MATH 223B: ALGEBRAIC NUMBER THEORY

SALIM TAYOU

1. Tuesday, January 23

1.1. **Bookeeping.** The grading of the course will be based on occasional problem sets and a final presentation (one hour and fifteen minutes at the end of the semester) on some suitable topic.

1.2. **Motivating Questions and Course Outline.** A major problem in number theory is that of trying to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This Galois group controls all finite extensions of $\mathbb{Q}$, which, recall, are number fields. If $K/\mathbb{Q}$ is finite and Galois, then $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This begs the following question: can any finite group G be of the form $\mathrm{Gal}(K/\mathbb{Q})$? This is called the *inverse Galois problem.*

Class field theory aims to describe not the entirety of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but its *abelianization* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab}$. It attempts to do so using only information about the field $\mathbb{Q}$ itself. Now, how explicit is this description? In other words, given a number field K, how do we go about constructing abelian extensions of K? Classically, this is called *Kronecker's dream of youth.* For example, for $K = \mathbb{Q}$, every abelian extension is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ (this is Kronecker–Weber). For $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 1$, a similar result is also possible (relies on the theory of complex multiplication). The same question can be answered for K a local field, but for general K the answer is not clear.

The following is an outline for the class:

(1) Review of local class field theory and abstract class field theory;
(2) Global class field theory;
(3) Brauer groups and central simple algebras;
(4) Analytic methods: L-functions and zeta functions.

1.3. **Review of Local Class Field Theory.** Let K be a local field, complete with respect to a discrete valuation with finite residue field. We fix the following notation: let $v_K : K^* \longrightarrow \mathbb{Z}$ be the discrete valuation on K, where we set $v_K(0) = \infty$; let $\mathcal{O}_K = \{x \in K \mid v_K(x) \geq 0\}$ be the discrete valuation ring associated to v_K; let π_K be a uniformizer; let $\mathcal{P}_K = \{x \in K \mid v_K(x) > 0\}$ be its maximal ideal; let $k = \mathcal{O}_K/\mathcal{P}_K$ be the finite residue field; let $q = |k|$, and set $|a| = q^{-v_K(a}$; and let $U_K = \{x \in K^* \mid v_K(x) = 0\}$. The following proposition is proved in Neukirch Chapter 2.

Proposition 1.1. *A local field K is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.*

Let $G = \mathrm{Gal}(\overline{K}/K)$. Recall that this is a profinite group, and $G^{ab} = \mathrm{Gal}(\overline{K}/K)^{ab}$.

Theorem 1.2. *There exists a canonical isomorphism for every finite Galois extension L/K*

$$r_{L/K} : \mathrm{Gal}(L/K)^{ab} \longrightarrow K^*/N_{L/K}(L^*)$$

called the reciprocity homomorphism.

Corollary 1.3. *The association $L \mapsto \mathcal{N}_L = N_{L/K}(L^*)$ gives a one-to-one correspondence between finite abelian extensions L/K and open subgroups of K^* of finite index. This correspondence is inclusion reversing: $L_1 \subset L_2$ if and only if $\mathcal{N}_{L_2} \subset \mathcal{N}_{L_1}$. Moreover, we have $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ and $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$.*

Now, we outline the construction of $r_{L/K}$. Let $\tilde{K}/K$ be the maximal unramified extension. Because unramified extensions of K bijectively correspond to extensions of the residue field, the maximal unramified extension of K corresponds to $\overline{k}$, the algebraic closure of k. Thus, we have an isomorphism

$$\mathrm{Gal}(\tilde{K}/K) \to \mathrm{Gal}(\overline{k}/k) \simeq \widehat{\mathbb{Z}}$$

under which the Frobenius element, φ_K, is sent to 1. This determines a surjective map $d : G = \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\tilde{K}/K) \simeq \widehat{\mathbb{Z}}$. Now, let $A = \overline{K}^*$, $A^{\mathrm{Gal}(\overline{K}/L)} = L^*$. If L/K is a finite extension, then we use e_L and f_L to denote the *ramification index* and the *inertia degree.* It is not difficult to check that v_L/e_L prolongs v_K to L^*, where

$$\frac{1}{e_L} v_L(L^*) = \frac{1}{[L:K]} v_K(N_{L/K}(L^*)).$$

Hence,

$$v_K(N_{L/K}(L^*)) = f_L v_L(L^*) = f_L\mathbb{Z}.$$

Let $\sigma \in \mathrm{Gal}(L/K)$, and let $\tilde{\sigma}$ be an extension to $\mathrm{Gal}(\tilde{L}/K)$ such that $\tilde{\sigma}|_{\tilde{K}} = \varphi_K^n$ for some $n \geq 1$. Set $\Sigma = \tilde{L}^{\tilde{\sigma}}$, and let $\pi_\Sigma \in \Sigma$ a prime element. Then $r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \bmod N_{L/K}L^*$. As an exercise, see what happens in the unramified case.

1.4. **Abstract Class Field Theory.** Let G be a profinite group (perhaps $\mathrm{Gal}(\overline{K}/K)$ for some field K). Let A be a continuous G-module so that the map $G \times A \to A$ is continuous when A is endowed with the discrete topology. Let $G_L \subset G$ be some closed subgroup (in the concrete example given in the previous parenthetical, G_L would correspond to the Galois group of some intermediate extension $\overline{K}/L/K$). The open subgroups of G are also closed; we will be interested in the open subgroups of finite index. Let

$$A_L = \{x \in A \mid x^\sigma = x \text{ for all } \sigma \in G_L\}.$$

The condition that A is continuous is equivalent to writing

$$A = \bigcup_{[L:K]<\infty} A_L.$$

For every extension L/K, we have $G_L \subset G_K$ and $A_K \subset A_L$, and if the extension is finite, then we have a norm map $N_{L/K} : A_L \to A_K$ given by

$$N_{L/K}(x) = \prod_\sigma x^\sigma,$$

where the product runs over a set of representatives of G_K/G_L. If L/K is Galois (i.e., G_L is normal in G_K), then A_L is $G(L/K) = G_K/G_L$-module with $A^{G(L/K} = A_K$. Now, fix a choice of continuous surjective morphism $d : G \to \widehat{\mathbb{Z}}$. Let $I = \ker(d)$ be its *inertia groups.* Note that $I = G(\tilde{K}/K)$. For any L, we have maps

$$I_L \longrightarrow G_L \xrightarrow{d} \widehat{\mathbb{Z}},$$

and note that $I_L = I \cap G_L = G_{\tilde{L} = G_L \cap G_{\tilde{K}}} = G_{L\tilde{K}}$. Therefore, $\tilde{L} = L\tilde{K}$. Let $f_L = (\widehat{Z}d(G_L))$ and $e_L = (II_L)$. If f_L is finite, then

$$d_L = \frac{1}{f_L} d : G_L \longrightarrow \widehat{\mathbb{Z}},$$

giving an isomorphism $d_L : G(\tilde{L}/L) \longrightarrow \widehat{\mathbb{Z}}$.

Definition 1.4. The element $\varphi_L \in G(\tilde{L}/L)$ with $d_L(\varphi_L) = 1$ is called the *Frobenius* over L.

In fact, the map $\mathrm{Frob}(\tilde{L}/K) = \{\sigma \in \mathrm{Gal}(\tilde{L}/K) \mid d(\sigma) \geq 1\} \longrightarrow \mathrm{Gal}(L/K)$ is surjective and if $\tilde{\sigma} \in \mathrm{Frob}(\tilde{L}/K)$, $\Sigma = \tilde{L}^{\sigma}$, $[\Sigma : K] < \infty$, then $\tilde{\Sigma} = \tilde{L}$, $f_{\Sigma/K} = d(\tilde{\sigma})$, and $\tilde{\sigma} = \varphi_{\Sigma}$.

Definition 1.5. A *henselian valuation* of A_K with respect to $d : G \longrightarrow \widehat{\mathbb{Z}}$ is a homomorphism: $v : A_K \longrightarrow \widehat{\mathbb{Z}}$ such that

(1) $v(A_K) = Z \supset \mathbb{Z}$ and $Z/nZ = \mathbb{Z}/n\mathbb{Z}$;
(2) $v(N_{L/K}(A_L)) = f_L Z$ for all L/K finite extensions.

We define for L/K finite

$$v_L = \frac{1}{f_L}(v \circ N_{L/K}) : A_K \twoheadrightarrow Z$$

and $v_L = v_{L^\sigma} \circ \sigma$ for all $\sigma \in G$.

Definition 1.6. A *prime element* of A_L is an element π_L such that $v_L(\pi_L) = 1$. Let $U_L = \{u \in A_L \mid v_L(u) = 0\}$.

2. Thursday, January 25

2.1. **Abstract Class Field Theory, continued.**

The following is the main theorem of abstract class field theory:

Theorem 2.1 (Abstract Class Field Theory). *Let L/K be finite and Galois. Then there exists a canonical morphism*

$$r_{L/K} : G(L/K) \longrightarrow A_K/N_{L/K}A_L$$

which induces an isomorphism $G(L/K)^{ab} \simeq A_K/N_{L/K}A_L$. The resulting correspondence $L \mapsto \mathcal{N}_L = N_{L/K}A_L$ induces a bijection

$$\{L/K \text{ finite abelian}\} \longleftrightarrow \{\text{open subgroups of } A_K\}.$$

This correspondence is inclusion reversing, so $L_1 \subset L_2$ if and only if $\mathcal{N}_{L_1} \supset \mathcal{N}_{L_2}$. Moreover, we have $\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ and $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$.

2.2. **Global Class Field Theory.**

In what follows, we introduce some of the main objects needed for Global Class Field Theory. Let K be a number field with absolute Galois group $G = \mathrm{Gal}(\overline{K}/K)$. Recall that in abstract class field theory, we started with some G-module A. In the local setting, we had $A = K^*$; in the global setting, it is natural to ask what the G-module A will be. In the following, a *prime* $\mathfrak{p}$ is taken to be an absolute value on K. If $\mathfrak{p}$ is archimedean, then $\mathfrak{p}$ is said to be *infinite*; if $\mathfrak{p}$ is nonarchimedean, then $\mathfrak{p}$ is said to be *finite*. For any prime $\mathfrak{p}$ of K, we can complete K at $\mathfrak{p}$, and local class field theory yields an isomorphism $\mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})^{ab} \longrightarrow \widehat{K_{\mathfrak{p}}}^*$. We would like to package together the modules $\widehat{K_{\mathfrak{p}}}^*$ into some G-module.

Definition 2.2. Let K be a number field. The *adèle ring* is the restricted product of all the $K_\mathfrak{p}$'s, for $\mathfrak{p}$ finite or infinite:

$$\mathbb{A}_K = \prod_{\mathfrak{p}}{}' K_\mathfrak{p} = \left\{ (x_\mathfrak{p}) \in \prod_{\mathfrak{p}} K_\mathfrak{p} \;\middle|\; x_\mathfrak{p} \in O_{K_\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p} \right\}$$

(here, for $N_i \subset M_i$ the prime notation $\prod_i' M_i$ denotes the set of tuples $(m_i)_i$ with $m_i \in N_i$ for all but finitely many i). If $\mathfrak{p}$ is infinite, then we can take $O_{K_\mathfrak{p}} = K_\mathfrak{p}$, though this is a matter of convention.

Note that there is a natural diagonal map $K \hookrightarrow \mathbb{A}_K$ given by $x \mapsto (x)_\mathfrak{p}$. For every set of primes S containing $S_\infty = \{\sigma : K \to \mathbb{C} \text{ up to conjugacy}\}$ (note that S_∞ is the set of infinite primes of K), let

$$\mathbb{A}_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} O_{K_\mathfrak{p}} \subset \mathbb{A}_K.$$

Note that

$$\mathbb{A}_K = \varinjlim_{S \text{ finite}} \mathbb{A}_K^S.$$

Now, $\mathbb{A}_K^S$ inherits the product topology from $K_\mathfrak{p}$ and $O_{K_\mathfrak{p}}$, and if $S \subset S'$, then the natural map $\mathbb{A}_K^S \hookrightarrow \mathbb{A}_K^{S'}$ is continuous. Hence, $\mathbb{A}_K$ is endowed with the inductive limit topology, which makes it into a topological ring. Its basic open sets take the form

$$W = \prod_{\mathfrak{p}\in S} W_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} O_{K_\mathfrak{p}},$$

where S is some finite set of primes containing S_∞ and $W_\mathfrak{p} \subset K_\mathfrak{p}$ is open. Warning: the topology on $\mathbb{A}_K$ is not the one induced by the product $\prod' \subset \prod$. Note that $\prod_{\mathfrak{p}\in S} O_{K_\mathfrak{p}}$ is compact, so $\mathbb{A}_K$ is locally compact. We also have:

Lemma 2.3. *The space $\mathbb{A}_K$ is Hausdorff.*

Proof. Note that it is sufficient to separate an arbitrary nonzero $x \in \mathbb{A}_K$ from 0. There exists some $\mathfrak{p}$ such that $x_\mathfrak{p} \neq 0$, apply the fact that $K_\mathfrak{p}$ is Hausdorff (in fact, it is a metric space) to separate in the $\mathfrak{p}$-component. □

Definition 2.4. The *idèle group* is the restricted product

$$\prod_{\mathfrak{p}}{}' K_\mathfrak{p}^* = \{(\alpha_\mathfrak{p})_\mathfrak{p} \mid \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{ for all but finitely many } \mathfrak{p}\}$$

with respect to the unit groups $O_\mathfrak{p}^*$, where $U_\mathfrak{p} = O_{K_\mathfrak{p}}^*$ if $\mathfrak{p}$ is finite, $U_\mathfrak{p} = \mathbb{R}_{>0}$ for $\mathfrak{p}|\infty$ and $K_\mathfrak{p} = \mathbb{R}$, and $U_\mathfrak{p} = \mathbb{C}^*$ for $\mathfrak{p}|\infty$ and $K_\mathfrak{p} = \mathbb{C}$.

The notion of *idèle* comes from Chevalley is a modification of the notion of ideal. The term adèle is a portmanteau of the phrase "additive idèle." As in the above, for an S-finite set of primes (with $S \supset S_\infty$), we define the S-idèle to be

$$I_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \subset I_K.$$

Similarly, we have

$$I_K = \varinjlim_{S \text{ finite}} I_K^S,$$

and we also have a diagonal embedding $i : K^* \hookrightarrow I_K$ given by $x \mapsto (x)_{\mathfrak{p}}$. Elements in the image of $i : K^* \hookrightarrow I_K$ are called *principal idèles*, and we call $i(K^*)$ the *group of principal idèles*. The intersection $K^S = K^* \cap I_K^S$ is the group of *S-units*. Note that $x \in K^S$ if and only if $x \in U_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$ (x is a unit for $\mathfrak{p}$ finite and is greater than 0 if $K_{\mathfrak{p}} = \mathbb{R}$). If $S = S_\infty$, then $K^S = \mathcal{O}_K^*$ (note that $v_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p}$ in this case).

