arrow[d, "\mathrm{inv}_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes, and when L/K is Galois we have an isomorphism of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & H^2(\mathrm{Gal}(L/K), L^\times) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_{L/K}"] & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/L), K^{\mathrm{sep}\,\times}) \arrow[r] \arrow[d, "\mathrm{inv}_K"] & 0 \\
0 \arrow[r] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

14.3. Proof of local Artin reciprocity. Let K be a nonarchimedean local field.

Let us recall the invariant map

$$\operatorname{inv}_K : H^2(\operatorname{Gal}(K^{\text{sep}}/K), K^{\text{sep}\,\times}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

which descends to

$$\operatorname{inv}_{L/K} : H^2(\operatorname{Gal}(L/K), L^\times) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for every finite Galois extension L/K.

We also defined the local Artin map, which is the inverse of

$$G^{\text{ab}} \cong H_1(G,\mathbb{Z}) = \hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\sim} \hat{H}^0(G, L^\times) = K^\times/\operatorname{N}(L^\times).$$

The first map is an isomorphism via $G^{\text{ab}} \cong I_G/I_G^2$, mapping $\overline{g} \mapsto (g-1)+I_G^2$. The last map is given by Tate's theorem 13.4.2, which requires choosing a generator $u_{L/K} \in H^2(G, L^\times)$, the fundamental class, which is the inverse image of $\frac{1}{[L:K]}$ under $\operatorname{inv}_{L/K}$. It is nontrivial (and shown on the problem set) that the local Artin maps are all compatible, so we may define the Artin homomorphism

$$\theta_K : K^\times \to \operatorname{Gal}(K^{\text{sep}}/K)^{\text{ab}} = \operatorname{Gal}(K^{\text{ab}}/K).$$

Our goal is to show part 1 of local CFT, i.e. θ_K restricted to K^{unr} sends any uniformizer π of $K^\times$ to the arithmetic Frobenius Frob_K. Clearly, it suffices to show this for finite unramified L/K. Let $\sigma = \operatorname{Frob}_{L/K}$, which generates the cyclic $G = \operatorname{Gal}(L/K)$. What we need to show is, the sequence of isomorphisms (writing out the isomorphism in Tate's theorem)

$$G \cong I_G/I_G^2 = H_0(G, I_G) \xrightarrow{\delta_0^{-1}} H_1(G,\mathbb{Z}) = \hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\hat{\delta}_0} \hat{H}^{-1}(G, I_G) \xrightarrow{\hat{\delta}_{L/K}} \hat{H}^0(G, L^\times) = K^\times/\operatorname{N}(L^\times)$$

sends σ precisely to the coset of π. Remembering that $\hat{H}^{-1}(G, I_G) = \hat{H}_0(G, I_G) = H_0(G, I_G)$, we see that $\hat{\delta}_0 \circ \delta_0^{-1} = \text{id}$. So this simplifies to showing that the map $\hat{\delta}_{L/K}$ appearing in the proof of Tate's theorem sends the class of $\sigma - 1 \in I_G/I_G^2$ to the class of π in $K^\times/\operatorname{N}(L^\times)$.

Let us look inside $\hat{\delta}_{L/K}$. It comes from the snake lemma

$$\begin{tikzcd}
 & L^\times_G \arrow[r] \arrow[d] & L^\times(\varphi)_G \arrow[r, "\alpha"] \arrow[d, "\hat{N}_G"] & I_G/I_G^2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (L^\times)^G \arrow[r, "\beta"] & L^\times(\varphi)^G \arrow[r] & (I_G)^G &
\end{tikzcd}$$

where φ is a cochain in $H^2(G, L^\times)$ representing $u_{L/K}$. By definition, one preimage of $[\sigma - 1]$ under α is $[x_\sigma]$, so it suffices to show that $N_G(x_\sigma)$ represents the class of the uniformizer. Let us compute

$$N_G(x_\sigma) = \sum_{i=0}^{n-1} \sigma^i x_\sigma = \prod_{i=0}^{n-1} \varphi(\sigma^i, \sigma).$$

So we have to write down an explicit 2-cochain φ representing $u_{L/K}$. Recall that $u_{L/K}$ is the element in $H^2(G, L^\times)$ that gets sent to the 1-cochain $f : \sigma \mapsto 1/[L:K]$ in the composition ($\operatorname{inv}_{L/K}$)

$$H^2(G, L^\times) \xrightarrow{\sim} H^2(G,\mathbb{Z}) \xrightarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}).$$

So let us trace through the steps. To pull f back to a cochain in $H^2(G,\mathbb{Z})$, consider the snake lemma again, and we see that it is represented by the coboundary of a cocycle $\overline{f} : G \to \mathbb{Q}$ that agrees with f mod $\mathbb{Z}$. Computing this, we see

$$d^1(\overline{f})(\sigma^i, \sigma^j) = \sigma^i \overline{f}(\sigma^j) - \overline{f}(\sigma^{i+j}) + \overline{f}(\sigma^i) = \frac{i+j}{n} - \frac{(i+j) \bmod n}{n}.$$

Now, pull this back to a cochain $\varphi : G^2 \to L^\times$; this is just done by composing with valuation. In particular, we can pick φ such that $\varphi(\sigma^i, \sigma^j) = \pi$ when $i + j \geq n$. So, now we finally have

$$N_G(x_\sigma) = \prod_{i=0}^{n-1} \varphi(\sigma^i, \sigma) = \pi,$$

as desired. This proves the entirety of local CFT.

Finally, we show the norm limitation theorem, which shows that all norm groups arise through abelian extensions (i.e. you cannot extend local Artin reciprocity beyond K^{ab}).

14.3.1. Theorem (norm limitation)**.** *Let L/K be a finite extension of nonarchimedean local fields, E/K its maximum abelian subextension. Then* $\mathrm{N}(L^\times) = \mathrm{N}(E^\times)$.

Proof. It is clear that $\mathrm{N}(L^\times) \subseteq \mathrm{N}(E^\times)$. When L/K is Galois, by local Artin reciprocity,

$$K^\times/\mathrm{N}(E^\times) \cong \mathrm{Gal}(E/K)^{\mathrm{ab}} = \mathrm{Gal}(E/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}} \cong K^\times/\mathrm{N}(L^\times),$$

as desired. When L/K is not Galois, let M be its Galois closure. Let $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$, and $M^{[G,G]}$ is the maximal abelian extension in M/K. Then $E = M^{[G,G]} \cap M^H = M^{[G,G]H}$, so $\mathrm{Gal}(M/E) = [G,G]H$. Since $[H,H] = [G,G] \cap H$, we then have the commutative diagram

$$\begin{tikzcd}
L^\times \arrow[r, "\theta_{M/L}"] \arrow[d, "\mathrm{N}"] & H^{\mathrm{ab}} = H/[H,H] \arrow[d, "\iota"] \\
K^\times \arrow[r, "\theta_{M/K}"] \arrow[d, equal] & G^{\mathrm{ab}} = G/[G,G] \arrow[d, "\pi"] \\
K^\times \arrow[r, "\theta_{E/K}"] & \mathrm{Gal}(E/K) = G/[G,G]H.
\end{tikzcd}$$

Consider any $a \in \mathrm{N}_{E/K}(E^\times)$, then $a \in \ker(\theta_{E/K})$, so $\theta_{M/K}(a) \in \ker\pi = \operatorname{im}\iota$. By surjectivity of $\theta_{M/L}$, there exists $b \in L^\times$ with $a/\mathrm{N}_{L/K}(b) \in \ker\theta_{M/K} = \mathrm{N}_{M/K}(M^\times)$. Now let $c \in M^\times$ such that $\mathrm{N}_{M/K}(c) = a/\mathrm{N}_{L/K}(b)$, then $a = \mathrm{N}_{L/K}(b)\,\mathrm{N}_{M/K}(c) = \mathrm{N}_{L/K}(b\,\mathrm{N}_{M/L}(c)) \in \mathrm{N}(L^\times)$, as desired. □

14.4. Lubin–Tate formal groups. See paper notes.

14.5. Proof of local existence theorem.

15. Miscellaneous topics

15.1. Extensions of absolute values. The appendix collects material not covered in the lectures (but important nonetheless).

15.1.1. Proposition (Strong Hensel's lemma)**.** *Let K be complete wrt a nontrivial, nonarchimedean absolute value $|\,|$. Let $\mathcal{O}_K$, $\mathfrak{m}_K$ be the corresponding valuation ring and maximal ideal. Let $f(x) \in \mathcal{O}_K[x]$ such that its image $\overline{f}$ in $\frac{\mathcal{O}_K}{\mathfrak{m}_K}[x]$ is nonzero. Suppose $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\frac{\mathcal{O}_K}{\mathfrak{m}_K}[x]$ where $\overline{g}$ is monic and $\overline{g}, \overline{h}$ are relatively prime. Then we have lifts $g, h \in \mathcal{O}_K[x]$ such that $f(x) = g(x)h(x)$, and $g(x)$ is monic with degree equal to* $\deg\overline{g}$.

15.1.2. Corollary. *Let $f(x)$ be irreducible in $K[x]$, with degree n. Then*

$$|f| := \max(|a_0|, \dots, |a_n|) = \max(|a_0|, |a_n|).$$

15.1.3. Proposition (Complete archimedean fields)**.** *Let K be complete with respect to a nontrivial, archimedean absolute value. Then $(K, |\,|)$ is isometrically isomorphic to either $(\mathbb{R}, |\,|_\infty^r)$ or $(\mathbb{C}, |\,|_\infty^r)$ for some $0 < r \le 1$.*

15.1.4. Theorem. *Let K be complete wrt a nontrivial absolute value $|\,|$, and L/K a finite extension of degree n. Then*

$$\|\beta\| := |\,\mathrm{N}_{L/K}(\beta)|^{1/n}$$

is the unique absolute value on L extending that on K, and L is complete with respect to $\|\,\|$.

Proof. If $|\,|$ is archimedean, then there is not much to show because of proposition 15.1.3. Assume for the rest that $|\,|$ is nonarchimedean. We will show that so is $\|\,\|$.

Lemma. *For $\beta \in L$, if $\|\beta\| \le 1$, then $\|1+\beta\| \le 1$.*

Proof of lemma. Let $\beta \in L$, $\|\beta\| = 1$. Let $f_\beta(x) \in K[x]$ be its minimal polynomial. Then

$$\mathrm{N}_{L/K}(\beta) = ((-1)^{\deg f_\beta} f_\beta(0))^{[L:K(\beta)]},$$

which implies $|f_\beta(0)| = \|\beta\|^{\deg f_\beta} \le 1$. Then by corollary 15.1.2, $f_\beta(x) \in \mathcal{O}_K[x]$.

Since the minimal polynomial of $1+\beta$ is $f_\beta(x-1)$,

$$\|1+\beta\|^n = |\operatorname{N}_{L/K}(1+\beta)| = |((-1)^{\deg f_\beta} f_\beta(-1))^{[L:K(\beta)]}| \le 1,$$

which proves the lemma. □

By the lemma, if $\|\alpha\| \le \|\beta\|$, we then have $\|\alpha+\beta\| = \|\beta\| \left\|1+\alpha\beta^{-1}\right\| \le \|\beta\|$, which is the nonarchimedean triangle inequality. Uniqueness follows because any two absolute values on L are norms on L (as K-vector spaces), which must induce the same topology on L, so they must be equivalent absolute values, so one must be a power of another, so they must be equal since they agree on K. Completeness is also clear. □

Even better, it is easy to see that these extensions are compatible with each other, i.e. this gives us a unique extension of an absolute value on $\overline{K}$.

15.2. Cyclotomic fields. Let n be a positive integer, ζ_n a primitive root of unity. The goal in this subsection is to show:

15.2.1. Theorem. *The ring of integers in the cyclotomic extension* $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *is* $\mathbb{Z}[\zeta_n]$.

We will in fact prove a bit more about the discriminant of cyclotomic extensions along the way.

Our strategy is to first show Theorem 15.2.1 in the case where $n = p^r$ is a prime-power, then use that to deduce the general case.

For simplicity, let $\zeta = \zeta_{p^r}$ be a primitive p^r-th root of unity. Let $\mathcal{O}$ be the ring of integer in $\mathbb{Q}(\zeta)$.

15.2.2. Proposition. $\mathbb{Z}[\zeta] \cap p\mathcal{O} = p\mathbb{Z}[\zeta]$.

15.2.3. Proposition. $\operatorname{disc}\mathbb{Z}[\zeta]$ *is a power of* p.

We first see how the above two propositions imply that $\mathcal{O} = \mathbb{Z}[\zeta]$. Clearly $\mathbb{Z}[\zeta] \subseteq \mathcal{O}$. If $p \mid (\mathcal{O} : \mathbb{Z}[\zeta])$, then $\mathcal{O}/\mathbb{Z}[\zeta]$ has a subgroup of order p. Then there exists $a \in \mathcal{O}, a \notin \mathbb{Z}[\zeta]$, such that $pa \in \mathbb{Z}[\zeta]$, so $pa \in \mathbb{Z}[\zeta] \cap p\mathcal{O} = p\mathbb{Z}[\zeta]$, which implies $a \in \mathbb{Z}[\zeta]$, a contradiction. Thus, $p \nmid (\mathcal{O} : \mathbb{Z}[\zeta])$. But $(\mathcal{O} : \mathbb{Z}[\zeta])^2 \cdot \operatorname{disc}\mathcal{O} = \operatorname{disc}\mathbb{Z}[\zeta]$ is a power of p, so $\mathcal{O} = \mathbb{Z}[\zeta]$.

Proof of proposition 15.2.2. It is clear that $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, and $(1-\zeta)^i$ $(0 \le i \le p^{r-1}(p-1)-1)$ forms a $\mathbb{Z}$-basis for $\mathbb{Z}[1-\zeta]$.

Lemma. $\operatorname{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$.

Proof of lemma. The conjugates of $1-\zeta$ are $1-\alpha$, where α are the roots of

$$P(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1.$$

The product of these $(1-\alpha)$ is precisely $P(1) = p$. □

Let $\sum_i c_i(1-\zeta)^i \in \mathbb{Z}[1-\zeta] \cap p\mathcal{O}$, where $c_i \in \mathbb{Z}$. We will prove via induction on i that $p \mid c_i$. Because $\operatorname{N}(1-\zeta) = p$, $p \in (1-\zeta)$, so $(1-\zeta) \cap \mathbb{Z} = (p)$. So $c_0 \in (1-\zeta) \cap \mathbb{Z}$ implies $p \mid c_0$. For the induction step, suppose we have shown $p \mid c_0, \dots, c_{i-1}$. It suffices to show that $(1-\zeta)^{p^{r-1}(p-1)} \in p\mathcal{O}$, since then we can cancel out factors of $(1-\zeta)$ and repeat the same argument to show $p \mid c_i$. We know that p is the product of all $p^{r-1}(p-1)$ conjugates of $1-\zeta$, so it suffices to show $\frac{1-\zeta^i}{1-\zeta}$ is a unit in $\mathcal{O}$ for all i, which is easy to see. □

Proof of proposition 15.2.3. $\operatorname{disc}\mathbb{Z}[\zeta] = \operatorname{disc}(1, \zeta, \dots, \zeta^{p^{r-1}(p-1)-1})$, which is equal to $\operatorname{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(P'(\zeta))$ up to sign. After a easy computation (using the lemma above), we in fact have $\operatorname{disc}\mathbb{Z}[\zeta] = \pm p^{p^{r-1}(r(p-1)-1)}$. □

This finishes our proof of theorem 15.2.1 in the case $n = p^r$. In general, use induction on the number of distinct prime divisors of n, with the additional claim that $\operatorname{disc}\mathcal{O}_n$ divides $n^{\phi(n)}$. The base case is handled above. Say $n = p^r m$, where $p \nmid m$. It is clear that then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m)$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = \phi(p^r)\phi(m) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. It suffices to show that $\mathcal{O}_n$, the ring of integers in $\mathbb{Q}(\zeta_n)$, is included in $\mathcal{O}_{p^r} \cdot \mathcal{O}_m$, which by induction hypothesis is $\mathbb{Z}[\zeta_{p^r}]\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_n]$.

Given an element $\alpha \in \mathcal{O}_n$, it must be of the form

$$\alpha = \frac{1}{d}\sum_{i,j} c_{i,j}\zeta_{p^r}^i \zeta_m^j$$

where $d, c_{i,j} \in \mathbb{Z}$, since $\zeta_{p^r}^i \zeta_m^j$ forms a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_n)$. Because the discriminants $\operatorname{disc} \mathbb{Z}[\zeta_{p^r}]$ and $\operatorname{disc} \mathbb{Z}[\zeta_m]$ are coprime, it suffices to show d divides each of these determinants.

Let σ be the automorphism on $\mathbb{Q}(\zeta_n)$ sending $\zeta_{p^r} \mapsto \zeta_{p^r}^a$ and $\zeta_m \mapsto \zeta_m$. Then

$$\sigma\alpha = \frac{1}{d} \sum_{i,j} c_{i,j} \zeta_{p^r}^{ai} \zeta_m^j = \sum_i \zeta_{p^r}^{ai} x_i$$

where $x_i := \sum_j c_{i,j} \zeta_m^j / d$. Varying a and solving for x_i by Cramer's rule, we see that $x_i \cdot \operatorname{disc} \mathbb{Q}(\zeta_{p^r})$ is integral over $\mathbb{Z}$. So $d \mid \operatorname{disc} \mathbb{Q}(\zeta_{p^r})$, and similar for $\operatorname{disc} \mathbb{Q}(\zeta_m)$. Finally, it is easy to show $\operatorname{disc} \mathcal{O}_n$ divides $n^{\phi(n)}$ through a direct computation. This completes the proof.

15.3. Kummer theory.

15.3.1. Definition. Let G be a group which acts upon an abelian group $(M, +)$. Then $H^1(G, M)$ is the group of functions $f : G \to M$ such that $f(gh) = f(g) + gf(h)$, modulo functions of the form $f : g \mapsto gx - x$ $(x \in M)$.

15.3.2. Theorem (Hilbert's theorem 90)**.** *Let L/K be a finite Galois extension, $G = \operatorname{Gal}(L/K)$, then $H^1(G, L^\times) = 0$.*

In the case where G is cyclic and generated by σ, suppose $a \in L^\times$ with norm 1. Then the function $f : G \to L^\times$ given by

$$\sigma^n \mapsto a \cdot \sigma(a) \cdot \cdots \cdot \sigma^{n-1}(a)$$

must be of form $\sigma^n \mapsto \sigma^n(b)/b$ for some $b \in L^\times$, so in particular $a = b/\sigma(b)$.

15.3.3. Theorem. *Let K be a field that contains ζ_n. Then every degree-n cyclic extension L/K is of form $K(\alpha^{1/n})$, where $\alpha^{1/d} \notin K$ for $1 \neq d \mid n$.*

Proof. Let L/K be a degree-n cyclic extension with $\sigma \in G$ generating the Galois group. By Hilbert 90, there exists $t \in L^\times$ with $\zeta_n^r = \sigma^r(t)/t$. So t^n is fixed by G and $t^n = \alpha \in K$, and $L = K(t) = K(\alpha^{1/n})$.

Conversely, it is clear that there is an injective map $\operatorname{Gal}(K(\alpha^{1/n})/K) \to \mathbb{Z}/n\mathbb{Z}$. Surjectivity is clear in the case n is prime, and in general, the image of this map cannot be contained in $p\mathbb{Z}/n\mathbb{Z}$ for any $p \mid n$, and therefore is the whole group $\mathbb{Z}/n\mathbb{Z}$. □

15.3.4. Definition. Let K be a field that contains ζ_n. The *Kummer pairing*

$$\operatorname{Gal}(\overline{K}/K) \times K^\times \to \{1, \zeta_n, \dots, \zeta_n^{n-1}\}$$

is defined by: given $\sigma \in \operatorname{Gal}(\overline{K}/K)$, $z \in K^\times$, choose $y \in \overline{K}$, with $y^n = z$, and define $\langle \sigma, z \rangle = \sigma(y)/y$.

15.3.5. Theorem. *The Kummer pairing induces an isomorphism*

$$K^\times/(K^\times)^n \cong \operatorname{Hom}_{cts}(\operatorname{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}).$$

15.3.6. Proposition. *Let n be an odd prime power, K a field with $\operatorname{char} K$ coprime to n. Let $L = K(\zeta_n)$ and $M = L(\alpha^{1/n})$ for some $\alpha \in L^\times$. Define $\omega : \operatorname{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\zeta_n^{\omega(g)} = g(\zeta_n)$. Then M/K is abelian iff $g(a)/a^{\omega(g)} \in (L^\times)^n$ for all g.*

CHAPTER 6

Algebraic Topology

CHAPTER 7

Algebraic Geometry

1. Category theory

1.1. Lemma. *Consider the following cochain complex:*

$$\cdots \to C^{i-1} \xrightarrow{f^{i-1}} C^i \xrightarrow{f^i} C^{i+1} \to \dots$$

Then we have two pairs of short exact sequences:

- $0 \to \ker f^i \to C^i \to \operatorname{im} f^i \to 0$ *and* $0 \to \operatorname{im} f^{i-1} \to \ker f^i \to H^i(C^\bullet) \to 0$*;*
- $0 \to \operatorname{im} f^{i-1} \to C^i \to \operatorname{coker} f^{i-1} \to 0$ *and* $0 \to H^i(C^\bullet) \to \operatorname{coker} f^{i-1} \to \operatorname{im} f^i \to 0$.

1.2. Proposition (FHHF theorem)**.** *Let $F : \mathscr{A} \to \mathscr{B}$ be a covariant functor between abelian categories, and let $C^\bullet$ be a cochain complex in $\mathscr{A}$.*

(a) If F is right exact, there is a natural morphism $FH^\bullet(C^\bullet) \to H^\bullet F(C^\bullet)$.
(b) If F is left exact, there is a natural morphism $H^\bullet F(C^\bullet) \to FH^\bullet(C^\bullet)$.
(c) If F is exact, the two morphisms are inverses of each other.

Proof. (a) Applying F on $C^i \to C^{i+1} \to \operatorname{coker} f^i \to 0$, we get a natural isomorphism $F \operatorname{coker} f^i \to \operatorname{coker} Ff^i$. Applying F on $0 \to \operatorname{im} f^i \to C^{i+1} \to \operatorname{coker} f^i \to 0$, we get a natural epimorphism $F \operatorname{im} f^i \twoheadrightarrow \operatorname{im} Ff^i$. Applying F on $0 \to H^i(C^\bullet) \to \operatorname{coker} f^{i-1} \to \operatorname{im} f^i \to 0$ and chasing diagrams, we get a natural map $FH^i(C^\bullet) \to H^i F(C^\bullet)$.

(b) Applying F on $0 \to \ker f^i \to C^i \to C^{i+1}$, we get a natural isomorphism $\ker Ff^i \to F \ker f^i$. Applying F on $0 \to \ker f^i \to C^i \to \operatorname{im} f^i \to 0$, we get a natural monomorphism $\operatorname{im} Ff^i \hookrightarrow F \operatorname{im} f^i$. Applying F on $0 \to \operatorname{im} f^{i-1} \to \ker f^i \to H^i(C^\bullet) \to 0$ and chasing diagrams, we get a natural map $H^i F(C^\bullet) \to FH^i(C^\bullet)$.

(c) Carefully trace where each element goes. □

1.3. Proposition (Exactness and (co)limits)**.** *Limits commute with limits and right adjoints. In particular, right adjoints and limits are both left exact since they commute with* ker*.*

Colimits commute with colimits and left adjoints. In particular, left adjoints and colimits are both right exact since they commute with coker*.*

In Mod_A, colimits over filtered index categories are exact.

2. Sheaves

2.1. The espace étalé of a (pre)sheaf. Let $\mathcal{F}$ be a (pre)sheaf on X. We can construct a topological space F and a continuous $\pi : F \to X$ as follows:

- As a set, $F = \coprod_{p \in X} \mathcal{F}_p$.
- Open sets of F are generated by the following base: given an open $U \subseteq X$ and $f \in \mathcal{F}(U)$, the set $\{(p, U, f) : p \in U\}$ is open.

Then $\pi : F \to U$ is a *local homeomorphism.*

2.2. Stalks and sheafification.

2.3. Sheaf on a base. Suppose X is a topological space with $\{B_i\}$ as a base of the topology. Suppose we're given the following information:

- To each B_i, we have an associated set/abelian group/ring/module $\mathcal{F}(B_i)$;
- For each $B_i \subseteq B_j$, a restriction map $\operatorname{res}_{B_i,B_j} : \mathcal{F}(B_i) \to \mathcal{F}(B_j)$; this should be the identity when $i = j$;
- If $B_i \subseteq B_j \subseteq B_k$, then $\operatorname{res}_{B_i,B_k} = \operatorname{res}_{B_j,B_k} \circ \operatorname{res}_{B_i,B_j}$.

- If $B = \bigcup B_i$, then if $f, g \in \mathcal{F}(B)$ restricts to the same function on each $\mathcal{F}(B_i)$, then $f = g$;
- If $B = \bigcup B_i$, and $f_i \in \mathcal{F}(B_i)$ such that if for any $B_k \subseteq B_i \cap B_j$, f_i and f_j restrict to the same function on B_k, then there exists $f \in \mathcal{F}(B)$ such that f restricts on each f_i on each patch.

This is called a *sheaf on a base*. Given this information, the sheaf on any open set can be uniquely determined up to unique isomorphism.

2.4. Inverse image sheaf.

3. Affine schemes

3.1. Spectrum of a ring.

3.2. Hilbert's Nullstellensatz.

3.3. Topological properties of affine schemes.

3.3.1. Definition. A topological space X is *Noetherian* if it satisfies the d.c.c. on closed sets.

3.3.2. Proposition. *Let X be Noetherian. Then every nonempty closed set Z can be uniquely expressed as a finite union $Z = Z_1 \cup \cdots \cup Z_n$ of irreducible closed sets, none contained in any other.*

4. Schemes

4.1. Proj construction. Given a (commutative) ring A, Spec produces from it a locally ringed space $\operatorname{Spec} A$. If we take $A = k[x_1, \ldots, x_n]$, then $\operatorname{Spec} A$ is the affine n-space $\mathbb{A}^n_k$. Similarly, the Proj construction takes a $\mathbb{Z}_{\geq 0}$-graded ring S as input, and produces from this data a scheme (not necessarily affine!) $\operatorname{Proj} S$, and in the special case $S = k[x_0, \ldots, x_n]$, $\operatorname{Proj} S$ is the projective n-space $\mathbb{P}^n_k$.

4.1.1. Definition. Let S be a $\mathbb{Z}_{\geq 0}$-graded ring. The scheme $\operatorname{Proj} S$ is given by:

- As a set, the points in $\operatorname{Proj} S$ are the homogeneous prime ideals $\mathfrak{p}$ such that $S_+ \notin \mathfrak{p}$;
- As a topological space, the closed sets are given by $V(I) = \{[\mathfrak{p}] \in \operatorname{Proj} S : I \subseteq \mathfrak{p}\}$, for homogeneous ideals $I \subseteq S_+$. Equivalently, the topology is given by the base of distinguished opens $D(f) = \{[\mathfrak{p}] \in \operatorname{Proj} S : f \notin \mathfrak{p}\}$, for homogeneous $f \in S_+$.
- As a locally ringed space, the structure sheaf is given on the base by $\mathcal{O}_{\operatorname{Proj} S}(D(f)) = (S_f)_{\deg 0}$.

4.1.2. Definition. Let S be a finitely generated graded ring over A. Then a scheme of the form $\operatorname{Proj} S$ is called a *projective scheme over A*. An quasicompact open subscheme of a projective A-scheme is called a *quasiprojective A-scheme.*

4.2. Properties of schemes.

4.2.1. Proposition. *Let X be a scheme. Then the points of X correspond bijectively to irreducible closed sets of X, via the map*

$$x \mapsto \overline{\{x\}}.$$

Proof. Because the closure of an irreducible set is irreducible, this is a well-defined map. Conversely, given an irreducible closed set $T \subseteq X$, consider an affine open U such that $T \cap U \neq \varnothing$. Then $T \cap U$ is an irreducible closed set in U, so it corresponds to a unique generic point in U. For affine opens U, V both intersecting T, $U \cap V$ must also intersect T because T is irreducible. Pick an affine open $W \subseteq U \cap V$ that is distinguished in both U and V and also intersects T. Then the unique generic point corresponding to $T \cap W$ must simultaneously be the unique generic points corresponding to $T \cap U$ and $T \cap V$. In other words, there is a unique point $x \in T$ that is the unique generic point corresponding to $T \cap U$ for all affine opens U intersecting T.

We claim that $T = \overline{\{x\}}$; indeed for any closed $K \subseteq X$ containing x, and for any point $t \in T$, there is an affine open U containing t (and by default containing x too), $K \cap U$ contains x, so it must contain $T \cap U$ (the closure of $\{x\}$ in $T \cap U$). In particular, $t \in K$ as well. □

4.2.2. Proposition. *Let X be a quasicompact scheme, then any point has a closed point in its closure.*

4.2.3. Definition. A scheme X is called *reduced* if all stalks are reduced rings. Equivalently, for all open U, $\mathcal{O}_X(U)$ is reduced.

4.2.4. Definition. A property P for affine open subsets of a scheme X is called *affine-local* if it satisfies:

- If an affine open $\operatorname{Spec} A$ satisfies P, then any $\operatorname{Spec} A_f$ satisfies P also.
- If $f_1, \dots, f_n \in A$ generate the unit ideal, and all $\operatorname{Spec} A_{f_i}$ satisfy P, then $\operatorname{Spec} A$ satisfies P as well.

4.2.5. Lemma (Affine Communication Lemma)**.** *Suppose P is an affine-local property, and* $X = \bigcup_{i\in I} \operatorname{Spec} A_i$ *where each* $\operatorname{Spec} A_i$ *satisfies property P. Then any affine open in X satisfies P.*

Properties defined in this way:

- Locally Noetherian
- Noetherian
- Locally of finite type over B
- Finite type over B

4.3. Varieties.

An affine scheme that is reduced and of finite type over k is called an *affine k-variety.* A reduced quasiprojective k-scheme called a *projective k-variety.* In general, a *variety* is a reduced, separated, finite type k-scheme.

4.4. Normality and factoriality.

A scheme X is *normal* if all of its local rings are integrally closed domains.

Because being integrally closed is a local property, $\operatorname{Spec} A$ for A integrally closed is an affine normal scheme. For a quasicompact scheme, this can also be checked at closed points only.

A scheme X is *factorial* if all of its local rings are UFDs. Since UFDs are all integrally closed, factorial schemes are normal. Factoriality is not affine-local.

4.5. Associated points.

In the affine case, the associated points of an A-module M are primes $\mathfrak{p} \subset A$ of the form $\mathfrak{p} = \operatorname{Ann}(m)$ for some $m \in M$. (See here; also, taking $M = A/I$, we recover the usual associated points of an ideal.) They have the following properties:

4.5.1. Theorem. *Suppose A is Noetherian and $M \neq 0$ is finitely generated. Then:*

(1) $\operatorname{Ass}(M)$ *is nonempty and finite.*
(2) The natural map $M \to \prod_{\mathfrak{p}\in\operatorname{Ass}(M)} M_{\mathfrak{p}}$ *is injective.*
(3) $\bigcup_{\mathfrak{p}\in\operatorname{Ass}(M)}$ *is precisely the set of zerodivisors of M.*
(4) Associated primes commute with localization:

$$\operatorname{Ass}_{S^{-1}A}(S^{-1}M) = \operatorname{Ass}_A(M) \cap \operatorname{Spec} S^{-1}A.$$

In general (see here):

4.5.2. Definition. Let X be a scheme, and F a quasicoherent sheaf. A point $x \in X$ is *associated to F* if $\mathfrak{m}_x$ is an associated point of the $\mathcal{O}_{X,x}$-module F_x.

4.5.3. Proposition. *Let X be locally Noetherian, F quasicoherent. Let $U = \operatorname{Spec} A$ be an affine open, $x \in U$ corresponds to $\mathfrak{p} \subset A$, $M = \Gamma(U, F)$, then $x \in \operatorname{Ass}(F) \iff \mathfrak{p} \in \operatorname{Ass}(M)$.*

4.5.4. Definition. Let X be a scheme, F a quasicoherent sheaf. An *embedded associated point* is an associated point that is not minimal.

4.5.5. Proposition. *Let X be locally Noetherian, and F coherent (e.g. $\mathcal{O}_X$). Then the generic points of irreducible components of* $\operatorname{Supp} F$ *are associated points, and the rest of the associated points are embedded.*

4.6. Weakly associated points.

5. Morphisms of schemes

5.1. Morphisms to affine schemes.

These have a nice characterization:

5.1.1. Proposition. *The following are equivalent:*

- *There is a morphism of schemes* $X \to \operatorname{Spec} A$*;*
- *For every open $U \subseteq X$, $\mathcal{O}_X(U)$ is an A-algebra;*
- *There is a ring map $A \to \mathcal{O}_X(X)$.*

5.2. Morphisms from affine schemes. Given any point $p \in X$, there is a canonical morphism $\operatorname{Spec} \mathcal{O}_{X,p} \to X$. Composing this with the map induced by $\mathcal{O}_{X,p} \to \kappa(p)$, we get a canonical $\operatorname{Spec} \kappa(p) \to X$, often written just as $p \to X$.

More generally: for a local ring $(A, \mathfrak{m})$, a scheme morphism $\pi : \operatorname{Spec} A \to X$ sending $\mathfrak{m}$ to p corresponds bijectively to local homomorphisms $\mathcal{O}_{X,p} \to A$.

5.2.1. Definition (functor of points)**.** Let Z be a scheme, the *Z-valued points* of X (denoted $X(Z)$) are the maps $Z \to X$. (When $Z = \operatorname{Spec} A$ or $\operatorname{Spec} k$, they are the A- or k-valued points.)

If we're working with schemes over a base scheme B, then this data should also include a $Z \to B$ making $Z \to X \to B$ commute.

5.3. Functoriality of Proj. Suppose $\phi : S \to R$ is a map of graded rings (i.e. there exists $\mathbb{N}_+$ such that S_n maps to R_{dn} for all n). This induces a morphism of schemes

$$\phi^* : (\operatorname{Proj} R) \backslash V(\phi(S_+)) \to \operatorname{Proj} S,$$

as follows: given $f \in S_+$, there is a map of rings $S_f \to R_{\phi(f)}$, hence a map of rings $(S_f)_{\deg 0} \to (R_{\phi(f)})_{\deg 0}$, hence a morphism of affine schemes $\operatorname{Spec}(R_{\phi(f)})_{\deg 0} \to \operatorname{Spec}(S_f)_{\deg 0}$, i.e. $D(\phi(f)) \to D(f) \hookrightarrow \operatorname{Proj} S$. These glue together to form the desired morphism of schemes.

In particular, if $V(\phi(S_+))$ is empty, then we get an actual morphism $\operatorname{Proj} R \to \operatorname{Proj} S$. This is satisfied when $\operatorname{rad}(\phi(S_+)) = R_+$. (Recall from §4.1 that the radical turns out to be equal to the intersection of all homogeneous primes containing the ideal.)

5.4. Veronese subring.

5.5. The relative point of view. Instead of thinking of properties of objects, it might be better to understand them as properties of morphisms between objects. For example, given a property P about schemes, one often turns it into a property about morphisms of schemes as follows: say $\pi : X \to Y$ has P if and only if for every affine open $U \subset Y$, $\pi^{-1}(U)$ has P.

5.6. Green flags to look for in a property of morphisms.

(1) It is *local on the target*: for a morphism $\pi : X \to Y$ and a open cover V_i of Y, π satisfies P iff all $\pi|_{\pi^{-1}(V_i)}$ satisfy P.
(2) It is closed under composition.
(3) It is closed under base change, pullback, fibered products, etc.
(4) . . .

5.7. Finiteness conditions on morphisms. Recall that a scheme is called *quasicompact* if it is the union of finitely many affine schemes, and a scheme is called *quasiseparated* if the intersection of any two quasicompact open subsets is quasicompact. We turn them into properties of schemes as discussed in §5.5. These are both affine-local on the target and closed under composition. Conversely, a scheme X is quasicompact (resp. quasiseparated) if the canonical $X \to \operatorname{Spec} \mathbb{Z}$ is so. Note that many schemes we commonly encounter are qcqs: in particular, all affine schemes are qcqs, and all Noetherian schemes are qcqs.

5.7.1. Definition (affine morphisms)**.** A morphism $\pi : X \to Y$ is *affine* if the preimage of any affine open in Y is affine open in X. Affine morphisms are automatically qcqs.

5.7.2. Lemma (qcqs lemma)**.** *If X is qcqs, $s \in \mathcal{O}_X(X)$, then the natural map $\mathcal{O}_X(X)_s \to \mathcal{O}_X(X_s)$ is an isomorphism.*

PROOF. Use the qcqs property as a finite presentation. □

5.7.3. Proposition. *Affineness is affine-local on the target. In other words, affineness of a morphism can be checked on affine covers of the target.*

PROOF. □

5.7.4. Definition (finite morphisms)**.** An affine morphism $\pi : X \to Y$ is *finite* if for any affine $\operatorname{Spec} A \subset Y$, $\pi^{-1}(\operatorname{Spec} A)$ is the spectrum of a ring that is a finitely generated module over A.

Finiteness is also affine-local on the target.

5.7.5. Example. Examples of finite morphisms:

- Branched covers: consider the map $k[u] \to k[t]$ given by $u \mapsto p(t)$ for a polynomial p. Then $\operatorname{Spec} k[t] \to \operatorname{Spec} k[u]$ is a finite morphism.
- Closed embeddings: A/I is a finite A-module (generated by 1), so $\operatorname{Spec} A/I \to \operatorname{Spec} A$ is a finite morphism.
- Normalization: $k[x,y]/(y^2 - x^2 - x^3) \mapsto k[t]$ by $x \mapsto t^2 - 1$, $y \mapsto t^3 - t$ induces a morphism of schemes $\operatorname{Spec} k[t] \to \operatorname{Spec} k[x,y]/(y^2 - x^2 - x^3)$. This is a finite morphism, and it is in fact an isomorphism from $D(t^2 - 1)$ to $D(x)$.

5.7.6. Proposition (7.3.H)**.** *If $X \to \operatorname{Spec} k$ is a finite morphism, then X is a finite union of points with the discrete topology, each point with residue field a finite extension of k.*

Proof. We must have $X = \operatorname{Spec} A$, where A is a k-algebra that is finitely generated as a module. Then A is Noetherian and any prime $\mathfrak{p} \subset A$ is maximal, so the (finitely many) irreducible components of A, which correspond to minimal primes, are all closed points. Therefore $\operatorname{Spec} A$ is finite discrete, and the residue field at each point $[\mathfrak{p}]$ is a finite extension of k. □

5.7.7. Corollary (7.3.K)**.** *Finite morphisms have finite fibers.*

5.7.8. Definition (integral morphisms)**.** A morphism $\pi : X \to Y$ is *integral* if it is affine, and for every affine open $\operatorname{Spec} B \subset Y$, $\operatorname{Spec} A = \pi^{-1}(\operatorname{Spec} B)$, $B \to A$ is an integral extension.

Because integrality is an affine-local property, a morphism being integral is affine-local on the target. Also, finite morphisms are integral, and integral morphisms are closed (they map closed sets to closed sets).

5.7.9. Definition (finite type morphisms)**.** A morphism $\pi : X \to Y$ is *locally of finite type* if for every affine open $\operatorname{Spec} B \subset Y$, and for every $\operatorname{Spec} A \subset \pi^{-1}(\operatorname{Spec} B)$, $B \to A$ expresses A as a finitely generated B-algebra. We say π is *finite type* if it is quasicompact and locally of finite type.

5.7.10. Proposition (7.3.P)**.** *A morphism is finite iff it is integral and of finite type.*

5.7.11. Definition (finitely presented morphisms)**.** A morphism $\pi : X \to Y$ is *locally finitely presented* if for every affine open $\operatorname{Spec} B \subset Y$, $\pi^{-1}(\operatorname{Spec} B) = \bigcup_i \operatorname{Spec} A_i$ with each $B \to A_i$ finitely presented. We say π is finitely presented if it is locally finitely presented and qc*qs*.

It is clear that if Y is locally Noetherian, then locally of finite presentation is the same as locally of finite type, and finite presentation is the same as finite type.

5.7.12. Proposition. *Locally finitely presented-ness is affine-local on both the target and the source.*

5.8. Elimination theory.

5.8.1. Lemma (Generic freeness)**.** *Let B be a Noetherian integral domain, A a finite type algebra over B, and M a finitely generated A-module. Then there exists $f \in B$ such that M_f is a free B_f-module.*

5.8.2. Theorem (Chevalley's theorem)**.** *Let $\pi : X \to Y$ be a finite type morphism between Noetherian schemes. Then the image of any constructible set is constructible.*

5.8.3. Theorem (Fundamental theorem of elimination theory)**.** *The map $\mathbb{P}^n_A \to \operatorname{Spec} A$ is closed, for any ring A.*

5.9. Closed subschemes, and related constructions.

5.9.1. Definition. A *closed embedding* $\pi : X \hookrightarrow Y$ is an affine morphism where for each $\operatorname{Spec} B \subseteq Y$ and $\operatorname{Spec} A = \pi^{-1}(\operatorname{Spec} B)$, the induced ring map $B \to A$ is surjective.

5.9.2. Definition (equivalent to the above)**.** A *closed embedding* $\pi : X \to Y$ is a morphism such that π induces a homeomorphism of the underlying topological space of X onto a closed subset of the topological space of Y, and the induced map $\pi^\sharp : \mathcal{O}_Y \to \pi_*\mathcal{O}_X$ of sheaves on Y is surjective.

Ideal sheaf, scheme-theoretic image, intersection and union of closed subschemes

5.10. Effective Cartier divisors and regular sequences.

5.10.1. Definition. A *locally principal* closed subscheme $\pi : X \hookrightarrow Y$ is one for which there exists an open cover U_i of Y, such that each $\pi^{-1}(U_i) \to U_i$ is isomorphic to a closed subscheme $V(s_i) \subset U_i$, where $s_i \in \mathcal{O}_Y(U_i)$. Equivalently, we may as well take all U_i to be affine.

5.10.2. Definition. An *effective Cartier divisor* is a locally principal closed subscheme where the ideal sheaf is locally generated near every point by a non-zero divisor.

5.10.3. Example. Consider $\operatorname{Spec} A$, where $A = k[w,x,y,z]/(wz - xy)$. Let X be the open subscheme $D(y) \cup D(w)$. The closed subscheme defined by $V(z/y)$ on $D(y)$ and $V(x/w)$ on $D(w)$ is an effective Cartier divisor, but it is not generated by a single element of $\operatorname{Frac} A$.

5.10.4. Definition. Let M be an A-module. A sequence $x_1, \dots, x_r$ of elements in A is called an *M-regular sequence* if:

- For each i, x_i is not a zero divisor for $M/(x_1, \dots, x_{i-1})M$ (exists no $m \in M \backslash (x_1, \dots, x_{i-1})M$ such that $mx_i \in (x_1, \dots, x_{i-1})M$), and
- $(x_1, \dots, x_r)M \neq M$.

In particular, an A-regular sequence is just called a regular sequence.

5.10.5. Example. For any M-regular sequence $x_1, \dots, x_n$, and positive integers $a_1, \dots, a_n$, the sequence $x_1^{a_1}, \dots, x_n^{a_n}$ is a regular sequence too.

5.10.6. Example. Let $A = k[x,y,z]/(x-1)z$. Then $x, (x-1)y$ is a regular sequence, while $(x-1)y, x$ is not.

5.10.7. Theorem. *Let A be a Noetherian local ring, and M a finitely generated A-module. Then any M-regular sequence remains regular when reordered.*

5.10.8. Definition (regular embedding)**.** Let $\pi : X \to Y$ be a locally closed embedding. Say that π is a *regular embedding* of codimension r at $x \in X$ if in $\mathcal{O}_{Y,\pi(x)}$, the ideal of X is generated by a regular sequence of length r. Say that π is a *regular embedding* if it is at all points.

5.11. Fiber products.

5.12. An interlude on closed points.

5.12.1. Proposition. *Let X be a scheme locally of finite type over a field k. If $x \in \operatorname{Spec} A \subset X$ corresponds to a maximal ideal in some affine open subscheme of X, then x is a closed point in X.*

Proof. Suppose x corresponds to $\mathfrak{m} \subset A$, then $\kappa(x) = A/\mathfrak{m}$. By the nullstellensatz, $A/\mathfrak{m}$ is a finite extension of k. Now, suppose $\operatorname{Spec} B \subset X$ is some other affine open containing x, and say x corresponds to a prime $\mathfrak{p} \subset B$. Then $\kappa(x) = \operatorname{Frac} B/\mathfrak{p}$, so in particular $k \subseteq B/\mathfrak{p} \subseteq \kappa(x)$. So $B/\mathfrak{p}$ is an integral extension of k, so it is a field as well, i.e. $\mathfrak{p}$ is maximal. So $\{x\}$ is closed in X. □

5.12.2. Proposition. *Let X be a scheme locally of finite type over k. Suppose we have a morphism $\pi : \operatorname{Spec} k \to X$, then its image is a closed point.*

Proof. Let $\operatorname{Spec} A \subset X$ be an affine open subscheme. The morphism π factors through $\operatorname{Spec} A$, so we get $\phi : \operatorname{Spec} k \to \operatorname{Spec} A$. Suppose $\mathfrak{m}$ is the kernel of the corresponding map $A \to k$, and $\mathfrak{p}$ is the prime ideal corresponding to the image of π. Then we get a map of stalks $A_\mathfrak{p} \to k$ through which the map $A \to k$ factors. Suppose $a \notin \mathfrak{p}$, then a is invertible in $A_\mathfrak{p}$, so it is not in the kernel of $A \to k$, so $\mathfrak{m} \subseteq \mathfrak{p}$. Since $\mathfrak{m}$ is maximal, $\mathfrak{m} = \mathfrak{p}$, so we conclude by the previous proposition. □

5.12.3. Proposition. *Let X be a scheme locally of finite type over $k = \overline{k}$. Then closed points of X are in bijection with k-points of X.*

Proof. The bijection is given by:

- Given a k-point $\operatorname{Spec} k \to X$, this maps to its image, which is a closed point in X;
- Given a closed point $x \in X$, its field of fractions is k by the nullstellensatz, so we get $\operatorname{Spec} k = \operatorname{Spec} \kappa(x) \to X$.

