COURSE NOTES CLASS FIELD THEORY

1. Adèles and idèles of number fields

- List of topics of first course in 10-minute segments.

(1-3) Review of algebraic number theory: Integers in number fields, Dedekind domains, factorization of prime ideals, $\sum e_i f_i = n$; finiteness of class number, Dirichlet unit theorem.

(4) p-adic numbers, definition

(5) p-adic numbers, structure of multiplicative group

(6) p-adic completions of number fields

(7) Krasner's lemma

(8) Applications of Krasner's lemma

- PAUSE

(9) Galois extensions of number fields, decomposition group, inertia group

(10) Galois extensions of p-adic fields, inertia group

(11) Artin map

(12) Adèles: basic properties

(13) Idèles: basic properties

(14) Compactness of idèles

(15) Artin map, again

(16-17) Statement of main theorems of class field theory

1.1. **Completions of number fields.**

1.1.1. *Extensions of norms.*

Proposition 1.1. *Let K be a p-adic field. Then $\mathcal{O}_K$ is a DVR.*

Proof. Because $\mathcal{O}_K$ is the ring of integers in a finite extension of $\mathbb{Q}_p$ it is a Dedekind ring. But $\mathbb{Z}_p$ has a unique maximal ideal, so $\mathcal{O}_K$ has only finitely many maximal ideals. Using the Chinese Remainder Theorem one sees this impllies $\mathcal{O}_K$ is a PID. Say $\mathfrak{m}_i$, $i = 1, \ldots, r$ is the set of maximal ideals, with $\mathfrak{m}_i = (\varpi_i)$. We will prove all the $\mathfrak{m}_i$ are equal.

Fix $\mathfrak{m} = \mathfrak{m}_i = (\varpi)$. We can localize $\mathcal{O}_K$ at $\mathfrak{m}$; let R be the corresponding subring of K. It is a DVR with maximal ideal $\mathfrak{m}_R$ and since $p \subset \mathfrak{m}$ but is not invertible in $\mathcal{O}_K$, we have $pR = \mathfrak{m}_R^e$ for some e. Now let $|\bullet|_{\mathfrak{m}}$ be the $\mathfrak{m}$-adic absolute value, normalized to coincide with $|\bullet|_p$ on $\mathbb{Q}_p$:

$$|\varpi^a|_{\mathfrak{m}} = (\frac{1}{p})^{\frac{a}{e}}.$$

Note that K is a finite-dimensional vector space over $\mathbb{Q}_p$, hence is complete with respect to any p-adic norm. Clearly $|\bullet|_{\mathfrak{m}}$ is a p-adic norm, with the property that

$$\lim_i |x|_{\mathfrak{m}}^i = 0 \Leftrightarrow x \in \mathfrak{m}_R.$$

But by the uniqueness we already showed any two p-adic norms on K define the same topology. Thus $\mathfrak{m}_R$ doesn't depend on $\mathfrak{m}$, so the maximal ideal is unique. □

Lemma 1.2. *With K as above, let $|\bullet|_1$ and $|\bullet|_2$ be two multiplicative p-adic norms on K. Then there is a positive number λ such that*

$$|\bullet|_1 = |\bullet|_2^{\lambda}.$$

Moreover, if they both restrict to the same norm on $\mathbb{Q}_p$ then $\lambda = 1$.

We have seen that they define the same topology on K. Proof in notes.

1.1.2. *Tensor product and integer rings.*

Define tensor product of free modules.

Example $\mathbb{Q} \otimes F$ where F is a finite abelian group.

1.1.3. *Krasner's lemma.*

We begin with a lemma.

Lemma 1.3. *Let L/K be a Galois extension of p-adic fields, with compatible norms $|\bullet|_L$ and $|\bullet|_K$. For any $g \in Gal(L/K)$, we have*

$$|g(x)|_L = |x|_L, \ \forall x \in L.$$

This follows immediately from the uniqueness of the extension of the norm to L.

Proposition 1.4 (Krasner's lemma)**.** *Let K be a p-adic field. Let $\alpha, \beta \in \bar{K}$. If α is closer to β than to any conjugate of α (over K), then $K[\alpha] \subset K[\beta]$.*

Proof. Let L denote the Galois closure of $K(\alpha, \beta)$. By Galois theory, it suffices to show that if $\sigma \in Gal(L/K)$ fixes β then $\sigma(\alpha) = \alpha$. But

$$|\sigma(\alpha) - \beta| = |\sigma(\alpha) - \sigma(\beta)| = |\alpha - \beta|$$

because $\sigma(\beta) = \beta$ and $|\sigma(x)| = |(x)|$ for any $x \in L$ by the preceding Lemma.

Hence by the non-archimedean property,

$$|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| \leq |\alpha - \beta|.$$

Since $\sigma(\alpha)$ is a conjugate of α over K, the hypothesis now implies that $\sigma(\alpha) = \alpha$. □

We define a norm on $K[X]$ by setting $||\sum_i a_i X^i|| = \max_i |a_i|_K$.

Lemma 1.5. *Suppose $F \subset K[X]$ is a bounded subset of monic polynomials in $K[X]$:*

$$F \subset \{f \in K[X] \mid ||f|| \leq M\}$$

for some $M > 0$ Then there is $M' > 0$ such that $|\beta|_K \leq M'$ for all $f \in F$ and all roots β of f.

Proof. Let $f \in F$ of degree n and $\beta \neq 0$ be a root of f. Thus $\sum_0^n a_i \beta^i = 0$ and thus

$$|\beta^n| \leq |a_j| \beta^j$$

for some j; so $\beta^{n-j} \leq M$. □

Now fix $f \in K[X]$ monic irreducible, $f = \prod(X - \alpha_i)$ with distinct roots in a Galois extension L. Suppose g is a second monic polynomial. We choose $\epsilon > 0$ and suppose $||f - g|| < \epsilon$ (thus g and f have the same degree). Let $F = F_\epsilon$ denote the set of such g; this is a bounded set, so by the last Lemma the set of roots β of g is bounded in norm by some M'. It then follows that for any η we can choose ϵ so that

$$\prod_i |(\beta - \alpha_i)|_K = |f(\beta)|_K = |(f - g)(\beta)|_K \leq \eta$$

for all roots β of any $g \in F_\epsilon$ (because $|(f - g)(\beta)|_K$ is bounded by $\epsilon \cdot M'$). It follows that at least one $|(\beta - \alpha_i)|_K$ must be small, and we can choose η so that

$$|(\beta - \alpha_i)|_K < |\alpha_i - \alpha_j|_K$$

for all $i \neq j$. Say β belongs to α_i; then Krasner's lemma implies $K[\alpha_i] \subset K[\beta]$. But since f is irreducible and g has the same degree as f, we must have $K[\alpha_i] = K[\beta]$ and g is irreducible.

Corollary 1.6. *Let $K/\mathbb{Q}_p$ be any p-adic field. Then there is a number field E with $[E : \mathbb{Q}] = [K : \mathbb{Q}_p]$ and an embedding $E \hookrightarrow K$ that generates K over $\mathbb{Q}_p$.*

Proof. We may take K generated by the root α of f as above. Approximate f as closely as necessary by $g \in \mathbb{Q}[X]$ and let $E = \mathbb{Q}(\beta)$ where β is a root of g belonging to α. Let L be the Galois closure of $K/\mathbb{Q}_p$, and then there is an embedding $E \hookrightarrow L$ and Krasner's Lemma implies the image is contained in and generates K. □

1.1.4. *Galois theory of p-adic fields.*

Proposition 1.7. *Let L/K be an unramified extension of p-adic fields. Then L is a Galois extension and is generated by roots of unity of order prime to p.*

Proof. Say k_L/k_K is the extension of residue fields, so $[L : K] = f = [k_L : k_K]$, with $q = k_K$. Clearly $k_L = k_K(\zeta_{q^f-1})$. On the other hand, every element of $\mathcal{O}_L$ is a power series in a uniformizer of K with coefficients in $\omega(k_L)$, which are roots of unity of order prime to p. So L is Galois over K. □

The *maximal unramified extension* of K is thus the extension generated by all roots of 1 of order prime to p, and is abelian with Galois group isomorphic to $Gal(\bar{k}_K/k_K) \xrightarrow{\sim} \hat{\mathbb{Z}}$ with topological generator $Frob_q$.

Structure of $K^\times$. The valuation homomorphism $val : K^\times/O^\times \xrightarrow{\sim} \mathbb{Z}$ with $val(\varpi) = 1$ for any uniformizing parameter ϖ.

1.2. Adèles and idèles of $\mathbb{Q}$.

1.2.1. *Topology.*

Definition 1.8. Topology on $\mathbf{A}$

Proposition 1.9. *The inclusion of $\mathbb{Q}$ in $\mathbf{A}$ is discrete and $\mathbf{A}/\mathbb{Q}$ is compact.*

Definition 1.10. Haar measure

1.2.2. *Product formula.* DONE

1.3. **Adèles and idèles of number fields.**

Proposition 1.11. *The inclusion of K in $\mathbf{A}_K$ is discrete and $\mathbf{A}_K/K$ is compact.*

Proof. Discreteness: proved in class.

Let $C = C_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v \subset \mathbf{A}_K$, where C_∞ is a compact fundamental domain in K_∞ for the integers $\mathcal{O}_K$. To prove that $\mathbf{A}_K/K$ is compact, we need to show that $C+K = \mathbf{A}_K$, in other words, that $\mathbf{A}_{K,S} \subset C+K$ for every finite set S of finite primes. Let $\mathcal{O}_{(S)}$ denote the subset of $k \in K$ such that $k \in \mathcal{O}_{v'}$ for $v' \notin S$. We first prove that $\mathcal{O}_{(S)}$ is dense in $\prod_{v\in S} K_v$, and moreover, that Indeed, $\mathcal{O}_K$ is dense in $\prod_{v\in S} \mathcal{O}_v$ by the Chinese remainder theorem. So let $(a_v) \in \prod_{v\in S} K_v$. We can find $0 \neq s \in \mathcal{O}_K$ such that $b_v = s \cdot a_v \in \mathcal{O}_v$ for all $v \in S$. Let $S' \supset S$ be the set of primes dividing s (plus all those in S if necessary) and let

$$M = \sup_{v\in S} ||s||^{-1}.$$

For $v' \in S' \setminus S$ we let $b'_v = a'_v = 0$. By the previous observation, for any $\epsilon > 0$ there exists $r \in \mathcal{O}_v$ such that, for all $v \in S'$,

$$||r - b_v||_v < \frac{\epsilon}{M}.$$

Thus, letting $k = \frac{r}{s}$, we have

$$||k - a_v||_v = ||\frac{r}{s} - \frac{b_v}{s}||_v = ||s||_v^{-1} \cdot ||r - b_v||_v < M \cdot \frac{\epsilon}{M} < \epsilon$$

for all $s \in S'$; in particular, $k \in \mathcal{O}_{v'}$ for $v' \in S' \setminus S$. Thus $k \in \mathcal{O}_{(S)}$. This proves the claim.

(State Artin-Whaples and Strong Approximation.)

In the proof, we have found elements θ_i such that

$$|\lim_r \frac{\theta_i^r}{1+\theta_i^r}|_j = \delta_{ij}.$$

We want to find a $\xi \in K$ such that

$$|\xi - \alpha_i|_i < \epsilon, \forall i.$$

Let $a_i \in K$ with $|a_i - \alpha_i|_i < \epsilon/2$ and define

$$\xi = \sum_j \frac{\theta_j^r}{1+\theta_j^r} a_j$$

for very large r. Then

$$|\xi - \alpha_i|_i \leq |\xi - a_i|_i + |a_i - \alpha_i|_i.$$

We can disregard the second term. Then

$$|\xi - a_i|_i \leq \sum_{j \neq i} |\frac{\theta_j^r}{1+\theta_j^r} a_j|_i + |\frac{\theta_i^r}{1+\theta_i^r} a_i - a_i|_i$$

All but the last term are close to 0 and the final term is about $|a_i|_i \cdot \epsilon$.

Now let $(a_v) \in \mathbf{A}_{K,S}$. Choose $k \in \mathcal{O}_{(S)}$ such that $||k - a_v|| \leq 1$ for $v \in S$. Then

$$(b_v) = (a_v - k) \in K_\infty \times \prod_{v \nmid \infty} \mathcal{O}_v.$$

Thus it remains to show that there exists $r \in \mathcal{O}_K$ such that $r + (b_v) \in C$. But this is clear. □

1.3.1. *Product formula and Haar measure.*

1.3.2. *The idèle class group and the Artin map.*

1.3.3. *Minkowski's theorem.*

1.3.4. *Trace and discriminant.* Let $S \supset R$ be an extension of p-adic integer rings with fraction fields L/K, $[L : K] = n$. The trace map $Tr_{L/K} : S \to R$, but elements of L may have trace in R without being in S. Let

$$B : L \times L \to K; B(x, y) = Tr_{L/K}(xy).$$

This is a non-degenerate symmetric bilinear form. Thus the R-dual of S with respect to B:

$$\mathfrak{d}_{L/K}^{-1} = \{x \in S \mid B(x, y) \in R \forall y \in S\}$$

is free of rank n over R and contains S. Then $\mathfrak{d}_{L/K}^{-1}$ is clearly a fractional ideal of S, so its inverse $\mathfrak{d}_{L/K}$ is called the *different* of S/R. We let $D_{L/K} = N_{L/K}(\mathfrak{d}_{L/K})$; this is an integral ideal of R.

For now we write $\mathfrak{d}$ and D for short. If $M \supset N$ is a pair of free R modules of rank n then there is a linear transformation $A \in M(n, R)$ such that $A \cot M = N$. We write $[M : N] = \det(A) \cdot R$; the ideal doesn't depend on the choice of A.

Lemma 1.12. $D = [\mathfrak{d} : S] = [S : \mathfrak{d}]$.

Proof. Suppose $\mathfrak{d} = \mathfrak{m}_S^{-a}$ for some $a \geq 0$. Then $D = N_{L/K}(\mathfrak{m}_S)^a$. But $[\mathfrak{m}_S^{-a} : S] = [S : \mathfrak{m}_S^a] = [S : \mathfrak{m}_S]^a$ so it suffices to show that $[S : \mathfrak{m}_S] = N_{L/K}(\mathfrak{m}_S)$. It suffices to show that

$$N_{L/K}(J) = [S : J]$$

for any ideal $J \subset S$. But $J = (a)$ is principal and $[S : J] = (\det A_a) = (N_{L/K}(a))$ because J is the image of S under multiplication by a. □

Lemma 1.13. *Let S be free over R with basis $\{u_i\}$. Then D is the principal ideal* $(\det B(u_i, u_j))$.

Proof. Let $\{v_i\} \subset L$ be the dual basis of $\{u_i\}$ and let A be the matrix with $A(v_i) = u_i$. Then $[\mathfrak{d} : S] = (\det(A))$. But

$$\det B(u_i, u_j) = \det B(u_i, A(v_j)) = \det(A) \det B(u_i, v_j) = \det(A).$$

□

Lemma 1.14. *Suppose $S = R[x]$ where x is the root of a polynomial g of degree n. Then $D = (N_{L/K}(g'(x))$.*

In fact $D = \det tr_{L/K}(x^i x^j)$ and $g'(x) = \prod_k (x - x_k)$ where the x_k are the other roots of g. Then this relation can be found in "any old-fashioned book on algebra."

Theorem 1.15. *L/K is unramified if and only if $\mathfrak{d}_{L/K} = S$ if and only if $D_{L/K} = R$.*

The equivalence of the last two is clear. Suppose first L/K is unramified, so S is generated over R by the lifts u_i of a basis $\bar{u}_k$ of k_L/k_K. Now tr_{k_L/k_K} defines a non-degenerate bilinear form on $k_L \times k_L$ because k_L/k_K is separable. Indeed, this follows from the previous lemma, with R replaced by k_K, because $g'(x) \neq 0$ if g is a separable polynomial.

Now suppose $D = R$. In Cassel-Fröhlich, p. 20, Proposition 4, it is proved that $val_K(D) \geq (e-1)f$ by considering the inclusion

$$N = \mathfrak{m}_L/\mathfrak{m}_K \subset A = S/\mathfrak{m}_K,\ B = k_L = A/N.$$

Since A is filtered by a sequence of ideals N^i with associated graded isomorphic to k_L^e, it follows that for any $a \in A$ with image $\bar{a} \in k_L$,

$$Tr_{A/k_K} a = eTr_{k_L/k_K}(\bar{a}).$$

Now $\dim_{k_K} A = ef$, $\dim_{k_K} N = (e-1)f$. Choose a basis a_i of A so that the first $(e-1)f$ elements form a basis of N. Lift the a_i to $u_i \in S$; then the first $(e-1)f$ rows of the matrix $(Tr_{L/K}(u_i u_j)$ all belong to $\mathfrak{m}_K$. Thus the determinant of the matrix is divisible by $\mathfrak{m}_K^{(e-1)f}$, which proves the claim. So if $D = R$ then $(e-1)f = 0$, i.e. $e = 1$ and L/K is unramified.

1.4. **Finiteness of class group and unit theorem.**

1.4.1. *Compactness of the unit idèle class group.* In what follows, K is any number field. For $\mu > 1$ define

$$(\mathbf{A}_K^\times)_\mu = \{x \in \mathbf{A}_K^\times \mid \mu^{-1} \leq ||x||_{\mathbf{A}} \leq \mu.\}$$

Proposition 1.16. *Let $a \in \mathbf{A}_K^\times$. Let dh denote a Haar measure on $\mathbf{A}_K$, and consider the measure dh_a on $\mathbf{A}_K$ defined by*

$$\int_{\mathbf{A}_K} \phi(x) dh_a = \int_{\mathbf{A}_K} \phi(a^{-1}x) dh.$$

Then $dh_a = ||a||_{\mathbf{A}} dh$.

Proof. We know that $dh_a = \nu(a)dh$ for some homomorphism from $\mathbf{A}_K^\times$ to $\mathbb{R}^+$. So it suffices to check on elements of each local factor K_v. Since this is well known at archimedean primes (by the chain rule), it comes down to checking when ϕ is the characteristic function 1_v of O_v, and $a \in K_v^\times$, then the local Haar measure $dh_{v,a} = ||a||_v dh_v$. Clearly $O_v^\times \subset \ker \nu$ so it suffices to check for a uniformizer π of K_v that $\nu(\pi) = Nv^{-1}$. In other words, that

$$\int_{K_v} 1_v(\pi^{-1}x) dh = Nv^{-1}.$$

But the left hand side is the volume of $\{x \mid \pi^{-1}x \in O_v\} = m_v$ which is $[O_v : m_v]^{-1} = Nv^{-1}$. □

Lemma 1.17 (Minkowski's lemma)**.** *Let G be a locally compact group with a Haar measure dg. Let $\Gamma \subset G$ be a discrete subgroup such that $\Gamma\backslash G$ is compact. Let $X \subset G$ be a measurable subset such that*

$$\int_X dg > \int_{\Gamma\backslash G} dg.$$

Then there exist two elements $g \neq h \in X$ such that $g^{-1}h \in \Gamma$.

Theorem 1.18. *For any $\mu \geq 1$, $(\mathbf{A}_K^\times)_\mu$ is a closed subset of $(\mathbf{A}_K^\times)$. The quotient of $(\mathbf{A}_K^\times)_\mu$ by $K^\times$ is compact.*

Proof. That it is closed follows from the continuity of the function $|| \bullet ||_{ad}$. We prove compactness by a version of Minkowski's proof. First we assume $\mu > 1$. Consider the compact group $\mathbf{A}_K/K$. It has a unique Haar measure that gives it total measure 1. But $\mathbf{A}_K$ itself is not compact, so we can choose a compact subset $C \subset \mathbf{A}_K$ with measure $> \mu$. (For example, take any compact subset and then expand it by multiplying it by a sufficiently large power of p^{-1} in $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$.) Let

$$s : \mathbf{A}_K \times \mathbf{A}_K \to \mathbf{A}_K; m : \mathbf{A}_K \times \mathbf{A}_K \to \mathbf{A}_K;\ s(x,y) = x - y; m(x,y) = x \cdot y.$$

Define

$$C' = s(C \times C), C'' = m(C' \times C').$$

Since s and m are continuous, both C' and C'' are compact.