Recall from the proof of the Dirichlet Unit Theorem that

$$\mathcal{O}_K^* \longrightarrow \prod_{\mathfrak{p} \in S_\infty} \mathbb{R} = \mathbb{R}^{r_1 + r_2},$$

where r_1 is the number of real embeddings and r_2 the number of complex embeddings up to conjugation. Moreover, we also have that

$$\lambda : \mathcal{O}_K^* \longrightarrow \prod_{\mathfrak{p} \in S_\infty} \mathbb{R},$$

where λ takes $x \mapsto (\log |x|_{\mathfrak{p}})$. Let

$$H = \left\{ (x_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in S_\infty} \mathbb{R} \;\middle|\; \sum_{\mathfrak{p}} x_{\mathfrak{p}} = 0 \right\}.$$

Note that $\lambda(\mathcal{O}_K^*)$ is a lattice in H and that $\ker(\lambda) = \mu(K)$, the group of roots of unity in K. In general, we have the following theorem.

Theorem 2.5. *For S finite with $S \supset S_\infty$, there is a map $\lambda : K^S \longrightarrow \prod_{\mathfrak{p} \in S} \mathbb{R}$ taking $x \mapsto (\log |x|_{\mathfrak{p}})$. The map has kernel $\mu(K)$, and $\lambda(K^S)$ is a lattice in $H = \{(x_{\mathfrak{p}}) \mid \sum_{\mathfrak{p}} x_{\mathfrak{p}} = 0\}$. Therefore, $\lambda(K^S)$ has rank $|S| - 1$ (recall that $|S_\infty| = r_1 + r + 2$).*

Proof. Let $S_f = S \setminus S_\infty$. There are exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^* \arrow[r] \arrow[d, "\lambda'"'] & K^S \arrow[r] \arrow[d, "\lambda"'] & J(S_f) \arrow[d, hook, "\lambda''"'] \\
0 \arrow[r] & \prod_{\mathfrak{p} \in S_\infty} \mathbb{R} \arrow[r] & \prod_{\mathfrak{p} \in S} \mathbb{R} \arrow[r, "\varphi"] & \prod_{\mathfrak{p} \in S_f} \mathbb{R},
\end{tikzcd}$$

where $J(S_f)$ is the group ideals generated by $\mathfrak{p} \in S_f$. The rightmost vertical map λ'' takes $\prod_{\mathfrak{p} \in S_f} \mathfrak{p}^{v_{\mathfrak{p}}} \mapsto (-v_{\mathfrak{p}} \log |\mathfrak{p}|)$. This in turn gives an exact sequence

$$0 \longrightarrow \operatorname{im}(\lambda') \longrightarrow \operatorname{im}(\lambda) \longrightarrow \varphi(\operatorname{im}(\lambda)) \subset \operatorname{im}(\lambda'').$$

Note that $\operatorname{im}(\lambda')$ is a discrete subgroup of $\prod_{\mathfrak{p} \in S_\infty} \mathbb{R}$ of rank $|S_\infty| - 1$ and that $\varphi(\operatorname{im}(\lambda))_{\mathfrak{p}}$ is a discrete subgroup of rank at most $|S_f|$. if h is the class number, then $h(\lambda''(J(S_f))) \subset \varphi(\operatorname{im}(\lambda)) \subset \lambda''(J(S_f))$, so $\varphi(\operatorname{im}(\lambda))$ has rank $|S_f|$. Therefore, $\operatorname{im}(\lambda)$ is discrete of rank $|S| - 1$, as desired. □

Definition 2.6. The quotient $C_K = I_K / K^*$ is called the *idèle class group* of K.

3. Tuesday January 30

Recall for K a number field we can define the ring of adèles $\mathbb{A}_K = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}$ with respect to $\mathcal{O}_{\mathfrak{p}}$, which contains a copy of K via the diagonal embedding. The group of units in $\mathbb{A}_K$ is the idèle group $I_K = \prod'_{\mathfrak{p}} K_{\mathfrak{p}}^*$, which likewise contains a copy of K^* via the diagonal embedding. Recall that I_K / K^* is called the *idèle class group*. This definition and terminology are reminiscent of another number theoretic object: the ideal class group Cl_K.

Recall that Cl_K is defined in the following way. Suppose O_K is a Dedekind domain. Let $J_K = J(O_K)$ be the free abelian group generated by the prime ideals of O_K. If P_K denotes the principal ideals aO_K for $a \in K^*$, then $\mathrm{Cl}_K = J_K/P_K$. The following theorem is well-known:

Theorem 3.1. *The ideal class group* Cl_K *is finite.*

However, despite their similarity, this is not always the case for the idèle class group. Let S_∞ denote the set of infinite primes, i.e., the primes $\mathfrak{p}$ such that $\mathfrak{p}|\infty$. Then note that

$$I_K^{S_\infty} = \prod_{p|\infty} K_\mathfrak{p}^* \times \prod_{p\not|\infty} U_\mathfrak{p},$$

and

$$I_K/I_K^{S_\infty} = \prod_{\mathfrak{p}\not|\infty} K_\mathfrak{p}/U_\mathfrak{p} \simeq J_K,$$

where we note that $K_\mathfrak{p}^*/U_\mathfrak{p} \simeq \mathbb{Z}$. More succinctly, we have a short exact sequence

$$1 \longrightarrow I_K^{S_\infty} \longrightarrow J_K \longrightarrow 1,$$

where the third map sends

$$\alpha \mapsto \prod_{\mathfrak{p}\not|\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}.$$

Note that K^* is sent to P_K under the third map. Hence,

$$1 \longrightarrow I_K^{S_\infty}/K^* \longrightarrow C_K \longrightarrow \mathrm{Cl}_K \longrightarrow 1$$

is exact.

Proposition 3.2. *We have* $I_K = I_K^S K^*$ *if* S *is large enough.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the classes of $\mathrm{Cl}_K = J_K/P_K$. If S contains $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \cup S_\infty$, then $I_K = I_K^S K^*$. For $\alpha \in I_K$, consider the corresponding principal ideal $(\alpha) \in J_K$, and write

$$(\alpha) = \prod_i \mathfrak{p}_i^{n_i}(\alpha')$$

for some $\alpha' \in K^*$. Then $\alpha(\alpha')^{-1} \in I_K^S$, implying $\alpha \in I_K^S K^*$. □

Proposition 3.3. *The diagonal embedding* $K^* \hookrightarrow I_K$ *realizes* K^* *as a discrete subset of* I_K.

Proof. It suffices to find an open neighborhood W of 1 that does not contain any other element in K^*. Let

$$W = \{a \mid |a_\mathfrak{p}|_\mathfrak{p} = 1 \text{ if } \mathfrak{p} \not| \infty \text{ and } |a_\mathfrak{p} - 1| < 1 \text{ if } \mathfrak{p}|\infty\} = \prod_{\mathfrak{p}|\infty} D_\mathfrak{p} \times \prod_{\mathfrak{p}\not|\infty} U_\mathfrak{p},$$

where $D_\mathfrak{p}$ is some disk.

Suppose $x \neq 1$ is such that $x \in W \cap K^*$. Then

$$\prod_\mathfrak{p} |x_\mathfrak{p} - 1|_\mathfrak{p} = 1$$

since $x - 1 \in K^*$, but

$$\prod_{\mathfrak{p}|\infty} |x_\mathfrak{p} - 1|_\mathfrak{p} = \prod_\mathfrak{p} |x_\mathfrak{p} - 1|_\mathfrak{p} \times \prod_{\mathfrak{p}\not|\infty} |x_\mathfrak{p} - 1|_\mathfrak{p} < 1,$$

where the inequality follows because, in the first product, the terms are strictly less than 1. □

The above implies the existence of a topology on $C_K = I_K/K^*$. This also allows us to define an *absolute norm* on I_K given by $r : I_K \longrightarrow \mathbb{R}_+$ taking $\alpha \mapsto \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}$. In fact, this gives a continuous homomorphism $r : C_K \longrightarrow \mathbb{R}_+$.

Theorem 3.4. *The fiber of 1 under r, $r^{-1}(1)$ (which we denote using C_K^0) is compact.*

Proof. Define I_K^0 to be $r^{-1}(1)$ for the map $r : I_K \longrightarrow \mathbb{R}_+$. By Proposition 3.2, we have that $I_K = I_K^S K^*$ for S large enough. Recall the function

$$\lambda : I_K^S \longrightarrow \prod_{\mathfrak{p}|S} \mathbb{R}$$

given by

$$\alpha \mapsto \prod_{\mathfrak{p}|S} (-\log |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}).$$

Moreover, recall that the image of $K^S = K^* \cap I_K^S$ under λ is a complete lattice with rank $|S| - 1$ inside the hyperplane given by $\sum |\alpha_{\mathfrak{p}}| = 0$. Let $I_K^{S,0} = I_K^S \cap I_K^0$. The kernel of λ is compact. Pick a fundamental domain W^0 in the image of λ. We note that $\lambda^{-1}(W^0)$ is compact and that $\lambda^{-1}(W^0)$ surjects onto $I_K^{S,0}/K^*$. □

Recall that in $K_{\mathfrak{p}}$ there is a nested basis of open neighborhoods

$$U_{\mathfrak{p}} \supset U_{\mathfrak{p}}^{(1)} \supset U_{\mathfrak{p}}^{(2)},$$

where if $\mathfrak{p} \nmid \infty$ we have $U_{\mathfrak{p}}^{(n)} = 1 + \mathfrak{p}^n$ if $n > 0$. If $\mathfrak{p}|\infty$, then $U_{\mathfrak{p}}^{(n)} = \mathbb{R}_+$ for $\mathfrak{p}$ real and $U_{\mathfrak{p}}^{(n)} = \mathbb{C}^*$ for $\mathfrak{p}$ complex.

Definition 3.5. Set

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

for $n_{\mathfrak{p}} \geq 0$ and $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. The group

$$I_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$$

is called the *congruence subgroup* mod $\mathfrak{m}$ and the group $C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} K^*/K^*$ is called the *ray class group* mod $\mathfrak{m}$.

Theorem 3.6. *The closed subgroups of C_K with finite index are precisely those subgroups containing some $C_K^{\mathfrak{m}}$.*

Proof. Note that $C_K^{\mathfrak{m}}$ is open because $I_K^{\mathfrak{m}}$ is open in I_K. We have

$$[C_K : C_K^{\mathfrak{m}}] = [C_K : I_K^{S_\infty} K^*/K^*][I_K^{S_\infty} K^*/K^* : C_K^{\mathfrak{m}}],$$

where we note that $[C_K : I_K^{S_\infty} K^*/K^*] = |\mathrm{Cl}_K| < \infty$, and

$$[I_K^{S_\infty} K^*/K^* : C_K\mathfrak{m}] \leq [I_K^{S_\infty} : I_K^{\mathfrak{m}}] = \prod_{\mathfrak{p}\nmid\infty} [U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}] \prod_{\mathfrak{p}|\infty} [K_{\mathfrak{p}}^* : U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}] < \infty.$$

Hence, $C_K^{\mathfrak{m}}$ is open and has finite index in C_K, so $C_K^{\mathfrak{m}}$ is closed, since we may write

$$C_K = \bigsqcup g C_K^{\mathfrak{m}}$$

and

$$C_K^{\mathfrak{m}} = C_K \setminus \left(\bigsqcup_{g \neq 1} C_K^{\mathfrak{m}} \right).$$

Any $W \supset C_K^{\mathfrak{m}}$ must then be closed of finite index, since $[C_K : C_K^{\mathfrak{m}}] \geq [W : C_K^{\mathfrak{m}}] < \infty$.

Conversely, if W is closed and of finite index, then W must be open. Hence, the preimage of W under the map $I_K \longrightarrow C_K$ (i.e., WK^*) contains a subset of the form

$$\prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in S} W_{\mathfrak{p}},$$

where S is a finite set of primes of K containing S_∞ and $W_{\mathfrak{p}}$ is an open neighborhood of 1 in $K_{\mathfrak{p}}^*$. If $\mathfrak{p} \in S$ is finite, then we may choose $W_{\mathfrak{p}} = U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$. If $\mathfrak{p} \in S$ is real, then we choose $W_{\mathfrak{p}} \subset \mathbb{R}_+$. Thus, we see that the subgroup WK^* generated by the above open is of the form $I_K^{\mathfrak{m}}$, so W contains $C_K^{\mathfrak{m}}$. □

4. Thursday February 2

4.1. **Ray Class Groups.** Recall that for K a number field, the ideèle group is the restricted product

$$I_K = \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}^*$$

with respect to $\mathcal{O}_{\mathfrak{p}}^* \subset K_{\mathfrak{p}}^*$. The group $C_K = I_K/K$ is called the idèle class group. For $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, the congruence subgroup mod $\mathfrak{m}$ is $I_K^{\mathfrak{m}}$, and we can define the ray class group mod $\mathfrak{m}$ to be $C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}/K^*$.

We would like an ideal-theoretic description of the ray class group $C_K/C_K^{\mathfrak{m}}$. Let $J_K^{\mathfrak{m}}$ be the group of fractional ideals that are coprime to $\mathfrak{m}$. For $a \in K$ such that $a = b/c$ for $b, c \in \mathcal{O}_K$, the condition $a \equiv 1 \bmod \mathfrak{m}$ is equivalent to the condition that $(b, \mathfrak{m}) = (c, \mathfrak{m}) = 1$ and $b - c$ is divisible by $\mathfrak{m}$ Let

$$P_K^{\mathfrak{m}} = \{(a) \mid a \equiv 1 \mod \mathfrak{m} \text{ and } a \text{ is totally positive}\}$$

(recall that a totally positive means that for every $\sigma : K \hookrightarrow \mathbb{R}$, we have $\sigma(a) > 0$). Set $\mathrm{Cl}_K^{\mathfrak{m}} = J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$.

Proposition 4.1. *The map $I_K \longrightarrow J_K$ induces an isomorphism $C_K/C_K^{\mathfrak{m}} \simeq \mathrm{Cl}_K^{\mathfrak{m}}$.*

Proof. Let

$$I_K^{(\mathfrak{m})} = \{\alpha \in_K \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \text{ for all } \mathfrak{p}|\mathfrak{m}\}.$$

We claim that $I_K = I_K^{(\mathfrak{m})} K^*$. It suffices to show that for each $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$ in I_K, there exists some $d \in K^*$ such that $d\alpha = (d\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in I_K^{(\mathfrak{m})}$. In other words, $d\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ for all $\mathfrak{p}|\mathfrak{m}$. Such a d exists by the Approximation Theorem.

Hence, we have a map $I_K^{(\mathfrak{m})} \longrightarrow J_K^{\mathfrak{m}}$ taking

$$(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \longmapsto I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}.$$

Composing with the quotient $J_K^{\mathfrak{m}} \longrightarrow J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$, note that the resulting map $I_K^{(\mathfrak{m})} \longrightarrow J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ has kernel $K^* \cap I_K^{(\mathfrak{m})}$. Since $I_K = I_K^{\mathfrak{m}} K^*$, we have $C_K = I_K/K^* = I_K^{(\mathfrak{m})} K^*/K^*$. Therefore,

$$C_K/C_K^{\mathfrak{m}} = (I_K/K^*)/(I_K^{(\mathfrak{m})} K^*/K^*) = (I_K^{(\mathfrak{m})} K^*/K^*)/(I_K^{(\mathfrak{m})} K^*/K^*),$$

which proves the result. □

Example 4.2. Let $m \geq 1$ and $\mathfrak{m} = (m)$. Then

$$C_{\mathbb{Q}}/C_{\mathbb{Q}}^{\mathfrak{m}} \simeq \mathrm{Cl}_{\mathbb{Q}}^{\mathfrak{m}} \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

because the map $J_{\mathbb{Q}}^{\mathfrak{m}} \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ taking $(a) \mapsto \{\overline{a} \text{ where } a > 0\}$ is surjective with kernel $\{(a) \mid a \equiv 1 \mod \mathfrak{m}, a > 0\}$.

