NUMBER THEORY

ZIFAN WANG

Abstract. 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.

Contents

Date: July 1, 2023.

1. Absolute values

Definition 1.1. 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*.

Example 1.2. 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.

Definition 1.3. Two absolute values on k are *equivalent* if they induce the same topology.

Proposition 1.4. *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. □

Corollary 1.5. *If two absolute values $|\ |_1$ and $|\ |_2$ on k are inequivalent, then there exists $x \in k$ such that $|x|_1 < 1$ and $|x|_2 > 1$.*

Proposition 1.6. *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 $|x + y| \leq |y| = \max(|x|, |y|)$. □

Corollary 1.7. *In a field of positive characteristic, every absolute value is nonarchimedian.*

Theorem 1.8 (weak approximation theorem)**.** *Let k be a field, and let $|\ |_1, \ldots, |\ |_n$ be pairwise inequivalent nontrivial absolute values on k. Let $a_1, \ldots, a_n \in k$, and $\varepsilon > 0$. Then there exists $x \in k$ such that $|x - a_i|_i < \varepsilon$ for each $i = 1, \ldots, n$.*

Proof. First, we find z such that $|z|_1 > 1$ and $|z|_2, \ldots, |z|_n < 1$. The induction basis $n = 2$ follows from [1.5]. Suppose we have found z such that $|z|_1 > 1$ and $|z|_2, \ldots, |z|_n < 1$. 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 $\left|\frac{z^m}{1+z^m}\right|_2, \ldots, \left|\frac{z^m}{1+z^m}\right|_n \to 0$. 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 $a_1 \neq 0$, $a_2, \ldots, a_n = 0$. This amounts to finding y such that $|y - 1|_1, |y|_2, \ldots, |y|_n$ 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. □

Theorem 1.9 (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 $n = a_k b^k + a_{k-1}b^{k-1} + \cdots + a_0$, where $a_0, \ldots, a_k \in \{0, \ldots, b-1\}$. Let $C = \max_{1 \leq m \leq b-1} |m|/m^\alpha$. Then $|n| \leq |a_k|b^{\alpha k} + |a_{k-1}|b^{\alpha(k-1)} + \cdots + |a_0| \leq C(a_k^\alpha b^{\alpha k} + \cdots + a_0^\alpha) \leq C(a_k b^k + \cdots + a_0)^\alpha = Cn^\alpha$. 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 [1.6], $|\ |$ 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 $|\ |_p^e$. □

Theorem 1.10 (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) □

2. Valuations

Definition 2.1. 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 ∞.

Definition 2.2. 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. □

Proposition 2.3. *Let A be a valuation ring of $K = \mathrm{Frac}(A)$. 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. □

Proposition 2.4. *Let A be a subring of a field K. Then its integral closure in K is the intersection of all valuation rings of K containing A.*

Proof. Atiyah–MacDonald, Corollary 5.22. □

Proposition 2.5. *Let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation, and let A be its valuation ring. Suppose $x_1, \dots, x_n \in K$ and $v(x_1) < v(x_i)$ for all $i \geq 2$. Then $v(x_1 + \cdots + x_n) = v(x_1)$.*

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

3. Discrete valuation rings

Definition 3.1. 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 [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. □

Proposition 3.2. *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 $U_0/U_1 \cong k^\times$. □

Proposition 3.3. *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.

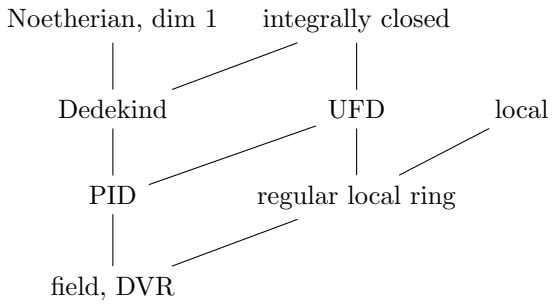
Proof. (i) follows from the previous proposition.

(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 $u^m = v_n$. □

Example 3.4. 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.

Remark 3.5. 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 $\implies$ Dedekind;
- Dedekind + UFD $\implies$ PID;
- Dedekind + local $\implies$ field or DVR.

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

Definition 3.6. 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.

Example 3.7. 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 $t = t^3/t^2 \in \mathrm{Frac}(A)$ is integral over A but not in A.

4. Integral extensions

Proposition 4.1. *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.

Proposition 4.2. *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. $\square$

Example 4.3 (Integral closure resolves codimension-1 singularities)**.** Let $A = k[x, y]/(y^2 - x^3)$. We saw in the previous section 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 $y^2 - x^3 = 0$.

5. Localization

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

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

Proposition 5.1. $\dim A = \sup\{\dim A_{\mathfrak{p}} : \mathfrak{p} \in \operatorname{Spec} A\}$. *(easy)*

Proposition 5.2. *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.

6. Dedekind domains

Definition 6.1. Let A be an integral domain, $K = \operatorname{Frac}(A)$. 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 $\{x \in K : xI \subset A\}$.

Definition 6.2. 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) $\implies$ (ii): If $\mathfrak{p} \neq 0$, then $A_{\mathfrak{p}}$ is a DVR. If $\mathfrak{p} = 0$ then $A_{\mathfrak{p}} = \operatorname{Frac}(A)$ 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) $\implies$ (i): easy. □

Example 6.3. 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* $\operatorname{Div}(A)$ of A. The set of principal fractional ideals forms a subgroup, and the quotient is called the *class group* $\operatorname{Cl}(A)$.

Invertibility is a local property:

Proposition 6.4. *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.

Corollary 6.5. *In a Dedekind domain A, every nonzero fractional ideal is invertible.*

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

Proposition 6.6. *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 $v_{\mathfrak{p}}(I) = n$.

Proposition 6.7. *(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 $v_{\mathfrak{p}}(I) = \min v_{\mathfrak{p}}(x_i)$.*

Corollary 6.8. *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 $r, s \in A$. □

Corollary 6.9. *For any fractional ideal I of A, there only exist finitely many $\mathfrak{p} \leq 0$ such that $v_{\mathfrak{p}}(I) \neq 0$.*

Theorem 6.10. *There is an isomorphism of abelian groups:*

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

Proposition 6.11. *Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, $J = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$. Then*

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

Theorem 6.12. *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) $\implies$ (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
$K = \operatorname{Frac}(A)$	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

Theorem 6.13 (Strong approximation theorem)**.** *Let A be a Dedekind domain, $K = \operatorname{Frac}(A)$. 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 $v_{\mathfrak{p}_i}(x) = f_i$.

Corollary 6.14. *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 $x \in K = \operatorname{Frac}(A)$ such that $v_{\mathfrak{p}_i}(x) = e_i$, so in fact $I = (x)$. □

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.

Lemma 7.1. *Let $\alpha \in \overline{K}$, $L = K(\alpha)$. Then $[L : K] \geq |\operatorname{Hom}_K(L, \overline{K})|$ 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 $[K(\beta) : K] = \frac{[K(\alpha):K]}{[K(\alpha):K(\beta)]} = \frac{\operatorname{Hom}_K(K(\alpha), \overline{K})}{\operatorname{Hom}_{K(\beta)}(K(\alpha), \overline{K})} = \operatorname{Hom}_K(K(\beta), \overline{K})$, which shows that β is separable over K as well. Therefore L/K is separable. □

Proposition 7.2. *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;*
- *$[L : K] = |\operatorname{Hom}_K(L, \overline{K})|$.*

Corollary 7.3. *Let M/L, L/K be finite separable extensions, then M/K is separable as well.*

Lemma 7.4. *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 $F = K$.

Theorem 7.5 (Primitive element theorem)**.** *Let L/K be a finite separable extension. Then $L = K(\alpha)$ for some element $\alpha \in L$.*

Theorem 7.6 (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.*

Theorem 7.7 (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.*

Proposition 7.8. *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.

Definition 7.9. 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.

Definition 7.10. A field K is called *separably closed* if its only separable extension is K itself.

8. Étale algebras

Definition 8.1. 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.

Proposition 8.2. *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:

Proposition 8.3. *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'. □

Proposition 8.4. *Let L/K be an étale algebra, Ω a separably closed field containing K. Then*

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

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

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

□

9. Norm and trace

Definition 9.1. 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

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

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

Proposition 9.2. *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*

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

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

Theorem 9.3. *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 8.4 and 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. □

Proposition 9.4 (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*

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

Theorem 9.5. *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*

$$\mathrm{N}_{C/A}(c) = \mathrm{N}_{B/A}(\mathrm{N}_{C/B}(c)),$$

$$\mathrm{Tr}_{C/A}(c) = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(c)).$$

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

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 $e_1, \ldots, e_n$ of V allows the definition of the *discriminant*

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

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 $e_1, \ldots, e_n$ of V, there is a *dual basis* $f_1, \ldots, f_n$ 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 $\langle e_i, e_j \rangle = \delta_{ij}$.

11. Dedekind extensions

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

Proposition 11.1. *For any element $\ell \in L$, there exists $s \in A$ such that $s\ell \in B$.*

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

Proposition 11.2. *If $b \in B$, then $\operatorname{Tr}_{L/K}(b) \in A$.*

We define the *trace pairing*:

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

Proposition 11.3. *The trace pairing is nondegenerate.*

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

$$\det(\operatorname{Tr}(\beta_i \beta_j)) = \det\left(\sum_{\sigma_k} \sigma_k(\beta_i)\sigma_k(\beta_j)\right) = \det(\sigma_k(\beta_i)) \det(\sigma_k(\beta_j)) = \det(\sigma_k(\beta_i))^2.$$

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* $M^* = \{x \in L : \operatorname{Tr}(xm) \in A \ \forall m \in M\}$. This is order-reversing.

Proposition 11.4. *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 $u_1, \ldots, u_n$ 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, $\operatorname{Tr}(v_i u_j) = \delta_{ij}$. So $B \subseteq B^* \subseteq M^*$, and B is finitely generated (since A is Noetherian). □

Theorem 11.5. *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. □

Corollary 11.6. *$\mathcal{O}_K$ is Dedekind.*

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

Theorem 11.7 (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.*

Corollary 11.8. *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*.

12. 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 $\mathfrak{p}B$.

Proposition 12.1. $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K] =: n$.

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, $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K]$. □

Proposition 12.2. *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. □

Corollary 12.3. *There are at most n primes lying over $\mathfrak{p}$.*

Definition 12.4. 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.

Definition 12.5. A prime $\mathfrak{p} \subset A$:

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

Definition 12.6. A discrete valuation w on L is said to *extend* the discrete valuation v on K if $w|_K = e \cdot v$ for some $e \in \mathbb{Z}_+$.

Proposition 12.7. *Fix $\mathfrak{p} \subset A$. Then there is a bijection*
$$\{\text{primes } \mathfrak{q} \mid \mathfrak{p}\} \iff \{\text{discrete valuations } w \text{ extending } v_\mathfrak{p}\}$$
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 $w = v_{\mathfrak{q}}$. □

13. 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.

Theorem 13.1 (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)	$(z - z_0)$, $z_0 \neq 0$

14. Index of A-lattices

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

Definition 14.1. 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 section 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

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

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

Proposition 14.2. *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. □

Corollary 14.3. *If $I \subset A$ is an integral ideal, then $\chi(A/I) = I$.*

Definition 14.4. 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.

Proposition 14.5. *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 $(A : xA)_A = \chi(A/(x)) = (x)$. □

15. Inclusion and ideal norm

We continue to work in the AKLB setup.

Definition 15.1. 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.*

Proposition 15.2. *The following two diagrams commute:*

$$\begin{array}{ccc} L^\times & \xrightarrow{x\mapsto(x)} & \mathcal{I}_B \\ \uparrow & & \uparrow{\scriptstyle i} \\ K^\times & \xrightarrow{x\mapsto(x)} & \mathcal{I}_A, \end{array} \qquad \begin{array}{ccc} L^\times & \xrightarrow{x\mapsto(x)} & \mathcal{I}_B \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle N} \\ K^\times & \xrightarrow{x\mapsto(x)} & \mathcal{I}_A. \end{array}$$

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 14.5, $(B : (x))_A = (\det(L \xrightarrow{x} L)) = (\mathrm{N}_{L/K}(x))$. 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 $\mathfrak{p}$, $(B : (x))_A = (\mathrm{N}_{L/K}(x))$. □

Proposition 15.3. *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 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

$$\begin{array}{ccc} \mathcal{I}_B & \longrightarrow & \mathcal{I}_{B_\mathfrak{p}} \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N_\mathfrak{p}} \\ \mathcal{I}_A & \longrightarrow & \mathcal{I}_{A_\mathfrak{p}} \end{array}$$

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. □

Proposition 15.4. *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 $f_* : \operatorname{Div} Y \to \operatorname{Div} X$

16. 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.