It suffices to verify that these two are inverses. Given a closed point $x \in X$, it is clear from definition that the image of $\operatorname{Spec} \kappa(x) \to X$ is x. On the other hand, given a k-point $\operatorname{Spec} k \to X$, it is given by $\operatorname{Spec} k \to \operatorname{Spec} A \subseteq X$, where A/k is the maximal ideal corresponding to the image x of the k-point. So $A/k = \kappa(x)$, which finishes the proof. □

5.12.4. Corollary. *Let $f : X \to Y$ be a morphism between schemes over k locally of finite type. Then f maps closed points to closed points. In particular, maps between k-schemes map closed points to closed points.*

5.13. Separated morphisms.

5.13.1. Definition. A morphism of schemes $\pi : X \to Y$ is *separated* if the diagonal map $\Delta_\pi : X \to X \times_Y X$ is a closed embedding.

To see that this definition isn't too crazy, we notice the following.

5.13.2. Proposition. *Let $\pi : X \to Y$ be a morphism. The diagonal $\Delta_\pi : X \to X \times_Y X$ is a locally closed embedding (i.e. a closed subscheme of an open subscheme).*

Proof. Cover Y by affine opens V_i, and $\pi^{-1}(V_i)$ by affine opens U_{ij}. Then $U_{ij} \times_{V_i} U_{ij}$ is an affine open subscheme of $X \times_Y X$ by definition, and these cover the image of Δ_π. Further, it is clear that $\Delta_\pi^{-1}(U_{ij} \times_{V_i} U_{ij}) = U_{ij}$, and $\Delta|_{U_{ij}}$ is a closed embedding. □

5.13.3. Definition. A *variety* over a field k is a reduced, separated, finite-type k-scheme.

Because a locally closed embedding whose image is closed is in fact a closed embedding, to check that $\pi : X \to Y$ is separated, it suffices to check that the image of Δ is closed.

Examples of separated morphisms:

- Locally closed embeddings (also called *immersions*);
- Morphisms between affine schemes;
- All quasiprojective A-schemes (with morphism to $\operatorname{Spec} A$);
- Any morphism between varieties is automatically separated and finite type (this will follow from the cancellation theorem).

5.13.4. Lemma (Magic diagram). *Let X_1, X_2, Y, Z be objects in a category where fiber products exist. Suppose we are given maps $f_1 : X_1 \to Y$, $f_2 : X_2 \to Y$, and $g : Y \to Z$. Then the following diagram is a Cartesian square:*

$$\begin{tikzcd}
X_1 \times_Y X_2 \arrow[r] \arrow[d] & X_1 \times_Z X_2 \arrow[d, "f_1 \times f_2"] \\
Y \arrow[r, "\Delta"] & Y \times_Z Y.
\end{tikzcd}$$

5.13.5. Proposition. *Let X be separated over a ring A. Then for $U, V \subset X$ affine opens, $U \cap V$ is an affine open as well.*

Proof. Consider the following fiber product:

$$\begin{tikzcd}
U \cap V \arrow[r] \arrow[d] & U \times_A V \arrow[d] \\
X \arrow[r, hook, "\Delta"] & X \times_A X
\end{tikzcd}$$

Here, $U \cap V = U \times_X V$ is the fiber product because of the magic diagram. Now, because the bottom map is a closed embedding, so is the top map. Since $U \times_A V$ is an affine scheme, so is $U \cap V$. □

5.13.6. Proposition. *Separatedness is well-behaved:*

1. *affine-local on the target;*
2. *stable under composition;*
3. *stable under base change.*

Proof. (1) This follows from the fact that $\pi : X \to Y$ is separated if and only if $\operatorname{im}(\Delta)$ is closed.

(2) Suppose $f : X \to Y, g : Y \to Z$ are separated. Consider the following commutative diagram

$$\begin{tikzcd}
X \arrow[r, hook, "\Delta_f"] & X \times_Y X \arrow[r] \arrow[d] & X \times_Z X \arrow[d] \\
& Y \arrow[r, hook, "\Delta_g"] & Y \times_Z Y
\end{tikzcd}$$

The square is Cartesian by the magic diagram, so the top map $X \times_Y X \to X \times_Z X$ is a closed embedding. So the composition $X \to X \times_Z X$, which can be verified to be the diagonal of $g \circ f$, is a closed embedding.

(3) Suppose

$$\begin{tikzcd}
X \arrow[r] \arrow[d] & Y \arrow[d] \\
Z \arrow[r] & W
\end{tikzcd}$$

is a pullback square, where $Z \to W$ is separated. It suffices to show that

$$\begin{tikzcd}
X \arrow[r, "\Delta"] \arrow[d] & X \times_Y X \arrow[d] \\
Z \arrow[r, "\Delta"] & Z \times_W Z
\end{tikzcd}$$

is also a pullback square, which is a straightforward diagram chase. □

5.13.7. Proposition. *Let $\pi : X \to Y$ be a morphism of Z-schemes, and $Y \to Z$ separated. Then its* graph *$\Gamma_\pi : X \xrightarrow{(\mathrm{id},\pi)} X \times_Z Y$ is a closed embedding.*

5.13.8. Proposition (Cancellation theorem). *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$, and suppose P is a property of morphisms, such that:*

- *P is stable under composition;*
- *P is stable under base change;*
- *$g \circ f$ satisfies P;*
- *$\Delta_g : Y \to Y \times_z Y$ satisfies P.*

Then f satisfies P also.

Proof. We have the following Cartesian squares:

$$\begin{tikzcd}
X \times_Z Y \arrow[r, "\pi"] \arrow[d] & Y \arrow[d, "g"] \\
X \arrow[r, "g \circ f"] & Z.
\end{tikzcd}$$

Here, because $g \circ f$ satisfies P, so does $\pi : X \times_Z Y \to Y$. Also, we have

$$\begin{tikzcd}
X = X \times_Y Y \arrow[r, "\Gamma"] \arrow[d, "f"] & X \times_Z Y \arrow[d] \\
Y \arrow[r, "\Delta_g"] & Y \times_Z Y,
\end{tikzcd}$$

and because Δ_g satisfies P, so does Γ. But $\pi \circ \Gamma$ is easily verified to be simply f, so f satisfies P also. □

5.13.9. Theorem (Reduced to separated theorem)**.** *Suppose X, Y are schemes over Z, where X is reduced, and $Y \to Z$ is separated. Let $\pi, \pi' : X \to Y$ be morphisms over Z. Suppose $U \subseteq X$ is a dense open on which π and π' agree. Then $\pi = \pi'$.*

Proof. Let V be the fiber product

$$\begin{tikzcd}
V \arrow[r] \arrow[d] & Y \arrow[d, "\Delta"] \\
X \arrow[r, "(\pi;\pi')"] & Y \times_Z Y.
\end{tikzcd}$$

Because Δ is a closed embedding, so is $V \hookrightarrow X$. Because $\pi|_U = \pi'|_U$, we get a map $U \to V$ through the universal property of V. But U is an open subscheme of X. Because U is dense, $V = X$ as sets. Because X is reduced, $V = X$ as schemes. So $\pi = \pi'$ on all of X. □

5.14. Dominant rational maps between irreducible varieties.

5.14.1. Definition. A *rational map* between schemes $X \dashrightarrow Y$ is a map $U \to Y$ where U is a dense open in X. Two rational maps $X \dashrightarrow Y$ are *equivalent* if $\alpha|_W = \beta|_W$ on some dense open $W \subseteq U \cap V$.

5.14.2. Definition. A morphism of schemes is *dominant* if its image is dense.

Fix a field k (algebraically closed when necessary), consider the category of irreducible varieties over k, with morphisms as dominant rational maps.

Given an irreducible variety X, because irreducible and reduced implies integral, it has a unique generic point η. The stalk at η is the *function field* $K(X)$, which is equal to the fraction field $\operatorname{Frac} A$ of any affine open $\operatorname{Spec} A \subseteq X$. Given a rational map $X \dashrightarrow Y$, this induces a field homomorphism at the stalks of the generic points.

5.14.3. Theorem. *The functor described above gives an equivalence of categories between irreducible varieties with dominant rational maps and finitely generated field L/k with inclusions of fields.*

5.15. Ax-Grothendieck theorem.

5.15.1. Theorem (Ax-Grothendieck)**.** *Let X be a variety over $\mathbb{C}$, $f : X \to X$ a morphism over $\mathbb{C}$. Suppose that the map of $\mathbb{C}$-points $X(\mathbb{C}) \to X(\mathbb{C})$ is injective (as a set), then it must be surjective.*

We will define the *spreading out* of X, which is a finite type scheme over $\operatorname{Spec} R$, for some finitely generated $\mathbb{Z}$-algebra $R \subset \mathbb{C}$.

Cover X by (finitely many, since X is quasicompact) affine schemes U_i, which are of the form $\operatorname{Spec} \mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_r$ since X is finite type and by Hilbert's basis theorem. Because X is separated, $U_i \cap U_j$ is also affine of the above form. Even further, each $f^{-1}(U_i)$ is covered by finitely many affine opens U_{ij}, because morphisms between varieties are automatically quasicompact, and the U_{ij}'s are again of the above form. So we can take R to be the $\mathbb{Z}$-algebra generated by all coefficients of f_i appearing in U_i, $U_i \cap U_j$, and U_{ij}'s, and define $\mathcal{X}$ by glueing together $\operatorname{Spec} R[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. The map $f : X \to X$ also spreads out to a map $F : \mathcal{X} \to \mathcal{X}$. By definition, this satisfies the following Cartesian squares:

$$\begin{tikzcd}
X \arrow[r] \arrow[d, "f"'] & \mathcal{X} \arrow[d, "F"] \\
X \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\
\operatorname{Spec} \mathbb{C} \arrow[r] & \operatorname{Spec} R.
\end{tikzcd}$$

Now, set $U = X \times_{\mathbb{C}} X \backslash \Delta(X)$, an open subscheme of $X \times_{\mathbb{C}} X$. Let W be the fiber product

$$\begin{tikzcd}
W \arrow[rr] \arrow[d] & & X \arrow[d] \\
U \arrow[r, hook] & X \times_{\mathbb{C}} X \arrow[r, "f \times_{\mathbb{C}} f"] & X \times_{\mathbb{C}} X,
\end{tikzcd}$$

and supposing $x \in X$ is a point, let Z be the fiber

$$\begin{tikzcd}
Z \arrow[r] \arrow[d] & \operatorname{Spec} \mathbb{C} \arrow[d, "x"] \\
X \arrow[r, "f"] & X.
\end{tikzcd}$$

Then $X(\mathbb{C}) \to X(\mathbb{C})$ is injective implies that $W = \varnothing$, and we wish to show surjectivity at x, i.e. $Z \neq \varnothing$.

Because spreading out behaves well with fiber products, we can similarly define the spread-out of x, U, W, Z as $\chi, \mathcal{U}, \mathcal{W}, \mathcal{Z}$.

Sketch of proof:

- Reduce the problem into showing that given $W = \varnothing$, show that $Z \neq \varnothing$.
- Spread out to get $\mathcal{X}, F, \chi, \mathcal{U}, \mathcal{W}, \mathcal{Z}$.
- $W = \varnothing$ implies $\mathcal{W} \times_R K = \varnothing$, where $K = \operatorname{Frac} R$. This implies the image of $\pi_{\mathcal{W}} : \mathcal{W} \to \operatorname{Spec} R$, which is constructible by Chevalley, does not include the generic point η_R. So $\eta_R \notin \overline{\operatorname{im} \pi_{\mathcal{W}}}$, so we may invert finitely many elements of R so that $\operatorname{im} \pi_{\mathcal{W}} = \varnothing$, i.e. $\mathcal{W} = \varnothing$.
- Let t be a closed point in $\operatorname{Spec} R$, $F_t : \mathcal{X}_t \to \mathcal{X}_t$ be the induced map. Then $\kappa(t)$ is a finite field $\mathbb{F}_q$. Because $\mathcal{W}_t(\mathbb{F}_q) = \varnothing$, the map $\mathcal{X}_t(\mathbb{F}_q) \to \mathcal{X}_t(\mathbb{F}_q)$ is injective, hence surjective. So $\mathcal{Z}_t \neq \varnothing$ for all closed points t.
- So $\pi_{\mathcal{Z}} : \mathcal{Z} \to \operatorname{Spec} R$ has image containing all closed points, which are dense in $\operatorname{Spec} R$. So the generic point η_R is contained in the image, which is constructible by Chevalley. So $\mathcal{Z} \times_R K \neq \varnothing$, which implies $Z \neq \varnothing$. This concludes the proof.

5.15.2. Lemma. *Let S be a constructible set in $\operatorname{Spec} R$, R Noetherian. If $\eta_R \notin S$, then $\eta_R \notin \overline{S}$.*

Proof. Write $S = \coprod_i (U_i \cap K_i)$ as the disjoint union of locally closed sets over a finite index set. Then $\overline{S} = \bigcup_i \overline{U_i \cap K_i}$. Suppose for contradiction $\eta_R \in \overline{U_i \cap K_i}$ for some i, then $\operatorname{Spec} R = \overline{U_i \cap K_i} \subseteq K_i$, so $K_i = \operatorname{Spec} R$ and U_i is a dense open in $\operatorname{Spec} R$, so $\eta_R \in U_i$, which implies $\eta_R \in S$, a contradiction. □

5.15.3. Lemma. *Let $k \subseteq \mathbb{C}$ be a subfield, V a k-variety. Then the following are equivalent:*

- $V = \varnothing$;
- $V_{\mathbb{C}} := V \times_k \mathbb{C} = \varnothing$;
- $V_{\mathbb{C}}(\mathbb{C}) = \varnothing$.

5.16. Proper maps. Just as separatedness captures the topological concept of a Hausdorff space, properness is meant to capture the concept of compactness. Of course, quasicompactness won't do the job. Recall the topological notion:

5.16.1. Definition. A map of topological spaces is *proper* if the inverse image of any compact set is compact.

5.16.2. Definition. A *universally closed* map $f : M \to N$ of topological spaces is one such that for all $P \to N$, $f_P : P \times_N M \to P$ is a closed map.

We remark that the map from M to a point is universally closed iff M is compact.

The same definition moves over to schemes:

5.16.3. Definition. A *universally closed* morphism $f : X \to Y$ of schemes is one such that for all $Z \to Y$, $f_Z : Z \times_Y X \to Z$ is a closed morphism.

5.16.4. Definition. A morphism of schemes $\pi : X \to Y$ is *proper* if it is finite type, separated, and universally closed.

So, $X \to \operatorname{Spec} k$ being universally closed corresponds to X being "compact".

5.16.5. Example. Examples of proper morphisms:

- Closed embeddings;
- Properness is stable under composition and base change;
- $\mathbb{P}^n_A \to \operatorname{Spec} A$ is proper; as a consequence, any projective morphism $Z \hookrightarrow \mathbb{P}^n_A \to \operatorname{Spec} A$ is proper.
- In contrast, $\mathbb{A}^1_{\mathbb{C}}$ is not proper (this fits your intuition that a line is not compact). This can be seen by the following square:

$$\begin{tikzcd}
\mathbb{A}^2 \arrow[r] \arrow[d] & \mathbb{A}^1 \arrow[d] \\
\mathbb{A}^1 \arrow[r] & \bullet
\end{tikzcd}$$

But the left map is not closed: $V(xy - 1)$ maps to $D(x)$, which is not closed.

5.17. Chow's lemma. Chow's lemma says that "a proper morphism is fairly close to being a projective morphism". Note that by the fundamental theorem of elimination theory, projective morphisms are proper.

5.17.1. Theorem (Chow)**.** *Let $f : X \to S$ be a separated, finite type morphism of Noetherian schemes. Then for there exists a diagram*

$$\begin{tikzcd}
X' \arrow[r, hook, "i"] & \mathbb{P}^n_X \arrow[r, "f'"] \arrow[d, "\pi'"] & \mathbb{P}^n_S \arrow[d, "\pi"] \\
& X \arrow[r, "f"] & S
\end{tikzcd}$$

where the square is Cartesian, i is a closed immersion, $f' \circ i$ is an immersion, and $\pi' \circ i$ is surjective and induces an isomorphism on a dense open set $U \subseteq X$.

In the case f is proper, f' must then be closed, so X' is a projective S-scheme that surjects onto X and is an isomorphism over a dense open of X.

5.18. Valuative criteria.

5.18.1. Theorem (valuative criteria)**.** *We have the following criteria:*

- *Let $f : X \to Y$ be quasiseparated, then f is separated iff for every valuation ring V with field of fractions K, $X_Y(V) \to X_Y(K)$ is injective.*
- *Let $f : X \to Y$ be quasicompact, then f is universally closed iff for every valuation ring V with field of fractions K, $X_Y(V) \to X_Y(K)$ is surjective.*
- *Let $f : X \to Y$ be quasiseparated and finite type, then f is proper iff for every valuation ring V with field of fractions K, $X_Y(V) \to X_Y(K)$ is bijective.*

(Aside: in fact, universally closed implies quasicompact. Also, a map of schemes is a closed immersion if and only if it is a proper monomorphism.)

6. Dimension and smoothness

6.1. Definitions of dimension. The Krull dimension of a scheme is a purely topological construction and does not depend on the sheaf structure.

6.1.1. Lemma. *Let X be a topological space, $U \subseteq X$ open. Then there is a bijection between closed irreducible subsets of U and closed irreducible subsets of X that meet U, given by*

$$\begin{aligned} K \subseteq U &\longmapsto \overline{K} \subseteq X \\ L \cap U \subseteq U &\longleftarrow\!\shortmid L \subseteq X. \end{aligned}$$

Proof. First, we show that given a closed irreducible set $K \subseteq X$ that meets U, $\overline{K \cap U} = K$. Because K meets U, $K \cap U^c \neq K$, so because $K = \overline{K \cap U} \cup (K \cap U^c)$ is irreducible, $K = \overline{K \cap U}$.

Next, we show that given a closed subset $K \subset U$, $\overline{K} \cap U = K$. Clearly $K \subseteq \overline{K} \cap U$. Since K is closed in U, $K = L \cap U$ for some closed $L \subseteq X$. Then $\overline{K} \cap U \subseteq L \cap U = K \subseteq \overline{K} \cap U$, so equality holds.

Now we are ready to show the bijection. It suffices to show both maps are well-defined, since the above two paragraphs shows that the two maps are inverses of each other. Given a closed irreducible $K \subset U$, it is clear that its closure $\overline{K}$ is closed in X and meets U. To show it is irreducible, suppose $\overline{K} = C_1 \cup C_2$ for closed C_1, C_2. Then $K = \overline{K} \cap U = (C_1 \cap U) \cup (C_2 \cap U)$, so WLOG $C_1 \cap U = K$. Then $C_1 \subseteq \overline{K} = \overline{C_1 \cap U} \subseteq C_1$, so equality holds and $C_1 = \overline{K}$.

Conversely, given a closed irreducible $L \subseteq X$ that meets U, $L \cap U$ is closed in U. To show it is irreducible, suppose $L \cap U = (C_1 \cap U) \cup (C_2 \cap U)$, where $C_1, C_2 \subseteq X$ are closed. Then

$$L = \overline{L \cap U} = \overline{(C_1 \cap U) \cup (C_2 \cap U)} = \overline{C_1 \cap U} \cup \overline{C_2 \cap U},$$

so WLOG $\overline{C_1 \cap U} = L$. Then $L \cap U = \overline{C_1 \cap U} \cap U = C_1 \cap U$. This shows $L \cap U$ is irreducible, which completes the proof. □

6.1.2. Corollary. *Suppose $X = \bigcup_i U_i$ is an open cover of a topological space. Then*

$$\dim X = \sup_i \dim U_i.$$

In particular, the dimension of a scheme can be checked on any affine open cover.

Proof. Consider any sequence

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subseteq X,$$

where Z_i are irreducible and closed. Because $Z_0 \neq \varnothing$, there exists U_i such that $Z_0 \cap U_i \neq \varnothing$. Then

$$\varnothing \neq Z_0 \cap U_i \subsetneq Z_1 \cap U_i \subsetneq \cdots \subsetneq Z_n \cap U_i \subseteq U_i$$

is also a chain of irreducible closed sets by the above lemma. This shows $\dim X \leq \sup_i \dim U_i$. Conversely, for any i and a chain of irreducible closed subsets

$$\varnothing \neq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subseteq U_i$$

of U_i,

$$\varnothing \neq \overline{Z_0} \subsetneq \overline{Z_1} \subsetneq \cdots \subsetneq \overline{Z_n} \subseteq X$$

is a chain of irreducible closed sets in X, again by the above lemma. So $\dim X \geq \sup_i \dim U_i$, so equality holds. □

6.1.3. Definition. The *codimension* $\operatorname{codim}_X Y$ of an irreducible subset $Y \subseteq X$ is the supremum of lengths of increasing chains of irreducible closed subsets starting with $\overline{Y}$. The corresponding ring-theoretic notion is the *height* $\operatorname{ht}\mathfrak{p}$ of a prime ideal $\mathfrak{p}$.

Warning: Noetherian rings can be infinite-dimensional. On the other hand, Noetherian local rings must have finite dimension.

6.1.4. Theorem (Krull's height theorem). *Let A be a Noetherian ring, I a proper ideal generated by r elements, then every minimal prime of I has height at most r.*

6.1.5. Theorem (Algebraic Hartogs's Lemma). *Let A be a Noetherian integrally closed domain. Then*

$$A = \bigcap_{\operatorname{ht}\mathfrak{p}=1} A_{\mathfrak{p}}.$$

Intuitively, this says that on a normal Noetherian scheme, a rational function that is regular outside a closed set of codimension at least 2 can be uniquely extended to a regular function on the whole scheme. Compare this with Hartogs's lemma in complex analysis.

Proof. This is trivially true when $\dim A \leq 1$. In general, suppose for contradiction $x \in \operatorname{Frac} A$ belongs to $A_{\mathfrak{p}}$ for every prime of height 1, and $x \notin A$. Let $I = \{a \in A : ax \in A\}$, then $1 \notin I$, so there exists a minimal prime $\mathfrak{q} \supseteq I$. Because $I_{\mathfrak{q}} = \{a \in A_{\mathfrak{q}} : ax \in A_{\mathfrak{q}}\}$ is not equal to $A_{\mathfrak{q}}$, we see that $\mathfrak{q}$ has height at least 2.

Localize at $\mathfrak{q}$ to assume WLOG that $(A, \mathfrak{q})$ is a local ring and $\mathfrak{q}$ is the unique prime containing I. Then $\mathfrak{q} = \operatorname{rad}(I)$, and because A is Noetherian, $\mathfrak{q}$ is finitely generated, so $I \supseteq \mathfrak{q}^n$ for some n. Take the smallest such n. Consider an element $t \in \mathfrak{q}^{n-1} \backslash I$, and let $z = xt$. Because $t \notin I$, $z = xt \notin A$, but $z\mathfrak{q} \subseteq x\mathfrak{q}^n \subseteq xI \subseteq A$.

Now, if $z\mathfrak{q} \not\subseteq \mathfrak{q}$, then $z\mathfrak{q} = A$, so $\mathfrak{q} = \frac{1}{z}A$ is a principal ideal, contradicting $\operatorname{ht}\mathfrak{q} \geq 2$. So we conclude that $z\mathfrak{q} \subseteq \mathfrak{q}$, and we have a faithful $A[z]$-action on the finitely generated A-module $\mathfrak{q}$, so z is integral over A. But A is integrally closed, so $z \in A$, a contradiction. □

6.2. Dimension of fibers.

The main theorem here is the following:

6.2.1. Theorem. *Let X, Y be irreducible varieties, $\pi : X \to Y$ a dominant map. Suppose* $\dim X = a$, $\dim Y = b$. *Then:*

- *For any $y \in \operatorname{im}\pi$, $\dim \pi^{-1}(y) \geq a - b$.*
- *There exists a dense open $U \subset Y$, such that for any $y \in U$, $\dim \pi^{-1}(y) = a - b$.*
- *Given a point $x \in X$, define $e(x)$ to be the maximal* $\dim Z$, *where Z ranges among the irreducible components of $\pi^{-1}(\pi(x))$ containing x. Then $e(x)$ is an upper semi-continuous function: the sets $X_n = \{x \in X : e(x) \geq n\}$ are closed.*

6.3. Cotangent and tangent spaces.

6.3.1. Proposition. *Let X be a scheme, $f \in \mathcal{O}_x(X)$, $p \in V(f)$ a closed point, and $\overline{f}$ the image of f in $T^*_{X,p}$. Then*

$$T^*_{V(f),p} = T^*_{X,p}/\langle \overline{f} \rangle$$

6.3.2. Proposition (Jacobian computes Zariski cotangent space)**.** *Let X be a finite type k-scheme, so that locally it is* $\operatorname{Spec} k[x_1, \dots, x_n]/(f_1, \dots, f_r)$*. Then for any closed point p, $T^*_{X,p} = \operatorname{coker} J$, where $J : k^r \to k^n$ is the linear map given by the Jacobian matrix*

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_1}(p) & \cdots & \frac{\partial f_r}{\partial x_1}(p) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n}(p) & \cdots & \frac{\partial f_r}{\partial x_n}(p) \end{bmatrix}.$$

Proof. Translate p to the origin, and use the previous proposition repeatedly. □

Given a morphism of schemes $f : X \to Y$, mapping $p \in X$ to $q \in Y$, there is a naturally induced ring map $T^*_{Y,q} \to T^*_{X,p}$. If $\kappa(p) = \kappa(q)$, the above is a linear map, and we also get a map $T_{X,p} \to T_{Y,q}$.

6.4. Regularity and smoothness.

6.4.1. Proposition. *For a Noetherian local ring $(A, \mathfrak{m}, k)$, $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.*

Proof. By Nakayama, a set of generators of $\mathfrak{m}/\mathfrak{m}^2$ over k lifts to a set of generators of $\mathfrak{m}$, which is at least $\operatorname{ht} \mathfrak{m} = \dim A$. □

6.4.2. Definition (regular local ring)**.** A *regular local ring* is a Noetherian local ring $(A, \mathfrak{m}, k)$ such that $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$.

6.4.3. Definition (regularity)**.** A locally Noetherian scheme X is *regular* at $p \in X$ if $\mathcal{O}_{X,p}$ is a regular local ring. The word *nonsingular* is synonymous. Otherwise, we say X is *singular* at p.

X is *regular* if it is regular at all points, and it is *singular* otherwise.

6.4.4. Example. Regular local rings of dimension 0 are fields, while regular local rings of dimension 1 are DVRs.

6.4.5. Proposition (Jacobian criterion)**.** *Suppose $X = \operatorname{Spec}[x_1, \dots, x_n]/(f_1, \dots, f_r)$ has pure dimension d. (As usual, $k = \overline{k}$). Then a k-point $p \in X$ is regular iff $\dim \operatorname{coker} J(p) = d$ at p.*

Proof. We know $\dim T^*_{X,p} = \dim \operatorname{coker} J(p) = d$. So it suffices to show that $\dim \mathcal{O}_{X,p} = d$. But this is clear since p is a closed point and X has pure dimension d. □

In fact, for finite-type k-schemes, it suffices to check regularity at closed points (this is a hard fact). So for such schemes, regular of pure dim d is equivalent to every irreducible component having dim d and $\dim \operatorname{coker} J(p) = d$ for all k-points p. But this still requires $k = \overline{k}$. For general k, we have an alternate notion of *smoothness over* $\operatorname{Spec} k$:

6.4.6. Definition. A scheme X/k is *smooth of dimension d over k* if there exists an affine cover by $\operatorname{Spec} k[x_1, \dots, x_n]/(f_1, \dots, f_r)$, for which the Jacobian matrix has $\dim \operatorname{coker} = d$ at all points.

Remark: k-smoothness is equivalent to the Jacobian being corank d everywhere for every affine open cover (and by any choice of generators of the ring corresponding to such an open set).

Regularity/smoothness correspond to the notion of "smoothness" in the world of manifolds. So:

schemes	manifolds
Separated	Hausdorff
Universally closed	Compact
Proper	Compact + Hausdorff
Krull dimension	Dimension
Zariski (co)tangent space	(Co)tangent space
Regular, smooth	Smooth
Singular	Singular

More or less by definition, for a finite type scheme X/k of pure dim d, where $k = \overline{k}$, X is regular at all closed points iff X is smooth over k.

6.4.7. Theorem. *Comparison between regularity and smoothness:*

(a) If k is perfect, every regular finite type k-scheme is smooth over k.
(b) Every smooth k-scheme is regular (with no hypotheses on perfection).

6.4.8. Example. Let $k = \mathbb{F}_p(t)$, L a field extension given by $L = k[x]/(x^p - t)$. Let $X = \operatorname{Spec} L$, then it is regular since L is a field. But it is not smooth of dimension 0 since the derivative of $x^p - t$ vanishes.

6.4.9. Theorem. *Regular local rings are domains, so regular implies reduced. (In fact, they are UFDs, but this is a much harder fact.)*

6.5. Bertini's theorem.

6.5.1. Theorem (Bertini)**.** *Suppose X is a smooth subvariety of $\mathbb{P}^n_k$. Then there is a dense open $U \subseteq \mathbb{P}^{n*}_k$ such that for any closed point $H \in U$ (corresponding to a hyperplane in $\mathbb{P}^n_k$), H does not contain any irreducible component of X, and $H \cap X$ is k-smooth.*

7. Quasicoherent sheaves

7.1. Basic definitions.

7.1.1. Definition. Let X be a scheme. A *quasicoherent sheaf* $\mathcal{E}$ on X is an $\mathcal{O}_X$-module where there exists an affine cover $\{U_i = \operatorname{Spec} A_i \subseteq X\}$, such that $\mathcal{E}|_{U_i} \cong \widetilde{M_i}$ for A_i-modules M_i.

7.1.2. Proposition. *Let $X = \operatorname{Spec} A$, $\mathcal{E}$ a quasicoherent sheaf on X, then $\mathcal{E} \cong \widetilde{M}$ for $M = \Gamma(X, \mathcal{E})$.*

Proof. Define $\phi : \widetilde{M} \to \mathcal{E}$ on each $D(f)$ by the natural map $M_f \to \Gamma(D(f), \mathcal{E})$. Check that these are bijections using the sheaf axioms. □

7.1.3. Definition. Let X be Noetherian, then $\mathcal{E}$ is a *coherent* sheaf if there exists an affine cover $\{U_i = \operatorname{Spec} A_i \subseteq X\}$, such that $\mathcal{E}|_{U_i} \cong \widetilde{M_i}$ for *finitely generated* A_i-modules M_i.

Warning: locally free of rank r is not an affine local condition.

7.1.4. Proposition. *There is an equivalence of categories A-Mod $\longleftrightarrow$ QCoh(Spec A).*

7.1.5. Corollary. *Exact sequences of qcoh sheaves implies exactness on* affine *opens.*

7.1.6. Example. Tensor product of qcoh sheaves: on affine opens, $(\mathcal{E}_1 \otimes \mathcal{E}_2)(U) \cong \mathcal{E}_1(U) \otimes \mathcal{E}_2(U)$. This is the same as the sheafification of the obvious presheaf tensor product.

7.1.7. Proposition. *Let $\mathcal{F}$ be a finite type qcoh sheaf on X, then its rank at a point is upper-semicontinous on X.*

7.2. f_* and f^*.

7.2.1. Proposition. *Let $f : X \to Y$ be qcqs. If $\mathcal{E} \in \operatorname{QCoh}(X)$, then $f_*\mathcal{E} \in \operatorname{QCoh}(Y)$.*

7.2.2. Definition. f^* in the affine case: for $f : \operatorname{Spec} A \to \operatorname{Spec} B$, $\mathcal{F} = \widetilde{N}$, then $f^*\mathcal{F} = \widetilde{A \otimes_B N}$.

In general, cover $f : X \to Y$ by $f|_U : U \to V$ between affine opens. Pull $\mathcal{F}$ back on each of them, and glue together by universal property. Quasicoherence is obvious.

7.2.3. Proposition. $f^* \dashv f_*$. □

7.2.4. Proposition. *The pullback f^* sends coherent sheaves (resp. locally free of rank r) on Y to coherent sheaves (resp. locally free of rank r) on X.*

7.2.5. Proposition (base change map)**.**

7.2.6. Proposition (projection formula)**.** *Let $\pi : X \to Y$ be qcqs, and $\mathcal{F}, \mathcal{G}$ QCoh sheaves on X, Y. Then there is a natural map $\pi_*\mathcal{F} \otimes \mathcal{G} \to \pi_*(\mathcal{F} \otimes \pi^*\mathcal{G})$, which is an isomorphism when either (1) $\mathcal{G}$ is locally free or (2) π is affine.*

7.3. Invertible sheaves.

7.3.1. Definition. An *invertible sheaf* on X is an $\mathcal{O}_X$-module locally free of rank 1.

Why are invertible sheaves so important?

- Use global sections of an invertible sheaf $\mathcal{L}$ as replacement for $\Gamma(X, \mathcal{O}_X)$.
- Invertible sheaves are "dual" to Weil divisors.

Invertible sheaves are preserved under $\otimes$.

7.3.2. Definition. The *dual* $\mathcal{L}^\vee$ of a qcoh sheaf $\mathcal{L}$ is defined on affine opens by

$$\Gamma(U, \mathcal{L}^\vee) := \operatorname{Hom}_{\Gamma(U,\mathcal{O}_U)}(\Gamma(U, \mathcal{L}), \Gamma(U, \mathcal{O}_U)).$$

This is also a qcoh sheaf. There is a natural pairing

$$\mathcal{L} \otimes \mathcal{L}^\vee \to \mathcal{O}_X$$

which is an isomorphism when $\mathcal{L}$ is invertible.

7.3.3. Definition. The invertible sheaves on X forms an abelian group, called the Picard group $\operatorname{Pic}(X)$. Given $f : X \to Y$, $f^* : \operatorname{Pic}(Y) \to \operatorname{Pic}(X)$ is a group homomorphism.

7.3.4. Example. Consider $X = \mathbb{P}^1$, then there is a homomorphism $\mathbb{Z} \to \operatorname{Pic}(X)$ mapping $a \mapsto \mathcal{O}(a)$. This is in fact an isomorphism.

In general, for $X = \mathbb{P}^n$, then we can similarly define $\mathcal{O}(a)$, and $\mathbb{Z} \to \operatorname{Pic}(X)$ is again an isomorphism.

7.4. Weil divisors. Let X be a Noetherian irreducible regular scheme. (Regular local rings are UFDs, so X will be factorial.)

In topology, for a smooth compact oriented manifold M with dimension d, $H^k(M) \cong H_{d-k}(M)$. For schemes and $k = 1$, the left side is $\operatorname{Pic}(X)$, and the right side should be "codimension 1 subsets of X".

Let $p \in X$ be a codimension-1 point. Then $\mathcal{O}_{X,p}$ is a DVR. For $f \in K(X)$, we may define $v_p(f)$ by the discrete valuation.

7.4.1. Definition. A *Weil divisor* on X is a $\mathbb{Z}$-linear finite sum of irreducible codimension-1 subsets $\sum a_Y[Y]$.

For nonzero $f \in K(X)$, its principal Weil divisor

$$\operatorname{div} f = \sum_Y v_Y(f)[Y].$$

This is a finite sum.

By Hartogs's lemma 6.1.5, if $f \in K(X)^\times$ such that $v_Y(f) \geq 0$ for all Y, then $f \in \mathcal{O}_X(X)$. If $(f) = 0$, then both $f, f^{-1} \in \mathcal{O}_X(X)$, so $f \in \mathcal{O}_X(X)^\times$.

It is not hard to see that the principal divisors on $\mathbb{P}^1$ all have degree 0. In contrast, all Weil divisors of $\mathbb{A}^1$ are principal.

7.4.2. Definition. The *class group* of X is $\operatorname{Cl}(X) = \operatorname{Weil}(X)/\operatorname{Prin}(X)$.

7.4.3. Example. Let $X = \operatorname{Spec} \mathcal{O}_K$, then $\operatorname{Cl}(X) = \operatorname{Cl}_K$.

7.4.4. Theorem. *There is a natural isomorphism* $\operatorname{Pic}(X) \to \operatorname{Cl}(X)$.

Given $\mathcal{L} \in \operatorname{Pic}(X)$, and a nonzero section $s \in \Gamma(X, \mathcal{L})$, consider an irred codim 1 subset Y and its generic point p_Y. Pick an open neighborhood U of p_Y (equivalently, $U \cap Y \neq \infty$), such that $\mathcal{L}|_U \cong \mathcal{O}_U$, so that we can talk about $v_Y(s) = v_Y(s|_U)$. This is easily checked to be well-defined. So we can define

$$\operatorname{div}(s) := \sum_Y v_Y(s)[Y] \in \operatorname{Weil}(X).$$

7.4.5. Example. Consider the line bundle $\mathcal{O}(1)$ on $\mathbb{P}^1 = U_0 \cup U_1$, and the section s given by $t \in k[t]$ on U_0, and by $1 \in k[t^{-1}]$ on U_1. Then $\operatorname{div}(s) = [0]$ has degree 1.

7.4.6. Definition. A *rational section* of $\mathcal{L}$ is a section of $\mathcal{L}$ over some dense open $V \subset X$, modulo equivalence; two rational sections are the same if they agree on some smaller open.

Given any nonzero rational section s of $\mathcal{L}$, we may similarly define $\operatorname{div}(s)$: this time, s only represents a section on $U \cap V$, hence a rational function on U, to which we may still associate $v_Y(s)$. The set of $(\mathcal{L}, s)$ with $\otimes$ forms a group. What we will show is:

$$\begin{tikzcd}
0 \arrow[r] & K(X)^\times/\mathcal{O}_X(X)^\times \arrow[r] \arrow[d, "\cong"] & (\mathcal{L}, s) \arrow[r] \arrow[d, "\cong"] & \operatorname{Pic}(X) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \operatorname{Prin}(X) \arrow[r] & \operatorname{Weil}(X) \arrow[r] & \operatorname{Cl}(X) \arrow[r] & 0.
\end{tikzcd}$$

To show theorem 7.4.4, we need to show bijectivity of the middle vertical map.

Injectivity: Suppose $\operatorname{div}(s) = 0$ is defined on dense open V. For any irreducible codimension-1 D with generic point p, pick an affine open neighborhood $U = \operatorname{Spec} A$ of $p = [\mathfrak{p}]$, then there is an isomorphism $\mathcal{L}|_U \xrightarrow{\phi} \mathcal{O}_U$. Then the rational function that s corresponds to belongs to $A_\mathfrak{p}$. Since this holds for all height-1 $\mathfrak{p} \subset A$, $s \in A = \mathcal{O}_U(U)$. So these glue together to form a global section $s \in \mathcal{O}_X(X)$. We will show that the map $\mathcal{O}_X \to \mathcal{L}$ defined by s is an isomorphism. Indeed, locally, after composing with local trivializations $\phi : \mathcal{L}|_U \to \mathcal{O}_U$, $\phi s : \mathcal{O}_U \to \mathcal{O}_U$ still has no zeros and no poles, so it belongs to $\mathcal{O}_U(U)^\times$, i.e. is an isomorphism. Since ϕ and ϕs are both isomorphisms, so is s locally, hence globally.

Surjectivity: suppose D is a Weil divisor. Define the sheaf $\mathcal{O}(D)$ as follows: on any $U \subset X$ dense open, define

$$\Gamma(U, \mathcal{O}(D)) := \{x \in K(X)^\times : \operatorname{div}(x|_U) + D|_U \geq 0\}.$$

Define a rational section s_D of $\mathcal{O}(D)$ to be $1 \in \Gamma(U, \mathcal{O}(D)) \subseteq K(X)^\times$, where U is the complement of $\operatorname{Supp} D$. We claim that $(\mathcal{O}(D), s_D)$ is the desired preimage.

1. To show that $\mathcal{O}(D)$ is a line bundle: first, we find an open cover of X, where on each open set U, $D|_U$ is principal. Suppose $S = \operatorname{Supp} D$, then $X \backslash S$ is such an open. We then construct such an open neighborhood of each $p \in S$. Consider any irreducible divisor Y where $p \in Y$. Since X is factorial, every stalk $\mathcal{O}_{X,p}$ is a UFD. Since any open neighborhood of p contains the generic point η_Y of Y, there is a natural injection $\mathcal{O}_{X,p} \to \mathcal{O}_{X,\eta_Y}$. For each affine neighborhood $U = \operatorname{Spec} A$ of $p = [\mathfrak{p}]$ and $\eta_Y = [\mathfrak{q}]$, this is the natural localization $A_\mathfrak{p} \to A_\mathfrak{q}$. The preimage of $\mathfrak{q}A_\mathfrak{q}$ under this map is a height 1 prime in $\mathcal{O}_{X,p}$, a UFD, so it is principal, say generated by $f \in \mathcal{O}_{X,p} \subseteq K(X)$. WLOG we may choose $f \in A$, then f has no poles in U, and if it has a zero at a divisor Y' containing p, say with generic point $\eta_{Y'}$, then the preimage of $\mathfrak{m}_{\eta_{Y'}}$ in $\mathcal{O}_{X,p} \to \mathcal{O}_{X,\eta_{Y'}}$ is another height 1 prime $\mathfrak{r}$ containing f. Then $\mathfrak{q} = (f) \subseteq \mathfrak{r}$, which implies $\mathfrak{q} = \mathfrak{r}$. This shows that f only has a zero of order 1 at η_Y.

Now, let

$$U' = U \cap (X \backslash \bigcup_{\substack{Z \text{ irred codim 1} \\ p \notin Z}} Z)$$

which contains p, so it is a dense open. On U', $\operatorname{div}(f) = [Y]$.

Now, suppose $p \in Y_1, \ldots, Y_n$ where $D = \sum n_i[Y_i]$. Choose f_i so that on an open neighborhood of p, $\operatorname{div}(f_i) = [Y_i]$. Then on their intersections, which is an open neighborhood U of p,

$$\operatorname{div}|_U(\prod f_i^{n_i}) = \sum n_i[Y_i] = D|_U.$$

This shows that we can find an open cover of X where D is locally principal. Now, fix one open U in the cover, where $D = \operatorname{div}|_U(s)$. For each affine open $V \subseteq U$, there is an isomorphism $\Gamma(V, \mathcal{O}(D)) \cong \mathcal{O}_U(V)$ by sending $t \mapsto st$. This is functorial, so they glue together to form $\mathcal{O}(D)|_U \cong \mathcal{O}_U$. This shows that $\mathcal{O}(D)$ is locally free of rank 1.

2. To show that $\mathcal{O}(\operatorname{div}(s)) \cong \mathcal{L}$ for $(\mathcal{L}, s)$: We claim that any open U that trivializes $\mathcal{L}$ satisfies $\mathcal{O}(\operatorname{div}(s))|_U \cong \mathcal{O}_U$. Suppose $\mathcal{L}|_U \cong \mathcal{O}_U$ takes s to a rational function on U, which we also denote by s. Then for any affine open $V = \operatorname{Spec} A \subseteq U$,

$$\begin{aligned}
\Gamma(V, \mathcal{O}(\operatorname{div}(s))) &= \{t \in K^\times : \operatorname{div}_V(t) + \operatorname{div}_V(s) \geq 0\} \\
&= \{t \in K^\times : \operatorname{div}_V(st) \geq 0\} \\
&= \{t \in K^\times : st \in A\} \\
&= s^{-1}A,
\end{aligned}$$

which is isomorphic to $\mathcal{O}_V(V) = A$ as A-modules by sending t to st. Furthermore, this isomorphism is clearly functorial as V ranges among affine open subsets of U, so this induces an isomorphism of sheaves $\mathcal{O}(\operatorname{div}(s))|_U \cong \mathcal{O}_U$. Composing this with $\mathcal{O}_U \cong \mathcal{L}|_U$, for sections over U, this is the bijection sending t to st. Now, the set of Us (open sets trivializing $\mathcal{L}$) forms a base of the Zariski topology on X, and the isomorphism $\Gamma(U, \mathcal{O}(\operatorname{div}(s))) \to \Gamma(U, \mathcal{L})$ is clearly functorial, so this defines an isomorphism of sheaves $\mathcal{O}(\operatorname{div}(s)) \to \mathcal{L}$.

Suppose the canonical section "1" is a section of $\mathcal{O}(\operatorname{div}(s))$ over U. Its image is a section which, on each V in part (a) (i.e. affine opens that trivialize $\mathcal{L}$), agrees with $s|_V$. So its image is s by the sheaf axiom.

7.4.7. Corollary. $\operatorname{Pic}(\mathbb{P}^n_k) \cong \mathbb{Z}$.

Proof. There is an exact sequence $0 \to \mathbb{Z} \to \operatorname{Weil}(\mathbb{P}^n) \to \operatorname{Weil}(\mathbb{A}^n) \to 0$, where $\mathbb{A}^n = U_0$ is the complement of a hyperplane, and $\mathbb{Z}$ is freely generated by that hyperplane. This induces an exact $0 \to \mathbb{Z} \to \operatorname{Cl}(\mathbb{P}^n) \to \operatorname{Cl}(\mathbb{A}^n) \to 0$. But $\operatorname{Cl}(\mathbb{A}^n) = 0$. □

7.5. Quasicoherent sheaf of graded module.

7.6. Sections of line bundles. One theme we see here is that global sections of line bundles on X serve a similar purpose as functions on X.

7.6.1. Definition. Let X be a scheme, $\mathcal{L} \in \operatorname{Pic}(X)$, $s \in \Gamma(X, \mathcal{L})$, $p \in X$. The *value* of s at p, $s(p)$, is the image of s in the *fiber* $\mathcal{L}|_p := \mathcal{L}_p/\mathfrak{m}_p\mathcal{L}_p = \mathcal{L}_p \otimes_{\mathcal{O}_{X,p}} \kappa(p)$, which is naturally a 1-dim $\kappa(p)$-vector space. (In general this makes sense for any quasicoherent sheaf.)

For $s \in \Gamma(X, \mathcal{L})$, the locus of points where s does not vanish is denoted by $D(s)$. This is open.

A map $X \to \mathbb{A}^n_k$ is equivalent to choosing n global sections of $\mathcal{O}_X$. The analogous fact is:

7.6.2. Proposition. *Let X be an A-scheme, for a ring A. The following data are equivalent:*

- *A map $f : X \to \mathbb{P}^n_A$;*
- *A line bundle $\mathcal{L} \in \operatorname{Pic}(X)$, and sections $s_0, \ldots, s_n \in \Gamma(X, \mathcal{L})$, such that $X = \bigcup D(s_i)$.*

When $A = k$, on k-points, this is the map $X(k) \to \mathbb{P}^n(k)$ given by $p \mapsto [s_0(p), \ldots, s_n(p)]$.