Now take $a \in (\mathbf{A}_K^\times)_\mu$. Since $||a||_{\mathbf{A}} > \mu^{-1}$, it follows that $a \cdot C$ has measure > 1. Thus it follows from Minkowski's lemma that there are two elements $x \neq y \in C$ such that $s(ax, ay) = a(x - y) \in K^\times$. Let $c = x - y$, $d = ac$ so that $c \in C'$, $d \in K^\times$. Similarly, since $||a||_{\mathbf{A}} < \mu$, multiplication by a^{-1} has modulus $> \mu^{-1}$ and so again, $a^{-1} \cdot C$ has measure 1 there is $c' \in C'$, $d' \in K^\times$ such that $d' = a^{-1}c'$. It follows that

$$dd' = cc' \in C'' \cap K^\times.$$

Since C'' is compact and K is discrete (in $\mathbf{A}_K$) the intersection $\Sigma = C'' \cap K^\times$ is a finite set, say

$$\Sigma = \{s_1, \ldots, s_M\}; cc' = s_i.$$

This implies in particular that c and c' are invertible in $\mathbf{A}_K$ and $c'^{,-1} = s_i^{-1}c$ for some $s_i \in \Sigma$.

Now we return to a: we have $ad' = c' \in C'$ but also $(ad')^{-1} = c'^{,-1} = s_i^{-1}c \in \Sigma \cdot C'$. Let

$$H = C' \times \Sigma \cdot C' \subset \mathbf{A}_K \times \mathbf{A}_K.$$

This is a compact set of $\mathbf{A}_K$ and moreover, it follows from the definition of the topology on $\mathbf{A}_K^\times$ that the inverse image of H under the map

$$\varphi : \mathbf{A}_K^\times \to \mathbf{A}_K \times \mathbf{A}_K; \varphi(x) = (x, x^{-1})$$

is a compact subset of $\mathbf{A}_K^\times$. But $\varphi(ad') \in H$; $\varphi(a) \in H \cdot (d')^{-1}$. Thus modulo $K^\times$, we have

$$(\mathbf{A}_K^\times)_\mu \subset \varphi^{-1}(H) \pmod{K^\times}.$$

Thus $(\mathbf{A}_K^\times)_\mu$ is compact modulo $K^\times$.

The above proof was for $\mu > 1$, but $\mathbf{A}_K^1/K^\times = (\mathbf{A}_K^\times)_1/K^\times$ is closed in $(\mathbf{A}_K^\times)_\mu/K^\times$ for any $\mu > 1$ so the statement is value for $\mu = 1$ as well □

1.4.2. *Finiteness of class group.* The notation of Chevalley for the idèles is J_K, and that was used by Lang and Tate in their presentations of class field theory. However, I will write $\mathcal{C}(K) = (\mathbf{A}_K^\times)/K^\times$, $\mathcal{C}(K)^1 = \mathbf{A}_K^1/K^\times$. We let $U = U_K = \prod_v O_v^\times$ where the product runs over finite places. Let $\mathbf{A}_{K,\infty}^\times = \prod_{v|\infty} K_v^\times$, and

$$\mathbf{A}_{K,\infty}^1 = \mathbf{A}_K^1 \cap \mathbf{A}_{K,\infty}^\times = \ker[\mathbf{A}_{K,\infty}^\times \to \mathbb{R}^+](a_v) \mapsto \prod_{v|\infty} ||a_v||_v.$$

Recall that $I(K)$ is the group of fractional ideals of K; it is the free abelian group generated by the finite primes. For any finite prime $\mathfrak{p}_v$

of K we have the valuation map $val_v : K_v^\times \to \mathbb{Z}$. There is a surjective map

$$\mathbf{A}_K^\times \to I(K); (a_\infty, (a_v)) \mapsto \prod \mathfrak{p}_v^{val_v(a_v)}.$$

The kernel of this map is precisely $\mathbf{A}_{K,\infty}^\times \times U$. Thus we have

$$\mathbf{A}_K^1/[\mathbf{A}_{K,\infty}^1 \times U] \xrightarrow{\sim} \mathbf{A}_K^\times/\mathbf{A}_{K,\infty}^\times \times U \xrightarrow{\sim} I(K).$$

The first isomorphism follows from the fact that the map $||\bullet||_{\mathbf{A}}$ has a splitting (right inverse) $\mathbb{R}^+ \to \mathbf{A}_{K,\infty}^\times$. Now the subgroup $K^\times \subset \mathbf{A}_K^1$ has image $P(K)$, the subgroup of principal ideals of $I(K)$. Thus there is a surjective homomorphism

$$\mathbf{A}_K^1/K^\times \to \mathbf{A}_K^1/[\mathbf{A}_{K,\infty}^1 \times U] \cdot K^\times \xrightarrow{\sim} I(K)/P(K) = Cl(K).$$

But these maps are all continuous with the discrete topology on the right (this should be checked) and the left hand side is compact. It follows that $Cl(K)$ is a discrete compact group. Hence

Theorem 1.19. *For any number field K, the group $Cl(K)$ of ideal classes of K is finite.*

1.4.3. *Unit theorem and regulator.* We can rewrite the map above as a short exact sequence of continuous maps:

$$1 \to \mathbf{A}_{K,\infty}^1/[\mathbf{A}_{K,\infty}^1 \cap K^\times U] \to \mathbf{A}_K^1/K^\times U \to Cl(K).$$

Now we describe $\mathbf{A}_{K,\infty}^1 \cap K^\times U$: it consists of elements k_∞ that can be written in the form $k \cdot u^{-1}$ where $k \in K^\times$ and $u \in U$. In other words, if $\iota : K^\times \to \mathbf{A}_K^\times$ is the natural diagonal inclusion, then

$$\iota(k) = k_\infty \cdot U.$$

This means in particular that $\iota(k) \in O_v^\times$ for all finite v, in other words that the principal ideal (k) is the unit ideal; in other words, $k \in O_K^\times$. Let $\iota_\infty : K^\times \to \mathbf{A}_{K,\infty}$ be the archimedean inclusion. Here is a consistency check:

Lemma 1.20. $\iota_\infty(O_K^\times) \in \mathbf{A}_{K,\infty}^1$.

Proof. Indeed, consider the norm map on idèles: $N_{K/Q} : \mathbf{A}_K^\times \to \mathbf{A}^\times$. Recall that

$$\mathbf{A}_{K,\infty}^1 = \ker[\mathbf{A}_{K,\infty}^\times \to \mathbb{R}^+](a_v) \mapsto \prod_{v|\infty} ||a_v||_v = ||N_{K/\mathbb{Q}}((a_v))||_\infty.$$

If $(a_v) = \iota(k)$ for some $k \in K^\times$ then we have

$$||N_{K/\mathbb{Q}}((a_v))||_\infty = ||N_{K/\mathbb{Q}}(k)||_\infty.$$

If now $k \in O_K^\times$ then $N_{K/\mathbb{Q}}(k) = \pm 1$, and this implies the Lemma. $\square$

It follows from the continuity of the short exact sequence that

Proposition 1.21. *The quotient* $\mathbf{A}^1_{K,\infty}/[\mathbf{A}^1_{K,\infty} \cap K^\times U] = \mathbf{A}^1_{K,\infty}/\iota_\infty(O_K^\times)$ *is compact.*

This is essentially Dirichlet's unit theorem. For this, we define the *regulator* map $R : \mathbf{A}_{K,\infty} \to \mathbb{R}^{r_1+r_2}$:

$$R((a_{\sigma_i}; b_{\tau_j})) = (log(|a_{\sigma_1}|), \dots, log(|a_{\sigma_{r_1}}|; log(|b_{\tau_1}|), \dots, log(|b_{\tau_{r_2}}|^2).$$

Let $H \subset \mathbb{R}^{r_1+r_2}$ be the hypersurface $\{(a_i; b_j); \sum a_i + \sum 2b_j = 0\}$. Then it follows from the definition of the norm $|| \bullet ||_v$ that

$$R(\mathbf{A}^1_{K,\infty}) = H.$$

It follows that $H/R(\iota_\infty(O_K^\times)$ is compact.

Moreover,

$$\ker R = (\pm 1)^{r_1} \times U(1)^{r_2}$$

where $U(1) \subset \mathbb{C}^\times$ is the subgroup of elements of absolute value 1. On the other hand

Lemma 1.22. $\ker R \cap \iota(O_K^\times)$ *is the group* μ_K *of roots of unity in* $K^\times$*.*

Proof. By definition, $\ker R$ is the subgroup of $\mathbf{A}_{K,\infty}$ of elements (a_v) such that $|a_v| = 1$ for all $v \mid \infty$. If $a \in O_K^\times$ is in $\ker R$ it follows that $||a||_v = 1$ for all v. But we have proved that the only algebraic numbers with this property are roots of 1. □

Theorem 1.23 (Dirichlet)**.** *Let* $\mu_K \subset O_K^\times$ *denote the group of roots of unity. Then* $O_K^\times/\mu_K$ *is a free abelian group of rank* $r_1 + r_2 - 1$*.*

2. Tate's thesis

2.1. **Fourier analysis on locally compact abelian groups.** Explain self-dual measures.

We can define $\psi_\mathbb{Q} = \psi_\infty \times \prod_p \psi_p : \mathbf{A}_\mathbb{Q}/\mathbb{Q} \to \mathbb{C}^\times$ by letting ψ_p be as before and $\psi_\infty(x) = e^{-2\pi i x}$.

Lemma 2.1. *Let* $\psi : \mathbf{A}_K \to \mathbb{C}^\times$ *be a non-trivial additive character. Then for almost all* v*, the restriction* ψ_v *of* ψ *to* K_v *is trivial on* $\mathcal{O}_v$*. Moreover,* ψ *factors as the product* $\prod_v \psi_v$*.*

Proof. Let $U \subset \mathbb{C}^\times$ be a neighborhood of 1 containing no multiplicative subgroup except the identity. The inverse image $\psi^{-1}(U)$ contains an open neighborhood of 0, thus the kernel of ψ is an open subgroup, which must thereore contain $\mathcal{O}_v$ for all $v \notin S$ for a finite S. Now let $x = (x_v) \in \mathbf{A}$ and suppose $x \in \mathbf{A}_{K,T}$ for some $T \supset S$. Write $x = x_T \times x^T$, so $\psi(x) = \psi(x_T) = \prod_{v \in T} \psi(x_v) = \prod_{v \in T} \psi_v(x_v)$. □

Lemma 2.2. *Conversely, suppose for each v we have ψ_v such that, for all $v \notin S$, $\psi_v(\mathcal{O}_v) = 1$. Then $\prod_v \psi_v$ defines a continuous character of $\mathbf{A}_K$.*

It's enough to prove that this is continuous; this is left as an exercise.

Now let $\psi(x) = \psi_{\mathbb{Q}}(Tr_{K/\mathbb{Q}}x) = \prod_v \psi_v$ with $\psi_v(x) = \psi_{\mathbb{Q}}(Tr_{K_v/\mathbb{Q}_v}\alpha_v x)$ for all v, so $\psi_v \neq 1$ for all v. For any $\alpha \in \mathbf{A}$ let $\psi_\alpha(x) = \psi(\alpha x)$. This defines a homomorphism

$$\mathbf{A} \to \hat{\mathbf{A}},\ \alpha \mapsto \psi_\alpha.$$

Theorem 2.3. *1. This homomorphism defines a (bi)-continuous isomorphism between the adele group $\mathbf{A}_K$ and its Pontryagin dual.*

2. Moreover ψ_α is trivial on K if and only if $\alpha \in K$, so this determines an isomorphism between K and $\widehat{\mathbf{A}_K/K}$.

Proof. Let $\beta = \prod_v \beta_v$ be any character of $\mathbf{A}$. Expand S so that β_v and ψ_v are trivial on $\mathcal{O}_v$ for all v outside S, and moreover such that S contains all v archimedean or ramified over $\mathbb{Q}$. Let $\beta_S = \prod_{v\in S} \beta_v$. For each $v \in S$ we have $\beta_v = \psi_{v,\alpha_v}$ for some $\alpha_v \in K_v$, by the classification of characters of local fields. On the other hand, for $v \notin S$ we also have $\beta_v = \psi_{v,\alpha_v}$ and we need to make sure that $\alpha = (\alpha_v)$ is an adèle. In other words, we want $\alpha_v \in \mathcal{O}_v$ for almost all v. But by assumption, possibly expanding S, we have

$$\beta_v(x) = \psi_{\mathbb{Q}}(Tr_{K_v/\mathbb{Q}_v}\alpha_v x)$$

is trivial for $x \in \mathcal{O}_v$. This means $Tr_{K_v/\mathbb{Q}_v}\alpha_v x \in \mathbb{Z}_v$ for all $x \in \mathcal{O}_v$ and because v is unramified over $\mathbb{Q}$ this means α_v is in $\mathcal{O}_v$. This completes the proof of point 1.

Now for point 2, first suppose $K = \mathbb{Q}$. Assume ψ_α trivial on $\mathbb{Q}$. Subtracting by an element of $\mathbb{Q}$, we may assume

$$\alpha \in [-1/2, 1/2] \times \prod_p \mathbb{Z}_p.$$

By hypothesis $\psi_\alpha(n) = 1$ for all $n \in \mathbb{Z}$, and this implies $e^{-2\pi i\alpha_\infty} = 1$, taking $n = 1$; but this implies $\alpha_\infty = 0$ because it is in $[-1/2, 1/2]$. It follows that ψ_α is trivial on $\mathbb{R} \times \prod_p \mathbb{Z}_p$; but it is also trivial on $\mathbb{Q}$, hence trivial on $\mathbf{A}_{\mathbb{Q}}$.

Now here is an abstract proof that works in general. We know that $\mathbf{A}_K/K$ is compact, hence $\Lambda = \widehat{\mathbf{A}_K/K}$ is discrete. We also know that $\Lambda \subset \mathbf{A}_K$ by the map $\alpha \mapsto \psi_\alpha$, and $K \subset \Lambda$. Thus $\Lambda/K \subset \mathbf{A}_K/K$ is a discrete subgroup of a compact group, hence is finite. On the other hand, Λ is a K-vector space: if $\lambda \in \Lambda$ and $\alpha \in K$ then

$$\psi_{\alpha\cdot\lambda}(\xi) = \psi_\lambda(\alpha\xi) = 1 \forall \xi \in K,$$

hence $\alpha \cdot \lambda \in \Lambda$. Thus Λ/K is a vector space of dimension 0. □

We write $\mathbf{A} = \mathbf{A}_K$. We let $\psi : \mathbf{A}/K \to \mathbb{C}^\times$ be a non-trivial character.

Lemma 2.4. *Let $\Phi \in L^1(\mathbf{A})$ be continuous. Suppose*

$$\Theta(x) = \Theta_\Phi(x) := \sum_{\eta \in K} \Phi(x + \eta)$$

is uniformly absolutely convergent. Then for any $\xi \in K$,

$$\hat{\Theta}(\xi) = \hat{\Phi}(\xi)$$

where the Fourier transform on the right hand side views ψ as a character of $\mathbf{A}$.

Proof. We compute:
(2.5)

$$\begin{aligned}
\hat{\Theta}(\xi) &= \int_{\mathbf{A}/K} \Theta(x)\psi(x\xi)dx \\
&= \int_{\mathbf{A}/K} \sum_{\eta \in K} \Phi(x + \eta)\psi(x\xi)dx \\
&= \int_{\mathbf{A}} \Phi(x)\psi(x\xi) \text{ [because the convergence is uniform and } \psi(\eta\xi) = 1] \\
&= \hat{\Phi}(\xi)
\end{aligned}$$

□

We write Θ_Φ for the sum above. By the Fourier inversion theorem, assuming we are using a self-dual measure on $\mathbf{A}$, we find

$$\Theta_\Phi(x) = \sum_{\xi \in K} \hat{\Theta}_\Phi(\xi)\psi(-\xi x) = \sum_{\xi} \hat{\Phi}(\xi)\psi(-\xi x).$$

Now set $x = 0$. We find

Theorem 2.6 (Poisson summation)**.**

$$\Theta_\phi(0) = \Theta_{\hat{\Phi}}(0).$$

Proof. We have

$$\Theta_\Phi(0) = \sum_{\xi} \hat{\Phi}(\xi)\psi(0) = \sum_{\xi} \hat{\Phi}(0 + \xi) = \Theta_{\hat{\Phi}}(0).$$

□

2.2. **Eigendistributions on local fields.** Let K be a local field, $\mathcal{S} = \mathcal{S}(K)$ the Schwartz space, $\mathcal{S}' = Hom_{temp}(\mathcal{S}, \mathbb{C})$. Here *tempered* means just all linear functionals when K is nonarchimedean and it means continuous in all the semi-norms $f \mapsto sup|t^n d^m f|$ if K is archimedean. There is an action of $K^\times$ on $\mathcal{S}(K)$:

$$[r(a)f](x) = f(ax)$$

and a dual action on $\mathcal{S}'$:

$$(r'(a)\lambda, f) = (\lambda, r(a^{-1})f).$$

A continuous homomorphism $\omega : K^\times \to \mathbb{C}^\times$ is called a *quasicharacter* (often just a character). There are no eigenfunctions in $\mathcal{S}$ for the action of $K^\times$ but there are eigenvectors in $\mathcal{S}'$. An eigenvector in $\mathcal{S}'$ for the quasicharacter ω is called an ω-eigendistribution.

We limit ourselves to the nonarchimedean case. Write $K = 0 \cup K^\times$ as a union of two $K^\times$ orbits. There is an injection

$$C_c^\infty(K^\times) \hookrightarrow \mathcal{S}(K)$$

and dually a short exact sequence

$$0 \to \mathcal{S}_0' \to \mathcal{S}' \to C_c^\infty(K^\times)' \to 0.$$

Why is this exact? The right-hand arrow is surjective simply by duality. Now suppose λ restricts to zero on $C_c^\infty(K^\times)$. Suppose $f \in \mathcal{S}(K)$ and $f(0) = z \neq 0$. Then there is a neighborhood U of 0 such that $f(x) = z$ for all $x \in U$. Consider the function $f_U = f - z1_U$. By hypothesis $0 = \lambda(f_U) = \lambda(f) - z\lambda(1_U)$. Moreover, if $U \subset U'$ as before then $1'_U - 1_U \in C_c^\infty(K^\times)$ so $z\lambda(1_U)$ is independent of U. It follows that the kernel $\mathcal{S}_0'$ is 1 dimensional and spanned by the δ-function supported at 0.

We can consider ω-eigendistributions in each of these spaces. For $f \in C_c^\infty(K^\times)$, define

$$Z_\omega(f) = \int_{K^\times} f(t)\omega(t)d^\times t.$$

Lemma 2.7. *The linear functional $f \mapsto Z_\omega(f)$ spans the 1-dimensional space of ω-eigendistributions in $C_c^\infty(K^\times)'$. Moreover, if $\omega \neq 1$ then $\mathcal{S}_0'(\omega) = 0$.*

Proof. If $\omega = 1$ this space is one-dimensional by uniqueness of Haar measure, and Z_1 is a non-zero element of this space. For general ω we know that

$$r'(a)(Z_\omega)(f) = Z_\omega(r(a^{-1})(f)) = \int_{K^\times} f(a^{-1}t)\omega(t)d^\times t = \int_{K^\times} f(t)\omega(at)d^\times t$$

which equals $\omega(a)Z_\omega(f)$. And by the uniqueness of Haar measure again, this space is one-dimensional.