Lemma 16.1. *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. □

Corollary 16.2. *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:

Proposition 16.3. *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 $B = A[x]/(f(x))$. □

Proposition 16.4. *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 $A[x]/(f(x)) = B$. □

17. 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 $G = \operatorname{Gal}(L/K)$.

Proposition 17.1. *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:

Proposition 17.2. $e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = n$.

18. 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 $B/\mathfrak{q}$.

Proposition 18.1. *Suppose $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$. Then:*

- *$B/\mathfrak{q}$ is Galois over $A/\mathfrak{p}$;*
- *The natural map $D \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ 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 $b = \overline{b} \bmod \mathfrak{q}$ 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 $D \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is surjective. □

19. Inertia group

Definition 19.1. The *inertia group* $I_\mathfrak{q}$ satisfies the short exact sequence

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

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 $|D| = ef$, $|\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})| = [\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] = f$, 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 $I_H \leq D_H \leq H$.

Proposition 19.2. *$D_H = D \cap H$, $I_H = I \cap H$.* □

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

Proposition 19.3. *The following diagram commutes and has exact rows and columns:*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_H & \longrightarrow & D_H & \longrightarrow & \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_{\mathfrak{q}^H}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I & \longrightarrow & D & \longrightarrow & \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_{G/H} & \longrightarrow & D_{G/H} & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}^H}/\mathbb{F}_\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

20. 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.)

Definition 20.1. Assume AKLBG with finite residue fields. For $\mathfrak{q}$ unramified, define the Artin symbol

$$\left(\frac{L/K}{\mathfrak{q}}\right) := \mathrm{Frob}_\mathfrak{q}\,.$$

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

Definition 20.2 (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

$$\prod \mathfrak{p}_i^{e_i} \mapsto \prod \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}.$$

Remark 20.3. 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 $hg_1g_2^{-1} \in D$, 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.

21. Local fields

Definition 21.1. 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.

Proposition 21.2. *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 intersection 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. □

Proposition 21.3. *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. □

Lemma 21.4. *A locally compact topological vector space over a nondiscrete locally compact field has finite dimension.*

Theorem 21.5. *Any local field is either $\mathbb{R}, \mathbb{C}$, or a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.*

22. Hensel's lemma

Lemma 22.1 (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 $F(a) = 0$.*

Lemma 22.2 (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.*

23. Extensions of complete DVRs

Theorem 23.1. *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. □

Lemma 23.2. *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)

Corollary 23.3. *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:

Theorem 23.4. *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. □

24. 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:

Theorem 24.1. *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. □

25. 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 $a_0, a_1, \cdots \in K$, 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

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

Theorem 25.1 (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.

Proposition 25.2. *There exists a unique homomorphism*

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

satisfying:

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

□

26. 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.

Theorem 26.1. *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. □

Proposition 26.2. *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 $\phi : D_i \to \mathrm{Aut}(\widehat{L}_i/\widehat{K})$. Conversely, there is a map $\psi : \mathrm{Aut}(\widehat{L}_i/\widehat{K}) \to D_i$ 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. □

Proposition 26.3. *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. □

27. 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

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

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^*.

Definition 27.1. 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 $B \subseteq B^* \implies (B^*)^{-1} \subseteq B$.

Proposition 27.2. *For any prime $\mathfrak{p} \subset A$, $(\mathcal{D}_{B/A})_\mathfrak{p} = \mathcal{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$.*

Proposition 27.3. *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 $\widehat{L} = L \otimes_K \widehat{K} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \widehat{L_\mathfrak{q}}$, and $\widehat{B} = B \otimes_A \widehat{A} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \widehat{B_\mathfrak{q}}$ (cf. previous section). 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 $\widehat{B}^* = B^* \otimes_A \widehat{A} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \widehat{B_\mathfrak{q}}^*$. 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. □

28. 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.

Definition 28.1. Given elements $e_1, \dots, e_n \in L$, their *discriminant*

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

This has the following properties:

- If $e_1, \dots, e_n \in B$, $\operatorname{disc}(e_1, \dots, e_n) \in A$.
- Suppose $\phi \in \operatorname{End}_K(L)$ mapping $e_1, \dots, e_n$ to $e_1', \dots, e_n'$, then
$$\operatorname{disc}(e_1', \dots, e_n') = (\det \phi)^2 \operatorname{disc}(e_1, \dots, e_n).$$
- 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 $A = \mathbb{Z}$!)

Definition 28.2. 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 $\operatorname{disc}(x_1, \dots, x_n)$ for any n elements $x_1, \dots, x_n \in M$.

Proposition 28.3. *The discriminant $D(M)$ is finitely generated over A, and therefore it is a fractional A-ideal.*

Proof. Choose independent elements $e_1, \dots, e_n \in M$ 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. □

Proposition 28.4. *For any prime $\mathfrak{p} \subset A$, $(D_{B/A})_{\mathfrak{p}} = D_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$.*

Proposition 28.5. *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 $e_1, \dots, e_n \in L$,*

$$\operatorname{disc}(e_1, \dots, e_n) = \det(\sigma_i(e_j))_{i,j}^2.$$

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

Proposition 28.6. *For $x \in L$,*

$$\operatorname{disc}(1, x, x^2, \dots, x^{n-1}) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2.$$

Proof. This is the Vandermonde determinant. □

Definition 28.7. If $f = \prod(x - \alpha_i)$, then the *discriminant* of this polynomial

$$\operatorname{disc} f = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Proposition 28.8. *If A is a Dedekind domain, $f \in A[x]$ a monic separable polynomial, then* $\operatorname{disc}(f) = \operatorname{disc}(1, x, x^2, \dots, x^{n-1})$.

Definition 28.9. The *discriminant* ideal $D_{B/A} = D(B) \subseteq A$, which is an actual ideal in A.

Example 28.10. $D_{\mathbb{Z}[i]/\mathbb{Z}} = (-4) = (4)$.

29. Detecting ramification

Theorem 29.1. *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 $e_1, \dots, e_n$. Then B^* is free also, with the dual basis $e_1', \dots, e_n'$.

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

Theorem 29.2. *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 $\det(\operatorname{Tr}(\overline{b_i b_j}))_{i,j} \neq 0$, iff $\overline{\det(\operatorname{Tr}(b_i b_j)_{i,j})} \neq 0 \bmod \mathfrak{p}$, iff $\mathfrak{p} \nmid D_{B/A}$, iff $\mathfrak{q} \nmid \mathcal{D}_{B/A}$. □

Corollary 29.3. *Assume AKLB, $\mathfrak{p} \in A$, then L/K is unramified at $\mathfrak{p}$ (i.e. unramified at all primes above $\mathfrak{p}$) iff $\mathfrak{p} \nmid D_{B/A}$.*

Corollary 29.4. *Only finitely many pimes of B ramify.*

Example 29.5. 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 $D(\mathbb{Z}[\alpha]) = \operatorname{disc}(1, \alpha, \alpha^2) = \operatorname{disc}(x^3 - x - 1) = -23$. But $\operatorname{disc} \mathcal{O}_K = -23/m^2$ 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.

30. More on the different

There is a neat formula for the different in the case where B is monogenic:

Proposition 30.1. *If $B = A[\alpha]$, and f is the minimal polynomial of α, then $\mathcal{D}_{B/A} = (f'(\alpha))$.*

Lemma 30.2. *Under the hypotheses above,*

$$\operatorname{Tr}(\alpha^i / f'(\alpha)) = \begin{cases} 0, & \text{for } i = 0, 1, \dots, n-2 \\ 1, & \text{for } i = n-1 \end{cases}$$

and for all i, $\operatorname{Tr}(\alpha^i / f'(\alpha)) \in A$.

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 30.1. 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

$$(B^* : I) = (\det(\operatorname{Tr}(\alpha^{i+j} / f'(\alpha))_{i,j})) = (1)$$

by the lemma, so $B^* = I$, and $\mathcal{D}_{A/B} = (B^*)^{-1} = (f'(\alpha))$. □

Lemma 30.3. *Assume AKLB. Let $\mathfrak{a}$ be a fractional ideal of A, $\mathfrak{b}$ a fractional ideal of B. Then $\operatorname{Tr}(\mathfrak{b}) \subseteq \mathfrak{a}$ iff $\mathfrak{b} \subseteq \mathfrak{a}B^*$.*

Proof. Assume WLOG $\mathfrak{a} \neq 0$. Then $\operatorname{Tr}(\mathfrak{b}) \subseteq \mathfrak{a} \iff \mathfrak{a}^{-1} \operatorname{Tr}(\mathfrak{b}) \subseteq (1) \iff \operatorname{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq (1) \iff \mathfrak{a}^{-1}\mathfrak{b} \subseteq B^* \iff \mathfrak{b} \subseteq \mathfrak{a}B^*$. □

Proposition 30.4. *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: $2g_Y - 2 = n(2g_X - 2) + \deg R$.

31. Unramified extensions of complete DVRs

Theorem 31.1. *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.) □

32. 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

$$K^{\text{unr}} = \bigcup_{K' \subseteq K^{\text{sep}} : K'/K \text{ f. unram.}} K'.$$

Example 32.1. 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, $\mathbb{Q}_p^{\text{unr}}/\mathbb{Q}_p$ is an infinite Galois extension, with Galois group the profinite integers

$$\text{Gal}(\mathbb{Q}_p^{\text{unr}}/\mathbb{Q}_p) = \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell.$$

Note that $\mathbb{Q}_p^{\text{unr}}$ 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, $K = \text{Frac}\, A$ 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 $\text{Gal}(L/K') = I_{L/K'} = I_{L/K}$ 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 $p = \text{char}\, k$.

Definition 32.2. 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:

Theorem 32.3. *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. □

33. Continuity of roots

Lemma 33.1 (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 $\sigma \in \text{Aut}(\overline{K}/K(\beta))$ 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".

Proposition 33.2 (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 $g(x)=b_nx^n+\cdots+b_0$, 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. □

Corollary 33.3. *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 $F\mathbb{Q}_p=\mathbb{Q}_p(\beta)=K$. □

Corollary 33.4. *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 $\overline{\mathbb{Q}}\mathbb{Q}_p=\overline{\mathbb{Q}_p}$.*

Corollary 33.5. *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.

34. Lattices in $\mathbb{R}^n$

We move on to lattice methods in studying number fields (finite extensions of $\mathbb{Q}$).

Definition 34.1. 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 $m=n$.

Proposition 34.2. *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 $\mathbb{R}^n$.

Definition 34.3. 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 $E_i\in\Sigma$, $\mu(\bigcup_i E_i)=\sum_i\mu(E_i)$.

Theorem 34.4 (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;*
- *$\mu(S)=\inf\{\mu(U):S\subseteq U,U\text{ open}\}$;*
- *$\mu(U)=\sup\{\mu(K):K\subseteq U,K\text{ compact}\}$ 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:

Definition 34.5. A *fundamental domain* for $\Lambda \subset V$ is a measurable $F \subset V$ such that $V = \coprod_{\lambda \in \Lambda}(F + \lambda)$.

Proposition 34.6. *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 $\operatorname{vol}(G) = \operatorname{vol}(F)$. □

Definition 34.7. The *covolume* $\operatorname{covol}(\Lambda)$ of a full lattice Λ is defined to be the volume of any fundamental domain of Λ.

Proposition 34.8. *Suppose $\Lambda \supseteq \Lambda'$ are full lattices, then*

$$\operatorname{covol}(\Lambda') = (\Lambda : \Lambda') \operatorname{covol}(\Lambda).$$

35. Minkowski's lattice point theorem

Lemma 35.1. *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. □

Theorem 35.2 (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. □

Theorem 35.3 (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:

Theorem 35.4. *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 $x^2 + y^2 = p$. □

36. Global fields

Definition 36.1. A *global field* is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$.

37. Places

We transition to a discussion of places, which are like primes but generalizes to the archimedean case as well.

Theorem 37.1. *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.

Definition 37.2. 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 $\mathfrak{q} \mid (p)$.

Proposition 37.3. *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 89.4. □

Lemma 37.4. *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

Theorem 37.5. *$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{v|p} K_v$, for $p \leq \infty$.*

Example 37.6. 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.