Proof. $(\Longleftarrow)$: Recall that affine schemes $U_i = \operatorname{Spec} A[x_{0/i}, \ldots, x_{n/i}]$ cover $\mathbb{P}^n_A$. Given $(\mathcal{L}, s_0, \ldots, s_n)$, we define maps $D(s_i) \to U_i$ by specifying a ring homomorphism $A[x_{0/i}, \ldots, x_{n/i}] \to \Gamma(D(s_i), \mathcal{O}_X)$. Because $s_j \in \Gamma(D(s_i), \mathcal{L})$ and $s_i^{-1} \in \Gamma(D(s_i), \mathcal{L}^\vee)$, there is an element $s_j s_i^{-1} \in \Gamma(D(s_i), \mathcal{O}_X)$, which we map $x_{j/i}$ to. To check that these glue together, it suffices to show that

$$\begin{tikzcd}
A[x_{0/i}, \ldots, x_{n/i}]_{x_{j/i}} \arrow[r] \arrow[d] & \Gamma(D(s_i) \cap D(s_j), \mathcal{O}_X) \arrow[d, equal] \\
A[x_{0/j}, \ldots, x_{n/j}]_{x_{i/j}} \arrow[r] & \Gamma(D(s_i) \cap D(s_j), \mathcal{O}_X)
\end{tikzcd}$$

This is true because $x_{k/i} \mapsto x_{k/j} x_{i/j}^{-1} \mapsto s_k s_j^{-1} (s_i s_j^{-1})^{-1} = s_k s_i^{-1}$.

$(\Longrightarrow)$: Let $\mathcal{L} = f^* \mathcal{O}_{\mathbb{P}^n_A}(1)$, and $s_i = f^* x_i$ where $x_i \in A[x_0, \ldots, x_n]_{\deg 0} \cong \Gamma(\mathbb{P}^n_A, \mathcal{O}(1))$. Then $D(s_i) = D(f^* x_i) = f^{-1}(D(x_i))$, so $X = \bigcup D(s_i)$. □

7.6.3. Definition. Let $\mathcal{F}$ be a finite type quasicoherent sheaf on X. Say $\mathcal{F}$ is *globally generated* if for any point $p \in X$, there exists a set of $s_i \in \Gamma(X, \mathcal{F})$ such that $s_i(p)$ generate $\mathcal{L}|_p$ over $\kappa(p)$. Equivalently (Nakayama), there is a surjection of sheaves $\mathcal{O}^{\oplus I} \twoheadrightarrow \mathcal{L}$ where I is an index set.

7.6.4. Definition. Let X be a k-scheme. A finite dimensional k-subspace $W \subset \Gamma(X, \mathcal{L})$ is called a *linear series*. It is a *complete linear series* if $W \cong \Gamma(X, \mathcal{L})$ and is often written $|\mathcal{L}|$. Given a linear series W, the *base locus* is the set of points where all of W vanish. Then if W globally generates $\mathcal{L}$, we get a map $X \to \mathbb{P}^{\dim W - 1}_k$. We say $\mathcal{L}$ is *basepoint free* if is is globally generated.

7.6.5. Example. The Veronese embedding $\mathbb{P}^n \to \mathbb{P}^{\binom{n+1}{d}-1}$ can be seen as the map corresponding to picking the degree-d monomials in $\Gamma(\mathbb{P}^n, \mathcal{O}(d)) \cong k[x_0, \ldots, x_n]_{\deg d}$, which globally generate $\mathcal{O}(d)$.

7.6.6. Example. All maps $\mathbb{P}^m \to \mathbb{P}^n$ are be characterized by choosing a d and $n+1$ degree-d homogeneous polynomials in $k[x_0, \ldots, x_m]$ with no common zeros.

7.6.7. Theorem (Serre's Theorem A)**.** *Suppose $S_\bullet$ is generated in degree 1, and finitely generated over $A = S_0$. Then for any finite type quasicoherent sheaf $\mathcal{F}$ on $\operatorname{Proj} S$, there exists n_0 such that for all $n > n_0$, $\mathcal{F} \otimes \mathcal{O}(n) = \mathcal{F}(n)$ is finitely globally generated.*

7.6.8. Theorem (Curve to projective extension)**.** *Let C/k be a smooth curve (i.e. pure dimension one), Y projective over k, $p \in C$ a closed point. Then any map $f : C - p \to Y$ (uniquely) extends to C.*

Proof. Uniqueness follows from the reduced-to-separated theorem (regular local rings are reduced). To show existence, we make several reductions:

- Assume C is affine. This is because we can choose an affine neighborhood of p, and if the function is extended to that neighborhood, then it glues with f to form an extension on the whole of C.
- Assume $Y = \mathbb{P}^n_k$. This is because: suppose we have proven the theorem for $Y = \mathbb{P}^n_k$. Then we may extend $f : C - p \to Y \to \mathbb{P}^n_k$ to a map $f : C \to \mathbb{P}^n_k$. Take affine open neighborhood $\operatorname{Spec} A \subseteq C$ of p such that its image lands in $\mathbb{A}^n_k$. Then functions vanishing on $Y \cap \mathbb{A}^n_k$ pull back to functions vanishing at generic points of the irreducible components of C, hence they vanish on the entire C (by reducedness), so $\operatorname{Spec} A \to \mathbb{A}^n_k$ factors through $Y \cap \mathbb{A}^n_k$.

Now, because C is regular and p is a closed point, $\mathcal{O}_{C,p}$ is a DVR, so we can pick a uniformizer π. Pick a neighborhood V of p, such that $\pi \in \Gamma(V, \mathcal{O}_C)$. Shrink V so that $V = \operatorname{Spec} A$ is affine, π is nonvanishing on $V - p$, and the line bundle $\mathcal{L}$ induced by f is trivialized on $V - p$. Suppose $f|_{V-p} = [f_0 : f_1 : \cdots : f_n]$, $f_i \in A_\pi$ (where $V - p = \operatorname{Spec} A_\pi$). Let $m = \min v_\pi(f_i)$, then $t^{-m} g_0, \ldots, t^{-m} g_n \in A$ are $(n+1)$ functions with no common zeros, which gives a map $V \to \mathbb{P}^n_k$ extending f. This glues with f to produce an extension on the whole C. □

7.7. Ampleness. Ample line bundles are "positive" in certain senses, and ampleness roughly means "having many sections".

7.7.1. Definition. Let X be a proper A-scheme. An invertible sheaf $\mathcal{L}$ on X is *very ample* if there exist $n+1$ sections that globally generate $\mathcal{L}$ such that the induced map to $\mathbb{P}^n_A$ is a closed embedding.

Equivalently, $X \cong \operatorname{Proj} S_\bullet$, where $S_0 = A$ and S is generated in degree 1. Then $\mathcal{L}$ is *very ample* if $\mathcal{L} = \mathcal{O}(1)$.

7.7.2. Proposition. *If $\mathcal{L}$ is very ample, then so are $\mathcal{L}^{\otimes k}$ $(k \geq 1)$.*

Proof. Suppose $\mathcal{L} = f^* \mathcal{O}_{\mathbb{P}^n}(1)$ for $f : X \to \mathbb{P}^n$. Let $g : \mathbb{P}^n \to \mathbb{P}^N$, $N = \binom{n-1}{k} + 1$ be the Veronese embedding, so that $g^* \mathcal{O}_{\mathbb{P}^N}(1) = \mathcal{O}_{\mathbb{P}^n}(k)$. Then $(g \circ f)^* \mathcal{O}_{\mathbb{P}^N}(1) = f^* \mathcal{O}_{\mathbb{P}^n}(k) = f^* \mathcal{O}_{\mathbb{P}^n}(1)^{\otimes k} = \mathcal{L}^{\otimes_k}$, so $\mathcal{L}^{\otimes_k}$ is also pulled back from $\mathcal{O}(1)$ of a projective space, and $\mathcal{L} \hookrightarrow \mathbb{P}^n \hookrightarrow \mathbb{P}^N$ is a closed embedding. □

7.7.3. Lemma (extending sections)**.** *Let X be qcqs, $\mathcal{L}$ a invertible sheaf, $s \in \Gamma(X, \mathcal{L})$, $\mathcal{F}$ a quasicoherent sheaf. Then for any $t \in \Gamma(D(s), F)$, there exists $k \geq 0$, such that*

$$t \otimes s^{\otimes k} \in \Gamma(D(s), F \otimes \mathcal{L}^{\otimes k})$$

lies in the image of $\Gamma(X, F \otimes \mathcal{L}^{\otimes k})$. □

7.7.4. Definition (ample line bundles)**.** Let X be a proper A-scheme. An invertible sheaf $\mathcal{L}$ on X is *ample* if any of the following equivalent conditions hold:

(a) $\mathcal{L}^{\otimes k}$ is very ample for some $k \geq 1$.

(a') $\mathcal{L}^{\otimes k}$ is very ample for all $k \gg 0$.

(b) For all finite type quasicoherent sheaves $\mathcal{F}$, $\mathcal{F} \otimes \mathcal{L}^{\otimes k}$ is globally generated for some $k \geq 1$.

(b') For all finite type quasicoherent sheaves $\mathcal{F}$, $\mathcal{F} \otimes \mathcal{L}^{\otimes k}$ is globally generated for all $k \gg 0$.

(c) As f varies over global sections of $\mathcal{L}^{\otimes k}$ (over all $k \geq 1$), the open sets $D(f)$ form a base of the topology on X.

(c') In the above, the affine ones already form a base.

(c") In the above, the affine ones cover X.

Proof. Clearly, (a') $\implies$ (a), (b') $\implies$ (b), and (c') $\implies$ (c), (c").

(c) $\implies$ (c'): Consider $p \in X$ and any open neighborhood U of p. WLOG U is affine and trivializes $\mathcal{L}$. Then there exists $f \in \Gamma(\mathcal{L}^{\otimes k})$ such that $D(f) \subseteq U$. This $D(f)$ is affine.

(a) $\implies$ (c): Suppose $\mathcal{L}^{\otimes k}$ is very ample. Then there is a closed immersion $i : X \hookrightarrow \mathbb{P}^n$ and $i^*(\mathcal{O}_{\mathbb{P}^n}(1)) = \mathcal{L}^{\otimes k}$. Let Z be closed in X, and p a point in the complement of Z. We wish to find a neighborhood $D(f)$ of

p disjoint from Z. We can make Z into a closed subscheme. Then $Z \hookrightarrow X \hookrightarrow \mathbb{P}^n$ is a closed subscheme, so $Z \cong \operatorname{Proj} S_\bullet$ where $S = A[x_0, \ldots, x_n]/I$ for some homogeneous ideal I. Pick a homogeneous element $s \in I$, say of degree d, so that $s \in \Gamma(\mathbb{P}^n, \mathcal{O}(d))$. Then $f := i^*s \in \Gamma(X, \mathcal{L}^{\otimes kd})$ vanishes on Z, and does not vanish at p, which is what we want.

(b) $\Longrightarrow$ (c): Similar to above, we wish to find a neighborhood $D(f)$ of p disjoint from Z. Pick $\mathcal{F} = \mathcal{I}_Z$ to be the ideal sheaf of Z. Then since $\mathcal{I}_Z \otimes \mathcal{L}^{\otimes k}$ is globally generated for some k, there exists $s \in \Gamma(X, \mathcal{I}_Z \otimes \mathcal{L}^{\otimes k})$ such that $s(p) \neq 0$. Since $0 \to \mathcal{I}_Z \to \mathcal{O}_X$ is an injection, tensoring with the locally free $\mathcal{L}^{\otimes k}$ gives an injection $0 \to \mathcal{I}_Z \otimes \mathcal{L}^{\otimes k} \to \mathcal{L}^{\otimes k}$. Let $f \in \Gamma(X, \mathcal{L}^{\otimes k})$ denote the image of s, and we claim that this works. For any U trivializing $\mathcal{L}$, $f|_U$ is the image of $s|_U$ under $0 \to \mathcal{I}_Z|_U \to \mathcal{O}_U$, hence vanishes on $Z \cap U$. So s vanishes on Z. Since $p \notin Z$, there exists a neighborhood U of p trivializing $\mathcal{L}$ where $\mathcal{I}_Z|_U \cong \mathcal{O}_U$. So since $s(p) \neq 0$, $f(p) \neq 0$ as well, as desired.

(c") $\Longrightarrow$ (b'): Let $X = \bigcup D(f_i)$ be the union of finitely many affine opens, where $f_i \in \Gamma(X, \mathcal{L}^{\otimes a})$. (By scaling, a can be chosen not to depend on i.) On each $D(f_i) = \operatorname{Spec} A_i$, $\mathcal{F}$ is just some finitely generated A_i-module, so it is globally generated by $s_{ij} \in \Gamma(D(f_i), \mathcal{F})$. Extend these to $\widetilde{s}_{ij} \in \Gamma(X, \mathcal{F} \otimes \mathcal{L}^{\otimes k})$ where k can be chosen to not depend on i, j. Then $\widetilde{s}_{ij}$ generates $\mathcal{F} \otimes \mathcal{L}^{\otimes k}$ on each stalk, hence globally generates $\mathcal{F} \otimes \mathcal{L}^{\otimes k}$. In fact, this shows that $\mathcal{F} \otimes \mathcal{L}^{\otimes (k+na)}$ is globally generated for all $n \geq 0$. Arguing similarly for all residues mod a implies the desired statement.

(c") $\Longrightarrow$ (a): Let $X = \bigcup D(f_i)$ be the union of finitely many affine opens, where $f_i \in \Gamma(X, \mathcal{L}^{\otimes a})$ and $D(f_i) = \operatorname{Spec} A_i = A[a_{ij}]/I$, where $a_{ij} \in \Gamma(D(f_i), \mathcal{O}_X)$. Extend these to $\widetilde{a}_{ij} \in \Gamma(X, \mathcal{L}^{\otimes r})$. We may choose r so that $f_i, \widetilde{a}_{ij}$ are all global sections of $\mathcal{L}^{\otimes r}$. We claim that these give a closed embedding to a projective space. Since the linear series generated by f_i is already basepoint-free, this gives us a map $X \to \mathbb{P}^N_A$. We index the coordinates of $\mathbb{P}^N_A$ correspondingly with i and ij. Then it is clear that the ring homomorphisms $A[x_i, x_{ij}]/(x_k - 1) \to \Gamma(D(f_k), \mathcal{L}^{\otimes k}) = A_k$ are surjective. This shows that $X \to \mathbb{P}^N_A$ is a closed immersion.

(a), (b) $\Longrightarrow$ (a'): very ample tensor basepoint-free is very ample. □

There is another, more geometric, interpretation of ampleness.

7.7.5. Proposition (separating points and tangent vectors)**.** *Let X be proper over $k = \overline{k}$, $\mathcal{L}$ an invertible sheaf, and V a basepoint-free linear series giving a map $f : X \to \mathbb{P}^n$. If:*

- *for any two distinct k-points $x, y \in X$, there exists $s \in V$ with $s(x) = 0$, $s(y) \neq 0$;*
- *for any k-point x and nonzero tangent vector $\theta : \operatorname{Spec} \kappa(x)[\varepsilon] \to X$, there exists a section $s \in V$ vanishing at x such that the pullback of s along θ is nonzero,*

then $\mathcal{L}$ is very ample and f is a closed immersion.

7.8. Projective morphism. Recall that a morphism $X = \operatorname{Proj} S_\bullet \to \operatorname{Spec} A$, where $S_0 = A$ and $S_\bullet$ is finitely generated in degree 1, is called *projective*. We wish to define a notion of projectiveness over any base scheme.

7.8.1. Lemma. *Given a scheme Y, and the following data:*

- *for each affine open $U \subset Y$, a scheme $Z_U \to U$;*
- *for $V \subseteq U$, a map $\rho_{UV} : Z_V \subseteq Z_U$ such that $Z_V \cong Z_U \times_U V$;*
- *for $W \subset V \subset U$, $\rho_{UW} = \rho_{UV} \circ \rho_{VW}$,*

then there exists a scheme $\pi : Z \to Y$ such that $\pi^{-1}(U) = Z_U$.

Given a scheme Y, and a *graded quasicoherent sheaf of $\mathcal{O}_Y$-algebras $\mathscr{S}_\bullet = \bigoplus_{n \geq 0} \mathscr{S}_n$* such that

- $\mathscr{S}_0 = \mathcal{O}_Y$;
- $\operatorname{Sym}^\bullet \mathscr{S}_1 := \bigoplus \operatorname{Sym}^k \mathscr{S}_1 \to \mathscr{S}_\bullet$ is surjective,

we can define $\operatorname{Proj} \mathscr{S}_\bullet \to Y$ using the above gluing lemma. Also, the line bundles on each affine open glue together over $\operatorname{Proj} \mathscr{S}_\bullet$.

7.8.2. Example. Let $\mathcal{E}$ be locally free of rank r, then define $\mathscr{S}_\bullet = \operatorname{Sym}^\bullet \mathcal{E}$. Then $\operatorname{Proj} \mathscr{S}_\bullet$ is a *projective bundle* that locally looks like $U \times \mathbb{P}^{r-1}$ on affine opens trivializing $\mathcal{E}$.

7.8.3. Definition. A morphism $\pi : X \to Y$ is *projective* if $X \cong \operatorname{Proj} \mathscr{S}_\bullet$ for some $\mathscr{S}_\bullet$ as above.

Remark. Hartshorne defines projective morphisms as $X \hookrightarrow Y \times \mathbb{P}^n \to Y$, where the first map is a closed immersion.

7.9. Curves.

7.9.1. Theorem. *The following categories are equivalent:*

1. *Integral regular projective 1-dimensional k-varieties, and surjective k-morphisms.*
2. *Integral regular projective 1-dimensional k-varieties, and dominant k-morphisms.*
3. *Integral regular projective 1-dimensional k-varieties, and dominant rational maps.*
4. *Integral 1-dimensional k-varieties, and dominant rational maps.*
5. *The opposite category of finitely generated fields of transcendence degree 1 over k, and k-morphisms.*

8. Cohomology

8.1. Properties. Let $X \to \operatorname{Spec} A$ be separated. (This isn't absolutely necessary.) We will define for each $k \geq 0$ a functor $H^k(X, -) : \operatorname{QCoh}(X) \to A\text{-Mod}$, such that:

- $H^0(X, -) = \Gamma(X, -)$;
- Short exact sequences of QCoh sheaves gets sent to long exact sequences of A-modules;
- Let $\pi : X \to Y$ be a morphism of schemes, and $\mathcal{F} \in \operatorname{QCoh}(X)$. Then there exist $\alpha_k : H^k(Y, \pi_*\mathcal{F}) \to H^k(X, \mathcal{F})$, which are isomorphisms when π is affine, that extend $\alpha^0 : \Gamma(Y, \pi_*\mathcal{F}) \to \Gamma(X, \mathcal{F})$. This gives, for $G \in \operatorname{QCoh}(Y)$, a composition
$$H^k(Y, G) \to H^k(Y, \pi_*\pi^*G) \to H^k(X, \pi^*G).$$
- If X is covered by n affine open charts, then $H^k(X, -) = 0$ if $k \geq n$. In particular, if X is affine, then $H^1(X, -) = 0$ (which we recall from earlier).
- $H^k(X, \bigoplus \mathcal{F}_j) = \bigoplus H^k(X, \mathcal{F}_j)$.

A preview of what's to come:

8.1.1. Theorem (cohomologies of $\mathcal{O}(m)$)**.** *We have:*

- $H^0(\mathbb{P}^n_A, \mathcal{O}(m)) = A^{\binom{n+m}{m}}$ *if* $m \geq 0$, *and 0 if* $m \leq 0$*;*
- $H^n(\mathbb{P}^n_A, \mathcal{O}(m)) = A^{\binom{-m-1}{-m-1-n}}$ *if* $-m-1 \geq n$, *and 0 otherwise;*
- *All other cohomologies vanish.*

8.1.2. Theorem. *Let X be projective over A, and $\mathcal{F}$ a coherent sheaf. Then $\Gamma(X, \mathcal{F})$ is a finitely generated A-module.*

PROOF. We will show in fact that $H^k(X, \mathcal{F})$ are all finitely generated over A.

Let $i : X \hookrightarrow \mathbb{P}^n_A$ be a closed embedding, then $H^k(X, \mathcal{F}) = H^k(\mathbb{P}^n_A, i_*\mathcal{F})$. So we may WLOG assume $X = \mathbb{P}^n_A$. Use descending induction on k. In the base cases $k \geq n+1$, the cohomologies all vanish.

Recall that there exists a surjection $\mathcal{O}(m)^{\oplus a} \to \mathcal{F} \to 0$. Let K be the kernel, and unwind to a long exact sequence. Suppose we want to show $H^n(X, \mathcal{F})$ is finitely generated. A segment of the long exact sequence reads:
$$\cdots \to H^n(\mathcal{O}(m)^{\oplus a}) \to H^n(\mathcal{F}) \to 0$$
and since H^n commutes with direct sums and by the explicit calculations, $H^n(\mathcal{O}(m)^{\oplus a})$ is finitely generate, so $H^n(\mathcal{F})$ is as well. Suppose now we want to show this for $n-1$. Then
$$\cdots \to H^{n-1}(\mathcal{O}(m)^{\oplus a}) \to H^{n-1}(\mathcal{F}) \to H^n(K) \to \dots,$$
and since both the left and right are finitely generated, so is the middle. □

8.2. Definition. Let $\mathscr{U} = \{U_i\}_{i=1}^n$ be an affine cover of X, and let $\mathcal{F}$ be a quasicoherent sheaf. Define the Čech complex
$$C^k_{\mathscr{U}}(X, \mathcal{F}) := \prod_{\substack{|I|=k+1 \\ I=\{i_0,\dots,i_k\}\subseteq[n]}} \Gamma(U_{i_0} \cap \cdots \cap U_{i_k}, \mathcal{F})$$
with obvious differentials
$$d : C^k_{\mathscr{U}}(X, \mathcal{F}) \to C^{k+1}_{\mathscr{U}}(X, \mathcal{F})$$
by alternatingly summing over the restriction maps. A short exact sequence of QCoh sheaves induces a short exact sequence of Čech complexes (this is where it is crucial that we're working with QCoh sheaves), which then induces the long exact sequence. It is then obvious that if X is covered by n affine open charts, then H^k vanishes for $k \geq n$.

8.2.1. Theorem. *Let X be quasicompact and separated. The Čech cohomology is independent of the (finite) affine cover $\mathscr{U}$.*

Proof. The proof proceeds in several steps.

Step 1: it suffices to show that the Čech complexes of $\{U_i\}_{i=1}^n$ and $\{U_i\}_{i=1}^{n+1}$ are quasi-isomorphic.

Step 2: The kernel of the surjection $C_{\{U_i\}_{i=1}^{n+1}}(X,\mathcal{F}) \twoheadrightarrow C_{\{U_i\}_{i=1}^{n}}(X,\mathcal{F})$ is the chain complex whose k-th term is the product over all $I \subseteq [n+1]$ containing $n+1$, $|I| = k+1$. The goal is then to show that this is exact. But this is exactly the augmented Čech complex $C_{\{U_i \cap U_{n+1}\}_{i=1}^{n}}(U_{n+1},\mathcal{F})$. So it suffices to show that for affine schemes X, the Čech cohomology vanishes except at degree 0.

Step 3: Suppose that X is affine and $\{U_i\}$ cover X, and suppose U_n already is X. Then the augmented Čech complex of X surjects onto the augmented Čech complex of $U_1 \cap \cdots \cap U_{n-1}$, and the kernel is the Čech complex for U_n, which is just the Čech complex for X shifted by one. So by the cohomology long exact sequence, the cohomology of the middle row vanishes.

Step 4: In general, suppose X is affine and $\{U_i\}$ cover X. Then there is an affine cover $D(f_j)$ where each $D(f_j)$ lies inside some $\{U_i\}$. Then the Čech complex localized at each f_i is exact, so the original complex is exact as well. □

More consequences of cohomology:

8.2.2. Proposition. *Pushforwards of coherent sheaves by projective morphisms (of locally Noetherian schemes) is coherent.*

8.2.3. Proposition. *Suppose Y is locally Noetherian. Then a morphism $\pi : X \to Y$ is projective and affine iff it is finite.*

8.2.4. Proposition. *Suppose Y is Noetherian. Then a morphism $\pi : X \to Y$ is projective and has finite fiber iff it is finite.*

8.2.5. Proposition (fiber dimension of projective morphism is upper-semicontinuous)**.** *Let $\pi : X \to Y$ be projective, and let Y be locallly Noetherian. Then the set $\{q \in Y : \dim \pi^{-1}(q) \geq k\}$ is Zariski-closed.*

8.2.6. Theorem (Serre vanishing)**.** *Let $\mathcal{F}$ be coherent on a projective X/A. Then for all $m \gg 0$, $H^i(X,\mathcal{F}(m)) = 0$ for all $i > 0$.*

8.3. Euler characteristic, Hilbert functions. We work with a projective k-scheme X, and $\mathcal{F} \in \mathrm{Con}(X)$. The *Euler characteristic*

$$\chi(\mathcal{F}) := \sum_{i \geq 0} \dim_k H^i(X,\mathcal{F}).$$

For example, for $X = \mathbb{P}^n$, $\mathcal{F} = \mathcal{O}(m)$, then

$$\chi(\mathcal{O}(m)) = \frac{1}{n!}(m+1)(m+2)\dots(m+n)$$

for *all* m, n. A general heuristic is that χ is better behaved than individual cohomology groups, and we study the individual cohomologies by proving vanishing theorems.

8.3.1. Proposition. *Let $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ be an exact sequence of coherent sheaves. Then $\chi(\mathcal{G}) = \chi(\mathcal{F}) + \chi(\mathcal{H})$.*

Let $i : X \hookrightarrow \mathbb{P}_k^N$ be a fixed embedding. Then by definition, $\mathcal{O}_X(1) = i^*\mathcal{O}_{\mathbb{P}^N}(1)$.

8.3.2. Definition. The *Hilbert function* of $\mathcal{F}$ is defined by

$$h_{\mathcal{F}}(m) = \dim_k H^0(X,\mathcal{F}(m)) = \dim_k H^0(X,\mathcal{F} \otimes \mathcal{O}_X(1)^{\otimes m}).$$

8.3.3. Example. Let $\mathcal{F} = \mathcal{I}_X$ be the ideal sheaf of X. Then we have an exact sequence

$$0 \to \mathcal{I}_X \to \mathcal{O}_{\mathbb{P}^N} \to i_*\mathcal{O}_X \to 0.$$

Tensoring with $\mathcal{O}_{\mathbb{P}^N}(m)$, we get

$$0 \to \mathcal{I}_X(m) \to \mathcal{O}_{\mathbb{P}^N}(m) \to (i_*\mathcal{O}_X)(m) \to 0.$$

By the projection formula, $(i_*\mathcal{O}_X)(m) = i_*(\mathcal{O}_X(m))$. Taking $\Gamma(\mathbb{P}^n, -)$ gives us

$$0 \to H^0(\mathbb{P}^N,\mathcal{I}_X(m)) \to H^0(\mathbb{P}^N,\mathcal{O}(m)) \to H^0(X,\mathcal{O}_X(m))$$

where the last map is just restriction to X. So in other words, $H^0(\mathbb{P}^N, \mathcal{I}_X(m))$ should be interpreted as the degree-m homogeneous polynomials in $x_0, \dots, x_N$ that vanish on X. In particular, it depends on the way X is embedded into $\mathbb{P}^N$.

8.3.4. Theorem. *The function $t \mapsto \chi(\mathcal{F}(t))$ is a polynomial in $\mathbb{Q}[t]$ whose degree is $\dim \operatorname{Supp} \mathcal{F}$.*

Hence, by Serre vanishing, for $m \gg 0$, the Hilbert function is a polynomial, called the *Hilbert polynomial* $p_{\mathcal{F}}(m)$. In particular, the Hilbert polynomial $p_X(m)$ of $\mathcal{O}_X$ is a polynomial of degree $\dim X$.

PROOF. (TODO) □

8.3.5. Example. Let $X = V(f)$ be a degree-d hypersurface. Then

$$p_X(m) = p_{\mathbb{P}^n}(m) - p_{\mathbb{P}^n}(m-d) = \frac{1}{n!}((m+1)\dots(m+n) - (m+1-d)\dots(m+n-d)).$$

In particular, its leading term is $\frac{d}{n!}m^{n-1}$.

REMARK. In general, for a closed subscheme $X \hookrightarrow \mathbb{P}^n$, its *degree* is defined as the positive integer a such that the leading coefficient of $p_X(t)$ is $\frac{a}{n!}$. Another piece of information is the constant term $p_X(0) = \chi(X, \mathcal{O}_X)$. This is one minus the arithmetic genus.

8.4. Riemman-Roch for line bundles on a regular projective curve.

Let C be a regular projective curve over k (not necessarily alg. closed), D a Weil divisor. Recall that if $D = \sum a_p[p]$, then $\deg D = \sum a_p \deg p$.

8.4.1. Theorem. *We have* $\deg D = \chi(C, \mathcal{O}(D)) - \chi(C, \mathcal{O}_C)$.

8.4.2. Definition. For a line bundle $\mathcal{L}$ on C, define its degree $\deg \mathcal{L} = \chi(C, \mathcal{O}(D)) - \chi(C, \mathcal{O}_C)$.

8.4.3. Definition. For a scheme X, the *arithmetic genus* is defined to be $g = 1 - \chi(X, \mathcal{O}_X)$. When X is a integral projective curve over an algebraically closed field, it is true that $h^0(X, \mathcal{O}_X) = 1$, so $h^1(X, \mathcal{O}_X) = g$.

8.5. Remarks on sheaf cohomology.

8.5.1. Theorem (Künneth formula)**.** *Let X, Y projective schemes over k, $\mathcal{F} \in \mathrm{QCoh}(X)$, $\mathcal{G} \in \mathrm{QCoh}(Y)$. Define $\mathcal{F} \boxtimes \mathcal{G} = \pi_1^*\mathcal{F} \otimes \pi_2^*\mathcal{G}$, where π_1, π_2 are projection maps from $X \times Y$. Then*

$$H^m(X \times Y, \mathcal{F} \boxtimes \mathcal{G}) = \bigoplus_{p+q=m} H^p(X, \mathcal{F}) \otimes_k H^q(Y, \mathcal{G}).$$

8.5.2. Theorem (cup product)**.** *There is a ...*

8.6. Baby intersection theory.

8.6.1. Definition. Let X be a smooth projective scheme over k. Given a line bundles $\mathcal{L}_1, \dots, \mathcal{L}_n$

9. Curves of small genus

We use the machinery of cohomology of line bundles to study curves of small genus.

9.1. Definition. In this section, a *curve* C is a projective, geometrically integral, geometrically regular, dimension-1 scheme over a field k.

9.1. Preliminary tools.

9.1.1. Definition (degree of a finite morphism at a point)**.** Let $\pi : X \to Y$ be a finite morphism. Then $\pi_*\mathcal{O}_X$ is a finite type quasicoherent sheaf, so we may consider the rank d of $f_*\mathcal{O}_X$ at a point $y \in Y$. We call d the *degree* of π at y. Equivalently, the degree is $d = \dim_{\kappa(y)} \Gamma(\mathcal{O}_{\pi^{-1}(y)}, \pi^{-1}(y))$ (just unwind the definition).

REMARK. The degree of π is upper-semicontinuous on Y.

9.1.2. Lemma. *Let $\pi : X \to Y$ be a finite morphism of Noetherian schemes, whose degree at every point of Y is either 0 or 1. Then π is a closed embedding.*

9.1.3. Theorem (separating points and tangent vectors)**.** *Let k be algebraically closed. Let $\pi : X \to Y$ be a projective morphism of finite-type k-schemes that is injective on closed points and injective on tangent vectors at closed points. Then π is a closed embedding.*

PROOF. Since closed embeddings are affine-local on the target, we may WLOG $Y = \operatorname{Spec} B$. Since π is projective, its fiber dimension is upper-semicontinuous on Y, so $\{y \in Y : \dim \pi^{-1}(y) \geq 1\}$ is closed. If it is nonempty, then it contains a closed point, which contradicts with injectivity. So the fibers are finite type and dimension 0 over the Spec of a field, hence finite. So π is projective with finite fibers, hence finite (Theorem 8.2.4).

Now, for any *closed* point $y \in Y$, we claim that the degree of π at y is at most 1. Suppose $\pi^{-1}(y)$ is nonempty, then it contains 1 point x that is finite over $\operatorname{Spec} k$, so it has to be $\operatorname{Spec} A$, where A is a finite k-algebra with one prime ideal $\mathfrak{m}$. Then k must be the residue field. Suppose for contradiction that $\dim_k A \neq 1$, then $A_{\mathfrak{m}} \neq k$. But $A_{\mathfrak{m}} = \mathcal{O}_{\pi^{-1}(y),x} = \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,y}} k$, so $\mathfrak{m}_y \mathcal{O}_{X,x} \neq \mathfrak{m}_x$. So $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$ is not surjective as maps of k-vector spaces, which contradicts π being injective on tangent vectors, i.e. $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \to (\mathfrak{m}_y/\mathfrak{m}_y^2)^\vee$ being injective. So we conclude that the degree of π at closed points is at most 1. But since the degree of π is upper-semicontinuous, its degree at all points is at most 1. Hence we are done by the previous lemma. □

9.1.4. Lemma. *Suppose $\mathcal{L}$ is a degree $2g-2$ line bundle, then $h^0(C,\mathcal{L}) = g-1$ or g, with $h^0(C,\mathcal{L}) = g$ iff $\mathcal{L} = \omega_C$.*

9.1.5. Theorem. *Let k be algebraically closed. Suppose $\mathcal{L}$ is a line bundle on a curve C, and let $g = h^1(X, \mathcal{O}_X)$ be the arithmetic genus of C.*

- *If $\deg \mathcal{L} \geq 2g$, then $\mathcal{L}$ is basepoint-free.*
- *If $\deg \mathcal{L} \geq 2g+1$, then $\mathcal{L}$ is very ample (in fact, any basis of $\Gamma(C,\mathcal{L})$ gives a closed embedding $C \hookrightarrow \mathbb{P}_k^{\deg \mathcal{L} - g}$).*

9.2. Genus 0.

9.2.1. Example. The curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$ has genus 0, and is not isomorphic to $\mathbb{P}^1_{\mathbb{R}}$.

9.2.2. Proposition. *Any genus 0 curve C with a k-point is isomorphic to $\mathbb{P}^1_k$.*

9.2.3. Proposition. *All genus 0 curves can be described as conics in $\mathbb{P}^2_k$.*

9.2.4. Proposition. *Suppose C is a curve not isomorphic to $\mathbb{P}^1_k$, then any degree 1 line bundle $\mathcal{L}$ has $h^0(C,\mathcal{L}) < 2$. As a consequence, for degree-1 points p, q on C, $\mathcal{O}(p) \cong \mathcal{O}(q)$ iff $p = q$.*

9.3. Hyperelliptic curves.

Assume k algebraically closed with characteristic not 2.

9.3.1. Definition. A genus g curve C is *hyperelliptic* if it admits a double cover (i.e. degree 2 finite morphism) $\pi : C \to \mathbb{P}^1_k$ (which we may as well fix).

Then the preimage of any closed point consists of either 1 or 2 points.

9.3.2. Theorem (hyperelliptic Riemann-Hurwitz)**.** *Let C be a hyperelliptic curve with double cover $\pi : C \to \mathbb{P}^1_k$. Then π has $2g+2$ branch points (closed points $p \in \mathbb{P}^1_k$ where $\pi^{-1}(p)$ is a single point).*

9.3.3. Proposition. *Let $p_1, \dots, p_r$ be distinct closed points in $\mathbb{P}^1_k$. If r is even, then there is precisely one double cover branched at those points. If r is odd, then there are none.*

PROOF. Suppose 0 and ∞ are distinct from $p_1, \dots, p_r$. Then all branch points are in $\mathbb{A}^1$. Any double cover $C' \to \mathbb{A}^1$ gives rise to a quadratic field extension $K/k(x)$, which must be Galois. Find $y \in K$ such that the nontrivial element σ in the Galois group maps $y \mapsto -y$. Then $y^2 \in k(x)$, so we can replace y by an appropriate $k(x)$-multiple such that y^2 is a polynomial, monic with no repeated factors, say $y^2 = f(x) = x^N + a_{N-1}x^{N-1} + \cdots + a_0$. This is a curve C'_0 in $\mathbb{A}^2$, and by the Jacobian criterion, this curve is regular. Thus C'_0 and C' are both normalizations of $\mathbb{A}^1$ in $k[x](y)$, hence isomorphic. Because the branch points are $p_1, \dots, p_r$, we conclude that $f(x) = (x - p_1) \dots (x - p_r)$.

In the projective situation, we simply do the same for $k[u]$, $u = x^{-1}$, which gives rise to the curve C'' defined by $z^2 = (u - \frac{1}{p_1}) \dots (u - \frac{1}{p_r})$. So the double cover $C \to \mathbb{P}^1$ has to be glued using C' and C''. Thus, in $K(C)$, we must have $z^2 = u^r f(1/u) = f(x)/x^r = y^2/x^r$. If r is even, then there is a unique way to glue, i.e. identifying $z = y/x^{r/2}$. If r is odd, x does not have a square root in $k(x)[y]/(y^2 - f(x))$, so there is no way to glue C' and C'' together compatibly. □

Proof of hyperelliptic Riemann-Hurwitz. We now have an explicit description of $\pi : C \to \mathbb{P}^1_k$, in terms of covering it by two affine opens. Writing down the Čech complex then easily tells us that $g = h^1(C, \mathcal{O}_C) = \frac{r}{2} - 1$, as desired. □

9.3.4. Proposition. *Suppose $g \geq 2$. If $\mathcal{L}$ corresponds to a hyperelliptic cover $C \to \mathbb{P}^1$, then $\mathcal{L}^{\otimes(g-1)} \cong \omega_C$.*

Proof. Compose the hyperelliptic map with the $(g-1)$-th Veronese embedding

$$C \to \mathbb{P}^1 \to \mathbb{P}^{g-1}$$

then the pullback of $\mathcal{O}_{\mathbb{P}^{g-1}}(1)$ along this composition is $\mathcal{L}^{\otimes(g-1)}$. The pullback $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1)) \to H^0(C, \mathcal{L}^{\otimes(g-1)})$ is injective: if a hyperplane $s \in H^0(\mathbb{P}^{g-1}, \mathcal{O}(1))$ is pulled back to 0, then s vanishes on all of the image of C, so the image of C (a rational normal curve) is contained in a hyperplane, which is impossible. So $\mathcal{L}^{\otimes(g-1)}$ is a degree $2g-2$ line bundle that has at least g linearly independent sections, so it is equal to ω_C. □

9.3.5. Proposition. *Any curve of genus at least 2 admits at most one hyperelliptic cover.*

Proof. The hyperelliptic map, if it exists, can be reconstructed from the canonical linear series given by ω_C. □

9.3.6. Proposition. *A curve C of genus at least 1 is hyperelliptic iff it has a degree 2 line bundle $\mathcal{L}$ with $h^0(C, \mathcal{L}) = 2$.*

Proof. Suppose $\mathcal{L}$ is a degree 2 line bundle with $h^0(C, \mathcal{L}) \geq 2$. We claim $h^0(C, \mathcal{L}) = 2$. Suppose otherwise. Consider a closed point p, and the exact sequence $0 \to \mathcal{O}(-p) \to \mathcal{O}_C \to \mathcal{O}|_p \to 0$. Tensoring with $\mathcal{L}$ gives $0 \to \mathcal{L}(-p) \to \mathcal{L} \to \mathcal{L}|_p \to 0$. Writing down the long exact sequence gives $h^0(C, \mathcal{L}(-p)) + 1 \geq h^0(C, \mathcal{L}) \geq 3$, so $h^0(C, \mathcal{L}(-p)) \geq 2$. But $\mathcal{L}(-p)$ has degree 1, so this contradicts with Proposition 9.2.4. So $h^0(C, \mathcal{L}) = 2$. Let s_1, s_2 be linearly independent sections, we claim that this is basepoint-free. Suppose $\operatorname{div}(s_1) = p + q_1$, $\operatorname{div}(s_2) = p + q_2$. Then $\mathcal{O}(q_1) = \mathcal{L}(-p) = \mathcal{O}(q_2)$, which implies $q_1 = q_2$, so s_1/s_2 has no zeros and no poles and therefore constant, which contradicts them being linearly independent.

Now, return to the original problem. Suppose C is hyperelliptic, then the pullback of $\mathcal{O}_{\mathbb{P}^1}(1)$ is a degree 2 line bundle with at least 2 sections, so by our discussion above it has exactly 2 sections. Conversely, suppose $\mathcal{L}$ is a degree 2 bundle with 2 sections, then it is basepoint-free and thus gives a map to $\mathbb{P}^1$, which has degree 2. □

9.4. Genus 1: elliptic curves.

9.5. Genus 2. We claim that in this case all curves are hyperelliptic. Let C be a curve of genus $g = 2$. Then ω_C has degree $2g - 2 = 2$, and has 2 sections. By Proposition 9.3.6, it is basepoint-free and gives a double cover to $\mathbb{P}^1$. Conversely, any double cover gives a degree 2 line bundle with 2 sections, which must be ω_C.

9.6. Genus 3.

9.6.1. Proposition (canonical embedding)**.** *Let k be algebraically closed. Suppose C is not hyperelliptic, then ω_C gives a closed embedding $C \hookrightarrow \mathbb{P}^{g-1}$.*

Proof. To show ω_C is basepoint-free, it suffices to show that given any closed point p,

$$h^0(C, \omega_C(-p)) = h^0(C, \omega_C) - 1.$$

By Riemann-Roch: $h^0(C, \omega_C(-p)) - h^0(C, \mathcal{O}(p)) = \deg \omega_C(-p) - g + 1 = 2g - 3 - g + 1 = g - 2$. But $h^0(C, \mathcal{O}(p)) = 1$ by Proposition 9.2.4, so indeed $h^0(C, \omega_C(-p)) = g - 1 = h^0(C, \omega_C) - 1$.

Now, to show ω_C is very ample, it suffices to show that given any closed points p, q (not necessarily different),

$$h^0(C, \omega_C(-p-q)) = h^0(C, \omega_C) - 2.$$

By Riemann-Roch: $h^0(C, \omega_C(-p-q)) - h^0(C, \mathcal{O}(p+q)) = \deg \omega_C(-p-q) - g + 1 = 2g - 4 - g + 1 = g - 3$. Because C is not hyperelliptic, then the degree 2 line bundle $\mathcal{O}(p+q)$ must have $h^0(C, \mathcal{O}(p+q)) = 1$. So $h^0(C, \omega_C(-p-q)) = g - 2 = h^0(C, \omega_C) - 2$ as desired. □

Specializing to the genus 3 case, the canonical embedding gives an embedding $C \hookrightarrow \mathbb{P}^2$ as a degree 4 curve. Conversely, I claim that every quartic curve in $\mathbb{P}^2$ is canonically embedded. The curve has genus $1-p_C(0) = 1-\binom{2}{2}+\binom{-2}{2} = 3$. The embedding is given by a line bundle of degree 4 with at least 3 sections, so it has to be ω_C. In conclusion, there is a bijection between genus 3 non-hyperelliptic curves and quartics in $\mathbb{P}^2$ (up to $\mathrm{PGL}_3(k)$).

9.6.2. Example. The *Klein quartic* $x^3y+y^3z+z^3x=0$ has 168 automorphisms.

9.6.3. Definition. A curve admitting a degree 3 cover of $\mathbb{P}^1$ is called *trigonal.*

9.6.4. Proposition. *Every non-hyperelliptic genus 3 curve is trigonal.*

9.7. Genus 4. The canonical embedding i maps a genus 4 curve C as a sextic curve in $\mathbb{P}^3$. We claim that this is in bijection with regular complete intersections of a quadric surface and a cubic surface.

By Riemann-Roch,

$$h^0(C, i^*\mathcal{O}(2)) = h^0(C, \omega_C^{\otimes 2}) = \deg \omega_C^{\otimes 2} - g + 1 = 12-4+1 = 9,$$

while $h^0(\mathbb{P}^3, \mathcal{O}(2)) = \binom{5}{2} = 10$, so the pullback

$$H^0(\mathbb{P}^3, \mathcal{O}(2)) \to H^0(C, i^*\mathcal{O}(2))$$

has a nontrivial kernel. The kernel (which is $H^0(\mathbb{P}^3, \mathcal{I}_{C/\mathbb{P}^3} \otimes \mathcal{O}(2))$ from the closed subscheme exact sequence) is a quadric surface that contains C.

Now, this quadric surface Q is given by some quadratic form which can be represented by a matrix. We may as well diagonalize it (assuming $\operatorname{char} k \neq 2$). Its rank determines the shape of Q:

- rank 1: double plane
- rank 2: two planes
- rank 3: cone
- rank 4: regular quadric.

The first two cases cannot happen, i.e. C does not lie in a hyperplane, because $H^0(\mathbb{P}^3, \mathcal{O}(1)) \to H^0(C, \omega_C)$ is injective. So we conclude that Q is irreducible.

In addition, we claim that C cannot lie in two distinct quadric surfaces. Otherwise, by Bezout, their intersection has degree $2 \times 2 = 4 < 6$, but C is contained in this intersection, hence must have a larger degree.

So we ask, does C lie in a cubic surface? Repeating the same calculation, we see that

$$\dim \ker(H^0(\mathbb{P}^3, \mathcal{O}(3)) \to H^0(C, i^*\mathcal{O}(3))) \geq 5.$$

Since we require the cubic surface to not contain Q, a 4-dimensional subspace is forbidden, so there exists at least one cubic surface K not containing Q. Now, K and Q share no components, so $K \cap Q$ is a complete intersection, containing C as a closed subscheme. By Bezout's theorem, $K \cap Q$ has degree 6. By a calculation on Hilbert polynomials, $K \cap Q$ has genus $1-\binom{3}{3}+\binom{3-2}{3}+\binom{3-3}{3}-\binom{3-5}{3} = 4$. Since the genus and degree completely determine the Hilbert polynomial (which has degree 1), we conclude that $C = K \cap Q$.

Conversely, any regular complete intersection of a quadric Q and a cubic K is a curve C of genus 4 and degree 6. Then C does not lie inside a hyperplane, because otherwise (say it lies inside H), then $H \cap Q$ is a degree 2 curve containing C, a degree 6 curve, which is impossible. Thus, $\mathcal{O}_C(1)$ has degree 6 and at least 4 sections, so it must be equal to ω_C. This means that C is canonically embedded.