As for $\mathcal{S}_0'(\omega)$, the action of $K^\times$ is trivial, so it equals its 1-eigenspace. □

Theorem 2.8 (Uniqueness theorem)**.** *For any quasicharacter ω of $K^\times$ the space $\mathcal{S}'(\omega)$ is one-dimensional.*

Proof. For $\omega \neq 1$ this follows from the above exact sequence: it gives rise to a short exact sequence

$$0 \to \mathcal{S}_0'(\omega) \to \mathcal{S}'(\omega) \to C_c^\infty(K^\times)'(\omega)$$

with the left-term $= 0$ and the right term of dimension 1. We need to show that $Z_\omega \in C_c^\infty(K^\times)'$ extends to en element of $\mathcal{S}'$ if and only if $\omega \neq 1$. For this we introduce a complex variable s. Define

$$Z(s,\omega,f) = \int_{K^\times} f(t)\omega(t)||t||^s d^\times t = \int_K f(t)\omega(t)||t||^{s-1}dt.$$

This integral need not converge. However, we can estimate it as before. Suppose $|\omega| = 1$ – i.e., ω is unitary – $supp(f) \subset m_K^{-N}$ and $|f| < M$. Let $q = Nv$. Then

$$|Z(s,\omega,f)| \leq \int_{K^\times} |f(t)||\omega(t)|||t||^s d^\times t \leq M \cdot \sum_{n=-N}^{\infty} q^{-sn}$$

which is bounded by an absolutely convergent geometric series provided $Re(s) > 0$. (Similarly for $K = \mathbb{R}$.) Thus for $Re(s) > 0$ we obtain a convergent $\omega(s) = \omega(t)||t||^s$-eigendistribution. Suppose ω is unramified but not necessarily unitary; then there is $b \in \mathbb{C}$ (unique modulo $2\pi/log(q)$) such that $\omega = ||\bullet||^b$. Let ϖ be a uniformizer and consider the element $\tau = [1] - [\varpi^{-1}] \in \mathbb{Z}[K^\times]$. This element acts on $\mathcal{S}$ and since any $f \in \mathcal{S}$ is constant on a neighborhood of 0, say m_K^r, we see that for $x \in m_K^{r+1}$ that $\tau(f) \in C_c^\infty(K^\times)$. Let

$$Z_\tau(s,\omega,f) = Z(s,\omega,\tau(f)).$$

This is absolutely convergent and therefore defines an $\omega(s)$-eigendistribution in $C_c^\infty(K^\times)'$. Moreover, it is entire in s. On the other hand, for $Re(s) > 0$ we can write

$$Z_\tau(s,\omega,f) = Z(s,\omega,\tau(f)) = \int_{K^\times} f(t)\omega(t)|||t||^s d^\times t - \int_{K^\times} f(\varpi^{-1}t)\omega(t)|||t||^s d^\times t$$

which equals

$$\int_{K^\times} f(t)|||t||^{s+b} d^\times t - \int_{K^\times} f(\varpi^{-1}t)|||t||^{s+b} d^\times t = (1 - ||\varpi||^{-s-b})Z(s,\omega,f).$$

Thus we have the equality of distributions:

$$Z(s,\omega) = L(s,\omega)Z_\tau(s,\omega)$$

where $L(s,\omega) = (1-\omega(\varpi)q^{-s})^{-1}$. The only pole of $L(s,\omega)$ comes where $\omega||\bullet||^s = 1$. Away from there, it defines an $\omega(s)$-eigendistribution that lifts the one we have already seen in $C_c^\infty(K^\times)'$. Setting $s = 0$, this completes the proof when $\omega \neq 1$.

Now to complete the proof, we need to show that in the case $\omega = 1$, in the exact sequence

$$0 \to \mathbb{C}\delta_0 \to \mathcal{S}'(1) \to \mathbb{C} \cdot d^\times t$$

the Haar measure $d^\times t$ doesn't lift to $\mathcal{S}$. Consider the distribution $\lambda_0 \in \mathcal{S}'$ given by

$$f \mapsto \int_{K^\times} (f - f(0)1_{\mathcal{O}})d^\times t.$$

This is invariant under $\mathcal{O}^\times$ and satisfies $\lambda_0(1_{\mathcal{O}}) = 0$. Moreover, for $f \in C_c^\infty(K^\times)$, $\lambda_0(f)$ is just the integral over $d^\times t$ and hence $r'(\varpi)\lambda_0$ and λ_0 agree on $C_c^\infty(K^\times)$. It follows that

$$r'(\varpi)\lambda_0 - \lambda_0 = c\delta_0$$

for some constant c. It remains to show that $c \neq 0$. But

$$-c = -(r'(\varpi)\lambda_0 - \lambda_0, 1_{\mathcal{O}}) = (\lambda_0, r(\tau)1_{\mathcal{O}}) = \int_{K^\times} r(\tau)1_{\mathcal{O}}d^\times t = Z_\tau(0,1,1_{\mathcal{O}}) = 1$$

by the computation of the zeta integral. □

2.2.1. *The ramified local theory.* Suppose now that ω is nontrivial on $\mathcal{O}^\times$. Let $c(\omega)$ denote the conductor of ω, the smallest integer such that ω is trivial on $U_c = 1 + m_K^c \subset \mathcal{O}^\times$.

Lemma 2.9. *Suppose ω is ramified. For sufficiently large n (depending on f), the integral*

$$Z_n(s,\omega,f) = \int_{K^\times \setminus m_K^n} f(t)\omega(t)||t||^s d^\times t$$

is independent of n and defines an $\omega(s)$-eigendistribution on $\mathcal{S}$. In particular, $Z_\infty(s,\omega) = lim_n Z_n(s,\omega)$ gives an entire analytic continuation of $Z(s,\omega)$ for ω ramified.

Proof. The point is that f is constant on m_K^n for sufficiently large n. Then the integral over $m_K^n \setminus m_K^{n-1} = \varpi^n\mathcal{O}^\times$ is just

$$f(\varpi^n)||\varpi||^{ns}\int_{\mathcal{O}^\times} \omega(t)d^\times t = 0$$

because it is the integral of a non-trivial character. □

This completes the proof in the ramified case.

2.3. **The local functional equation.** We now write $Z_0 = Z_\tau$ in the unramified case and $Z_0 = Z_\infty$ in the ramified case. In both cases $Z_0(0,\omega)$ defines a basis of $\mathcal{S}'(\omega)$ and we also have

$$Z_0(0,\omega) = \frac{Z(s,\omega)}{L(s,\omega)}$$

where $L(s,\omega) = 1$ if ω is ramified.

Now we apply the Fourier transform to an ω-eigendistribution, where if λ is a distribution, we set

$$(\hat{\lambda}, f) = (\lambda, \hat{f})$$

This definition depends on the choice of additive character ψ and Haar measure dx. We choose dx to be the *self-dual* measure relative to ψ, so that

$$\hat{\hat{f}}(x) = f(-x)$$

by Fourier inversion.

Lemma 2.10. *Suppose $\lambda \in \mathcal{S}'(\omega)$. Then $\hat{\lambda} \in \mathcal{S}'(\omega^{-1}\omega_1)$ where $\omega_1(t) = ||t||$.*

Proof. This is just the change of variables formula. We write this down, using $\mathcal{F}$ for the Fourier transform of functions. The hypothesis is that $r'(a)(\lambda)(f) = \omega(a)\cdot\lambda(f)$. Now

$$(r'(a)\hat{\lambda}, f) = (\hat{\lambda}, r(a^{-1})f) = (\lambda, \mathcal{F}(r(a^{-1})(f))).$$

We compute

$$\begin{aligned}\mathcal{F}(r(a^{-1})(f))(x) &= \int_K r(a^{-1})(f)(y)\psi(xy)dy = \int_K f(a^{-1}y)\psi(xy)dy \\ &= ||a|| \int_K f(y)\psi(axy)dy = ||a|| r(a)(\mathcal{F}(f))(x).\end{aligned}$$

Then

$$\begin{aligned}(\lambda, \mathcal{F}(r(a^{-1})(f))) =& ||a||(\lambda, r(a)\mathcal{F}(f)) = ||a||(r'(a^{-1})\lambda, \mathcal{F}(f)) \\ &= ||a||\omega(a^{-1})(\lambda, \mathcal{F}(f)) = ||a||\omega^{-1}(a)(\hat{\lambda}, f).\end{aligned}$$

□

By the uniqueness theorem we thus have that

$$Z_0(\widehat{1-s,\omega^{-1}}) = \varepsilon(s,\omega,\psi)Z_0(s,\omega)$$

for some nonzero constant $\varepsilon(s,\omega,\psi)$.

Corollary 2.11 (Local functional equation)**.** *For any $f \in \mathcal{S}$, we have the local functional equation*

$$\frac{Z(1-s,\omega^{-1},\hat{f})}{L(1-s,\omega^{-1})} = \varepsilon(s,\omega,\psi)\frac{Z(s,\omega,f)}{L(s,\omega)}.$$

2.4. **The archimedean theory.** The theory is similar, except that the space of invariant Schwartz distributions supported at 0 is infinite dimensional and spanned by the successive derivatives of the Dirac distributions, i.e. $f \mapsto f^{(n)}(0)$ for $n \geq 0$. The local L-factors are of the form $\pi^{-(s+a)/2}\Gamma(\frac{s+a}{2})$, $a = 0, 1$ depending on whether $\omega(-1) = 1$ or -1 (if $K = \mathbb{R}$) or $(2\pi)^{1-s}\Gamma(s)$ in the complex case, up to a shift.

2.5. **The global functional equation.** We have already proved the following version of the Poisson summation formula. Let $\Phi \in \mathcal{S}(\mathbf{A}_K)$, and define

$$\Theta_\Phi(x) = \sum_{\xi \in K} \Phi(x+\xi) \in C^\infty(\mathbf{A}_K/K).$$

The Fourier transform on $\mathbf{A}_K$ is defined with respect to the self-dual measure.

Theorem 2.12 (Poisson summation formula)**.** *For any $\Phi \in \mathcal{S}(\mathbf{A}_K)$, we have*

$$\Theta_\Phi(0) = \Theta_{\hat{\Phi}}(0).$$

We let $x \in \mathbf{A}_K^\times$ and define $\Phi_x(y) = \Phi(xy)$, $y \in \mathbf{A}_K$. Then

$$\hat{\Phi}_x(y) = ||x||_{\mathbf{A}}^{-1} \cdot \hat{\Phi}(x^{-1}y). \tag{2.13}$$

If $\omega : \mathbf{A}_K^\times / K^\times \to \mathbb{C}^\times$ is a quasicharacter, we define the zeta integral

$$Z(s,\omega,\Phi) = \int_{\mathbf{A}_K^\times} \omega(x)\Phi(x)||x||^s d^\times x$$

whenever this converges; we are writing $||x|| = ||x||_{\mathbf{A}}$. We may assume $|\omega| = 1$ (otherwise incorporating the norm into the s variable, and we also assume Φ is a pure tensor: $\Phi = \otimes_v \Phi_v$, where for $v \notin S$ we have $\Phi_v = 1_{\mathcal{O}_v}$. Then this integral factors over the places of K:

$$Z(s,\omega,\Phi) = \prod_v Z(s,\omega_v,\Phi_v).$$

Note that if $\Phi_v = 1_{\mathcal{O}_v}$ for all finite v, and $\omega \equiv 1$, then this is

$$\prod_{v \in S_\infty} Z(s,1,\Phi_v) \cdot \zeta_K(s)$$

where ζ_K is the Dedekind zeta function. In general, for almost all v we have

$$Z(s, \omega_v, \Phi_v) = (1 - \omega_v(\varpi_v) N v^{-s})^{-1}).$$

Thus the Euler product is bounded by the Euler product for the Dedekind zeta function, and so it converges absolutely for $Re(s) > 1$.

Now we carry out the analytic continuation and functional equation. Let $D \subset \mathbf{A}_K^1$ be a fundamental domain modulo $K^\times$, so that

$$\mathbf{A}_K^\times = \mathbb{R}_+ \times K^\times \times D \sim (SD \coprod TD) \times K^\times, \ S = (0,1), T = (1, \infty).$$

Here $\sim$ means "up to a set of measure zero." Then (in the range of absolute convergence)

$$\begin{aligned} Z(s, \omega, \Phi) &= \sum_{\xi \in K^\times} [\int_{\xi \cdot SD} \omega(x)\Phi(x)||x||^s d^\times x + \int_{\xi \cdot TD} \omega(x)\Phi(x)||x||^s d^\times x] \\ &= \sum_{\xi \in K^\times} [\int_{SD} \omega(x)\Phi_x(\xi)||x||^s d^\times x + \int_{TD} \omega(x)\Phi_x(\xi)||x||^s d^\times x] \end{aligned}$$

because $||\xi|| = \omega(\xi) = 1$ for $\xi \in K^\times$. Then this continues

$$\begin{aligned} Z(s, \omega, \Phi) &= [\int_{SD} \omega(x) \sum_{\xi \in K^\times} \Phi_x(\xi)||x||^s d^\times x + \int_{TD} \omega(x) \sum_{\xi \in K^\times} \Phi_x(\xi)||x||^s d^\times x \\ &= [\int_{SD} \omega(x)[\Theta_{\Phi_x}(0) - \Phi(0)]||x||^s d^\times x + \int_{TD} \omega(x)[\Theta_{\Phi_x}(0) - \Phi(0)]||x||^s d^\times x \\ &= [\int_{SD} \omega(x)\Theta_{\Phi_x}(0)||x||^s d^\times x + \int_{TD} \omega(x)\Theta_{\Phi_x}(0)||x||^s d^\times x] - \Phi(0)[Z(\omega)] \end{aligned}$$

where we set $\omega_s(x) = \omega(x)||x||^s$ and then

$$Z(\omega) = \int_0^\infty \int_D \omega_s(tx) d^\times x dt/t.$$

We also write

$$Z(s, \omega, \Phi) = \int_0^\infty Z_t(s, \omega, \Phi) dt/t$$

where

$$Z_t(s, \omega, \Phi) = \int_{\mathbf{A}_K^1} \omega_s(tx)\Phi(tx) d^\times x.$$

Lemma 2.14. *The integral $\int_1^\infty Z_t(s, \omega, \Phi) dt/t$ defines an entire function of s.*

Proof. The point is that for $x \in D$, $|\omega_s(tx)| = |\omega_s(t)| \cdot ||x||^s = |\omega_s(t)|$ is independent of x. For $B > 1$, $t > 1$, and $\sigma = Re(s) < B$ we have

$$|\omega_s(t)| = |t|^\sigma = |t|^B \cdot |t|^{\sigma - B} \leq |\omega_B(t)|$$

Thus
$$|\int_1^\infty \int_{\mathbf{A}_K^1} \omega_s(tx)\Phi(tx)d^\times x dt/t| \leq |\int_1^\infty \int_{\mathbf{A}_K^1} \omega_B(tx)\Phi(tx)d^\times x dt/t| \leq |Z(B,\omega,\Phi)|$$
which is an absolutely convergent integral. □

Lemma 2.15. *For all t, ω we have*
$$Z_t(s,\omega,\Phi)+\Phi(0)\int_D \omega_s(tx)d^\times x = Z_{1/t}(1-s,\omega^{-1},\hat{\Phi})+\hat{\Phi}(0)\int_D \omega_{1-s}^{-1}(x/t)d^\times x.$$

Proof. This is exactly the result of applying Poisson summation, in view of (2.13). Indeed, we write this down. The left hand side is
$$\int_D \omega_s(tx)\Theta_{\Phi_{tx}}(0)d^\times x.$$
Poisson summation identifies the theta function in the integral as
$$\Theta_{\Phi_{tx}}(0) = \Theta_{\widehat{\Phi_{tx}}}(0).$$
By (2.13)
$$\widehat{\Phi_{tx}}(\xi) = ||tx||_{\mathbf{A}}^{-1}\hat{\Phi}((tx)^{-1}\xi)$$
so that
$$\Theta_{\widehat{\Phi_{tx}}}(0) = ||tx||_{\mathbf{A}}^{-1}\sum_\xi \hat{\Phi}((tx)^{-1}\xi).$$
Inserting this in the integral for Z_t we get
$$\int_{\mathbf{A}_K^1} ||tx||_{\mathbf{A}}^{-1}\omega_s(tx)\hat{\Phi}(tx)^{-1}d^\times x$$
Exchanging x and x^{-1} this is
$$\int_{\mathbf{A}_K^1} t^{-1}\omega_s(t(x)^{-1})||x||_{\mathbf{A}}\hat{\Phi}(t^{-1}x)d^\times x$$
or
$$\int_{\mathbf{A}_K^1} \omega^{-1}(t^{-1}x)||x/t||^{-s}||x/t||\hat{\Phi}(t^{-1}x)d^\times x = \int_{\mathbf{A}_K^1} \omega^{-1}(t^{-1}x)||x/t||^{1-s}\hat{\Phi}(t^{-1}x)d^\times x.$$
And this is just the right hand side.

□

Thus if $\Phi(0) = \hat{\Phi}(0) = 0$, we have
$$\int_0^1 Z_t(s,\omega,\Phi) = \int_0^1 Z_{1/t}(1-s,\omega^{-1},\hat{\Phi}) = \int_1^\infty Z_t(1-s,\omega^{-1},\hat{\Phi})$$
which we have seen is an entire function of s; but for the same reason so is $\int_{TD}$. Thus if $\Phi(0) = \hat{\Phi}(0) = 0$ $Z(s,\omega,\Phi)$ has an analytic continuation to an entire function of s.

In general,

$$\int_a^b \int_D \omega_s(tx) d^\times x dt/t = \int_a^b \omega_s(t) \int_{\mathbf{A}_K^1/K^\times} \omega(x) d^\times x$$

and the inner integral is 0 unless $\omega \equiv 1$, in which case it equals $vol(D) = vol(\mathbf{A}_K^1/K^\times)$.

In particular, if ω is ramified at any finite place, again $Z(s, \omega, \Phi)$ is entire, and we have

$$Z(s, \omega, \Phi) = Z(1 - s, \omega^{-1}, \hat{\Phi}).$$

But this means

$$\prod_v Z(s, \omega_v, \Phi_v) = \prod_v Z(1 - s, \omega^{-1}, \hat{\Phi}).$$

Combine this with the local functional equation of distributions:

$$Z_0(\widehat{1 - s, \omega_v^{-1}}) = \varepsilon(s, \omega_v, \psi_v) Z_0(s, \omega_v)$$

Write

$$\Lambda(s, \omega) = \prod_v L(s, \omega), Z_0(s, \omega, \Phi) = \prod_v Z_0(s, \omega_v, \Phi_v)$$

which converges absolutely for $Re(s) > 1$. Thus we have an equality of distributions

$$\Lambda(s, \omega) Z_0(s, \omega) = Z(s, \omega, \bullet) = Z(\widehat{1 - s, \omega^{-1}}) = \Lambda(1-s, \omega^{-1}) Z_0(\widehat{1 - s, \omega^{-1}})$$

and applying the local functional equation, we have

$$\Lambda(s, \omega) Z_0(s, \omega) = \prod_v \varepsilon(s, \omega_v, \psi_v) \Lambda(1 - s, \omega^{-1}) Z_0(s, \omega).$$

But for any s, ω we can find Φ such that $Z_0(s, \omega, \Phi) = 1$, so this yields the global functional equation

Theorem 2.16 (Global functional equation)**.** *The product* $\varepsilon(s, \omega) = \prod_v \varepsilon(s, \omega_v, \psi_v)$ *is entire and non-vanishing and*

$$\Lambda(s, \omega) = \varepsilon(s, \omega, \psi) \Lambda(1 - s, \omega^{-1}).$$

Finally, if $\omega = 1$ we determine the poles.

$$\begin{aligned} Z(s, \omega, \Phi) &= [\int_{SD} \omega(x) \Theta_{\Phi_x}(0) ||x||^s d^\times x + \int_{TD} \omega(x) \Theta_{\Phi_x}(0) ||x||^s d^\times x] - \Phi(0)[Z(\omega)] \\ &= \int_1^\infty [Z_t(s, \omega, \Phi) + Z_t(1 - s, \omega^{-1}, \hat{\Phi})] dt/t + (vol(D)) \int_0^1 [\hat{\Phi}(0) t^{s-1} - \Phi(0) t^s] dt/t \\ &= \int_1^\infty [Z_t(s, \omega, \Phi) + Z_t(1 - s, \omega^{-1}, \hat{\Phi})] dt/t + (vol(D))[\frac{\hat{\Phi}(0)}{s - 1} - \frac{\Phi(0)}{s}]. \end{aligned}$$

The integral on the left is entire, as we have seen, but if $\omega = 1$ then $\Phi(0) = 1$, $\hat{\Phi}(0) = \sqrt{|D_K|}^{-1}$ for our choice of Φ and therefore the residue at $s = 1$ is precisely $vol(\mathbf{A}_K^1/K^\times)$:

Theorem 2.17. *The Dedekind zeta function of K has a pole at $s = 1$ (resp. at $s = 0$) with residue $vol(\mathbf{A}_K^1/K^\times)\sqrt{|D_K|}^{-1}$ (resp. $-vol(\mathbf{A}_K^1/K^\times)$), which equals precisely*

$$\frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\mu_K \sqrt{|D_K|}}.$$

2.6. **The first fundamental inequality (analytic proof).** Let L/K be an extension of number fields, $n = [L : K]$. We write $C_K = \mathbf{A}_K^\times/K^\times$, $C_L = \mathbf{A}_L^\times/L^\times$. Consider the following group:

$$C_K/N_{L/K}C_L.$$

Proposition 2.18. *The group $C_K/N_{L/K}C_L$ is finite.*

Proof. Let v be a place of K, $w \mid v$ a place of L. If v is real then $N_{L_w/K_v}L^\times{}_w$ is of index 1 or 2 in $K^\times{}_v$. So it suffices to prove the finiteness of the index of the norms in $\mathbf{A}_K^1/K^\times$. Using the exact sequence

$$1 \to \mathbf{A}_{K,\infty}^1/[\mathbf{A}_{K,\infty}^1 \cap K^\times U] \to \mathbf{A}_K^1/K^\times U \to Cl(K)$$

and the finiteness of $Cl(K)$ we see it suffices to show that the image of the map $N_{L/K}U_L \to U_K$ has finite index. This follows from two facts:

(1) If v is unramified in L then for any $w \mid v$ $N_{L/K}U_w = U_v$;
(2) For any finite w, $N_{L/K}U_w$ is of finite index in U_v

These are purely local statements. The second is easy: If $m = [L_w : K_v]$ then $N_{L/K}U_w$ contains U_v^m. Choose $r > s = v(m)$; then for any $x \in O_v$, with uniformizer $\varpi \in m_v$,

$$(1 + x\varpi^r)^m \equiv 1 + mx\varpi^r \pmod{m\varpi^{r+1}} = \varpi^{r+s+1}.$$

Thus U_v^m contains $1 + m_v^{r+s+1}$.