Corollary 37.7. *The places $v \mid p$ correspond bijectively to* $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}_p})/\operatorname{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

Definition 37.8. If $v \mid p$, the *normalized absolute value* on K_v is $|x|_v = |\operatorname{N}_{K_v/\mathbb{Q}_p}(x)|_p$.

Proposition 37.9. *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. □

Example 37.10. 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 $|x|_v$.

Theorem 37.11 (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. □

38. Orders

We are on our way to apply Minkowski's lattice point formula to say something nontrivial about the ideal class group.

Definition 38.1. 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

$$\langle x, y\rangle = \sum_{\sigma : K \hookrightarrow \mathbb{C}} \sigma x \cdot \overline{\sigma y}.$$

Proposition 38.2. $\operatorname{covol}(\mathcal{O}) = \sqrt{|\operatorname{disc}\mathcal{O}|}$.

Proof. Let $e_1, \dots, e_n$ 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 $\operatorname{covol}(\mathcal{O}) = \sqrt{|\operatorname{disc}\mathcal{O}|}$. □

Corollary 38.3. *Suppose I is an invertible fractional $\mathcal{O}$-ideal, then* $\operatorname{covol}(I) = \sqrt{\operatorname{disc}\mathcal{O}} \cdot N(I)$.

39. 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).

Theorem 39.1. *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 $|N(a)| \le m \cdot |N(I)|$.*

Proof. Let $S = \{z = (z_\sigma)_{\sigma\in\operatorname{Hom}_\mathbb{Q}(K,\mathbb{C})} \in K_\mathbb{R} : \sum|z_\sigma| < t\}$, where t is a constant we fix later. Then it is not hard to show that $\operatorname{vol}(S) = 2^r\pi^s\frac{t^n}{n!}$. Choose t such that $\operatorname{vol}(S) > 2^n\operatorname{covol}(I)$. By Minkowski's lattice point theorem, there exists nonzero $a \in I$ lying in S, such that $t > \sum_\sigma|\sigma a| \ge n\sqrt[n]{\prod_\sigma|\sigma a|} = n\sqrt[n]{|\operatorname{N}_{K,\mathbb{Q}}(a)|}$. 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

$$|N(a)| = |\operatorname{N}_{K,\mathbb{Q}}(a)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|\operatorname{disc}\mathcal{O}|}\cdot|N(I)| = m\cdot|N(I)|,$$

as desired. □

Corollary 39.2. *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 $|N(a)| \le m\cdot|N(I)|$. This means that $(a)I^{-1}$ is an integral ideal in the target ideal class, whose norm is at most m. □

Lemma 39.3. *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. □

Theorem 39.4. *The class group of a number field is finite.*

Proposition 39.5. $\sqrt{\operatorname{disc}\mathcal{O}_K} \ge \frac{n^n}{n!}(\frac{\pi}{4})^s \ge \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$.

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, $m \ge 1$. □

Corollary 39.6. *If $K \ne \mathbb{Q}$, then $|\operatorname{disc}\mathcal{O}_K| > 1$. In other words, there are no everywhere unramified nontrivial extensions of $\mathbb{Q}$.*

Proposition 39.7. *There are finitely many number fields K with $|\operatorname{disc}\mathcal{O}_K| < B$, for any real B.*

Proof. By proposition 39.5, it suffices to show that there are finitely many such number fields of any fixed degree n.

Case 1: K is totally real. Let $S := \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_1| \le 2B^{1/2}, |x_i| < 1 \text{ for all } i \ne 1\}$. Then $\operatorname{vol}(S) \approx 2^{n+1}B^{1/2} > 2^n|\operatorname{disc}\mathcal{O}_K|^{1/2} = 2^n\operatorname{covol}(\mathcal{O}_K)$. By Minkowski, there exists a nonzero $\alpha \in \mathcal{O}_K \subset \mathbb{R}^n$ in S. Then $\prod|\alpha_i| = |N(\alpha)| \ge 1$ while $|\alpha_2|, \dots, |\alpha_n| < 1$, which forces $|\alpha_1| > 1$. If $\mathbb{Q}(\alpha) \ne K$, 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 $S := \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |z_1|^2 \le cB^{1/2}, |x_i|, |z_j| < 1 \text{ for all } i \text{ and for all } j \ne 1\}$, where c is large enough that $\operatorname{vol}(S) > 2^n\operatorname{covol}(\mathcal{O}_K)$. The argument in Case 1 continues verbatim. □

Lemma 39.8. *Let K be a number field of degree n, then for any prime p, $v_p(D_K) \le n\lfloor\log_p n\rfloor + n - 1$.*

Proof. We have $v_p(D_K) = v_p(N(\mathcal{D}_K)) = \sum_{\mathfrak{q}|p} f_\mathfrak{q} v_\mathfrak{q}(\mathcal{D}_K) \le \sum_{\mathfrak{q}|p} f_\mathfrak{q}(e_\mathfrak{q} - 1 + v_p(e_\mathfrak{q})) \le n - 1 + n\lfloor\log_p n\rfloor$ by trivial bounding. □

Theorem 39.9 (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. □

40. 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:

Definition 40.1. The adèle ring $\mathbb{A}_K$ of a global field K is the *restricted product*

$$\prod_v{}'(K_v, \mathcal{O}_v),$$

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.)

Proposition 40.2. *$\mathbb{A} = \mathbb{A}_K$ 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.

Proposition 40.3. *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 $\mathbb{Z} \hookrightarrow \mathbb{R}$:

Theorem 40.4. *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 40.3. 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 $[0, 1]$. □

41. Idèle group

Definition 41.1. 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 $\mathbb{A}^\times \hookrightarrow \mathbb{A} \times \mathbb{A}$, $x \mapsto (x, x^{-1})$.

Proposition 41.2. *$K^\times$ 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. □

Definition 41.3. 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.

Definition 41.4. The group $\mathbb{A}_1^\times = \ker(\mathbb{A}^\times \xrightarrow{||} \mathbb{R}_{>0}^\times)$.

Proposition 41.5. *$K^\times$ 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:

$$\mathrm{Cl}(\mathcal{O}_K) = \mathcal{I}/K^\times = \frac{\mathbb{A}^\times}{K^\times \cdot \prod \mathcal{O}_v^\times}.$$

Definition 41.6. The *idèle class group* is $\mathbb{A}^\times/K^\times$.

Theorem 41.7. *$\mathbb{A}_1^\times/K^\times$ is compact.*

This is a hard theorem and directly implies finiteness of the class group.

Definition 41.8. For $d = (d_v)_v \in \mathbb{A}^\times$, define the adelic parallelotope (box)

$$\mathbb{L}(d) := \{(x_v) \in \mathbb{A} : |x_v|_v \le |d_v|_v \text{ for all } v\},$$

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.

Theorem 41.9 (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 $|x|_v \le |d_v|_v$ 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 $L(d)$. □

42. 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.

Corollary 42.1. *If $a, b \in \mathbb{A}^\times$ such that $|b| > c|a|$ (where) c is as in theorem 41.9. 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 $u\mathbb{L}(a) \subseteq \mathbb{L}(b)$. □

Lemma 42.2. *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. □

Lemma 42.3. *If $b \in \mathbb{A}^\times$, $|b|$ sufficiently large, then $\mathbb{A} = K + \mathbb{L}(b)$.*

Proof. Combine the previous two claims. □

Theorem 42.4 (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. □

43. Compactness of $\mathbb{A}_1^\times / K^\times$

Lemma 43.1. *$\mathbb{A}_1^\times$ 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. □

Theorem 43.2. *$\mathbb{A}_1^\times / K^\times$ 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. □

44. Finiteness of the class group, second proof

We will use the compactness of $\mathbb{A}_1^\times / K^\times$ to show:

Theorem 44.1 (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). □

45. Dirichlet's unit theorem

Definition 45.1. 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 $\mu = (\mathcal{O}_S^\times)_{\mathrm{tors}} = (K^\times)_{\mathrm{tors}}$ be the group of roots of unities.

Define a continuous homomorphism

$$\begin{aligned} \mathrm{Log} : \mathbb{A}_S^\times &\to \mathbb{R}^S \\ (a_v) &\mapsto (\log |a_v|_v)_{v \in S}. \end{aligned}$$

Lemma 45.2. *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.* □

Lemma 45.3. *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. □

Corollary 45.4. $\ker(\mathrm{Log} : \mathcal{O}_S^\times \to \mathbb{R}^S) = \mu$, *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. □

Theorem 45.5 (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 $|S| - 1$. □

46. 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:

Proposition 46.1. *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.

Corollary 46.2. *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 $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proposition 46.3. *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 §16). 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 $\Phi_{p^r}(x) \bmod \mathfrak{p}$. So $(\mathcal{O}_k)_\mathfrak{p}[\zeta_{p^r}]$ is a DVR (?), and therefore integrally closed. □

47. Zeta functions

We transition to yet another topic: analytic number theory. A good reference is Davenport's *Multiplicative Number Theory*.

Definition 47.1 (Riemann zeta function)**.** For $\Re(s) > 1$,

$$\zeta(s) := \prod_p \frac{1}{1-p^{-s}} = \sum_{n\geq 1} n^{-s}.$$

Definition 47.2 (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. $\mathrm{N}(\mathfrak{p}) = p^{[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]} = |\mathcal{O}_K/\mathfrak{p}|$.

Proposition 47.3. *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. □

Proposition 47.4. *$\zeta(s) = \frac{1}{s-1} + \phi(s)$, where $\phi(s)$ extends to a holomorphic function on $\Re(s) > 0$.*

Proof. For $\Re(s) > 1$,

$$\begin{aligned}
\zeta(s) &= \sum_{n\geq 1} n^{-s} \\
&= \sum_{n\geq 1} n(n^{-s} - (n+1)^{-s}) \\
&= \sum_{n\geq 1} \left(n \int_n^{n+1} s x^{-s-1} dx \right) \\
&= s \int_1^\infty \lfloor x \rfloor \, x^{-s-1} dx \\
&= \frac{1}{s-1} + \left(1 - s \int_1^\infty \{x\} x^{-s-1} dx \right),
\end{aligned}$$

where the latter term (which we call $\phi(s)$) converges absolutely for $\Re(s) > 0$, and uniformly so on $\Re(s) \geq \varepsilon$ for any $\varepsilon > 0$. □

Proposition 47.5. *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 $0 < \Re(s) < 1$, conjectured to all lie on $\Re(s) = 1/2$.*

48. Character theory of finite abelian groups

Theorem 48.1 (Dirichlet)**.** *If $\gcd(a, m) = 1$, then there exist infinitely many primes congruent to a mod m.*

Definition 48.2. 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.

Proposition 48.3. *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 $s = 0$. □

Proposition 48.4. *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.

Theorem 48.5 (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. □

49. Proof of Dirichlet's theorem, minus two theorems

Definition 49.1. 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 $\Re(s) > 1$.

Proposition 49.2. *If $\chi \neq \mathbf{1}$ (the trivial character), then $L(s, \chi)$ extends to a holomorphic function for $\Re(s) > 0$.*

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 $\Re(s) > 0$. Furthermore, it converges uniformly on $\Re(s) \geq \varepsilon$ for every ε, so L can be extended holomorphically to $\Re(s) > 0$. □

Proof of theorem 48.1, Dirichlet's theorem on arithmetic progressions. Writing the indicator function as the sum of characters,

$$\begin{aligned}\sum_{p\equiv a} p^{-s} &= \sum_p p^{-s}\left(\frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\chi(p)\right)\\ &= \frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\left(\sum_p \chi(p)p^{-s}\right)\\ &= \frac{1}{\phi(m)}\sum_\chi \chi(a^{-1})\left(\log L(s,\chi)+O(1)\right)\\ &= \frac{1}{\phi(m)}\log L(s,\mathbf{1}) + \frac{1}{\phi(m)}\sum_{\chi\neq\mathbf{1}}\chi(a^{-1})\log L(s,\chi)+O(1).\end{aligned}$$

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 $s=1$. □

Theorem 49.3. *Up to Euler factors at primes dividing m,*

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod_{\chi:(\mathbb{Z}/m\mathbb{Z})^\times\to\mathbb{C}^\times} L(s,\chi).$$

Theorem 49.4. *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 49.3. 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

$$\prod_{\mathfrak{p}\mid p}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1} = (1-(p^{-s})^{f_p})^{-g_p}.$$

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. □

Theorem 49.5 (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,*

$$\lim_{s\to1}(s-1)\zeta_K(s) = \frac{\mathrm{vol}(\mathbb{A}_1^\times/K^\times)}{\mathrm{vol}(\mathbb{A}/K)} = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K/w_k}{\sqrt{|D_K|}},$$

where $h_K=\#\,\mathrm{Cl}_K$, $w_K=\#\mu_K$.