9.8. Genus 5. We can mimic the genus 4 case: the dualizing sheaf ω_C has degree $2g-2=8$ and $g=5$ sections, so it canonically embeds C as a degree 8 curve in $\mathbb{P}^4$. By Riemann-Roch,

$$h^0(C, \omega_C^{\otimes 2}) = \deg \omega_C^{\otimes 2} - g + 1 = 16-5+1 = 12,$$

while $h^0(\mathbb{P}^4, \mathcal{O}(2)) = \binom{4+2}{4} = 15$. So

$$\dim \ker(H^0(\mathbb{P}^4, \mathcal{O}(2)) \to H^0(C, \omega_C^{\otimes 2})) \geq 3.$$

Then there exist 3 linearly independent quadrics containing C. (However, we will see later that not all genus 5 curves are canonically embedded as the complete intersection of 3 quadrics; the exceptional ones are precisely the trigonal curves.)

Conversely, suppose C is the regular complete intersection of 3 quadrics. Then its genus is given by the inclusion-exclusion formula:

$$g = 1 - \binom{4}{4} + 3 \cdot \binom{4-2}{4} - 3 \cdot \binom{4-4}{4} + \binom{4-6}{4} = 5.$$

Also, C has degree $2^3 = 8$ by Bezout's theorem. To show it is canonically embedded, it suffices to show $\mathcal{O}_C(1)$ has at least 5 sections, i.e. it does not lie in a plane. Suppose it does, then C is a closed subscheme of the complete intersection of two quadrics and a plane, which is a curve of degree $2^2 = 4$. But C has degree $8 > 4$, so it cannot be contained in a curve of degree 4, a contradiction. So $\mathcal{O}_C(1)$ has degree 8 and at least 5 sections, so it must be isomorphic to ω_C, as desired.

Unfortunately, this stops working for genus $g \geq 6$:

9.8.1. Proposition. *Any canonical genus g curve, where $g \geq 6$, is not a complete intersection.*

10. Differentials

In this section we take another familiar object in differential geometry (differential forms) and transport it to schemes.

As motivation, consider the case where U is an open set in $\mathbb{R}^n$. Then we have a map $d : C^\infty(U) \to \Omega^1(U)$, mapping $f \mapsto \sum_{i=1}^n \frac{\partial f}{\partial x_i} dx_i$, which satisfies $d(fg) = f(dg) + (df)g$. On any smooth manifold M, we have the same construction on every coordinate patch, which glue together. More generally, for a smooth map $M \to N$, we have the notion of a sheaf of *relative* differential forms.

The corresponding algebraic version is the "cotangent sheaf".

10.1. Affine case.

We start from the simplest (affine) case.

10.1.1. Definition. Let $i : B \to A$ be a map of rings. The *module of derivations* is an A-module M, and a map of abelian groups $d : A \to M$ (not a map of A-modules!) such that:

- $i(B) \subset \ker d$;
- $d(aa') = a(da') + (da)a'$.

Note that then d is a map of B-modules.

10.1.2. Definition. The module of Kähler differentials $(\Omega_{A/B}, d)$ is the universal such module: given any module of derivation (M, d'), there exists a unique map of A-modules $p : \Omega_{A/B} \to M$, such that $p \circ d = d'$. It is constructed as

$$\Omega_{A/B} = \operatorname{pr} \bigoplus_{a \in A} Ada \Big/ \langle d(i(b)), d(a+a') - d(a) - d(a'), d(aa') - ad(a') - d(a)a' \rangle.$$

Note that if A is a finitely generated algebra over B by $a_1, \ldots, a_n$, then $\Omega_{A/B}$ is a finitely generated module over A by $da_1, \ldots, da_n$. It is even finitely presented when A is.

10.1.3. Example. Let $A = B[x_1, \ldots, x_n]$, then $\Omega_{A/B} = \bigoplus_{i=1}^n Adx_i$, with $df(x_1, \ldots, x_n) = \sum_{i=1}^n \frac{\partial f}{\partial x_i} dx_i$.

10.1.4. Example. Let $A = B[x, y]/(f(x, y))$. Then

$$\Omega_{A/B} = \frac{Adx \oplus Ady}{(\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy)}.$$

Say $A = k[x, y]/(xy)$, then $\Omega_{A/k} = (Adx \oplus Ady)/(ydx + xdy)$. Its rank at all points $(x, y) \neq (0, 0)$ is 1, but the rank jumps to 2 at $(0, 0)$. This already indicates that $\Omega_{A/B}$ captures smoothness information.

10.1.5. Lemma. *Let $T \subset B$, $S \subset A$ be multiplicatively closed sets such that $i(T) \subset S$, then*

$$\Omega_{S^{-1}A/T^{-1}B} = S^{-1}\Omega_{A/B}.$$

10.1.6. Lemma. *Let $C \to B \to A$ be maps of rings. Then*

$$A \otimes \Omega_{B/C} \to \Omega_{A/C} \to \Omega_{A/B} \to 0$$

is exact, where the first map is given by $a \otimes db \mapsto ad(i(b))$ and the second map is $da \mapsto da$.

Remark. In manifolds: let $M \xrightarrow{\pi} N \to \{*\}$ be smooth, then $0 \to T_{M/N} \to T_M \to \pi^* T_N \to 0$ is exact. Dualize to get a similar expression as in lemma 10.1.6.

Remark. If the maps of $\operatorname{Spec} A \to \operatorname{Spec} B \to \operatorname{Spec} C$ are smooth, then the sequence in lemma 10.1.6 is short exact (the leftmost map is injective).

10.1.7. Lemma. *Let $C \to B \to A$ be maps of rings, where $A = B/I$. Then we can continue the exact sequence to the left:*

$$I/I^2 \xrightarrow{\delta} A \otimes \Omega_{B/C} \to \Omega_{A/C} \to 0$$

where I/I^2 is a $B/I = A$-module, and $\delta : i \mapsto 1 \otimes di$; note that it is well-defined because $\delta(ii') = i \otimes di' + i' \otimes di \in I \otimes \Omega_{B/C}$, hence is zero.

Remark. In the differential-geometric picture: $M \to N$ is an embedded submanifold, and we have an exact sequence

$$0 \to T_M \to T_N|_M \to \text{normal bundle} \to 0.$$

So I/I^2 is called the *conormal sheaf* of $\operatorname{Spec} A \hookrightarrow \operatorname{Spec} B$.

In general, there is a way to extend the right exact sequence into a long exact sequence, analogous to sheaf cohomology. The difficulty is that we're starting with a sequence of rings, which is not an abelian category. This is called André–Quillen homology.

10.2. The cotangent sheaf. Let $\pi : X \to Y$ be a morphism of schemes. Define the cotangent sheaf $\Omega_{X/Y}$, a sheaf of $\mathcal{O}_X$-modules, by gluing together on affine opens. The tangent sheaf $T_{X/Y} = \Omega_{X/Y}^\vee$.

There is another way to define this. In the affine case, let $B \to A$ be a ring map. Consider

$$I = \ker(A \otimes_B A \xrightarrow{a \otimes a' \mapsto aa'} A),$$

which is generated by tensors of the form $a \otimes 1 - 1 \otimes a$. Then one can show that I/I^2, which is an $A = A \otimes_B A/I$-module, is just $\Omega_{A/B}$, with $d : A \to I/I^2$ sending $a \mapsto (a \otimes 1 - 1 \otimes a) \pmod{I^2}$. We can use this to directly define $\Omega_{X/Y}$, as the sheaf $\mathcal{I}/\mathcal{I}^2$ where $\mathcal{I}$ is the ideal sheaf of $\Delta : X \to X \times_Y X$.

The analogous versions of lemmata 10.1.6 and 10.1.7 are then:

10.2.1. Lemma. *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$ be maps of schemes, then we have an exact sequence*

$$f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0.$$

10.2.2. Lemma. *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$ be maps of schemes, where f is a closed immersion. then we have an exact sequence*

$$\mathcal{I}/\mathcal{I}^2 \to f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to 0,$$

where $\mathcal{I}$ is the ideal sheaf of f, and $\mathcal{I}/\mathcal{I}^2$ is the conormal sheaf.

The following proposition justifies the importance of Ω.

10.2.3. Proposition. *Suppose X is a scheme over k, and $p \in X(k)$. Then*

$$i_p^*\Omega_{X/k} = T_p^\vee = \mathfrak{m}/\mathfrak{m}^2$$

is the Zariski cotangent space at p.

Proof. When $X = \operatorname{Spec} A$, a k-point is a maximal ideal $\mathfrak{m} \subset A$ with $A/\mathfrak{m} = k$. So it suffices to show $\Omega_{A/k} \otimes_A k \cong \mathfrak{m}/\mathfrak{m}^2$. Taking the dual, we have to show

$$\operatorname{Hom}(\mathfrak{m}/\mathfrak{m}^2, k) \cong \operatorname{Hom}(\Omega_{A/k} \otimes_A k, k).$$

The RHS is $\operatorname{Hom}(\Omega_{A/k}, k)$ by tensor-hom adjunction, and by the universal property this is just k-derivations $d : A \to k$. This necessarily kills k and $\mathfrak{m}^2$, so induces a map $\mathfrak{m}/\mathfrak{m}^2 \to k$. Conversely, any map $\mathfrak{m}/\mathfrak{m}^2 \to k$ extends to a k-derivation $d : A \to k$. □

10.2.4. Example. Let $X = \mathbb{P}_k^1$, and consider $\Omega_{\mathbb{P}^1/k}$, which is a line bundle. In fact, by taking an affine chart $\mathbb{A}^1 = \operatorname{Spec} k[x]$ and a rational section dx of the line bundle, because

$$dx = d(1/x^{-1}) = \frac{1}{(x^{-1})^2} d(x^{-1}),$$

we conclude that $\Omega_{\mathbb{P}^1/k} \cong \mathcal{O}(-2) \cong \omega_{\mathbb{P}^1}$. In fact, this is true for all smooth projective curves.

10.2.5. Example. In the case $X = \mathbb{P}^n_k$, we have a map

$$\mathcal{O}_X \xrightarrow{x_0,\ldots,x_n} \mathcal{O}(1)^{\oplus(n+1)}$$

and dualizing it we get the *Euler sequence*

$$(*) \qquad 0 \to \Omega_{\mathbb{P}^n/k} \to \mathcal{O}(-1)^{\oplus(n+1)} \xrightarrow{x_0,\ldots,x_n} \mathcal{O}_X \to 0.$$

(Intuition: $\mathbb{C}^\times \to \mathbb{C}^{n+1}\backslash 0 \xrightarrow{\pi} \mathbb{P}^n$, which gives $0 \to \langle \sum x_i \frac{\partial}{\partial x_i}\rangle \to \bigoplus \mathbb{C}\frac{\partial}{\partial x_i} \to \pi^* T_{\mathbb{P}^n} \to 0$.)

Proof. Write $(*)$ as a map of graded modules: let $S = k[x_0,\ldots,x_n]$, then $S(-1)$ shifts the indexing toward the left by 1. Then let M be the kernel

$$(**) \qquad 0 \to M \to S(-1)^{\oplus(n+1)} \to S \to 0$$

where the latter map is given by $e_i \mapsto x_i$ (e_i is the generator of each copy of $S(-1)$, which has degree 1). To calculate $\widetilde{M}$ on each $D(x_i)$, we localize $(**)$ at x_i and take the degree 0 component. It is a free k-vector space spanned by $\frac{1}{x_i}(e_j - \frac{x_j}{x_i}e_i)$, and we take each of these to $d(x_{j/i})$, which are free generators of the sections of $\Omega_{\mathbb{P}^n/k}$ over $D(x_i)$. It suffices then to check that these isomorphisms glue together to show that $\Omega_{\mathbb{P}^n/k} \cong \widetilde{M}$. □

The *canonical bundle* $K_{\mathbb{P}^n/k} := \bigwedge^n \Omega_{\mathbb{P}^n/k}$ can then be calculated as $\mathcal{O}(-n-1)$, which is just the sheaf $\omega_{\mathbb{P}^n/k}$ appearing in Serre duality. This will be true for all smooth projective varieties.

10.3. Smoothness. Recall the definition of smoothness over a field: $X \to \operatorname{Spec} k$ is smooth of dimension d if it can be covered with affine charts $\operatorname{Spec} k[x_1,\ldots,x_n]/(f_1,\ldots,f_r)$ where the Jacobian matrix has corank d at all points. We now make an equivalent, cleaner definition:

10.3.1. Definition. Let X be a k-scheme, then X is *smooth of dimension* d if X is locally of finite type, of pure dimension d, and $\Omega_{X/k}$ is locally free of rank d.

10.3.2. Theorem (conormal exact sequence for smooth varieties)**.** *Let $i : X \hookrightarrow Y$ be smooth k-varieties of dimension d, e. Then*

$$0 \to \mathcal{I}/\mathcal{I}^2 \to i^*\Omega_Y \to \Omega_X \to 0$$

is exact, and $\mathcal{I}/\mathcal{I}^2$ is locally free of rank $e - d$. (Recall this is not usually left exact.) Conversely, if Y is smooth, $\mathcal{I}/\mathcal{I}^2$ is locally free, and the above sequence is exact, then X is smooth.

The normal sheaf is $N_{X/Y} = (\mathcal{I}/\mathcal{I}^2)^\vee$. When $X \hookrightarrow Y$ is a (Weil) divisor, the conormal sheaf $\mathcal{I}/\mathcal{I}^2$ is denoted by $\mathcal{O}_X(-X)$, by which we really mean $\mathcal{O}_Y(-X)|_X$.

10.3.3. Proposition (adjunction formula)**.** *Let $i : X \hookrightarrow Y$ be a divisor, then*

$$\omega_X = i^*(\omega_Y \otimes \mathcal{O}_Y(X)).$$

Proof. By the conormal exact sequence, we see that

$$i^*K_Y = i^*(\bigwedge^{\dim Y} \Omega_Y) = \bigwedge^{1}(\mathcal{I}/\mathcal{I}^2) \otimes \bigwedge^{\dim Y - 1} \Omega_X = i^*\mathcal{O}_Y(-X) \otimes K_X,$$

and we know $K_X = \omega_X$ for smooth projective varieties. □

10.4. Invariants. We can use $\Omega_{X/k}$ and $\bigwedge^q \Omega_{X/k} = \Omega^q_{X/k}$ to define invariants, such as the *Hodge numbers*

$$h^p(X, \Omega^q_{X/k}).$$

What's interesting is that for $p = 0$ we get *birational invariants*:

10.4.1. Theorem. *Let X, Y be smooth projective varieties that are birationally isomorphic. Then $h^0(X, \Omega^q_{X/k}) = h^0(Y, \Omega^q_{Y/k})$.*

This works not just for $\bigwedge^q$, but for any covariant tensor operation.

10.4.2. Definition (plurigenera)**.** The rth plurigenus of a smooth projective k-variety X is $h^0(X, K_X^{\otimes r})$.

10.4.3. Definition (Kodaira dimension)**.** By asymptotic Riemann-Roch, $h^0(X, K_X^{\otimes r})$ is eventually polynomial in r. The Kodaira dimension $\kappa(X)$ is the degree of this polynomial (defined to be -1 if the polynomial is identically zero).

10.5. Riemann-Hurwitz theorem.

10.5.1. Theorem. *Let $\pi : X \to Y$ be a finite separable morphism of regular projective curves, of pure degree n. Then*

$$2g(X) - 2 = n(2g(Y) - 2) + \deg R,$$

where R is the ramification divisor.

As an application, we may count the number of tangent lines from a point $p \in \mathbb{P}^2$ to a degree d plane curve $C \subset \mathbb{P}^2$. (The answer is $d^2 - d$.)

11. Flatness

The idea is to capture "nice families of schemes".

11.1. Algebra.

11.1.1. Definition. Let X be a scheme, $\mathcal{F} \in \mathrm{QCoh}(X)$, then $\mathcal{F}$ is *flat* if $\mathcal{F}_x$ is flat over $\mathcal{O}_{X,x}$ (or equivalently, affine locally instead of stalkwise).

Let $f : X \to Y$ be a morphism, then it is *flat* if for $x \in X$, $y = f(x) \in Y$, $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is flat.

11.1.2. Example. Closed embeddings in general will not be flat. For example, $\operatorname{Spec} k \xrightarrow{0} \mathbb{A}^1$ is not flat, because k is not a flat $k[x]$ module: take $k[x] \xrightarrow{[x]} k[x]$.

11.1.3. Lemma. *Let $0 \to N_1 \to N_2 \to N_3 \to 0$ be a short exact sequence of A-modules, where N_3 is flat. Then for any A-module M,*

$$0 \to N_1 \otimes M \to N_2 \otimes M \to N_3 \otimes M \to 0$$

is exact.

Proof. $\mathrm{Tor}_1(N_3, M) = 0$. □

Geometrically: suppose $0 \to \mathcal{E}_1 \to \mathcal{E}_2 \to \mathcal{E}_3 \to 0$ are QCoh on Y, where $\mathcal{E}_3$ is flat. Then for any morphism $f : X \to Y$, pulling back to $0 \to f^*\mathcal{E}_1 \to f^*\mathcal{E}_2 \to f^*\mathcal{E}_3 \to 0$ is also exact.

11.1.4. Lemma. *Suppose $0 \to M_1 \to M_2 \to M_3 \to 0$, then:*

- *If M_2, M_3 are flat, so is M_1;*
- *If M_1, M_3 are flat, so is M_2.*

11.1.5. Lemma. *Suppose $0 \to M_1 \to \cdots \to M_n \to 0$ is an exact complex. If $M_2, \ldots, M_n$ are flat, then so is M_1.*

11.1.6. Lemma. *Suppose $0 \to M_1 \to \cdots \to M_n \to 0$ is an exact complex, where all M_i are flat. The for any N, $0 \to M_1 \otimes N \to \cdots \to M_n \otimes N \to 0$ is exact.*

11.1.7. Proposition. *Let $(A, \mathfrak{m}, k)$ be a local Noetherian ring. Then any finitely generated, flat A-module is free.*

Proof. By Nakayama, we can pick lifts of generators of $M \otimes_A k$ to get

$$0 \to K \to A^{\oplus r} \to M \to 0.$$

Since M is flat, tensoring with k gives an exact sequence

$$0 \to K \otimes_A k \to k^{\oplus r} \to M \otimes k \to 0,$$

but $k^{\oplus r} \cong M \otimes k$, so $K \otimes_A k = 0$, so $K = 0$ by Nakayama. □

11.1.8. Theorem. *Suppose for any finitely generated ideal $I \subset A$, $\mathrm{Tor}_1(M, A/I) = 0$. Then M is flat.*

11.1.9. Corollary. *Let A be a PID. Then M is flat iff M is torsion-free.*

11.1.10. Corollary. *Let $\pi : X \to C$ be dominant, where X is integral and C is a regular curve. Then π is flat.*

Proof. It suffices to check that $\mathcal{O}_{X,x}$ are torsion free. But since π is dominant, this is automatically true. □

11.1.11. Example. The resolution of a node is not flat.

11.2. Geometry.

Assume all schemes are locally Noetherian or something.

11.2.1. Theorem. *Let $f : X \to Y$ be a flat morphism. Given $x \in X$, $y = f(x) \in Y$, then*

$$\dim_x(X_y) = \dim_x X - \dim_y Y.$$

Here $\dim_x$ means local dimension, i.e. dimension of the local ring at x.

PROOF. Use induction on $\dim_y Y$. We may replace Y by $\operatorname{Spec} \mathcal{O}_{Y,y}$ and X by $X \times_Y \operatorname{Spec} \mathcal{O}_{Y,y}$. The base case $\dim Y = 0$ is easy, since then $X_y = X$ (as topological spaces) and $\dim X_y = \dim X - 0$. In general, suppose $\dim Y = n$. Pick $t \in \mathfrak{m}_Y \subset \mathcal{O}_{Y,y}$ a non-zero-divisor. By flatness (which is just torsion-free over local ring), the image of t under $f^\# : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is also a non-zero-divisor. By Krull's principal ideal theorem, every irreducible component of $V(t) \hookrightarrow Y$ has codimension 1, and so is every irreducible component of $V(f^\#(t)) \hookrightarrow X$. We are then done by inductive hypothesis. □

11.2.2. Theorem. *Let $X \to Y$ be projective, $\mathcal{F} \in \operatorname{Con}(X)$ flat over Y. Then the map*

$$y \mapsto \chi(\mathcal{F}|_{X_y})$$

is locally constant.

Remark: conversely, let $X \hookrightarrow \mathbb{P}^n \times Y \to Y$, $\mathcal{F} \in \operatorname{Con}(X)$, and Y is reduced. If the Hilbert polynomials $p_{\mathcal{F}|_{X_y}}(t)$ are independent of the choice of $y \in Y$, then $\mathcal{F}$ is flat over Y.

PROOF. Reduce to $Y = \operatorname{Spec} A$. It is enough to show that $\chi(\mathcal{F}(m)|_{X_y})$ is independent of Y for m sufficiently large. By Serre vanishing, pick m large enough so that $H^k(X, \mathcal{F}(m)) = 0$ for $k \geq 1$. Then the augmented Čech complex associated to $\mathcal{F}(m)$

$$0 \to H^0(X, \mathcal{F}(m)) \to C^0(X, \mathcal{F}(m)) \to \cdots \to C^n(X, \mathcal{F}(m)) \to 0$$

is a long exact sequence, and since $\mathcal{F}$ is flat over Y, all but the first term are flat over A. Then so is $H^0(X, \mathcal{F}(m))$. Since it is flat and finitely presented, it is projective (locally free).

Now, to restrict it to X_y, it is enough to tensor this Čech complex with $\kappa(y)$, which by flatness gives another exact complex. We then conclude that $H^k(X_y, \mathcal{F}(m)|_{X_y}) = 0$ for $k \geq 1$, and is equal to $H^0(X, \mathcal{F}(m)) \otimes_A \kappa(y)$ for $k = 0$. This number is dependent of y since $H^0(X, \mathcal{F}(m))$ is locally free. □

11.2.3. Corollary. *Let $X \hookrightarrow \mathbb{P}^n \times Y \to Y$ be flat, and Y is connected. Then the Hilbert polynomials $p_{X_y}(t)$ are independent of the choice of $y \in Y$.*

11.2.4. Corollary. *Let $C \times Y \to Y$ be a flat morphism, where C is a projective curve and Y is connected. Let $\mathcal{L}$ be a line bundle on $C \times Y$. Then $\deg \mathcal{L}|_{C \times \{y\}}$ is independent of $y \in Y$.*

Suppose we have a family of schemes, parametrized by one parameter $t \neq 0$. We would like to define a limit at $t = 0$. In other words, if we have a scheme lying over, say, $\mathbb{A}^1 - \{0\}$, we would like to uniquely extend it to be over $\mathbb{A}^1$.

11.2.5. Theorem (uniqueness of flat limits)**.** *Let A be a DVR, $K = \operatorname{Frac} A$. Let η be the generic point of $\operatorname{Spec} A$. Let X be a Noetherian scheme over $\operatorname{Spec} A$. Given a closed subscheme $Z_\eta \hookrightarrow X_\eta$ of the generic fiber, consider its scheme-theoretic closure $Z = \overline{Z_\eta} \hookrightarrow X$. Then this is the unique closed subscheme $Z \hookrightarrow X$ that is flat over $\operatorname{Spec} A$, and restricts to Z_η on X_η.*

CHAPTER 8

Riemannian Geometry

1. Curvature

1.1. Riemannian metrics. Let M be a smooth manifold. We will use Einstein summation notation throughout: unless otherwise specified, an index repeated once in superscript and once in subscript is assumed to be summed over.

1.1.1. Definition. A *Riemannian metric* g on M is a smooth $(0,2)$-tensor field that is a positive-definite symmetric bilinear form $T_pM \times T_pM \to \mathbb{R}$ for each $p \in M$.

1.1.2. Definition. A smooth manifold M equipped with a Riemannian metric g is called a *Riemannian manifold.*

In a coordinate chart $x = (x^1, \dots, x^n) : U \to \mathbb{R}^n$, where $U \subset M$, g takes the form

$$g = g_{ij} dx^i dx^j$$

where $g_{ij} = g(\frac{\partial}{\partial x^i}, \frac{\partial}{\partial x^j})$. Given another coordinate chart $\widetilde{x}$, the tensor transforms like

$$\widetilde{g}_{ij} = \frac{\partial x^k}{\partial \widetilde{x}^i} \frac{\partial x^\ell}{\partial \widetilde{x}^j} g_{k\ell}.$$

Given an immersion $f : M \to N$, if g is a Riemannian metric on N, f^*g is naturally a metric on M. In particular, submanifolds of $\mathbb{R}^n$ naturally inherit its metric.

1.1.3. Proposition. *Any smooth manifold admits a Riemannian metric.*

PROOF. Pick a partition of unity (possible since smooth manifolds are assumed to be paracompact) to glue together local Euclidean metrics. □

1.1.4. Definition. In any local coordinate $x^1, \dots, x^n$, consider the inverse matrix $(g^{ij}) := (g_{ij})^{-1}$, and define the *inverse metric* g^{-1} as a $(2,0)$-tensor as $g^{-1}(dx^i, dx^j) = g^{ij}$.

PROOF. To see g^{-1} is coordinate-independent, let $\widetilde{x}$ be another system of coordinates. Let $A_i^j = \frac{\partial \widetilde{x}^j}{\partial x^i}$ and $(A^{-1})_k^\ell = \frac{\partial x^\ell}{\partial \widetilde{x}^k}$. By the transformation rule of $(0,2)$-tensors, $(\widetilde{g}_{ij}) = A^{-1}(g_{k\ell})(A^{-1})^t$. So under this basis, $\widetilde{g}^{-1}(d\widetilde{x}^i, d\widetilde{x}^j) = \widetilde{g}^{ij} = ((\widetilde{g}_{k\ell})^{-1})^{ij} = (A^t(g_{k\ell})^{-1}A)^{i,j}$.

Note also that $d\widetilde{x}^i = \sum_j \frac{\partial \widetilde{x}^i}{\partial x^j} dx^j$, so $g^{-1}(d\widetilde{x}^i, d\widetilde{x}^j) = \sum_{k,\ell} \frac{\partial \widetilde{x}^i}{\partial x^k} \frac{\partial \widetilde{x}^j}{\partial x^\ell} g^{-1}(dx^k, dx^\ell)$. But this is exactly the same as $(A^t(g_{k\ell})^{-1}A)^{i,j}$. So we have shown that $g^{-1} = \widetilde{g}^{-1}$ is indeed coordinate-independent. □

1.1.5. Definition. Given a metric, we can define:

- For $v \in T_pM$, define $|v| = \sqrt{g_p(v,v)}$.
- For $v, w \in T_pM$, define their angle θ by $g_p(v,w) = |v||w|\cos\theta$.
- For $\alpha \in T_p^*M$, define $|\alpha| = \sqrt{g_p(\alpha,\alpha)}$ (here we used the inverse metric, which is commonly and abusively also written as g).
- In general, g defines a positive definite symmetric bilinear form on $T_pM^{\otimes r} \otimes T_p^*M^{\otimes s}$ for any (r,s).
- For a smooth curve $\gamma : [a,b] \to M$, define its length
$$L(\gamma) = \int_a^b |\gamma'(t)| dt.$$
- For an open set $U \subset M$ with coordinates $x : U \to \mathbb{R}^n$, define its volume
$$\mathrm{Vol}(U) = \int_{x(U)} \sqrt{\det(g_{ij})} dx_1 \dots dx_n.$$

Given a metric g, we can have a natural correspondence between vector fields (upper indices) and 1-forms (lower indices), as follows.

1.1.6. Definition. Define a map $\flat : \Gamma \to \Gamma^*$, sending $V \mapsto g(V, -)$. Similarly, we have $\sharp : \Gamma^* \to \Gamma$, sending $\alpha \mapsto g^{-1}(\alpha, -)$.

In coordinates, this is given by

$$V_i := (V^\flat)_i = V^k g_{ki},$$

$$\alpha^i := (\alpha^\sharp)^i = \alpha_k g^{ki}.$$

Similarly, we can raise/lower indices for arbitrary tensors.

1.1.7. Example. Let $f \in C^\infty(M)$. Its *gradient* $\nabla f := (df)^\sharp$. In local coordinates, this is $\nabla f = g^{ij} \frac{\partial f}{\partial x^i} \partial_j$.

1.2. Affine connections.

1.2.1. Definition. An *affine connection* on a smooth manifold M is a map $\nabla : \Gamma(M) \times \Gamma(M) \to \Gamma(M)$, $(X, Y) \mapsto \nabla_X Y$, satisfying:

- $C^\infty(M)$-linearity in X;
- $\mathbb{R}$-linearity in Y;
- Leibniz rule in Y, i.e. $\nabla_X(fY) = X(f)Y + f\nabla_X Y$ for $f \in C^\infty(M)$.

For example, the directional derivative in $\mathbb{R}^n$ is an affine connection.

Warning: affine connections are generally *not* $(1, 2)$-tensors!

The data of an affine connection, in local coordinates, is encoded in the Christoffel symbols Γ^k_{ij}, which are smooth functions on the coordinate patch.

1.2.2. Definition. Let $x = (x^1, \dots, x^n)$ be a local coordinate, then define the *Christoffel symbols* Γ^k_{ij} so that

$$\nabla_{\partial_i}(\partial_j) = \Gamma^k_{ij}\partial_k.$$

For $X = X^i\partial_i$, $Y = Y^j\partial_j$, we then have

$$\nabla_X Y = X^i(\partial_i Y^j)\partial_j + X^i Y^j \Gamma^k_{ij}\partial_k.$$

One can interpret the first term as the “naive guess” of the directional derivative, and the second term as a compensation term to account for the manifold’s own geometry.

Note that the value of $\nabla_X Y$ at a point p only depends on $X(p)$, but depends on Y on a neighborhood of p.

We may extend $\nabla_X(-)$ to act on any tensor (not just vector fields), by the principle

$$\nabla_X(T \otimes S) = (\nabla_X T) \otimes S + T \otimes (\nabla_X S).$$

For example,

- $\nabla_X(f) = X(f) = df(X)$ for functions;
- $\nabla_X(\alpha)(Y) = X(\alpha(Y)) - \alpha(\nabla_X Y)$ for 1-forms.

The general formula is, for an (r, s)-tensor T, ∇T is an $(r, s+1)$-tensor:

$$\begin{aligned}(\nabla T)(\alpha_1, \dots, \alpha_r, V_0, V_1, \dots, V_s) &:= (\nabla_{V_0} T)(\alpha_1, \dots, \alpha_r, V_1, \dots, V_s) \\ &= V_0(T(\alpha_1, \dots, \alpha_r, V_1, \dots, V_s)) - \sum_{p=1}^{r} T(\dots, \nabla_{V_0}(\alpha_p), \dots) \\ &\quad - \sum_{q=1}^{s} T(\dots, \nabla_{V_0}(V_q), \dots).\end{aligned}$$

1.3. Parallel transport. Let $\gamma : [a,b] \to M$ be a smoothly immersed curve. Let $\Gamma = \Gamma(\gamma^* TM)$ denote the space of vector fields along γ, i.e. smooth functions $V : [a,b] \to TM$ such that $V(t) \in T_{\gamma(t)}M$.

Define $D : \Gamma \to \Gamma$ in local coordinates x by

$$(DV)(t) = (\partial_t V^i(t) + (\partial_t \gamma^j(t)) V^k(t) \Gamma^i_{jk}) \partial_i|_{\gamma(t)}$$

where $V(t) = V^i(t)\partial_i|_{\gamma(t)}$, and $\gamma^i(t) = x^i(\gamma(t))$. We call this the *covariant derivative of V along γ*.

This satisfies the following:

(1) For any vector field W on M such that $W(\gamma(t)) = V(t)$, we have

$$(DV)(t) = (\nabla_{\gamma'(t)} W)(\gamma(t)).$$

To see this, expand the RHS in local coordinates:

$$\begin{aligned}(\nabla_{\gamma'(t)} W)(\gamma(t)) &= \partial_t \gamma^i(t) \cdot \nabla_{\partial_i}(W^j \partial_j)(\gamma(t)) \\ &= \partial_t \gamma^i(t) \cdot (W^j \Gamma^k_{ij} \partial_k + \partial_i W^j \partial_j)(\gamma(t)) \\ &= \partial_t \gamma^i(t) W^j(\gamma(t)) \Gamma^k_{ij}(\gamma(t)) \partial_k + \partial_t (W^j \circ \gamma)(t) \partial_j \\ &= \partial_t \gamma^i(t) V^j(t) \Gamma^k_{ij}(\gamma(t)) \partial_k + \partial_t V^j(t) \partial_j\end{aligned}$$

which, after re-indexing, is the same as what we defined.

(2) For smooth function f on $[a,b]$, $D(f \cdot V)(t) = f'(t)V(t) + f(t)(DV)(t)$.

1.3.1. Definition. A vector field V along γ is *parallel* if $DV = 0$. Equivalently, a vector field W on M is *parallel* if $\nabla_{\gamma'} W = 0$.

Note from the coordinate expression that being parallel is a system of n linear ordinary differential equations for n functions (at least locally, where coordinate charts exist), so it is uniquely solved along the curve. In particular, specifying $V(a)$ gives us a unique $V(b)$ which deserves to be called the *parallel transport* of $V(a)$ along γ.

1.4. The Levi–Civita connection. An affine connection ∇ on a smooth manifold, equipped with a metric tensor g (a nondegenerate symmetric smooth $(0,2)$-tensor field) is called

- *symmetric* if $\nabla_X Y - \nabla_Y X = [X,Y]$. (In local coordinates, this means $\Gamma^k_{ij} = \Gamma^k_{ji}$.)
- *metric-compatible* if $X(g(Y,Z)) = g(\nabla_X Y, Z) + g(Y, \nabla_X Z)$. (This means that the derivative "misses" g.)

1.4.1. Theorem. *There exists an unique affine connection on a Riemannian manifold (M,g) satisfying the two conditions above. This is called the* Levi–Civita connection.

Proof. Using metric compatibility, we get

$$X(g(Y,Z)) = g(\nabla_X Y, Z) + g(Y, \nabla_X Z),$$

$$Y(g(X,Z)) = g(\nabla_Y X, Z) + g(X, \nabla_Y Z),$$

$$Z(g(X,Y)) = g(\nabla_Z X, Y) + g(X, \nabla_Z Y).$$

Adding 1 and 2 and subtracting 3, and using symmetry:

$$X(g(Y,Z)) + Y(g(X,Z)) - Z(g(X,Y)) = 2g(\nabla_X Y, Z) - g([X,Y],Z) + g([X,Z],Y) + g([Y,Z],X).$$

This is called the *Koszul formula.* Note that since g is non-degenerate, this uniquely determines $\nabla_X Y$, hence uniquely determines the connection. □

In local coordinates, the Christoffel symbols can be shown to be

$$\Gamma^k_{ij} = \frac{1}{2} g^{kp}(\partial_i g_{jp} + \partial_j g_{ip} - \partial_p g_{ij}).$$

This shows that the Levi–Civita connection is intrinsic to (M,g).

Recall that any affine connection can be extended to act on arbitrary tensors.

1.4.2. Definition. We say a tensor T on M is *parallel* if $\nabla T = 0$.

1.4.3. Example. Consider the $(0,2)$-tensor g, then

$$(\nabla_{V_0} g)(V_1, V_2) = V_0(g(V_1, V_2)) - g(\nabla_{V_0}(V_1), V_2) - g(V_1, \nabla_{V_0}(V_2)),$$

so $\nabla g = 0$ means precisely metric compatibility.

1.4.4. Example. For $V = V^i \partial_i$, $\alpha = \alpha_i dx^i$, and $T = T_i^j dx^i \otimes \partial_j$, the component functions of ∇V, $\nabla \alpha$, ∇T are

$$\begin{aligned} \nabla_i V^j &= \partial_i V^j + V^k \Gamma_{ik}^j \\ \nabla_i \alpha_j &= \partial_i \alpha_j - \alpha_k \Gamma_{ij}^k \\ \nabla_i T_j^k &= \partial_i T_j^k + T_j^p \Gamma_{ip}^k - T_q^k \Gamma_{ij}^q. \end{aligned}$$

The general rule can be derived similarly. Note that ∇_i is *not* the same as ∂_i.

1.5. The Riemann curvature tensor. Let (M, g) be a Riemannian manifold, and let ∇ be the Levi–Civita connection.

1.5.1. Definition. The *Riemann curvature tensor* is a $(1,3)$-tensor $R : \Gamma \times \Gamma \times \Gamma \to \Gamma$, defined as

$$R(X,Y)Z = \nabla_Y(\nabla_X Z) - \nabla_X(\nabla_Y Z) + \nabla_{[X,Y]} Z.$$

Commonly, this is also viewed as a $(0,4)$-tensor via definition 1.1.6, i.e.

$$R(X,Y,Z,W) = g(R(X,Y)Z, W).$$

1.5.2. Exercise. Check that R is actually a tensor, i.e. $C^\infty(M)$-linear in X, Y, and Z.

1.5.3. Example. On Euclidean space with the usual inner product, ∇ is just the covariant derivative, and it is clear that R vanishes. So Euclidean space is "flat" in the sense that there is no curvature.

In local coordinates, we can write $R(\partial_i, \partial_j)\partial_k = R_{ijk}{}^\ell \partial_\ell$, or as a $(0,4)$-tensor $R(\partial_i, \partial_j, \partial_k, \partial_\ell) = R_{ijk\ell} = R_{ijk}{}^p g_{p\ell}$. So it seems like we need n^4 parameters to specify the curvature tensor on an n-manifold, but proposition 1.5.5 below shows that there is a lot of redundancy, and in fact R has only $D(n) = \frac{1}{12} n^2(n^2 - 1)$ algebraically independent components. When $n = 2$, $D(n) = 1$, and this is precisely the Gauss curvature for a surface, which also coincides with the scalar curvature (**??**). When $n = 3$, $D(n) = 6$, and this is specified by the $\frac{n(n+1)}{2} = 6$ components of the Ricci curvature (definition 1.6.5).

1.5.4. Exercise. Verify that $R_{ijk}{}^\ell$ can be expressed only in terms of the metric components g, i.e. it is intrinsic to the Riemannian manifold.

1.5.5. Proposition. *We have the following identities:*

(1) $R(X,Y,Z,W) = -R(Y,X,Z,W)$*;*
(2) $R(X,Y,Z,W) = R(Z,W,X,Y)$*;*
(3) $R(X,Y,Z,W) = -R(X,Y,W,Z)$*;*
(4) (First Bianchi identity) $R(X,Y)Z + R(Y,Z)X + R(Z,X)Y = 0$*;*
(5) (Second Bianchi identity) $(\nabla_X R)(Y,Z)W + (\nabla_Y R)(Z,X)W + (\nabla_Z R)(X,Y)W = 0$.

1.5.6. Proposition. *The second Bianchi identity can be also written as*

$$(\nabla_X R)(Y,Z,W,V) + (\nabla_Y R)(Z,X,W,V) + (\nabla_Z R)(X,Y,W,V).$$

In coordinates: $\nabla_i R_{jk\ell m} + \nabla_j R_{ki\ell m} + \nabla_k R_{ij\ell m} = 0$*, where* $\nabla_i R_{jk\ell m} = (\nabla_{\partial_i} R)(\partial_j, \partial_k, \partial_\ell, \partial_m)$ *and so on.*

This just follows from the metric-compatibility of ∇.

1.6. Sectional, Ricci, and scalar curvature. Let (M, g) be a Riemannian manifold, and R its Riemann curvature tensor.

1.6.1. Definition. Let $p \in M$, and $\sigma \subset T_pM$ a two-dimensional subspace. The *sectional curvature* is defined as

$$K(p, \sigma) = \frac{R(v,w,v,w)}{g(v,v)g(w,w) - g(v,w)^2}$$

for any basis $\{v, w\}$ of σ. This does not depend on the specific basis chosen.

For example, when M is a surface, $\sigma = T_pM$ is the only choice, and it turns out that $K(p) = K(p, \sigma)$ is precisely the Gauss curvature.

1.6.2. Exercise. If (M, g) has constant sectional curvature k (for all p, for all $\sigma \subset T_pM$), then

$$R(X, Y, Z, W) = k(g(X, Z)g(Y, W) - g(X, W)g(Y, Z)).$$

1.6.3. Example. The sphere $S^n \subset \mathbb{R}^{n+1}$ with radius r with the Euclidean metric has constant sectional curvature $k = 1/r^2$. The hyperbolic upper-half plane $H = \{(x, y) \in \mathbb{R}^2 : y > 0\}$ with metric $\frac{1}{y^2}(dx \otimes dx + dy \otimes dy)$ has constant sectional curvature $k = -1$.

1.6.4. Lemma. *Let V be an n-dimensional vector space, and g a symmetric bilinear form on V.*

- *Let $T : V \to V$ be a linear map, then $\operatorname{Tr} T = \sum_{i=1}^n g(Te_i, e_i) = g^{ij} g(T\partial_i, \partial_j)$, where e_i is any orthonormal basis.*
- *Let $T : V \times V \to \mathbb{R}$ be a bilinear form, treated as a linear map $V \to V$ by raising index. Then its trace $\operatorname{Tr} T = \sum_{i=1}^n T(e_i, e_i) = g^{ij} T(\partial_i, \partial_j)$.*

1.6.5. Definition. For $X, Y \in T_pM$, the *Ricci curvature*

$$\operatorname{Ric}(X, Y) = \operatorname{Tr}(Z \mapsto R(X, Z)Y) = \sum_{i=1}^n R(X, e_i, Y, e_i)$$

where $e_1, \dots, e_n$ is any orthonormal basis for T_pM.

Note that due to symmetry of R, this is the only nonzero trace of R, and $\operatorname{Ric}(X, Y) = \operatorname{Ric}(Y, X)$. In local coordinates $\operatorname{Ric}_{ik} = \operatorname{Ric}(\partial_i, \partial_k) = R_{ipk}{}^p = g^{j\ell} R_{ijk\ell}$. Note also that

$$\operatorname{Ric}(e_i, e_i) = \sum_{j \neq i} R(e_i, e_j, e_i, e_j)$$

is $(n-1)$ times the average sectional curvature of all 2-planes containing e_i.

1.7. Cartan formalism.

Let (M, g) be a Riemannian manifold, $p \in M$, and $E_1, \dots, E_n$ an orthonormal frame of vector fields defined on some neighborhood U of p. Let ω^i be the dual frame of 1-forms.

1.7.1. Definition. The *connection 1-forms* ω_i^j are defined by $\nabla_X E_i = \omega_i^j(X) E_j$. The *curvature 2-forms* Ω_i^j are defined by $R(X, Y)E_i = \Omega_i^j(X, Y)E_j$.

1.7.2. Proposition. *These differential forms satisfy the following:*

(1) They are $\mathfrak{so}_n$-valued, i.e. $\omega_i^j = -\omega_j^i$ and $\Omega_i^j = -\Omega_j^i$.
(2) $d\omega^i = \omega^j \wedge \omega_j^i$.
(3) $d\omega_i^j = \Omega_i^j - \omega_i^k \wedge \omega_k^j$.
(4) $\omega^j \wedge \Omega_j^i = 0$.
(5) $d\Omega_i^j = \omega_k^j \wedge \Omega_i^k - \omega_i^k \wedge \Omega_k^j$.

Proof. (1) $\omega_i^j(X) = g(\nabla_X E_i, E_j) = -g(E_i, \nabla_X E_j) = -\omega_j^i(X)$ by metric compatibility of ∇. Antisymmetry of Ω_i^j follows from (3).

(2) $d\omega^i(E_k, E_\ell) = E_k \delta_\ell^i - E_\ell \delta_k^i - \omega^i[E_k, E_\ell] = -\omega^i(\nabla_{E_k} E_\ell - \nabla_{E_\ell} E_k) = -\omega^i(\omega_\ell^j(E_k)E_j - \omega_k^j(E_\ell)E_j) = \omega_k^i(E_\ell) - \omega_\ell^i(E_k)$, where the second step uses symmetry of ∇. On the other hand, $(\omega^j \wedge \omega_j^i)(E_k, E_\ell) = \delta_k^j \omega_j^i(E_\ell) - \delta_\ell^j \omega_j^i(E_k) = \omega_k^i(E_\ell) - \omega_\ell^i(E_k)$, which is identical to $d\omega^i(E_k, E_\ell)$.

(3) Similar to (2), this is just a computation.

(4)(5) follows from (2)(3) by applying d again and using $d^2 = 0$. □

1.8. Application: Chern–Gauss–Bonnet theorem.

2. Geodesics

2.1. The geodesic equation. Geodesics are the curves that naturally flow with the curvature on a Riemannian manifold. In other words, its tangent vector field should be parallel along the curve itself. Physically it is a free particle constrained to move on the manifold, with some initial position and velocity, but no external force.

2.1.1. Definition. Let $I \subset \mathbb{R}$ be an interval. A curve $\gamma : I \to M$ is a *geodesic* if $\nabla_{\gamma'}\gamma' = 0$.

2.1.2. Exercise. Show that:

(1) Let $V(t) = V^i(t)\partial_i$ be a vector field along any curve γ, then $\nabla_{\gamma'}V = (\partial_t V^i(t))\partial_i$.
(2) Geodesics have constant speed, i.e. $\partial_t|\gamma'(t)| = 0$.

2.1.3. Example. Geodesics in $\mathbb{R}^n$ with the Euclidean metric are straight lines. Geodesics in $\mathbb{S}^n$ with the round metric are great circles. Geodesics in the upper-half plane model of hyperbolic space are half-circles centered on the x-axis and vertical lines. But in general geodesics can be quite complicated.

In local coordinates $x = (x^1, \dots, x^n)$, we can write $\gamma^i = x^i \circ \gamma$, and for a vector field V along γ we can write $V = V^i(t)\partial_i$. Then $\nabla_{\gamma'}V = 0$ becomes the *parallel transport equation*

$$0 = (\partial_t V^k + \Gamma^k_{ij} V^i \partial_t \gamma^j)\partial_k. \tag{2.1.4}$$

In particular, plugging in $V = \gamma'$ gives the *geodesic equation*

$$0 = (\partial_t^2 \gamma^k + \Gamma^k_{ij} \partial_t \gamma^i \partial_t \gamma^j)\partial_k. \tag{2.1.5}$$

Both of them are systems of ordinary differential equations, so we have the following:

2.1.6. Theorem (Existence, uniqueness and smooth dependence of geodesics)**.** *The following are true:*

(1) (Existence) For any $p \in M$, $v \in T_pM$, there exists a maximal existence time $t_{p,v} \in (0, \infty]$, and a geodesic $\gamma_{p,v} : [0, t_{p,v}) \to M$ with $\gamma_{p,v}(0) = p$, $\gamma'_{p,v}(0) = v$.
(2) (Uniqueness) If $\gamma_1 : I_1 \to M$ and $\gamma_2 : I_2 \to M$ are geodesics, and there exists $t \in I_1 \cap I_2$ such that $\gamma_1(t) = \gamma_2(t)$, $\gamma_1'(t) = \gamma_2'(t)$, then $\gamma_1 = \gamma_2$ on $I_1 \cap I_2$.
(3) (Smooth dependence) The map $(p, v) \mapsto t_{p,v}$ is lower-semicontinuous, meaning that the preimage of $(c, \infty]$ is open for any $c \in \mathbb{R}$; the map $(p, v, t) \mapsto \gamma_{p,v}(t)$ is smooth in all entries, when defined.