Recall that $(\mathbb{Z}/m\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \simeq C_{\mathbb{Q}}/C_{\mathbb{Q}}^{\mathfrak{m}}$.

If K is a number field and L/K is a finite abelian extension such that $\mathrm{Gal}(L/K) \simeq C_K/C_K^{\mathfrak{m}}$, then we say that L is a *ray class field.*

4.2. **Idèles in Field Extensions.** We would like to understand the behavior of idèles in field extensions. Let L/K be a finite extension. For $\mathfrak{p} \subset \mathcal{O}_K$, suppose $\mathfrak{p}\mathcal{O}_L = Q_1^{n_1} \cdots \mathbb{Q}_r^{n_r}$. Recall that for any Q lying over $\mathfrak{p}$, we get a field extension $\iota_Q : K_{\mathfrak{p}} \longrightarrow L_Q$. Moreover, recall that the algebra $L \otimes_K K_{\mathfrak{p}}$ splits as

$$L \otimes_K K_{\mathfrak{p}} = \prod_{Q/\mathfrak{p}} L_Q. \tag{1}$$

Note that $K_{\mathfrak{p}}$ embeds into $L \otimes_K K_{\mathfrak{p}}$ as $x \mapsto 1 \otimes x \simeq (\iota_Q(x))_Q$. We obtain an injective morphisms $I_K \longrightarrow I_L$ and $\mathbb{A}_K \longrightarrow \mathbb{A}_L$.

Let $\sigma : L_1 \longrightarrow L_2$ be an morphism that commutes with the inclusion of K into each L_i. Then there exists a corresponding morphism of idèles:

$$\begin{tikzcd}
I_{L_1} \arrow[rr, "\sigma"] & & I_{L_2} \\
& I_K \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

If L/K is Galois, then for any $\sigma \in \mathrm{Gal}(L/K)$, we get an such an automorphism $\sigma : I_L \longrightarrow I_L$ commuting with the inclusion of I_K in I_L. Hence, I_L is a $\mathrm{Gal}(L/K)$-module.

Proposition 4.3. *With notation as above, $I_L^{\mathrm{Gal}(L/K)} = I_K$.*

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ and $\mathfrak{p} \subset \mathcal{O}_K$ a prime. Recall that $\mathrm{Gal}(L/K)$ permutes the primes of L lying over $\mathfrak{p}$, i.e., for $Q/\mathfrak{p}$, we have $\sigma(Q)$ lying over $\mathfrak{p}$, and σ is a map $L_Q \longrightarrow L_{\sigma(Q)}$.

One inclusion is trivial: $I_K = (x_{\mathfrak{p}})_{\mathfrak{p}} \subset I_L^{\mathrm{Gal}(L/K)}$ since $\sigma(x_{\mathfrak{p}}) = x_{\mathfrak{p}}$ for all $\mathfrak{p}$.

For the other inclusion, suppose $(x_Q)_Q \in I_L$ is fixed by $\mathrm{Gal}(L/K)$. Note that there is a map $K_{\mathfrak{p}}^* \longrightarrow \prod_{Q/\mathfrak{p}} L_Q^*$ taking $x_{\mathfrak{p}} \mapsto (x_Q)_{Q/\mathfrak{p}}$. Recall the decomposition group of $Q/\mathfrak{p}$, given by $D_Q = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(Q) = Q\} \simeq \mathrm{Gal}(L_Q/K_{\mathfrak{p}}) \subset \mathrm{Gal}(L/K)$. If an element $(x_Q)_Q$ is fixed by $\mathrm{Gal}(L/K)$, then it is fixed by D_Q. Hence, $x_Q \in K_{\mathfrak{p}}^*$ for all Q. Now, recall that the Galois group $\mathrm{Gal}(L/K)$ acts transitively on $\{Q \mid Q|\mathfrak{p}\}$. It follows that $x_Q = x_{Q'}$ for all Q, Q' lying over $\mathfrak{p}$. Thus, $(x_Q)_Q \in I_K$, as desired. □

4.3. **The Norm Map.** For each $Q/\mathfrak{p}$, recall from local class field theory the norm map

$$N_{L_Q/K_{\mathfrak{p}}} : L_Q^* \longrightarrow K_{\mathfrak{p}}^*$$

taking $x \in L_Q$ to the determinant of the multiplication-by-x map $m_x : L_Q \longrightarrow L_Q$. This induces a map $N_{L/K} : I_L \longrightarrow I_K$ taking

$$((x_Q)_{Q/\mathfrak{p}})_{\mathfrak{p}} \mapsto \left(\prod_{Q/\mathfrak{p}} N_{L_Q/K_{\mathfrak{p}}}(x_Q) \right)_{\mathfrak{p}} .$$

Another way to think about this map is as follows. Let $x \in I_L$. Consider the multiplication-by-x map $\mathbb{A}_L \longrightarrow \mathbb{A}_L$ which takes $y \mapsto xy$. As a ring, $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$. This fact is simply a global version of (1). Note that $\mathbb{A}_L$ is a finite $\mathbb{A}_K$-module. We may alternatively define $N_{L/K}(x) = \det(m_x)$.

Exercise 4.4. Check that the two definitions of the norm map $N_{L/K} : L \longrightarrow K$ agree.

5. Tuesday February 6

We take a moment to disambiguate some potentially confusing notation. Recall that

$$I_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U^{(}_{\mathfrak{p}} n_{\mathfrak{p}})$$

for $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$, and

$$I_K^{(\mathfrak{m})} = \{\alpha \in I_K \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \text{ for all } \mathfrak{p} | \mathfrak{m}, \infty\}.$$

Note that $I_K^{\mathfrak{m}} \subset I_K^{(\mathfrak{m})}$.

Proposition 5.1. *Let L/K be a finite extension with $\alpha = (\alpha_Q)_Q \in I_L$. Then $N_{L/K}(\alpha) \in I_K$ and*

$$N_{L/K}(\alpha) = \left(\prod_{Q/\mathfrak{p}} N_{LQ/K\mathfrak{p}}(\alpha_Q) \right)_{\mathfrak{p}} .$$

Also, for a tower of number fields $M/L/K$, we get a map

$$I_K \longrightarrow I_L \longrightarrow I_M$$

and $N_{M/K} = N_{L/K} \circ N_{M/L}$. If the extensions are Galois with $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, then we have that

$$N_{L/K}(\alpha) = \prod_{\sigma \in G/H} \sigma(\alpha).$$

Let L/K be a finite extension of number fields. Then we have the following commutative diagram:

$$\begin{tikzcd}
I_K \arrow[r, hook] \arrow[d] \arrow[dr, dashed, "\psi"] & I_L \arrow[d] \\
C_K = I_K/K^* \arrow[r] & C_L = I_L/L^*
\end{tikzcd}$$

Proposition 5.2. *The map $C_K \longrightarrow C_L$ is injective.*

Proof. Note that the kernel of ψ is simply $L^* \cap I_K$. If L/K is Galois, then $I_K = I_L^G$, and $L^* \cap I_K = K^*$. If the extension is Galois, then we can simply pass to a Galois closure M/L. □

Proposition 5.3. *If L/K is Galois, then C_L is a $G = \mathrm{Gal}(L/K)$-module and $C_L^G = C_K$.*

Proof. That C_L is a G-module follows from the fact that I_L is a G-module and L^* is a G-submodule.

Note that $C_K \subset C_L^G$. For the reverse inclusion, let $\bar{x} \in C_L^G$ with $x \in I_L$ such that $\sigma(x) = \bar{x}$. Then $\sigma(x) = x\alpha^\sigma$ for $\alpha^\sigma \in L^*$. Let $\sigma_1, \sigma_2 \in G$. Then

$$x\alpha^{\sigma_1\sigma_2} = \sigma_1\sigma_2(x) = \sigma_1(x)\sigma_1(\alpha^{\sigma_2}) = x\alpha^{\sigma_1}\sigma_1(\alpha^{\sigma_2}),$$

so $\alpha^{\sigma_1\sigma_2} = \alpha^{\sigma_1}\sigma_1(\alpha^{\sigma_2})$. Hence $\alpha^\sigma \in H^1(G, L^*) = 0$ by Hilbert 90. Therefore, there exists $u \in L^*$ such that $\alpha^\sigma = \sigma(u)/u$, implying $\sigma(x/u) = x/i$ for all $\sigma \in G$. It follows that $x/u \in C_K$ and $\overline{x/u} = \bar{x}$. Thus, $C_L^G \subset C_K$, as desired.

Another way to see this is to recall that following exact sequence:

$$\begin{tikzcd} 1 \arrow[r] & L^* \arrow[r] & I_L \arrow[r] & C_L \arrow[r] & 1. \end{tikzcd}$$

Taking G-invariants, we get an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & L^{*G} \arrow[r] & I_L^G \arrow[r] & C_L^G \arrow[r] & H^1(G, L^*) \end{tikzcd}$$

(group cohomology G in abelian groups is R^*F, where F is the functor taking G-invariants). Since $H^1(G, L^*) = 0$ by Hilbert 90, and since $K^* = L^{*G}$ and $I_L^G = I_K$, the result falls out. □

5.1. **Herbrand Quotients.** Let A be a G-module.

Definition 5.4. Let

$$h(G, A) = \frac{\#H^0(G, A)}{\#H^{-1}(G, A)},$$

where $H^0(G, A) = A^G/N_GA$ and $H^{-1}(G, A) = N_GA/I_GA$ (recall that $N_GA = \{a \in A \mid N_Ga = 1\}$ and $I_GA = \{a^{\sigma-1} \mid a \in A\}$).

If

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 1 \end{tikzcd}$$

is an exact sequence of G-mdoules, then $h(G, B) = h(G, A)h(G, C)$. Moreover, if $H \subset G$ is a subgroup with B an H-module, then

$$H^i(G, \mathrm{Ind}_G^H(B)) = H^i(H, B)$$

for $i \in \{0, -1\}$ as long as G is finite. Recall that $\mathrm{Ind}_G^H(B) = \{f : C \to B \mid f(xh) = f(x)^h, h \in H\}$.

Theorem 5.5 (Class Field Axiom)**.** *For L/K a finite Galois extension, then*

$$\#H^i(G(L/K), I_L) = \begin{cases} [L : K] & \textit{if } i = 0; \\ 1 & \textit{otherwise.} \end{cases}$$

Let L/K be some finite Galois extension, and let $\mathfrak{p} \subset O_K$. Recall that $L_\mathfrak{p} = L \otimes_K K_\mathfrak{p} = \prod_{Q/\mathfrak{p}} L_Q$ and that $I_L = \prod'_{\mathfrak{p} \subset O_K} L_\mathfrak{p}^*$. For each $\mathfrak{p}$, fix a $Q/\mathfrak{p}$. The corresponding decomposition group is given by $G_Q = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(Q) = Q\}$. Note that

$$L_\mathfrak{p} = \prod_{\sigma \in G/G_Q} L_{Q^\sigma} = \prod_{\sigma \in G/G_Q} \sigma(L_Q)$$

and that

$$U_{L,\mathfrak{p}} = \prod_{\sigma \in G/G_Q} U_{Q^\sigma} = \prod_{\sigma \in G/G_Q} \sigma(U_Q).$$

Proposition 5.6. *We have that*

$$L_{\mathfrak{p}}^* = \operatorname{Ind}_G^{G_Q}(L_Q^*)$$

and

$$U_{L,\mathfrak{p}} = \operatorname{Ind}_G^{G_Q}(U_Q).$$

Proof. Let G be a finite group with $H \subset G$ a subgroup and A an H-module. Then

$$\operatorname{Ind}_G^H(A) = \prod_{\sigma \in G/H} A^\sigma;$$

from this the result follows. □

Let S be a finite set of primes containing S_∞, and let $\overline{S}$ be the corresponding set of primes of L above S. I.e., $\overline{S} = \{Q \mid Q/\mathfrak{p} \text{ for some } \mathfrak{p} \in S\}$. Let $I_L^S = I^{\overline{S}}$.

Proposition 5.7. *Assume L/K is cyclic and that S contains all primes ramified in L. Then*

$$H^i(G, I_L^S) = \bigoplus_{\mathfrak{p} \in S} H^i(G_Q, L_Q^*).$$

Moreover,

$$H^i(G, I_L) \simeq \bigoplus_{\mathfrak{p}} H^i(G_Q, L_Q^*).$$

Proof. Recall that

$$I_L^S = \left(\bigoplus_{\mathfrak{p} \in S} L_{\mathfrak{p}}^* \right) \oplus V$$

as G-modules, where

$$V = \prod_{\mathfrak{p} \notin S} U_{L,\mathfrak{p}}.$$

Thus,

$$H^i(G, I_L^S) = \bigoplus_{\mathfrak{p} \in S} H^i(G, L_{\mathfrak{p}}^*) \oplus H^i(G, V).$$

We have $H^i(G, L_{\mathfrak{p}}^*) \simeq H^i(G_Q, L_Q^*)$ and, as an exercise, one can check that

$$V \hookrightarrow \prod_{\mathfrak{p} \notin S} H^i(G, U_{L,\mathfrak{p}})$$

(one cannot just distribute the cohomology, since the product is infinite). By induction (in the group theoretic sense), we have that

$$H^i(G, U_{L,\mathfrak{p}}) \simeq H^i(G_Q, U_Q).$$

For $\mathfrak{p} \notin S$, we have that $L_Q/K_{\mathfrak{p}}$ is unramified. So by local class field theory, $H^i(G_Q, U_Q) = \{1\}$.

For the second part, recall that

$$I_L = \varprojlim_S I_L^S,$$

so

$$H^i(G, I_L) \simeq \varprojlim H^i(G, I_L^S) = \bigoplus_{\mathfrak{p}} H^i(G_Q, L_Q^*),$$

as desired. □

By Hilbert 90, we have that $H^{-1}(G_Q, L_Q^*) = 0$. Hence, $H^{-1}(G, I_L) = 0$. For $i = 0$, we have that $I_K/N_{L/K}(I_L) = \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{L_Q/K_{\mathfrak{p}}}(L_Q^*)$. Thus, $x \in I_K$ is a norm if and only if $x_{\mathfrak{p}}$ is a norm for all $\mathfrak{p}$.

Proposition 5.8. *Let L/K be a cyclic extension with S a subset of primes of K containing both the infinite and ramified primes. Then $h(G, I_L^S) = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$, where $n_{\mathfrak{p}} = [L_Q : K_{\mathfrak{p}}]$.*

Proof. Recall that

$$\#H^{-1}(G, I_L^S) = \prod_{\mathfrak{p}\in S} \#H^{-1}(G_Q, L_Q^*) = 1,$$

since $\#H^{-1}(G_Q, L_Q^*) = 1$. Moreover, $H^0(G, I_L^S) = \prod_{\mathfrak{p}\in S} H^0(G_Q, L_Q)$. Now, local class field theory tells us that $\#H^0(G_Q, L_Q^*) = (K_{\mathfrak{p}}^* N_{L_Q/K_{\mathfrak{p}}}(L_Q^*)) = n_{\mathfrak{p}}$, so $h(G, I_L^S) = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$. □

We would like to compute $h(G, L^S)$. Recall that $L^S = L \cap I_L^S$.