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.

50. Measure theory

Definition 50.1. 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*.

Example 50.2. 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*.

Definition 50.3. 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.)

Definition 50.4. 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.)

51. 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 $|\int f| \leq \int |f|$.

Theorem 51.1 (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 $\int f = \lim \int f_n$.*

Theorem 51.2 (Dominated convergence theorem)**.** *Suppose measurable functions $f_1, f_2, \dots : X \to \mathbb{C}$ 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 $\int f = \lim \int f_n$.*

Definition 51.3. 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).

Definition 51.4. 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.

Definition 51.5. 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:

Theorem 51.6 (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.

Example 51.7. Let $X = \mathbb{R}^n$, the Riemann integral corresponds to the Lebesgue measure.

Example 51.8. 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.

52. Haar measures

Definition 52.1. Let G be a LCH topological group. A *left Haar measure* on G is a nonzero left-invariant outer Radon measure.

Theorem 34.4 says that such a measure always exists and is unique up to multiplication by a positive constant.

Proposition 52.2. *G is compact iff $\mu(G) < \infty$. In this case, the* normalized Haar measure *is the unique Haar measure with $\mu(G) = 1$.*

Example 52.3. 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.

Definition 52.4. 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.

53. Duality of locally compact abelian groups

54. Dec. 7

55. Dec. 9

56. Dec. 12

57. Dec. 14

58. Kronecker–Weber theorem

Theorem 58.1 (global KW)**.** *Any finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$.*

Theorem 58.2 (local KW)**.** *Any finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}_p(\zeta_m)$.*

Lemma 58.3 (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*

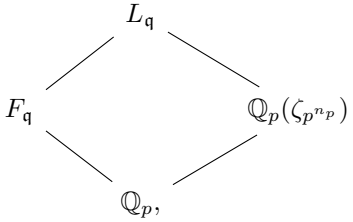
$$\mathrm{Gal}(L_1L_2/K) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) : \sigma_1|_{L_1\cap L_2} = \sigma_2|_{L_1\cap L_2}\}.$$

Proposition 58.4. *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



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

$$|I| \le \prod |I_p| = \prod \phi(p^{n_p}) = \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

Let L^I be the fixed field of I. Then $L^I/\mathbb{Q}$ is unramified, so $L^I = \mathbb{Q}$. This means

$$[L : \mathbb{Q}] = [L : L^I] = |I| \le [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \le [L : \mathbb{Q}],$$

so $L = \mathbb{Q}(\zeta_m)$ as desired. □

Proposition 58.5. *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, $\ell = p \ge 3$;
- 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. 32.3). 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 $\mathrm{disc}(x^e - u)$, 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. □

Lemma 58.6. $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.

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, $p \ge 3$. 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

$$\mathrm{Gal}(K(\zeta_{p^{r+1}(p^{p^r}-1)})/\mathbb{Q}_p) \subseteq \mathrm{Gal}(K/\mathbb{Q}_p) \times (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}$$

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. □

Definition 58.7 (semidirect product)**.** Let G be a group, $N \triangleleft G$ 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 $\phi : H \to \mathrm{Aut}(N)$. 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.

Proposition 58.8 (Schur-Zassenhaus lemma)**.** *Let $N \triangleleft G$ with $|N|$ and $|G/N|$ coprime, then there exists a section $G/N \to G$. Consequently $G = N \rtimes G/N$.*

Proposition 58.9. *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. □

Theorem 58.10. *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 $G_1 \triangleleft G_0 \triangleleft G$ (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 58.8, $G_0 \cong G_1 \ltimes G_0/G_1$.

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. □

Remark 58.11. 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.

59. The Artin map

Now fix L/K an abelian extension of global fields, so that we have the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{Frob}_{\mathfrak{p}} =: \sigma_{\mathfrak{p}}$$

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:

Proposition 59.1. *Let K be a number field, L/K abelian. Then the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is surjective.*

Proposition 59.2. *The primes in $\ker \psi_{L/K}$ are the primes in K that split completely in L.* □

Proposition 59.3. *Let $K \subseteq L \subseteq M$ be a tower of abelian extensions of global fields. Then the Artin maps commute with the restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$.*

60. Ray class groups

Proposition 60.1. *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.)

Definition 60.2. 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.

Definition 60.3. 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 $K \hookrightarrow K_v = \mathbb{R}$.

Definition 60.4. 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 $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$.

Definition 60.5. 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*.

Lemma 60.6. *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. □

Proposition 60.7. *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, $\ker(g) = \mathcal{O}_K^\times$, $\ker(g \circ f) = \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$, $\operatorname{coker}(g) = \mathcal{I}_K^{\mathfrak{m}}/\operatorname{im}(K^{\mathfrak{m}}) = \mathrm{Cl}_K$ by the previous lemma, and $\operatorname{coker}(g \circ f) = \mathrm{Cl}_K^{\mathfrak{m}}$. The kernel-cokernel exact sequence yields

$$0 \to \ker(f) \to \ker(g \circ f) \to \ker(g) \to \operatorname{coker}(f) \to \operatorname{coker}(g \circ f) \to \operatorname{coker}(g) \to 0,$$

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 $(\operatorname{sgn}(\alpha_v), \overline{\alpha} = \overline{a}\overline{b}^{-1})$. 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. □

Corollary 60.8. *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

$$\phi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty}, \quad \phi(\mathfrak{m}_0) = |(\mathcal{O}_K/\mathfrak{m}_0)^\times| = \prod_{\mathfrak{p}|\mathfrak{m}_0} |(\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times| = \mathrm{N}(\mathfrak{m}_0) \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - \mathrm{N}(\mathfrak{p})^{-1}).$$

61. Polar density

Definition 61.1. 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 $\Re(s) > 1$.

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.

Definition 61.2. If $\zeta_{K,S}^n$ 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

$$\delta(S) = \lim_{n \to \infty} \frac{\#\{\mathfrak{p} \in S : \mathrm{N}(\mathfrak{p}) \le n\}}{\#\{\mathfrak{p} : \mathrm{N}(\mathfrak{p}) \le n\}}.$$

Proposition 61.3. *If S has a natural density, then it has a Dirichlet density, and the two densities agree.*

Proof. 18.786 problem set 2. □

Proposition 61.4. *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 $\zeta_{K,S}^n$ 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 $d(S) = m/n = \rho(S)$. □

Proposition 61.5. *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 $\rho(S) \leq \rho(T)$ 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. □

62. 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 section is to show the surjectivity of the Artin map.

Theorem 62.1. *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 $\rho(S) = \frac{1}{n}\rho(T) = \frac{1}{n}$. □

Corollary 62.2. *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. □

Corollary 62.3. *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.

Lemma 62.4. *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 $|D_\mathfrak{q}| = 1$. □

Theorem 62.5. *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 $L \subseteq M$. □

Theorem 62.6 (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. □

Theorem 62.7. *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 62.5 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 $L \subseteq K(\mathfrak{m})$.

63. Conductors

Definition 63.1. 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 $R_K^{\mathfrak{m}}$.

Definition 63.2. 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.

Lemma 63.3. *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 $\mathcal{C}_2 = \mathcal{C}_1 \mathcal{R}_K^{\mathfrak{m}_2}$.

Proposition 63.4. *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 $\mathfrak{m} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$.*

Corollary 63.5. *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 $\mathcal{C}'' \sim \mathcal{C}$.*

Definition 63.6. 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 $\mathcal{R}_K^{\mathfrak{c}} \subseteq \mathcal{C}$.

Proposition 63.7. *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 $\mathfrak{c} = \mathfrak{m}$. □

Example 63.8. 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 $\mathbb{Q}$.

Example 63.9. 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 $\mathbb{Q}(\zeta_n)$.

64. Ray class characters

Definition 64.1. 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 $\mathrm{Cl}_K^{\mathfrak{m}}$.

Example 64.2. 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. $\chi(-1) = 1$.

Definition 64.3. 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.

Definition 64.4. The *conductor* of a ray class character is the conductor of its kernel (which is a congruence subgroup).

Proposition 64.5. *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?)

Definition 64.6. 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.)

65. Weber L-functions

Definition 65.1 (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 $\Re(s)>1$.

This generalizes Dirichlet L-functions ($K=\mathbb{Q}$) and Dedekind zeta functions ($\chi=\mathbf{1}$), both of which generalize the Riemann zeta function.

Proposition 65.2. *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. □

Proposition 65.3. *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*

$$d(S)=\begin{cases}1/n, & \text{if } L(1,\chi)\neq 0 \text{ for all } \chi\neq\mathbf{1} \text{ in } X(\mathcal{C});\\ 0, & \text{otherwise.}\end{cases}$$

(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 $e(\chi)=1$. □

Proposition 65.4. *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 $\{\mathfrak{p}\in IC\}$ has Dirichlet density the same as the trivial coset.*

Proof. Same proof, just change the indicator function. □

Corollary 65.5. *The coset $\{p\in IC\}$ 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. □

Corollary 65.6. *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 $1/[I_K^{\mathfrak{m}} : \mathcal{C}]$. □

66. Second main inequality of CFT

Definition 66.1. 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.)

Proposition 66.2. *Let L/K be a finite abelian extension of local or global fields. For each prime $\mathfrak{p}$ of K,*

$$v_{\mathfrak{p}}(L/K) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is unramified} \\ 1 & \text{if } \mathfrak{p} \text{ is tamely ramified} \\ \geq 2 & \text{if } \mathfrak{p} \text{ is wildly ramified.} \end{cases}$$

Proof. See 18.786 pset 2. □

Remark 66.3. The conductor and the discriminant are supported on the same primes (but the valuations can be very different).

Lemma 66.4. *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. □

Definition 66.5. 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

$$T_{L/K}^{\mathfrak{m}} = \mathcal{R}_K^{\mathfrak{m}} \mathrm{N}_{L/K}(\mathcal{I}_L^{\mathfrak{m}}),$$

where $\mathcal{I}_L^{\mathfrak{m}}$ are the fractional $\mathcal{O}_L$-ideals coprime to $\mathfrak{m}_0\mathcal{O}_L$.

Proposition 66.6. *Let L/K be a finite abelian extension of global fields, $\mathfrak{m}$ a modulus divisible by $\mathfrak{c}(L/K)$, then $\mathrm{Spl}(L/K) \lesssim \{\mathfrak{p} \in T_{L/K}^{\mathfrak{m}}\}$.*

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 $\mathfrak{q} \in \mathcal{I}_K^{\mathfrak{m}}$ and $\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}$, so $\mathfrak{p}$ is in $T_{L/K}^{\mathfrak{m}}$. □

Theorem 66.7 (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*

$$[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}] \leq [L : K].$$

Proof. Follows from corollary 65.6. □

The goal now is to show that this is actually an equality.

67. Global CFT via ideals

What we are working towards is the following:

Theorem 67.1 (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:

$$\begin{array}{ccc} \{\text{finite abelian } L/K \text{ with } \mathfrak{c}(L/K) \mid \mathfrak{m}\} & \xrightarrow{L \mapsto T^{\mathfrak{m}}_{L/K}} & \{\text{congruence subgroups of modulus } \mathfrak{m}\} \\ {\scriptstyle L \mapsto \mathrm{Gal}(L/K)}\downarrow & & \downarrow{\scriptstyle \mathcal{C} \mapsto I^{\mathfrak{m}}_K/\mathcal{C}} \\ \{\text{quotients of } \mathrm{Gal}(K(\mathfrak{m})/K)\} & \xleftarrow[\psi^{\mathfrak{m}}_{L/K}]{} & \{\text{quotients of } \mathrm{Cl}^{\mathfrak{m}}_K\} \end{array}$$

Definition 67.2. 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.

68. Simple pole of ζ_K at $s = 1$

In this section 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:

Proposition 68.1. *Let $a_1, a_2, \cdots \in \mathbb{C}$ 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 $\Re(s) > \sigma$ 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:

Proposition 68.2. *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".

Definition 68.3. Let X, Y be metric spaces. A map $f : X \to Y$ is *Lipschitz continuous* if there exists $c > 0$, such that $d(f(u), f(v)) \leq cd(u, v)$ for all $u, v \in X$.

This is a stronger condition than uniform continuity.

Definition 68.4. 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 $f : [0, 1]^d \to X$.