2.1.7. Exercise. Show that geodesics are homogeneous, i.e. for $a \in \mathbb{R}$, $\gamma_{p,v}(at) = \gamma_{p,av}(t)$ whenever defined.

2.1.8. Example. Consider $\mathbb{R}^2 - \{(1, 0)\}$ with the Euclidean metric. Suppose we start from a point $p = (0, y)$ with initial velocity $v = \partial_x$. Then $t_{p,v} = \infty$ for all $y \neq 0$, but $t_{p,v} = 1$ for $y = 0$. So this space is not "geodesically complete" since not all geodesics exist forever. Coincidentally, this space is not complete in the sense of metric spaces either. Could these be related?

2.1.9. Exercise (Geodesics exit every compact set)**.** Let $p \in M$, $v \in T_pM$, such that $t_{p,v} < \infty$. Let $K \subset M$ be compact, then there exists $t_K < T_{p,v}$ such that $\gamma_{p,v}(t) \in M\backslash K$ for all $t \in (t_K, t_{p,v})$.

2.2. The exponential map.

2.2.1. Definition. For each $p \in M$, define $\mathcal{O}_p \subset T_pM$ by $\mathcal{O}_p = \{v \in T_pM : t_{p,v} > 1\}$. It is open and star-shaped. Define $\mathcal{O} = \coprod_p \mathcal{O}_p \subset TM$; it is open.

2.2.2. Definition (Exponential map)**.** Let $\exp : \mathcal{O} \to M$ be defined by $(p, v) \mapsto \gamma_{p,v}(1)$. It is smooth by theorem 2.1.6.

2.2.3. Definition (Distance function)**.** Let (M, g) be a Riemannian manifold, we define for $p, q \in M$:

$$d(p, q) = \inf_{\gamma} L(\gamma),$$

where the infimum is taken among all piecewise smooth curves $\gamma : [0, 1] \to M$, with $\gamma(0) = p$, $\gamma(1) = q$.

2.2.4. Proposition. *The function $d : M \times M \to \mathbb{R}$ is a metric on M. In other words, it satisfies $d(p, q) \geq 0$ (with equality iff $p = q$), $d(p, q) = d(q, p)$, and $d(p, q) + d(q, r) \geq d(p, r)$ for any $p, q, r \in M$.*

To prove this (in particular the first part), we need to develop some theory about the exponential map.

2.2.5. Lemma. *For any $p \in M$, the exponential map $\exp_p : \mathcal{O}_p \to M$ is a local diffeomorphism at $0 \in T_pM$.*

Proof. It suffices to show $d(\exp_p)_0 : T_pM = T_0(T_pM) \to T_pM$ is invertible. In fact, it is the identity: $d(\exp_p)_0(v) = \frac{d}{dt}\big|_{t=0} \exp_p(tv) = \frac{d}{dt}\big|_{t=0}\gamma_{p,v}(t) = v$ by definition. □

2.2.6. Proposition (Normal coordinates)**.** *Let $p \in M$. There exist coordinates $x = (x^1, \dots, x^n)$ for some neighborhood U of p, such that $g_{ij}(x) = \delta_{ij} + O(x^2)$.*

Proof. Let $e_1, \dots, e_n$ be an orthonormal frame at p, then in a neighborhood U of p the functions $x^i(\exp_p(v)) = \langle v, e_i\rangle$ are well-defined coordinates. Since $d(\exp_p)_0 = \mathrm{id}$, $g(\partial_i, \partial_j)(p) = \delta_{ij}$. Furthermore, in these coordinates, the straight lines through p are geodesics, so they satisfy the geodesic equation

$$\partial_t^2\gamma^k + \Gamma_{ij}^k \partial_t\gamma^i\partial_t\gamma^j = 0$$

so $\Gamma_{ij}^k(p) = 0$. Then $\partial_k g_{ij}(p) = g(\nabla_k\partial_i, \partial_j)(p) + g(\partial_i, \nabla_k\partial_j)(p) = 0$, which implies $g_{ij}(x) = \delta_{ij} + O(x^2)$. □

In preparation for Gauss's lemma, consider a smooth map $F : (-\varepsilon, \varepsilon) \to [0, 1] \to M$, thought of as a family of curves (this idea is important later in the variational theory of geodesics). Let $F_s = dF_{(s,t)}\partial_s$, $F_t = dF_{(s,t)}\partial_t$ be vector fields along F (i.e. sections of F^*TM).

2.2.7. Lemma. $\nabla_{F_s}F_t = \nabla_{F_t}F_s$. *In other words, $[F_s, F_t] = 0$.*

Proof. Around $p \in \operatorname{im} F$, choose local coordinates x^i. Let $F^i(s,t) = x^i(F(s,t))$. Then $F_t(s,t) = \partial_t F^i(s,t)\partial_i$ and $F_s(s,t) = \partial_s F^j(s,t)\partial_j$, so

$$\nabla_{F_s}F_t = \nabla_{F_s}(\partial_t F^i(s,t)\partial_i) = \frac{\partial^2 F^i}{\partial s\partial t}\partial_i + \partial_t F^i \nabla_{F_s}\partial_i = \frac{\partial^2 F^k}{\partial s\partial t}\partial_k + \partial_t F^i \partial_s F^j \nabla_{\partial_j}\partial_i,$$

which is symmetric in s and t since $[\partial_i, \partial_j] = 0$. □

Consider the special case where F is a *variation through geodesics*: let $p \in M$, $v \in \mathcal{O}_p$, $w \in T_pM$, then for ε small enough, $t(v + sw) \in \mathcal{O}_p$ for $s \in (-\varepsilon, \varepsilon)$, $t \in [0, 1]$. Let $F(s,t) = \exp_p(t(v + sw))$.

2.2.8. Theorem (Gauss's lemma)**.** *For any s, t, $|F_t(s,t)| = |v + sw|$ and $\langle F_s, F_t\rangle(0,t) = t\langle v, w\rangle$.*

Commonly, this lemma is also written as $\langle d(\exp_p)_v(v), d(\exp_p)_v(w)\rangle = \langle v, w\rangle$, i.e. $\exp_p$ is a *radial isometry.* This just follows from the second equation by plugging in $t = 1$.

2.2.9. Theorem (Hopf–Rinow)**.** *Let (M, g) be a Riemannian manifold. Among the following, (1)—(4) are equivalent, and all imply (5):*

(1) There exists $p \in M$ such that $\exp_p$ is defined on all of T_pM;
(2) M satisfies the Heine–Borel property, i.e. any closed and bounded subset (of course, with respect to the distance function d) is compact.
(3) (M, d) is complete as a metric space, i.e. every Cauchy sequence converges.
(4) For all $p \in M$, $\exp_p$ is defined on all of T_pM.
(5) For any $p, q \in M$, there exists a geodesic γ from p to q, such that $L(\gamma) = d(p, q)$.

2.2.10. Remark. If any of (1)—(4) is satisfied, call M *complete.* It is not true that (5) is also equivalent: consider say the open interval.

2.2.11. Corollary. *Closed (i.e. compact without boundary) manifolds are complete.*

2.3. Variational theory.

2.3.1. Definition. A *variation* of a curve $\alpha : [a, b] \to M$ is a smooth map $F : (-\varepsilon, \varepsilon) \times [a, b] \to M$ such that $F(0, t) = \alpha(t)$. It is *proper* if $F(s, 0) = \alpha(a)$ and $F(s, 1) = \alpha(b)$ for all s. Often we write $\alpha_s(t) = F(s, t)$.

2.3.2. Definition. The *energy* of a piecewise smooth curve $\alpha : [a, b] \to M$ is $E(\alpha) = \frac{1}{2}\int_a^b |\alpha'(t)|^2 dt$. Note that unlike length, it is not invariant under reparametrization.

2.3.3. Exercise. For any piecewise smooth curve $\alpha : [a, b] \to M$, we have the inequality

$$d(\alpha(a), \alpha(b)) \le L(\alpha) \le \sqrt{2(b-a)E(\alpha)}.$$

2.3.4. Definition. Define the *variation field* as $V(t) = F_s(0, t) \in \Gamma(\alpha^*TM)$. Define the *acceleration field* as $X(t) = (\nabla_{F_s}F_s)(0, t) \in \Gamma(\alpha^*TM)$.

2.3.5. Proposition (First and second variation of energy)**.** *Let α be a smooth curve, and F a variation.*

(1) $\frac{d}{ds}E(\alpha_s)\big|_{s=0} = \langle V(t), \alpha'(t)\rangle\big|_{t=a}^{b} - \int_a^b \langle V(t), \nabla_{\alpha'(t)}\alpha'(t)\rangle dt$.

(2) $\frac{d^2}{ds^2}E(\alpha_s)\big|_{s=0} = \langle X(t), \alpha'(t)\rangle\big|_a^b - \int_a^b \langle X(t), \nabla_{\alpha'(t)}\alpha'(t)\rangle dt + \int_a^b (|\nabla_{\alpha'(t)}V(t)|^2 - R(\alpha', V, \alpha', V))dt$.

2.3.6. Corollary. *For a proper variation F of a smooth curve α,*

(1) $\frac{d}{ds}E(\alpha_s)\big|_{s=0}$ *iff α is a geodesic.*

(2) *If α is a geodesic, then $\frac{d^2}{ds^2}E(\alpha_s)\big|_{s=0} = I(V,V)$, where I is the* index form

$$I(Y,W) = \int_a^b (\langle \nabla_{\alpha'}Y, \nabla_{\alpha'}W\rangle - R(\alpha', Y, \alpha', W))dt.$$

2.3.7. Definition. Let $\alpha : [a,b] \to M$ be a geodesic. A vector field V along α is called a *Jacobi field* if any of the following equivalent conditions hold:

(1) V arises as a variation of α through geodesics. More precisely, there exists a variation F of α such that each α_s is a geodesic, and V is the variation field of F.

(2) $\nabla_{\alpha'}\nabla_{\alpha'}V + R(\alpha', V)\alpha' = 0$.

2.3.8. Remark. Suppose V is a Jacobi field, then

$$\begin{aligned} I(V,V) &= \int_a^b (|\nabla_{\alpha'}V|^2 + \langle \nabla_{\alpha'}\nabla_{\alpha'}V, V\rangle)dt \\ &= \int_a^b \nabla_{\alpha'}(\langle \nabla_{\alpha'}V, V\rangle)dt = \langle \nabla_{\alpha'}V, V\rangle\big|_a^b = \frac{1}{2}(\frac{\partial}{\partial t}|V|^2)\big|_a^b. \end{aligned}$$

2.3.9. Proposition. *Suppose V is a Jacobi field along $\alpha : [a,b] \to M$ from p to q, such that $V(a) = 0$ and $(\nabla_{\alpha'}V)(a) = w \in T_pM$. Then $V(t) = d(\exp_p)_{tv}(tw)$, where $v = \alpha'(a)$.*

Finally, we discuss conjugate points and stability.

2.3.10. Definition. A geodesic $\alpha : [a,b] \to M$ is *stable* (with fixed endpoints) if for all vector fields V along α with $V(a) = V(b) = 0$, $I(V,V) \geq 0$.

2.3.11. Exercise. If α is length-minimizing, then it is stable.

2.3.12. Definition. We say $t_0 \neq t_1 \in [a,b]$ are *conjugate points* along α, if there exists a nonzero Jacobi field V along α with $V(t_0) = V(t_1) = 0$.

2.3.13. Proposition. *Let $\alpha : [a,b] \to M$ be a geodesic, then α is unstable iff there exists $\tau \in (a,b)$ such that $\alpha(a), \alpha(\tau)$ are conjugate.*

Proof. ($\Longleftarrow$): suppose there exists $\tau \in (a,b)$ such that $\alpha(a), \alpha(\tau)$ are conjugate points. Let $V(t)$ be the nontrivial Jacobi field along α that vanishes at a and τ. Define the piecewise smooth vector field $\widetilde{V}$ along α by $\widetilde{V}(t) = V(t)$ for $a \leq t \leq \tau$ and $\widetilde{V}(t) = 0$ for $\tau \leq t \leq b$. Then

$$I(\widetilde{V}, \widetilde{V}) = \int_a^\tau (|\nabla_{\alpha'}V|^2 - R(\alpha', V, \alpha', V))dt = \langle (\nabla_{\alpha'}V)(t), V(t)\rangle\big|_{t=a}^{\tau} = 0.$$

So, assuming stability, for any vector field X along α with $X(a) = X(b) = 0$, we have that $0 \leq I(\widetilde{V}+sX, \widetilde{V}+sX) = 2sI(\widetilde{V}, X) + s^2V(X,X)$. Note that $\frac{d}{ds}\big|_{s=0} I(\widetilde{V}+sX, \widetilde{V}+sX) = 2I(\widetilde{V}, X)$. If $I(\widetilde{V}, X) \neq 0$ then there exists s (with small absolute value) such that $I(\widetilde{V}+sX, \widetilde{V}+sX) < I(\widetilde{V}, \widetilde{V}) = 0$, which contradicts stability. So $I(\widetilde{V}, X) = 0$. On the other hand, since V is a Jacobi field, $R(\alpha', V, \alpha', X) = -\langle \nabla_{\alpha'}\nabla_{\alpha'}V, X\rangle$, so

$$0 = I(\widetilde{V}, X) = \int_a^\tau (\langle \nabla_{\alpha'}V, \nabla_{\alpha'}X\rangle + \langle \nabla_{\alpha'}\nabla_{\alpha'}V, X\rangle)dt = \langle (\nabla_{\alpha'}V)(t), X(t)\rangle\big|_{t=a}^{\tau} = \langle (\nabla_{\alpha'}V)(\tau), X(\tau)\rangle$$

for any X vanishing at a and b. Since $X(\tau)$ can be any vector, we conclude that $(\nabla_{\alpha'}V)(\tau) = 0$. But since V is a Jacobi field, it is uniquely determined by $V(\tau)$ and $(\nabla_{\alpha'}V)(\tau)$, which are both zero, so $V \equiv 0$, contradiction.

($\Longrightarrow$): suppose α is unstable, then the first (smallest) eigenvalue of the Jacobi operator (acting on the completion of the space of all smooth vector fields along α which vanish at endpoints)

$$L : V \mapsto \nabla_{\alpha'}\nabla_{\alpha'}V - R(\alpha', V)\alpha'$$

is negative. Let $\lambda_1(\tau)$ denote the smallest eigenvalue when L is restricted to act on vector fields along $\alpha|_{[a,\tau]}$ (which vanish at endpoints). Then $\lambda_1(b) < 0$, and λ_1 is non-increasing on $(a, b]$ (because for $\tau_1 < \tau_2$, if a vector field V along $\alpha|_{[a,\tau_1]}$ satisfies $LV = \lambda V$, then the vector field $\widetilde{V}$ along $\alpha|_{[a,\tau_2]}$ which is equal to V on $[a, \tau_1]$ and zero on $[\tau_1, \tau_2]$ satisfies $L\widetilde{V} = \lambda\widetilde{V}$). So, it is enough to show that $\lambda_1(\tau)$ is positive for τ close to a, and conclude by intermediate value theorem that there exists τ where L has a zero eigenvalue (i.e. Jacobi field), so that $\alpha(a), \alpha(\tau)$ are conjugate.

Now, for any smooth vector field V along $\alpha|_{[a,\tau]}$, vanishing at endpoints, we have

$$\int_a^\tau |\nabla_{\alpha'} V|^2 dt \geq \int_a^\tau |\partial_t |V||^2 dt \geq \frac{\pi^2}{(\tau - a)^2} \int_a^\tau |V|^2 dt$$

where the first step by Kato's inequality and the second step by Wirtinger's inequality. Also, for any point $p \in \operatorname{im}(\alpha)$, the quantity $\frac{R(\alpha', V, \alpha', V)(p)}{|V(p)|^2}$ by some absolute constant not depending on $V(p)$ by compactness, and by compactness again there is a constant K such that $R(\alpha', V, \alpha', V)(p) \leq K \cdot |V(p)|^2$ for any V and p. So

$$\int_a^\tau R(\alpha', V, \alpha', V) dt \leq K \cdot \int_a^\tau |V|^2 dt.$$

Together, we get $I(V, V) \geq \left(\frac{\pi^2}{(\tau-a)^2} - K\right) \int_a^\tau |V|^2 dt$. So, the Rayleigh quotient

$$\lambda_1(\tau) = \inf_{V \neq 0} \frac{I(V, V)}{\int_a^\tau |V|^2 dt} \geq \frac{\pi^2}{(\tau - a)^2} - K$$

is positive for τ sufficiently close to a. This completes the proof. □

2.4. Segment domain, cut locus, injectivity and conjugacy radii. Let (M, g) be a complete Riemannian manifold.

2.4.1. Definition. Let $p \in M$. The *segment domain* of p is

$$\operatorname{seg}(p) = \{v \in T_pM : d(p, \exp_p(v)) = |v|\}.$$

In other words, it is the set of tangent vectors whose geodesic is minimizing. Clearly, it is a closed and star-shaped set.

Define also $\operatorname{seg}^\circ(p) = \{tv : v \in \operatorname{seg}(p), 0 \leq t < 1\}$. One of the main results in this subsection is that $\operatorname{seg}^\circ(p)$ is just the interior of $\operatorname{seg}(p)$.

2.4.2. Definition. Let $p \in M$. The *cut locus* is $\operatorname{cut}(p) = M \setminus \exp_p(\operatorname{seg}^\circ(p))$.

2.4.3. Proposition. *Suppose $v \in \overline{T_pM \setminus \operatorname{seg}^\circ(p)}$. Then at least one of the following two things happen:*

- *$d(\exp_p)_v$ is singular;*
- *there exists $w \neq v$, $w \in \operatorname{seg}(p)$, such that $\exp_p(v) = \exp_p(w)$.*

2.4.4. Theorem. *We have the following:*

1. *$d(\exp_p)_v$ is invertible for all $v \in \operatorname{seg}^\circ(p)$.*
2. *If $v \in \operatorname{seg}^\circ(p)$ and $w \in \operatorname{seg}(p)$, and $\exp_p(v) = \exp_p(w)$, then $v = w$.*
3. *$\operatorname{seg}^\circ(p)$ is open.*
4. *The exponential map $\exp_p : \operatorname{seg}^\circ(p) \to M \setminus \operatorname{cut}(p)$ is a diffeomorphism.*

This motivates the following definitions:

2.4.5. Definition. The *injectivity radius* of p is

$$\operatorname{inj}(p) = \sup\{R : \exp_p|_{B_0(R)} \text{ is a diffeomorphism}\}.$$

The *conjugacy radius* of p is

$$\operatorname{conj}(p) = \sup\{R : \exp_p|_{B_0(R)} \text{ is nonsingular}\}.$$

By definition, $\operatorname{inj}(p) \leq \operatorname{conj}(p)$. The two can differ in general: consider the flat torus (as a quotient of $\mathbb{R}^2$), then some geodesics will close up, and $\exp_p$ is non-injective without ever becoming singular.

Finally, here are two results we state without proof. The second one is not easy.

2.4.6. Proposition. *Let $p \in M$, $q \in \operatorname{cut}(p) \neq \varnothing$, such that $d(p,q) = d(p, \operatorname{cut}(p))$. Then either q is conjugate to p along a geodesic from p to q, or there exists exactly 2 minimizing geodesics from p to q which close up to form a loop.*

2.4.7. Theorem (Klingenberg's estimates)**.** *The following estimates for the injective radius hold:*

- *If n is even and M is orientable, and $0 \leq \sec \leq 1$, then $\operatorname{inj}(M) \geq \pi$.*
- *If $n \geq 3$ and M is simply connected, and $\frac{1}{4} \leq \sec \leq 1$, then $\operatorname{inj}(M) \geq \pi$.*

3. Comparison geometry

3.1. Main theorems.

We will be proving several theorems that deduce global topological information of a Riemannian manifold from local curvature information.

3.1.1. Theorem (Bonnet–Myers)**.** *Let (M,g) be a complete n-dimensional Riemannian manifold, such that there exists $\kappa > 0$ with $\operatorname{Ric}(V,V) \geq \kappa(n-1)|V|$ for all vector fields V. Then every geodesic of length greater than $\pi/\sqrt{\kappa}$ is unstable. Consequently it is compact and has finite fundamental group.*

3.1.2. Theorem (Synge)**.** *Let (M,g) be a closed n-dimensional Riemannian manifold with positive sectional curvature. Then, if n is even and M is orientable, then M is simply connected; if n is odd, then M is orientable.*

3.1.3. Theorem (Preissmann)**.** *Let (M,g) be a closed n-dimensional Riemannian manifold with negative sectional curvature. Then any nontrivial abelian subgroup of $\pi_1(M)$ is isomorphic to $\mathbb{Z}$.*

3.1.4. Theorem (Cartan–Hadamard)**.** *Let (M,g) be a complete, simply connected Riemannian manifold with non-positive sectional curvature. Then for any $p \in M$, $\exp_p : T_pM \to M$ is a diffeomorphism.*

3.1.5. Theorem (Space forms)**.** *Let (M,g) be a complete, simply connected Riemannian manifold with constant sectional curvature $\kappa \in \{-1,0,1\}$. Then (M,g) is isometric to the hyperbolic space $\mathbb{H}^n$, Euclidean space $\mathbb{R}^n$, or the sphere $\mathbb{S}^n$, respectively.*

3.2. Proof of the Bonnet–Myers theorem.

3.3. Proof of the Cartan–Hadamard theorem.

3.3.1. Definition. Let M be a Riemannian manifold, $f \in C^\infty(M)$. Define its *Hessian* $\nabla^2 f = \operatorname{Hess}(f)$ to be a symmetric $(0,2)$-tensor such that

$$(\nabla^2 f)(X,Y) = g(\nabla_X(\nabla f), Y) = X(Y(f)) - (\nabla_X Y)(f).$$

Recall that ∇f is the gradient (example 1.1.7) of f. In local coordinates,

$$\operatorname{Hess}(f)(\partial_i, \partial_j) = \nabla_i \nabla_j f = \frac{\partial^2 f}{\partial x^i \partial x^j} - \nabla_{ij}^k \frac{\partial f}{\partial x^k}.$$

3.3.2. Proposition. *Let (M,g) be a complete Riemannian manifold. Let $p \in M$ and define a function $\rho(x) = d(p,x)$, so that ρ^2 is smooth on $\operatorname{seg}^\circ(p)$. For $v \in \operatorname{seg}^\circ(p)$, $q = \exp_p(v)$, $w \in T_qM$, let $\alpha(t) = \exp_p(tv)$, and W the unique Jacobi field along α such that $W(0) = 0$ and $W(1) = w$. Then,*

- $\nabla(\frac{1}{2}\rho^2)(q) = \alpha'(1)$.
- $\nabla^2(\frac{1}{2}\rho^2)_q(w,w) = I(W,W) = \frac{1}{2}\frac{\partial}{\partial t}\big|_{t=1}|W|^2$,

3.3.3. Corollary. *Let $w_0, w_1 \in T_qM$ such that w_0 is parallel to $d(\exp_p)_v(v) = \alpha'(1)$, and w_1 is orthogonal to it. Then $\nabla^2(\frac{1}{2}\rho^2)_q(w_0,w_0) = |w_0|^2$ and $\nabla^2(\frac{1}{2}\rho^2)_q(w_0,w_1) = 0$.*

3.3.4. Theorem (Rauch comparison theorem)**.** *Let (M,g) be a Riemannian manifold with $\sec \leq \mu$. Let $\alpha : [0,\ell] \to M$ be a unit-speed geodesic, and V a Jacobi field along α which is orthogonal to α'. Suppose $f : [0,\ell] \to \mathbb{R}$ solves $f''(t) + \mu f(t) = 0$ with initial condition $f(0) = |V(0)|$ and $f'(0) = \frac{d}{dt}\big|_{t=0}|V(t)|$. Then $t \mapsto \frac{|V(t)|}{f(t)}$ is non-decreasing for $t \in (0,\ell)$. In particular, $|V(t)| \geq f(t)$.*

3.3.5. Corollary. *Let (M,g) be a Riemannian manifold with $\sec \leq \mu$. Let $\alpha : [0,\ell] \to M$ be a unit-speed geodesic, such that $\alpha(0)$ and $\alpha(\ell)$ are conjugate along α. Then $\mu > 0$ and $\ell \geq \pi/\sqrt{\mu}$.*

3.3.6. Theorem.

3.3.7. Corollary (Hessian comparison)**.** *Let (M, g) be a Riemannian manifold with* $\sec \leq \mu$. *Let $F(t)$ be an antiderivative to $f(t)$. For any $p \in M$, we have the following estimate on on $M \setminus \operatorname{cut}(p)$:*

$$\nabla^2 F(\rho) \geq F''(\rho) g.$$

3.3.8. Remark. Equivalently, we can write this as $\nabla^2 \rho \geq \operatorname{ct}_\mu(\rho)(g - d\rho \otimes d\rho)$.

3.3.9. Definition. Define the *divergence* of a vector field $V \in \Gamma(TM)$ by

$$\operatorname{div}(V) = \sum_{i=1}^{n} g(\nabla_{e_i} V, e_i) \in C^\infty(M)$$

for any orthonormal basis e_i of T_pM. In coordinates, $\operatorname{div}(V) = \nabla_i V^i = \partial_i V^i + \Gamma^i_{ij} V^j$.

3.3.10. Definition. Define the *Laplacian* of $f \in C^\infty(M)$ by $\Delta f = \operatorname{div}(\nabla f)$. Call f *harmonic* if $\Delta f = 0$.

CHAPTER 9

Étale cohomology

1. Flatness

1.1. Flat modules.

1.1.1. Proposition. *Let A be a ring, M an A-module. TFAE:*

(1) M is flat;
(2) $\operatorname{Tor}_i^A(M,N)=0$ for any A-module N and $i\geq 1$;
(3) $\operatorname{Tor}_i^A(M,N)=0$ for any finitely generated A-module N and $i\geq 1$;
(4) $\operatorname{Tor}_1^A(M,N)=0$ for any A-module N;
(5) $\operatorname{Tor}_1^A(M,N)=0$ for any finitely generated A-module N;
(6) $\operatorname{Tor}_1^A(M,A/I)=0$ for any ideal $I\subseteq A$;
(7) $\operatorname{Tor}_1^A(M,A/I)=0$ for any finitely generated ideal $I\subseteq A$;
(8) For any ideal $I\subseteq A$, the map $I\otimes_A M\to M$ is injective;
(9) For any finitely generated ideal $I\subseteq A$, the map $I\otimes_A M\to M$ is injective.

Proof. Obviously:

$$\begin{tikzcd}
(1) \arrow[r] & (2) \arrow[r] \arrow[d] & (4) \arrow[d] & (6) \arrow[r, leftrightarrow] \arrow[d] & (8) \\
& (3) \arrow[r] & (5) \arrow[ru] & (7) \arrow[r, leftrightarrow] & (9).
\end{tikzcd}$$

The remaining implications:

(4) $\implies$ (1): For any short exact sequence $0\to Q\to P\to N\to 0$, we have the Tor long exact sequence

$$\cdots\to\operatorname{Tor}_1^A(M,N)\to M\otimes Q\to M\otimes P\to M\otimes N\to 0,$$

so $0\to M\otimes Q\to M\otimes P\to M\otimes N\to 0$ is exact.

(5) $\implies$ (4): Let N be an A-module. We use the fact that $N=\varinjlim N'$, where N' ranges among the finitely generated submodules of N, ordered by inclusion. This is a filtered colimit, which is exact (AB5) and commutes with left adjoints, such as tensor products. So for any short exact sequence $0\to Q\to P\to M\to 0$ that ends with M, tensoring with N is exact. Now we take P to be free (therefore flat), so $\operatorname{Tor}_1^A(N,P)=0$. Then the Tor exact sequence reads

$$\cdots\to 0\to\operatorname{Tor}_1^A(N,M)\to Q\otimes N\to P\otimes N\to M\otimes N\to 0,$$

so $\operatorname{Tor}_1^A(N,M)\to Q$ is injective and its image is zero. So $\operatorname{Tor}_1^A(N,M)=0$ as desired.

(6) $\implies$ (5): Consider a finitely generated N. Then there exists a filtration

$$0=N_0\subset N_1\subset\cdots\subset N_n=N,$$

where each N_i/N_{i-1} is generated by one element, i.e. isomorphic as A-module to A/I for some ideal I. Induct on i and we wish to show $\operatorname{Tor}_1^A(M,N_i)=0$. The base case $i=1$ is clear. For the induction step, we have the exact sequence

$$0\to N_{i-1}\to N_i\to N_i/N_{i-1}\to 0,$$

and by the Tor long exact sequence, $\operatorname{Tor}_1^A(M,N_i)=0$.

(7) $\implies$ (6): Use the fact that $A/I=\varinjlim A/I'$ where I' ranges among the finitely generated ideals contained in I, ordered by inclusion. Then we can mimic the argument in the implication (5) $\implies$ (4). □

1.1.2. Proposition. *Let M be flat, then tensoring with M commutes with intersections.* □

1.1.3. Proposition (flatness and localizations)**.** *Let A be a ring, $S\subset A$ a multiplicative subset. Then:*

(i) *$S^{-1}A$ is flat over A;*
(ii) *Let M be flat over A, then $S^{-1}M$ is flat over $S^{-1}A$;*
(iii) *Suppose $A \to B$ is a ring homomorphism that sends S to a subset of a multiplicative subset $T \subseteq B$, and let N be a B-module. If N is flat over A, then $T^{-1}N$ is flat over $S^{-1}A$;*
(iv) *Suppose $A \to B$ is a ring homomorphism, and N is a B-module. If $N_{\mathfrak{m}}$ is flat over A for every maximal ideal $\mathfrak{m} \subset B$, then N is flat over A.*

PROOF. (iii) Notice that $T^{-1}N \otimes_A \bullet = T^{-1}(N \otimes_A \bullet)$ is an exact functor, so $T^{-1}N$ is flat over A. So $S^{-1}T^{-1}N = T^{-1}N$ is flat over $S^{-1}A$.

(iv) Injectivity is a local property. □

1.1.4. Proposition (flatness and torsion-free)**.** *Let A be a ring.*

(i) *If $a \in A$ is a non-zerodivisor, and M is a flat A-module, then $M \to M$ given by $m \mapsto am$ is injective; in particular, if A is a domain, then M is torsion-free.*
(ii) *Let A be a Dedekind domain, then any torsion-free A-module is flat.*

PROOF. (i) Because a is not a zero-divisor, the map $A \to A_a$ is injective, and so is $M \to M \times_A A_a$ since M is flat. Suppose $am = 0$ for some $m \in M$, then $m \mapsto m \otimes 1 = am \otimes a^{-1} = 0$, so $m = 0$ as well by injectivity.

(ii) Suppose M is torsion-free. It suffices to show that $M_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m} \subset A$, i.e. we may assume that A is a DVR. Let $I \subseteq A$ be any ideal, then I is principal, say generated by r, and the map $A \to I$ given by $1 \mapsto r$ is an isomorphism of A-modules. So $M \to I \otimes_A M$, $m \mapsto r \otimes m$ is an isomorphism. Composing this with the natural map $f : I \otimes_A M \to M$, $r \otimes m \mapsto rm$, gives us the map $M \to M$, $m \mapsto rm$, which is injective since M is torsion-free. So f is injective as well, which shows that M is flat. □

1.2. Flat morphisms.

2. Faithfully flat descent

2.1. Faithfully flat morphisms.

2.1.1. Proposition. *Let A be a ring, M an A-module. TFAE:*

(1) *The functor $N \mapsto M \otimes N$ is exact and faithful;*
(2) *Any sequence $N' \to N \to N''$ is exact iff $M \otimes N' \to M \otimes N \to M \otimes N''$ is exact;*
(3) *M is flat, and $M \otimes N = 0$ implies $N = 0$;*
(4) *M is flat, and $M/\mathfrak{m}M \neq 0$ for any maximal ideal $\mathfrak{m}$ of A.* □

If any of the following holds, we say M is *faithfully flat* over A.

2.1.2. Corollary. *Let $A \to B$ be a map of local rings that maps the maximal ideal of A into the maximal ideal of B. Then if a nonzero, finitely generated B-module M is flat over A, it is faithfully flat over A.*

2.1.3. Proposition. *Let $A \to B$ be a map of rings. If there exists a B-module M faithfully flat over A, then* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is onto.*

PROOF. The fiber over $\mathfrak{p} \subset A$ is $\operatorname{Spec} B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. Since $M \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is faithfully flat over $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, it is a nonzero $B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$-module, so $B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \neq 0$. □

2.1.4. Corollary. *Let $A \to B$ be a map of rings. Suppose there exists a finitely generated B-module M faithfully flat over A, whose support is* $\operatorname{Spec} B$*. Then for any $\mathfrak{p} \in \operatorname{Spec} A$, if $\mathfrak{q}$ is minimal among those containing $\mathfrak{p}B$, then $\mathfrak{q}^c = \mathfrak{p}$.*

PROOF. By corollary 2.1.2, $M_{\mathfrak{q}}$ is faithfully flat over $A_{\mathfrak{q}^c}$. By proposition 2.1.3, $\operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{q}^c}$ is onto. Then by minimality of $\mathfrak{q}$, $\mathfrak{q}B_{\mathfrak{q}}$ is the preimage of $\mathfrak{p}A_{\mathfrak{q}^c}$, so $\mathfrak{p} = \mathfrak{q}^c$ as desired. □

2.1.5. Proposition. *Let $\phi : A \to B$ be a map of rings. TFAE:*

(1) *B is faithfully flat over A;*
(2) *B is flat over A, and $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective;*
(3) *B is flat over A, and for any maximal $\mathfrak{m} \subset A$, there exists a maximal $\mathfrak{n} \subset B$ with $\mathfrak{m} = \mathfrak{n}^c$;*

(4) *B is flat, and for any A-module M, $M \to M \otimes_A B$ is injective;*
(5) *For any ideal I of A, $I \otimes_A B \to B$ is injective, and $\phi^{-1}(IB) = I$.*
(6) *ϕ is injective and $\operatorname{coker}\phi$ is flat over A.*

Proof. It is clear that (1) $\implies$ (2) $\implies$ (3).

(3) $\implies$ (1): It suffices to show that $B/\mathfrak{m}B \neq 0$ for any maximal $\mathfrak{m}$ of A. Pick $\mathfrak{n} \subset B$ such that $\mathfrak{n}^c = \mathfrak{m}$, then there is a surjection $B/\mathfrak{m}B \to B/\mathfrak{n} \neq 0$.

(1) $\implies$ (4): Since B is faithfully flat, it suffices to show $M \otimes_A B \to M \otimes_A B \otimes_A B$ is injective. But this has a left inverse $M \otimes_A B \otimes_A B \to M \otimes_A B$ given by $m \otimes b_1 \otimes b_2 \mapsto m \otimes b_1 b_2$.

(4) $\implies$ (5): Since $A/I \to (A/I) \otimes_A B = B/IB$ is injective, $\phi^{-1}(IB) \subseteq I$, so $\phi^{-1}(IB) = I$.

(5) $\implies$ (3): We know B is flat, and $\phi^{-1}(\mathfrak{m}B) = \mathfrak{m}$, so any maximal ideal $\mathfrak{n}$ containing $\mathfrak{m}B$ pulls back to $\mathfrak{n}^c = \mathfrak{m}$.

(4) $\implies$ (6): Putting $M = A$, we see that ϕ is injective. Let M be any A-module. The long exact sequence reads

$$(*) \qquad 0 \to \operatorname{Tor}_1^A(B, M) \to \operatorname{Tor}_1^A(\operatorname{coker}\phi, M) \to M \to M \otimes_A B.$$

Since B is flat, $\operatorname{Tor}_1^A(B, M) = 0$. Since $M \to M \otimes_A B$ is injective, we conclude that

$$\operatorname{Tor}_1^A(\operatorname{coker}\phi, M) = 0,$$

which implies that $\operatorname{coker}\phi$ is flat.

(6) $\implies$ (4): This time $(*)$ tells us that $\operatorname{Tor}_1^A(B, M) = 0$ and $M \to M \otimes_A B$ is injective. □

2.1.6. Proposition (faithful flatness and completions). *Let A be Noetherian, and let $I \subset A$ be an ideal. Then the I-adic completion $\widehat{A}$ is flat over A, and it is faithfully flat iff $I \subseteq \operatorname{rad}(A)$.* □

2.1.7. Proposition. *Let A be a ring, $I \subset A$ an ideal, and M an A-module. If either*

- *I is nilpotent, or*
- *A is Noetherian, $I \subset \operatorname{rad}(A)$, and M is finitely generated,*

then TFAE:

(1) *M is free;*
(2) *M/IM is free over A/I, and $\operatorname{Tor}_1^A(M, A/I) = 0$;*
(3) *M/IM is free over A/I, and*

$$(M/IM) \otimes_{A/I} \left(\bigoplus_{n \geq 0} I^n/I^{n+1} \right) \to \bigoplus_{n \geq 0} I^n M/I^{n+1} M$$

is an isomorphism.

Proof. □

2.2. The Amitsur complex.

2.3. Descent data, and stacks.

2.4. Descent of quasicoherent sheaves.

3. Quasi-finite morphisms

3.1. Finite morphisms.

3.1.1. Proposition (finite implies proper). *Any finite morphism $f : Y \to X$ is separated, finite type, and universally closed.*

Proof. Properness is affine-local on the target, so assume X, Y are affine. Then the first two requirements are obvious; the third follows from the going-up theorem and the fact that finite morphisms are stable under base change. □

3.1.2. Proposition. *Let $f : X \to \operatorname{Spec} k$ be finite type, then TFAE:*

(1) *$X = \operatorname{Spec} A$ where A is Artinian;*
(2) *X is finite and discrete;*

(3) *X is discrete;*
(4) *f is finite.*

Proof. (1) $\implies$ (2): Artinian rings have finitely many prime ideals, and all primes are maximal.

(3) $\implies$ (2): Discrete plus quasicompact implies finite.

(2) $\implies$ (4): For any affine open $\operatorname{Spec} A \subseteq X$, A is Noetherian and has dimension 0, so A is Artinian, so it is uniquely the product of Artinian local rings. So X is affine ($\mathcal{O}_X(X)$ is the product of the Artinian local rings corresponding to each point of X).

(4) $\implies$ (1): Say $X = \operatorname{Spec} A$. Then A is a finitely generated k-module, so $\dim A = \operatorname{tr\,deg} \operatorname{Frac} A = 0$, so A is Artinian. □

3.2. Quasifinite morphisms.

3.2.1. Definition. A morphism of schemes $f : Y \to X$ is *quasifinite* if it is finite-type and has finite fibers. An A-algebra B is *quasifinite* if it is finite-type and for all prime ideals $\mathfrak{p} \subset A$, $B \times_A \kappa(\mathfrak{p})$ is a finite $\kappa(\mathfrak{p})$-module (i.e. $\operatorname{Spec} B \to \operatorname{Spec} A$ is quasifinite).

Since finite morphisms have finite fibers, finite implies quasifinite.

3.2.2. Proposition. *Quasifiniteness is stable under composition and base change, and any immersion is quasifinite.* □

It follows that any open subscheme of a finite morphism is quasifinite. Conversely:

3.2.3. Theorem (Zariski's main theorem, Grothendieck's form: EGA IV$_3$, Thm 8.12.6)**.** *Let X be quasicompact, then any separated, quasifinite morphism $f : Y \to X$ factors into $Y \to Y' \to X$, where $Y \to Y'$ is an open embedding, and $Y' \to X$ is finite.*

3.2.4. Corollary (proper and quasifinite implies finite)**.** *Let X be quasicompact, then any proper, quasifinite morphism $f : Y \to X$ is finite.*

Proof. Let $f = g \circ f'$ where $f' : Y \to Y'$ is an open immersion and $g : Y' \to X$ is finite. Since g is finite, it is separated (proposition 3.1.1), so Δ_g is a closed immersion, which is proper. So Δ_g and f are both proper, so by cancellation theorem, f' is proper as well, so its image is closed. Therefore, f' is a closed immersion, hence finite as well, so f is finite. □

3.2.5. Exercise. Let $f : Y \to X$ be separated and finite type, X irreducible. If the fiber over the generic point $\eta \in X$ is finite, then there is a nonempty open $U \subseteq X$ such that f is finite over U.

Proof. (TODO) □

3.3. Zariski's main theorem.

4. Unramified morphisms

In the next three sections, we introduce three classes of morphisms of schemes: unramified, smooth, and étale morphisms. They correspond respectively to the notions of immersions, submersions, and local isomorphisms in differential geometry. As is usual, we use our geometric intuition to guide algebraic definitions.

4.1. Module of differentials. Given a ring homomorphism $A \to B$, we may naturally define a B-module $\Omega_{B/A}$, whose classical analogy is the (relative) cotangent bundle on $\operatorname{Spec} B$.

4.1.1. Definition. The *module of Kähler differentials* of a ring map $A \to B$ is a B-module $\Omega_{B/A}$ together with an A-derivation $\mathrm{d} : B \to \Omega_{B/A}$, defined equivalently by any of the following:

(1) universal property: it represents the covariant functor $\mathrm{Mod}_B \to \mathrm{Set}$ which sends $M \mapsto \operatorname{Der}_A(B, M)$.
(2) construction: it is the free B-module generated by symbols $\mathrm{d}b$, for $b \in B$, modulo the submodule generated by $\mathrm{d}a$ ($a \in A$), $\mathrm{d}(b + b') - \mathrm{d}b - \mathrm{d}b'$, and $\mathrm{d}(bb') - b\mathrm{d}b' - b'\mathrm{d}b$.
(3) diagonal: it is I/I^2 where $I = \ker(B \otimes_A B \xrightarrow{b\otimes b' \mapsto bb'} B)$, and $\mathrm{d} : B \to I/I^2$ is given by $b \mapsto 1 \otimes b - b \otimes 1$.

4.1.2. Example. Some common and useful examples:

- If $A \to B$ is a quotient map or a localization, $\Omega_{B/A} = 0$.
- If $B = A[x_1, \ldots, x_n]$, then $\Omega_{B/A} \cong \bigoplus_i B\,\mathrm{d}x_i$.
- If $B = A[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ then $\Omega_{B/A} \cong (\bigoplus_i B\,\mathrm{d}x_i)/\langle \mathrm{d}f_1, \ldots, \mathrm{d}f_m\rangle$. In particular, $\Omega_{B/A}$ is finitely presented (resp. finitely generated) as a B-module if B is finitely presented (resp. finitely type) as an A-algebra.
- If L/K is a finite separable field extension, then $\Omega_{L/K} = 0$.

4.1.3. Example (Elliptic curves)**.** Consider the affine plane curve $y^2 = x^3 + ax + b$ over an algebraically closed field k. Let $A = k[x, y]/(y^2 - x^3 - ax - b)$ be its coordinate ring. The module of differentials is

$$\Omega_{A/k} = \frac{k\mathrm{d}x \oplus k\mathrm{d}y}{\langle 2y\mathrm{d}y - (3x^2 + a)\mathrm{d}x\rangle}.$$

Consider the distinguished opens $D(3x^2 + a)$ and $D(2y)$ which cover $\operatorname{Spec} A$ if $4a^3 - 27b^2 \neq 0$ (i.e. the curve is nonsingular). On each of them, $\Omega_{A/k}$ is isomorphic to a free rank 1 module.

4.1.4. Proposition (Pullback of differentials)**.** *Let $A \to B$, $A \to A'$ be ring maps, and let $B' = A' \otimes_A B$. Then $\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_B B'$ as B'-modules.*

In particular, taking $A' = S^{-1}A$ for a multiplicative subset S, we have $\Omega_{S^{-1}B/A} \cong \Omega_{S^{-1}B/S^{-1}A} \cong S^{-1}\Omega_{B/A}$.

4.1.5. Proposition (Cotangent exact sequence)**.** *Let $A \to B \to C$ be ring maps. Then there is a natural exact sequence of C-modules*

$$\Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

4.1.6. Proposition (Conormal exact sequence)**.** *In the above situation, suppose the map $B \to C$ is a quotient map with kernel I. Then there is a natural exact sequence of C-modules*

$$I/I^2 \to \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0,$$

where the first map is induced by $\mathrm{d} : B \to \Omega_{B/A}$.

4.1.7. Proposition (Fiber at rational point)**.** *Let B be a k-algebra, and $\mathfrak{m} \subset B$ a maximal ideal with residue field k. Then $\Omega_{B/k} \otimes_B k \cong \mathfrak{m}/\mathfrak{m}^2$.*

4.2. Unramified ring maps.

4.2.1. Definition. Let $A \to B$ be a ring map. Say B is *formally unramified* over A if any of the following equivalent conditions hold:

(1) for any A-algebra R and an ideal $I \subset R$, such that $I^2 = 0$, the natural map $\operatorname{Hom}_A(B, R) \to \operatorname{Hom}_A(B, R/I)$ is injective;
(2) in condition (1), replace $I^2 = 0$ with I nilpotent;
(3) the module of differentials $\Omega_{B/A} = 0$.

Intuitively, being formally unramified means that the map on tangent spaces is injective, i.e. tangent vectors lift uniquely: take $R = k[\varepsilon]/(\varepsilon^2)$ and $I = (\varepsilon)$ for example.

Proof. (1) $\Longrightarrow$ (3): Consider the A-algebra $B \oplus \Omega_{B/A}$, with $(x_1, y_1)(x_2, y_2) := (x_1x_2, x_1y_2 + x_2y_1)$, and map $A \to B \oplus \Omega_{B/A}$ given by $a \mapsto (a, 0)$. In this ring, $\Omega_{B/A}$ is an ideal of square zero, and the quotient ring is B. But there are two lifts of the identity $B \to B$ to A-algebra homomorphisms $B \to B \oplus \Omega_{B/A}$: one maps $b \mapsto (b, 0)$, the other $b \mapsto (b, \mathrm{d}b)$. So $\mathrm{d}b = 0$, and $\Omega_{B/A}$ is trivial.