Theorem 5.9. *We have that*

$$h(G, L^S) = \frac{1}{n} \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}.$$

The proof is left as required reading.

Corollary 5.10. *For L/K a cyclic extension of degree n, we have $h(G, C_L) = n$.*

Proof. Let S be a set of primes containing the infinite and ramified primes such that $I_L = I_L^S L^*$. Then the sequence

$$1 \longrightarrow L^S \longrightarrow I_L^S \longrightarrow I_L^S L^*/L^* \longrightarrow 1$$

is exact (recall that $I_L^S L^*/L^* = C_L$). Then $h(G, C_L) = h(G, I_L^S)/h(G, L^S) = n$. □

6. Thursday February 8

6.1. **Class Field Axiom.** Recall the following result from last time: for a cyclic extension L/K, the Herbrand quotient $h(G, C_L) = [L : K]$, where $G = \mathrm{Gal}(L/K)$. To prove the class field axiom, note that we must show that $\#H^0(G, C_L) = [L : K]$ and $H^{-1}(G, C_L) = 1$. We will prove that $H^0(G, C_L) = [L : K]$. We will also use Kummer extensions.

Let K be a number field with $\mu_n \subset K$, where μ_n denotes the group of nth roots of unity. Assume $n = p^k$, and let L/K be Galois with $\mathrm{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z})^r$. Let S be the finite set of primes

$$S = \{\mathfrak{p} \mid \mathfrak{p}|n, \infty \text{ and } \mathfrak{p} \text{ is ramified in } L \text{ and } I_K = I_K^S K^*\},$$

and let s denote $|S|$. Also let $K^S = I_K^S \cap K^*$ denote the S-units in K.

Proposition 6.1. *With notation as above, $s \geq r$. Moreover, there exists a set T of $s - r$ primes such that $L = K(\sqrt[n]{\Delta})$, and Δ is the kernel of the map $K^S \longrightarrow \prod_{\mathfrak{p}\in T} K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^n$.*

Theorem 6.2. *Let T be as before. Let*

$$I_K(S, T) = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\in T} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S\cup T} U_{\mathfrak{p}},$$

and let $C_K(S, T) = I_K(S, T)K^*/K^*$. Then $C_K(S, T) \subset N_{L/K}(C_L)$ and $[C_K : C_K(S, T)] = [L : K]$. Finally, if L/K is cyclic, then $N_{L/K}(C_L) = C_K(S, T)$.

Assuming the above results, we have the following theorem.

Theorem 6.3 (Class Field Axiom)**.** *For any cyclic extension L/K of number fields, we have that*

$$\#H^i(\mathrm{Gal}(L/K), C_L) = \begin{cases} [L:K] & \textit{if } i = 0; \\ 1 & \textit{if } i = -1. \end{cases}$$

Proof. Note that it suffices to show that $\#H^0(G(L/K), C_L) = [L:K]$, and we do so by induction on the degree. The base case is immediate. Suppose $[L:K] = n$, and let M be an intermediate extension such that $[M:K] = p$ and $[L:M] = n/p$ for some prime divisor p of n. Then we have the exact sequence

$$1 \longrightarrow C_M/N_{L/M}(C_L) \longrightarrow C_K/N_{L/K}(C_L) \longrightarrow C_K/N_{M/K}(C_M) \longrightarrow 1$$

since $N_{L/K} = N_{M/K} \circ N_{L/M}$. For $x \in C_M$, we have

$$N_{M/K}(x) = N_{L/K}(y) = N_{M/K}(N_{L/M}(y)),$$

so $N_{M/K}(x/N_{L/M}(y)) = 1$. Then there exists some z such that $x/N_{L/M}(y) = N_{L/M}(z)$ (prove this as an exercise). Therefore, $x = N_{L/M}(yz)$, and we have injectivity. Note that $C_M/N_{L/M}(C_L) = H^0(G(L/M), C_M)$, $C_K/N_{L/K}(C_L) = H^0(G(L/K), C_L)$, and $C_K/N_{M/K}(C_M) = H^0(G(M/K), C_M)$.

If $p < n$, then the result follows from the inductive hypothesis and the above exact sequence, since $[M:K][L:M] = [L:K]$.

If $p = n$, then let $K' = K(\mu_p)$ and $L' = L(\mu_p)$. Let $d = [K':K]$. Then $d|(p-1) = [\mathbb{Q}(\mu_p) : \mathbb{Q}]$. Since $[L:K] = p$, we have $\gcd(d, [L:K]) = 1$. Therefore, by Galois theory, we have $G(L/K) \simeq G(L'/K')$, where we note that $\#G(L'/K') = 0$. Now, L'/K' is cyclic and contains μ_p. By Theorem 6.2, it follows that $\#H^0(L'/K') = [L':K'] = p$. We will prove that $\#H^0(\mathrm{Gal}(L/K), C_L)$ divides p, from which the result will follow (recall what we proved about the Herbrand quotient). We claim that $H^0(G_L, C_L) \to H^o(G_{L'}, C_{L'})$ is injective. We have maps $C_K \to C_{K'} \to C_{K'}/N_{L'/K'}(C_{L'})$; under the composition of these maps $N_{L/K}(C_L)$ is sent to 1, so the composition factors through $C_K/N_{L/K}(C_L)$. This gives us the map $H^0(G_L, C_L) \to H^o(G_{L'}, C_{L'})$; we now prove it is injective. Notice that $H^0(L/K)$ has exponent p, since $x^p \in N_{L/K}(x)$ for all $x \in C_p$. Hence, the map $H^0(L/K) \to H^0(L/K)$ taking $u \mapsto u^d$ is an isomorphism, since $(d,p) = 1$. Let $\overline{x} \in H^0(L/K)$ be such that $\overline{x} = 1$ in $H^0(G_{L'}, C_{L'})$. Write $\overline{x} = \overline{y}^d$ for $\overline{y} \in H^0(L/K)$ and $\overline{y} = 1$ in $H^0(L'/K')$, so $y = N_{L'/K'}(z')$ for $z' \in C_{L'}$. Then

$$y^d = N_{K'/K}(N_{L'/K'}(z')) = N_{L'/K}(z') = N_{L/K}(N_{L'/L}(z')),$$

where $N_{L'/L}(z')$ is some element $u \in C_L$, so $\overline{x} = N_{L/K}(u)$ for $u \in C_L$. □

One consequence of this result is the *Hasse Norm Theorem*:

Theorem 6.4 (Hasse Norm Theorem)**.** *For L/K a cyclic extension, $x \in K^*$ is a norm if and only if x is a norm in $K_{\mathfrak{p}}^*$ for all $\mathfrak{p}$.*

Proof. Let $G = \mathrm{Gal}(L/K)$ and $G_Q = \mathrm{Gal}(L_Q/K_{\mathfrak{p}})$. We have the following exact sequence

$$1 \longrightarrow L^* \longrightarrow I_L \longrightarrow C_L \longrightarrow 1,$$

which gives an exact sequence

$$1 = H^{-1}(G, C_L) \longrightarrow H^0(G, L^*) \longrightarrow H^0(G, I_L) = \bigoplus H^0(G_Q, L_Q^*).$$

Therefore, $K^*/N_{L/K}L^* \simeq H^0(G, L')$ injects into $\bigoplus K_{\mathfrak{p}}^*/N_{L_Q/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^*)$. □

We now prove Theorem 6.2, the result used in the proof of the class field axiom.

Proof of Theorem 6.2. We have the following exact sequence

$$1 \longrightarrow I_K^{S\cup T}/I_K(S,T)\cap K^* \longrightarrow I_K^{S\cup T}/I_K(S,T) \longrightarrow I_K^{S\cup T}K^*/I_K(S,T)K^* \longrightarrow 1.$$

Hence, $\#(I_K^{S\cup T}K^* : I_K(S,T)K^*/K^*) = [C_K : C_K(S,T)]$. Moreover, we also have $\#(I_K^{S\cup T}\cap K^* : I_K(S,T)\cap K^*) = (K^{S\cup T} : (K^{S\cup T})^n)$. Now, $K^{S\cup T} \simeq \mathbb{Z}^{2s-r-1}\times \mu_n$, so $(K^{S\cup T} : (K^{S\cup T})^n) = n^{2s-r}$. For the last part, we can directly compute that

$$(I_K^{S\cup T} : I_K(S,T)) = \prod_{\mathfrak{p}\in S}(K_{\mathfrak{p}}^* : K_{\mathfrak{p}}^{*n}) = \prod_{\mathfrak{p}\in S}(n^2/|n|\mathfrak{p}) = n^{2s}\prod_{\mathfrak{p}}|n|_{\mathfrak{p}}^{-1} = n^{2s}.$$

Also, $(C_K : C_K(S,T)) = n^{2s}/n^{2s-r} = n^r = [L : K]$. For the inclusion $C_K(S,T) \subset N_{L/K}(C_L)$, let $\alpha \in C_K(S,T)$. We have to check that $\alpha \in N_{L/K}(C_L)$; it is enough to check this *locally*. For $\mathfrak{p}\in S$ and $\alpha_{\mathfrak{p}} \in (K_{\mathfrak{p}}^*)^n$, we have $\alpha_{\mathfrak{p}} = N(K_{\mathfrak{p}}(\sqrt[n]{K_{\mathfrak{p}}^*}))$, and since $L_Q \subset K_{\mathfrak{p}}(\sqrt[n]{K_{\mathfrak{p}}^*})$, we have $\alpha_{\mathfrak{p}}$ is a norm in $K_{\mathfrak{p}}$. For $\mathfrak{p}\in T$, we have $L_Q = K_{\mathfrak{p}}$, since $L = K(\sqrt[n]{\Delta})$ for $\Delta \subset (K_{\mathfrak{p}}^*)^n$. For $\mathfrak{p}\notin S\cup T$, we have that $L_Q/K_{\mathfrak{p}}$ is unramified and $\alpha_{\mathfrak{p}}$ is a unit. Local theory implies that $\alpha_{\mathfrak{p}}$ is an nth power.

If L/K is cyclic, then

$$[L:K] \leq [C_K : N_{L/K}(C_L)] \leq [C_K : C_K(S,T)] = [L:K],$$

which forces equality. □

7. Thursday February 15

Recall Theorem 6.3, which tells us that the idèle class group satisfies the class field axiom. In order to apply abstract class field theory, we need two morphisms $d : G_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$ and $v : C_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$.

Proposition 7.1. *Let $\Omega/\mathbb{Q}$ be*

$$\Omega = \mathbb{Q}(\zeta_n \mid \zeta_n^n = 1 \textit{ for all } n).$$

Let $T = G(\Omega/\mathbb{Q})^{tor} \subset G(\Omega/\mathbb{Q})$, and let $\tilde{Q} = \Omega^T$. Then $\tilde{Q}$ is a $\widehat{\mathbb{Z}}$-extension of Q.

Proof. Note that we may write Ω as the injective limit

$$\omega = \varinjlim_n Q(\zeta_n).$$

Hence,

$$\mathrm{Gal}(\Omega/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varprojlim_n(\mathbb{Z}/n\mathbb{Z})^* = \widehat{\mathbb{Z}}^*.$$

We have $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ (prove this as an exercise). Thus, $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p^*$, and recall that $\mathbb{Z}_p^* = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ for p odd and that $\mathbb{Z}_2^* = \mathbb{Z}_2\times\mathbb{Z}/2\mathbb{Z}$. Now, we may write

$$\widehat{\mathbb{Z}}^* = \widehat{\mathbb{Z}} \times \prod_{p\neq 2}\mathbb{Z}/(p-1)\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

The factor $\widehat{\mathbb{Z}}$ is torsion free. Letting $\widehat{T} = \prod_{p\neq 2}\mathbb{Z}/(p-1)\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, we see that $T = G(\Omega/\mathbb{Q})^{tors} \subset \widehat{T}$. In fact, T is dense in $\widehat{T}$, i.e., $\overline{T} = \widehat{T}$. Because $\Omega^T = \Omega^{\widehat{T}}$ (the fixed field of a subgroup is equal to the field fixed by its closure), we have

$$\mathrm{Gal}(\Omega^{\widehat{T}}/\mathbb{Q}) = \mathrm{Gal}(\Omega/\mathbb{Q})/\overline{T} = \widehat{\mathbb{Z}}.$$

□

In other words, we have a morphism

$$d : G_{\mathbb{Q}} \twoheadrightarrow G_{\Omega^{\overline{T}}/\mathbb{Q}} \simeq \widehat{\mathbb{Z}}.$$

For the $G_{\mathbb{Q}}$-module, let

$$A = \varinjlim_{[K:\mathbb{Q}]<\infty} C_K.$$

Note that $A_K = A^{G(\overline{\mathbb{Q}}/K)} = C_K = I_K/K^*$.

Now, we would like to define a valuation map

$$v : C_Q \to \widehat{\mathbb{Z}}.$$

Let L/K be a finite abelian extension. We define the norm residue symbol $I_K \to G(L/K)$ by taking $\alpha \mapsto [\alpha, L/K] = \prod_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$, where $(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$ is the norm residue symbol from local class field theory. If L/K is infinite, then we can define

$$[\ , L/K] : I_K \to G(L/K)$$

via the compatibility rule $[\ , L/K]|_{L'} = [\ , L'/K]$ for L'/K finite. Putting these all together gives a surjective homomorphism

$$v : I_{\mathbb{Q}} \to \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}},$$

as desired.

Armed with these definitions, we can now prove the statement of global class field theory.

Theorem 7.2 (Global Class Field Theory)**.** *Let L/K be a finite extension. We have a reciprocity homomorphism*

$$r_{L/K} : \mathrm{Gal}(L/K)^{ab} \to C_K/N_{L/K}(C_L).$$

This map is an isomorphism with inverse

$$r_{L/K}^{-1} = (\ , L/K) : C_K \to \mathrm{Gal}(L/K)^{ab}$$

(in fact this map can be defined from $I_K \to \mathrm{Gal}(L/K)^{ab}$). Moreover, the following diagram is commutative:

$$\begin{tikzcd}
K_{\mathfrak{p}}^* \arrow[r, "(\ ;L_Q/K_{\mathfrak{p}})"] \arrow[d] & G(L_Q/K_{\mathfrak{p}}) \arrow[d] \\
C_K \arrow[r, "(\ ;L/K)"] & G(L/K)
\end{tikzcd}$$

7.1. **Brauer Groups.** A reference for the following is Weil's *Basic Number Theory.* Let k be a field, and let A be a k-algebra (with unit, not necessarily commutative) that is finite-dimensional over k.

Definition 7.3. Such an A is called *central* if $Z(A) = k$.

Example 7.4. A classical example is $A = M_n(k)$, the $n \times n$ matrix algebra with entries in k.

Another example is the *Hamilton quaternions*, where $k = \mathbb{R}$ and

$$A = \mathbb{R}(i, j \mid i^2 = j^2 = -1, ij = -ji).$$

This is 4-dimensional over $\mathbb{R}$. More generally, for any field k with characteristic not 2, for $a, b \in k^*$ we can define the quaternion algebra

$$A = k \oplus ki \oplus kj \oplus kij,$$

where we set $i^2 = a$, $j^2 = b$, and $ij = -ij$. As an exercise, determine the following: when is $A \simeq M_2(k)$? We can rephrase the question as follows: when does

$$M_2(k) = k \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \oplus k \begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \oplus k \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \oplus k \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}?$$

Note that because $j^2 = 1$ (in the above example), the $a, b \in k^*$ fixed previously only depend on their images in $k^*/(k^*)^2$. Hence, the above isomorphism holds when $a, b \in (k^*)^2$.