Lemma 68.5. *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 $\partial S_{\leq 1}$ 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 $(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \mapsto (\operatorname{Log} x) \times (\operatorname{sgn} x_1, \dots, \operatorname{sgn} x_{r_1}) \times (\arg z_1, \dots, \arg z_{r_2})$.

Analyzing $S_{\leq 1}$, 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 $S_{\leq 1}$. So its boundary is clearly $(n-1)$-Lipschitz parametrizable, proving the theorem.

Remark 68.6. If we keep track of the coefficient of the linear term, we actually get the analytic class number formula.

69. Group cohomology

Definition 69.1. 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.

Remark 69.2. When G is a topological group, we need to require the G-action to be continuous.

Example 69.3. 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 $\operatorname{Gal}(L/K)$-modules.
- For $A, B \in \operatorname{Mod}_G$, the abelian group $\operatorname{Hom}_{\mathrm{Ab}}(A, B)$ has a natural G-module structure: $(g\phi)(a) = g\phi(g^{-1}a)$.

Definition 69.4. For $A \in \operatorname{Mod}_G$, the subgroup $A^G = \{a \in A : ga = a \text{ for all } g \in G\}$ is the subgroup of *G-invariants*.

Example 69.5. $\operatorname{Hom}_G(A, B) \cong \operatorname{Hom}_{\mathrm{Ab}}(A, B)^G$. In particular, $\operatorname{Hom}_G(\mathbb{Z}, A) \cong A^G$.

Any morphism of G-modules $A \to B$ restricts to a morphism $A^G \to B^G$. We thus have a functor $\bullet^G : \operatorname{Mod}_G \to \operatorname{Mod}_G$ (in fact the subcategory of trivial G-modules, which is just Ab), which is left exact because it is $\operatorname{Hom}_G(\mathbb{Z}, \bullet)$. (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 $\bullet^G : \operatorname{Mod}_G \to \mathrm{Ab}$. In particular $H^0(G, A) = A^G$.

Now, we give another definition of group cohomology using cochains.

Definition 69.6. 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

$$H^n(G,A) = \frac{Z^n(G,A)}{B^n(G,A)}.$$

Example 69.7. 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 $H^1(G,A) = \operatorname{Hom}_{\mathrm{Grp}}(G,A) = \operatorname{Hom}_{\mathrm{Ab}}(G^{\mathrm{ab}}, A)$.

We give a useful interpretation of $H^2(G,A)$.

Definition 69.8. 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 section $s : G \to E$, 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \theta} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

commutes.

Proposition 69.9. *$H^2(G,A)$ 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 $A \rtimes G$.

Lemma 69.10. *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. □

Lemma 69.11. *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 $0 \to C^\bullet(G,A) \to C^\bullet(G,B) \to C^\bullet(G,C) \to 0$.* □

Theorem 69.12. *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

$$\begin{array}{ccccccc} \operatorname{coker} d_A^{n-1} & \longrightarrow & \operatorname{coker} d_B^{n-1} & \longrightarrow & \operatorname{coker} d_C^{n-1} & \longrightarrow & 0 \\ \downarrow{\scriptstyle d_A^n} & & \downarrow{\scriptstyle d_B^n} & & \downarrow{\scriptstyle d_C^n} & & \\ 0 \longrightarrow \ker d_A^{n+1} & \longrightarrow & \ker d_B^{n+1} & \longrightarrow & \ker d_C^{n+1} & & \end{array}$$

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 $\overline{f} \in H^i(G,B)$. □

Definition 69.13 (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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0, \end{array}$$

  the diagram

$$\begin{array}{ccc} T^i(A'') & \xrightarrow{\delta} & T^{i+1}(A') \\ \downarrow & & \downarrow \\ T^i(B'') & \xrightarrow{\delta} & T^{i+1}(B') \end{array}$$

  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.

Definition 69.14. 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 $\sum n_g g \mapsto \sum n_g \in \mathbb{Z}$.

Lemma 69.15. *The standard resolution is exact, so that it is a free resolution of* $\mathbb{Z}$ *as a (trivial)* $\mathbb{Z}[G]$*-module.*

Definition 69.16 (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 $\mathrm{Hom}_R(\bullet, A)$ to $P_\bullet \to 0$ and deleting the $\mathrm{Hom}(B, A)$-term, we get a cochain complex

$$0 \to \mathrm{Hom}(P_0, A) \to \mathrm{Hom}(P_1, A) \to \dots,$$

then $\mathrm{Ext}^n_R(B, A)$ is defined as its n-th cohomology.

Lemma 69.17. *The groups* $\mathrm{Ext}^n_R(B, A)$ *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 $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, as the n-th cohomology of

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{d_1^*} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], A) \xrightarrow{d_2^*} \dots.$$

Proposition 69.18. *We have isomorphisms of abelian groups* ($n \geq 0$)*:*

$$\Phi^n : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{n+1}], A) \to C^n(G, A)$$

by

$$\phi \mapsto [(g_1, \dots, g_n) \mapsto \phi(1, g_1, g_1g_2, \dots, g_1g_2 \cdots g_n)].$$

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

$$\phi(g_0, \dots, g_n) = g_0 \phi(1, h_1, h_1h_2, \dots, h_1h_2 \cdots h_n) = 0,$$

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. □

Corollary 69.19. $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

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.

Corollary 69.20. $H^n(G, A \oplus B) = H^n(G, A) \oplus H^n(G, B)$.

Proof. This is because in general,

$$\operatorname{Ext}^i_R(\bigoplus M_\alpha, N) = \prod \operatorname{Ext}^i_R(M_\alpha, N) \quad \text{and} \quad \operatorname{Ext}^i_R(M, \prod N_\alpha) = \bigoplus \operatorname{Ext}^i_R(M, N_\alpha)$$

for any R-modules M and N. □

Definition 69.21. Let $H \leq G$ be a subgroup, A and H-module. The *induced* G-module

$$\operatorname{Ind}_H^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A,$$

and the *coinduced* G-module

$$\operatorname{CoInd}_H^G(A) := \operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A).$$

Theorem 69.22. *If H has finite index in G, then* $\operatorname{Ind}_H^G(A) \cong \operatorname{CoInd}_H^G(A)$.

When $H = \{1\}$ we just write Ind^G and CoInd^G.

Lemma 69.23. *Group cohomology of coinduced modules from the trivial group:*

$$H^n(G, \operatorname{CoInd}^G(A)) = \begin{cases} A, & \text{if } n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. For $n \geq 1$ we have isomorphisms of abelian groups

$$\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^n], \operatorname{CoInd}^G(A)) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G^n], A),$$

given by

$$\phi \mapsto [z \mapsto \phi(z)(1)]$$
$$[z \mapsto [y \mapsto \phi(yz)]] \hookleftarrow \phi.$$

so $H^n(G, \operatorname{CoInd}^G(A)) = H^n(\{1\}, A)$ for $n \geq 0$. Just use the stupid resolution $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$. □

70. 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 $\operatorname{Ind}_H^G(A)$, we really think of $\mathbb{Z}[G]$ as a *right* $\mathbb{Z}[H]$-module, and then "manually" define the extra structure of $\operatorname{Ind}_H^G(A)$ as a $\mathbb{Z}[G]$-module, by $g(\alpha \otimes a) = (g\alpha) \otimes a$. Similarly, the $\mathbb{Z}[G]$-module structure on $\operatorname{CoInd}_H^G(A)$ is given by $(g\phi)(\alpha) = \phi(\alpha g)$.

Lemma 70.1. *When G is finite, there is a canonical isomorphism* $\operatorname{CoInd}^G(A) \cong \operatorname{Ind}^G(A)$ *given by*

$$\phi \mapsto \sum_{g \in G} g^{-1} \otimes \phi(g)$$
$$(g^{-1} \mapsto a) \hookleftarrow g \otimes a.$$

where $(g^{-1} \mapsto \alpha)$ maps g' to 0 for $g' \neq g^{-1}$.

Definition 70.2 (group homology)**.** The n-th group homology with coefficients in A is

$$H_n(G, A) = \operatorname{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A) = L_n(\mathbb{Z} \otimes_{\mathbb{Z}[G]} \bullet)(A) = L_n(\bullet \otimes_{\mathbb{Z}[G]} A)(\mathbb{Z}).$$

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 $\bullet \otimes_{\mathbb{Z}[G]} A$.

Lemma 70.3. $H_n(G, A \oplus B) \cong H_n(G, A) \oplus H_n(G, B)$.

Proof. This is just because Tor commutes with arbitrary direct sums and filtered colimits in each variable. □

Definition 70.4 (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:

Lemma 70.5. *Group homology of induced modules from the trivial group:*

$$H_n(G, \mathrm{Ind}^G(A)) = \begin{cases} A, & \text{if } n = 0; \\ 0, & \text{otherwise.} \end{cases}$$

71. Tate cohomology

Lemma 71.1. *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 $\hat{N}_G : A_G \to A^G$.* □

Definition 71.2 (Tate (co)homology)**.** Define $\hat{H}^n(G, A) = H^n(G, A)$ for $n > 0$, and $\hat{H}^0(G, A) = \mathrm{coker}\, \hat{N}_G$. 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:

Theorem 71.3. *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*

$$\begin{aligned} \dots &\to \hat{H}_1(G, A) \to \hat{H}_1(G, B) \to \hat{H}_1(G, C) \\ &\to \hat{H}_0(G, A) \to \hat{H}_0(G, B) \to \hat{H}_0(G, C) \\ &\to \hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C) \\ &\to \hat{H}^1(G, A) \to \hat{H}^1(G, B) \to \hat{H}^1(G, C) \to \dots \end{aligned}$$

Furthermore, this is functorial.

Proof. Apply the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} H_1(G, C) & \longrightarrow & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \hat{H}_G} & & \downarrow{\scriptstyle \hat{H}_G} & & \downarrow{\scriptstyle \hat{H}_G} & & \\ 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & H^1(G, A). \end{array}$$

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. □

Lemma 71.4. *$\hat{H}^n(G, A \oplus B) \cong \hat{H}^n(G, A) \oplus \hat{H}^n(G, B)$, and $\hat{H}_n(G, A \oplus B) \cong \hat{H}_n(G, A) \oplus \hat{H}_n(G, B)$.*

Theorem 71.5. *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. □

Corollary 71.6. *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

$$(*) \qquad \cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

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.

Theorem 71.7. *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 $\hat{H}_0(G, A)$.*

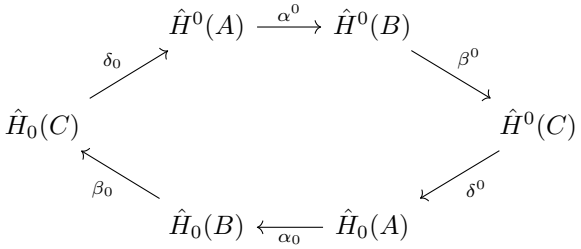
Proof. Apply the tensor and hom functors on $(*)$. □

72. Herbrand quotient

Definition 72.1. 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

$$h(A) = h^0(A)/h_0(A) \in \mathbb{Q}.$$

Proposition 72.2. *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*



where the map δ^0 is given by $\hat{H}^0(C) \cong \hat{H}^{-2}(C) = \hat{H}_1(C) \to \hat{H}_0(A)$. □

Corollary 72.3. *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. □

Corollary 72.4. *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 $h_0(A) = \#\ker(\hat{N_G}) = \#\operatorname{coker}(\hat{N_G}) = h^0(A)$. □

Corollary 72.5. *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 $h(A) = \#(G)^{\operatorname{rk} A}$.* □

Lemma 72.6. *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 $0 \to \operatorname{im}\alpha \to B \to \operatorname{coker}\alpha \to 0$ □

Corollary 72.7. *Let $A \subseteq B$ be a submodule with finite index, then $h(A) = h(B)$.*

73. 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.

Lemma 73.1 (linear independence of automorphisms)**.** *Let L/K be finite Galois, then the set $\mathrm{Aut}_K(L)$ 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 $f_1, \dots, f_n \in \mathrm{Aut}_K(L)$ and $a_1, \dots, a_n \in L^\times$ 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. □

Lemma 73.2. *Let L/K finite Galois, $G = \mathrm{Gal}(L/K)$. Then:*

(i) $\hat{H}^0(G, L) = \hat{H}^1(G, L) = 0$;
(ii) $\hat{H}^0(G, L^\times) \cong K^\times / \mathrm{N}(L^\times)$, and $\hat{H}^1(G, L^\times)$ is trivial.