As for the first, let $G = Gal(L_w/K_v) = Gal(k(w)/k(v))$, so that $N_{L_w/K_v}a = \prod_{\sigma\in G}\sigma(a)$. We will prove that

$$N_{k(w)/k(v)}k(w)^\times = k(v)^\times,\ Tr_{k(w)/k(v)}k(w) = k(v)$$

as applications of cohomology of groups (although they are easy enough to prove anyway; for example, $\sum_{\sigma\in G} : k(w) \to k(w)$ is not identically zero as a homomorphism of $k(v)$-vector spaces by Dedekind's theorem on independence of characters). It follows that $N_{L_w/K_v}U_w$ contains the roots of unity in U_v by the Teichmüller lift, so it remains to show that the image of the norm contains the 1-units. But say $u = 1 + \varpi x_1$ for

some $x_1 \in \mathcal{O}_w$. Note that ϖ is a uniformizer of m_w as well as of m_v. Then

$$N_{L_w/K_v}(u) \equiv 1 + Tr(x_1)\varpi \pmod{m_v^2}$$

This implies that the image of the norm is surjective mod $1 + m_v^2$, and by induction we obtain surjectivity. □

Proposition 2.19. *The series $\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}$, where p runs over all prime ideals in $\mathcal{O}_K$, is asympotic to $\log(\frac{1}{s-1})$ when $s \to 1$. The series $\sum_p \sum_{k\geq 2} p^{-ks}$ is bounded when $s \to 1$.*

Proof. The variable s is real and greater than 1. In a neighborhood of $s = 1$ we know that $\zeta_K(s) = \frac{1}{s-1} \cdot \phi(s)$ where $\phi(1) \neq 0$ is the residue. Thus

$$\log(\zeta_K(s)) = \log(\frac{1}{s-1}) + \log(\phi) \sim \log(\frac{1}{s-1}).$$

We consider

$$\log(\zeta_K(s)) = -\sum_{\mathfrak{p}} \log(1 - N\mathfrak{p}^{-s}) =$$

$$= \sum_{\mathfrak{p}} \sum_{k\geq 1} \frac{1}{kN\mathfrak{p}^{ks}} = \sum_{\mathfrak{p}} N\mathfrak{p}^{-s} + \sum_{\mathfrak{p}} \sum_{k\geq 2} \frac{1}{k\mathfrak{p}^{ks}}.$$

Now the second sum is majorized by $[K : \mathbb{Q}] \sum_p \sum_{k\geq 2} p^{-ks}$ where the sum runs over *rational* prime numbers. This is the sum of the geometric series

$$\sum_p \frac{1}{p^s(p^s - 1)} \leq \sum_p \frac{1}{p(p-1)} \leq \sum_n \frac{1}{n(n-1)} = 1.$$

So the second term is bounded in a neighborhood of 1, and so $\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}$ is asymptotic to $\log(\zeta_K(s)$ which is asymptotic to $\log(\frac{1}{s-1})$ when $s \to 1$. □

Theorem 2.20 (First fundamental inequality)**.** *The index $h = [C_K : N_{L/K}C_L]$ is bounded by $n = [L : K]$.*

Proof. This can also be proved by cohomology of groups, but the analytic proof is shorter and follows essentially the proof of Dirichlet's theorem on primes in an arithmetic progression. We know that h is finite, so the set of $X(L/K)$ characters $\omega : C_K \to \mathbb{C}^\times$ that are trivial on $N_{L/K}C_L$ is finite of order h. Let ω_0 denote the trivial character. For all $\omega \neq \omega_0$, the L-function $L(s, \omega)$ is entire, and in particular has a holomorphic extension to a region containing the point $s = 1$ (this is easier than the functional equation). On the other hand, $L(s, \omega_0)$ has a

simple pole at $s = 1$ (whose residue we have computed). In particular, as in the proof of Dirichlet's theorem

$$\log L(s, \omega_0) \sim \sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s} \sim \log(\frac{1}{s-1})$$

where $\sim$ means the difference is holomorphic near $s = 1$; here $\mathfrak{p}$ runs over the set of prime ideals in K; the other terms in the logarithm of the Euler product are irrelevant for the pole. For this, see Proposition 2.19 below.

Now $L(s, \omega) = \prod_{\mathfrak{p}}(1 - \omega(\mathfrak{p})N\mathfrak{p}^{-s})^{-1}$ where we set $\omega(\mathfrak{p}) = 0$ if $\omega_{\mathfrak{p}}$ is ramified. Thus it can also be written

$$L(s, \omega) = \sum_{J} \frac{\omega(J)}{NJ^s}$$

where J runs over ideals in $\mathcal{O}_K$ and ω is extended to a map from ideals to μ_∞ by multiplicativity.

Similarly, for $\omega \in X(L/K)$ we have $L(s, \omega)$ is holomorphic at $s = 1$, and the argument above shows that

$$\log L(s, \omega) = \sum_{\mathfrak{p}} \frac{\omega(\mathfrak{p})}{N\mathfrak{p}^s} + g(s, \omega) \tag{2.21}$$

where $g(s, \omega)$ is a Dirichlet series that is absolutely convergent for $Res > 1/2$. We know in fact that $L(1, \omega) \neq 0$, but even if we didn't know that we would see that the singularity of $\log L(s, \omega)$ is contained in the sum.

Let H be the set of prime ideals that are equivalent (modulo principal ideals) to norms of primes from L/K. Now we can write

$$\sum_{\omega \in X(L/K)} \sum_{\mathfrak{p}} \frac{\omega(\mathfrak{p})}{N\mathfrak{p}^s} = h \cdot \sum_{\mathfrak{p} \in H} \frac{1}{N\mathfrak{p}^s}$$

by orthogonality of characters. On the other hand, using (2.21) we have that the left hand side is equivalent to (see Proposition 2.19 for ϕ)

$$\log(\phi(s)) + \log \frac{1}{s-1} + \sum_{\omega \neq \omega_0} [\log L(s, \omega) - g(s, \omega)] := hf(s) + \log \frac{1}{s-1}.$$

Thus we have

$$\sum_{\mathfrak{p} \in H} \frac{1}{N\mathfrak{p}^s} = \frac{1}{h} \log \frac{1}{s-1} + f(s). \tag{2.22}$$

If $L(1,\omega)=0$ with a zero of order r then

$$\lim_{s=1} \log L(s,\omega) - g(s,\omega) \sim \log(s-1)^r \to -\infty$$

In particular, $\limsup_{s \to 1} f(s) = M < +\infty$.

On the other hand, the Dedekind zeta function of L also has a simple pole at $s=1$. Let B be the set of primes that split completely in L/K. Then we have

$$\log \zeta_L(s) \sim \sum_{\mathfrak{P}} \frac{1}{N\mathfrak{P}^s} \sim n \cdot \sum_{\mathfrak{p}\in B} \frac{1}{N\mathfrak{p}^s}$$

because the primes that don't split completely over K also are negligeable. In other words,

$$\sum_{\mathfrak{p}\in B} \frac{1}{N\mathfrak{p}^s} = \frac{1}{n} \log \frac{1}{s-1} + G(s) \tag{2.23}$$

where $|G(s)| < M'$ is bounded near $s=1$. But $B \subset H$. Thus we can subtract (2.23) from (2.22) and the result is positive near $s=1$ (s real):

$$\begin{aligned} 0 \le \sum_{\mathfrak{p}\in H} \frac{1}{N\mathfrak{p}^s} - \sum_{\mathfrak{p}\in B} \frac{1}{N\mathfrak{p}^s} &= [\frac{1}{h} - \frac{1}{n}] \log \frac{1}{s-1} + f(s) - G(s) \\ &\le [\frac{1}{h} - \frac{1}{n}] \log \frac{1}{s-1} + M + M' \end{aligned}$$

in a neighborhood of $s=1$. Since $\log \frac{1}{s-1} \to +\infty$ as $s \to 1^+$, this implies $h \le n$. $\square$

3. Cohomology of groups

3.1. **Definitions.** Let Γ be a group, $\mathbb{Z}[\Gamma]$ the group ring. If M is any Γ-module let $M^\Gamma \subset M$ be the subgroup of m such that $\gamma(m) = m$ for all $\gamma \in \Gamma$. Then there is an isomorphism

$$Hom_{\mathbb{Z}[\Gamma]}(\mathbb{Z}, M) \xrightarrow{\sim} M^\Gamma.$$

The left-hand side is a Hom over the ring $\mathbb{Z}[G] = S$. This has right-derived functors $Ext^i_{\mathbb{Z}[\Gamma]}(\mathbb{Z}, M)$, also called $H^i(\Gamma, M)$. These are computed as follows. If

$$\ldots \to \Lambda_i \to \Lambda_{i-1} \to \ \ldots \ \to \Lambda_1 \to \Lambda_0 \to \mathbb{Z}$$

is a resolution of $\mathbb{Z}$ by free or projective $\mathbb{Z}[\Gamma]$-modules, set $C^i(M) = Hom_{\mathbb{Z}[\Gamma]}(\Lambda_i, M)$. This gives a complex

$$0 \to C^0(M) \xrightarrow{d_0} C^1(M) \xrightarrow{d_1} C^2(M) \ldots.$$

Then $H^i(\Gamma, M) = \ker(d_i)/im(d_{i-1})$.

To make this explicit, let $\Lambda_i = \mathbb{Z}[\Gamma \times \cdots \times \Gamma]$ ($i+1$ copies) which is a free $\mathbb{Z}$-module with basis $(\gamma_0, \ldots, \gamma_i)$. This is a Γ-module through the diagonal action $g(\gamma_0, \ldots, \gamma_i) = (g\gamma_0, \ldots, g\gamma_i)$. Then $C^i(M) = Hom_{\mathbb{Z}[\Gamma]}(\Lambda_i, M)$ is the set

$$\{(\gamma_0, \ldots, \gamma_i) \mapsto f(\gamma_0, \ldots, \gamma_i) \mid f(g\gamma_0, \ldots, g\gamma_i) = g \cdot f(\gamma_0, \ldots, \gamma_i)\}.$$

The differentials are given by

$$\Lambda_i \xrightarrow{\delta_i} \Lambda_{i-1};\ \delta_i(\gamma_0, \ldots, \gamma_i) = \sum_{j=0}^{i} (-1)^j (\gamma_0, \ldots, \hat{\gamma}_j, \ldots, \gamma_i).$$

This is set up so that $\delta_{i-1} \circ \delta_i = 0$ because each term appears twice with opposite sign.

Proposition 3.1. *The complex* $\ldots \Lambda_i \xrightarrow{\delta_i} \Lambda_{i-1}$ *is exact.*

Proof. This is proved by constructing a chain homotopy.

$$H : \Lambda_{\bullet - 1} \to \Lambda_\bullet; H(\gamma_0, \ldots, \gamma_{i-1}) = (1, \gamma_0, \ldots, \gamma_{i-1}).$$

Then one shows that

$$(\delta \circ H + H \circ \delta)(\gamma_0, \ldots, \gamma_i) = (\gamma_0, \ldots, \gamma_i).$$

So if $\delta_i(A) = 0$ we have

$$A = \delta_{i+1}(HA) + H\delta_i(A) = \delta_{i+1}(HA)$$

is a coboundary. □

Since any $f \in C^i(M)$ is homogeneous for the action of Γ, we may always assume $\gamma_0 = 1$, set

$$\varphi(g_1, \ldots, g_i) = f(1, g_1, g_1g_2, \ldots, g_1g_2 \ldots g_i).$$

Then translating d_i to the φ we have

$$d\varphi(g_1, \ldots g_{i+1}) = g_1\varphi(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \varphi(g_1, \ldots, g_jg_{j+1}, \ldots, g_{i+1} + (-1)^{i+1}\varphi(g_1, \ldots, g_i).$$

Write $C_h^i(M)$ for the space of φ corresponding to $f \in C^i(M)$.

We work this out in low degree. Since $C^0(M) = Hom_{\mathbb{Z}[\Gamma]}(\mathbb{Z}[\Gamma], M) = Hom_{\mathbb{Z}}(\mathbb{Z}, M) = M$, we have for $\varphi = m \in M$

$$d_0(m)(g) = g \cdot m - m; H^0(\Gamma, M) = \ker d_0 = M^G$$

as required. If the action of Γ on M is trivial, then $d_0 = 0$. If $\varphi \in C_h^0(M)$ then

$$d_1\varphi(g_1, g_2) = g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1).$$

So

$$d_1\varphi = 0 \Leftrightarrow \varphi(g_1g_2) = g_1\varphi(g_2) + \varphi(g_1).$$

Such a φ is called a *crossed homomorphism*. If the action of Γ on M is trivial, then $Im(d_0) = 0$ and $H^1(\Gamma, M) = \ker(d_1) = Hom(\Gamma, M)$. In particular, $H^1(\Gamma, \mathbb{Z}) = Hom(\Gamma, \mathbb{Z})$.

Similarly, $Z^2(\Gamma, M) = \ker(d_2)$ is the set of $\varphi(g_1, g_2)$ such that

$$g_1\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_1, g_2) = 0.$$

Beyond H^2 one rarely uses explicit cocycles.

If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then we have the long exact sequence

$$0 \to (M')^\Gamma \to M^\Gamma \to (M'')^\Gamma \to H^1(\Gamma, M') \to H^1(\Gamma, M) \to H^1(\Gamma, M'') \to \ldots.$$

3.2. **Homology.** One defines homology dually as

$$H_i(\Gamma, M) = Tor_i^{\mathbb{Z}[\Gamma]}(\mathbb{Z}, M).$$

Thus $H_0(\Gamma, M) = \mathbb{Z} \otimes_{\mathbb{Z}[\Gamma]} M$ is the quotient of M by the subgroup generated by

$$1 \otimes g(m) - g(1) \otimes m = 1 \otimes g(m) - 1 \otimes m.$$

In other words, it's the largest quotient of M on which Γ acts trivially, the group of *coinvariants*.

3.3. **Examples.**

Definition 3.2. The Γ module M is coinduced if there is a $\mathbb{Z}$-module N such that

$$M = Hom_{\mathbb{Z}}(\mathbb{Z}(\Gamma), N).$$

Now for any M',

$$Hom_{\mathbb{Z}[\Gamma]}(M', M) = Hom_{\mathbb{Z}[\Gamma]}(M', Hom_{\mathbb{Z}}(\mathbb{Z}(\Gamma), N)) \xrightarrow{\sim} Hom_{\mathbb{Z}}(M', N).$$

This is a general identity of change of ring: if R is a subring of S and M' (resp. N) is an S-module (resp. an R-module) then

$$Hom_S(M', Hom_R(S, N)) \xrightarrow{\sim} Hom_R(M', N);\ [m' \mapsto \phi_{m'}] \mapsto [m' \mapsto \phi_{m'}(1)]$$

whereas

$$[m' \mapsto [s \mapsto \lambda(sm)] \leftarrow \lambda \in Hom_R(M', N).$$

It then follows that, if M is coinduced, then

$$\forall i > 0\ H^i(\Gamma, M) = Ext^i_{\mathbb{Z}[\Gamma]}(\mathbb{Z}, M) \xrightarrow{\sim} Ext^i_{\mathbb{Z}}(\mathbb{Z}, N) = 0.$$

Thus coinduced modules are acyclic.

Similarly, $H_i(\Gamma, M) = 0$ for $i > 0$ if $M = \mathbb{Z}[G] \otimes_{\mathbb{Z}} N$ is *induced*.

3.3.1. H_1.

Proposition 3.3. *For any Γ with trivial action on $\mathbb{Z}$, $H_1(\Gamma, \mathbb{Z}) \xrightarrow{\sim} \Gamma/[\Gamma, \Gamma] = \Gamma^{ab}$.*

Proof. There is a short exact sequence of Γ-modules

$$0 \to I_\Gamma \to \mathbb{Z}[\Gamma] \to \mathbb{Z} \to 0$$

where I_Γ is the augmentation ideal. Moreover, for any M, $H_0(\Gamma, M) = M/I_\Gamma M$ by definition. Since $\mathbb{Z}[G]$ is acyclic, we get a long exact sequence

$$0 \to H_1(\Gamma, \mathbb{Z}) \hookrightarrow H_0(\Gamma, I_\Gamma) = I_\Gamma/(I_\Gamma)^2 \to \mathbb{Z}[G]/I_\Gamma \to \mathbb{Z} \to 0.$$

Thus the last map is an isomorphism and $H_1(\Gamma, \mathbb{Z}) \xrightarrow{\sim} I_\Gamma/(I_\Gamma)^2$. But the map $g \mapsto g - 1$ induces an isomorphism

$$\Gamma/[\Gamma, \Gamma] \xrightarrow{\sim} I_\Gamma/(I_\Gamma)^2,$$

as one checks by direct computation. □

3.3.2. *Hilbert's theorem 90.* As an example of proofs with cocycles, here is a basic theorem in Galois theory:

Theorem 3.4 (Hilbert Theorem 90)**.** *If L/K is a finite Galois extension with Galois group G then $H^1(G, L^*) = 0$.*

Proof. Let $g \mapsto a(g) \in L^*$ be a cocycle. For any $c \in L$, let $\beta(c) = \sum_{g\in G} a(g)g(c)$. By Dedekind's theorem on linear independence of homomorphisms, this function $\beta : L \to L$ is not identically zero. If $\beta(c) \neq 0$ we write $\beta = \beta(c) \in L^\times$. Then for any $\gamma \in G$, we have

$$\gamma(\beta) = \sum_g \gamma(a(g))\gamma \cdot g(c).$$

But since a is a cocycle, we have

$$a(\gamma \cdot g) = \gamma(a(g)) \cdot a(\gamma)$$

so that

$$\gamma(\beta) = \sum_g a(\gamma)^{-1} \cdot a(\gamma \cdot g) \cdot (\gamma \cdot g)(c) = a(\gamma)^{-1} \cdot \beta.$$

In other words

$$a(\gamma) = \gamma(\beta)^{-1} \cdot \beta = \gamma(\alpha) \cdot \alpha^{-1}$$

with $\alpha = \beta^{-1}$. This precisely means $a = d_0(\alpha)$ is a coboundary. □

Example: finite fields. Suppose G is a cyclic group of order n, with generator g. Then

$$\Lambda = \mathbb{Z}[G] \simeq \mathbb{Z}[X]/(X^n-1) = \mathbb{Z}[X]/(T\cdot N);\ T = X-1, N = 1+X+\cdots+X^{n-1}.$$

Thus we have the following resolution of $\mathbb{Z}$ by free Λ-modules:

$$\ldots \Lambda \xrightarrow{T} \Lambda \xrightarrow{N} \Lambda \xrightarrow{T} \Lambda \xrightarrow{N} \mathbb{Z}$$

where T is multiplication by T and N is multiplication by N. The exactness follows from uniqueness of factorization in Λ. It follows that, for any G-module A, the operations T and N can be defined on N, and there are isomorphisms

$$H^i(G, A) = [\ker N : A \to A]/[ImT : A \to A];$$

for $i \geq 1$ odd, resp.

$$H^i(G, A) = [\ker T : A \to A]/[ImN : A \to A]$$

for $i \geq 2$ even. In particular, there is a (canonical) isomorphism

$$H^i(G, A) \xrightarrow{\sim} H^{i+2}(G, A),\ i \geq 1.$$

Now suppose $G = Gal(L/K)$ where L and K are finite fields of order q', q respectively. Then G is cyclic, so the above resolution applies. Moreover, $N = N_{L/K}$. We see by Hilbert's Theorem 90 that

$$0 = H^1(G, L^*) = [\ker N_{L/K}]/(ImT)$$

where $ImT = \{gx/x, x \in L^*\}$. In particular, $|Im(T)| = |\ker N|$. But of course

$$q' - 1 = |Im(T)||\ker T| = |Im(N)||\ker N|$$

so it follows that

$$Im(N) = \ker T = \{x \in L^* \mid g(x) = x\} = K^*.$$

Hence we have proved that

Proposition 3.5. *If L/K is an extension of finite fields, then $N_{L/K} : L^* \to K^*$ is surjective.*

3.4. **Functoriality.** Suppose $H \subset G$. Let N be an H-module, $I_H^G(N) = Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], N)$ the induced module, where $\mathbb{Z}[G]$ is a left $\mathbb{Z}[H]$-module and the action of G is on the right: $r(g)f(g') = f(g'g)$. We have Frobenius reciprocity (as in the notes):

$$Hom_G(A, I_H^G(N)) \xrightarrow{\sim} Hom_H(A, N)$$

canonically. In particular, for each i

$$C^i(G, I_H^G(N)) = Hom_G(\Lambda_i(G), I_H^G(N)) \xrightarrow{\sim} Hom_H(\Lambda_i(G), N) \simeq' C^i(H, N)$$

becaue $\Lambda_i(G)$ is still a free H-resolution of $\mathbb{Z}$. Since these isomorphisms are functorial we obtain

Proposition 3.6 (Shapiro's Lemma)**.** *There are canonical isomorphisms*

$$H^i(G, I_H^G(N)) \xrightarrow{\sim} H^i(H, N)$$

for all N.