Proposition 7.5. *If A, B are two central k-algebra, then $A \otimes_k B$ is also a central k-algebra.*

Proof. Let $(e_i)_i$ and $(f_j)_j$ be bases of A and B over k, respectively. Let

$$x = \sum_i e_i \otimes y_i \in Z(A \otimes_k B),$$

where $y_i \in B$. For all $b \in B$, we have $x(1 \otimes b) = (1 \otimes b)x$ if and only if

$$\sum_i e_i \otimes y_i b = \sum_i e_i \otimes b y_i,$$

which is the case only if $y_i b = b y_i$ for all i, which implies $y_i \in Z(B)$, so $y_i = \alpha_i \in k$. Hence,

$$x = \sum_i \alpha_i e_i \otimes 1 = z \otimes 1$$

for some $z \in A$, then $z \in Z(A)$ implies that $z = \alpha \in k$, implying $x = \alpha(1 \otimes 1) \in k$. □

Remark 7.6. Let $K \hookrightarrow L$ be an extension of fields. For A a central K-algebra, then $A \otimes_K L$ is also a central L-algebra.

As a convention, a module M over A is a left-module that is finite dimensional over K (so $1 \cdot m = m$ for all $m \in M$).

Definition 7.7. A module M is called *simple* if $M \neq 0$ and $N \subset M$ a sub-M-module implies $N = 0$ or $N = M$.

An algebra A is *simple* if the only two-sided ideals are A and 0.

The study of Brauer groups is the study of central simple algebras over K.

If M is an A-module, then the *annihilator* of M

$$\mathrm{Ann}(M) = \{x \in A \mid xm = 0 \text{ for all } m \in M\}$$

is a two-sided ideal. If $\mathrm{Ann}(M) = 0$, then M is said to be *faithful* (as an A-module).

Proposition 7.8. *Let A be a K-algebra with a faithful simple A-module M. Then every left A-module is isomorphic to a direct sum*

$$\bigoplus_{i \in I} M_i,$$

where I is a finite index set and $M_i \simeq M$.

Proof. First, we show the result for A. Consider a finite subset $\{m_1, \dots, m_n\} \in M$ such that $\mathrm{Ann}(m_1, \dots, m_n) = \mathrm{Ann}(M)$. Let n be minimal for this property. Let $A_i = \mathrm{Ann}(m_{i+1}, \dots, m_n)$, and consider the submodule $M_i = A_i m_i$ of M. In fact, we can view this as a map $A_i \longrightarrow M$ taking $x \mapsto x m_i$ with kernel A_{i-1}. Hence, $A_i / A_{i-1} \simeq M_i \subset M$. By our choice of n, the quotient

$A_i/A_{i-1} \simeq M_i$ is nonzero. Since M is simple, it must be that $M_i \simeq M$. We have $A_0 = 0$ and $A_n = A$, so the A_i's give a filtration of A. By induction, we see that the map

$$A_i \to \bigoplus_{k=1}^{i} M$$

given by $x \mapsto (xm_1, \ldots, xm_i)$ is a bijection. It follows that $A = A_n \simeq \bigoplus_{k=1}^{n} M$.

Now, let M' be an A-module. Let $\{m'_1, \ldots, m'_r\}$ be a basis over K. We have a surjective homomorphism

$$A^r \to M'$$

given by $(x_i) \mapsto \sum_i x_i m'_i$. By what we proved in the preceding paragraph, we have $A^r \simeq M^{nr}$, so it is enough to study the kernel of the surjection $M^{rn} \to M'$, which we call K. Let $I \subset \{1, \ldots, nr\}$ be maximal such that $K \oplus \bigoplus M^I$ is a direct sum. For simplicity, let $I = \{1, \ldots, j\}$. We have

$$K \oplus \bigoplus_{i=1}^{j} M_i$$

and

$$K \oplus \bigoplus_{i=1}^{j} M_i + M_{j+1}.$$

By hypothesis, we must have $K \cap M_{j+1} \neq \{0\}$. But $K \cap M_{j+1}$ is a left A-module contained in M_{j+1}. Therefore, we must have $M_{j+1} = K \cap M_{j+1}$, so $M_{j+1} \subset K$. It follows that $K \oplus \bigoplus_I M_i = M^{nr}$, so $M' \simeq \bigoplus M^I$. □

Proposition 7.9. *Let A and M be as in the above, and let $D = \mathrm{End}_A(M)$. Then D is a finite-dimensional division algebra over K and $A \simeq M_n(D)$ (as algebras) for some $n \geq 1$.*

Proof. Any A-module endomorphism $f : M \to M$ has $\ker(f)$ and $\mathrm{im}(f)$ also as A-modules. The simplicity of M implies that $f = 0$ or f is a bijection. We have $A \simeq M^n$ as A-modules, so $\mathrm{End}_A(A) \simeq \mathrm{End}_A(M^n) \simeq M_n(\mathrm{End}_A(M))$. Now, $D = \mathrm{End}_A(M)$, and

$$K = Z(A) = Z(M_n(\mathrm{End}_A(M))) = Z(\mathrm{End}_A(M)) = Z(D),$$

as desired. □

8. Tuesday February 20

Theorem 8.1. *A central K-algebra A is simple if and only if $M \simeq M_n(D)$, where D is a division algebra over K. The integer n is unique, as is the division algebra D up to isomorphism.*

Proof. For the forward direction, note that A simple implies that A has a left simple faithful A-module. This follows because we can choose a left ideal $\{0\} \neq I \subset A$ of minimum dimension over K. We see that I is a simple nonzero left A-module. Now, recall that I is faithful if the map $F : A \to \mathrm{End}_A(I)$ has kernel zero. Note that $\ker(F) = \mathrm{Ann}_A(I)$ is a two-sided ideal of A; hence $\ker(F) = 0$ or $\ker(F) = A$. But since $I \neq 0$, we must have $\ker(F) = 0$. Hence, $A \simeq M_n(D)$ with $D = \mathrm{End}_A(M)$.

Conversely, suppose $A \simeq M_n(D)$. Let $e_{ij} \in M_n(D)$ denote the matrix with (i, j)-entry equal to 1 and all other entries 0. Let $0 \neq a \in A$, and consider the two-sided ideal $\langle a \rangle$ generated by a. Then $\langle a \rangle = A$. This follows because $e_{ij} a e_{hk} = a_{jh} e_{ik}$ and at least one such $a_{jh} \neq 0$. Hence, a_{jh} is invertible, implying that $e_{ik} \in \langle a \rangle$. Thus, A is a simple algebra. The centrality of A follows because $Z(M_n(D)) = Z(D) = K$. Let $M = Ae_{11}$. We claim that $\mathrm{End}_A(M) \simeq D$. If $f : M \longrightarrow M$ is a left A-module morphism, then $f(x) = ax$ for $a \in D$. Hence, M is a simple left A-module, and $D = \mathrm{End}_A(M)$ implies D is unique. The uniqueness of n follows from the formula $\dim_K(A) = n^2 \dim(D)$. □

Let A/K be an algebra. We define its *opposite* algebra, A^{op}, to be the K-algebra with underlying set A and multiplication $a * b = ba$, where the multiplication ba is done in A.

Proposition 8.2. *Let $C = A \otimes_K A^{op}$. For $a, b \in A$, let $f(a, b) \in \mathrm{End}_K(A)$ be the map taking $x \mapsto axb$. Define $F : C \longrightarrow \mathrm{End}_K(A)$ by $F(a \otimes b) = f(a, b)$. Then A is simple over K if and only if F is surjective, which is the case if and only if $C \simeq \mathrm{End}_K(A)$.*

Proof. Let $N = \dim_K(A)$. Assume that A is not simple: let $0 \neq I \subsetneq A$ be some nontrivial, proper two-sided ideal. For all $c \in C$, we have I is invariant under $F(c)$. Writing $A = I \oplus \tilde{I}$ for some $\tilde{I}$, by considering F as a block-diagonal matrix we see that F is not surjective.

Now, assume that A is simple. Let $C' = \ker(F) = \mathrm{Ann}_C(M)$, where $M = A$ regarded as a C-module. We first claim that M is a simple C-module. To see why this is the case, note that the data of a C-submodule is equivalent to that of a two-sided ideal. We can check that $\mathrm{End}_C(M) = K$ (prove this as an exercise). We conclude that M is a simple, faithful left C/C'-module. Hence,

$$C/C' \simeq M_n(\mathrm{End}_{C/C'}(M)) \simeq M_n(\mathrm{End}_C(M)) \simeq M_n(K),$$

and $Z(C/C') = K$. It follows that $N = \dim_K(M) = n$, so $\dim_K(C/C') = n^2 = N^2 = \dim_K(C)$. This forces $C' = 0$. □

Corollary 8.3. *Now, we profit from our hard work. The following are true:*

(1) *Let L/K be an extension of fields. Then A is central and simple over K if and only if $A_L = A \otimes_L K$ is a central simple algebra.*
(2) *If $K \hookrightarrow L$, where L is algebraically closed, then A is simple over K if and only if $A_L \simeq M_n(L)$.*
(3) *If A is a central simple algebra over K, then $\dim_K A = n^2$.*
(4) *If A and B are central simple algebras over K, then $A \otimes_K B$ is also a central simple algebra over K.*
(5) *Suppose that $\dim_K A = n^2$ and that L is an extension of K. Let $F : A \longrightarrow M_n(L)$ be a homomorphism of K-algebras. Then the a homomorphism of L-algebras $F_L : A_L \longrightarrow M_n(L)$ is an isomorphism.*
(6) *Suppose that K/L is a degree-n extension and that A/K is simple with $\dim_K A = n^2$. If $L' \subset A$ with $L' \simeq L$, then $A_L \simeq M_n(L)$. In other words, A_L* splits.
(7) *If A/K is a simple algebra and $\alpha : A \longrightarrow A$ is a K-automorphism, then $\alpha(x) = a^{-1}xa$ for some $a \in A^*$ for all $x \in A$.*

Proof. We prove each result one at a time.

(1): $F : C \longrightarrow \mathrm{End}_K(A)$ is an isomorphism if and only if $F \otimes L : C_L = C \otimes_K L \longrightarrow \mathrm{End}_L(A_L) = \mathrm{End}_K(A) \otimes_K L$.

(2): By (1), A is simple if and only if A_L is simple, which is the case if and only if $A_L \simeq M_n(D)$ for D/L a division algebra. If $L \neq D$, then take $\xi \in D \setminus L$ and note that $\xi : D \longrightarrow D$ defines an L-linear map given by multiplication by ξ. By Cayley–Hamilton, ξ is algebraic over L, which forces $\xi \in L$. Therefore, $D = L$.

(3): This follows from (2).

(4): We base-change to some algebraically closed field L. By part (2), we have $A_L \simeq M_n(L)$ and $B_L \simeq M_m(L)$. Hence,

$$(A \otimes_K B) \otimes L = A_L \otimes_L \otimes B_L \simeq M_{nm}(L);$$

the result follows from (2).

(6): Without loss of generality, we can assume $L = L'$, in which case A is an L-vector space. Then the map $A \longrightarrow M_n(L) = \mathrm{End}_L(A)$ is an isomorphism by (5).

(7): See page 166 of Weil's *Basic Number Theory.* □

Proposition 8.4. *If A/K is a simple central algebra, then $A_L \simeq M_n(L)$ for L a separable closure of K.*

The above can be found on page 166 of Weil's *Basic Number Theory.*

Proposition 8.5. *Let A be a central simple algebra over K. Then there exists a nonzero linear form* $\mathrm{tr} : A \longrightarrow K$ *(the reduced trace) and a map $N : A \longrightarrow K$ (the reduced determinant) such that for all extensions L/K and $F : A \longrightarrow \mathrm{End}_L(M)$, we have* $\mathrm{tr}(a) = \mathrm{tr}(F(a))$ *and* $N(a) = \det(F(a))$*. If $A = M_n(K)$, $M = K^n$, and $F : A \longrightarrow M_n(K)$, then* tr *is the trace of a matrix and N is the determinant of a matrix.*

8.1. **Brauer Groups.** Let K be a field, and let A and A' be two central simple algebras over K. Then we say $A \sim A'$ (pronounced A is *similar* to A') if $A \simeq M_n(D)$ and $A' \simeq M_k(D)$ for the same division algebra D. We say that A and A' have the same class; denote this by $[A] = [A']$. Let $\mathrm{Br}(K)$ denote the classes of central simple algebras over K under this equivalence.

Theorem 8.6. *We have that* $\mathrm{Br}(K)$ *is an abelian group for the following group law:*

$$[A][A'] = [A \otimes_K A'].$$

This operation has inverse given by $[A]^{-1} = [A^{op}]$ *and trivial class* $1 = [K] = [M_n(K)]$.

Proof. The product is well-defined: for $A \simeq M_n(D)$ and $A' \simeq M_k(D')$, we have $D \otimes D' \simeq M_m(D'')$, where D'' is uniquely defined. Hence, $A \otimes_K A' \simeq M_{nkm}(D'')$; since D'' is uniquely defined, it follows that the product is well-defined.

The associativity and commutativity are left as exercises for the reader. Recall that $C = A \otimes A^{op} \simeq \mathrm{End}_K(A) = M_n(K)$, as desired. □

9. Thursday February 22

The following is supplemented by Chapter IV of Milne's notes on Class Field Theory.

Definition 9.1. Let K be a field and A a central simple algebra over K. Let L be an extension of K such that $A_L = A \otimes_K L \simeq M_n(L)$. Then L is called a *splitting field* of A, and A_L is a *split* central simple algebra.

Proposition 9.2. *Let A be a central simple algebra over K. Then there exists a finite separable extension L/K such that A_L is split.*

Proof. Let K^{sep} denote the separable closure of K, and consider $A \otimes_K K^{sep} \simeq M_n(K^{sep})$. Consider the elementary matrix $E_{ij} \in M_n(K^{sep})$; recall that these elements form a finite K^{sep}-algebra basis for $M_n(K^{sep})$. Now, we can write the image of E_{ij} in $A \otimes_K K^{sep}$ as

$$a_{ij} = \sum_{k \in I_{ij}} \mu_k \otimes v_k,$$

where $\mu_k \in A$ and $v_k \in K^{sep}$. Let $L = K(v_k)$, where $k \in I_{ij}$ for all i, j. It follows that L/K is a finite separable finite extension with $A \otimes_K L \simeq M_n(L)$, as desired. □

The above proposition implies that, for L/K an extension, $\mathrm{Br}(L/K) \subset \mathrm{Br}(K)$, where $\mathrm{Br}(L/K)$ is the set of central simple algebras over K split by L. From the proposition, we have

$$\mathrm{Br}(K) = \bigcup_{\substack{L \subset K^{sep} \\ [L:K] < \infty}} \mathrm{Br}(L/K).$$

9.1. **Brauer Groups and Cohomology.** Let L/K be a Galois extension.