Proof. For (i): first, since $\ker(\sigma - 1 : L \to L) = L^G = K$, and $\mathrm{im}(N_G) = \mathrm{im}(\mathrm{Tr}_{L/K}) = K$ (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 $\mathrm{im}(N_G) = \mathrm{N}(L^\times)$. 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 $\mathrm{Gal}(L/K)$ 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 $w \mid v$.

Definition 73.3. The *decomposition group* D_w of a place $w \in M_L$ is the stabilizer

$$D_w := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(w) = w\}.$$

We know $\mathrm{Gal}(L/K)$ acts transitively on $\{w \mid v\}$, so the D_w's are conjugate.

Remark 73.4. 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 $v \in M_K$.

Definition 73.5. Let L/K be an extension of number field. Let $e_0 = \prod_{v \nmid \infty} e_v$ and $e_\infty = \prod_{v \mid \infty} e_v$, $e(L/K) = e_0 e_\infty$.

Theorem 73.6 (Herbrand unit theorem)**.** *Let L/K be a Galois extension of number fields, and let $w_1, \dots, w_{r+s}$ be the archimedean places of L. Then there exist $\varepsilon_1, \dots, \varepsilon_{r+s} \in \mathcal{O}_L^\times$, such that:*

- *$\sigma(\varepsilon_i) = \varepsilon_j \iff \sigma(w_i) = w_j$, for $\sigma \in G$;*
- *$\varepsilon_1, \dots, \varepsilon_{r+s}$ generate a finite index subgroup of $\mathcal{O}_L^\times$;*
- *$\varepsilon_1 \varepsilon_2 \dots \varepsilon_{r+s} = 1$, and all other multiplicative relations are multiples of this.*

Proof. Pick $v_1, \dots, v_{r+s} \in \mathcal{O}_L^\times$ (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 $w_1, \dots, w_m$ lie in distinct orbits. For $i = 1, \dots, r+s$, 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. □

74. The ambiguous class number formula

Lemma 74.1 (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 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 $\hat{H}_0(G, L^\times)$. □

Remark 74.2. 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, $\hat{H}^1 = \hat{H}_0$.

Corollary 74.3 (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 $\beta \in L^\times$.*

Theorem 74.4. *Let L/K finite cyclic, then*

$$h(\mathcal{O}_L^\times) = \frac{e_\infty(L/K)}{[L : K]}.$$

Proof. Let $\varepsilon_1, \dots, \varepsilon_{r+s}$ 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

$$0 \to \mathbb{Z} \to \bigoplus_{v|\infty} A_v \xrightarrow{\phi} A \to 0,$$

where ψ sends $w_i \mapsto \varepsilon_i$. We are done because $h(\mathbb{Z}) = \#G = [L : K]$. □

Lemma 74.5. *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, $\sum_{\mathfrak{q}|\mathfrak{p}} v_\mathfrak{q}(I) = 0$. Since $G = \mathrm{Gal}(L/K)$ is cyclic, we can order $\{\mathfrak{q} \mid \mathfrak{p}\} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$ 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. $I \in \mathrm{im}(\sigma - 1)$. 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 $h^0(\mathcal{I}_L) = [\mathcal{I}_L^G : N(\mathcal{I}_L)] = [\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : N(\mathcal{I}_L)] = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$. □

Theorem 74.6 (ambiguous class number formula)**.** *Let L/K be a finite cyclic extension of number fields. Then*

$$\#\,\mathrm{Cl}_L^G = \frac{e(L/K)\#\,\mathrm{Cl}_K}{n(L/K)[L : K]},$$

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

$$0 \to \mathcal{P}_L^G \to \mathcal{I}_L^G \to \mathrm{Cl}_L^G \to H^1(\mathcal{P}_L) \to 0,$$

since $H^1(\mathcal{I}_L) \cong \hat{H}_0(\mathcal{I}_L) = 0$. Therefore, $\#\,\mathrm{Cl}_L^G = h_0(\mathcal{P}_L) \cdot [\mathcal{I}_L^G : \mathcal{P}_L^G]$.

Consider the inclusions $\mathcal{P}_K \subseteq \mathcal{P}_L^G \subseteq \mathcal{P}_L$, so

$$[\mathcal{I}_L^G : \mathcal{P}_L^G] = \frac{[\mathcal{I}_L^G : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{[\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{e_0(L/K)\#\,\mathrm{Cl}_K}{[\mathcal{P}_L^G : \mathcal{P}_K]}.$$

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

$$\frac{h^0(\mathcal{O}_L^\times)}{h_0(\mathcal{P}_L)} = \#\,\mathrm{im}\, f = [\mathcal{O}_K^\times : \mathrm{N}(L^\times) \cap \mathcal{O}_K^\times].$$

Therefore,

$$\#\,\mathrm{Cl}_L^G = \frac{h_0(\mathcal{P}_L)e(L/K)\#\,\mathrm{Cl}_K}{h_0(\mathcal{O}_L^\times)[L : K]} = \frac{e(L/K)\#\,\mathrm{Cl}_K}{n(L/K)[L : K]},$$

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 $\#\,\mathrm{Cl}_L[2] = \frac{e_0(L/K)}{2}$, i.e. its $\mathbb{Z}/2\mathbb{Z}$-rank is $\#\{p \mid D\} - 1$. This has applications in factoring integers.

75. First main inequality of CFT

Lemma 75.1. *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:

Theorem 75.2 (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. □

Corollary 75.3 (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 66.7, 75.2. 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.

76. Local CFT

In this section 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

$$K^{\text{ab}} = \bigcup_{L \subseteq K^{\text{sep}} : L/K \text{ finite abelian}} L$$

$$K^{\mathrm{unr}} = \bigcup_{L \subseteq K^{\mathrm{sep}} : L/K \text{ finite unramified}} L$$

be the maximal abelian and unramified extensions of K (inside K^{sep}), so $K \subseteq K^{\mathrm{unr}} \subseteq K^{\mathrm{ab}} \subseteq K^{\mathrm{sep}}$. 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

$$\{\text{extensions } L/K \text{ in } K^{\mathrm{ab}}\} \longleftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(K^{\mathrm{ab}}/K)\}$$

$$\{\text{Galois extensions}\} \longleftrightarrow \{\text{closed normal subgroups}\}$$

$$\{\text{finite extensions}\} \longleftrightarrow \{\text{open subgroups}\}.$$

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 $\psi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$.

Theorem 76.1 (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 $K^\times/\mathrm{N}_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$.*

Remark 76.2. 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.

Definition 76.3. 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.

Remark 76.4. 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.

Corollary 76.5. *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. □

Corollary 76.6. *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 $\mathrm{N}(L^\times) \le H \le K^\times$. 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 $\mathrm{N}(F^\times) \cong H$. □

Lemma 76.7. *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 76.7, 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. □

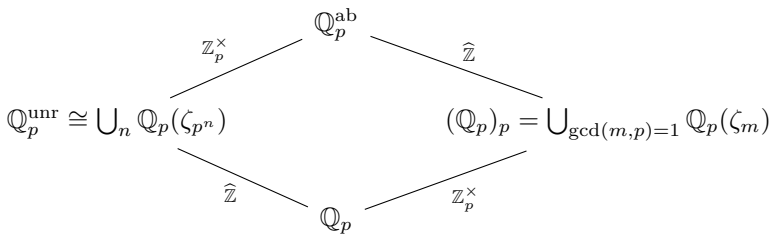
When K is archimedean, $\widehat{K^\times}$ is either trivial ($K = \mathbb{C}$) or has order 2 ($K = \mathbb{R}$). So we focus on the nonarchimedean case. By picking a uniformizer π, we get a non-canonical isomorphism $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$. So $\widehat{K^\times} \cong \widehat{\mathcal{O}_K^\times} \times \widehat{\mathbb{Z}} = \mathcal{O}_K \times \widehat{\mathbb{Z}}$, 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

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \theta_K} & & \downarrow{\scriptstyle \phi} & & \\
1 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}}) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{unr}}/K) & \longrightarrow & 1
\end{array}$$

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 $\pi \in \mathrm{N}(L^\times)$.

Example 76.8. 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:



77. Global CFT via idèles

Let K be a global field. Recall the group of idèles

$$\mathbb{I}_K = \mathbb{A}_K^\times := \prod_v{}' (K_v^\times, \mathcal{O}_v^\times).$$

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & C_K & \longrightarrow & 1 \\ & & {\scriptstyle x\mapsto(x)}\downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \\ 1 & \longrightarrow & \mathcal{P}_K & \longrightarrow & \mathcal{I}_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 1 \end{array}$$

where C_K is the idèle class group.

Definition 77.1. Given finite separable L/K, define the norm map

$$\mathrm{N}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$$

mapping

$$(a_w)_w \mapsto \left(\prod_{w|v} \mathrm{N}_{L_v/K_w}(a_w) \right)_v.$$

This behaves well with the other norm maps:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathcal{I}_L \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle N} \\ K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathcal{I}_K, \end{array}$$

so this induces a map

$$\begin{array}{ccc} C_L & \twoheadrightarrow & \mathrm{Cl}_L \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ C_K & \twoheadrightarrow & \mathrm{Cl}_K. \end{array}$$

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

$$\theta_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Definition 77.2. This is called the *global Artin homomorphism*.

Proposition 77.3. *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*

$$\begin{array}{ccc} K_w^\times & \xrightarrow{\theta_{L_w/K_v}} & \mathrm{Gal}(L_w/K_v) \\ \downarrow{\scriptstyle i_v} & & \downarrow{\scriptstyle \phi_w} \\ \mathbb{I}_K & \xrightarrow{\theta_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. □

Now we are ready to state the main theorems of the idèle-theoretic formulation of global CFT.

Theorem 77.4 (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*

$$\begin{array}{ccc} C_L & \xrightarrow{\theta_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ C_K & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

commutes.

Remark 77.5. There is then an inclusion-reversing bijection

$$\{\text{finite index open subgroups } H \leq C_K\} \longleftrightarrow \{\text{finite abelian extensions } L/K \text{ in } K^{\mathrm{ab}}\}$$

$$H \mapsto (K^{\mathrm{ab}})^{\theta_K(H)}$$
$$\mathrm{N}_{L/K}(C_L) \hookleftarrow L.$$

Remark 77.6. 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 67.1). 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.

78. Dimension shifting

In the next few sections 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 $\mathrm{Gal}(L/K) \cong \hat{H}^0(\mathrm{Gal}(L/K), L^\times)$.

Definition 78.1. 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).

Lemma 78.2. *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 $\mathbb{Z}[G]$.

Lemma 78.3. *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:

Theorem 78.4 (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.

Proposition 78.5. *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 $\hat{H}^0$. □

Corollary 78.6. *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. □

Corollary 78.7. *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. □

79. 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

$$\varphi_n : H_n(H, \mathrm{Res}^G_H(A)) \to H_n(G, A), \quad \varphi^n : H^n(G, A) \to H^n(H, \mathrm{Res}^G_H(A)).$$

Definition 79.1. 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

$$H^n(G, B) \xrightarrow{\varphi^n} H^n(H, B) \xrightarrow{\phi^n} H^n(H, A).$$

Definition 79.2. 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 $\phi : A \xrightarrow{\mathrm{id}} A$.

Example 79.3. 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.

Definition 79.4. 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

$$N_{G/H} := \sum_{s \in S} s \in \mathbb{Z}[G], \quad N_{G/H}^{-1} := \sum_{s \in S} s^{-1} \in \mathbb{Z}[G].$$

Define a restriction map on homology by

$$\begin{aligned} \mathrm{Res} : H_0(G, A) &\to H_0(H, A) \\ a + I_G A &\mapsto N_{G/H}^{-1} a + I_H A \end{aligned}$$

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

$$\begin{array}{ccc} H_0(G, A) & \xrightarrow{\alpha_0} & H_0(G, B) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ H_0(H, A) & \xrightarrow{\alpha_0} & H_0(H, B) \end{array}$$

commutes.