In particular, if A is an induced module – i.e., induced from $\{1\}$ – then $H^i(G, A) = 0$ for all $i > 0$.

We write $I(M) = I_1^G(M)$. For any G-module M there is an embedding $M \hookrightarrow I(M)$ by sending

$$m \mapsto \phi_m; \phi_m(g) = g \cdot m \ \forall g \in G.$$

Check that this is a homomorphism of G-modules. Thus there is some exact sequence

$$0 \to M \to I(M) \to N \to 0$$

where N is the cokernel, and thus for all $i > 0$ an isomorphism

$$H^i(G, N) \xrightarrow{\sim} H^{i+1}(G, M).$$

More generally, if A is a G module, and $H \to G$ is a homomorphism, then A becomes an H-module, and there are canonical functorial maps

$$C^i(G, A) \to C^i(H, A)$$

compatible with the differentials, hence canonical functorial maps

$$H^i(G, A) \to H^i(H, A) \tag{3.7}$$

If $H \subset G$ then (3.7) is called *restriction*; if $G = H/N$ is a quotient by a normal subgroup then (3.7) is called *inflation*. Note that $\varphi \in H^1(G, A)$ comes from $H^1(G/H, A)$ then $\varphi(h) = \varphi(1) = v$, say for all $h \in H$, i.e. $\varphi(1) = \varphi(h) = \varphi(h \cdot 1) = 1 \cdot \varphi(h) + \varphi(1)$ which implies that $\varphi(h) = 0$ for all $h \in H$.

Proposition 3.8 (Inflation-restriction sequence)**.** *Let $H \subset G$ be a normal subgroup. There is a short exact inflation-restriction sequence for any G-module A:*

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A).$$

Remark 3.9. In fact one can replace the group on the right by $H^0(G/H, H^1(H, A))$.

Proof. First: suppose $\varphi \in Z^1(G, A)$ maps to a coboundary upon restriction to H, say $\varphi(h) = ha - a$ for all $h \in H$. Then φ is cohomologous to $\varphi'(g) = \varphi(g) - ga + a$; and $\varphi'(h) = 0$ for all $h \in H$. Then

$$\varphi'(hg) = g\varphi'(h) + \varphi'(g) = \varphi'(g) \Rightarrow \varphi' \in Z^1(G/H, A).$$

But moreover

$$\varphi'(g) = \varphi'(gh) = h\varphi'(g) + \varphi'(h) = h\varphi'(g) \Rightarrow \varphi'(g) \in A^H.$$

This also shows that the composition is zero. The injectivity on the left is similar: if f inflates to a coboundary, i.e. suppose $f(g)$ is constant mod H, lies in A^H and $f(g) = ga - a$ for some $a \in A$. In particular $f(h) = 0$ which implies that $a \in A^H$. □

There is a generalization:

Proposition 3.10 (Inflation-restriction sequence, higher q)**.** *With H, G, A as above, $q > 1$, assume $H^i(H, A) = 0$ for all $1 \leq i \leq q - 1$. Then the sequence*

$$0 \to H^q(G/H, A^H) \to H^q(G, A) \to H^q(H, A)$$

is exact.

Proof. Induction on q. We know it for $q = 1$, assume it's true for $q - 1$. Write

$$0 \to A \to I(A) \to A' \to 0$$

with $I(A)$ induced as before. Then $H^i(H, A') = H^{i+1}(H, A) = 0$ for $i \leq q-2$. Moreover,

$$0 \to A^H \to I(A)^H \to A'^{,H} \to H^1(H, A) = 0$$

by hypothesis; and

$$I(A)^H = Hom_{\mathbb{Z}}(\mathbb{Z}[G], A)^H = Hom_{\mathbb{Z}}(\mathbb{Z}[G/H], A)$$

is an induced module for G/H, hence has trivial higher cohomology. Thus we have

$$H^{q-1}(G/H, A'^H) = H^q(G/H, A^H)$$

and we have the commutative diagram

$$\begin{array}{ccccccc} 0 \to & H^{q-1}(G/H, (A')^H) & \to & H^{q-1}(G, A') & \to & H^{q-1}(H, A') \\ & \downarrow\delta & & \downarrow\delta & & \downarrow\delta \\ 0 \to & H^q(G/H, A^H) & \to & H^q(G, A) & \to & H^q(H, A) \end{array}$$

in which the vertical arrows are all isomorphisms and the top line is exact by induction. Thus the bottom line is exact. □

3.5. **Herbrand quotient.** Continuing with finite cyclic groups, we define $h_0(A) = |H^2(G, A)| = |\ker(T)/Im(N)|$, $h_1(A) = |H^1(G, A)| = |\ker(N)/Im(T)|$, $h(A) = h_0(A)/h_1(A)$ the Herbrand quotient, whenever these groups are finite. The preceding argument can be formalized:

Proposition 3.11. *Suppose A is a finite G-module. Then $h(A) = 1$.*

Proof. There are exact sequences:

$$0 \to H^0(G, A) = A^G \to A \xrightarrow{T} A \to A_G = H_0(G, A) \to 0;$$

$$0 \to H^1(G, A) \to A_G \xrightarrow{N} A^G \to \hat{H}^0(G, A) \to 0;$$

where we define the *Tate cohomology group* $\hat{H}^0$ by this diagram, so that $h_0(A) = |\hat{H}^0(G, A)|$. The first diagram shows that $|A^G| = |A_G|$ and the second shows that $h_0 = h_1$. □

Proposition 3.12. *Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules. Suppose two of the three Herbrand quotients $h(A), h(B), h(C)$ are defined. Then so is the third, and we have*

$$h(B) = h(A)h(C).$$

In particular, if $f : A \to B$ is a G-homomorphism with finite kernel and cokernel, and if one of $h(A), h(B)$ is defined, then so is the other, and $h(A) = h(B)$.

Proof. For the last sentence, we have

$$0 \to K \to A \to Im(f) \to 0; 0 \to Im(f) \to B \to C \to 0$$

and we derive the claim from the first statement in two steps.

Thus it suffices to prove the first claim. The long exact sequence is periodic:

$$\dots H^1(C) \to H^2(A) \to H^2(B) \to H^2(C) \to H^1(A) \to H^1(B) \to H^1(C) \to H^2(A) \dots$$

so it can be represented as a hexagon with all arrows exact. By rotating the hexagon we may suppose $h(A)$ and $h(B)$ are defined, and we have the following exact cyclic diagram:

$$\dots H_1 \to H_2 \to H_3 \to H_4 \to H_5 \to H_6 \to H_1 \dots$$

Let $M_i = im(H_i \subset H_{i+1})$ for each i, $m_i = |M_i|$. By hypothesis we have H_1, H_2, H_4, H_5 finite, and this suffices to show that the other two are finite as well. Moreover, $|H_i| = m_i \cdot m_{i-1}$ for all i. Now $h(A) = |H_1|/|H_4| = \frac{m_1 m_6}{m_3 m_4}$, $h(B) = |H_2|/|H_5| = \frac{m_1 m_2}{m_5 m_4}$, $h(C) = |H_3|/|H_6| = \frac{m_2 m_3}{m_5 m_6}$ and the equality is obvious. □

We want to apply this to the action of $G = Gal(L/K)$ on $A = L^\times$ when L/K is a cyclic extension of p-adic fields of degree n. In that case $h_0(A) = |\ker(T)/Im(N)| = K^\times/N_{L/K}L^\times$, whereas $h_1(A) = 1$ by Hilbert's theorem 90. We have

$$1 \to U_L \to L^\times \stackrel{val}{\to} \mathbb{Z} \to 1$$

where *val* is the valuation map. The action of G on $\mathbb{Z}$ is trivial and $N : \mathbb{Z} \to \mathbb{Z}$ is multiplication by n. Thus $h_0(\mathbb{Z}) = n$ whereas $\ker(N) = 0$ so that $h_1(\mathbb{Z}) = 1$. Thus

Lemma 3.13. *The Herbrand quotient of $\mathbb{Z}$ is n. In particular, if the Herbrand quotient of U_L exists and equals m, then $|K^\times/N_{L/K}L^\times| = h(L^\times) = m \cdot n$.*

We will show in fact that $h(U_L) = 1$, and thus that $|K^\times/N_{L/K}L^\times| = n = |Gal(L/K)$. The easiest way to prove this is by using the logarithm map $\log : U_L \to L$. Note that

$$1 \to U_L^1 \to U_L \to k_L^\times \to 1$$

is an exact sequence of G-modules, so $h(U_L) = h(U_L^1)$ if the latter exists.

3.5.1. *The p-adic logarithm and exponential.* For any $x \in m_L$, we can define

$$\log(1+x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i}$$

provided this converges. Similarly, we can define

$$exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

Proposition 3.14. *The power series for* $\log(1+x)$ *converges whenever* $|x| < 1$ *and*

$$\log(1+x) \equiv x \pmod{x \cdot m_L}$$

provided $val(x) > \frac{e}{p-1}$.

Similarly, $\exp(x)$ *converges for all* x *such that* $val(x) = \frac{e}{p-1}$ *and on that disk*

$$val(x) = val(exp(x) - 1)$$

Thus on the disk defined by that inequality, $x \mapsto \log(1+x)$ *and* $x \mapsto \exp(x)$ *are inverse maps.*

Proof. This is an estimate of divisibility. We write v_p for the usual p-adic valuation, so $val = ev_p$. First for log. We need to show that if $val(x) > \frac{e}{p-1}$ and $n \geq 2$ then

$$|x^n/n| < |x|.$$

Say $p^r \leq n < p^{r+1}$; then $val(n) \leq er$, so that

$$val(x^n/n) - val(x) = (n-1)val(x) - val(n) \geq nval(x) - er > e[\frac{n-1}{p-1} - r]$$

and we already see that the right hand side tends to infinity as $n \to \infty$, so $\log(1+x)$ converges on all U_L^1. But moreover, if $n \geq p^r$ then $n-1 \geq (p-1)p^{r-1}$ so in particular $\frac{n-1}{p-1} \geq p^{r-1} \geq r$ for any $r \geq 0$. This completes the claim about log.

Now if we write $n = a_0 + a_1 p + \cdots + a_r p^r$ in p-adic digits, with $0 \leq a_i \leq p-1$, we have

$$[n/p^i] = a_i + a_{i+1}p + \cdots + a_r p^{r-i}$$

for any i. It follows that the number of integers $b \leq n$ such that $p^i \mid b$ is $a_i + a_{i+1}p + \cdots + a_r p^{r-i}$, and thus

$$v_p(n!) = \cdot \sum_{i=1}^{r} (a_i + a_{i+1}p + \cdots + a_r p^{r-i}) = \sum_{i=1}^{r} a_i \sum_{j=1}^{i} p^{j-1}.$$

Thus

$$(p-1)v_p(n!) = (p-1)a_1 + (p^2-1)a_2 + \cdots + (p^r-1)a_r] = n - \sum_{i=0}^{r} a_i.$$

It follows that

$$val(x^n/n!) = nval(x) - val(n!) = nval(x) - e\frac{n-\sum a_i}{p-1} > n[val(x) - \frac{e}{p-1}] > 0.$$

This shows again that for $n \geq 2$ we have $val(x^n/n!) > val(x)$ if $val(x) - \frac{e}{p-1} > 0$. □

Thus U_L^1 contains a subgroup U^+ of finite index that is isomorphic to (ϖ_L^d) for some d as G-module. It follows that $h(U_L^1) = h(U^+) = h((\varpi_L^d)) = h(\mathcal{O}_L)$. But by the normal basis theorem, $\mathcal{O}_L$ has a lattice V generated over $\mathcal{O}_K$ by elements $e_1, ge_1, \ldots, g^{n-1}e_1$ for some $e_1 \in \mathcal{O}_L$. Again, this lattice is of finite index, but it is also induced, so $H^1(G,V) = 0$ and $H^0(G,V)\{a[1+g+g^2+\cdots+g^{n-1}]e_1, a \in \mathcal{O}_K\} = Tr_G(V)$; in other words $\hat{H}^0(G,V) = 0$. It follows that $1 = h(V) = h(U_L)$. Thus

Theorem 3.15. *If L/K is a cyclic extension of p-adic fields, then $|K^\times/N_{L/K}L^\times| = [L:K]$.*

3.6. **Homology, corestriction, Tate cohomology.** Suppose $[G:H]$ is finite. Then there is a map from A^H to A^G: if $\{\gamma_i\}$ is a set of representatives for G/H then

$$Cor(x) = \sum_i \gamma_i(x) \in A^G, \ \forall x \in A^H.$$

It is clearly independent of the choice of coset representatives. We want to define it for higher H^i. This requires a detour through some additional technicalities.

First, homology, which is dual to cohomology. Let A be a G-module, and define A_G to be the largest quotient of A on which G acts trivially; in other words,

$$A_G = A/I_G A = A/ < ga - a, \forall g \in G, a \in a > .$$

This can be recognized as a tensor product:

$$A_G = A \otimes_{\mathbb{Z}[G]} \mathbb{Z}$$

where $\mathbb{Z}[G]$ acts trivially on $\mathbb{Z}$. This is a group, and if $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules then

$$\ldots A_G \to B_G \to C_G \to 0$$

is exact. We write $H_0(G,A) = A_G$ and define the left-derived functors $H_i(G,A)$ so that there is a long exact sequence

$$\dots H_i(G,A) \to H_i(G,B) \to H_i(G,C) \to H_{i-1}(G,A) \dots \to H_0(G,C) \to 0.$$

This can be constructed using the standard complex again. Recall that

$$\dots P_i \to P_{i-1} \to \dots \to P_0 \to \mathbb{Z} \to 0$$

is a canonical free resolution of $\mathbb{Z}$ as a Λ-module. Then we write

$$H_i(G,A) = H_i(P_\bullet \otimes_\Lambda A) = Z_i(G,A)/\delta(P_{i+1} \otimes_\Lambda A).$$

Note that if $A = \Lambda$ then the sequence $P_\bullet \otimes_\Lambda \Lambda$ is exact except at $i = 0$, where its cohomology is just $H_0(G,\Lambda) = \mathbb{Z}$. Thus the sequence $0 \to I_G \to \Lambda \to \mathbb{Z} \to 0$ gives isomorphisms

$$H_i(G,\mathbb{Z}) \xrightarrow{\sim} H_{i-1}(G, I_G)$$

for $i \geq 1$. In particular

Lemma 3.16.

$$H_1(G,\mathbb{Z}) = I_G/I_G^2 \xrightarrow{\sim} G/[G,G]$$

where the inverse map takes $g \mapsto (g-1)$.

The second claim is an exercise.

More generally, we have

Proposition 3.17. *If* $A = \Lambda_G \otimes B = P(B)$ *for any abelian group* B *then* $H_i(G,A) = 0$ *for* $i > 0$.

Proof. Indeed, the standard complex for $P(B)$ is just $P_\bullet \otimes_{\mathbb{Z}} B$. But P_i is a free $\mathbb{Z}$-module for every i so this sequence is exact. □

If $H \subset G$ then there is a corestriction map

$$Cor : H_q(H,A) \to H_q(G,A)$$

because $\mathbb{Z}[H] \subset \mathbb{Z}[G]$ and thus the canonical map $P_\bullet(H) \to P_\bullet(G)$ gives

$$P_\bullet(H) \otimes_{\mathbb{Z}[H]} A \to P_\bullet(G) \otimes_{\mathbb{Z}[H]} A \to P_\bullet(G) \otimes_{\mathbb{Z}[G]} A$$

where the second map is a special case of the general fact: if $R \to S$ is a homomorphism of rings and M, N are right (respectively left) S-modules, then there is a canonical map of groups

$$M \otimes_R N \to M \otimes_S N.$$

Now assume G is finite and let $N = \sum_{g \in G} g \in \Lambda$. Note that $N \cdot I_G = 0$ as a submodule of Λ, so that, for any G-module A, $I_G \cdot A \subset \ker(N)$.

On the other hand, $Im(N) \subset A^G$ because it is just the corestriction for the inclusion of $\{1\}$ in G. Thus there is a functorial map

$$N^* : H_0(G, A) \to H^0(G, A)$$

and we can define the Tate cohomology groups

$$\hat{H}_0(G, A) = \ker N^*;\ \hat{H}^0(G, A) = A^G / Im(N^*)$$

For $i \neq 0$ we let $\hat{H}^i = H^i$ if $i > 0$, $\hat{H}^{-i} = H_{i-1}$ if $i \geq 2$, $\hat{H}^{-1} = \hat{H}_0$. Moreover, for any $\mathbb{Z}$-module B, there is a canonical isomorphism of G-modules.

$$Hom_{\mathbb{Z}}(\Lambda, B) = I(B) \to P(B) = \Lambda \otimes B;\ \varphi \mapsto \sum_{g \in G} g \otimes \varphi(g).$$

It follows that $H_i(G, I(B)) = H^i(G, I(B)) = 0$ if $i \neq 0$. Moreover,

$$H^0(P(B)) = P(B)^G = \{x = \sum_g g \otimes b_g \mid hx = x \forall h \in G\}$$

which implies $b_g = b$ for all g. But then $H^0(P(B)) = Im(N^*)$, so $\hat{H}^0(P(B)) = 0$. Similarly, $\ker N^* : P(B) \to H^0(G, A)$ is precisely $I_G \cdot P(B)$, so $\hat{H}_0(P(B)) = 0$ as well. Thus $I(B) = P(B)$ is acyclic for $\hat{H}$ in every degree.

Theorem 3.18. *For every short exact sequence* $0 \to A \to B \to C \to 0$ *of* G*-modules there is a long exact sequence*

$$\ldots \hat{H}^i(G, A) \to \hat{H}^i(G, B) \to \hat{H}^i(G, C) \to \hat{H}^{i+1}(G, A) \ldots$$

that extends infinitely in both directions.

Proof. This is proved by using

$$N^* : [A_G \to B_G \to C_G] \to [A^G \to B^G \to C^G]$$

to glue together the homology and cohomology sequences where they end. Then the snake lemma gives a map from

$$\hat{H}_0(G, C) = [\ker N^* : C_G \to C^G]$$

to

$$[coker N^* : A_G \to A^G] = \hat{H}^0(G, A).$$

In the same way we have an exact sequence

$$\hat{H}_0(G, A) \to \hat{H}_0(G, B) \to \hat{H}_0(G, C) \to \hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C)$$

and we need to show that the map

$$H_1(G, C) \to H_0(G, A)$$

has image in $\ker N^*$ and that the image of N^* in $H^0(G,C)$ maps to 0 in $H^1(G,A)$. But this follows directly from the explicit calculation of the coboundary maps (see §2 and §3 in Chapter 4 of Cassels-Fröhlich). □

Suppose $G \supset H$. By embedding any A in an induced module for G, hence for H, we can use dimension-shifting to define $Cor : \hat{H}^i(H,A) \to \hat{H}^i(G,A)$ and $Res : \hat{H}^i(G,A) \to \hat{H}^i(H,A)$ for all i.