Theorem 9.3. *Let A be a central simple algebra over K with $K \subset L \subset A$ (L is field that is a K-subalgebra of A). Then the following are equivalent:*

(*1*) $L = C_A(L)$;
(*2*) $[A : K] = [L : K]^2$;
(*3*) *L is a maximal commutative K-subalgebra.*

Proof. See page 130 of Milne's notes. Recall that $[A : K] = [L : K][C(L) : K]$, so (1) is equivalent to (2). □

Corollary 9.4. *For D a division algebra over k, the maximal subfields containing k are exactly those of degree $\sqrt{[D : k]}$. Such fields are the splitting fields of D.*

Corollary 9.5. *Let A be a central simple algebra over k. Then L splits A if and only if there exists $B \sim A$ in $\mathrm{Br}(K)$ such that $[B : k] = [L : k]^2$.*

Corollary 9.6. *If A is a central simple algebra over k, then the minimal degree of a splitting field is $\sqrt{[D : k]}$, where $A \simeq M_n(D)$ for D a unique division algebra. This quantity is called the* index *of A in $\mathrm{Br}(k)$.*

Let L/K be a Galois extension. Let

$$\mathcal{A}(L/K) = \{\text{central simple algebras} A/K \mid L \subset A, [A : K] = [L : K]^2\}.$$

Let $A \in \mathcal{A}(L/K)$ and $\sigma \in \mathrm{Gal}(L/K)$. We have the following theorem:

Theorem 9.7 (Skolem–Noether)**.** *For simple $B_1, B_2 \subset A$, a central simple algebra over K, and $f : B_1 \longrightarrow B_2$ an automorphism, then f is inner. In other words, $f(n) = gng^{-1}$ for $g \in A^*$.*

By Skolem–Noether, σ from the above is inner. Hence, for all $x \in L$, we have

$$\sigma(x) = e_\sigma x e_\sigma^{-1}$$

for $e_0 \in A^*$. For $\sigma, \tau \in \mathrm{Gal}(L/K)$, we have $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ for all $x \in L$, so $e_{\sigma\circ\tau} x e_{\sigma\circ\tau}^{-1} = e_\sigma e_\tau x e_\tau^{-1} e_\sigma^{-1}$. Hence, $e_\tau^{-1} e_\sigma^{-1} e_{\sigma\circ\tau} \in C(L) = L \cap A^* = L^*$. There exists $\varphi(\sigma, \tau) \in L^*$ with $\varphi(\sigma, \tau)^{-1} = e_\tau^{-1} e_\sigma^{-1} e_{\sigma\circ\tau}$, so $e_{\sigma\circ\tau}\varphi(\sigma, \tau) = e_\sigma e_\tau$. Thus, we have obtained a function $\varphi : G \times G \longrightarrow L^*$, which is what we need for Galois cohomology. For $\sigma_1, \sigma_2, \sigma_3 \in G$, we have

$$e_{\sigma_1\sigma_2\sigma_3} x e_{\sigma_1\sigma_2\sigma_3}^{-1} = e_{\sigma_1\sigma_2} e_{\sigma_3} x e_{\sigma_3}^{-1} e_{\sigma_1\sigma_2}^{-1}.$$

Some more work shows (prove the following as an exercise) that $\delta\varphi(\sigma_1, \sigma_2, \sigma_3) = 1$, which is the case if and only if

$$\sigma_1(\varphi(\sigma_2, \sigma_3))\varphi(\sigma_1\sigma_2, \sigma_3)^{-1}\varphi(\sigma_1, \sigma_2\sigma_3)\varphi(\sigma_2, \sigma_3)^{-1} = 1,$$

implying that $\varphi \in Z^2(G(L/K), L^*)$. Hence, $(\varphi) \in H^2(G(L/K), L^*)$, and the class (φ) does not depend on e_σ. Thus, f_σ and φ_f differ from φ by a coboundary. In other words, $\sigma(n) = f_\sigma x f \sigma^{-1} = e_\sigma x e_\sigma^{-1}$. Let $\mu_\sigma = e_\sigma^{-1} f_\sigma \in L^*$. Then $e_\sigma \mu_\sigma = f_\sigma$ and

$$\varphi_f(\sigma,\tau) = f_{\sigma\tau}^{-1} f_\sigma f_\tau = \mu_{\sigma\tau}^{-1} e_{\sigma\tau}^{-1} e_\sigma \mu_\sigma e_\tau \mu_\tau = \mu_{\sigma\tau}^{-1} \varphi(\sigma,\tau) e_\tau^{-1} \mu_\sigma e_\tau \mu_\tau = \varphi(\sigma,\tau)[\mu_\sigma^{-1} e_\tau^{-1} \mu_\sigma e_\tau \mu_\tau],$$

and $e_\tau^{-1} \mu_\sigma e_\tau = \sigma^{-1}(\mu_\sigma)$ is a coboundary.

We have a map $\gamma : \mathcal{A}(L/K) \longrightarrow H^2(L/L)$, where $A \mapsto \gamma(A)$ its *factor set.*

Theorem 9.8. *We have that γ is surjective and the fibers are isomorphism classes.*

Proof. For $\varphi : G \times G \longrightarrow L^*$ a 2-cocycle, set

$$A(\varphi) = \bigoplus_{\sigma \in G} L e_\sigma$$

with multiplication law $e_\sigma e_\tau = \varphi(\sigma,\tau) e_{\sigma\tau}$. The cocycle condition implies that this law is associative and that $e_1 = 1$ is the unit. In fact, we have that $A(\varphi)$ is a central simple algebra, and $\gamma(A(\varphi)) = \varphi$.

If $\gamma(A) = \gamma(A')$, we will show that... □

10. Tuesday February 27

Let the setup be as above. To check the cocycle conditions, let $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Gal}(L/K)$. We see that

$$e_{\sigma_1}(e_{\sigma_2}\sigma_3) = e_{\sigma_1}\varphi(\sigma_2,\sigma_3)e_{\sigma_2\sigma_3} = \sigma_1(\varphi(\sigma_2,\sigma_3))e_{\sigma_1}e_{\sigma_2\sigma_3} = \sigma_1(\varphi(\sigma_2,\sigma_3))\varphi(\sigma_1,\sigma_2\sigma_3)e_{\sigma_1\sigma_2\sigma_3}$$

is the same as

$$(e_{\sigma_1}e_{\sigma_2})e_{\sigma_3} = \varphi(\sigma_1,\sigma_2)e_{\sigma_1\sigma_2}e_{\sigma_3} = \varphi(\sigma_1,\sigma_2)\varphi(\sigma_1\sigma_2,\sigma_3)e_{\sigma_1\sigma_2\sigma_3},$$

implying that $\varphi \in Z^2(G, L^*) \longrightarrow H^2(G, L^*)$.

We claim that $\gamma : \mathcal{A}(L/K)/\simeq \longrightarrow H^2(G(L,K), L^*)$ taking $A \mapsto (\varphi(\sigma,\tau))_{\sigma,\tau}$ is an isomorphism with a section (for an introduction to Galois cohomology, see Cassels' and Frölich's book).

Lemma 10.1. *Let A/K be a central simple algebra, with $L \subset A$, and $n = [A : K] = [L : K]^2 = n^2$. Let $(e_\sigma)_\sigma$ be as before. Then $A = \bigoplus_{\sigma \in G} L e_\sigma$.*

Proof. Because $\dim_L(A) = n$, it suffices to show that $(e_\sigma)_{\sigma \in G}$ are linearly independent. Let $(e_\sigma)_{\sigma \in I}$ be a maximal linearly independent family over L. Let $\tau \in G \setminus I$. Then $e_\tau = \sum_{\sigma \in I} a_\sigma e_\sigma$ with not all a_σ zero. For every $b \in L$,

$$\sum_{\sigma \in I} \tau(b) a_\sigma e_\sigma = \tau(b) e_\tau = e_\tau b = \sum_{\sigma \in I} a_\sigma e_\sigma b = \sum_{\sigma \in I} a_\sigma \sigma(b) e_\sigma,$$

which implies that

$$\sum_{\sigma \in I} a_\sigma (\tau(b) - \sigma(b)) e_\sigma = 0.$$

The linear independence of the $(e_\sigma)_{\sigma \in I}$ forces $a_\sigma \neq 0$ for some σ, implying that $\tau(b) = \sigma(b)$ for all $b \in L$, which is a contradiction. □

Thus, if $\gamma(A) = \gamma(A')$, then we get an induced isomorphism of algebras $f : A = \bigoplus L e_\sigma \longrightarrow A' = \bigoplus L e_\sigma$ taking $e_\sigma \mapsto e'_\sigma$ (there is still something to be checked here, in particular that

$[\varphi(\sigma,\tau)] = [\varphi'(\sigma,\tau)]$). In the other direction, let $\varphi : G \times G \to L$ be a 2-cocycle (also called a *factor set*). Then define the *crossed-product algebra*

$$A(\varphi) = \bigoplus_{\sigma \in G} Le_\sigma,$$

where $e_\sigma e_\tau = \varphi(\sigma,\tau)e_{\sigma\tau}$ and $\sigma(x)e_\tau = e_\tau x$ for all $x \in L$.

Lemma 10.2. *With notation as above, $A(\varphi)$ is a central simple algebra over K, $L \subset A(\varphi)$, and $[A(\varphi) : K] = [L : K]^2$.*

Proof. To see that $C_L(A(\varphi)) = L$, note that L embeds into $A(\varphi)$ as Le_1. Write $\alpha \in A(\varphi)$ as

$$\alpha = \sum a_\sigma e_\sigma \in A(\varphi)$$

and suppose that $\alpha x = x\alpha$ for all $x \in L$. Then

$$\sum a_\sigma \sigma(x) e_\sigma = \sum x a_\sigma e_\sigma,$$

implying that $a_\sigma(\sigma(x) - x) = 0$ for all $x \in L$. Hence, $a_\sigma \neq 0$ forces $\sigma = 1$, so $\alpha = a_1 e_1 \in L$.

Let $x \in Z(A(\varphi))$. To show that $x \in L$, consider $xe_\sigma = e_\sigma x = \sigma(x)e_\sigma$. Then $x = \sigma(x)$ for all $\sigma \in G$, so $x \in K$.

Now let $I \subset A(\varphi)$ be a two-sided ideal. Then I is an L-vector space. If there exists σ with $e_\sigma \in I$, then $I = A(\varphi)$ because $e_\tau e_\sigma = \varphi(\tau,\sigma)e_{\sigma\tau}$ where $\varphi(\tau,\sigma) \in L^*$. Assume $I \neq 0$. Let

$$\alpha = \sum_{\sigma \in J} a_\sigma e_\sigma \in I$$

with $|J|$ minimal. Write $\alpha = e_{\sigma_0} + \cdots$. If $a_{\sigma_1} \neq 0$ for $\sigma_1 \neq \sigma_0$. Then for all $a \in L$, we have

$$\sigma_1(a)\alpha - \alpha a = \sum_{\sigma \in J} a_\sigma(\sigma_1(a) - \sigma(a))e_\sigma \in I.$$

There exists a such that $\sigma_1(a) \neq \sigma(a)$, implying that the sum in the above vanishes at $\sigma = \sigma_1$, so we can take $J \setminus \{\sigma_1\}$ as our index set. However, this contradicts the definition of J, implying $\alpha = e_{\sigma_0}$. □

Lemma 10.3 (Lemma 3.14 in Milne). *With notation as above,*

$$A(\varphi + \varphi') \simeq A(\varphi) \otimes_k A(\varphi').$$

Corollary 10.4. *As a result, we have an isomorphism of groups*

$$H^2(G(L,K), L^*) \simeq \mathrm{Br}(L/K).$$

Proof. If $A \in \mathrm{Br}(L/K)$, then there exists a central simple algebra B such that $B \sim A$ and $L \subset B$ with $[B : K] = [L : K]^2$. □

Corollary 10.5. *Fix $K \subset K^{sep}$ a separable closure of K. Then*

$$\mathrm{Br}(K) = \varinjlim_{\substack{L/K \text{ finite, Galois} \\ L \subset K^{sep}}} \mathrm{Br}(L/K) = \varinjlim H^2(G(L/K), L^*) \simeq H^2(\mathrm{Gal}(K^{sep}/K), (K^{sep})^*).$$

Remark 10.6. We have $\mathrm{Br}(L/K) \simeq H^2(G(L/K), L^*)$, and recall that $H^2(G(L/K), L^*)$ is killed by multiplication by $[L : K]$. Hence, $\mathrm{Br}(L/K)$ is torsion, implying $\mathrm{Br}(K)$ is torsion.

Open problem (period-index problem): Given a central simple algebra A over k, then $[A] \in \mathrm{Br}(k)$ is torsion. If $n = [L : K]$, where $L \subset D$ a division algebra, and $A \sim M_n(D)$, then $n[A] = 0$.

The integer n is called the index of A. The period of A is the order of $[A]$ in $\mathrm{Br}(K)$. By the above, we have that the period divides the index; but are they equal? It depends on K. There are many cases where they are known to be equal, but several other cases where they are not.

10.1. The Brauer Group of Some Special Fields.

Let k be a finite field. Then

$$H^2(\mathrm{Gal}(L/K), L^*) = 0$$

for all finite extensions L/k. Hence, $\mathrm{Br}(k) = 0$. This follows from the following theorem.

Theorem 10.7 (Wedderburn). *Any division algebra which is finite as a set is a field.*

For $\mathbb{R}$, we have $\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = \{1, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$. Hence,

$$H^2(\mathrm{Gal}(\mathbb{C}, \mathbb{R}), \mathbb{C}^*) \simeq \mathbb{R}^*/N(\mathbb{C}^*) \simeq \mathbb{Z}/2\mathbb{Z}.$$

A nontrivial cocycle is given by $\varphi : G \times G \longrightarrow \mathbb{C}^*$, where

$$\varphi(\rho, \tau) = \begin{cases} -1 & \text{if } \rho = \tau = \sigma; \\ 1 & \text{otherwise.} \end{cases}$$

We have $A(\varphi) = \mathbb{H}$, so we see that the central simple algebras over $\mathbb{R}$ are either isomorphic to $M_n(\mathbb{R})$ or $M_n(\mathbb{H})$.

11. Thursday February 29

Let $(K, |\cdot|)$ be a non-archimedean local field. Let D be a division algebra over K with $[D : K] = n^2$. For every subfield $K \subset L \subset D$, the absolute value $|\cdot|$ has a unique extension to L. If $\alpha \in D \setminus \{0\}$, then $K(\alpha)$ is a finite extension of $K \subset D$, and hence $|\alpha|$ is well-defined. Thus, we have an extension $|\cdot| : D \longrightarrow \mathbb{R}_{\geq 0}$. It satisfies the following properties

(1) $|\alpha| = 0$ if and only if $\alpha = 0$
(2) $|\alpha\beta| = |\alpha||\beta|$
(3) $|\alpha + \beta| \leq \max(|\alpha|, \beta)$.

As an exercise, show that $|\alpha| = |N_{L/K}(\alpha)|^{1/[L:K]}$; (3) is also left as an exercise.