If G is finite, then $\mathrm{Res}(\ker \hat{N}_G) \subseteq \ker \hat{N}_H$, so we have an induced map

$$\hat{H}_0(G, A) \to \hat{H}_0(H, A).$$

Similarly, define the corestriction for cohomology

$$\begin{aligned} \mathrm{CoRes} : H^0(H, A) &\to H^0(G, A) \\ a &\mapsto N_{G/H} a \end{aligned}$$

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 $0 \to I_G \otimes_{\mathbb{Z}} A \to \mathrm{Ind}^G(A) \to A \to 0$, we can uniquely extend

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_1(G, A) & \longrightarrow & H_0(G, I_G \otimes_{\mathbb{Z}} A) & \longrightarrow & H_0(G, \mathrm{Ind}^G(A)) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \exists!} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\ 0 & \longrightarrow & H_1(H, A) & \longrightarrow & H_0(H, I_G \otimes_{\mathbb{Z}} A) & \longrightarrow & H_0(H, \mathrm{Ind}^G(A)) & \longrightarrow & 0 \end{array}$$

and similarly dimension shifting gives maps $\mathrm{Res} : H_n(G, A) \to H_n(H, A)$.

Similarly, we get $\mathrm{CoRes} : H^n(H, A) \to H^n(G, A)$. Restriction and corestriction are transitive and δ-functorial.

Proposition 79.5. *Let A be a G-module, $H \leq G$ fintie index, then* $\mathrm{CoRes} \circ \mathrm{Res}$ *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. □

80. Inflation

Definition 80.1. 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*

$$\mathrm{Inf} : H^n(G/H, A^H) \to H^n(G, A)$$

and the map induced by $\varphi : G \to G/H$ and $\phi : A \to A_H$ is the *coinflation*

$$\mathrm{CoInf} : H_n(G, A) \to H_n(G/H, A_H).$$

These are also δ-functorial.

Example 80.2. In degree $n = 0$, Inf and CoInf are just the identity maps on A_G and A^G.

Example 80.3. Let $f : G^n \to A$ be a n-cochain representing $\gamma \in H^n(G, A)$. Then $\mathrm{Res}(\gamma) \in H^n(H, A)$ 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 $\mathrm{Inf}(\gamma) \in H^n(G, A)$ is given by composing f with the projection $G^n \to (G/H)^n$.

Theorem 80.4 (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*

$$0 \to H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A)$$

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 $\gamma \in \ker \text{Inf}$. 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, $\text{im Inf} \subseteq \ker \text{Res}$. To show equality, let $f : G \to A$ be a 1-cochain representing $\gamma \in \ker \text{Res}$. 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 $\text{Hom}_{\mathbb{Z}}(I_G, A)$ satisfies the hypothesis for n. By inductive hypothesis,

$$0 \to H^n(G/H, \text{Hom}_{\mathbb{Z}}(I_G, A)^H) \xrightarrow{\text{Inf}} H^n(G, \text{Hom}_{\mathbb{Z}}(I_G, A)) \xrightarrow{\text{Res}} H^n(H, \text{Hom}_{\mathbb{Z}}(I_G, A))$$

is exact. By dimension shifting again,

$$0 \to H^{n+1}(G/H, A^H) \xrightarrow{\text{Inf}} H^{n+1}(G, A) \xrightarrow{\text{Res}} H^{n+1}(H, A)$$

is exact. □

Remark 80.5. There is an analogous theorem for CoRes and CoInf:

$$H_n(H, A) \xrightarrow{\text{CoRes}} H_n(G, A) \xrightarrow{\text{CoInf}} H_n(G/H, A_H) \to 0$$

is exact, if $H_i(H, A) = 0$ for $1 \leq i \leq n-1$.

81. Tate's theorem

Theorem 81.1. *Let A be a G-module, where G is finite. Suppose for all $H \leq G$, 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 $n \geq 1$ (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 $n \geq 1$, 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

$$H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A) \xrightarrow{\text{CoRes}} H^n(G, A)$$

which is multiplication by $(G:H)$, a number coprime to p. But for $n \geq 1$, 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 $n \geq 1$. 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. □

Theorem 81.2 (Tate's theorem)**.** *Let A be a G-module where G finite, and suppose for every $H \leq G$, $H^1(H,A) = 0$ 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 81.2. 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 81.1, 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. □

82. Continuous cohomology

Let us switch gears to developing more cohomology theory, this time for profinite (more generally, topological) groups, taking the topology into account.

Definition 82.1. 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.

Lemma 82.2. *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 $a \in A$, $\mathrm{Stab}(a)$ 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 $\mathrm{Stab}(a)$ is open. Since G is compact, $\mathrm{Stab}(a)$ has finite index, hence finitely many conjugates; their intersection 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.

Lemma 82.3. *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)!

Theorem 82.4. *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.

83. Cohomology of profinite groups

Definition 83.1. 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

$$\mathrm{Inf} : H^n(G/K, A^K) \to H^n(G/H, A^H).$$

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 $H^n(G/N, A^N)$.

Theorem 83.2. *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 $(G/N)^n \to A^N$. □

Corollary 83.3. *For every profinite G and discrete G-module A, $H^n(G, A)$ is torsion for all $n \geq 0$.*

Proof. By proposition 78.5, each $H^n(G/N, A^N)$ is torsion. The direct limit of torsion abelian groups is torsion as well. □

Corollary 83.4 (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 73.2. □

Theorem 83.5. *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. □

Definition 83.6. 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:

Theorem 83.7 (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*

$$0 \to H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A)$$

is exact.

Remark 83.8. 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.

Remark 83.9. 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.

84. 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 $G = \text{Gal}(L/K)$ 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:

Theorem 84.1. *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 $\hat{H}^0(G, \mathcal{O}_L^\times) = \mathcal{O}_K^\times / \operatorname{N}(\mathcal{O}_L^\times)$. 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 $G = \text{Gal}(\ell/k)$, 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 72.4). Consequently, $k^\times / \operatorname{N}(\ell^\times) = \hat{H}^0(G, \ell^\times) = 0$, so the norm map on residue fields is surjective. By Lemma 73.2, $k/\operatorname{Tr}(\ell) = \hat{H}^0(G, \ell) = 0$, so the trace map on residue fields is surjective as well.

I claim that these are sufficient to imply that $\operatorname{N}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$. Suppose we are given $u \in \mathcal{O}_K^\times$. By the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_L^\times & \xrightarrow{\bmod \mathfrak{q}} & \mathcal{O}_L^\times/U_L^1 \cong \ell^\times \\ \downarrow \text{N} & & \downarrow \text{N} \\ \mathcal{O}_K^\times & \xrightarrow{\bmod \mathfrak{p}} & \mathcal{O}_K^\times/U_K^1 \cong k^\times, \end{array}$$

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 $u/\operatorname{N}(v_1) \in U_K^1$. By the commutative diagram

$$\begin{array}{ccc} U_L^1 & \longrightarrow & U_L^1/U_L^2 \cong \ell \\ \downarrow{\scriptstyle \operatorname{N}} & & \downarrow{\scriptstyle \operatorname{Tr}} \\ U_K^1 & \longrightarrow & U_K^1/U_K^2 \cong k, \end{array}$$

we may pick $w_2 \in U_L^1$ such that $\operatorname{N}(w_2) \equiv u/N(v_1)$ modulo U_K^2. Taking $v_2 = w_2 v_1$, we see that $u/\operatorname{N}(v_2) \in U_K^2$. 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 $u/\operatorname{N}(v)$ 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 $H \leq G$, $H = \operatorname{Gal}(L/L^H)$. So we may just apply the above to the extension L/L^H. □

In the proof, we have shown the following:

Corollary 84.2. *Let L/K be finite unramified, then the norm map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.* □

Corollary 84.3. *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 $\operatorname{Gal}(L^N/K) \cong G/N$, 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 83.2). □

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 78.6). 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 $\operatorname{Frob}_{M/K}$ in any finite extension M/K in L.

Definition 84.4. The *invariant map* is defined by the composition

$$\operatorname{inv}_{L/K} : H^2(G, L^\times) \to H^2(G, \mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}.$$

Note that this is very canonical. In particular, it is functorial in L in the sense that for $K \subseteq M \subseteq L$ unramified,

$$\begin{array}{ccc} H^2(\operatorname{Gal}(M/K), M^\times) & \xrightarrow{\quad\operatorname{Inf}\quad} & H^2(\operatorname{Gal}(L/K), L^\times) \\ & {\scriptstyle \operatorname{inv}_{M/K}} \searrow \quad \swarrow {\scriptstyle \operatorname{inv}_{L/K}} & \\ & \mathbb{Q}/\mathbb{Z} & \end{array}$$

commutes.

Theorem 84.5. *The invariant map $\operatorname{inv}_K := \operatorname{inv}_{K^{\mathrm{unr}}/K}$ is the unique isomorphism*

$$\operatorname{inv}_K : H^2(\operatorname{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z},$$

such that for any finite unramified L/K in K^{unr}, composing with the inflation map gives isomorphisms

$$\operatorname{inv}_{L/K} : H^2(\operatorname{Gal}(L/K), L^\times) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

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. □

85. The invariant map: general case

Now we have to figure out how to deal with ramification.

Proposition 85.1. *Let L/K be a finite extension, not necessarily unramified and not necessarily Galois. There is a canonical homomorphism ϕ that makes*

$$\begin{array}{ccc} H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) & \xrightarrow{\phi} & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

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

$$\begin{aligned} 0 \to H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) &\xrightarrow{\mathrm{Inf}'} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/K), L^{\mathrm{unr}\,\times}) \\ &\xrightarrow{\mathrm{Res}'} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}}), L^{\mathrm{unr}\,\times}). \end{aligned}$$

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:

$$\begin{array}{ccccccc} H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}\,\times}) & \longrightarrow & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Z}) & \longrightarrow & H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \phi} & & \downarrow & & \downarrow{\scriptstyle [e]\circ\phi} & & \downarrow{\scriptstyle [L:K]} \\ H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}\,\times}) & \longrightarrow & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Z}) & \longrightarrow & H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where the leftmost square is induced by

$$\begin{array}{ccc} K^{\mathrm{unr}\,\times} & \xrightarrow{v_K} & \mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle [e]} \\ L^{\mathrm{unr}\,\times} & \xrightarrow{v_L} & \mathbb{Z}, \end{array}$$

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*:

Theorem 85.2 (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 72.5, $h(\mathbb{Z}) = n$. 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 72.7 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 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 §25), 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 71.5). In fact, they are *cohomologically trivial*, i.e. for any $H \le G$ 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)... □

Corollary 85.3. *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. □

Theorem 85.4. *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

$$\begin{array}{ccc} H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/L), K^{\mathrm{sep}\,\times}) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, and when L/K is Galois we have an isomorphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^2(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\mathrm{Inf}} & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(K^{\mathrm{sep}}/L), K^{\mathrm{sep}\,\times}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \\ 0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

86. Proof of local Artin reciprocity

Let K be a nonarchimedean local field.

Let us recall the invariant map

$$\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

which descends to

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for every finite Galois extension L/K.

We also defined the local Artin map, which is the inverse of

$$G^{\mathrm{ab}} \cong H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^0(G, L^\times) = K^\times / \mathrm{N}(L^\times).$$

The first map is an isomorphism via $G^{\mathrm{ab}} \cong I_G/I_G^2$, mapping $\overline{g} \mapsto (g-1) + I_G^2$. The last map is given by Tate's theorem 81.2, 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 $\mathrm{inv}_{L/K}$. It is nontrivial (and shown on the problem set) that the local Artin maps are all compatible, so we may define the Artin homomorphism

$$\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

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 $\sigma = \mathrm{Frob}_{L/K}$, which generates the cyclic $G = \mathrm{Gal}(L/K)$. What we need to show is, the sequence of isomorphisms (writing out the isomorphism in Tate's theorem)

$$G \cong I_G/I_G^2 = H_0(G, I_G) \xrightarrow{\delta_0^{-1}} H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\hat{\delta}_0} \hat{H}^{-1}(G, I_G) \xrightarrow{\hat{\delta}_{L/K}} \hat{H}^0(G, L^\times) = K^\times / \mathrm{N}(L^\times)$$

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 $\hat{\delta}_0 \circ \delta_0^{-1} = \mathrm{id}$. 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 $K^\times/\mathrm{N}(L^\times)$.

Let us look inside $\hat{\delta}_{L/K}$. It comes from the snake lemma

$$\begin{array}{ccccccccc} & & L_G^\times & \longrightarrow & L^\times(\varphi)_G & \xrightarrow{\alpha} & I_G/I_G^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \hat{N}_G} & & \downarrow & & \\ 0 & \longrightarrow & (L^\times)^G & \xrightarrow{\beta} & L^\times(\varphi)^G & \longrightarrow & (I_G)^G & & \end{array}$$

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 $(\mathrm{inv}_{L/K})$

$$H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z}) \xrightarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}).$$

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}).