Proposition 3.19. *Suppose $[G:H] = n$. Then $Cor \circ Res = n$. In particular, if G has order n, then all the groups $\hat{H}^q(G,A)$ are annihilated by n.*

Proof. For the first claim, this is true for $\hat{H}^0$: Suppose $x \in A^G$. Then $Res(x) = x$ and $Cor(Res(x)) = \sum_{\gamma_i} \gamma_i(x) = nx$ because $\gamma_i(x) = x$ for all i, where γ_i are coset representatives as before. The claim then follows by dimension shifting because Cor and Res commute with the coboundary maps for Tate cohomology.

For the second claim, we take $H = \{1\}$; then $Res(\hat{H}^i(G,A) \subset \hat{H}^i(\{1\},A) = 0$. So multiplication by n factors through the 0 map. □

Corollary 3.20. *Suppose $S \subset G$ is a p-Sylow subgroup. Then $Res : \hat{H}^q(G,A) \to \hat{H}^q(S,A)$ is injective on the p-primary subgroup of $\hat{H}^q(G,A)$.*

In particular, if $x \in \hat{H}^q(G,A)$ restricts to 0 for every Sylow subgroup then $x = 0$.

Proof. Suppose $|G| = n = m \cdot p^a$ for some m prime to p. Let $x \in \hat{H}^q(G,Z)$ and suppose $p^r x = 0$ for some $r > 0$ but that $Res(x) = 0$ in $\hat{H}^q(S,A)$. Now $mx = Cor \circ Res(x) = 0$ by hypothesis, but since $(p^r, m) = 1$ we can find $A, B \in \mathbb{Z}$ such that $Ap^r + Bm = 1$; thus $x = 0$.

Now in general $x \in \hat{H}^q(G,A)$ is of order dividing n, say $x = \sum x_p$ where x_p is of p-primary order. Suppose $x \in \hat{H}^q(G,A)$ restricts to 0 for every Sylow subgroup. If $S_p \subset G$ is a p-Sylow subgroup then $0 = Res_{S_p}(x) = Res_{S_p}(x_p)$ because the other summands are annihilated by $|S_p|$ and by a number prime to p. By the first part of the Corollary $x_p = 0$. Thus $x = 0$. □

Theorem 3.21. *Suppose G is finite and A is a G-module such that $H^1(G',M) = H^2(G',M) = 0$ for all subgroups $G' \subset G$. Then $\hat{H}^r(G,M) = 0$ for all $r \in \mathbb{Z}$.*

Proof. The previous Corollary allows us to replace G by its Sylow subgroups. Thus it suffices to assume G *solvable* (even nilpotent). In particular, we can assume by induction that it is true for a proper normal subgroup $H \subset G$ with G/H cyclic. In particular, since H satisfies

the hypotheses of the theorem, $\hat{H}^r(H, M) = 0$ for all r by induction. In particular, we have the inflation-restriction sequence

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M) = 0$$

for all $r \geq 1$. Apply this to $r = 1$ and $r = 2$ and we find $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$. Since G/H is cyclic, this implies that $\hat{H}^r(G/H, M^H) = 0$ for all r. Thus $H^r(G, M) = 0$ for all $r > 0$.

We next prove that $\hat{H}^0(G, M) = 0$. Let $x \in M^G \subset M^H$. Since $\hat{H}^0(G/H, M^H) = 0$, there exists $y \in M^H$ such that $N_{G/H}(y) = x$. But $\hat{H}^0(H, M) = M^H/(ImN_H)$ so there is $z \in M$ such that $N_H(z) = y$, and thus

$$N_G(z) = N_{G/H} \circ N_H(z) = x$$

and $\hat{H}^0(G, M) = 0$.

To prove $\hat{H}^r(G, M) = 0$ for $r < 0$ we apply dimension-shifting:

$$0 \to M' \to P(M) \to M \to 0$$

which implies that $\hat{H}^r(G', M) = \hat{H}^{r+1}(G', M')$ for G' any subgroup of G. By what we already know we have $\hat{H}^0(G', M) = \hat{H}^1(G', M) = 0$ and so M' satisfies the hypotheses of the theorem, hence by the last paragraph $\hat{H}^{-1}(G, M) = 0$. We can repeat this argument for each degree to conclude the proof for solvable G, hence for all G as above. □

Theorem 3.22 (Tate's theorem)**.** *Let G be a finite group and let C be any G module. Suppose for all $H \subset G$,*

(a) $H^1(H, C) = 0$*;*
(b) $H^2(H, C)$ *is cyclic of order $|H|$.*

Then the choice of a generator for $H^2(G, C)$ determines canonical isomorphisms

$$\hat{H}^r(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{r+2}(G, C)$$

for all $r \in \mathbb{Z}$.

This is proved in Cassels-Fröhlich and in Milne's notes as Theorem 3.11.

4. Local reciprocity

Let L/K be a finite abelian extension of p-adic fields, $G = Gal(L/K)$, $C = L^\times$; we write $\hat{H}^r(L/K, A) = \hat{H}^r(G, A)$ for any G-module A. Hypothesis (a) of Tate's theorem is Hilbert's theorem 90. Hypothesis (b) holds for $H \subset G$ cyclic. We will devote this section to proving (b) for all H, which comes down to the following theorem.

Theorem 4.1. *Let L/K be a finite Galois extension of degree n. Then there is a canonical isomorphism*

$$inv_{L/K} : H^2(L/K, L^\times) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

In fact, there are canonical isomorphisms

$$inv_K : H^2(\bar{K}/K, \bar{K}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}; inv_L : H^2(\bar{L}/L, \bar{K}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

and a commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

This will have the consequence

$$\hat{H}^r(L/K, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{r+2}(L/K, L^\times).$$

Apply this to $r = -2$ and we find

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

This is half of the local reciprocity theorem; the other half is the

Theorem 4.2 (Existence Theorem)**.** *Every open subgroup of $K^\times$ is of the form $N_{L/K}L^\times$ for some finite abelian extension L/K.*

To make sense of the groups $H^2(\bar{K}/K, \bar{K}^\times)$ we define the cohomology of the profinite group $\Gamma = Gal(\bar{K}/K)$ as the colimit with respect to inflation maps of the cohomology of its finite quotients:

$$H^*(\Gamma, A) = \varinjlim_H H^*(\Gamma/H, A^H)$$

where H runs through open normal subgroups of Γ. We only apply this to modules A such that $A = \varinjlim A^H$ as above. This is the case for $\bar{K}^\times$. In particular

Proposition 4.3. *For any such module A, $H^r(\Gamma, A)$ is a torsion group for $r > 0$.*

This is because each of the $H^r(\Gamma/H, A^H)$ is the cohomology of a finite group and is thus $|\Gamma/H|$-torsion.

Proposition 4.4. *The theorem holds when $\bar{K}$ and $\bar{L}$ are replaced by the maximal unramified extensions K^{un} and L^{un}.*

First, consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

For G finite, $H^i(G, \mathbb{Q}) = 0$ for $i > 0$ because it is $|G|$-torsion but multiplication by $|G|$ defines an automorphism of $\mathbb{Q}$. Thus there is a canonical isomorphism

$$\delta : \hat{G} = Hom(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

(where the first notation only really applies if G is abelian).

Corollary 4.5. *Let $\Gamma = Gal(K^{un}/K) \xrightarrow{\sim} \hat{\mathbb{Z}}$. The valuation map $v : (K^{un})^\times \to \mathbb{Z}$ defines an isomorphism*

$$H^2(\Gamma, (K^{un})^\times) \to H^2(\Gamma, \mathbb{Z}) \xrightarrow{\sim} Hom(\Gamma, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$$

where the next to last arrow is δ^{-1}.

Proof. Let K_n be the unramified extension of K of degree n, U_n its subgroup of units. We have already seen that $H^i(K_n/K, U_n) = 0$ for all $i > 0$; indeed this is true by the Herbrand quotient for any finite cyclic extension. Thus we have the isomorphism

$$1 \to U_n \to K_n^\times \to \mathbb{Z} \to 0$$

$$v : H^2(K_n/K, K_n^\times) \xrightarrow{\sim} H^2(K_n/K, \mathbb{Z})$$

for all n. Passing to the limit over n we have the first isomorphism in the Corollary, and the rest is automatic. □

We already know by the Herbrand quotient that $|H^2(6K, K'^{,\times})| = |\hat{H}^0(K'/K, K'^{,\times})| = [K' : K]$ when $K' \subset K^{un}$. So we need to construct canonical isomorphisms that make the diagram commute.

We will thus have to prove that the map $H^2(K^{un}/K, (K^{un})^\times) \to H^2(\bar{K}/K, \bar{K}^\times)$ is an isomorphism. We observe at least the following:

Lemma 4.6. *The inflation map $H^2(K^{un}/K, (K^{un})^\times) \to H^2(\bar{K}/K, \bar{K}^\times)$ is injective.*

Proof. Let $G = Gal(\bar{K}/K)$, $I = Gal(\bar{K}/K^{un})$ (the inertia group). Then $H^1(I, \bar{K}^\times) = 0$ by Hilbert's theorem 90, so the inflation restriction sequence for H^2 is exact:

$$0 \to H^2(G/I, (K^{un})^\times) \to H^2(G, \bar{K}^\times$$

which is exactly the claim. □

Next, we prove the commutative diagram when $\bar{K}$ and $\bar{L}$ are replaced by the maximal unramified extensions K^{un} and L^{un}:

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{\text{Res}} & H^2(L^{un}/L) \\ \downarrow{\scriptstyle \text{inv}_K} & & \downarrow{\scriptstyle \text{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The commutativity of this diagram implies in particular that

Proof. Since L^{un} is obtained by adjoining all the roots of 1 prime to p to L, we have $L^{un} = L \cdot K^{un}$. Thus the map $\Gamma_L = Gal(L^{un}/L) \to \Gamma_K = Gal(K^{un}/K)$ is injective. Let e be the ramification index over L/K; thus the map

$$v(K^{un,\times}) = v(K^\times) \to v(L^\times) = v(L^{un,\times})$$

is the inclusion of $e\mathbb{Z} \subset \mathbb{Z}$. It follows that the maps

$$H^2(\Gamma_K, K^{un,\times}) \xrightarrow{\sim} H^2(\Gamma_K, \mathbb{Z});\ H^2(\Gamma_L, L^{un,\times}) \xrightarrow{\sim} H^2(\Gamma_L, \mathbb{Z})$$

are related by multiplication by e. Thus so is the map

$$Hom(\Gamma_K, \mathbb{Q}/ZZ) = H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) \to H^1(\Gamma_L, \mathbb{Q}/ZZ) = Hom(\Gamma_L, \mathbb{Q}/ZZ)$$

On the other hand, let F_K, F_L denote the Frobenius elements in Γ_K, Γ_L; at any finite level their images generate, and $\Gamma_L = \Gamma_K^f$ where f is the residue field degree. It follows that, at any finite level K_n/K, letting $L_n = K_n \cdot L$, the map that takes F_K to $\frac{1}{n}$ takes F_L to $\frac{f}{n}$. Thus the diagram commutes when multiplied by $ef = [L : K]$. □

We write $Br(K) = H^2(\bar{K}/K, \bar{K}^\times)$, $Br(L/K) = H^2(L/K, L^\times)$.

Corollary 4.7. *Suppose L/K is a Galois extension of degree n. Then the kernel of the restriction map $H^2(\Gamma_K, K^{un,\times}) \to H^2(\Gamma_L, L^{un,\times})$ is of order n. Thus $H^2(L/K, L^\times)$ contains a cyclic subgroup of order n whose image in $Br(K)$ is contained in the image of $H^2(\Gamma_K, K^{un,\times})$.*

Proof. The first statement follows directly from the commutativity of the diagram. But then we have the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ker(Res) & \longrightarrow & Br(K^{un}/K) & \xrightarrow{Res} & Br(L^{un}/L) \\ & & \downarrow & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} \\ 0 & \longrightarrow & Br(L/K) & \xrightarrow{Inf} & Br(K) & \xrightarrow{Res} & Br(L) \end{array}$$

The bottom inflation-restriction sequence is exact because Hilbert 90 implies $H^1(Gal(\bar{K}/L, \bar{K}^\times) = 0$. An earlier lemma shows that the inflation maps are injective, thus the left-hand vertical map is also injective, which implies the second claim. □

Lemma 4.8. *Let L/K be a finite Galois extension of local fields of degree n. Then $Br(L/K)$ is cyclic of degree n.*

Proof. We have seen that $|Br(L/K)| \geq n$. We now show $|Br(L/K)| \leq n$. We already know that if L/K is cyclic, then the Herbrand quotient computation implies that $|Br(L/K)| = n$. Now (recall) $G = Gal(L/K)$ is solvable for any p-adic field. Thus we can argue by induction on $n = |G|$. If G is cyclic we are done; if not, there is an intermediate Galois extension $L \supsetneq E \supsetneq K$ with $H = Gal(L/E)$ of order m dividing n. Because $H^1(H, L^\times) = 0$ we have the exact sequence:

$$0 \to H^2(G/H, E^\times) \to H^2(G, L^\times) \to H^2(H, L^\times);$$

$$0 \to Br(L/E) \to Br(L/K) \to Br(E/K).$$

Thus $|Br(L/K)| \leq |Br(L/E)||Br(E/K)| = m \cdot n/m$ so $|Br(L/K)| = n$. Since we know it contains a cyclic subgroup of order n, it is cyclic. □

Theorem 4.9. *For every p-adic field K there is an isomorphism $inv_K : Br(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Moreover, if L/K is a finite extension of degree n, then there is a short exact sequence*

$$0 \to Br(L/K) \to Br(K) = \mathbb{Q}/\mathbb{Z} \overset{\times n}{\to} Br(L) = \mathbb{Q}/\mathbb{Z}$$

Proof. The short exact sequence is the inflation-restriction sequence in degree n. The earlier Corollary shows that the restriction map from $Br(K)$ to $Br(L)$ is multiplication by n. □

Then as promised, Tate's Theorem yields

Theorem 4.10. *Let L/K be a Galois extension of p-adic fields with Galois group G of order n. There is a canonical isomorphism*

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

5. Global class field theory

5.1. **Cohomology of idèle classes.** The aim of this section is to prove the second inequality:

Theorem 5.1. *If L/K is a* cyclic *extension of number fields, then $|C_K^\times / N_{L/K} C_L^\times| \geq [L : K]$.*

Combined with the first inequality, this implies that $|C_K^\times / N_{L/K} C_L^\times| = [L : K]$, and this is the starting point for the isomorphisms of class field theory. We begin by relating this index to cohomology:

Lemma 5.2. *If L/K is a finite Galois extension, then $\hat{H}^0(G, C_L) = C_K^\times / N_{L/K} C_L^\times$.*

Proof. Consider the short exact sequence of G-modules:

$$1 \to L^\times \to \mathbf{A}_L^\times \to C_L.$$

Since $H^1(G, L^\times) = 0$ by Hilbert's Theorem 90, we have an exact sequence for H^0:

$$1 \to K^\times \to \mathbf{A}_K^\times \to H^0(G, C_L) \to 1.$$

It follows that $\hat{H}^0(G, C_L) = H^0(G, C_L)/N_{L/K}C_L^\times = C_K/N_{L/K}C_L^\times$. □

Now we begin by computing the Herbrand quotient of C_L by writing it as the quotient of something local by an appropriate lattice. For any finite set S of places of L, define the *S-units* $U_{L,S} \subset L^\times$ of L to be the subgroup of elements that are units at all (finite) places not in S.

Lemma 5.3. *There is a finite set of places S of L, containing S_∞ and all primes ramified in L/K, and invariant under $G = Gal(L/K)$, such that the composite map*

$$\mathbf{A}_{L,S}^\times \to \mathbf{A}_L^\times \to C_L$$

is surjective, with kernel $U_{L,S}$.

Proof. We know that there is a short exact sequence

$$1 \to \mathbf{A}_{L,S_\infty}^\times \cdot L^\times \to \mathbf{A}_L^\times \to Cl(L) \to 1.$$

Since the class group $Cl(L)$ is finite, it is generated by a finite set Σ of prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$. Let S be the smallest set of places containing S_∞ and Σ and invariant under G; it is still finite, and the above observation shows the first claim. It changes nothing to add the set of ramified primes, so we do that as well. Now we have $C_L = \mathbf{A}_L^\times/L^\times = \mathbf{A}_{L,S}^\times \cdot L^\times/L^\times$, so the kernel is clearly $L^\times \cap \mathbf{A}_{L,S}^\times$, and this is easily seen to coincide with $U_{L,S}$. □

We will now compute $h(L, S) := h(\mathbf{A}_{L,S}^\times)$ and $h(U_{L,S})$. First, every $w \in S$ lies above some place v of K. Let S_K be the set of places of K below S. Then

$$\mathbf{A}_{L,S}^\times = \prod_{v \in S_K} \prod_{w|v} L_w^\times \times U^S$$

where $U^S = \prod_{w \notin S} U_w$.

Lemma 5.4. *For any place v of K, let $G_{w_0} \subset G$ denote the decomposition group at some $w_0 \mid v$. For all i there are isomorphisms*

$$H^i(G, \prod_{w|v} L_w^\times) \xrightarrow{\sim} H^i(G_{w_0}, L_{w_0}^\times);$$

$$H^i(G, \prod_{w|v} U_w^\times) \xrightarrow{\sim} H^i(G_{w_0}, U_{w_0}^\times).$$

In particular, the right-hand side depends only on v and not on the choice of w_0, so we write it $H^i(G^v, L^v), H^i(G^v, U^v)$

Proof. Indeed, since G permutes the $w \mid v$ transitively, we have the isomorphism

$$\prod_{w|v} L_w^\times = \Lambda_G \otimes_{\Lambda_{G_{w_0}}} L_{w_0}^\times$$

of G-modules, and likewise for U_{w_0}. Thus the Lemma is a consequence of Shapiro's Lemma. □

Proposition 5.5. *For any $i \in \mathbb{Z}$ we have*

$$\hat{H}^i(G, \mathbf{A}_L^\times) = \oplus_v \hat{H}^i(G^v, L^v).$$

Proof. We write $\mathbf{A}_L^\times = \varinjlim_S \mathbf{A}_{L,S}^\times$ where S runs over sets of primes of K containing all the ramified or archimedean primes and the notation means that one takes products over all divisors of primes in S. Now we have shown that, if v is unramified in L, then

$$\hat{H}^i(G, \prod_{w|v} U_w) = \hat{H}^i(G^v, U^v) = 0$$

for all i. It follows that

$$\hat{H}^i(G, \mathbf{A}_{L,S}^\times) = \prod_{v \in S} \hat{H}^i(G^v, L^v) = \oplus_{v \in S} \hat{H}^i(G^v, L^v)$$

Taking the limit over S we obtain the result. □

Corollary 5.6 (Local Corollary)**.** *(a) $H^1(G, \mathbf{A}_L^\times) = 0$.*

(b) $H^2(G, \mathbf{A}_L^\times) = \oplus_v H^2(G^v, L^v) = \oplus_v (\frac{1}{[L^v : K_v]}\mathbb{Z}/\mathbb{Z})$.

Theorem 5.7. *Suppose L/K is a cyclic extension of degree n. Then $h(C_L) = n$.*

Proof. By the exact sequence already introduced, we know that

$$h(C_L) = h(\mathbf{A}_{L,s}^\times)/h(U_{L,S}).$$

so we need to compute the two terms. By the local Corollary above, we know that $h^1(\mathbf{A}_{L,s}^\times) = 1$ and $h^2(\mathbf{A}_{L,s}^\times) = \prod_{v \in S_K} n_v$ where n_v is the order of the local decomposition group. In order to compute $h(U_{L,S})$ we need to construct two lattices M_1, M_2 in a real vector space V, invariant under G, such that $h(M_1) = \prod_{v \in S_K} n_v$ and $h(M_2) = nh(U_{L,S})$. This will imply

$$h(U_{L,S}) = (\prod n_v)/n$$

and thus $h(C_L) = n$. Here we are using the fact that

Fact 5.8. *Any two G-invariant lattices in the same vector space have the same Herbrand quotient, whether or not they are commensurable.*

The proof uses character theory: If M_1 and M_2 generate the same real vector space V and are invariant under G, then $M_1 \otimes \mathbb{Q}$ and $M_2 \otimes \mathbb{Q}$ have the same character, thus are isomorphic as representations of G. Thus they contain isomorphic lattices $N_1 \equiv N_2$, which *are* commensurable with M_1 and M_2, respectively; but then $h(M_1) = h(N_1) = h(N_2) = h(M_2)$.