Now, let $q = |\mathcal{O}_K/\mathfrak{m}| = |\kappa|$, where κ is the residue field of K. Write $|\alpha| = q^{-\mathrm{ord}(\alpha)}$. We see that we have the following diagram

$$\begin{tikzcd} K^* \arrow[r, "\mathrm{ord}"] \arrow[d] & \mathbb{Z} \arrow[d] \\ D^* \arrow[r, "\mathrm{ord}"] & \frac{1}{n}\mathbb{Z}, \end{tikzcd}$$

since the maximal degree of a subfield contained in D is n. Let

$$\mathcal{O}_D = \{\alpha \in D \mid \mathrm{ord}(\alpha) \geq 0\} \qquad \text{and} \qquad \mathfrak{p} = \{\alpha \in D \mid \mathrm{ord}(\alpha) > 0\}.$$

For all subfields $L \subset D$, we have $\mathcal{O}_D \cap L = \mathcal{O}_L$ and $\mathfrak{p} \cap L = \mathfrak{p}_L$. Every $\mathcal{O}_D$-ideal of $\mathcal{O}_D$ is of the form $\mathfrak{p}^n$ for $n \geq 0$. Then $\mathcal{O}_D\mathfrak{p}_K = \mathfrak{p}_K\mathcal{O}_D = \mathfrak{p}^e$ for some $e \geq 1$. We have $e \leq n$, since any element $x \in \mathfrak{p}$ has $\mathrm{ord}(x^e) \in \mathbb{Z}$, so $\mathrm{ord}(x) \in \frac{1}{e}\mathbb{Z}$. The algebra $\mathcal{O}_D/\mathfrak{p}$ is a division algebra and it is finite (it is a κ-vector space of finite dimension). By Theorem 10.7, we have that $\mathcal{O}_D/\mathfrak{p}$ is a field. Let $f = [\mathcal{O}_D/\mathfrak{p} : \kappa]$, and let $a \in \mathcal{O}_D$ be such that $\mathcal{O}_D/\mathfrak{p} = \kappa[\bar{a}]$. Note that $f \leq [K(a) : K] \leq n$, so $f \leq n$.

We claim that $n^2 = ef$. To see why this is the case, consider the following filtration

$$\mathfrak{p}^e \subset \mathfrak{p}^{e-1} \subset \cdots \subset \mathfrak{p} \subset \mathcal{O}_D.$$

We have that $|\mathfrak{p}^i/\mathfrak{p}^{i+1}| = |\mathcal{O}_D/\mathfrak{p}| = q^f$. Hence, $|\mathcal{O}_D/\mathfrak{p}^e| = |\mathcal{O}_D/\mathfrak{p}_K\mathcal{O}_D| = q^{ef}$ and

$$\mathcal{O}_D = \bigoplus_{i=1}^{n^2} \mathcal{O}_K e_i.$$

Now,

$$\mathcal{O}_D/\mathfrak{p}_K\mathcal{O}_D = \bigoplus_{i=1}^{n^2} \mathcal{O}_K/\mathfrak{p}_K,$$

implying that $|\mathcal{O}_D/\mathfrak{p}_K\mathcal{O}_D| = q^{n^2}$. This implies $n^2 = ef$; the inequalities $e \leq n$ and $f \leq n$ force $e = f = n$. Since $e > 1$ (unless $n = 1$), then D is ramified over K (or $D = K$). Moreover, $L = K(a)$ has degree $f = n$ and it is unramified over K. Hence, $[L : K] = \sqrt{[D : K]}$ implies that L splits D. Thus, D is split by an unramified extension of K, and we have $\mathrm{Br}(K) \simeq \mathrm{Br}(K^{unr}/K)$.

We can define a map $\mathrm{inv}_K : \mathrm{Br}(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$ in the following way: let D/K be a division algebra. Let $K \subset L \subset D$ be unramified of degree n. Let $\sigma \in \mathrm{Gal}(L/K)$ be the Frobenius automorphism. There exists $\alpha \in D$ such that $\sigma(x) = \alpha x \alpha^{-1}$ for all $x \in L$ (by the Skolem–Noether Theorem). Hence, α is determined up to some element of $C_D(L) = L$. Therefore, $\mathrm{ord}(\alpha) \in \mathbb{Q}/\mathbb{Z}$ is well-defined independently from α. For $\alpha' = u\alpha$ for $u \in L$, then

$$\mathrm{ord}(\alpha') = \mathrm{ord}(\alpha) + \mathrm{ord}(u),$$

and $\mathrm{ord}(u) \in \mathbb{Z}$. We define $\mathrm{inv}_K(D) = \mathrm{ord}(\alpha) \in \mathbb{Q}/\mathbb{Z}$.

Example 11.1. Let L/K be unramified of degree n with Frobenius element $\sigma \in \mathrm{Gal}(L/K)$. Then

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j \leq n - 1; \\ \pi \in \mathfrak{p}_K = (\pi) & \text{if } i + j > n - 1. \end{cases}$$

Show as an exercise that φ is a cocycle and that $\mathrm{inv}_K(A(\varphi) = 1/n$.

Theorem 11.2. *The map* $\mathrm{inv}_K : \mathrm{Br}(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$ *is a bijection.*

Proof. Suppose L/K an unramified extension. From local class field theory, we have a surjective norm map $N : U_L = \mathcal{O}_L^* \to U_K = \mathcal{O}_K^*$; we also have that $H^2(G, U_L) = 0$. Writing $L^* = U_L \times \pi^{\mathbb{Z}}$, we see that

$$H^2(G, L^*) \simeq H^2(G, \pi^{\mathbb{Z}}) \simeq H^2(G, \mathbb{Z}),$$

where in the right-most cohomology the action of G on $\mathbb{Z}$ is trivial. We have the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Q} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

and the following cohomological long exact sequence

$$\begin{tikzcd} 0 = H^1(G,\mathbb{Q}) \arrow[r] & \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[r] & H^2(G,\mathbb{Z}) \arrow[r] & H^2(G,\mathbb{Q}) \end{tikzcd}.$$

We have that

$$H^2(G, \mathbb{Q}) \simeq \{\text{central extensions } 1 \to \mathbb{Q} \to A \to G \to 1\}.$$

We will show next time that

$$\{\text{central extensions } 1 \to \mathbb{Q} \to A \to G \to 1\} = \{1 \to \mathbb{Q} \to \mathbb{Q} \times G \to G \to 1\}.$$

Hence, we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathrm{Br}(L/K) \arrow[r] & 0. \end{tikzcd}$$

Taking the inductive limit over all unramified extensions L/K, we see that

$$\mathrm{Br}(K^{unr}/K) = \mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z},$$

as desired. □

12. Tuesday March 5

12.1. The Brauer Group of a Global Field.

Let K be a number field. There is a map

$$\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$$

Recall that $\mathrm{Br}(K_v) \simeq \mathbb{Q}/\mathbb{Z}$ if v is a finite place, $\mathrm{Br}(\mathbb{R}) \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and $\mathrm{Br}(\mathbb{C}) = 0$. Hence, we have a map

$$\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z},$$

where the second map is given by $\sum_v \mathrm{inv}_v$.

Theorem 12.1. *The sequence*

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Br}(K) \arrow[r] & \bigoplus_v \mathrm{Br}(K_v) \arrow[r, "\sum_v \mathrm{inv}_v"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

is exact.

Let L/K be a Galois extension.

Lemma 12.2. *The map*

$$\mathrm{Br}(L/K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_Q/K_{\mathfrak{p}})$$

is injective.

Proof. Recall that we have

$$\mathrm{Br}(L/K) \simeq H^2(G(L/K), L^*)$$

and that

$$\mathrm{Br}(L_Q/K_{\mathfrak{p}}) \simeq H^2(G(L_Q/K_{\mathfrak{p}}), L_Q^*).$$

Assume that L/K is finite and Galois. Then we have the following exact sequence of $G(L/K)$-modules

$$\begin{tikzcd} 0 \arrow[r] & L^* \arrow[r] & I_L \arrow[r] & C_L \arrow[r] & 0. \end{tikzcd}$$

This yields a long exact sequence

$$\begin{tikzcd} H^1(G, C_L) \arrow[r] & H^2(G, L^*) \simeq \mathrm{Br}(L/K) \arrow[r] & H^2(G, I_L) \simeq \bigoplus_{\mathfrak{p}} H^2(G_Q, L_Q^*) \simeq \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_Q/K_{\mathfrak{p}}). \end{tikzcd} ,$$

which can be reexpressed as

$$\begin{tikzcd} 0 = H^1(G, I_L) \arrow[r] & H^1(G, C_L) \arrow[r] & \mathrm{Br}(L/K) \arrow[r] & \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_Q/K_{\mathfrak{p}}), \end{tikzcd}$$

where the first equality follows from Hilbert 90. Thus, we see that the map in the problem statement is injective if and only if $H^1(G, C_L) = 0$, which we proved in global class field theory. Taking the limit over L implies the desired result, since

$$\mathrm{Br}(K) = \bigcup_{L/K \text{ finite, Galois}} \mathrm{Br}(L/K),$$

as desired. □

Corollary 12.3. *A central simple algebra over K is split if and only if it splits over K_v for all v.*

Proof of Theorem 12.1. It remains to show exactness at the middle term of the sequence. The first thing to check is that for all $x \in \mathrm{Br}(K)$, then $\sum_v \mathrm{inv}_v(x) = 0$. For a quaternion algebra A over K, if A_v is a division algebra, then we say that A_v is ramified. The number of places v such that A_v is ramified is even, which implies that $\sum_v \mathrm{inv}_v(x) = 0$. □

Lemma 12.4. *Let L/K be finite and Galois. Then for all $\alpha \in H^2(L/K) = H^2(G(L/K), L^*)$, we have*

$$\sum_v \mathrm{inv}_v(\alpha) = 0.$$

Proof. Recall from global class field theory that for L/K abelian, we have the reciprocity homomorphism

$$r_{L/K}^{-1} = \Phi_{L/K} : I_K \to G(L/K)$$

factors through C_K if and only if $K^* \subset \ker(\Phi_{L/K})$. We will show that $K^* \subset \ker(\Phi_{L/K})$ if and only if $\sum_v \mathrm{inv}_v(\alpha) = 0$

Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$, where G acts on $\mathbb{Q}/\mathbb{Z}$ trivially. The exact sequence

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

gives us a map

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$$

taking $\chi \mapsto \delta_\chi$. Then we have the following diagram:

$$\begin{tikzcd}
K^* = H^0(G, L^*) \arrow[r] \arrow[d, "\cup\delta_\chi"] & I_K = H^0(G, I_L) \arrow[r, "\Phi_{L/K}"] \arrow[d, "\cup\delta_\chi"] & G \arrow[d, "\chi"] \\
H^2(G, L^*) \arrow[r] & H^2(G, I_L) \arrow[r, "\sum_v \mathrm{inv}_v"] & \mathbb{Q}/\mathbb{Z};
\end{tikzcd}$$

the right square of the above commutes (see Proposition 3.6 in Chapter 3 in Milne's notes). The maps $\cup\delta_\chi$ come from the cup product

$$H^0(G, L^*) \times H^2(G, \mathbb{Z}) \to H^2(G, L^*).$$

Since L/K is cyclic, we have $\chi(G) \subset \frac{1}{n}\mathbb{Z}/\mathbb{Z}$; we may choose χ to be an isomorphism. Thus, we can modify the above diagram to be

$$\begin{tikzcd}
K^*/N_{L/K}(L^*) \arrow[r] \arrow[d, "\cup\delta_\chi"] & I_K/N_{L/K}(I_L) \arrow[r, "\Phi_{L/K}"] \arrow[d, "\cup\delta_\chi"] & G \arrow[d, "\chi"] \\
H^2(G, L^*) \arrow[r] & H^2(G, I_L) \arrow[r, "\sum_v \mathrm{inv}_v"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z};
\end{tikzcd}$$

the three vertical maps are isomorphisms. From global class field theory, we have exactness in the middle for L/K cyclic.

Now, we need to show that for any central simple algebra A/K, there exists cyclic L/K such that A_L is split.

To see that $\sum_v \mathrm{inv}_v(\alpha) = 0$ implies $K^* \subset \ker(\Phi_{L/K})$, note that for all $a \in K^*$, $\chi(\Phi_{L/K}(a)) = 0$, which implies $\Phi_{L/K}(a) = 0$ and hence that $K^* \subset \ker(\Phi_{L/K})$. □

(Look up Grunewald–Wang Theorem (Milne)).

12.2. **Global Class Field Theory.** For K a number field, we have a bijective correspondence

$$L \mapsto \mathcal{N}_L = N_{L/K}(C_L)$$

between finite abelian extensions and closed subgroups of C_K of finite index. Let $\mathfrak{m} = \prod_{\mathfrak{p} \times \infty} \mathfrak{p}^{n_\mathfrak{p}}$ be a module in K. Then

$$C_K^\mathfrak{m} = I_K^\mathfrak{m} K^*/K^* \subset C_K$$

is closed of finite index, and the class field $K^\mathfrak{m}/K$ corresponds to $\mathrm{Gal}(K^\mathfrak{m}/K) \simeq C_K/C_K^\mathfrak{m}$.

Remark 12.5. For L/K finite abelian, then there exists $\mathfrak{m}$ such that $C_K^\mathfrak{m} \subset \mathcal{N}_L$ if and only if $L \subset K^\mathfrak{m}$. The quantity $f = \gcd(\mathfrak{m}, C_K^\mathfrak{m} \subset \mathcal{N}_L)$ is called the *conductor* of L; this is compatible with the conductor from local class field theory.

If $\mathfrak{m} = 1$, then we have $\mathrm{Gal}(K^1/K) \simeq \mathrm{Cl}_K^1$ and the following exact sequence

$$1 \longrightarrow \mathcal{O}^*/\mathcal{O}_+^* \longrightarrow \prod_\mathfrak{p} \mathbb{R}^*/\mathbb{R}_+^* \longrightarrow \mathrm{Cl}_K^1 \longrightarrow \mathrm{Cl}_K \longrightarrow 1.$$

The field K^1 is called the *big Hilbert class field* of K.

Proposition 12.6. *We have that K^1 is the maximal unramified abelian extension of K.*

Definition 12.7. The *Hilbert class field H* is the field such that $\mathrm{Gal}(K/K) \simeq \mathrm{Cl}_K$, the ideal class group of K. In fact, H is the maximal unramified abelian extension of K where the infinite real places remain real (i.e., they are split).

How does one go about producing abelian extensions? For $K = \mathbb{Q}$, take $\mathfrak{m} = (m)$. Then $K^\mathfrak{m} = \mathbb{Q}(\zeta_m)$ is the mth cyclotomic extension; Kronecker–Weber implies that any abelian extension of $\mathbb{Q}$ embed into $\mathbb{Q}(\zeta_m)$ for some m. In other words, any abelian extension of $\mathbb{Q}$ is contained by adjoining . This is also known for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$. For an elliptic curve over $\mathbb{C}$ with complex multiplication (i.e., with $\mathrm{End}(E) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{-D})$), the Hilbert class field H of K is given by $H = K(j(E))$. For $K = \mathbb{Q}(\sqrt{D})$ and $D \geq 2$, analogous results are unknown.

13. Tuesday March 19

13.1. **Analytic Methods in Algebraic Number Theory.** Let K be a number field. The main object of study in the sequel will be the *Dedekind zeta function*

$$\zeta_K(s) = \sum_{0 \neq I \subset \mathcal{O}_K} \frac{1}{|I|^s},$$

where $s \in \mathbb{C}$ is such that $\mathrm{Re}(s) > 1$. For $K = \mathbb{Q}$, this is just the Riemann zeta function $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^2}$.