(3) $\Longrightarrow$ (1): Any A-derivation of B is zero. Suppose $f, g : B \to R$ both lift the same $B \to R/I$, then $f - g$ lands in I. In fact, since $I^2 = 0$, it is an A-derivation $B \to I$, so it is zero. □

4.2.2. Proposition (Formally unramified is a local property)**.** *Let $A \to B$ be a ring map. The following are equivalent:*

(1) $A \to B$ is formally unramified.
(2) For all primes $\mathfrak{q} \subset B$, $A \to B_{\mathfrak{q}}$ is formally unramified.
(3) For all primes $\mathfrak{q} \subset B$, and $\mathfrak{p} = \mathfrak{q} \cap A$, $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is formally unramified.

4.2.3. Definition. Let $A \to B$ be a ring map. Say it is *unramified* if it is formally unramified and of finite presentation (following EGA). For a prime $\mathfrak{q} \subset B$, say it is *unramified at* $\mathfrak{q}$ if there exists $g \in B \backslash \mathfrak{q}$ such that $A \to B_g$ is unramified.

4.2.4. Remark. Some sources such as [1] use finite type instead of finite presentation hypotheses. In locally Noetherian cases this of course doesn't matter.

4.2.5. Definition. Suppose $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ are Noetherian local rings, and $A \to B$ is a local ring map which is essentially of finite presentation (meaning that B is a localization of a finitely presented A-algebra). We say $A \to B$ is an *unramified local ring map* if $\mathfrak{n} = \mathfrak{m}B$ and $B/\mathfrak{n}$ is a finite separable extension of $A/\mathfrak{m}$.

4.2.6. Proposition. *Let A be a Noetherian ring, and $A \to B$ a finitely presented ring map. Let $\mathfrak{q} \subset B$ be a prime and $\mathfrak{p} = \mathfrak{q} \cap A$. Then it is unramified at $\mathfrak{q}$ iff $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is an unramified local ring map.*

Proof. ($\Longrightarrow$) There exists $g \in B \backslash \mathfrak{q}$ such that $A \to B_g$ is unramified. Then $\mathfrak{q}' = \mathfrak{q}B_g$ is a prime ideal, and $(B_g)_{\mathfrak{q}'} = B_{\mathfrak{q}}$. By pullback of differentials (proposition 4.1.4), $\kappa(\mathfrak{p}) \to B_g \otimes_A \kappa(\mathfrak{p}) = (A \backslash \mathfrak{p})^{-1} B_g / \mathfrak{p}(A \backslash \mathfrak{p})^{-1} B_g$ is unramified.

($\Longleftarrow$) □

4.3. Local structure theory.

4.4. Unramified morphisms.

4.4.1. Definition. A morphism of schemes $f : Y \to X$ is *unramified* if it is locally of finite presentation and for all $y \in Y$, the local ring map $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is unramified.

5. Smooth morphisms

5.1. Smooth ring maps.

5.2. Smooth morphisms.

6. Étale morphisms

6.1. Étale ring maps.

6.1.1. Definition. A ring homomorphism $A \to B$ is *étale* if it is finitely presented, unramified, and flat.

6.1.2. Example (Étale over a field)**.** An étale k-algebra, where k is a field, is a finite product of finite separable extensions of k.

6.1.3. Example. A *standard étale map* is a map of form $A \to B = (A[x]/P)_Q$, where $P(x) \in A[x]$ is a polynomial and $Q \in A[x]/P$ such that $P'(x)$ is a unit in the localization. It is clearly flat and finitely presented, and it is unramified because $\Omega_{B/A} = (\Omega_{(A[x]/P)/A})_Q = (A[x]/(P, P'))_Q = 0$.

6.1.4. Definition. A local ring homomorphism $A \to B$ is *local étale* (in EGA IV, *étale essentiellement*) if $B \simeq C_{\mathfrak{p}}$ (over A) for some étale A-algebra C and prime ideal $\mathfrak{p}$ above the maximal ideal $\mathfrak{m} \subset A$.

6.1.5. Proposition. *Let $A \to B$ be local étale. Then B is*

1. *regular,*
2. *reduced,*
3. *Cohen-Macaulay, or*
4. *integrally closed,*

if and only if A is.

6.1.6. Remark. The same does not hold for the property of being an integral domain.

6.2. Étale morphisms.

6.2.1. Definition. A locally finitely presented morphism $f : X \to Y$ is called *étale* if one of the following equivalent conditions hold:

- f is flat and unramified.
- (functorial description) For each affine scheme $Y' \to Y$ and each closed subscheme Y'_0 of Y' defined by a nilpotent ideal sheaf, $\mathrm{Hom}_Y(Y', X) \to \mathrm{Hom}_Y(Y'_0, X)$ is a bijection.

6.2.2. Proposition. *The following facts are true about étale morphisms:*

- *Open immersions are étale;*
- *If $f : X \to Y$ and $g : Y \to Z$ are étale, then so is $g \circ f$;*
- *If $f : X \to X'$ and $g : Y \to Y'$ are étale over S, then so is $f \times_S g : X \times_S Y \to X' \times_S Y'$.*
- *If $g : Y \to Z$ and $g \circ f : X \to Z$ are étale, then so is f.*

Proof. (TODO) □

7. Henselian rings

7.1. Henselian rings.

7.1.1. Definition (for proof, see [1], chapter 1)**.** A local ring $(A, \mathfrak{m}, k)$ is *Henselian* if it satisfies the following equivalent conditions:

(1) (Finite algebra decomposes) For any finite A-algebra B, the canonical map $B \to \prod_{\mathfrak{n}} B_{\mathfrak{n}}$ is an isomorphism, where $\mathfrak{n}$ runs through all (finitely many, since B is semilocal) maximal ideals of B.

(2) (Hensel's lemma) Suppose a monic $F \in A[x]$ has image $f \in k[x]$ which factors as $f = gh$, where g, h are coprime monic polynomials in $k[x]$, then $F = GH$ for monic $G, H \in A[x]$ whose images are g, h.

(3) (Quasifinite implies finite) For any A-algebra B, if $B = C_{\mathfrak{p}}$ for some finitely generated A-algebra C and $\mathfrak{p}$ above $\mathfrak{m}$, and if $A \to B$ is quasifinite ($B/\mathfrak{m}B$ is finite over k), then B is finite over A.

(4) (Geometric meaning) Let $X = \operatorname{Spec} A$, $x \in X$ the closed point, then for any étale X-scheme Y and $y \in Y_x$ a $\kappa(x)$-point, there exists a unique section $X \to Y$ mapping $x \mapsto y$.

A Henselian ring A is *strictly Henselian* if k is separably closed.

7.1.2. Example. Here are some naturally-occuring examples of (strictly) Henselian rings:

- fields;
- any ring with a unique prime ideal;
- more generally, a local ring A is Henselian iff A_{red} is;
- complete Noetherian local rings;
- the ring of convergent power series over $\mathbb{R}$ or $\mathbb{C}$.

More examples can be obtained from Henselization (section 7.2).

7.1.3. Remark (Intuition about Henselian rings)**.** There is an analogy: local rings are to Zariski topology as strictly Henselian rings are to étale topology, as Henselian rings are to Nisnevich topology.

7.1.4. Theorem. *Let $(A, \mathfrak{m}, k)$ be a Henselian local ring. The map $B \mapsto B/\mathfrak{m}B$ gives an equivalence between the category of finite étale algebras over A and the category of finite étale algebras over k.*

7.2. Henselization. Let $(A, \mathfrak{m}, k)$ be any local ring, and fix a local homomorphism $\phi : A \to K$, where K is a field. Consider the *set* of all diagrams

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\phi"'] & B \arrow[dl] \\
K &
\end{tikzcd}$$

where $A \to B$ is local-étale (definition 6.1.4) with trivial residue field extension, and $B \to K$ is local. A map between two such diagrams is given by a local homomorphism $B_1 \to B_2$ that commutes with the rest of the diagram.

7.2.1. Proposition (EGA IV.18.6.3)**.** *The following are true:*

(1) There is at most one map between any two such diagrams;
(2) For any two objects, one can find an object which both objects map to.

Consequently, this poset actually forms a filtered category. So we get a filtered colimit $\widetilde{A} = \varinjlim B$, with local homomorphisms $A \to \widetilde{A}$ and $\widetilde{A} \to k$.

7.2.2. Proposition. *The ring $\widetilde{A}$ is Henselian, and is strictly Henselian if K is separably closed.*

7.2.3. Proposition. *The local ring map $A \to \widetilde{A}$ is faithfully flat.*

7.2.4. Proposition. *The ring $\widetilde{A}$ is*

(1) regular,
(2) reduced,
(3) Cohen-Macaulay, or
(4) integrally closed,

if and only if A is.

7.2.5. Definition (Henselization)**.** When $\phi : k \to K$ is an isomorphism, $\widetilde{A} = A^h$ is called the *Henselization* of A. When K is separably closed, $\widetilde{A} = A^{sh}$ is called a *strict Henselization* of A.

7.2.6. Proposition (Properties of Henselization)**.** *The following are true:*

(1) For any Henselian ring B, the map $\mathrm{Hom}_{loc}(A^h, B) \to \mathrm{Hom}_{loc}(A, B)$ is bijective.
(2) For any strictly Henselian ring B with residue field ℓ and a fixed embedding $\ell \to K$, the map $\mathrm{Hom}_{loc}(A^{sh}, B) \to \mathrm{Hom}_{loc}(A, B)$ is bijective. Here the maps are assumed to respect their residue field embeddings into K.
(3) $\mathfrak{m}A^h$ is the maximal ideal of A^h, and the residue field map $k \to A^h/\mathfrak{m}A^h$ is an isomorphism.
(4) $\mathfrak{m}A^{sh}$ is the maximal ideal of A^{sh}, and the residue field map $k \to A^{sh}/\mathfrak{m}A^{sh}$ is a separable closure of k in K.

7.2.7. Example. Let X be a scheme, $P : \operatorname{Spec} \Omega \to X$ a geometric point. Then $\mathcal{O}_{X,P}$ is the strict Henselization of $\mathcal{O}_{X,x}$ with respect to $\kappa(x) \hookrightarrow \Omega$.

8. Abelian categories

8.1. Additive categories.

8.1.1. Definition. An *additive category* is a category $\mathscr{C}$ where:

- Finite products and coproducts exist;
- A zero object exists;
- For any objects $A, B \in \mathscr{C}$, $\mathrm{Hom}(A, B)$ has the structure of an abelian group, and composition of morphisms is bilinear.

8.1.2. Proposition. *In an additive category, $A \oplus B$ is isomorphic to $A \times B$.* □

8.1.3. Definition. A functor $F : \mathscr{C} \to \mathscr{C}'$ between additive categories is an *additive functor* if $F(u + v) = F(u) + F(v)$ for morphisms u, v.

8.1.4. Proposition. *Additive functors send the zero object to the zero object.*

Proof. An object $A \in \mathscr{C}$ in an additive category is the zero object if and only if $\mathrm{id}_A = 0_A$, and both are preserved by an additive functor. □

8.1.5. Definition (kernel, cokernel, image, coimage)**.** Given $u : A \to B$ in an additive category $\mathscr{C}$, the *kernel* $\ker(u)$, if it exists, is an equivalence class of monomorphisms $\ker : \ker(u) \to A$, such that any $C \to A \to B$ is zero iff $C \to A$ factors through $\ker(u) \to A$. It is unique if it exists.

Similarly, the *cokernel* $\mathrm{coker}(u)$ can be defined, and is a quotient object of B.

Finally, define the *image* $\mathrm{im}(u) = \ker(\mathrm{coker}(u))$, and the *coimage* $\mathrm{coim}(u) = \mathrm{coker}(\ker(u))$.

8.1.6. Proposition. *If both $\mathrm{im}(u)$ and $\mathrm{coim}(u)$ exist, then there is a natural morphism*

$$\overline{u} : \mathrm{coim}(u) \to \mathrm{im}(u),$$

such that $u : A \to B$ factors through $A \twoheadrightarrow \mathrm{coim}(u) \xrightarrow{\overline{u}} \mathrm{im}(u) \hookrightarrow B$. □

8.2. Abelian categories.

8.2.1. Definition. An *abelian category* $\mathscr{C}$ is an additive category that satisfies:

- (AB1) All kernels and cokernels exist;
- (AB2) For any $u : A \to B$, $\overline{u} : \operatorname{coim}(u) \to \operatorname{im}(u)$ is an isomorphism.

8.2.2. Proposition. *For an object $A \in \mathscr{C}$ in an abelian category, the set of subobjects of A are in bijection with the set of quotient objects of A, given by:*

$$[u : B \hookrightarrow A] \longmapsto [A \twoheadrightarrow \operatorname{coker}(u)],$$
$$[v : A \twoheadrightarrow B] \longmapsto [\ker(v) \hookrightarrow A].$$

Further, the subobjects of A form a lattice: for $A_1, A_2 \hookrightarrow A$,

$$A_1 \cup A_2 = \operatorname{im}(A_1 \oplus A_2 \to A),$$
$$A_1 \cap A_2 = \ker(A \to A/A_1 \times A/A_2),$$

and similarly do the quotient objects of A. □

8.2.3. Proposition. *A map $u : A \to B$ is mono iff* $\ker(u) = 0$*, and u is epi iff* $\operatorname{coker}(u) = 0$*.* □

8.2.4. Proposition. *In an abelian category, mono and epi together implies isomorphism.* □

8.2.5. Proposition. *The sequence $0 \to A \to B \to C$ is exact iff*

$$0 \to \operatorname{Hom}(M, A) \to \operatorname{Hom}(M, B) \to \operatorname{Hom}(M, C)$$

is exact for all M. □

8.2.6. Proposition. *Let $\mathscr{C}$ be any category, $\mathscr{C}'$ be an abelian category, then $Hom(\mathscr{C}, \mathscr{C}')$ is an abelian category (with exactness pointwise).* □

8.2.7. Theorem (Freyd-Mitchell embedding theorem)**.** *Let $\mathscr{C}$ be a small abelian category, then there exists a unital ring R (not necessarily commutative) and a fully faithful exact functor $F : \mathscr{C} \to R$*-Mod*.*

8.3. Injective objects.

8.3.1. Definition (injective objects)**.** In an abelian category $\mathscr{C}$, an object M is *injective* if the contravariant functor $A \mapsto \operatorname{Hom}(A, M)$ is exact. (It is automatically left exact; right exactness is the same as saying that for any subobject $A' \hookrightarrow A$, any morphism $A' \to M$ extends to $A \to M$.)

8.3.2. Definition (enough injectives)**.** An abelian category $\mathscr{C}$ has *denough injectives* if for each $A \in \mathscr{C}$, there exists a mono $A \hookrightarrow M$, where M is injective.

8.4. Grothendieck categories.

8.4.1. Definition. A collection of objects $\{Z_i\}_{i \in I}$ in $\mathscr{C}$ is a *family of generators* if for each $A \in \mathscr{C}$, $B \hookrightarrow A$, $B \neq A$, there exists $i \in I$ and a morphism $Z_i \to A$ that does not factor through B.

8.4.2. Definition. A *Grothendieck category* $\mathscr{C}$ is an abelian category that has a family of generators, and satisfies the following two axioms:

- (AB3) Arbitrary coproducts exist.
- (AB5) Assume AB3, and filtered colimits of short exact sequences are exact. Equivalently, for a filtered family of subobjects $A_i \hookrightarrow A$, $\varinjlim A_i = \sum A_i$.

8.4.3. Proposition. *Suppose $\mathscr{C}$ is an abelian category that satisfies (AB3). TFAE:*

(1) $\{Z_i\}$ is a family of generators;
(2) $Z = \bigcup_i Z_i$ is a generator;
(3) For each $A \in \mathscr{C}$, there exists an epi $\bigoplus Z \twoheadrightarrow A$.

8.4.4. Theorem (Grothendieck)**.** *Let $\mathscr{C}$ be a Grothendieck category, then $\mathscr{C}$ has enough injectives.*

8.4.5. Example. Ab, R-Mod, $\operatorname{Sh}(X)$, $\operatorname{QCoh}(V)$, etc.

8.4.6. Proposition. *Let $\mathscr{C}$ be any category, $\mathscr{C}'$ be an abelian category.*

(i) If $\mathscr{C}'$ satisfies (AB5), then so does $Hom(\mathscr{C}, \mathscr{C}')$.

(ii) If $\mathscr{C}'$ satisfies (AB3) and has generators, then so does $Hom(\mathscr{C},\mathscr{C}')$.

Proof. Item (i) is not hard to show pointwise. For (ii), given any object $Z \in \mathscr{C}'$ and $A \in \mathscr{C}$, define an object $Z_A \in Hom(\mathscr{C},\mathscr{C}')$ by

$$B \mapsto \coprod_{\mathrm{Hom}(A,B)} Z,$$

with the obvious morphisms. Then observe that $\mathrm{Hom}_{Hom(\mathscr{C},\mathscr{C}')}(Z_A, F) \cong \mathrm{Hom}_{\mathscr{C}'}(Z, F(A))$ naturally. From this, it is not hard to show that if Z is a generator of $\mathscr{C}'$, then the Z_A's form a family of generators for $Hom(\mathscr{C},\mathscr{C}')$. □

8.5. Derived functors.

8.5.1. Definition (∂-functors)**.** Let $\mathscr{C}$ be abelian, $\mathscr{C}'$ additive. A (covariant) ∂-functor $\mathscr{C} \to \mathscr{C}'$ is:

- a system of additive functors $T^i : \mathscr{C} \to \mathscr{C}'$ ($i \geq 0$), and
- connecting morphisms $\delta : T^i(A'') \to T^{i+1}(A')$, for every $i \geq 0$ and each short exact $0 \to A' \to A \to A'' \to 0$ in $\mathscr{C}$,

satisfying:

- Given a map of short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & A' \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & B' \arrow[r] & B \arrow[r] & B'' \arrow[r] & 0, \end{tikzcd}$$

  the diagram

$$\begin{tikzcd} T^i(A'') \arrow[r, "\delta"] \arrow[d] & T^{i+1}(A') \arrow[d] \\ T^i(B'') \arrow[r, "\delta"] & T^{i+1}(B') \end{tikzcd}$$

  commutes;
- Given an exact sequence $0 \to A' \to A \to A'' \to 0$, the sequence

$$0 \to T^0(A') \to T^0(A) \to T^0(A'') \xrightarrow{\delta} T^1(A') \to \dots$$

  is a chain complex.

When $\mathscr{C}'$ is abelian as well, the ∂-functor is called *exact* if the above chain complex is exact.

8.5.2. Definition. A *morphism* of two ∂-functors T^i, T'^i is a system of natural transformations $f^i : T^i \to T'^i$ that commute naturally with ∂.

8.5.3. Definition (universal)**.** A ∂-functor $T = (T^i) : \mathscr{C} \to \mathscr{C}'$ is *universal* if for each ∂-functor $T' = (T'^i)$ and each natural transformation $f^0 : T^0 \to T'^0$, there is a unique extension to a morphism of ∂-functors $T \to T'$.

8.5.4. Definition (effaceable)**.** An additive covariant functor $F : \mathscr{C} \to \mathscr{C}'$ is *effaceable* if for each object $A \in \mathscr{C}$, there is a monomorphism $u : A \to M$ in $\mathscr{C}$ such that $F(u) = 0$.

8.5.5. Proposition. *Let $\mathscr{C}$ be an abelian category with enough injectives, then $F : \mathscr{C} \to \mathscr{C}'$ is effaceable iff $F(M) = 0$ for all injective M.* □

8.5.6. Theorem. *Let $\mathscr{C}, \mathscr{C}'$ be abelian categories, and $T = (T^i) : \mathscr{C} \to \mathscr{C}'$ be an exact ∂-functor. Then if each T^i is effaceable for $i > 0$, then T is universal. If, in addition, $\mathscr{C}$ has enough injectives, then the converse is also true.*

8.5.7. Definition (right derived functors)**.** Let $F : \mathscr{C} \to \mathscr{C}'$ be a left exact additive covariant functor between abelian categories. Then its right derived functors R^iF ($i \geq 0$) is the (unique) universal exact ∂-functor extending F.

8.5.8. Theorem. *When $\mathscr{C}$ has enough injectives, right derived functors exist for every left exact additive covariant functor F.*

Proof. For $A \in \mathscr{C}$, consider an injective resolution

$$0 \to A \to M^0 \to M^1 \to M^2 \to \dots$$

Then $R^iF(A)$ is defined as the ith cohomology of

$$0 \to F(M^0) \to F(M^1) \to F(M^2) \to \dots.$$

This is functorial and does not depend on the particular injective resolution chosen, because any two resolutions extending the same map are chain homotopic. Also, $R^iF(M) = 0$ for $i > 0$ and M injective, because of the injective resolution $0 \to M \to M \to 0$, which shows that (R^iF) is universal.

It remains to check that this is exact. Given a short exact sequence $0 \to A' \to A \to A'' \to 0$, take injective resolutions $0 \to A' \to M'^i$ and $0 \to A'' \to M''^i$, then we can construct an injective resolution $0 \to A \to M^i$, where $M^i = M'^i \oplus M''^i$, such that $0 \to M'^i \to M^i \to M''^i \to 0$ is exact (horseshoe lemma). Applying F, each $0 \to F(M'^i) \to F(M^i) \to F(M''^i) \to 0$ is then exact as well, which gives a desired long exact sequence. □

We will see this construction in a different light in section 12.

9. More categorical constructions

9.1. Group objects.

9.2. Spectral sequences.

9.2.1. Proposition (five-term exact sequence)**.** *For a cohomological spectral sequence $E_2^{p,q} \Longrightarrow E^{p+q}$, the sequence*

$$0 \to E_2^{1,0} \to E^1 \to E_2^{0,1} \to E_2^{2,0} \to E^2$$

is exact.

9.2.2. Theorem (Grothendieck spectral sequence)**.** *Let $\mathscr{C}, \mathscr{C}'$ be abelian categories with enough injectives, and $\mathscr{C}''$ another abelian category. Let $F : \mathscr{C} \to \mathscr{C}'$, $G : \mathscr{C}' \to \mathscr{C}''$ be left exact covariant additive functors, and suppose F maps injective objects to G-acyclic objects (ones for which R^iG is zero for $i > 0$). Then for each $A \in \mathscr{C}$, there is a spectral sequence*

$$E_2^{p,q} = R^pG(R^qF(A)) \Longrightarrow E^{p+q} = R^{p+q}(G \circ F)(A),$$

and this is functorial in A.

Proof. (TODO) □

9.3. Limits and colimits.

9.3.1. Proposition. *If an abelian category satisfies (AB3), then it has arbitrary colimits, and colimit is right exact.* □

9.3.2. Proposition. *Right (resp. left) adjoints commute with limits (resp. colimits).* □

9.3.3. Definition (pseudofiltered and filtered)**.** A category $\mathscr{I}$ is *pseudofiltered* if it satisfies:

- (PS1) Each $i \to j$, $i \to j'$ can be extended to $j \to k$, $j' \to k$, such that the square commutes;
- (PS2) Each $f, g : i \to j$ can be extended to $h : j \to k$ such that $h \circ f = h \circ g$.

It is *filtered* if for any two objects j, j', there exists an object k and morphisms $j \to k$, $j' \to k$.

9.3.4. Definition. A full subcategory $\mathscr{B}$ of a category $\mathscr{A}$ is *final* if any object $A \in \mathscr{A}$ has a morphism $A \to B$, where $B \in \mathscr{B}$.

9.3.5. Proposition. *Let $F : \mathscr{I} \to \mathscr{C}$ be a functor where $\mathscr{I}$ satisfies (PS1), and $\mathscr{J}$ be a final subcategory of $\mathscr{I}$. Then the natural map*

$$\varinjlim F \to \varinjlim F|_{\mathscr{J}}$$

is an isomorphism. In particular, if $\mathscr{I}$ has a final object ∞, then $\varinjlim F \cong F(\infty)$.

9.4. Sites.

9.4.1. Definition (sites)**.** A *site* consists of:

- a category $\mathscr{C}$;
- a collection $\operatorname{cov}(\mathscr{C})$ of *coverings*, i.e. families of morphisms $\{U_i \to U\}_{i\in I}$,

satisfying:

- Given a covering $\{U_i \to U\}_{i\in I}$, and any morphism $V \to U$, the fiber products $U_i \times_U V$ exist and $\{U_i \times_U V \to V\}_{i\in I}$ is a covering as well;
- If $\{U_i \to U\}_{i\in I}$ and $\{U_{ij} \to U_i\}_{j\in J_i}$ are covering families, then so is $\{U_{ij} \to U\}_{i\in I, j\in J_i}$;
- Any isomorphism $\{V \to U\}$ is a covering.

9.4.2. Definition (morphisms of sites)**.** A morphism of sites $(\mathscr{C}, \operatorname{cov}(\mathscr{C})) \to (\mathscr{C}', \operatorname{cov}(\mathscr{C}'))$ is a functor F of categories, such that:

- For any covering $\{U_i \to U\}$ in $\operatorname{cov}(\mathscr{C})$, $\{F(U_i) \to F(U)\} \in \operatorname{cov}(\mathscr{C}')$;
- Given a covering $\{U_i \to U\}_{i\in I}$, and any morphism $V \to U$, the maps $f(U_i \times_U V) \to f(U_i) \times_{f(U)} f(V)$ are isomorphisms.

10. Sheaves on sites

10.1. Definition (sheaves on sites)**.** Let $\mathscr{D}$ be a category that admits arbitrary products. A $\mathscr{D}$-valued *presheaf* on a site $(\mathscr{C}, \operatorname{cov}(\mathscr{C}))$ is a contravariant functor $F : \mathscr{C}^{op} \to \mathscr{D}$. It is a *sheaf* if for every covering $\{U_i \to U\}$,

$$0 \to F(U) \to \prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \times_U U_j)$$

is exact. (This makes sense when $\mathscr{D} = \text{Set}, \text{Ab}, R\text{-Mod}$, etc.)

A morphism of (pre)sheaves is a natural transformation of functors.

Fix a site $T = (\mathscr{C}, \operatorname{cov}(\mathscr{C}))$. The category of abelian presheaves on T is denoted by $\mathscr{P}$, and the category of abelian sheaves on T is denoted by $\mathscr{S}$, which is a full subcategory of $\mathscr{P}$.

10.2. Definition (universal effective epi)**.** Let $\mathscr{C}$ be a category with fiber products. An epi $f : U \to V$ is an *effective epimorphism* if for any Z,

$$0 \to \operatorname{Hom}(V, Z) \to \operatorname{Hom}(U, Z) \rightrightarrows \operatorname{Hom}(U \times_V U, Z)$$

is exact. It is an *universal effective* epimorphism if any pullback is effective as well.

More generally, a *family of effective epimorphisms* is a family $\{U_i \to V\}$ such that for any Z,

$$0 \to \operatorname{Hom}(V, Z) \to \prod_i \operatorname{Hom}(U_i, Z) \rightrightarrows \prod_{i,j} \operatorname{Hom}(U_i \times_V U_j, Z)$$

is exact. It is a family of *universal effective* epimorphisms if any pullback is effective as well.

10.3. Proposition. *Let $\{U_i \to U\}, \{U_{ij} \to U_i\}$ be families of universal effective epimorphisms, then so is $\{U_{ij} \to U\}$.* □

10.4. Definition (canonical topology)**.** Let $\mathscr{C}$ be a category with fiber products. The *canonical topology* is a site whose coverings are the families of universal effective epimorphisms.

10.5. Proposition. *With the canonical topology, every representable presheaf of sets (ones of form $U \mapsto \operatorname{Hom}(U, Z)$) is a sheaf. Moreover, the canonical topology is the finest topology in which all representable presheaves of sets are sheaves.* □

10.1. Canonical topology on the category of left G-sets.

Let $\mathscr{C}$ be the category of left G-sets with G-maps as morphisms, and equip it with the canonical Grothendieck topology.

10.1.1. Proposition. *A family $\{U_i \to U\}$ is in $\operatorname{cov}(\mathscr{C})$ iff the images of U_i cover U.* □

10.1.2. Proposition. *The category of left G-sets is in equivalence with the category of sheaves of sets on $\mathscr{C}$, where the equivalence is given by*

$$S \mapsto \operatorname{Hom}(\bullet, S)$$
$$F(G) \leftarrow\!\shortmid F$$

where $F(G)$ is a left G-set by: for $x \in F(G)$, gx is defined as the image of x under the morphism $F(G) \to F(G)$ induced by the map $G \to G$, $h \mapsto hg$.

Proof. The key part is constructing isomorphisms

$$F(H) \to \operatorname{Hom}_{\mathscr{C}}(H, F(G))$$

functorial in H. Consider the covering $\{\phi_h : G_h \to H\}$, where each G_h is a copy of the G-set G, and ϕ_h maps 1_G to h. Since F is a sheaf,

$$0 \to F(H) \to \prod_{h \in H} F(G_h) \rightrightarrows \prod_{h_1, h_2 \in H} F(G_{h_1} \times_H G_{h_2})$$

is exact. It is not hard to verify that, for an element $(x_h)_h \in \prod F(G_h)$,

$$(x_h)_h \in \operatorname{im}(F(H) \to \prod F(G_h)) \Longrightarrow x_{gh} = gx_h \Longrightarrow (x_h)_h \in \ker(\prod F(G_h) \to \prod F(G_{h_1} \times_H G_{h_2})),$$

so all implications are reversible. This gives a natural isomorphism between $F(H)$ and its image in $\prod F(G_h)$, which is the set of G-maps $H \to F(G)$. □

10.1.3. Corollary. *The category of left G-modules is in equivalence with the category of sheaves of abelian groups on $\mathscr{C}$.* □

10.2. Canonical topology on the category of continuous G-sets. Let G be a profinite group.

10.2.1. Proposition. *The open normal subgroups H of G form a neighborhood basis of 1, and $G \cong \varprojlim G/H$.*

A *continuous G-set* is a G-set U whose action $G \times U \to U$ is continuous (U equipped with the discrete topology).

10.2.2. Proposition. *TFAE:*

(1) U is a continuous G-set;
(2) For every $u \in U$, $\operatorname{Stab}(u)$ is open;
(3) $U = \bigcup U^H$, where H ranges among open normal subgroups of G.

Consider the category $\mathscr{C}$ of continuous G-sets and G-maps, with the canonical topology. As before:

10.2.3. Proposition. *A family $\{U_i \to U\}$ is in $\operatorname{cov}(\mathscr{C})$ iff the images of U_i cover U.* □

10.2.4. Proposition. *The category of continuous G-sets is in equivalence with the category of sheafs of sets on $\mathscr{C}$, where the equivalence is given by*

$$U \mapsto \operatorname{Hom}(\bullet, U)$$
$$\varinjlim F(G/H) \leftarrow\!\shortmid F$$

where $\varinjlim F(G/H)$ is a continuous G-set as usual.

Proof. We will repeatedly use the argument in Proposition proposition 10.1.2. The nontrivial part is to give a natural isomorphism $F(U) \cong \operatorname{Hom}_G(U, \varinjlim F(G/H))$.

First, using the covering $\{U^H \to U\}$, we may identify $F(U) \cong \varprojlim F(U^H)$.

Next, fix an open normal subgroup H. Using the covering $\{G/H \to U^H\}$ sending 1 to each element in U^H, we may identify

$$F(U^H) \cong \operatorname{Hom}_{G/H}(U^H, F(G/H)\}.$$

Next, we wish to show that

$$(*) \qquad \operatorname{Hom}_{G/H}(U^H, F(G/H) \cong \operatorname{Hom}_G(U^H, \varinjlim_{H' \subseteq H} F(G/H')).$$

This is because, given a fixed $H' \subset H$, $\{G/H' \to G/H\}$ is a covering, so $F(G/H)$ is identified with $F(G/H')^{H/H'}$, so the map $F(G/H) \to \varinjlim F(G/H')$ identifies $F(G/H)$ with $\varinjlim F(G/H')^H$, which proves $(*)$. Putting everything together:

$$\begin{aligned} F(U) &\cong \varprojlim F(U^H) \\ &\cong \varprojlim \mathrm{Hom}_{G/H}(U^H, F(G/H)) \\ &\cong \varprojlim \mathrm{Hom}_G(U^H, \varinjlim F(G/H')) \\ &\cong \mathrm{Hom}_G(\varinjlim U^H, \varinjlim F(G/H')) \\ &\cong \mathrm{Hom}_G(U, \varinjlim F(G/H)), \end{aligned}$$

as desired. □

10.2.5. Corollary. *The category of continuous G-modules is in equivalence with the category of sheafs of abelian groups on $\mathscr{C}$.*

10.3. Functors f_p and f^p. Let $f : T \to T'$ be a functor between the underlying categories of two sites. (It does not have to be a morphism of sites, aka a *continuous functor*.) Let $\mathscr{P}, \mathscr{P}'$ be the categories of abelian presheaves on F, F'.

10.3.1. Definition. Given an abelian presheaf F' on T', we may define an abelian presheaf f^pF' on T by $U \mapsto F'(f(U))$. This is an additive, exact functor $f^p : \mathscr{P}' \to \mathscr{P}$ that commutes with colimits.

10.3.2. Proposition. *The functor f^p has a left adjoint $f_p : \mathscr{P} \to \mathscr{P}'$.*

Proof. First, we define the presheaf f_pF. Let $U' \in T'$, then consider the category $\mathscr{I}_{U'}$ of pairs (U, ϕ) where $U \in T$ and $\phi : U' \to f(U)$ is a morphism. Define

$$f_pF(U') = \varinjlim F(U)$$

where the colimit is taken across all (U, ϕ) as above. Let $\phi' : U' \to V'$ be a morphism, there is an induced functor $\mathscr{I}_{V'} \to \mathscr{I}_{U'}$, hence a morphism $f_pF(V') \to f_pF(U')$.

It remains to show that

$$\mathrm{Hom}(f_pF, G') \cong \mathrm{Hom}(F, f^pG')$$

functorially, which is routine. □

10.3.3. Corollary. *If f_p is exact, then f^p maps injectives to injectives.* □

10.3.4. Corollary. *If $F \in \mathscr{P}$ is represented by $Z \in T$, i.e. $F(U) = \mathrm{Hom}(U, Z)$, then f_pF is represented by $f(Z)$.* □

10.3.5. Example. Taking T the site with only one object and one arrow, and T' any site, let $i : T \to T'$ map the singular object to $U \in T'$. Then $\mathscr{P} = \mathrm{Ab}$, and $i^p : \mathscr{P}' \to \mathscr{P}$ maps F to $F(U)$. Conversely, given an abelian group A and $V \in T'$, $i_pA(V) = \bigoplus_{\mathrm{Hom}(V,U)}(A)$. This is exact, so we conclude that if F is an injective sheaf, then $F(V)$ is injective for all $V \in T'$.

10.4. Sheafification. Let T be a site, $\mathscr{P}$ be the category of abelian presheaves on T, and $\mathscr{S}$ be the category of abelian sheaves. Let $i : \mathscr{S} \to \mathscr{P}$ be the embedding functor.

10.4.1. Theorem. *The functor i has a left adjoint, the sheafification functor $\mathscr{P} \to \mathscr{S}$.*

Proof. Consider a functor $\dagger: \mathscr{P} \to \mathscr{P}$, sending

$$F \mapsto F^\dagger : F^\dagger(U) = \check{H}^0(U, F).$$

it is routine to verify that $F^\dagger$ is an abelian presheaf, $\dagger$ is indeed a functor, and there is a canonical morphism $F \to F^\dagger$. Now, observe that any morphism $F \to G$, where G is a sheaf, factors uniquely as $F \to F^\dagger \to G$. Uniqueness can be seen by noting that if $F \to G$ is the zero map, then so are the induced maps $H^0(\{U_i \to U\}, F) \to H^0(\{U_i \to U\}, G) = G(U)$, and we can simply pass to the colimit.

This finishes the proof of adjointness, provided that $F^\dagger$ is a sheaf. Unfortunately, this is not always true, but it is indeed true that $(F^\dagger)^\dagger =: F^\sharp$ is a sheaf, which we prove in the next proposition. Intuitively, the correct functor should replace a global section with the collection of local sections that agree *locally* on their overlaps, hence the need to sheafify in two steps. □

10.4.2. Proposition. *A presheaf F is* separated *if $F(U) \to \prod F(U_i)$ is injective for each covering $\{U_i \to U\}$. Then:*

(i) If F is any presheaf, $F^\dagger$ is separated.

(ii) If F is separated, then $F^\dagger$ is a sheaf, and $F \to F^\dagger$ is an monomorphism.

Proof. Item (i) is routine. For (ii), we first show that $F \to F^\dagger$ is a monomorphism, i.e. $F(U) = H^0(\{U \to U\}, F) \to \check{H}^0(U, F)$ is injective. In fact, it suffices to show that for any refinement of coverings $\{V_j \to U\} \to \{U_i \to U\}$, $H^0(\{U_i \to U\}, F) \to H^0(\{V_j \to U\}, F)$ is injective. Say s is in the kernel. Consider the covering $\{V_j \times_U U_i \to U\}$ and refinement maps $\{V_j \times_U U_i \to U\} \xrightarrow{pr_2} \{U_i \to U\}$, and $\{V_j \times_U U_i \to U\} \xrightarrow{pr_1} \{V_j \to U\} \to \{U_i \to U\}$. By lemma 11.1.7, the two induce the same maps in H^0, so s is mapped to 0 in $H^0(\{V_j \times_U U_i \to U\}, F)$. This map is given by the restriction of

$$\prod F(U_i) \to \prod F(V_j \times_U U_i),$$

which is injective since F is separated.

Now, we show that $F^\dagger$ is a sheaf. Suppose $s = (s_i) \in \prod_i F^\dagger(U_i)$ is in the kernel. Pick representing elements $s_i \in H^0(\{U_{ik} \to U_i\}, F)$. Then we have that the images of s_i, s_j in $H^0(U_i \times_U U_j, F)$ agree, so they agree in some common refinement of $\{U_{ik} \times_U U_j \to U_i \times_U U_j\}$ and $\{U_{jl} \times_U U_i \to U_i \times_U U_j\}$. In fact, by the injectivity proven in the above paragraph, this means that they agree in any common refinement, such as $H^0(\{U_{ik} \times_U U_{jl} \to U_i \times_U U_j\}, F) \subseteq \prod_{k,l} F(U_{ik} \times_U U_{jl})$. Now, define the element $t \in H^0(\{U_{ik} \to U\}, F) \hookrightarrow F^\dagger(U)$ by $t_i = s_i \in \prod_k F(U_{ik})$, which lies in the kernel by the above reasoning. This shows that $F^\dagger$ is a sheaf. □

10.4.3. Corollary. *An abelian presheaf F is a sheaf iff for each covering $\{U_i \to U\}$, there is a refinement $\{U'_j \to U\}$ such that*

$$0 \to F(U) \to \prod F(U'_j) \to \prod F(U'_{j_1} \times_U U'_{j_2}) \tag{$*$}$$

is exact.

Proof. The coverings which satisfy $(*)$ then forms a final subcategory of all coverings, so the colimit restricted to these coverings is the same as the colimit over all coverings. So $F \to F^\dagger$ is an isomorphism, so F is a sheaf. □

10.5. The category of abelian sheaves.

10.5.1. Theorem. *The category $\mathscr{S}$ of abelian sheaves on a site T is a Grothendieck category, and therefore has enough injectives.*

Proof. First, $\mathscr{S}$ is an additive category as a full subcategory of $\mathscr{P}$ that contains 0.

Next, we construct the kernels and cokernels of a morphism $F \to G$. The kernel $K = K^\sharp$ is constructed pointwise and can be easily verified to be a sheaf. The cokernel $C^\sharp$ is defined to be the sheafification of the presheaf cokernel C, and this satisfies the universal property by the adjunction.

The image $I^\sharp$ is defined similarly by sheafifying the presheaf image I. Since $0 \to I \to G \to C \to 0$ is exact, so is $0 \to I^\sharp \to G^\sharp \to C^\sharp$ (left exactness of $\check{H}^0$). So $I^\sharp = \ker(\operatorname{coker}(F^\sharp \to G^\sharp))$ in $\mathscr{S}$. To show that this is isomorphic to the coimage $J^\sharp$, let J be the presheaf coimage. Then $u : J \to I$ is an isomorphism. So $u^\sharp : J^\sharp \to I^\sharp$, which coincides with the natural map from coimage to image, is an isomorphism.

Next, we show that $\mathscr{S}$ satisfies (AB3). Let F_i be a family of sheaves, and let F be their pointwise, presheaf direct sum. Again by the adjunction, $F^\sharp$ is the sheaf direct sum.

Next, we show that $\mathscr{S}$ satisfies (AB5). Let $A_i \hookrightarrow B$ be a filtered family of subobjects, and we wish to show $\sum A_i = \varinjlim A_i$. Let $A = \sum A_i$ in $\mathscr{P}$, then $A^\sharp = \sum A_i$ in $\mathscr{S}$, since sheafification commutes with direct sums and images. In the AB5 category $\mathscr{P}$, there is a unique extension $A \to B$. This induces a unique extension $A^\sharp \to B$, once again by the adjunction. This shows (AB5).

Finally, we show that $\mathscr{S}$ has a set of generators. In fact, since the presheaves $Z_U \in \mathscr{P}$ generate $\mathscr{P}$, given a monomorphism of sheaves $A \hookrightarrow B$, there exists $Z_U \to B$ that does not factor through A. Then the induced $Z_U^\sharp \to B$ does not factor through A either. So $Z_U^\sharp$ is a set of generators. □

10.5.2. Proposition. *The sheafification functor $\sharp : \mathscr{P} \to \mathscr{S}$ is exact.*

Proof. As a left adjoint, it is clearly right exact. Also, $i \circ \sharp$ is left exact, thus so is $\sharp$. □

10.6. Functors f_s and f^s. Let $f : T \to T'$ be a map of sites. Define $\mathscr{P}, \mathscr{S}, \mathscr{P}', \mathscr{S}'$. Define the two functors f_s, f^s as:

$$f_s = \sharp' \circ f_p \circ i : \mathscr{S} \to \mathscr{S}',$$
$$f^s = \sharp \circ f^p \circ i' : \mathscr{S}' \to \mathscr{S}.$$

It is clear that $f^s = f^p \circ i'$.

10.6.1. Proposition. *f_s is left adjoint to f^s. If, moreover, f_s is exact, then f^s maps injectives to injectives.* □

10.6.2. Example (direct and inverse image)**.** Let T, T' be the sites of open sets of two topological spaces X, X', and let $\pi : X' \to X$ be a continuous map, which induces a map of sites $f : T \to T'$. Then f^s is called the *direct image* functor, and f_s the *inverse image* functor.

10.6.3. Example (G-sets)**.** Let T, T' be the canonical topologies on the category of left G, G'-sets. Let $\pi : G' \to G$ be a homomorphism of groups, which induces a map of sites $f : T \to T'$. Denote $\pi_* = f^s, \pi^* = f_s$. Identifying abelian sheaves with G-modules, we can write explicitly

$$\pi_*(A') = \mathrm{Hom}_{G'}(G, A')$$

as a G-module by $(ga)(h) = a(hg)$, and

$$\pi^*(A) = A$$

as a G'-module (cf. corollary 10.3.4). In the case $G' \subseteq G$, the module $\pi_*(A') = \mathrm{Hom}_{G'}(G, A')$ is called the *co-induced* G-module $\mathrm{CoInd}_{G'}^{G} A$. The adjunction then translates to half of Frobenius reciprocity.

10.6.4. Example (continuous G-sets)**.** Let G, G' be profintie groups, and T, T' be the canonical topologies on the category of smooth left G, G'-sets. Let $\pi : G' \to G$ be a smooth homomorphism of groups, which induces a map of sites $f : T \to T'$. Denote $\pi_* = f^s, \pi^* = f_s$. Identifying abelian sheaves with continuous G-modules, we can write explicitly

$$\pi_*(A') = \mathrm{Hom}_{G'}^{cts}(G, A') = \varinjlim \mathrm{Hom}_{G'}(G/H, A')$$

and

$$\pi^*(A) = A.$$

10.6.5. Proposition. *Suppose T, T' have final objects and finite fiber products, and $f : T \to T'$ preserves them. Then f_s is exact.*

Proof. It is sufficient to show f_p is left exact, i.e. given a fixed $U' \in T$, the functor $\mathscr{P} \to \mathrm{Ab}$, $F \mapsto f_p F(U')$, is left exact. Let $\mathcal{I}$ be the category of pairs (U, ϕ), where $\phi : U' \to f(U)$ is a morphism in T'. Then $f_p F(U') = \varinjlim_{(U,\phi)} F(U)$ taken over the category $\mathcal{I}^{op}$, so it suffices to show that $\mathcal{I}^{op}$ is pseudofiltered. In fact, it is filtered, and this follows from the assumptions on final objects and fiber products. □

Consequently, in all three examples above, f^s maps injective objects to injective objects.

11. Cohomology of sheaves

11.1. Čech cohomology. Let T be a site, $\mathscr{P}$ the abelian category of presheaves of abelian groups on T. It satisfies (AB5) and has generators, so it has enough injectives, so right derived functors exist for every left exact covariant additive functor $F : \mathscr{P} \to \mathrm{Ab}$. Also, exactness is verified pointwise.

11.1.1. Proposition. *All colimits exist in $\mathscr{P}$ and are constructed pointwise. Colimits are additive and right exact, and are exact if they are pseudofiltered (AB5).*

11.1.2. Definition. Let $\{U_i \to U\}$ be a covering. Define a functor

$$H^0(\{U_i \to U\}, \bullet) : \mathscr{P} \to \mathrm{Ab}$$
$$F \mapsto \ker(\prod F(U_i) \rightrightarrows \prod F(U_i \times_U U_j)).$$

Then it is left exact and additive, so we may define $R^q H^0(\{U_i \to U\}, \bullet) =: H^q(\{U_i \to U\}, \bullet)$, the *$q$-th Čech cohomology group associated to $\{U_i \to U\}$ with values in F.*

11.1.3. Theorem. *Let $C^\bullet(\{U_i \to U\}, F)$ be the Čech cochain, then its q-th cohomology group can be canonically identified with $H^q(\{U_i \to U\}, F)$.*

Proof. It is sufficient to show that the q-th cohomologies $\widetilde{H}^q(\{U_i \to U\}, F)$ of $C^\bullet(\{U_i \to U\}, F)$ form a *universal* ∂-functor extending $H^0 = \widetilde{H}^0$, which in turn follows from each $\widetilde{H}^q$ being *effaceable*, for $q \geq 1$, i.e. kills all injective objects. Let F be an injective sheaf. Let $Z_U : V \mapsto \bigcup_{\mathrm{Hom}(V,U)} \mathbb{Z}$ be the generators of $\mathscr{P}$, which satisfy $\mathrm{Hom}(Z_U, F) \cong \mathrm{Hom}(\mathbb{Z}, F(U)) \cong F(U)$. Then

$$C^q(\{U_i \to U\}, F) \cong \mathrm{Hom}(\bigoplus_{i_0,\dots,i_q} Z_{U_{i_0} \times_U \cdots \times_U U_{i_q}}, F).$$

Since F is injective, it suffices to show that the complex

$$(*) \qquad \cdots \to \bigoplus_{i,j} Z_{U_i \times_U U_j}(V) \to \bigoplus_i Z_{U_i}(V) \to 0$$

is exact, for all V. Fix an arbitrary map $\phi : V \to U$, we denote $S = \coprod_i \mathrm{Hom}_\phi(V, U_i)$, where $\mathrm{Hom}_\phi(V, U_i)$ consists of morphisms that commute with ϕ and $U_i \to U$. Then to show $(*)$ is exact, it suffices to show that

$$\cdots \to \bigoplus_{S \times S} \mathbb{Z} \to \bigoplus_S \mathbb{Z} \to 0$$

is exact. But the identity on this chain complex is null-homotopic, so its homology groups are all zero, i.e. is exact. □

11.1.4. Definition. A *refinement map* of coverings $\{U'_j \to U\}_{j \in J} \to \{U_i \to U\}_{i \in I}$ consists of a map $\varepsilon : J \to I$ of index sets, and U-morphisms $f_j : U'_j \to U_{\varepsilon(j)}$.