So we need to find V and the two lattices. We let $V = \mathbb{R}^S$, $M_1 = \mathbb{Z}^S \subset \mathbb{R}^S$. Then by Shapiro's Lemma,

$$\hat{H}^i(G, M_1) = \hat{H}^i(G^v, \mathbb{Z})$$

with the trivial action. But $\hat{H}^0(G_v, \mathbb{Z}) = \mathbb{Z}/|G_v|\mathbb{Z}$ has order n_v, while $H^1(G_v, \mathbb{Z}) = Hom(G_v, \mathbb{Z}) = 0$ because G_v is a finite group. Thus

$$h(M_1) = \prod_{v \in S} n_v.$$

On the other hand, we think of $\mathbb{R}^S$ as the space of functions from S to $\mathbb{R}$. For each $u \in U_{L,S}$, we define a function

$$\lambda_u : S \to \mathbb{R}; \lambda_u(w) = \log ||u||_w.$$

This defines a homomorphism $\lambda : U_{L,S} \to V$. If $S = S_\infty$, then $U_{L,S} = \mathcal{O}_L^\times$, $V = \mathbb{R}^{r_1+r_2}$, and the image of λ is a lattice in $H \subset V$ which is the hyperplane for which $\sum_v a_v = 0$.

Fact 5.9. *For any S, the image of λ is a lattice in the hyperplane in V defined in the same way.*

The orthogonal hyperplane is spanned by the vector $e_0 = (1, \ldots, 1)$ and $\lambda(U_{L,S}) \oplus \mathbb{Z}e_0$ is an invariant lattice M_2 in V. Since e_0 is fixed under G, we have

$$h(M_2) = h(U_{L,S})h(\mathbb{Z}) = h(U_{L,S}) \cdot n.$$

This completes the proof. □

Corollary 5.10. *The second inequality: $|C_K^\times / N_{L/K} C_L^\times| = [L : K]$ when L/K is cyclic. Moreover $h_1(C_L) = 1$ in this case.*

Proof. We have already seen that $h(C_L) = h_0(C_L)/h_1(C_L) = n$, so $h_0(C_L) = nh_1(C_L) \geq n$. On the other hand, we proved that $h_0(C_L) = |C_K^\times / N_{L/K} C_L^\times|$. This implies the second inequality, and combined with the first inequality this gives both claims in the corollary. □

This has a remarkable consequence:

Theorem 5.11. *Let L/K be a cyclic extension of degree $n > 1$. Then there are infinitely many primes of K that do not split completely in L.*

Proof. Suppose not, and let S be the finite set of primes of K that do not split completely in L. Let $a \in \mathbf{A}_K^\times$. By the approximation theorem, there is an $\alpha \in K^\times$ such that $\alpha \cdot a$ is very close to 1 at all primes in S, hence is a local norm at all $v \in S$. For $v \notin S$, $\alpha \cdot a$ is a local norm because every element is a local norm, because v splits completely in L. Thus there is some $b \in \mathbf{A}_L^\times$ such that

$$\alpha \cdot a = N_{L/K} b$$

in other words, $C_K / N_{L/K} C_L = 1$. This contradicts the second inequality. □

5.2. **Surjectivity of the Artin map.** We begin by recalling a definition from the very beginning of algebraic number theory. Let L/K be an abelian extension with Galois group G, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then the decomposition group $D_\mathfrak{p} \subset G$ is well-defined and independent of the prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in $\mathcal{O}_L$. Let S denote the set of primes that ramify in L/K, and suppose $\mathfrak{p} \notin S$. Then

$$D_\mathfrak{p} \xrightarrow{\sim} Gal(k(\mathfrak{P})/k(\mathfrak{p}))$$

for any $\mathfrak{P} \mid \mathfrak{p}$. Let $Frob_\mathfrak{p} \in Gal(k(\mathfrak{P})/k(\mathfrak{p}))$ denote the generator $x \mapsto x^{N\mathfrak{p}}$. Then $Frob_\mathfrak{p}$ defines a canonical element, denoted

$$(\mathfrak{p}, L/K) \in G.$$

This defines the *Artin map*

$$I^S \to G$$

where I^S is the group of ideals prime to S. The original Takagi-Artin reciprocity law is the statement that the Artin map defines an isomorphism $I^S / * * \xrightarrow{\sim} G$ for an appropriate subgroup $**$ of the group of ideals, involving the norms . The adèlic formalism of class field theory does not depend on the choice of S. We note the following fact:

Lemma 5.12. *Let $L \supset F \supset K$ be a tower of abelian extensions. Let $\mathfrak{p} \subset K$ a prime ideal unramified in L. Then*

$$(\mathfrak{p}, L/K) \mid_F = (\mathfrak{p}, F/K).$$

Proof. Let $k(\mathfrak{P}) \supset k(\mathfrak{p}') \supset k(\mathfrak{p})$ be the corresponding sequence of residue fields, where $\mathfrak{p}' = \mathfrak{P} \cap F$. Then the Frobenius for $k(\mathfrak{P})/k(\mathfrak{p})$, restricted to $k(\mathfrak{p}')$, is clearly the Frobenius for $k(\mathfrak{p}')/k(\mathfrak{p})$. So the Lemma is obvious. □

Theorem 5.13. *Let L/K be an abelian extension, and let $S' \supset S$ be any finite set of primes of K containing those ramified in L. Then the Artin map from $I^{S'}$ to $Gal(L/K)$ is surjective.*

Proof. Let $H \subset G$ denote the image of $I^{S'}$ and let $F = L^H$. We need to show that $F = K$. By definition, for any $\mathfrak{p} \notin S'$, $(\mathfrak{p}, L/K)$ fixes F. In other words $D_{\mathfrak{p}}$ fixes F. But the Lemma implies that $1 = (\mathfrak{p}, L/K) \mid_F = (\mathfrak{p}, F/K)$ for any $\mathfrak{p} \notin S'$. This means precisely that every $\mathfrak{p} \notin S'$ splits completely in F. Since $Gal(F/K)$ is abelian, it has a non-trivial cyclic quotient, say $Gal(F'/K)$. It follows that all but finitely many $\mathfrak{p}$ split completely in F', and this contradicts the Theorem obtained from the Second Inequality. □

5.3. **Interlude: Kummer theory.** We will soon need to exhibit explicit abelian extensions of a number field K. We know that nth roots of elements of $K^\times$ give rise to extensions of degree dividing n, provided the nth roots of unity are in K. Here we formalize this using cohomology of groups.

Let $\bar{K}/K$ denote the algebraic closure, $G = Gal(\bar{K}/K)$. Let $n \geq 1$. We consider the short exact sequence of G-modules:

$$1 \to \mu_n \to \bar{K}^\times \stackrel{t \mapsto t^n}{\to} \bar{K}^\times \to 1$$

where μ_n is the group of nth roots of unity in $\bar{K}$. The exactness is just the assertion that every element of $\bar{K}^\times$ has an nth root – indeed, has n-distinct nth roots. Clearly $H^0(G, \bar{K}^\times) = K^\times$. The long exact cohomology sequence thus yields

$$0 \to \mu_n(K) \to K^\times \stackrel{t \mapsto t^n}{\to} K^\times \to H^1(G, \mu_n) \to H^1(G, \bar{K}^\times) = 0$$

where the last equality is Hilbert 90. In other words, we have an isomorphism

$$K^\times/(K^\times)^n \stackrel{\sim}{\longrightarrow} H^1(G, \mu_n).$$

Concretely, if $a \in K^\times$, there is some $b \in \bar{K}$ with $b^n = a$. Then $\delta_a(\sigma) = \sigma(b)/b$ is an element of μ_n for any $\sigma \in G$, and the map $\sigma \mapsto \delta_a(\sigma)$ is a cocycle whose class in $H^1(G, \mu_n)$ doesn't depend on the choice of b.

Suppose $\mu_n(K) = \mu_n$. Then $H^1(G, \mu_n) = Hom(G, \mu_n) = Hom(G^{ab}, \mu_n)$. Thus we have the *Kummer pairing*

$$K^\times/(K^\times)^n \times G^{ab}/G^{ab,n} \to \mu_n$$

and the cohomology isomorphism exactly is equivalent to the assertion that this is a perfect pairing of $\mathbb{Z}/n\mathbb{Z}$-modules. In particular, if all the nth roots of 1 are in K, then every abelian extension of K of degree n is a *Kummer extension* – that is, it is generated by the nth roots of some element of $K^\times$. This shows that every abelian extension of K is contained in a Kummer extension of some cyclotomic extension. For this reason, cyclotomic fields play a central role in CFT.

5.4. **The reciprocity law.** In this section L/K is a finite abelian extension of number fields. We have defined two local maps from idèles to Galois groups. First, suppose v is an unramified place for L/K. We define

$$r_v : K_v^\times \to K_v^\times/\mathcal{O}_{K_v}^\times \to Gal(L_w/K_v) \subset Gal(L/K)$$

by sending ϖ_v to $Frob_v$. On the other hand, for any v, we have the local reciprocity isomorphism

$$r_v : K_v^\times/N_{L_w/K_v}L_w^\times \xrightarrow{\sim} Gal(L_w/K_v) \subset Gal(L/K).$$

Theorem 5.14. *These two maps coincide when v is unramified.*

Proof. This will follow from the Lubin-Tate theory. □

Theorem 5.15. *(a) Define $r : \mathbf{A}_K^\times \to Gal(L/K)$ by $r((a_v)) = \prod_v r_v(a_v)$. Suppose $a \in K^\times$. Then $r(a) = 1$.*

(b) For any finite extension L/K of number fields, and any $\alpha \in Br(L/K) = H^2(L/K, L^\times)$ we have

$$\sum_v inv_v(\alpha) = 0.$$

The proofs of (a) and (b) are intertwined and this is where cyclotomic fields play an important role. Before embarking on the proofs, we state the reciprocity law, which is a consequence of (a) and the two inequalities.

Theorem 5.16 (Reciprocity law)**.** *Let L/K be a finite abelian extension of number fields. Then the reciprocity law defines an isomorphism*

$$r : \mathbf{A}_K^\times/K^\times N_{L/K}\mathbf{A}_L^\times \to Gal(L/K).$$

Proof. Part (a) of the last theorem states that the map $r = \prod_v r_v : \mathbf{A}_K^\times \to Gal(L/K)$ factors through $\mathbf{A}_K^\times/K^\times$. On the other hand, each r_v is trivial on the local norms, so r factors through $r : \mathbf{A}_K^\times/K^\times N_{L/K}\mathbf{A}_L^\times$. The map is surjective by the compatibility of the local r_v with the global Artin maps and by the argument involving the second inequality. On the other hand, the first inequality states that

$$|\mathbf{A}_K^\times/K^\times N_{L/K}\mathbf{A}_L^\times| \leq |Gal(L/K)|.$$

Thus the surjective map must be an isomorphism. □

5.4.1. *Consequences of the reciprocity law for cyclotomic extensions.* We know the cyclotomic reciprocity law if $L/\mathbb{Q}$ is contained in a cyclotomic field $K_n = \mathbb{Q}(\zeta_n)$ for some $n > 1$: there is an isomorphism

$$\alpha_n : (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} Gal(K_n/\mathbb{Q}); \alpha_n(a) = [\zeta_n \mapsto \zeta_n^a].$$

Now the inclusion map $\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times \to \mathbf{A}_\mathbb{Q}^\times/\mathbb{Q}^\times \cdot \mathbb{R}_+^\times$ is an isomorphism (by unique factorization in $\mathbb{Z}$) and we see that

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} C_\mathbb{Q}/U(n)\mathbb{R}_+^\times$$

where $U(n) = \prod_{p\nmid n} \mathbb{Z}_p^\times \times \prod_{p^a||n}(1 + p^a\mathbb{Z}_p)$. Thus we have a sequence of maps for each place v of $\mathbb{Q}$:

$$\theta_v : \mathbb{Q}_v^\times \to C_\mathbb{Q} \to (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} G = Gal(K_n/\mathbb{Q}).$$

Now our goal is to prove that the product of the local norm residue maps

$$\prod_v r_v(a) = 1 \in G \ \forall a \in \mathbb{Q}^\times.$$

It suffices to take $n = q^r$ for a prime q and $r \geq 1$, because – this was proved in the homework – $r_{K/\mathbb{Q}_v}(a)|_{K'} = r_{K'/\mathbb{Q}_v}(a)$ if $K \supset K' \supset \mathbb{Q}_v$. We can check separately for $a = -1$ and $a = p$ prime, since these generate $\mathbb{Q}^\times$.

First suppose $q = p$. Then $r_p(p) = 1$, because p is a norm in any pth power cyclotomic extension, $r_\infty(p) = 1$ because $p > 0$, and $r_v(p) = 1$ for $v \neq p$ because p is a unit.

Next, suppose $q \neq p$. Then $r_q(p)(\zeta) = \zeta^{p^{-1}}$ by Lubin-Tate theory, $r_\infty(p) = 1$ still, $r_v(p) = 1$ if $v \neq p, q$ because p is a unit at v and v is unramified in K_n, and $r_p(p)(\zeta) = Frob_p(\zeta) = \zeta^p$ because $\mathbb{Q}_p(\zeta)$ is unramified over $\mathbb{Q}_p$. Thus $r_q(p) \circ r_p(p)(\zeta) = \zeta$.

Finally, $r_\infty(-1)$ equals complex conjugation, because it's the only non-trivial element of $Gal(\mathbb{C}/\mathbb{R})$; $r_v(-1) = 1$ for $v \neq q$ because -1 is a unit and v is unramified; and $r_q(-1)(\zeta) = \zeta^{-1}$ as above because $-1 = (-1)^{-1}$. Thus we have

Proposition 5.17. *Part (a) of the reciprocity law holds for subfields of cyclotomic extensions of* $\mathbb{Q}$.

Now we show:

Lemma 5.18. *Suppose part (a) of the reciprocity law holds for an abelian extension L/K. Then it holds for LK'/K' for any extension K'/K. In particular, part (a) of the reciprocity law holds for any cyclotomic extension of K'.*

Proof. We need to determine the relation between the local reciprocity laws for LK'/K' and L/K; note that $Gal(LK'/K') \hookrightarrow Gal(L/K)$. Let $E, F' \supset F$ be two extensions of p-adic fields, $E' = EF'$, $G = Gal(E/F)$ abelian, $H = Gal(E'/F') \subset G$. Consider

$$H = \hat{H}^{-2}(H, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^0(H, E'^{,\times});\ G = \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^0(G, E^\times).$$

Fact 5.19. *These diagrams are related by corestriction. More precisely, there is a commutative diagram*

$$\begin{array}{ccccc} F'^{,\times} & \longrightarrow & \hat{H}^0(H, E'^{,\times}) & \xrightarrow{r_{F'}} & H = \hat{H}^{-2}(H, \mathbb{Z}) \\ {\scriptstyle Cor = N_{F'/F}}\downarrow & & & & \downarrow{\scriptstyle Cor} \\ F^\times & \longrightarrow & \hat{H}^0(G, E^\times) & \xrightarrow{r_F} & G = \hat{H}^{-2}(G, \mathbb{Z}) \end{array}$$

where the corestriction on the left is the norm map and the corestriction on the right is inclusion.

The proof uses the interpretation of the local norm residue map as cup product with the fundamental class, properties of the cup product, and identification of the restriction on the fundamental class. I return to this later if I have time. (It was given as the second problem on Assignment 6.)

It follows that there is a global commutative diagram

$$\begin{array}{ccc} \mathbf{A}_{K'}^\times & \xrightarrow{r_{K'}} & Gal(LK'/K') \\ {\scriptstyle Cor = N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \iota} \\ \mathbf{A}_K^\times & \xrightarrow{r_K} & Gal(L/K) \end{array}$$

where ι is the inclusion. It follows that if $a \in K'^{,\times}$ then $\iota(r_{K'}(a)) = r_{\mathbb{Q}}(N_{K'/K}(a)) = 1$ by assumption that the reciprocity law holds for K. Thus it holds for K' because ι is injective. □

We now drop the K' and let K be a general number field. We note the following consequence of the Second Inequality

Theorem 5.20. *If L/K is a Galois extension, $G = Gal(L/K)$, then $H^1(G, C_L) = 0$.*

Proof. It suffices by a theorem on cohomology of finite groups to replace G by a p-Sylow subgroup; thus we may assume G nilpotent. If G is cyclic then it follows from the Second Inequality. Now induct on $|G|$; if $H \subset G$ is a proper normal subgroup, with G/H cyclic, we have

$$0 \to H^1(G/H, C_{L^H}) \to H^1(G, C_L) \to H^1(H, C_L)$$

and since the two outer groups vanish by induction, so does $H^1(G, C_L)$. □

Proposition 5.21. *Let K be a number field and let $\alpha \in Br(K)$. Then there is a cyclic cyclotomic extension L/K such that $Res_{L/K}(\alpha) = 0 \in Br(L)$.*

Proof. First of all, for any Galois extension E/K, $G = Gal(E/K)$ the short exact sequence

$$1 \to E^\times \to \mathbf{A}_E^\times \to C_E \to 1$$

yields

$$H^1(G, C_E) = 0 \to Br(E/K) \to H^2(G, \mathbf{A}_E^\times) = \oplus_v Br(E^v/K_v)$$

where the first 0 is the previous theorem and the expression on the left follows from the computation of the cohomology of the idèle group. Passing to the limit over E, we find the important embedding

$$0 \to Br(K) \hookrightarrow \oplus_v Br(K_v)$$

Thus the Proposition comes down to proving that, given α with $inv_v(\alpha) = \frac{a_v}{b_v}$ for $v \in S$ (and $inv_v(\alpha) = 0$ otherwise), there is a cyclic cyclotomic L/K such that $[L_w : K_v]$ is a multiple of b_v for every $v \in S$; indeed $res_{L_w/K_v} : Br(K_v) \to Br(L_w)$ is multiplication by $[L_w : K_v]$.

Now we have to play with cyclotomic fields. The proof is finished by the following Lemma. □

Lemma 5.22. *Let $K/\mathbb{Q}$ be a finite extension, S a finite set of primes of K, and a positive integer m, there exists a cyclic cyclotomic extension L/K whose local degrees are divisible by m at all non-archimedean $v \in S$ and by 2 at every real place of S; in other words, L is totally imaginary.*

Proof. By multiplying m by $[K : \mathbb{Q}]$ we may reduce to $K = \mathbb{Q}$. Let q be an odd prime, $r \geq 1$; then $Gal(K_{q^r}/\mathbb{Q}) = C_{q-1} \times C_{q^{r-1}}$ where C_d is the cyclic group of order d. In particular, it has a subfield $L(q, r)$ with $Gal(L(q, r)/\mathbb{Q})$ cyclic of order q^{r-1}. Now complete at some prime p: since

$$\lim_{r\to\infty} [\mathbb{Q}_p(\zeta_{q^r}) : \mathbb{Q}_p] = \infty$$

(because any finite extension of $\mathbb{Q}_p$ has only finitely many roots of 1) and since $[\mathbb{Q}_p(\zeta_{q^r}) : \mathbb{Q}_p \cdot L(q, r)] \leq q - 1$ for all r, it follows that

$$[\mathbb{Q}_p \cdot L(q, r) : \mathbb{Q}_p] \to \infty$$

as r goes to infinity; and since its Galois group is cyclic of order q^r, we may assume the local degrees are arbitrarily divisible by q.

If $q = 2$ then $Gal(K_{q^r}/\mathbb{Q}) \xrightarrow{\sim} = C_2 \times C_{2^{r-2}}$; one checks that the subfield $L(2, r)$ fixed by the cyclic group of order 2 is totally imaginary,

and the degree of its compositum with $\mathbb{Q}_p$ tends to infinity for any $p \in S$, as before.