Theorem 86.1 (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

$$\begin{array}{ccc}
L^\times & \xrightarrow{\theta_{M/L}} & H^{\mathrm{ab}} = H/[H,H] \\
\downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \iota} \\
K^\times & \xrightarrow{\theta_{M/K}} & G^{\mathrm{ab}} = G/[G,G] \\
\| & & \downarrow{\scriptstyle \pi} \\
K^\times & \xrightarrow{\theta_{E/K}} & \mathrm{Gal}(E/K) = G/[G,G]H.
\end{array}$$

Consider any $a \in \mathrm{N}_{E/K}(E^\times)$, then $a \in \ker(\theta_{E/K})$, so $\theta_{M/K}(a) \in \ker \pi = \mathrm{im}\, \iota$. 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. □

87. Lubin–Tate formal groups

See paper notes.

88. Proof of local existence theorem

89. Extensions of absolute values

The appendix collects material not covered in the lectures (but important nonetheless).

Proposition 89.1 (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 $\deg \overline{g}$.*

Corollary 89.2. *Let $f(x)$ be irreducible in $K[x]$, with degree n. Then*

$$|f| := \max(|a_0|, \ldots, |a_n|) = \max(|a_0|, |a_n|).$$

Proposition 89.3 (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 $0 < r \leq 1$.*

Theorem 89.4. *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 89.3. Assume for the rest that $|\,|$ is nonarchimedean. We will show that so is $\|\,\|$.

Lemma. *For $\beta \in L$, if $\|\beta\| \leq 1$, then $\|1 + \beta\| \leq 1$.*

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 $|f_\beta(0)| = \|\beta\|^{\deg f_\beta} \leq 1$. Then by corollary 89.2, $f_\beta(x) \in \mathcal{O}_K[x]$.

Since the minimal polynomial of $1 + \beta$ is $f_\beta(x - 1)$,

$$\|1 + \beta\|^n = |\,\mathrm{N}_{L/K}(1 + \beta)| = |((-1)^{\deg f_\beta} f_\beta(-1))^{[L:K(\beta)]}| \leq 1,$$

which proves the lemma. □

By the lemma, if $\|\alpha\| \leq \|\beta\|$, we then have $\|\alpha + \beta\| = \|\beta\| \left\|1 + \alpha\beta^{-1}\right\| \leq \|\beta\|$, 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 $\overline{K}$.

90. Cyclotomic fields

Let n be a positive integer, ζ_n a primitive root of unity. The goal in this section is to show:

Theorem 90.1. *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 90.1 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 $\mathbb{Q}(\zeta)$.

Proposition 90.2. $\mathbb{Z}[\zeta] \cap p\mathcal{O} = p\mathbb{Z}[\zeta]$.

Proposition 90.3. $\operatorname{disc} \mathbb{Z}[\zeta]$ *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 90.2. It is clear that $\mathbb{Z}[\zeta] = \mathbb{Z}[1 - \zeta]$, and $(1 - \zeta)^i$ $(0 \leq i \leq p^{r-1}(p - 1) - 1)$ forms a $\mathbb{Z}$-basis for $\mathbb{Z}[1 - \zeta]$.

Lemma. $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = p$.

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 $\mathrm{N}(1-\zeta) = p$, $p \in (1-\zeta)$, 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 $p \mid c_0, \ldots, c_{i-1}$. 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 90.3. $\operatorname{disc}\mathbb{Z}[\zeta] = \operatorname{disc}(1, \zeta, \ldots, \zeta^{p^{r-1}(p-1)-1})$, which is equal to $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(P'(\zeta))$ 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 90.1 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.

91. Kummer theory

Definition 91.1. 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 $f : g \mapsto gx - x$ $(x \in M)$.

Theorem 91.2 (Hilbert's theorem 90)**.** *Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$, 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 $a = b/\sigma(b)$.

Theorem 91.3. *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 $\mathrm{Gal}(K(\alpha^{1/n})/K) \to \mathbb{Z}/n\mathbb{Z}$. 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 $\mathbb{Z}/n\mathbb{Z}$. □

Definition 91.4. Let K be a field that contains ζ_n. The *Kummer pairing*

$$\mathrm{Gal}(\overline{K}/K) \times K^\times \to \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$$

is defined by: given $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $z \in K^\times$, choose $y \in \overline{K}$, with $y^n = z$, and define $\langle \sigma, z\rangle = \sigma(y)/y$.

Theorem 91.5. *The Kummer pairing induces an isomorphism*

$$K^\times/(K^\times)^n \cong \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}).$$

Proposition 91.6. *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 $\omega : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ 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.*

92. Solutions to 18.785 problem sets

(2.3) Let $d \neq 1$ be a squarefree integer, $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4; \\ \mathbb{Z}[\sqrt{d}] & \text{otherwise.} \end{cases}$$

Proof. Omitted. □

(3.1) Let A be Dedekind, K its field of fractions.

(a) Describe all nonzero A-submodules of K.

(b) Describe all subrings of K containing A.

Proof. (a) Let $M \subseteq K$ be a nonzero A-submodule, then $M_\mathfrak{p} \subseteq K$ is a nonzero $A_\mathfrak{p}$-submodule (for any nonzero prime $\mathfrak{p} \subset A$). These can only be of the form $\mathfrak{p}^n A_\mathfrak{p} = \{x \in K : v_\mathfrak{p}(x) \geq n\}$ for $n \in \mathbb{Z} \cup \{-\infty\}$. So $M = \bigcap_\mathfrak{p} M_\mathfrak{p} = \{x \in K : v_\mathfrak{p}(x) \geq n_\mathfrak{p}\}$ for some combination of $n_\mathfrak{p} \in \mathbb{Z} \cup \{-\infty\}$. But only finitely many $n_\mathfrak{p}$ could be strictly positive, since any x is contained in only finitely many primes. Conversely, if only finitely many $n_\mathfrak{p}$ are strictly positive, M is clearly nonempty. So we map the set of nonzero A-submodules of K injectively to the set of tuples $(n_\mathfrak{p})_\mathfrak{p}, n_\mathfrak{p} \in \mathbb{Z} \cup \{\infty\}$ where all but finitely many $n_\mathfrak{p} \leq 0$. To show surjectivity, it suffices to show that, given any collection of $\mathfrak{p}^{n_\mathfrak{p}} A_\mathfrak{p}$ where almost all $n_\mathfrak{p} \leq 0$,

$$\left(\bigcap \mathfrak{p}^{n_\mathfrak{p}} A_\mathfrak{p}\right)_\mathfrak{q} = \mathfrak{q}^{n_\mathfrak{q}} A_\mathfrak{q}$$

for any nonzero prime $\mathfrak{q}$. It is clear that the LHS is contained in the RHS. The reverse inclusion follows from strong approximation.

(b) Let $B \subset K$ be a subring containing A. Then it is automatically an A-module, so $B = \{x \in K : v_{\mathfrak{p}_i}(x) \geq n_i\}$ where finitely many n_i are positive. Since $A \subseteq B$, every $n_i \leq 0$. Since B is a ring, if some $n_i < 0$, then it is equal to negative infinity. So we have $B = \bigcap_{\mathfrak{p}_i} A_{\mathfrak{p}_i}$ for some collection of primes $\mathfrak{p}_i$. In particular, if A is a DVR, then $B = A$ or K. □

(3.2, Finitely generated modules over Dedekind domains)

In what follows, A is a Dedekind domain, and $K = \mathrm{Frac}(A)$.

(a) Let M be a finitely generated torsion A-module. Let $I = \mathrm{Ann}(M) \subseteq A$, then we can uniquely factor $I = \prod_i \mathfrak{p}_i^{e_i}$. By Chinese remainder theorem, $A/I = \bigoplus_i A/\mathfrak{p}_i^{e_i}$. Since M is an A/I-module, this induces a decomposition $M = \bigoplus_i M_i$, where each M_i is a $A/\mathfrak{p}_i^{e_i}$-module. Since $A/\mathfrak{p}_i^{e_i} = A_\mathfrak{p}/\mathfrak{p}_i^{e_i} A_\mathfrak{p}$ is a PID, we can use the structure theorem to write M_i as the direct sum of modules of the form A/I.

(b) Let P be a fractional ideal of A. Let $\psi : N \to P$ be a surjective homomorphism of A-modules. Let $\mathfrak{p}$ be a prime ideal of A, and consider the localized homomorphism $\psi_\mathfrak{p} : N_\mathfrak{p} \to P_\mathfrak{p}$ of $A_\mathfrak{p}$-modules. Since $P_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module, there is a local splitting $\phi_\mathfrak{p} : P_\mathfrak{p} \to N_\mathfrak{p}$. Since P is finitely presented, $\mathrm{Hom}_A(P, N)_\mathfrak{p} \cong \mathrm{Hom}_{A_\mathfrak{p}}(P_\mathfrak{p}, N_\mathfrak{p})$, so there exists $\Phi^\mathfrak{p} : P \to N$ whose localization at $\mathfrak{p}$ is equal to $s_\mathfrak{p}\phi_\mathfrak{p}$, for some $s_\mathfrak{p} \in A - \mathfrak{p}$. Then $\psi\Phi^\mathfrak{p}$ is $s_\mathfrak{p}$ times the identity on P, since it is so on the localization at $\mathfrak{p}$. Since $s_\mathfrak{p} \in A - \mathfrak{p}$, they generate the unit ideal in A, so there exist $a_\mathfrak{p}$ such that $\sum a_\mathfrak{p} s_\mathfrak{p} = 1$ (this is a finite sum). Let $\phi : N \to P$ be defined by $\phi = \sum a_\mathfrak{p} \Phi^\mathfrak{p}$, then $\psi\phi$ is the identity on P.

(c) Let M be a finitely generated torsion free A-module. Then M embeds into $M \otimes_A K = K^n$. Compose this with the projection onto the first coordinate, and let P be the image, which is a fractional ideal:

$$0 \to N \to M \to P \to 0.$$

Since P is projective, $M = N \oplus P$. Also, $N = \ker(M \to P)$ injects into K^{n-1}, so by induction we can write M as the direct sum of fractional ideals.

(d) Let M be a finitely generated A-module, and M_{tors} its torsion submodule. Then in

$$0 \to M_{\mathrm{tors}} \to M \to M/M_{\mathrm{tors}} \to 0,$$

since M/M_{tors} is torsion free and finitely generated, it is projective by the above, so $M = M_{\mathrm{tors}} \oplus M/M_{\mathrm{tors}}$.

(e) Because M is finitely generated, so is N, so N is a fractional ideal. Furthermore, for two $i_1, i_2 : M \otimes_A K \to K^n$, there exists an isomorphism $f : K^n \to K^n$ such that $f \circ i_1 = i_2$, so the fractional ideal induced by i_2 is exactly $\det f$ times the fractional ideal induced by i_1. Therefore, N is unique up to multiplication by a principal ideal.

(f) Embed $I_1 \oplus \cdots \oplus I_n \hookrightarrow K^n$ naturally. Then by definition the Steinitz class is generated by $i_1 \dots i_n$, where $i_1 \in I_1$, etc.

(g) If $I_1 \oplus \cdots \oplus I_n \cong J_1 \oplus \cdots \oplus J_m$, tensoring with K gives $m = n$, and it is clear that the two Steinitz classes are the same. Conversely, it suffices to show $I_1 \oplus \cdots \oplus I_n \cong A^{n-1} \oplus I_1 \dots I_n$. By induction, we show $I_1 \oplus I_2 \cong A \oplus I_1 I_2$. Without loss of generality, we can scale I_1, I_2 such that they are coprime integral ideals. Then there is an exact sequence

$$0 \to I_1 \cap I_2 \to I_1 \oplus I_2 \to I_1 + I_2 \to 0,$$

where $I_1 \cap I_2 = I_1 I_2$, $I_1 + I_2 = A$. Since A is free, $I_1 \oplus I_2 \cong I_1 I_2 \oplus A$ as desired.

(h) We show that $I_1 \oplus I_2 \oplus \ldots \cong A \oplus A \oplus \ldots$. Write inductively $I_n = P_n \oplus P_{n+1}^{-1}$, where $P_0 = A$. Then

$$\begin{aligned} I_1 \oplus I_2 \oplus \ldots &= (P_0 \oplus P_1^{-1}) \oplus (P_1 \oplus P_2^{-1}) \oplus \ldots \\ &= P_0 \oplus (P_1^{-1} \oplus P_1) \oplus (P_2^{-1} \oplus P_2) \oplus \ldots \\ &= A \oplus A \oplus \ldots. \end{aligned}$$

93. Solutions to 18.786 problem sets