Each refinement map induces a map of Čech cohomology groups in the opposite direction, which is ∂-functorial. Thus we may define:

11.1.5. Definition (Čech cohomology)**.** Let U be an object, $F \in \mathscr{P}$ an abelian presheaf. Then the *q-th Čech cohomology of U with values in F* is defined as

$$\check{H}^q(U, F) = \varinjlim_{\{U_i \to U\}} H^q(\{U_i \to U\}, F).$$

11.1.6. Theorem. *The functor $F \mapsto \check{H}^0(U, F)$ is left exact and additive, and its right derived functors are $\check{H}^q(U, F)$.*

Proof. It is sufficient to show that $\varinjlim$ takes exact sequences of functors of form $H^q(\bullet, F)$ to exact sequences in Ab. To do this, we first prove the following lemma:

11.1.7. Lemma. *Let $(f, \varepsilon), (g, \eta)$ be two refinement maps $\{U'_j \to U\} \to \{U_i \to U\}$, then they induce the same maps*

$$H^q(\{U_i \to U\}, F) \to H^q(\{U'_j \to U\}, F).$$

Proof. Let $h : \prod F(U_{i_0} \times_U U_{i_1}) \to \prod F(U_j)$ be the "homotopy" map induced by maps $U_j \to U_{\varepsilon(j)} \times_U U_{\eta(j)}$. Then the maps $f^0, g^0 : \prod F(U_i) \to F(U'_j)$ satisfy $f_0 - g_0 = h \circ d$, so they induce the same map in the zeroth cohomology, so they induce the same map in all cohomologies by universality. □

Back to the theorem: the lemma tells us that instead of taking the colimit across the category of coverings with all refinement maps as morphisms, we may as well consider the poset of all coverings, ignoring the different refinement maps. This is now a filtered category: given coverings $\{U_i \to U\}, \{U'_j \to U\}$, by the axioms of a site, $\{U_i \times_U U'_j \to U\}$ is a covering as well. So taking the colimit is now exact and we are done. □

11.2. Sheaf cohomology. Let T be a site, $\mathscr{S}$ the abelian category of sheaves of abelian groups on T. It satisfies (AB5) and has generators, so it has enough injectives, so right derived functors exist for every left exact covariant additive functor $F : \mathscr{S} \to \mathrm{Ab}$. In particular, consider the section functor $\Gamma_U : \mathscr{S} \to \mathrm{Ab}$ given by $F \mapsto F(U)$, which is left exact.

11.2.1. Definition. Define the q-th *sheaf cohomology*

$$H^q(U, F) := R^q\Gamma_U(F).$$

11.2.2. Example (group cohomology)**.** Let G be a group, A a left G-module, and e the one-element left G-set. Then $\Gamma_e(\mathrm{Hom}_G(\bullet, A)) = \mathrm{Hom}_G(e, A) \cong A^G$. So

$$H^q(e, \mathrm{Hom}_G(\bullet, A)) \cong H^q(G, A)$$

is the usual group cohomology. Conversely, given any G-set X, we may write it as the disjoint union of G-orbits X_i, then $X_i \cong G/H_i$ as G-sets. Then

$$H^q(X, \mathrm{Hom}_G(\bullet, A)) \cong \prod_i H^q(G/H_i, \mathrm{Hom}_G(\bullet, A)) \cong \prod_i H^q(H_i, A).$$

11.3. Čech-to-derived functor spectral sequence. Let T be a site, $\mathscr{P}$ the category of abelian presheaves on T, and $\mathscr{S}$ the category of abelian sheaves on T. The composition functor

$$\mathscr{S} \xrightarrow{i} \mathscr{P} \xrightarrow{\check{H}^0(U,\bullet)} \mathrm{Ab}$$

is equal to Γ_U. For $F \in \mathscr{S}$, let $\mathcal{H}^q(F) := R^q i(F)$ be the derived functors of i.

11.3.1. Proposition. *For each $U \in T$, we have, canonically,*

$$\mathcal{H}^q(F)(U) = H^q(U, F).$$

Proof. Taking $q = 0$, we have $H^0(U, F) = F(U) = \mathcal{H}^0(F)(U)$, so it is sufficient to show that $H^q(\bullet, F)$ (which are easily verified to be presheaves on T) form a universal ∂-functor $\mathscr{S} \to \mathscr{P}$. But both exactness and effaceability follow from the definition. □

11.3.2. Proposition. *For each abelian sheaf F, $\mathcal{H}^q(F)^\dagger = 0$ for $q \geq 1$.*

Proof. We know $\mathcal{H}^q(F)^\dagger \to \mathcal{H}^q(F)^\sharp$ is a monomorphism, so it suffices to show that $\mathcal{H}^q(F)^\sharp = 0$ for $q \geq 1$. Apply the Grothendieck spectral sequence to the composition of functors $\mathrm{id}_{\mathscr{S}} = \sharp \circ i$. □

11.3.3. Theorem (Čech-to-derived functor spectral sequence)**.** *Let F be an abelian sheaf.*

(i) For each covering $\{U_i \to U\}$, there is a spectral sequence

$$E_2^{p,q} = H^p(\{U_i \to U\}, \mathcal{H}^q(F)) \Longrightarrow H^{p+q}(U, F);$$

(ii) For each $U \in T$, there is a spectral sequence

$$E_2^{p,q} = \check{H}^p(U, \mathcal{H}^q(F)) \Longrightarrow H^{p+q}(U, F).$$

Proof. To apply the Grothendieck spectral sequence, we have to show that injective sheaves are G-acyclic in the category of presheaves, where $G = H^0(\{U_i \to U\}, \bullet)$ or $\check{H}^0(U, \bullet)$. Because $\sharp$ is exact, i maps injectives to injectives (corollary 10.3.3), which are G-acyclic for any additive left exact functor. □

We get edge morphisms $H^p(\{U_i \to U\}, F) \to H^p(U, F)$ and $\check{H}^p(U, F) \to H^p(U, F)$.

11.3.4. Corollary. *Let $\{U_i \to U\}$ be a covering, and F an abelian sheaf such that*

$$H^q(U_{i_0} \times_U \cdots \times_U U_{i_r}, F) = 0$$

for all $q \geq 1$. Then the edge morphisms $H^p(\{U_i \to U\}, F) \to H^p(U, F)$ are isomorphisms for all $p \geq 0$.

Proof. The given data implies that $H^p(\{U_i \to U\}, \mathcal{H}^q(F)) = 0$ for all $p \geq 0, q \geq 1$, so the edge morphisms are isomorphisms. □

11.3.5. Proposition. *The edge morphism $\check{H}^p(U, F) \to H^p(U, F)$ is isomorphic for $p = 0, 1$ and injective for $p = 2$.*

Proof. Using proposition 11.3.2, the five-term exact sequence rewrites as:

$$0 \to \check{H}^1(U,F) \to H^1(U,F) \to 0 \to \check{H}^2(U,F) \to H^2(U,F)$$

which proves the proposition. □

11.4. Flasque sheaves.

11.4.1. Definition. An abelian sheaf F on a site T is *flasque* (or *flabby*) if for all $q \geq 1$ and all coverings $\{U_i \to U\}$, $H^q(\{U_i \to U\}, F) = 0$.

11.4.2. Proposition. *The following are true about flasque sheaves:*

(i) Let $0 \to F' \to F \to F'' \to 0$ be exact in $\mathscr{S}$. If F' is flasque, then it is exact in $\mathscr{P}$.
(ii) Let $0 \to F' \to F \to F'' \to 0$ be exact in $\mathscr{S}$. If F', F are flasque, then so is F''.
(iii) If $F \oplus G$ is flasque, so is F.
(iv) Injective abelian sheaves are flasque. □

11.4.3. Corollary. *For an abelian sheaf F, TFAE:*

(1) F is flasque;
(2) For all $q \geq 1$, $\mathcal{H}^q(F) = 0$.

Proof. (1) $\Longrightarrow$ (2): Let $0 \to F \to M^0 \xrightarrow{f^0} M^1 \xrightarrow{f^1} M^2 \xrightarrow{f^2} \dots$ be an injective resolution in $\mathscr{S}$, we wish to show it is exact in $\mathscr{P}$. Split it into short exact sequences:

$$0 \to F \to M^0 \to \ker(f^1) \to 0$$
$$0 \to \ker(f^1) \to M^1 \to \ker(f^2) \to 0$$
$$\dots$$

Then by induction, each of $\ker(f^i)$ are flasque, and all these short exact sequences are exact in $\mathscr{P}$ as well. Thus the long sequence is exact in $\mathscr{P}$ too.

(2) $\Longrightarrow$ (1): By corollary 11.3.4, the edge morphisms $H^q(\{U_i \to U\}, F) \to H^q(U,F)$ are isomorphisms. □

11.4.4. Corollary. *Flasque resolutions can be used to compute sheaf cohomology.*

Proof. The key is that flasque sheaves are *i-acyclic*, by the previous corollary. So suppose we have an acyclic resolution $0 \to F \to M^i$. This splits into short exact sequences $0 \to K^i \to M^i \to K^{i+1} \to 0$, where $K^i = \ker(M^i \to M^{i+1})$. Its long exact sequence reads $0 \to H^q(K^{i+1}) \to H^{q+1}(K^i) \to 0$, since M^i are acyclic. So by induction, $H^q(F) \cong H^q(K^0) \cong H^1(K^{q-1})$, which by the long exact sequence

$$0 \to K^{q-1} \to M^{q-1} \to K^q \to H^1(K^{q-1}) \to 0$$

is equal to $K^q/\operatorname{im}(M^{q-1} \to K^q) \cong H^q(0 \to M^i)$ in the category of presheaves. □

11.4.5. Example. Every abelian sheaf is flasque iff $i : \mathscr{S} \to \mathscr{P}$ is exact. This occurs, for example, when T is the site of sets with the canonical topology.

11.5. The Leray spectral sequence.

Let $f : T \to T'$ be a map of sites, then $f^s : \mathscr{S}' \to \mathscr{S}$ is left exact, so right derived functors $R^q f^s$ exist.

11.5.1. Proposition. *The following diagram commutes:*

$$\begin{tikzcd}
\mathscr{S}' \arrow[r, "R^q f^s"] \arrow[d, "\mathcal{H}^q"] & \mathscr{S} \\
\mathscr{P}' \arrow[r, "f^p"] & \mathscr{P}. \arrow[u, "\sharp"']
\end{tikzcd}$$

In other words, given an abelian sheaf F' on T', $R^q f^s F'$ is the sheafification of the presheaf $U \mapsto H^q(f(U), F')$ on T.

Proof. Applying the Grothendieck spectral sequence to $f^s = (\sharp \circ f^p) \circ (i')$, we have a spectral sequence

$$E_2^{p,q} = R^p(\sharp \circ f^p)(\mathcal{H}^q(F')) \Longrightarrow R^{p+q} f^s F'.$$

For $p > 0$, $E_2^{p,q} = 0$ since $\sharp \circ f^p$ is exact. So $(f^p \mathcal{H}^q(F'))^\sharp = E_2^{0,q} = R^q f^s F'$. □

11.5.2. Proposition. *The functor f^s maps flasque objects in $\mathscr{S}'$ to flasque objects in $\mathscr{S}$. (Contrast this with the fact that if f_s is exact, then f^s maps injectives to injectives.)* □

11.5.3. Corollary. *Let $T'' \xrightarrow{g} T \xrightarrow{f} T'$ be maps of sites, then f^s maps flabby sheaves to g^s-acyclic sheaves.* □

Consequently, we can apply the Grothendieck spectral sequence:

11.5.4. Theorem (Leray spectral sequence)**.** *Let $T'' \xrightarrow{g} T \xrightarrow{f} T'$ be maps of sites, and F' an abelian sheaf on T'. Then there is a spectral sequence*

$$(*) \qquad E_2^{p,q} = R^p g^s (R^q f^s F') \Longrightarrow R^{p+q}(fg)^s(F').$$

In particular, taking T'' to be the site with one object $*$ and one morphism, and let g map $*$ to $U \in T$, the Leray spectral sequence reads

$$(**) \qquad E_2^{p,q} = H^p(U, R^q f^s F') \Longrightarrow H^{p+q}(f(U), F').$$

The edge morphisms read

$$E_2^{p,0} = H^p(U, f^s F') \to H^p(f(U), F')$$

$$H^q(f(U), F') \to R^q f^s(F')(U) = E_2^{0,q}$$

The latter can be interpreted as the sheafification map in proposition 11.5.1.

11.5.5. Example. Let $\pi : G' \to G$ be a homomorphism of groups, $U = \{e\}$ the one-element G-set, and identify the category of G'-modules with the category of abelian sheaves on $T_{G'}$. Then given a G'-module A', $(**)$ reads

$$E_2^{p,q} = H^p(G, R^q \pi_*(A')) \Longrightarrow H^{p+q}(G', A').$$

Here π_* is the functor as in example 10.6.3.

11.5.6. Example (Hochschild-Serre spectral sequence)**.** Let $H \trianglelefteq G$ be a normal subgroup, and $\pi : G \to G/H$ the natural homomorphism. Then for each left G-module A,

$$\pi_* A = \operatorname{Hom}_G(G/H, A) \cong A^H,$$

so $R^q \pi_*(A) = H^q(H, A)$, where we identify A with the abelian sheaf $\operatorname{Hom}_G(\bullet, A)$. Then the Leray spectral sequence in the previous example reads

$$E_2^{p,q} = H^p(G/H, H^q(H, A)) \Longrightarrow H^{p+q}(G, A).$$

The edge morphisms $H^p(G/H, A^H) \to H^p(G, A)$ are called *inflations*, and the edge morphisms $H^q(G, A) \to H^q(H, A)^{G/H}$ are called *restrictions*. The five-term exact sequence reads

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)^{G/H} \to H^2(G/H, A^H) \to H^2(G, A),$$

where the second-to-last map is also called the *transgression*.

11.5.7. Example (Shapiro's lemma)**.** Let $\pi : H \to G$ be an inclusion. Then π_* is exact, so $E_2^{p,q} = 0$ for $q \geq 1$. Consequently, the edge morphism $H^p(G, \operatorname{CoInd}_H^G(A)) \to H^p(H, A)$ is an isomorphism.

11.5.8. Example (Tate cohomology)**.** (TODO: example 3.7.11 in Tamme)

11.6. Localization. Let T be a site, $Z \in T$ an object, then there is naturally a site T/Z on the category of Z-objects. The map $i : T/Z \to T$ is then a map of sites.

11.6.1. Lemma. *The functor i^s is exact.*

Proof. We know from proposition 11.5.1 that $R^q i^s F = (i^p \mathcal{H}^q(F))^\sharp$. From proposition 11.3.2, $\mathcal{H}^q(F)^\sharp = 0$, so it suffices to show that i^p commutes with $\sharp$, which is easy to check. □

11.6.2. Corollary. *There are natural isomorphisms*

$$H^p(U \to Z, i^s F) \cong H^p(U, F)$$

given any abelian sheaf F on T, and any object $U \to Z$ in T/Z.

Proof. Applying the Leray spectral sequence, we get

$$E_2^{p,q} = H^p(U \to Z, R^q i^s F) \Longrightarrow H^{p+q}(U, F).$$

But $R^q i^s = 0$ when $q \geq 1$, so the edge morphism $H^p(U \to Z, i^s F) \to H^p(U, F)$ is isomorphic. □

11.6.3. Example. Let T_G be the canonical topology on left G-sets. Let $H \leq G$ be a subgroup, then the left cosets G/H is an object in T, and in fact the functor $T_G/(G/H) \to T_H$ given by $[A \xrightarrow{\phi} G/H] \mapsto \phi^{-1}(1_G H)$ is an equivalence of sites.

11.7. Comparison lemma.

11.7.1. Theorem (comparison lemma)**.** *Let $i : T' \to T$ be a map of sites, satisfying that:*

- *i is fully faithful (and therefore T' is equivalent to a full subcategory of T);*
- *A covering $\{U_i \to U\}$ of T, where all U_i and U are in T', is a covering in T';*
- *Each object $U \in T$ admits a covering $\{U_i \to U\}$, where $U_i \in T'$.*

Then i^s and i_s are quasi-inverses.

Proof. We will show that the unit $\eta : \mathrm{id}_{\mathscr{S}'} \to i^s \circ i_s$ and the counit $\varepsilon : i_s \circ i^s \to \mathrm{id}_{\mathscr{S}}$ are natural isomorphisms. (TODO) □

11.7.2. Corollary. *Let $i : T' \to T$ be a map of sites, satisfying that:*

- *i is fully faithful;*
- *Any covering $\{U_i \to U\}$ of $U \in T'$, where $U_i \in T$, admits a refinement $\{U'_j \to U\}$ where $U'_j \in T'$.*

Then $\eta : \mathrm{id}_{S'} \to i^s \circ i_s$ is a natural isomorphism, and i^s is exact.

Proof. The proof of exactness of i^s is similar to lemma 11.6.1, since the second condition tells us that i^p commutes with $\nmid$. □

11.7.3. Corollary. *Let $i : T' \to T$ be a map of sites, satisfying the two conditions in the previous corollary. Let $U \in T'$ and F, F' be abelian sheaves on T, T', then we have natural isomorphisms*

$$H^p(T'; U, i^s F) \to H^p(T; U, F)$$

and

$$H^p(T'; U, F') \to H^p(T; U, i_s F').$$

Proof. The former comes from the Leray spectral sequence

$$E_2^{p,q} = H^p(T'; U, R^q i^s F) \Longrightarrow H^{p+q}(T; U, F).$$

Since i^s is exact, the edge morphisms $H^p(T'; U, i^s F) \to H^p(T; U, F)$ are isomorprhisms.

The latter comes from the composite

$$H^p(T'; U, F') \to H^p(T'; U, i^s i_s F') \to H^p(T; U, i_s F')$$

where the two maps are both isomorphisms by the previous corollary. □

11.7.4. Example. Let G be a profinite group, T_G the canonical topology on continuous G-sets, and T'_G the canonical topology on *finite* continuous G-sets. Then it is easy to see that $i : T'_G \to T_G$ satisfies the three conditions in the comparison lemma theorem 11.7.1: each continuous G-set U can be covered by the orbits Gu for $u \in U$, which are finite since the stabilizer of u is open.

11.8. Noetherian topology.

11.8.1. Definition. Let T be a site. An object U is *quasicompact* if for any cover $\{U_i \to U\}_{i \in I}$, there exists a finite subset $I' \subseteq I$ such that $\{U_i \to U\}_{i \in I'}$ is still a cover.

We call T *Noetherian* if every object is quasicompact.

11.8.2. Example. Let X be a topological space, and T the site of open sets. Then X is a Noetherian space iff T is Noetherian.

Let T be a site. Then we may define a site T^f allowing only the finite coverings. Let $i : T^f \to T$ be the identity map. Clearly, i^s is fully faithful.

11.8.3. Proposition. *Let T be Noetherian. Then the following are true:*

(i) *i^s is an equivalence of categories.*

(ii) *There are δ-functorial isomorphisms $H^q(T^f; U, i^s F) \cong H^q(T; U, F)$ for any abelian sheaf F on T.*

(iii) *Flasque sheaves on T can be checked on finite covers.*

Let T be a site, and F_i a family of abelian sheaves on T indexed by some category $\mathcal{I}$. There are natural morphisms

$$(*) \qquad \varinjlim H^q(U, F_i) \to H^q(U, \varinjlim F_i)$$

which are not isomorphisms in general. However:

11.8.4. Theorem. *If T is Noetherian and $\mathcal{I}$ is pseudofiltered, then the map $(*)$ is an isomorphism.*

Proof. (TODO) □

For example, we obtain that $\varinjlim$ commutes with arbitrary direct sums.

12. Derived categories

12.1. The category of cochain complexes up to homotopy.

Let us first consider a concrete example. Let A be an abelian category, and denote by $K(A)$ the following category:

- objects: cochain complexes $(X^\bullet, d^\bullet)$;
- morphisms: maps of complexes *up to homotopy.* This means that $\mathrm{Hom}_{K(A)}(X, Y)$ is the abelian group of maps $X \to Y$ of chain complexes quotient the subgroup of maps that are null-homotopic.

This forms an *additive* category (in general not abelian).

Let $X[1]$ denote the complex given by $X[1]^n = X^{n+1}$, *with the sign of the differential flipped*; denote the functor $X \mapsto X[1]$ by T. It is an additive automorphism. Be careful that for a chain map $f : X \to Y$, the sign of $T(f)$ is not flipped; only the differentials are.

12.1.1. Definition. Let $u : X \to Y$ be a map of chain complexes. Define the *mapping cone* $C(u)$ of u by: $C^n(u) = X^{n+1} \oplus Y^n$, with differential $d(x^n, y^{n-1}) = (-dx^n, u(x^n) + d(y^{n-1}))$.

12.1.2. Definition. A *distinguished triangle* is a 6-tuple (X, Y, Z, u, v, w), where $X \xrightarrow{u} Y \xrightarrow{v} Z \xrightarrow{w} X[1]$, that is isomorphic (in $K(A)$) to one of the form $(X, Y, C(u), u, i, p)$.

Note there are obvious maps $Y \xrightarrow{i} C(u) \xrightarrow{p} X[1]$. It is not hard to check that $p : C(u) \to X[1]$ is isomorphic to the mapping cone of $i : Y \to C(u)$, and $u : X \to Y$ is isomorphic to the mapping cone of $-p[-1] : C(u)[-1] \to X$. So (X, Y, Z, u, v, w) is distinguished iff $(Y, Z, T(X), v, w, -T(u))$ is.

We also define the full subcategory of bounded complexes: $K_+(A), K_-(A), K_b(A)$ are the complexes (isomorphic to ones that are) bounded below, above, and on both sides, respectively.

12.2. Triangulated categories.

12.2.1. Definition. Let C be an additive category. Let $T : C \to C$ be an additive automorphism, called the *translation functor*. In addition, suppose there is collection of 6-tuples (X, Y, Z, u, v, w) called *triangles*, where $X \xrightarrow{u} Y \xrightarrow{v} Z \xrightarrow{w} T(X)$. Together, this data is called a *triangulated category* if the following are satisfied:

- (TR1) Every 6-tuple as above isomorphic to a triangle is a triangle itself. For every morphism $u : X \to Y$, there is a triangle of form (X, Y, Z, u, v, w). The 6-tuples $(X, X, 0, \mathrm{id}_X, 0, 0)$ are triangles.
- (TR2) The 6-tuple (X, Y, Z, u, v, w) is a triangle iff $(Y, Z, T(X), v, w, -T(u))$ is.
- (TR3) Given the solid arrows (rows represent triangles), there exists a (not necessarily unique) h making the diagram commute. (J. P. May observed that this axiom and the "if" part of (TR2) are actually redundant; but (TR3) itself is very often used.)

$$\begin{tikzcd}
X \arrow[r, "u"] \arrow[d, "f"'] & Y \arrow[r, "v"] \arrow[d, "g"'] & Z \arrow[r, "w"] \arrow[d, dashed, "h"] & T(X) \arrow[d, "T(f)"] \\
X' \arrow[r, "u'"] & Y' \arrow[r, "v'"] & Z' \arrow[r, "w'"] & T(X')
\end{tikzcd}$$

- (TR4) "Verdier's octahedral axiom": in the following diagram, suppose we are given all solid lines (collinear points represent triangles), then there exist f, g (the dotted maps) making the diagram commute, and forming a triangle together with $T(j) \circ i$. (This axiom relates the distinguished triangles formed from u, v, and $v \circ u$. Two more common ways of drawing this diagram are shown: the "braid" version and the original octahedral version.)

$$\begin{tikzcd}
&&& T(X) \arrow[dddr, equal] &&& \\
&& Z' \arrow[ur] \arrow[ddr, dashed, "f"] &&&& \\
& Y \arrow[ur, "j"] \arrow[dr, "v"] &&&&& \\
X \arrow[ur, "u"] \arrow[rr, "v\circ u"'] && Z \arrow[r] \arrow[drrr] & Y' \arrow[r] \arrow[drr, dashed, "g"] & T(X) \arrow[ddrr, "T(u)"] && \\
&&&&& X' \arrow[dr, "i"] \arrow[ddr, "T(j)\circ i"'] & \\
&&&&&& T(Y) \arrow[d, "T(j)"] \\
&&&&&& T(Z')
\end{tikzcd}$$

$$\begin{tikzcd}
X \arrow[rr, bend left, "v\circ u"] \arrow[dr, "u"'] && Z \arrow[rr, bend left] \arrow[dr] && X' \arrow[rr, bend left, "T(j)\circ i"] \arrow[dr, "i"'] && T(Z') \\
& Y \arrow[ur, "v"'] \arrow[dr, "j"'] && Y' \arrow[ur, dashed, "g"'] \arrow[dr] && T(Y) \arrow[ur, "T(j)"'] & \\
&& Z' \arrow[ur, dashed, "f"] \arrow[rr, bend right] && T(X) \arrow[ur, "T(u)"'] &&
\end{tikzcd}
\qquad
\begin{tikzcd}
&& Y' \arrow[drr, dashed, "g"] \arrow[ddll, "{[1]}"] && \\
Z' \arrow[urr, dashed, "f"] \arrow[d, "{[1]}"'] &&&& X' \arrow[llll, "T(j)\circ i"] \arrow[ddll, "i"', "{[1]}"] \\
X \arrow[rrrr, "v\circ u"] \arrow[drr, "u"'] &&&& Z \arrow[u] \arrow[uull] \\
&& Y \arrow[urr, "v"'] \arrow[uull, "j"] &&
\end{tikzcd}$$

If all but (TR4) are satisfied, C is said to be *pretriangulated*. It is a consequence of the first three axioms that for any triangle (X, Y, Z, u, v, w), the composition $v \circ u = 0$. In addition, using exercise 12.2.5 and the five lemma, it is easy to see that in (TR3), if f, g are isomorphisms, then so is h. Consequently, the triangle in (TR1) based at any $u : X \to Y$ is unique as well (but up to non-unique isomorphism).

12.2.2. Exercise. The previously mentioned category of cochain complexes, $K(A)$, is triangulated.

12.2.3. Definition. An additive functor $F : C \to C'$ between triangulated categories is a *covariant ∂-functor* if it commutes with T_C, T'_C and maps triangles to triangles. A *contravariant ∂-functor* F commutes with $T_C, T_{C'}^{-1}$ and maps triangles to triangles.

12.2.4. Definition. An additive functor $H : C \to A$ from a triangulated category to an abelian category is a (covariant) *cohomological functor* if for any triangle (X, Y, Z, u, v, w), the sequence

$$\cdots \to H(T^n X) \to H(T^n Y) \to H(T^n Z) \to H(T^{n+1} X) \to \ldots$$

is exact. Notice it suffices to require $H(X) \to H(Y) \to H(Z)$ to be exact.

12.2.5. Exercise. For any triangulated category C and object X, $\mathrm{Hom}_C(X, -)$ and $\mathrm{Hom}_C(-, X)$ are both cohomological functors. In addition, for $C = K(A)$, $H^0(-)$ is also a cohomological functor.

12.3. Localization. Let C be a category. Let S be a collection of morphisms in C, satisfying:

- (MS1) S is closed under composition, and contains all identity maps;
- (MS2) Any diagram $X \xrightarrow{s} Y \leftarrow Z$, such that $s \in S$, can be completed to

$$\begin{tikzcd}
W \arrow[r, "t"] \arrow[d] & Z \arrow[d] \\
X \arrow[r, "s"] & Y
\end{tikzcd}$$

where $t \in S$; and the same statement holds for all arrows reversed.

- (MS3) For any two morphisms $f, g : X \to Y$, there exists $s \in S$ such that $f \circ s = g \circ s$ if and only if there exists $t \in T$ such that $t \circ f = t \circ g$.

Such a collection S is called a *multiplicative system*.

12.3.1. Proposition. *There exists a category C_S, called the* localization of C with respect to S, *and a functor $Q : C \to C_S$, satisfying the following universal property:*

1. *For any $s \in S$, $Q(s)$ is an isomorphism.*
2. *Any functor $F : C \to D$, such that the images of elements in S are isomorphisms, uniquely factors through Q.*

Further, C_S is an additive category if C is.

Proof. One defines C_S as having the same objects as C, but define

$$\mathrm{Hom}_{C_S}(X, Y) = \varinjlim_{\substack{s : X' \to X \\ s \in S}} \mathrm{Hom}_C(X', Y) = \varinjlim_{\substack{t : Y \to Y' \\ t \in S}} \mathrm{Hom}_C(X, Y').$$

To see this equality, and to define the composition of morphisms (and showing it is well-defined) relies on using (MS1) through (MS3). □

Now, let C be a *triangulated* category, with translation functor T. Suppose S satisfies, in addition, that S is *compatible with the triangulation*, meaning that:

- (MS4) For $s \in S$, $T(s) \in S$.
- (MS5) In the situation of (TR3), if $f, g \in S$, then so is h.

12.3.2. Proposition. *In this situation, C_S admits a unique structure of a triangulated category such that $Q : C \to C_S$ is a ∂-functor, and it satisfies the corresponding universal property with respect to ∂-functors $F : C \to D$ mapping S to isomorphisms.*

Proof. Declare a triangle in C_S to be one isomorphic to the image of a triangle in C. It is clear that (TR1) and (TR2) hold. For an illustration of the general level of such arguments, let us verify (TR3). Let $(X, Y, Z, u, v, w), (X', Y', Z', u', v', w')$ be two triangles in C_S. Without loss of generality, they lie in the image of C. Let $f : X \to X'$, $g : Y \to Y'$ be morphisms in C_S. The key step is to find morphisms f', g', u_1, s, t in C, where $s, t \in S$, in the diagram which commutes in C

$$\begin{tikzcd}
X \arrow[r, "f'"] \arrow[d, "u"'] & X_1 \arrow[d, "u_1"'] & X' \arrow[l, "s"'] \arrow[d, "u'"'] \\
Y \arrow[r, "g'"'] & Y_1 & Y' \arrow[l, "t"]
\end{tikzcd}$$

with $f = s^{-1} \circ f'$, $g = t^{-1} \circ g$. By definition f is represented by a pair $(f' : X \to X_1,\ s : X' \to X_1)$. By (MS2) we may find Y_1' along with maps $\alpha : X_1 \to Y_1'$, $\beta : Y' \to Y_1'$ such that $\beta \in S$ and $\beta \circ u' = \alpha \circ s$. Now, $\beta \circ g : Y \to Y_1'$ is a morphism in C_S, and therefore is represented by some $(\delta : Y \to Y_1'',\ \gamma : Y_1' \to Y_1'')$ with $\gamma \in S$. The picture looks like this:

$$\begin{tikzcd}
X \arrow[r, "f'"] \arrow[d, "u"'] & X_1 \arrow[d, "\alpha"] & X' \arrow[l, "s"'] \arrow[d, "u'"] \\
Y \arrow[d, "\delta"'] & Y_1' \arrow[dl, "\gamma"] & Y' \arrow[l, "\beta"] \\
Y_1'' & &
\end{tikzcd}$$

Now, in C_S, we have $\gamma \circ \alpha \circ f' = \gamma \circ \beta \circ u' \circ f = \gamma \circ \beta \circ g \circ u = \delta \circ u$, i.e. the left pentagon commutes in C_S. Therefore, it commutes in C once we post-compose by another map $\eta : Y_1'' \to Y_1$ in S. Finally, we let $g' = \eta \circ \delta$, $u_1 = \eta \circ \gamma \circ \alpha$, and $t = \eta \circ \gamma \circ \beta$, completing the key step. Now, we may extend $u_1 : X_1 \to Y_1$ to a triangle $(X_1, Y_1, Z_1, u_1, v_1, w_1)$ in C, and by (MS5) we can extend this to the commutative diagram

$$\begin{tikzcd}
X \arrow[r, "u"] \arrow[d, "f'"'] & Y \arrow[r, "v"] \arrow[d, "g'"'] & Z \arrow[r, "w"] \arrow[d, "h'"] & T(X) \arrow[d, "T(f')"] \\
X_1 \arrow[r, "u_1"'] & Y_1 \arrow[r, "v_1"'] & Z_1 \arrow[r, "w_1"'] & T(X_1) \\
X' \arrow[r, "u'"'] \arrow[u, "s"] & Y' \arrow[r, "v'"'] \arrow[u, "t"] & Z' \arrow[r, "w'"'] \arrow[u, "r"'] & T(X') \arrow[u, "T(s)"']
\end{tikzcd}$$

where $r \in S$. Let $h = r^{-1} \circ h$, and we get a map of triangles as desired. □

12.4. The derived category. We now return to the example of $K(A)$, for an abelian category A. Let S be the collection of *quasi-isomorphisms* of chain complexes, i.e. ones that induce isomorphism on homology.

12.4.1. Proposition. *The collection S satisfies axioms* (L1) *through* (L5).

12.4.2. Definition. The *derived category $D(A)$* of A is the triangulated category $K(A)$ localized at S.

12.4.3. Example. Let $0 \to X \xrightarrow{u} Y \xrightarrow{v} Z \to 0$ be a short exact sequence of cochain complexes. In the present context, this is a triangle in $D(A)$: the map $w : Z \to X[1]$ is represented by $p : C(u) \to X[1]$ and a map $C(u) \to Z$, given by $X^{n+1} \oplus Y^n \ni (x, y) \mapsto v(y) \in Z^n$, which is a quasi-isomorphism.

We also define full subcategories $D_+(A), D_-(A), D_b(A)$ of complexes isomorphic to ones that are bounded below, above, and on both sides, respectively. By the following proposition (proof left as exercise), they can also be equivalently defined as the localization of $K_+(A), K_-(A), K_b(A)$ with repsect to quasi-isomorphisms.

12.4.4. Proposition. *Let C be a category, S a multiplicative system, D a full subcategory of C such that $S \cap D$ is a multiplicative system in D. Then, the natural map $D_{S\cap D} \to C_S$ is fully faithful, as long as one of the two following conditions hold:*

- *For any morphism $s : Y \to X$ in S, with $X \in D$, there exists a morphism $f : Z \to Y$ such that $Z \in D$ and $s \circ f \in S$;*
- *For any morphism $s : X \to Y$ in S, with $X \in D$, there exists a morphism $f : Y \to Z$ such that $Z \in D$ and $f \circ s \in S$.*

Now, we give an alternative description of $D_+(A)$.

12.4.5. Lemma. *Let I be a chain complex bounded below, consisting of injective objects. Let X be an exact (i.e. acyclic) complex. Then any map $f : X \to I$ is null-homotopic.*

12.4.6. Lemma. *Let I be a chain complex bounded below, consisting of injective objects. Let Y be another chain complex, and let $s : I \to Y$ be a quasi-isomorphism. Then it has a left homotopy inverse.*

Proof. Consider the mapping cone X of s. By the previous lemma, the map $p : X \to I[1]$ is null-homotopic. Let h be the homotopy, which splits into two sequences of maps $a : I^{n+1} \to I^n$ and $b : Y^n \to I^n$. The equality $dh + hd = p$ implies that b is a map of complexes $Y \to I$, and $b \circ s$ is homotopic to the identity. □

12.4.7. Lemma. *Suppose the abelian category A has enough injectives. Then any $X \in K_+(A)$ admits a quasi-isomorphism to a chain complex bounded below consisting of injective objects.*

Proof. Say $X^n = 0$ for $n < 0$. Let $I^n = 0$ for $n < 0$. Pick a mono $f^0 : X^0 \hookrightarrow I^0$ where I^0 is injective. Suppose we have constructed $I^0, \dots, I^{n-1}$. Pick a mono $(I^{n-1}/\operatorname{im}(I^{n-2})) \coprod_{X^{n-1}} X^n \hookrightarrow I^n$ (recall pushouts exist in any abelian category as a coequalizer), and let $d : I^{n-1} \to I^n$, $f^n : X^n \to I^n$ be the obvious maps. This satisfies the required properties, and in addition f^n are mono. □

Let I be the additive subcategory of injective objects of A. We analogously define $K_+(I)$. There is a natural functor $K_+(I) \to K_+(A) \to D_+(A)$. By lemma 12.4.6 and proposition 12.4.4, one sees that this is in fact fully faithful. Then, by lemma 12.4.7, we have:

12.4.8. Proposition. *Suppose A has enough injectives, then there is an equivalence $K_+(I) \simeq D_+(A)$.*

12.5. Derived functors, according to Verdier. Let $F : A \to B$ be an additive functor between abelian categories. It naturally extends to a functor $F : K(A) \to K(B)$. However, if F is not exact, this does not obviously extend to a functor $D(A) \to D(B)$.

Instead, using proposition 12.4.8, we may use the composition

$$\mathrm{R}F : D_+(A) \xrightarrow{\sim} K_+(I) \to K(A) \xrightarrow{F} K(B) \to D(B).$$

This is called the *derived functor* of F. It is a covariant δ-functor (definition 12.2.3).

By construction, the nth cohomology of the complex $\mathrm{R}F(M)$, where $M \in A$ is viewed as embedded in $D_+(A)$, is precisely the nth right derived functor $R^nF(M)$. The classical construction of a long exact sequence of right derived functors obtained from a short exact sequence of objects in A is then interpreted in this light using example 12.4.3.

13. Étale sheaves

13.1. The étale site.

13.1.1. Definition. The *(small) étale site* $X_{\text{ét}}$ of X is defined by:

- underlying category: étale X-schemes
- coverings: surjective families.

Denote by $\mathrm{PSh}(X_{\text{ét}})$ and $\mathrm{Sh}(X_{\text{ét}})$ the category of abelian (pre)sheaves on $X_{\text{ét}}$.

There is a map of sites $\varepsilon : X_{\text{zar}} \to X_{\text{ét}}$ from the Zariski site to the étale site. Applying the Leray spectral sequence, we get

$$E_2^{p,q} = H^p_{\text{Zar}}(X, R^q\varepsilon^s(F)) \Longrightarrow H^{p+q}_{\text{ét}}(X, F)$$

for each abelian sheaf F on $X_{\text{ét}}$.

13.2. Direct and inverse image functors. Let $f : X \to Y$ be a morphism of schemes. Then this induces a map of sites $f_{\text{ét}} : Y_{\text{ét}} \to X_{\text{ét}}$. So we may define

$$f_* = (f_{\text{ét}})^s : \widetilde{X}_{\text{ét}} \to \widetilde{Y}_{\text{ét}}$$
$$f^* = (f_{\text{ét}})_s : \widetilde{Y}_{\text{ét}} \to \widetilde{X}_{\text{ét}}$$

which are called the direct image and inverse image, respectively. More explicitly:

$$(f_*F)(Y') = F(Y' \times_Y X)$$
$$(f^*G)(X') = \varinjlim_{(Y',\phi)} G(Y')$$

where the colimit ranges through all X-morphisms $\phi : X' \to Y' \times_Y X$, or equivalently, all Y-morphisms $X' \to Y'$. In fact, f^* is exact by proposition 10.6.5. So we conclude that:

13.2.1. Proposition. *The following are true about f_* and f^*:*

(i) f^* is left adjoint to f_*;
(ii) f_* is left exact and maps injectives to injectives;
(iii) f^* is exact and commutes with colimits. □

Let $Y' \in Y_{\text{ét}}, F \in \widetilde{X}_{\text{ét}}$. The Leray spectral sequence reads:

$$E_2^{p,q} = H^p_{\text{ét}}(Y', R^qf_*(F)) \Longrightarrow H^{p+q}(Y' \times_Y X, F).$$

As in corollary 11.7.3, we obtain for $F \in \widetilde{X}_{\text{ét}}, G \in \widetilde{Y}_{\text{ét}}$, natural morphisms

$$H^p_{\text{ét}}(Y', f_*F) \to H^p_{\text{ét}}(Y' \times_Y X, F)$$

and

$$H^p_{\text{ét}}(Y', G) \to H^p_{\text{ét}}(Y' \times_Y X, f^*G)$$

obtained by composing $H^p_{\text{ét}}(Y', G) \to H^p_{\text{ét}}(Y', f_*f^*G) \to H^p(Y' \times_Y X, f^*G)$.

In general, let $f : X \to Y$, $g : Y \to Z$ be morphisms of schemes. Let $F \in \widetilde{X}_{\text{ét}}$, then we have

$$E_2^{p,q} = R^pg_*(R^qf_*(F)) \Longrightarrow R^{p+q}(gf)_*(F).$$

The edge morphisms can be easily read.

13.2.2. Definition (base-change morphism)**.** Let

$$\begin{tikzcd} X' \arrow[r, "f'"] \arrow[d, "v'"] & Y' \arrow[d, "v"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

be a commutative square of schemes. Let F be an abelian sheaf on $X_{\text{ét}}$. We consider the composition

$$\begin{aligned} R^p f_*(F) &\to R^p f_*(v'_* v'^* F) \\ &\to R^p(fv')_*(v'^* F) = R^p(vf')_*(v'^* F) \\ &\to v_*(R^p f'_* v'^* F), \end{aligned}$$

whose corresponding morphism under the adjunction is

$$v^*(R^p f_*(F)) \to R^p f'_*(v'^*(F)).$$

This is called the *base change morphism*, which is functorial in F.

13.2.3. Definition (restriction of a sheaf)**.** Let $f : X' \to X$ be étale. Then $X'_{\text{ét}}$ is naturally identified with $X_{\text{ét}}/X'$ as sites. Let $F \in \widetilde{X}_{\text{ét}}$. Define $F|_{X'} = f^* F$ as an abelian sheaf on $X'_{\text{ét}}$; this is the *restriction* of F on $X'_{\text{ét}}$. It is not hard to see that $F|_{X'}(U) = F(U)$ for $U \to X'$ étale.

13.2.4. Corollary (cf. corollary 11.6.2)**.** *There are canonical isomorphisms*

$$H^q(X_{\text{ét}}; X', F) \cong H^q(X'_{\text{ét}}; X', F/X').$$

13.3. The restricted étale site.

13.3.1. Definition. A morphism of schemes $f : X \to Y$ is *finitely presented* if it is locally finitely presented and qcqs. Define the *restricted étale site* $X_{\text{étfp}}$ as the category of finitely presented étale X-schemes, together with surjective covers.

13.3.2. Proposition. *Let X be quasicompact, then $X_{\text{étfp}}$ is a Noetherian site.*

Proof. Let $X' \to X$ be finitely presented and étale. Because X is quasicompact, so is X'. Because étale morphisms are open, if $\{X_i \to X'\}$ cover X', a finite subset cover X. □

There is an obvious map of sites $i : X_{\text{étfp}} \to X_{\text{ét}}$. The functors i^s, i_s are also denoted $\operatorname{res}, \operatorname{ext}$.

13.3.3. Proposition. *If X is quasi-separated, then* $\operatorname{res}, \operatorname{ext}$ *are quasi-inverses.*

Proof. To apply the comparison lemma, it suffices to show that for any étale X-scheme X', there exists a cover by finitely presented étale X-schemes X_i.

Let $f : X' \to X$ be the structure morphism. Let $x \in X'$ be a point, then there exists an affine open neighborhood $U = \operatorname{Spec} A$ of $f(x)$, whose preimage $f^{-1}(U)$ is covered by spectrums of finitely presented A-algebras. One of these, say $V \subseteq X'$, contains x. Then $f|_V : V \to X$ is finitely presented, because it is the composition $V \to U \subseteq X$ of a finitely presented morphism and a quasicompact (this uses X quasiseparated) open immersion, which is also finitely presented. □

13.3.4. Corollary. *Let X be qcqs, then $H^q_{\text{ét}}(X, \bullet)$ commutes with pseudofiltered colimits, e.g. direct sums.*

13.4. The case $X = \operatorname{Spec} k$. The setup is as follows. Let k be a field. Let $\overline{k}$ be the separable closure of k, so that $\overline{k}/k$ is Galois. Let $G = \operatorname{Gal}(\overline{k}/k)$. Let X' be a k-scheme, and $X'(\overline{k})$ the set of $\overline{k}$-points of X, which corresponds to pairs $(x' \in X', \phi : \kappa(x') \hookrightarrow \overline{k})$. There is a natural G-action on $X'(\overline{k})$, and for an open subgroup $H \leq G$, $X'(\overline{k})^H = X'(\overline{k}^H)$, where $\overline{k}^H/k$ is finite by infinite Galois theory. Furthermore, $X'(\overline{k})$ is a continuous G-set, since $X'(\overline{k}) = \bigcup_H X'(\overline{k}^H)$ (here $\kappa(x)/k$ is finite by nullstellensatz).

13.4.1. Theorem. *The functor $X' \mapsto X'(\overline{k})$ is an equivalence of sites* $(\operatorname{Spec} k)_{\text{ét}}$ *and T_G (with the canonical topology).*

This is not so surprising, since any étale k-algebra is the product of finitely many separable extensions of k anyways.

13.4.2. Corollary. *There is an equivalence of categories between* $(\widetilde{\operatorname{Spec} k})_{\text{ét}}$ *and the category of continuous* G*-modules, given by*

$$F \mapsto \varinjlim F(G/H) = \varinjlim F(\operatorname{Spec} k')$$

as k' *ranges among the finite (normal) subextensions of* $\overline{k}/k$*.*

The RHS is also the stalk F_P at the geometric $\overline{k}$-point $P = \operatorname{Spec} \overline{k} \to \operatorname{Spec} k$, cf. section 13.11.