Thus we take the compositum of $L(q,r)$ for all q dividing m for sufficiently large r, and add $L(2,r)$ to get rid of real places. □

5.4.2. *Proof of the reciprocity law.* We follow Tate's argument in Cassels-Fröhlich.

Lemma 5.23. *Let L/K be a finite abelian extension with Galois group G. Let $\chi \in \hat{G} = Hom(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$. If v is a place of K, let $\chi_v = \chi|_{D_v}$. Let $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z})$. If $(a_v) \in \mathbf{A}_K^\times$ let $(\overline{a_v})$ denote its image in $\hat{H}^0(G, \mathbf{A}_K^\times)$.*

Then for each v we have

$$inv_v(\overline{a_v} \cup \delta(\chi)) = \chi_v(r_v(a_v)).$$

In particular,

$$\sum_v inv_v(\overline{a_v} \cup \delta(\chi)) = \sum_v \chi_v(r_v(a_v)) = \chi(r_{L/K}((a_v))).$$

Corollary 5.24. *Let L/K be a cyclic cyclotomic extension. Suppose part (a) of the reciprocity theorem holds for K. Then part (b) holds for any $\alpha \in Br(L/K)$. In particular, part (a) implies part (b).*

Proof of Corollary. In the statement of the lemma, let χ be injective. Recall from the theory of Tate cohomology of cyclic groups that cup product with a generator of $H^2(G, \mathbb{Z})$ defines an isomorphism of functors $\hat{H}^0 \xrightarrow{\sim} H^2$. Apply this to cohomology of $L^\times$:

$$K^\times / N_{L/K} L^\times = \hat{H}^0(L/K, L^\times) \xrightarrow{\sim} Br(L/K),$$

we see that every $\alpha \in Br(L/K)$ is of the form $(\overline{a}) \cup \delta\chi$ for some $a \in K^\times$. It follows from the lemma that

$$\sum_v inv_v(\alpha) = \sum_v inv_v(\overline{a} \cup \delta(\chi)) = \sum_v \chi_v(r_v(a)) = \chi(r_{L/K}(a)) = 0,$$

where the last equality is the hypothesis that part (a) holds. This is precisely (b) for $\alpha \in Br(L/K)$. The final assertion then follows from the proposition on cyclotomic fields. □

Highly unenlightening proof of Lemma. We restate Tate's theorem in its full glory.

Tate's theorem: Let G be a group of order n and let C be any G module. Suppose for all $H \subset G$,

(a) $H^1(H, C) = 0$;
(b) $H^2(H, C)$ is cyclic of order $|H|$.

Then the choice of a generator $u \in H^2(G, C)$ determines canonical isomorphisms

$$a \mapsto u \cup a : \hat{H}^r(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{r+2}(G, C)$$

for all $r \in \mathbb{Z}$.

In the setting of local class field theory, we have $G = Gal(E/F)$ and $C = E^\times$ with $E = L_w$, $F = K_v$, $r = r_v$; then we let $u_{E/F} \in Br(L/K)$ denote the generator such that $inv(u_{E/F}) = \frac{1}{n} \in \mathbb{Q}/\mathbb{Z}$. Then

$$u_{E/F} \cup r_v(a_v) = \bar{a}_v \in \hat{H}^0(G, E^\times).$$

Now cup product is associative, so

$$\bar{a}_v \cup \delta(\chi_v) = u_{E/F} \cup r_v(a_v) \cup \delta(\chi_v) = u_{E/F} \cup r_v(a_v) \cup \delta(\chi_v)) = u_{E/F} \cup \delta(r_v(a_v) \cup \chi_v).$$

The last formula

$$r_v(a_v) \cup \delta(\chi_v)) = \delta(r_v(a_v) \cup \chi_v)$$

is a special case of the formula: if A and $0 \to B \to B' \to B'' \to 0$ are G-modules such that the tensor product

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

is still exact, then

$$\delta(a \cup b'') = a \cup \delta(b'') \in \hat{H}^{i+j+1}(G, A \otimes B)$$

with the obvious notation. In our present situation $r_v(a_v) \in \hat{H}^{-2}(G, A)$ with $A = \mathbb{Z}$ and the short exact sequence is $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, so the exactness is clear.

Now $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ and $r_v(a_v) \in \hat{H}^{-2}(G, \mathbb{Z})$ so

$$r_v(a_v) \cup \chi_v \in \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

so we identify $r_v(a_v) \cup \chi_v$ with an element in $\mathbb{Z}/n\mathbb{Z}$. Thus if we write $r_v(a_v) \cup \chi = \frac{r}{n}$ we have that $\delta(r_v(a_v) \cup \chi)$ equals the image of r in $\mathbb{Z}/n\mathbb{Z}$. Thus

$$\bar{a}_v \cup \delta(\chi_v) = u_{E/F} \cup \delta(r_v(a_v) \cup \chi_v) = r \cdot u_{E/F}$$

and $inv(\bar{a}_v \cup \delta(\chi_v)) = r \cdot inv(u_{E/F}) = \frac{r}{n}$. On the other hand, the following diagram commutes

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) \otimes H^1(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & G^{ab} \otimes Hom(G, \mathbb{Q}/\mathbb{Z}) \\ \cup \downarrow & & ev \downarrow \\ H^{-1}(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \end{array}$$

(this is the homework). Thus $\chi(r_v(a_v)) = r_v(a_v) \cup \chi = \frac{r}{n}$ again, so the identification follows. $\square$

The Lemma has a second corollary that completes the proof of the reciprocity law:

Corollary 5.25. *Part (b) of the reciprocity law implies part (a), and thus the reciprocity law.*

Proof. We have an abelian extension L/K with Galois group G and we need to prove that $r_{L/K}(a) = 1$ for any $a \in K^\times \subset \mathbf{A}_K^\times$. Let $\chi \in \hat{G}$. Let a^* denote the image of a in $\hat{H}^0(L/K)$. Then $a^* \cup \delta\chi \in H^2(G, L^\times) \subset Br(K)$. The image of $a^* \cup \delta\chi \in H^2(G, \mathbf{A}_L^\times)$ is then $\overline{a} \cup \delta(\chi)$. Then

$$\sum_v inv_v(\overline{a} \cup \delta(\chi)) = \chi(r_{L/K}(a)).$$

Assuming part (b) of the reciprocity law for $Br(K)$ we know that the left-hand side of the above equality equals 0 for all χ. Thus $\chi(r_{L/K}(a)) = 1$ for all $\chi \in \hat{G}$ and $a \in K^\times$. It follows that $r_{L/K}(K^\times) = 1$. □

The lemma has a third corollary: Suppose $E/F'/F$ is a tower of abelian extensions of p-adic fields with $G = Gal(E/F) \supset H = Gal(E/F')$. Suppose $\chi' \in Hom((G/H), \mathbb{Q}/\mathbb{Z})$ inflates to $\chi \in Hom(G, \mathbb{Q}/\mathbb{Z})$. Then under the natural inflation map $inf : \hat{H}^2(G/H, \mathbb{Z}) \to \hat{H}^2(G, \mathbb{Z})$, we have

$$inf(\delta(\chi')) = \delta(inf(\chi')) = \delta(\chi).$$

Suppose $a \in F^\times$; then

$$\chi(r_{E/F}(a)) = inv_F(\bar{a} \cdot \delta(\chi)) = inv_F(\bar{a} \cdot \delta(\chi')) = \chi'(r_{F'/F}(a)).$$

Since this is true for any χ', it follows that $r_{E/F}(a)|'_F = r_{F'/F}(a)$. Thus we can define $r_{F^{ab}/F}(a) \in Gal(F^{ab}/F)$ consistently by means of finite extensions.

5.5. **The existence theorem.**

Theorem 5.26. *Let K be a number field. Let $U \subset C_K$ be an open subgroup of finite index. Then there is an abelian extension L/K such that $U = N_{L/K}C_L$. (We say that U is a* **norm subgroup**.

We prove this by reduction to the simplest cases. In what follows K is fixed.

Lemma 5.27. *Suppose $U \supset V$ and V is a norm subgroup. Then U is a norm subgroup.*

Proof. Say $V = N_{E/K}C_E$, so the reciprocity map is an isomorphism

$$r : C_K/N_{E/K}C_E \xrightarrow{\sim} Gal(E/K).$$

Let $H = r(U) \subset Gal(E/K)$ and let $L = E^H$. Thus $C_K/U \xrightarrow{\sim} Gal(L/K)$. But by the reciprocity law, the kernel of the map $C_K \to Gal(L/K)$ is precisely $N_{L/K}C_L$. □

We write ζ_n for a primitive nth root of 1.

Proposition 5.28. *Suppose $\zeta_n \in K$. Let $S \supset S_\infty$ be a sufficiently large set of primes containing all primes dividing n and generators of $Cl(K)$. Suppose $a \in K^\times$ has the property that*

- *[a] For all $v \in S$, $a \in K_v^{\times,n}$.*
- *[b] For all $v \notin S$, $a \in \mathcal{O}_{K_v}^\times$.*

Then $a \in K^{\times,n}$.

Proof. Let $L = K(\sqrt[n]{a})$. This is an abelian extension of K by hypothesis. Now every $v \in S$ splits completely in L by hypothesis [a], so $K_v^\times \subset N_{L/K}\mathbf{A}_L^\times$. On the other hand, every $v \notin S$ is unramified in L by hypothesis [b], since S contains all primes dividing n, so $\prod_{v\notin S} \subset U_v \subset N_{L/K}\mathbf{A}_L^\times$. Since the primes in S generate $Cl(K)$, it follows that $\mathbf{A}_{K,S}^\times$ generates C_K, so $N_{L/K}C_L = C_K$ and $L = K$ by the reciprocity theorem. □

Lemma 5.29. *Let p be prime and suppose $\zeta_p \in K$. Let $\bar{V} \subset C_K$ be an open subgroup such that C_K/V is annihilated by p. Then $\bar{V}$ is a norm subgroup.*

Proof. Let S be as in the proposition. Let $\mathcal{U} = U_{K,S}$ be the group of S-units of K, and let $L = K(\sqrt[p]{\mathcal{U}})$. Let

$$W = W_S = \prod_{v\in S} K_v^{\times,p} \times \prod_{v\notin S} \subset U_v \subset \mathbf{A}_K^\times.$$

We prove that the image $\bar{W}$ of W in C_K equals $N_{L/K}C_L$ by showing

- (i) $W \subset N_{L/K}\mathbf{A}_L^\times$
- (ii) $[C_K : \bar{W}] = [C_K : N_{L/K}C_L] = p^s$ where $s = |S|$.

Point (i) is local. For any v, $N_{L/K}L_v^\times \supset K_v^{\times,p}$. This takes care of $v \in S$, and any $v \notin S$ is unramified in L, so we have shown (i).

Point (ii) requires a formula for the local power index. We know that

$$[C_K : N_{L/K}C_L] = [L : K] = [\mathcal{U} \cdot K^{\times,p} : K^{\times,p}]$$

where the first equality follows from reciprocity and the second from Kummer theory. so it suffices to show that

$$[C_K : \bar{W}] = [\mathcal{U} \cdot K^{\times,p} : K^{\times,p}] = [\mathcal{U} : \mathcal{U} \cap K^{\times,p}] = |\mathcal{U}/\mathcal{U}^p| = p^s$$

by the Dirichlet unit theorem for S-units, because $\mathcal{U} \supset \zeta_p$.

On the other hand, by our choice of S,

$$[C_K : \bar{W}] = [\mathbf{A}_{K,S}^\times \cdot K^\times : W \cdot K^\times] = [\mathbf{A}_{K,S}^\times : W]/[\mathbf{A}_{K,S}^\times \cap K^\times : W \cap K^\times]$$

where the second equality follows from

LEMMA 6.5 *Let A, B, and C be subgroups of some abelian group, and assume that $A \supset B$. Then*

$$(AC : BC)(A \cap C : B \cap C) = (A : B)$$

in the sense that, if two of the indexes are finite, so is the third, and the equality holds.

Now the denominator is just $[\mathcal{U} : \mathcal{U}^p] = p^s$ again, by the Proposition on local and global p-th powers. To determine the numerator, we use the

Fact 5.30. *Let F be a local field containing ζ_p. Then $[F^\times : (F^\times)^p] = p^2/||p||_F$.*

This is clear for $F = \mathbb{R}$ or $\mathbb{C}$ and it is one of the points skipped in the treatment of p-adic fields. See below for a sketch. It then follows that

$$[\mathbf{A}_{K,S}^\times : W] = \prod_{v \in S} [K_v^\times : (K_v^\times)^p] = \prod_{v \in S} p^2/||p||_v = \prod_{v \in S} p^2 = p^{2s}$$

because $||p||_v = 1$ for $v \notin S$, to the product formula implies $\prod_{v \in S} ||p||_v = 1$. We have proved point (ii).

Finally, let $\bar{V}$ be as in the statement, V its inverse image in $\mathbf{A}_K^\times$. Then V contains $W = W_S$ for some set S, and we have just shown that $\bar{W}$ is a norm subgroup. Thus $\bar{V}$ is a norm subgroup. □

Here is a proof of the formula $[F^\times : (F^\times)^p] = p^2/||p||_F$. Recall that

$$1/||\varpi_F||_F = N\mathfrak{m}_F = p^{ef} = p^{[F:\mathbb{Q}_p]}.$$

Now t suffices to show that $[\mathcal{O}_F^\times : (\mathcal{O}_F^\times)^p] = p/||p||_F = p \cdot p^{[F:\mathbb{Q}_p]}$ because we know that the valuation group is isomorphic to $\mathbb{Z}$. Moreover, $[\mathcal{O}_F^\times : \mathcal{O}_F^1]$, where $\mathcal{O}_F^1 = 1 + \mathfrak{m}$, is of order prime to p, so we can replace $\mathcal{O}_F^\times$ by $\mathcal{O}_F^1$. But now there is a p-adic analytic homomorphism

$$\log : \mathcal{O}_F^1 \to F$$

with open image. Thus the kernel is discrete, and since the domain is compact, the kernel is finite and consists of p-power roots of unity. This subgroup is non-trivial, by hypothesis, so if $V = Im(\log)$ it follows that

$$[\mathcal{O}_F^1 : (\mathcal{O}_F^1)^p] = p \cdot [V : pV].$$

But V is an open subgroup of an $[F : \mathbb{Q}_p]$-dimensional $\mathbb{Q}_p$-vector space, and this completes the proof.

The final step is to get rid of the cyclotomic hypothesis.

Lemma 5.31. *Let $U \subset C_K$ an open subgroup of finite index. Suppose $U' = N_{K'/K}^{-1}(U)$ is a norm subgroup for some finite cyclic extension K'/K. Then U is a norm subgroup.*

Proof. Let L/K' be the abelian extension corresponding to U'. Now L is a Galois extension of K because, if $\sigma \in Gal(K'/K)$ is a generator then the Artin map

$$r_{\sigma(L)/K'} : C_{K'} \to Gal(\sigma(L)/K')$$

for $\sigma(L)$ is given by $\sigma r_{L/K'}\sigma^{-1}$ and the corresponding norm subgroup then equals $\sigma(U') = U'$. Let $A = Gal(L/K')$, $G = Gal(L/K)$, $H = Gal(K'/K)$, which is cyclic. It suffices to show that $A = C_L/U'$ is central in G. Thus we have to show that

$$r_{L/K'}(\sigma(x)) = r_{L/K'}(x)\ \forall x \in C_L; r_{L/K'}(\sigma(x)/x) = 1.$$

But $N_{K'/K}(\sigma(x)/x) = 1$, so $\sigma(x)/x \in U'$ for all $x \in C_L$. □

Proof of the existence theorem. Suppose $U \subset C_K$ as in the theorem, with $D = [C_K : U]$. Let p be a prime dividing D, and let $K' = K(\zeta_p)$. It suffices by the lemma to prove that $U' = N_{K'/K}^{-1}(U)$ is a norm subgroup. Now the index $D' = [C_{K'} : U']$ divides D, so by induction on D we may assume $D' = D$. Let $C_{K'} \supset V \supset U'$ with $[C_{K'} : V] = p$. By the last lemma, V is a norm subgroup, say corresponding to the cyclic extension L/K'. Let $U'' = N_{L/K'}^{-1}(U')$. If we can show

$$[C_L : U''] < [C_{K'} : U'] = D$$

then we are finished by induction. But

$$N_{L/K'} : C_L/U'' \to C_{K'}/U'$$

is injective by definition of U'', and its image is V/U'. □

5.6. **Applications.**

5.6.1. *The Hilbert class field.*

Theorem 5.32. *Let K be a number field. Let H be the maximal abelian extension of K unramified at all primes (including archimedean primes). Then the Artin map is an isomorphism*

$$r_{H/K} : Cl(K) \xrightarrow{\sim} Gal(H/K).$$

Proof. First, we know by the existence theorem that the subgroup $\mathbf{A}_{K,S_\infty}^\times \subset \mathbf{A}_K^\times$ corresponds to a field H' whose Galois group is isomorphic to $Cl(K)$. Moreover, H' is abelian and unramified at all primes, by local reciprocity. In particular, $H \supset H'$. If $H \neq H'$ then

$$N_{H/K}\mathbf{A}_H^\times \subsetneq \mathbf{A}_{K,S_\infty}^\times$$

but then necessarily H would have to be ramified somewhere. □

Theorem 5.33 (Hauptidealsatz)**.** *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then $\mathfrak{p}\mathcal{O}_H$ is a principal ideal. In other words, every ideal of K becomes principal in the Hilbert class field.*

The proof, due to Fürtwängler, is somewhat technical because the Hilbert class field of H is not generally abelian over K.

5.6.2. *Kronecker-Weber theorem.*

Theorem 5.34 (Kronecker-Weber)**.** *Any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

Proof. The proof consists in three parts. Let $U_m \subset C_\mathbb{Q}$ be the image of the subgroup of $\mathbb{R}_+^\times \times \prod_p \mathbb{Z}_p^\times$ consisting of $u \equiv 1 \pmod m$. Then

- (i) $U_m \subset N_{K_m/\mathbb{Q}} C_{K_m}$, where $K_m = \mathbb{Q}(\zeta_m)$.
- (ii) $U_m = N_{K_m/\mathbb{Q}} C_{K_m}$
- (iii) Every open subgroup of $C_\mathbb{Q}$ of finite index contains U_m for some m.

The first is a local (ramification) computation, the second point is an index calculation, and the third is clear, because $C_\mathbb{Q}/\mathbb{R}_+^\times \xrightarrow{\sim} \prod_p \mathbb{Z}_p^\times$.

For (i): Write N_m for $N_{K_m/\mathbb{Q}}$. First, it's clear that $\mathbb{R}_+^\times \subset N_m \mathbf{A}_{K_m}^\times$ because there is nothing smaller. Next, suppose $m = q^r \cdot m'$ with $q \nmid m'$ and suppose we know $U_{m'} \subset N_{m'}(\mathbf{A}_{K_{m'}}^\times)$; in particular, it is in the image of the units at m'. Now $K_m/K_{m'}$ is unramified at primes dividing m', so the norm map on units is surjective, and it follows that $\prod_{p|m'} U_{m,p} \subset N_m(\mathbf{A}_{K_m}^\times)$ where $U_{m',p}$ is the p-adic part of $U_{m'}$. Thus it suffices to show that $U_{m,q}$ is also in the image. But we can write $N_m = N_{q^r} \circ N_{K_m/K_{q^r}}$ and $N_{K_m/K_{q^r}}$ is surjective on units at q, so it suffices to take $m = q^r$. But then q is totally ramified and we can apply the Lubin-Tate theory again: if $u \in \mathbb{Z}_q^\times$ then

$$r_{\mathbb{Q}_q^\times/\mathbb{Q}_q}(u)(\zeta) = \zeta^{u^{-1}}$$

and this equals ζ if $u \equiv 1 \pmod{q^r}$. Thus $U_q \subset N_m(C_{K_m})$.

For (ii): It follows from (i) and the reciprocity law that

$$|Gal(K_m/\mathbb{Q})| = |C_\mathbb{Q}/N_{K_m/\mathbb{Q}} C_{K_m}| \leq |C_\mathbb{Q}/U_m| = |\prod_p \mathbb{Z}_p^\times/U_m| = |(\mathbb{Z}/m\mathbb{Z})^\times| = |Gal(K_m/\mathbb{Q})|.$$

Thus we have equality in the middle and this implies (ii).

□

6. Lubin-Tate theory

6.1. **Ramification.**