13.4.3. Corollary. *Let* F *be an abelian sheaf on* $(\widetilde{\operatorname{Spec} k})_{\text{ét}}$*, then there are* ∂*-functorial isomorphisms*

$$H^q_{\text{ét}}(\operatorname{Spec} k, F) \to H^q(G, \varinjlim F(\operatorname{Spec} k'))$$

where the right side is Galois cohomology.

13.4.4. Corollary. *Let* k *be separably closed, then* $F \mapsto F(\operatorname{Spec} k)$ *is an equivalence of categories* $(\widehat{\operatorname{Spec} k})_{\text{ét}}$ *and* Ab*, hence additive and exact.*

13.5. Representable sheaves on $X_{\text{ét}}$**.** Here is an important criterion for a Zariski sheaf to be an étale sheaf.

13.5.1. Proposition. *Let* F *be a presheaf of sets on* $X_{\text{ét}}$*. Then to verify* F *is a sheaf, it suffices to verify it for the following two types of coverings:*

- $\{U'_i \to X'\}$*, where each map is an open embedding (i.e. "usual" coverings by open sets)*
- $\{Y' \to X'\}$*, a single surjective morphism of affine schemes.* □

13.5.2. Theorem. *The coverings in* $X_{\text{ét}}$ *are families of universal effective epimorphisms in the category of* X*-schemes.*

The converse is false; in other words, the étale topology is coarser than the canonical topology. However, when $X = \operatorname{Spec} k$, the two topologies agree.

Proof. The key part is to show that a surjective X-morphism of affine schemes is effective. This follows from a general result in faithfully flat descent theory. □

13.5.3. Corollary. *For each* X*-scheme* Z*, the functor* $X' \mapsto \operatorname{Hom}_X(X', Z)$ *is a sheaf of sets.*

13.5.4. Proposition. *Let* $f : Y \to X$ *be a morphism of schemes. If* Z *is an étale* X*-scheme, then*

$$f^* \operatorname{Hom}_X(\bullet, Z) \to \operatorname{Hom}_Y(\bullet, Z \times_X Y)$$

is an isomorphism.

13.5.5. Definition (group schemes)**.** A *group scheme* over a scheme X is an X-scheme G, together with either of the following equivalent data:

- a contravariant functor $Z \mapsto \operatorname{Hom}_X(Z, G)$ from schemes over X to Grp;
- a triple of morphisms $\mu : G \times_X G \to G$, $e : X \to G$, and $i : G \to G$, satisfying associativity, identity, and inverse axioms.

For a (commutative) group scheme G over X, let G_X denote the sheaf on $X_{\text{ét}}$ represented by G, which is a sheaf of (abelian) groups.

13.5.6. Example. Some examples of group schemes:

- the additive group $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[t] \times_{\mathbb{Z}} X$, and the functor sends $X' \mapsto \mathcal{O}_{X'}(X')$;
- the multiplicative group $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[t, t^{-1}] \times_{\mathbb{Z}} X$, and the functor sends $X' \mapsto \mathcal{O}_{X'}(X')^\times$;
- the n-th roots of unity $\mu_n = \operatorname{Spec} \mathbb{Z}[t]/(t^n - 1) \times_{\mathbb{Z}} X$, sending $X' \mapsto \{s \in \mathcal{O}_{X'}(X') : s^n = 1\}$.

We have the following exact sequence of abelian sheaves:

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$$

where the last map is raising to the n-th power.

13.5.7. Example. The constant sheaf $\underline{A}_X$, given an abelian group A, is defined as the sheafification of the abelian presheaf $X' \mapsto A$. Then one can verify that

$$\underline{A}_X(X') = \mathrm{Hom}_X(X', \coprod_A X) = \mathrm{Hom}_{\mathrm{Top}}(X', A).$$

When the connected components of X' are open (e.g. X' is locally Noetherian), this is the same as $\prod A$ over its connected components, but in general this is not true. In addition, it is clear that $\mathrm{Hom}(\underline{A}_X, F) \cong \mathrm{Hom}(A, F(X))$.

Consider the constant sheaf $\underline{\mathbb{Z}/(n)}_X$ on $X_{\text{ét}}$. The isomorphisms $\underline{\mathbb{Z}/(n)} \to \mu_n$ correspond to primitive roots of unities in the global section of X. Note however that even if $\underline{\mathbb{Z}/(n)} \sim \mu_n$, the defining group schemes are not necessarily isomorphic.

When n is invertible on X (equivalently, n is coprime to the characteristics of residue fields at every point), we have that μ_n and $\underline{\mathbb{Z}/(n)}$ are *locally isomorphic*, i.e. for every X', there exists a cover $\{X'_i \to X'\}$ in $X_{\text{ét}}$ where $\mu_n|_{X'_i} \cong \underline{\mathbb{Z}/(n)}|_{X'_i}$. In fact, given $X' = \operatorname{Spec} A$, consider $Y' = \operatorname{Spec} B$, $B = A[x]/(x^n - 1)$. Then $Y' \to X'$ is faithfully flat and unramified, hence an étale cover.

13.6. Étale cohomology of $(\mathbb{G}_a)_X$.

13.6.1. Proposition. *Let M be a quasicoherent sheaf of $\mathcal{O}_X$-modules on X. Then*

$$X' \mapsto \Gamma(X', M \otimes_{\mathcal{O}_X} \mathcal{O}'_X)$$

is an abelian sheaf on $X_{\text{ét}}$, denoted by $M_{\text{ét}}$. □

The functor $M \mapsto M_{\text{ét}}$, from the category of quasicoherent $\mathcal{O}_X$-modules to the category of abelian sheaves on $X_{\text{ét}}$, is additive and left exact (recall that $X' \to X$ is flat).

13.6.2. Theorem. *Let M be a quasicoherent $\mathcal{O}_X$-module. The edge morphisms*

$$H^p_{\mathrm{Zar}}(X, M) \to H^p_{\text{ét}}(X, M_{\text{ét}})$$

of the Leray spectral sequence

$$E_2^{p,q} = H^p_{\mathrm{Zar}}(X, R^q\varepsilon^s(M_{\text{ét}})) \Longrightarrow H^{p+q}_{\text{ét}}(X, M_{\text{ét}})$$

are isomorphisms.

Proof. As usual, it suffices to show that $R^q\varepsilon^s(M_{\text{ét}}) = 0$ for $q \geq 1$, where $\varepsilon : X_{\mathrm{Zar}} \to X_{\text{ét}}$.

Assume first X is affine. Let T be the full subcategory of $X_{\text{ét}}$ consisting of affine schemes. By the comparison theorem, $H^q(X_{\text{ét}}; X, M_{\text{ét}}) \cong H^q(T; X, M_{\text{ét}})$. We claim that $M_{\text{ét}}$ is flasque on T, which would imply what we wanted. Since T is Noetherian, flasque sheaves can be checked on finite covers, which can be further reduced to covers consisting of one single morphism $\{\operatorname{Spec} B \to \operatorname{Spec} A\}$. In this case, M is an A-module, so the Čech complex goes

$$0 \to M \to M \otimes_A B \to M \otimes_A B \otimes_A B \to \dots$$

which is exact since $A \to B$ is faithfully flat (the Amitsur complex).

In general, let X be any scheme. For any $X' \to X$ étale,

$$H^q(X_{\text{ét}}; X', M_{\text{ét}}) \cong H^q(X'_{\text{ét}}; X', M_{\text{ét}}|_{X'}) \cong H^q(X'_{\text{ét}}; X', (M|_{X'})_{\text{ét}}).$$

So $(R^q\varepsilon^s M_{\text{ét}})|_{X'} = R^q\varepsilon^s(M|_{X'})_{\text{ét}}$. Taking X' to be affine opens of X, we have shown that $R^q\varepsilon^s M_{\text{ét}}$ is zero when restricted to all affine opens, so it is zero. □

13.6.3. Corollary. *If X is affine, then $H^p_{\text{ét}}(X, M_{\text{ét}}) = 0$ for $p \geq 1$. In particular, taking $M = \mathcal{O}_X$ itself, we have $H^p_{\text{ét}}(X, (\mathbb{G}_a)_X) = 0$.*

13.7. The Artin-Schreier sequence. Let X be a scheme with prime characteristic p. This means the following equivalent things:

- $\operatorname{char} \Gamma(X, \mathcal{O}_X) = p$;
- $\operatorname{char} \Gamma(U, \mathcal{O}_X) = p$ for every open $U \subseteq X$;
- $\operatorname{char} \mathcal{O}_{X,x} = p$ at every point $x \in X$;
- X is an $\mathbb{F}_p$-scheme.

Consider the constant sheaf $\underline{\mathbb{Z}/(p)}$ on $X_{\text{ét}}$. The unit global section gives a morphism of sheaves

$$\underline{\mathbb{Z}/(p)} \to \mathbb{G}_a$$

which is easily verified to be injective. Let

$$F : \mathbb{G}_a \to \mathbb{G}_a$$

be the Frobenius.

13.7.1. Theorem. *The sequence*

$$0 \to \underline{\mathbb{Z}/(p)} \to \mathbb{G}_a \xrightarrow{F-\mathrm{id}} \mathbb{G}_a \to 0$$

is exact, where $F - \mathrm{id}$ *is the map* $x \mapsto x^p - x$ *on each* $\mathbb{G}_a(X') = \mathcal{O}_{X'}(X')$. *This is called the* Artin-Schreier sequence *on* X.

Proof. Exactness in the middle: suppose $s \in \mathcal{O}_{X'}(X')$ such that $s^p = s$, then $X' = V(s^p - s) = V(s(s-1)\dots(s-p+1)) = \bigsqcup V(s-i)$, so each closed subscheme $V(s-i)$ is open as well. So we conclude that s is in the image of the constant sheaf.

Surjectivity: Consider $s \in \mathbb{G}_a(X') = \mathcal{O}_{X'}(X')$. It suffices to show that there is a cover $\{X'_i \to X'\}$ in $X_{\text{ét}}$, such that each $s_i = s|_{X'_i} \in \mathcal{O}_{X'_i}(X'_i)$ is of the form $t_i^p - t_i$ for $t_i \in \mathcal{O}_{X'_i}(X'_i)$. It suffices to show this for $X' = \operatorname{Spec} A$ affine. Let $Y' = \operatorname{Spec} B$, where $B = A[t]/(t^p - t - s)$. Since B is free over A, $Y' \to X'$ is flat and surjective. It is unramified since $(t^p - t - s)' = -1$. This completes the proof. □

The Artin-Schreier sequence then gives the following long exact sequence:

$$\begin{aligned} 0 &\to H^0(X, \underline{\mathbb{Z}/(p)}) \to H^0(X, \mathcal{O}_X) \to H^0(X, \mathcal{O}_X) \\ &\to H^1(X, \underline{\mathbb{Z}/(p)}) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X) \\ &\to H^2(X, \underline{\mathbb{Z}/(p)}) \to \dots \end{aligned}$$

from which we obtain:

13.7.2. Corollary. *There is an exact sequence*

$$0 \to \frac{H^0(X, \mathcal{O}_X)}{(F - \mathrm{id})H^0(X, \mathcal{O}_X)} \to H^1(X, \underline{\mathbb{Z}/(p)}) \to H^1(X, \mathcal{O}_X)^F \to 0.$$

13.7.3. Corollary. *When* $X = \operatorname{Spec} A$ *is affine of characteristic* p,

$$H^q(X, \underline{\mathbb{Z}/(p)}) = \begin{cases} A/(F - \mathrm{id})A & \text{if } q = 1; \\ 0 & \text{if } q \geq 2. \end{cases}$$

13.7.4. Corollary (see here)**.** *Suppose* k *is separably closed of characteristic* p, *and* X *is a reduced, proper* k*-scheme. Then*

$$H^1(X, \underline{\mathbb{Z}/(p)}) \cong H^1(X, \mathcal{O}_X)^F.$$

13.8. Étale cohomology of $(\mathbb{G}_m)_X$.

13.8.1. Theorem (Hilbert's Theorem 90)**.** *There is a canonical isomorphism*

$$H^1_{\text{ét}}(X, \mathbb{G}_m) \cong \operatorname{Pic}(X),$$

where $\operatorname{Pic}(X)$ *is the Picard group of* X, *i.e.* $H^1_{\text{Zar}}(X, \mathcal{O}_X^\times)$.

Proof. Using the five-term exact sequence associated to $\varepsilon : X_{\text{Zar}} \to X_{\text{ét}}$, it suffices to show that $R^1\varepsilon^s(\mathbb{G}_m)_X = 0$. (TODO) □

We remark that by the usual Hilbert 90, $H^1_{\text{ét}}(\operatorname{Spec} k, \mathbb{G}_m) = H^1(\operatorname{Gal}(k), (k^{\text{sep}})^\times) = 0$. Another way to view this is that the above theorem tells us that $H^1_{\text{ét}}(\operatorname{Spec} k, \mathbb{G}_m) \cong \operatorname{Pic}(\operatorname{Spec} k)$, which is trivial because $\operatorname{Spec} k$ is just a point.

13.8.2. Definition (Brauer group)**.** The *Brauer group* of a field k is defined as

$$H^2_{\text{ét}}(\operatorname{Spec} k, \mathbb{G}_m) = H^2(\operatorname{Gal}(k), (k^{\text{sep}})^\times).$$

13.9. The Kummer sequence.

13.9.1. Theorem. *Let X be a scheme, and n is invertible on X. Then there is an exact sequence*

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{s \mapsto s^n} \mathbb{G}_m \to 0,$$

called the Kummer sequence *on X.*

Proof. This is essentially the same as Artin-Schreier, except that we use the observation that $\operatorname{Spec} A[t]/(t^n - s) \to \operatorname{Spec} A$ is etale for any ring A in which n is invertible. □

Denote, for an abelian group A, ${}_nA = \ker(a \mapsto na)$ and $A_n = \operatorname{coker}(a \mapsto na)$. Then we obtain from the Kummer sequence that:

13.9.2. Corollary. *There is an exact sequence*

$$0 \to H^0(X, \mathcal{O}_X^\times)_n \to H^1(X, \mu_n) \to {}_n\operatorname{Pic}(X) \to 0.$$

13.9.3. Corollary. *If $X = \operatorname{Spec} A$ for A local in which n is invertible,*

$$H^1(X, \mu_n) \cong A^\times/(A^\times)^n.$$

13.9.4. Corollary. *Suppose k is separably closed with characteristic coprime to n, and X is a reduced, proper k-scheme. Then*

$$H^1(X, \mu_n) \cong {}_n\operatorname{Pic}(X).$$

13.10. The sheaf of divisors on $X_{\text{ét}}$. Let X be a Noetherian scheme, so that it has finitely many irreducible components. Recall that $K = K(X)$, the ring of rational functions on X, is defined as the set of rational maps $X \to \mathbb{A}^1_{\mathbb{Z}}$, which has a natural ring structure. In this case, $K(X)$ is naturally isomorphic to the product $\prod \mathcal{O}_{X,\eta}$ of stalks at the generic points of each irreducible component.

Let $j : \operatorname{Spec} K \to X$ be the natural map, which induces a natural map of abelian sheaves $(\mathbb{G}_m)_X \to j_*(\mathbb{G}_m)_K$. If X has no embedded points (TODO: why necessary?), then j is dominant, then so are the $\operatorname{Spec} K \times_X X' \to X'$ (étale implies open), so we conclude that $(\mathbb{G}_m)_X \to j_*(\mathbb{G}_m)_K$ is injective. Therefore, we may define a sheaf Div_X by the short exact sequence

$$0 \to (\mathbb{G}_m)_X \to j_*(\mathbb{G}_m)_K \to \operatorname{Div}_X \to 0.$$

Intuitively, these are formal sums of codimension-1 subschemes modulo the principal ones.

Applying the long exact sequence associated to $\varepsilon : X_{\text{Zar}} \to X_{\text{ét}}$, we obtain

$$0 \to \mathcal{O}_X^\times \to \mathcal{K}_X^\times \to \varepsilon^s \operatorname{Div}_X \to R^1\varepsilon^s(\mathbb{G}_m)_X,$$

where $\mathcal{K}_X$ is the sheaf of rational functions on X: it is the sheafification of the presheaf mapping each open $U \subseteq X$ to $S^{-1}\Gamma(U, \mathcal{O}_X)$, where S is the set of elements in $\Gamma(U, \mathcal{O}_X)$ that are non-zerodivisors in all $\mathcal{O}_{X,u}$, $u \in U$. Because $R^1\varepsilon^s(\mathbb{G}_m)_X = 0$, $\varepsilon^s \operatorname{Div}_X$ is the usual sheaf of divisors in the Zariski topology.

If $f : X' \to X$ is also finite type, then X' is Noetherian and has no embedded components as well. In this case, applying f^s, we get $\operatorname{Div}_X|_{X'} = \operatorname{Div}|_{X'}$.

By EGA IV, there is a canonical morphism

$$\operatorname{Div}_X \to \bigoplus_x (i_x)_*\underline{\mathbb{Z}}$$

where x ranges among the points where the local rings have dimension 1. If X is regular, then this is an isomorphism.

Since X is qcqs, étale cohomology commutes with direct sums, so

$$H^1_{\text{ét}}(X, \operatorname{Div}_X) \cong \bigoplus_x H^1_{\text{ét}}(X, (i_x)_*\underline{\mathbb{Z}}).$$

13.10.1. Lemma. *Let X be a scheme, $x \in X$, $i_x : \operatorname{Spec} \kappa(x) \to X$, then*

$$H^1_{\text{ét}}(X, (i_x)_*\underline{A}) = 0,$$

where A is any torsion-free abelian group.

Proof. The group $H^1_{\text{ét}}(X, (i_x)_*\underline{A})$ injects into $H^1(\operatorname{Spec} \kappa(x), \underline{A}) = H^1(\operatorname{Gal}(\kappa(x)), A)$, which is the group of continuous maps $f : \operatorname{Gal}(\kappa(x)) \to A$, which there is none: suppose $f^{-1}(1_A) = H$ is an open subgroup, then $[G : H]$ is finite, which contradicts with the fact that A has no torsion. □

Consequently, $H^1_{\text{ét}}(X, \operatorname{Div}_X) = 0$ for X a regular Noetherian scheme.

13.10.2. Lemma. *Let X be a scheme, $x \in X$, $i_x : \operatorname{Spec}\kappa(x) \to X$, then*

$$R^1(i_x)_*(\mathbb{G}_m)_{\kappa(x)} = 0.$$

Proof. This is the sheafification of $H^1(X' \times_X \operatorname{Spec}\kappa(x), (\mathbb{G}_m)_{\kappa(x)})$, which is zero by Hilbert 90. □

13.10.3. Corollary. *Let X be a regular Noetherian scheme. There is an injection*

$$H^2_{\text{ét}}(X, (\mathbb{G}_m)_X) \hookrightarrow \prod \operatorname{Br}(K_i),$$

where K_i runs through the fields of rational functions on each irreducible component.

Proof. This is just the composition

$$H^2_{\text{ét}}(X, (\mathbb{G}_m)_X) \hookrightarrow H^2_{\text{ét}}(X, j_*(\mathbb{G}_m)_K) \hookrightarrow \prod H^2(\operatorname{Spec} K_i, (\mathbb{G}_m)_{K_i}) = \prod \operatorname{Br}(K_i),$$

where the first injection is because of $H^1_{\text{ét}}(X, \operatorname{Div}_X) = 0$, and the second is because of the previous lemma. □

13.10.4. Corollary. *Let X be a regular algebraic curve over a separably closed field k, then*

$$H^2(X, \mathbb{G}_m) = 0.$$

Proof. By Tsen's theorem, $\operatorname{Br}(K_i)$ all vanish, therefore so does $H^2(X, \mathbb{G}_m)$. □

13.10.5. Theorem (Tsen)**.** *Let K be a field of transcendental degree 1 over an algebraically closed field k. Then K is C^1 (meaning that any homogeneous polynomial of degree d with coefficients in K and at least $d+1$ variables has a nontrivial zero). Consequently, $H^q(\operatorname{Gal}(K), (K^{\text{sep}})^\times) = 0$ for all $q \geq 1$.*

13.11. Stalks. Let $\overline{x} : \operatorname{Spec}\Omega \to X$ be a geometric point of X, where Ω is separably closed. By corollary 13.4.2, the category of abelian sheaves on $(\operatorname{Spec}\Omega)_{\text{ét}}$ is equivalent to Ab via $\mathcal{F} \mapsto \mathcal{F}(\operatorname{Spec}\Omega)$.

13.11.1. Definition. The *stalk* of an abelian presheaf $\mathcal{F} \in \operatorname{PSh}(X_{\text{ét}})$ at the geometric point $\overline{x}$ is the colimit

$$\mathcal{F}_{\overline{x}} = \varinjlim_{U} \mathcal{F}(U),$$

as U ranges over the directed set of *étale neighborhoods* of $\overline{x}$. More precisely, we consider diagrams

$$\begin{tikzcd} & \operatorname{Spec}\Omega \arrow[dl] \arrow[d, "\overline{x}"] \\ U \arrow[r, "\text{étale}"'] & X. \end{tikzcd}$$

These form a filtered category, because for any étale neighborhoods U and V, 1) there is at most one morphism $U \to V$ if they are connected, and 2) $U \times_X V$ is also an étale neighborhood.

13.11.2. Example. Take $\mathcal{F} = \mathcal{O}_X$, then the *strict local ring* of X at $\overline{x}$ is defined as the stalk $\mathcal{O}_{X,\overline{x}}$. This is simply the strict Henselization of the local ring $\mathcal{O}_{X,x}$ where x is the underlying point of $\overline{x}$.

13.11.3. Proposition. *For any abelian presheaf $\mathcal{F}$, we have*

$$\mathcal{F}_{\overline{x}} := \overline{x}^*(\mathcal{F}^{\#})(\operatorname{Spec}\Omega).$$

In particular, $\mathcal{F}_{\overline{x}} \simeq \mathcal{F}^{\#}_{\overline{x}}$.

13.11.4. Example. Let $\mathcal{F}$ be represented by an étale group scheme G, then $\overline{x}^*\mathcal{F}$ is represented by $G \times_X \operatorname{Spec}\Omega$. So $\mathcal{F}_{\overline{x}} = \operatorname{Hom}_\Omega(\Omega, G \times_X \Omega) = \operatorname{Hom}_X(\Omega, G)$, i.e. the stalk $\mathcal{F}_{\overline{x}}$ consists of all Ω-points of G.

13.11.5. Proposition. *The following are true about stalks:*

(i) The functor $F \mapsto F_P$ from $\widetilde{X}_{\text{ét}}$ to Ab *is exact.*
(ii) If $v : P' \to P$ is a morphism of geometric points of X, then $F_{P'} \cong F_P$.
(iii) Let $f : X \to Y$ be a map of schemes, then for any abelian sheaf F on $Y_{\text{ét}}$, $(f^*F)_P \cong F_P$.

Proof. (i) Both u^* and Γ_P are exact (corollary 13.4.4). Note that the isomorphism in (ii) is not canonical. □

There is a similar definition of stalks as a colimit: consider the category of "étale neighborhoods of P", which consists of pairs (X', u'), where X' is étale over X, and $u' : P \to X'$ is an X-morphism. In fact, by definition of the presheaf functor f_p, we see that u^*F is the sheafification of the presheaf $(u_{\text{ét}})_pF$, which maps $P \mapsto \varinjlim_{(X',u')} F(X')$. Therefore, there is a canonical map

$$(*) \qquad \varinjlim_{(X',u')} F(X') \to F_P.$$

13.11.6. Proposition. *The above map* $(*)$ *is an isomorphism.*

Proof. In fact, it is clear that any abelian presheaf on $P_{\text{ét}}$ is a sheaf. □

13.11.7. Proposition. *More generally, let G be any presheaf on $X_{\text{ét}}$, then*

$$\varinjlim_{(X',u')} G(X') \to G_P^\sharp$$

is an isomorphism.

Proof. It suffices to show the following: let $f : T \to T'$ be a map of sites, and G a presheaf on T. Then $(f_pG)^\sharp \cong f_s(G^\sharp)$. This follows from adjunction. □

13.11.8. Proposition. *Mono, epi, and isomorphisms between abelian sheaves on $X_{\text{ét}}$ can be checked at the level of stalks at each point.* □

13.11.9. Corollary. *A global section $s \in F(X)$ is zero iff it is zero at each stalk.*

Proof. A global section is the same as a map of sheaves $\underline{\mathbb{Z}} \to F$. □

13.11.10. Definition (support)**.** Let $s \in F(X)$, then its *support* is

$$\operatorname{Supp}(s) = \{x \in X : s_{\overline{x}} \neq 0\}.$$

This is Zariski-closed: suppose $s_{\overline{x}} = 0$, then there is an étale X-scheme X', with $\phi : X' \to X$, such that $s|_{X'} = 0$. Then for any point $y \in \phi(X')$, which is a Zariski-open set, $s_{\overline{y}} = 0$.

The *support* of the sheaf F is *the closure of*

$$\operatorname{Supp}(F) = \{x \in X : F_{\overline{x}} \neq 0\}.$$

13.12. Godement resolution. This is a construction that came from sheaf theory on topological spaces. Let $\mathcal{F} \in \operatorname{Sh}(X_{\text{ét}})$, we will imbed $\mathcal{F}$ inside a flasque sheaf $\mathcal{G}^0(\mathcal{F})$, defined as follows.

13.13. Geometric meaning of first cohomology. The first Čech cohomology provides "gluing data" for geometric objects. If a class of objects on X satisfy étale descent, then it is classified by the first étale cohomology of X with coefficients in the sheaf of "transition functions". Here are two examples:

13.13.1. Definition. An $\mathcal{O}_{X,\text{ét}}$-module $\mathcal{L}$ is an *étale line bundle* if there exists an étale covering $\{U_i \to X\}$, such that $\mathcal{L}|_{U_i} \cong \mathcal{O}_{U_i,\text{ét}}$.

Let $\operatorname{Pic}_{\text{ét}}(X)$ be the group of isomorphism classes of étale line bundles, and let $\operatorname{Pic}(X)$ be the group of isomorphism classes of (Zariski) line bundes.

13.13.2. Proposition. *The natural map* $\operatorname{Pic}(X) \to \operatorname{Pic}_{\text{ét}}(X)$ *is an isomorphism.*

13.13.3. Corollary. *We have* $\check{H}^1(X, \mathcal{O}_{X,\text{ét}}^\times) \cong \operatorname{Pic}(X)$.

13.13.4. Definition. Let F be a finite abelian group. An etale $X' \to X$ is an *F-torsor* if F acts on X', and the map $(\coprod_F X) \times_X X' \to X' \times_X X'$, given by $(\sigma, x) \mapsto (\sigma(x), x)$, is an isomorphism.

13.13.5. Proposition. *The set of isomorphism classes of F-torsors is naturally bijective to elements of* $\check{H}^1(X, \underline{F}_X)$.

CHAPTER 10

D-Modules

1. Modules over the Weyl algebra

All rings are associative and unital, but not necessarily commutative.

1.1. Weyl algebras.

1.1.1. Definition. Let R be a commutative ring. The *Weyl algebra* $A_n(R)$ is the free associative R-algebra generated by $2n$ indeterminates $x_1, \dots, x_n, \partial_1, \dots, \partial_n$, modulo the relations $[x_i, x_j] = [\partial_i, \partial_j] = 0$, $[x_i, \partial_j] = -\delta_{i,j}$.

In this section, we study (finitely generated) modules over the non-commutative ring $A_n = A_n(k)$, where k is a fixed field of characteristic 0.

1.1.2. Remark. To give a $k[x_1, \dots, x_n]$-module M the structure of a left A_n-module is just to give a family of commuting k-linear endomorphisms $d_1, \dots, d_n$ of M, such that $d_i(x_j m) - x_j d_i(m) = \delta_{i,j} m$ for any $1 \leq i, j \leq n$. Similarly, for M to be a right A_n-module is just to have $d_i(x_j m) - x_j d_i(m) = -\delta_{i,j} m$. Thus, any left A_n-module can be made into a right A_n-module by flipping the sign of d_i, and vice versa.

1.1.3. Proposition. *$A_n(k)$ is a simple algebra, i.e. it has no nontrivial proper two-sided ideals.*

1.2. Examples. To systematically study solutions to differential equations, consider the following formalism.

Let $P_{ij} \in A_n(k)$ be differential operators, and we wish to solve the system of linear partial differential equations $\sum_{j=1}^q P_{ij} u_j = 0$, where $i = 1, \dots, p$ and u_j are a certain class of functions on which A_n acts (say, from the left). Consider the map of left A_n-modules $f : A_n^p \to A_n^q$, mapping each generator e_i $(1 \leq i \leq p)$ to $(P_{i1}, \dots, P_{iq}) \in A_n^q$. Let $M = \operatorname{coker} f$, then it is a finitely generated A_n-module. Then, for any A_n-module S (the class of functions we allow u_i to be), the k-vector space of solutions to the above system of differential equations is precisely $\operatorname{Hom}_{A_n}(M, S)$.

1.2.1. Example. Consider the 1-dimensional case, and consider $f(x) = e^x$. This solves $(\partial - 1)f = 0$, and in fact the A_1-module generated by f is isomorphic to $A_1/A_1(\partial - 1)$.

Functions naturally give rise to left A_n-modules. Dually, distributions[1] give rise to right A_n-modules.

1.2.2. Example. Consider the delta function δ_0, which acts on test functions by $f \mapsto f(0)$. Therefore it satisfies the equation $\delta_0 x_1 = \cdots = \delta_0 x_n = 0$, and in fact the right A_n-module generated by δ_0 is isomorphic to $A_n/(x_1, \dots, x_n)A_n$.

1.3. Filtered algebras and modules.

1.3.1. Definition. A *filtered algebra* over k is a k-algebra R along with a chain of k-subspaces

$$0 = F_{-1}R \subset F_0 R \subset F_1 R \subset \cdots \subset F_n R \subset \cdots \subset R,$$

such that $R = \bigcup F_i R$, $1 \in F_0 R$, and $F_i R \cdot F_j R \subset F_{i+j} R$.

1.3.2. Definition. To every filtered algebra R with filtration $F_\bullet R$, one can associate a graded algebra

$$S = \operatorname{gr} R = \bigoplus_{i \geq 0} F_i R / F_{i-1} R.$$

It is clear that if $[F_i R, F_j R] \subset F_{i+j-1} R$, then S is commutative.

[1] Here, continuous linear functionals on compactly supported smooth functions on $\mathbb{R}^n$, with the topology of uniform convergence of all derivatives on compact sets.

1.3.3. Example. On $A = A_n$ there are two natural filtrations:

- The Bernstein filtration has F_iA spanned by $x^\alpha\delta^\beta$, where $|\alpha| + |\beta| \le j$.
- The degree filtration has F_iA spanned by $x^\alpha\delta^\beta$, where $|\beta| \le j$.

Both give rise to the graded algebra $k[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$, but the Bernstein filtration makes all variables degree 1, while the degree filtration makes ∂'s degree 1 and x's degree 0.

Let us now focus on left A-modules.

1.3.4. Definition. Let M be a left A-module. Fix a filtration $F_\bullet A$. A *compatible filtration* $F_\bullet M$ is a chain of subspaces

$$0 = F_{-1}M \subset F_0M \subset F_1M \subset \cdots \subset F_nM \subset \cdots \subset M,$$

such that $M = \bigcup F_iM$, $F_iA \cdot F_jM \subset F_{i+j}M$, and F_iM are finitely generated F_0A-modules. Similarly one can form the *associated graded module* $\operatorname{gr} M = \bigoplus_{i\ge 0} F_iM/F_{i-1}M$, which is a graded module over $\operatorname{gr} A$.

1.3.5. Definition. A compatible filtration $F_\bullet M$ is *good* if any of the following equivalent conditions hold:

(1) $\operatorname{gr} M$ is finitely generated over $\operatorname{gr} A$.
(2) There exists j_0 such that for all $j \ge j_0$ and $i \ge 0$, $F_iA \cdot F_jM = F_{i+j}M$.

1.3.6. Proposition. *A left A-module M admits a good filtration iff M is finitely generated over A.*

1.3.7. Proposition. *Let $F_\bullet M, G_\bullet M$ be two compatible filtrations, where $F_\bullet M$ is good. Then there exists a positive integer c such that for any index $i \ge 0$, $F_iM \subset G_{i+c}M$.*

1.3.8. Proposition. *The Weyl algebra A is left Noetherian.*

Proof. Let M be a finitely generated A-module, and N a submodule. Since M is finitely generated, we can consider a good filtration $F_\bullet M$. This induces a compatible filtration $F_\bullet N$ by $F_iN = F_iM \cap N$. The associated graded $\operatorname{gr} N \subset \operatorname{gr} M$ is a $\operatorname{gr} A$-submodule, hence finitely generated; so the filtration is good, and N is finitely generated over A. □

1.4. Dimension. For this subsection, let M be a finitely generated left A-module. Choose a good filtration F_jM, compatible with the Bernstein filtration. We will define a notion of *dimension* of M.

Let us first recall:

1.4.1. Theorem (Hilbert syzygy theorem). *Every finitely generated graded $S = k[x_1, \ldots, x_n]$-module has a finite, graded, free resolution*[2] *of length at most n.*

In particular, we may apply this to $\operatorname{gr} M$ associated to some good filtration $F_\bullet M$. Counting the dimension (over k) of each graded piece shows that for j sufficiently large, $\dim_k \operatorname{gr}_j M = \dim_k(F_jM/F_{j-1}M)$ is a polynomial in j with rational coefficients, of degree at most $2n-1$. So $\dim_k F_jM$ is a polynomial in j with degree at most $2n$. This is the *Hilbert polynomial* $\chi(M, F_\bullet M, t)$, whose leading term is of form $\frac{m}{d!}t^d$. In fact, although χ may in general depend on $F_\bullet M$, it is not hard to see that:

1.4.2. Exercise. The numbers d and m do not depend on the good filtration $F_\bullet M$ we used.

1.4.3. Definition. Let $d = d(M)$ be the *dimension* of M, and $m = m(M)$ its *multiplicity.*

It is clear that $d \le 2n$. In fact there is also a surprising lower bound to dimension, which is certainly not true for modules over commutative rings:

1.4.4. Theorem (Bernstein's inequality). *Let $M \ne 0$, then $d(M) \ge n$.*

Proof. The key claim is that the action $F_i^BA \to \operatorname{Hom}_k(F_iM, F_{2i}M)$ is injective (B for Bernstein). This places a lower bound $\dim_k F_iM \cdot \dim_k F_{2i}M \ge \dim_k F_i^BM = \binom{i+2n}{i}$, which gives the inequality. □

1.4.5. Definition. M is *holonomic* if $M = 0$ or $d(M) = n$.

1.4.6. Proposition. *The following are true about holonomic modules:*

(1) For a short exact sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated left A-modules, M is holonomic iff both M' and M'' are.

[2] meaning that each term in the resolution is a direct sum of finitely many $S[e]$'s, and the maps are all degree 0 maps compatible with the grading.

(2) If M is holonomic, then it is both Noetherian and Artinian, and it has finite length.

1.4.7. Proposition (Dimension criterion for holonomicity)**.** *Let M be a left A-module (not necessarily finitely generated a priori). Let $F_\bullet M$ be a filtration compatible with the Bernstein filtration. Suppose there exist constants $a, b \geq 1$ such that*

$$\dim_k F_j M \leq \frac{a}{n!} j^n + b(j+1)^{n-1},$$

then M is holonomic (in particular finitely generated), with multiplicity at most a.

1.4.8. Example. The A_n-modules $k[x_1, \ldots, x_n]$ and $A_n/A_n(x_1, \ldots, x_n)$ are holonomic with multiplicity 1. The A_1-module $k[x, x^{-1}]$ is holonomic with multiplicity 2. In fact, for any nonzero polynomial $p \in k[x_1, \ldots, x_n]$, the A_n-module $M = k[x_1, \ldots, x_n, p^{-1}]$ is holonomic.

1.5. Equality of dimensions. In the last subsection, we defined the dimension of a finitely generated A-module M via the Hilbert polynomial of $\operatorname{gr} M$, using the Bernstein filtration. It is well-known that this is the same as the dimension of $\operatorname{Supp} \operatorname{gr} M$ as a module over $\operatorname{gr} A = k[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$. This latter definition generalizes to the degree filtration as well, and it will be shown that these two dimensions agree.

Consider the general framework. Let R be a filtered algebra, whose associated graded algebra S is a commutative Noetherian regular ring of dimension $2n$. For example, $R = A_n(k)$. Let M be a finitely generated left R-module. Since M is finitely generated, it has a good filtration $F_\bullet M$, hence we have an S-module $\operatorname{gr} M$. Consider

$$J(M) = \operatorname{rad}(\operatorname{Ann}_S(\operatorname{gr} M)).$$

Even though $\operatorname{Ann}_S(\operatorname{gr} M)$ may depend on the good filtration used (e.g. good filtrations of $M = A_1/A_1(x)$ corresponding to the generator 1 or ∂), we have:

1.5.1. Proposition. *The radical ideal $J(M)$ does not depend on the good filtration chosen.*

1.5.2. Example. Consider the degree filtration on A_n. Then a finitely generated A_n-module M is finitely generated over $k[x_1, \ldots, x_n]$ iff $(\partial_1, \ldots, \partial_n) \subset J(M)$.

1.5.3. Definition. The *characteristic variety* of M is the closed subscheme cut out by $J(M)$.

The main goal of this and the next subsection is to prove the following:

1.5.4. Theorem. *Let $d(M) = \dim \operatorname{Supp} \operatorname{gr} M = \dim S/J(M)$ and $j(M) = \min\{j \geq 0 : \operatorname{Ext}^j_R(M, R) \neq 0\}$. Then $d(M) + j(M) = 2n$.*

1.5.5. Corollary. *The dimension $d(M)$ for Bernstein and degree filtrations agree: they are both $2n - j(M)$.*

Note that $\operatorname{Ext}^j_R(M, R)$ can be given the structure of *right* R-modules.

The proof of theorem 1.5.4 proceeds in two main steps: (1) Prove the case where R is commutative; (2) Compare Ext groups of M and $\operatorname{gr} M$ using spectral sequences. We carry out step (1) now.

1.5.6. Lemma. *Let M be a finitely generated module over a commutative Noetherian ring R, and let N be an R-module. Let S be a multiplicative subset of R. Then for any $k \geq 0$,*

$$S^{-1}(\operatorname{Ext}^k_R(M, N)) \simeq \operatorname{Ext}^k_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

naturally.

1.5.7. Proposition. *Let S be a commutative Noetherian regular ring of dimension $2n$. Let M be a finitely generated S-module. Then $\operatorname{Ext}^j_S(M, S)$ vanishes except possibly for $2n - d(M) \leq j \leq 2n$, and $d(\operatorname{Ext}^j_S(M, S)) \leq 2n - j$ for all $j \geq 0$.*

Proof. First by lemma 1.5.6 we may localize at maximal ideals of S containing $\operatorname{Ann}(M)$, to assume that S is a regular Noetherian *local* ring of dimension $2n$. We use induction on $d = d(M)$.

When $d = 0$, $J(M) = \mathfrak{m}$ is the maximal ideal of S. Since $\mathfrak{m}$ is finitely generated, $\mathfrak{m}^\ell M = 0$ for some ℓ. By induction and the Ext long exact sequence for $0 \to \mathfrak{m}^\ell M \to \mathfrak{m}^{\ell-1} M \to \mathfrak{m}^{\ell-1} M/\mathfrak{m}^\ell M \to 0$, we may assume $\ell = 1$. In this case, M is a finite-dimensional $k = S/\mathfrak{m}$-vector space, so we can reduce to the case $M = k$. The Koszul complex for any $2n$ system of parameters for $\mathfrak{m}$ is a resolution for k, and it can be used to explicitly compute that $\operatorname{Ext}^j_S(k, S) = k$ for $j = 2n$, and zero otherwise. This proves the base case.

For the induction step, it suffices to assume there exists $f \in \mathfrak{m}$ which is a non-zero-divisor on M. By Stacks 0B52, $d(M/fM) = d(M) - 1$. The long exact sequence for $0 \to M \xrightarrow{f} M \to M/fM \to 0$ reads

$$\cdots \to \operatorname{Ext}^j(M/fM) \to \operatorname{Ext}^j(M) \xrightarrow{f} \operatorname{Ext}^j(M) \to \operatorname{Ext}^{j+1}(M/fM) \to \cdots$$

The first conclusion then follows from Nakayama lemma and the induction hypothesis. For the second conclusion, since $\operatorname{Ext}^j(M)/f\operatorname{Ext}^j(M)$ is a submodule of $\operatorname{Ext}^{j+1}(M/fM)$, we have

$$d(\operatorname{Ext}^j(M)) \leq 1 + d(\operatorname{Ext}^j(M)/f\operatorname{Ext}^j(M)) \leq 1 + d(\operatorname{Ext}^{j+1}(M/fM)) \leq 2n - j.$$

This finishes the proof. □

1.5.8. Proposition. *Under the above hypothesis, $d(M) + j(M) = 2n$.*

Proof. By the above proposition, for $j \geq j(M)$, $d(\operatorname{Ext}^j(M)) \leq 2n - j \leq 2n - j(M) \leq d(M)$, with strict inequality for $j > j(M)$. Suppose $d(\operatorname{Ext}^{j(M)}(M)) < d(M)$, so that if we let $E = \bigoplus_{j=2n-d(M)}^{2n} \operatorname{Ext}^j(M)$, then $d(E) < d(M)$. So there exists an element $f \in J(E) \backslash J(M)$, and after inverting f, $M \neq 0$ but all Ext groups $\operatorname{Ext}^j_S(M, S)$ vanish ($j \geq 0$), which is impossible. So $d(M) = d(\operatorname{Ext}^{j(M)}(M)) \leq 2n - j(M)$, in other words $j(M) \leq 2n - d(M)$. But $j(M) \geq 2n - d(M)$ by the above proposition, fo $j(M) = 2n - d(M)$. □

Therefore, in the setting of theorem 1.5.4, we have $d(\operatorname{gr} M) + j(\operatorname{gr} M) = 2n$. By definition $d(M) = d(\operatorname{gr} M)$, so our next task is to compare Ext groups of M and $\operatorname{gr} M$. To do this we need to construct a free resolution of M over R that also induces a corresponding resolution of $\operatorname{gr} M$ over S:

1.5.9. Proposition. *Let R be a filtered algebra, M a finitely generated left R-module with good filtration $F_\bullet M$, then there exists a free resolution*

$$\cdots \to L_2 \to L_1 \to L_0 \to M \to 0 \tag{1.5.10}$$

where each L_i is a finite direct sum of shifts $R[e]$ with filtration $F_j R[e] = F_{j+e} R$, and such that the induced

$$\cdots \to \operatorname{gr} L_2 \to \operatorname{gr} L_1 \to \operatorname{gr} L_0 \to \operatorname{gr} M \to 0$$

is exact.

We also need a consistent way to take duals.

1.5.11. Proposition. *Let L be a finitely generated left R-module with good filtration $F_\bullet L$. Then L^* carries a natural good filtration $F_j L^* = \{f \in L^* : f(F_i L) \subset F_{i+j} R \ \forall i \geq 0\}$. When $L \simeq R[e]$, $L^* \simeq R[-e]$.*

So, taking the dual of eq. (1.5.10), $\operatorname{Ext}^j_R(M, R)$ is the cohomology of this dual chain complex, and because $\operatorname{gr} L_j^* \simeq \operatorname{Hom}_S(\operatorname{gr} L_j, S)$, we have $\operatorname{Ext}^j_S(\operatorname{gr} M, S)$ is the cohomology of the associated graded complex of that dual complex. So the problem reduces to comparing the cohomology of a filtered chain complex and that of its associated graded complex.

1.6. Spectral sequence of a filtered complex. Let $(K^\bullet, d)$ be a cochain complex of modules over a fixed ring. Suppose each K^n is filtered by $F_j K^n$, compatible with the differential, such that $\bigcup_j F_j K^n = K^n$ and $\bigcap_j (F_j K^n + L) = L$ for every submodule $L \subset K^n$ (for example if $F_j K^n = 0$ for $j \ll 0$ then certainly this holds). There is a natural filtration

$$F_j H^n(K) = \operatorname{im}(H^n(F_j K) \to H^n(K))$$

under which it is not hard to see that

$$\operatorname{gr}_j H^n(K) = \frac{F_j K^n \cap \ker(d)}{F_{j-1} K^n \cap \ker(d) + F_j K^n \cap \operatorname{im}(d)}$$

and

$$H^n(\operatorname{gr}_j K) = \frac{F_j K^n \cap d^{-1}(F_{j-1} K^{n+1})}{F_{j-1} K^n + d(F_j K^{n-1})}.$$

Our goal is to compute the first using the second.

The idea is to approximate $F_j K^n \cap \ker(d)$ by $F_j K^n \cap d^{-1}(F_{j-\ell} K^{n+1})$ as $\ell \in \mathbb{N}$. More precisely, for $j, n \in \mathbb{Z}$ and $\ell \in \mathbb{N}$, let

$$Z^n_{\ell,j} = F_j K^n \cap d^{-1}(F_{j-\ell} K^{n+1}) \subset F_j K^n$$

and

$$B^n_{\ell,j} = Z^n_{\ell,j} \cap (F_{j-1}K^n + d(F_{j+\ell-1}K^{n-1})) = Z^n_{\ell-1,j-1} + d(Z^{n-1}_{\ell-1,j+\ell-1}),$$

and by construction the differential d induces differentials $d : Z^n_{\ell,j} \to Z^{n+1}_{\ell,j-\ell}$ and $d : B^n_{\ell,j} \to B^{n+1}_{\ell,j-\ell}$, hence they induce a degree $-\ell$ map of graded modules

$$d : E^n_\ell \to E^{n+1}_\ell, \text{ where } E^n_\ell = \bigoplus_j E^n_{\ell,j} = \bigoplus_j Z^n_{\ell,j}/B^n_{\ell,j}.$$

For example, $E^n_0 = \bigoplus_j F_jK^n/F_{j-1}K^n = \operatorname{gr} K^n$. We can also define $Z^n_{\infty,j} = F_jK^n \cap \ker d$ and $B_{\infty,j} = F_{j-1}K^n \cap \ker(d) + F_jK^n \cap \operatorname{im}(d)$ in the obvious way, so that $E^n_\infty = \operatorname{gr} H^n(K)$. So the cohomology of these complexes E^n_j interpolate between $H^n(\operatorname{gr} K)$ and $\operatorname{gr} H^n(K)$. In fact:

1.6.1. Lemma. $H^n(E^\bullet_{\ell,j}) \cong E_{\ell+1,j}$.

Bibliography

[1] Michel Raynaud. *Anneaux locaux henséliens*, volume Vol. 169 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1970.