Proposition 13.1. *The series $\sum_{n \geq 1} \frac{1}{n^2}$ converges absolutely for $\mathrm{Re}(s) > 1$ and uniformly on $\mathrm{Re}(s) \geq 1 + \sigma$ for $\sigma > 1$. Hence, ζ is a holomorphic function on $\mathrm{Re}(s) > 1$ and satisfies*

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

For more on the Riemann zeta function and its applications to number theory, see Daniel Marcus's *Number Fields.* The Riemann zeta function can be holomorphically extended to the entire complex plane $\mathbb{C}$ except at 1, where it has a pole. Let

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y},$$

which is absolutely convergent for $\mathrm{Re}(s) > 0$. Thus, $\Gamma(s)$ is holomorphic for $\mathrm{Re}(s) > 0$.

Lemma 13.2. *We have* $\Gamma(s) = s\Gamma(s)$, *implying* $\Gamma(s) = \Gamma(s+1)/s$ *for* $\mathrm{Re}(s) > 0$. *The above defines an analytic continuation of* Γ *to* $\mathbb{C}$ *with poles at* $-n$ *for* $n \in \mathbb{N}$. *The residue of the pole at* $-n$ *is* $(-1)^n/n!$. *We also have* $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$. *Finally,*

$$\Gamma(s)\Gamma(s+1/2) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s),$$

$\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(1) = 1$, *and* $\Gamma(n+1) = n!$.

Let

$$Z(s) = \pi^{-s/2}\Gamma\left(s/2\right)\zeta(s),$$

which is called the *completed zeta function*. This function will be better behaved than the Riemann zeta function.

Proposition 13.3. *For* $\mathrm{Re}(s) > 1$, *we have*

$$Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1)y^{s/2}\frac{dy}{y},$$

where

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{i\pi n^2\tau}$$

(θ is an example of a modular form).

Proof. Sketch of the proof:

$$Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \sum_{n\geq 1}\frac{\pi^{-s/2}}{n^2}\int_0^\infty e^{-y}y^{s/2}\frac{dy}{y} = \sum_{n\geq 1}\int_0^\infty e^{-y}\left(\frac{y}{\pi n^2}\right)^{s/2}\frac{dy}{y};$$

changing variables gives

$$\sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y}y^{s/2}\frac{dy}{y} = \int_0^\infty \left(\sum_{n\geq 1} e^{-\pi n^2 y}\right)y^{s/2}\frac{dy}{y},$$

where the equality above follows from applying one's favorite convergence theorem. □

Theorem 13.4. *The completed zeta function admits an analytic continuation to* $\mathbb{C} \setminus \{0,1\}$ *with simple poles at* $s = 0$ *and* $s = 1$, *both having residue* -1. *Moreover,* Z *satisfies*

$$Z(s) = Z(1-s).$$

Mellin transform: given $f : \mathbb{R}_+^* \longrightarrow \mathbb{C}$, the *Mellin transform* of f is

$$L(f,s) = \int_0^\infty (f(0) - f(\infty))y^s\frac{dy}{y},$$

assuming that $\lim_{t\to\infty} f(t) = f(\infty)$ exists and the integral converges.

Theorem 13.5 (Mellin Principle). *Suppose we have continuous* $f, g : \mathbb{R}_+^* \longrightarrow \mathbb{C}$ *satisfying the following properties. Suppose that* $f(y) = a_0 + O(e^{-cy^\alpha})$ *as* $y \longrightarrow \infty$ *and* $g(y) = b_0 + O(e^{-cy^\alpha})$ *as* $y \longrightarrow \infty$. *Next, assume that* $f(1/y) = cy^k g(y)$ *for some* $c \neq 0$ *and* $k > 0$. *Then the following hold.*

(1) $L(f,s)$ *and* $L(g,s)$ *converge absolutely and uniformly on compact domains of* $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > k\}$. *In particular,* $L(f,s)$ *and* $L(g,s)$ *are holomorphic on* $\mathrm{Re}(s) > k$.

(2) *$L(f,s)$ and $L(g,s)$ admit holomorphic extensions to the entire complex plane, except at* 0 *and* k*. At 0 and k there are poles with residues* $\mathrm{Res}_{s=0}(L(f,s)) = -a_0$, $\mathrm{Res}_{s=k}(L(f,s)) = cb_0$, $\mathrm{Res}_{s=0}(L(g,s)) = -b_0$, *and* $\mathrm{Res}_{s=k}(L(f,s)) = a_0/c$.

(3) *Functional equation: $L(f,s) = cL(g,s)$.*

Proof. Write

$$L(f,s) = \int_0^\infty (f(y) - f(\infty))y^s \frac{dy}{y}.$$

Near ∞, the integrand is $O(e^{-\beta y^\alpha})y^s/y$, which is integrable near ∞. Near 0, we make the change of variables $y = 1/y$ and write

$$(f(1/y)-a_0)\frac{1}{y^s}\frac{1}{y} = (cy^k g(y)-a_0)\frac{1}{y^{s+1}} = \frac{c}{y^{s+1-k}}\left(g(y) - \frac{a_0}{cy^k}\right) = (g(y)-b_0)\frac{c}{y^{s+1-k}}+\left(b_0 - \frac{a_0}{cy^k}\right)\frac{c}{y^{s+1-k}}.$$

The first summand in the right-hand side of the above is $O(e^{-\beta y^\alpha})$, which is integrable near ∞, and the second summand is integrable for $\mathrm{Re}(s+1-k) > 1$. Therefore, uniform convergence implies that $L(f,s)$ and $L(g,s)$ are analytic on $\mathrm{Re}(s) > k$.

Writing

$$L(f,s) = \int_0^1 (f(y) - f(\infty))y^s \frac{dy}{y} + \int_1^\infty (f(y) - f(\infty))y^s \frac{dy}{y}$$

as

$$c\int_1^\infty (g(y) - b_0)y^{k-s}\frac{dy}{y} + \int_1^\infty \left(cb_0 - \frac{a_0}{y^k}\right)\frac{dy}{y^{s+1-k}} + \int_1^\infty (f(y) - f(\infty))y^s\frac{dy}{y},$$

which can be reexpressed as

$$c\int_1^\infty (g(y) - g(\infty))y^{k-s}\frac{dy}{y} + \int_1^\infty (f(y) - f(\infty))y^s\frac{dy}{y} - \frac{a_0}{s} - \frac{cb_0}{k-s}.$$

Replace f by g, a_0 by b_0, b_0 by a_0, and c by $1/c$ to yield a similar expression which implies the functional equation. The integrals in the above expression are entire functions, which tells us the residues of the poles. □

Armed with the Mellin principle, we return to studying the completed zeta function

$$Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1)y^{s/2}\frac{dy}{y}.$$

Note that

$$2Z(2s) = \int_0^\infty (\theta(iy) - 1)y^s\frac{dy}{y}$$

is the Mellin transform of $f(y) = \theta(iy)$. We have $f(y) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 y}$, and $\theta(\tau) = \sum_n e^{i\pi n^2\tau}$ converges for $\mathrm{Im}(\tau) > 0$ and is holomorphic on $\mathbb{H}$. We are interested in the restriction of θ to the imaginary axis. By Poisson summation, we have

$$f(y) = \frac{1}{\sqrt{y}}f\left(\frac{1}{y}\right).$$

In particular, we have $k = 1/2$, $c = 1$, and

$$f(y) = 1 + \sum_{n\neq 0} e^{-\pi n^2 y},$$

which is $O(e^{-\pi y})$ as $y \longrightarrow \infty$. Thus, we may apply the Mellin principle, which implies the desired properties of $Z(s)$.

Corollary 13.6. *The Riemann zeta function $\zeta(s)$ has a holomorphic continuation to $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$ with residue 1. Then*

$$\zeta(1-s) = \frac{2}{(2\pi)^s}\Gamma(s)\cos(\pi s/2)\zeta(s).$$

Proof. Write $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ and use $Z(1-s) = Z(s)$. □

The discussion in this section is adapted from the last chapter of Neukirch.

14. Thursday March 21

Remark 14.1. We can compute the values of the zeta function using the Bernoulli numbers: $\zeta(1-k) = -B_k/k$. From this, we get

$$\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k},$$

which gives us the famous formulas $\sum \frac{1}{n^2} = \pi^2/6$, $\sum \frac{1}{n^4}$, etc. The values of ζ at the odd numbers are far more mysterious. It is a result due to Apéry that $\zeta(3)$ is irrational. See section 1 of the last chapter of Neukirch for more details.

14.1. Dirichlet L-Series.

Let $m \geq 1$ and $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, which is called a *Dirichlet character* mod m. We can extend χ to the integers by setting $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$, where $\chi(n_1) = \chi(\overline{n_1})$ for $(n_1, m) = 1$ and where $\chi(n_1) = 0$ for $(n_1, m) > 1$. To χ, we may associate the Dirichlet L-series

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

for $\mathrm{Re}(s) > 1$. Note that if $\chi = \mathbb{1}$ is the trivial character for $m = 1$, then $L(\mathbb{1}, 2) = \zeta(s)$.

For $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow S^1$, we say that χ is *primitive* if χ does not factor as $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/d\mathbb{Z})^* \longrightarrow S^1$ where $d|m$ and $d < m$. In other words, χ is primitive if there is some $u \in (\mathbb{Z}/m\mathbb{Z})^*$ not congruent to 1 mod m such that $u \mapsto 1$ mod d but $\chi(u) \neq 1$. The smallest m such that $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow S^1$ is primitive is called the *conductor* of χ.

Proposition 14.2. *We have that $L(\chi, s)$ converges absolutely and uniformly on $\mathrm{Re}(s) \geq 1 + \delta$ for $\delta > 0$, so $L(\chi, s)$ is holomorphic on $\mathrm{Re}(s) > 1$ and*

$$L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)/p^s}.$$

The proof of these results is almost exactly the same as the analogous proofs for the Riemann zeta function.

Theorem 14.3. *$L(\chi, s)$ admits a holomorphic continuation to $\mathbb{C} \setminus \{1\}$ with a pole at $s = 1$. If $\chi \neq \mathbb{1}$, then $L(\chi, s)$ is holomorphic on the entire complex plane.*

For $m > 1$ and $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}$ given by $\chi(x) = 1$, we have

$$L(\chi, s) = \prod_{p \nmid m} \frac{1}{1 - 1/p^s} = \zeta(s) \prod_{p|m}\left(1 - \frac{1}{p^s}\right).$$

More generally, for χ a character mod m and χ' a primitive character mod d that comes from χ, we have

$$L(\chi, s) = L(\chi', s) \prod_{p \mid m, p \nmid d} \left(1 - \frac{1}{p^s}\right).$$

Ultimately, this integral representation of $L(\chi, s)$ will allow us to apply the Mellin principle.

Definition 14.4. We define the *exponent* of χ as

$$\chi(-1) = (-1)^\epsilon \chi(1),$$

where $\epsilon = 0$ or $\epsilon = 1$. In the former case, χ is called an *even character*; in the latter, χ is *odd.*

We can extend a character χ to be a function of ideals by

$$\chi((n)) = \chi(n) \left(\frac{n}{|n|}\right)^\epsilon.$$

Such a character is called a *Hecke character* (or, in German, Größencharaktere). Let

$$\Gamma(\chi, s) = \Gamma\left(\frac{s+\epsilon}{2}\right) = \int_0^\infty e^{-y} y^{(s+\epsilon)/2} \frac{dy}{y}.$$

We have

$$\left(\frac{m}{\pi}\right)^{(s+\epsilon)/2} \Gamma(\chi, s) L(\chi, s) = \int_0^\infty \sum_{n=1}^\infty \chi(n) n^\epsilon e^{-\pi n^2 y/m} y^{(s+\epsilon)/2} \frac{dy}{y}.$$

Define the following theta series:

$$\theta(\chi, z) = \sum_{n \in \mathbb{Z}} \chi(n) n^\epsilon e^{i\pi n^2 z/m}.$$

If we set

$$g(y) = \sum_{n=1}^\infty \chi(n) n^\epsilon e^{-\pi n^2 y/m},$$

then

$$\theta(\chi, iy) = \chi(0) + 2g(y).$$

If $m = 1$, then replace χ by 1, and we get the usual Jacobi theta function $\theta(1, z) = \theta(z)$ (introduced previously).

Definition 14.5. The completed L series is $\Lambda(\chi, s) = L_\infty(\chi, s) L(\chi, s)$ for $\mathrm{Re}(s) > 1$, where

$$L_\infty(\chi, s) = \left(\frac{m}{\pi}\right)^{s/2} \Gamma(\chi, s)$$

is the *Euler factor* at ∞.

We have

$$\Lambda(\chi, s) = \frac{1}{2} \left(\frac{\pi}{m}\right)^{\epsilon/2} \int_0^\infty (\theta(\chi, iy) - \chi(0)) y^{(s+\epsilon)/2} \frac{dy}{y}.$$

Proposition 14.6. *For $a, b, \mu \in \mathbb{R}$ with $\mu > 0$, we have*

$$\theta_\mu(a, b, z) = \sum_{g \in \mu\mathbb{Z}} e^{\pi i (a+g)^2 z + 2\pi i b g}$$

converges absolutely on $\operatorname{Im}(z) > 0$ *and uniformly on* $\operatorname{Im}(z) \geq \delta$*. We have that*

$$\theta_\mu(a, b, -1/z) = e^{-2\pi iab}\frac{\sqrt{z/i}}{\mu}\theta_{1/\mu}(-b, a, z).$$

Proof. The basic idea is to use the Poisson summation formula. □

If we differentiate $\theta_\mu(a, b, -1/z)$ with respect to z and define

$$\theta_\mu^\epsilon(a, b, z) = \frac{1}{(2\pi i)^\epsilon z^\epsilon}\frac{d^\epsilon}{da^\epsilon}\theta_\mu(a, b, z),$$

then

$$\theta_\mu^\epsilon(a, b, -1/z) = (i^\epsilon e^{2\pi iab}\mu)^{-1}\left(\frac{z}{i}\right)^{\epsilon+1/2}\theta_{1/\mu}^\epsilon(-b, a, z).$$

Proposition 14.7. *Let* χ *be a primitive character. Then*

$$\theta(\chi, -1/z) = \frac{\tau(\chi)}{i^\epsilon\sqrt{m}}\left(\frac{z}{i}\right)^{\epsilon+1/2}\theta(\overline{\chi}, z),$$

where

$$\tau(\chi) = \sum_{v=0}^{m-1}\chi(v)e^{2\pi iv/m}$$

and $|\tau(\chi)| = \sqrt{m}$ *(see Neukirch or Marcus for an explicit formula).*

Proof. We have that

$$\theta(\chi, z) = \sum_{n\in\mathbb{Z}}\chi(n)n^\epsilon e^{i\pi n^2 z/m} = \sum_{a=0}^{m-1}\chi(a)\sum_{g\in m\mathbb{Z}}(a+g)^\epsilon e^{\pi i(a+g)^2 z/m} = \sum_{a=0}^{m-1}\chi(a)\theta_m^\epsilon(a, 0, z/m).$$

Making the substitution $z \mapsto -1/z$ gives the desired result. □

Theorem 14.8. *If* $\chi \neq \mathbb{1}$ *is a primitive Dirichlet character, then* $\Lambda(\chi, s)$ *has a holomorphic continuation to* $\mathbb{C}$ *and satisfies the functional equation*

$$\Lambda(\chi, s) = W(\chi)\Lambda(\overline{\chi}, 1-s),$$

where

$$W(\chi) = \frac{\tau(\chi)}{i^\epsilon\sqrt{m}}$$

for $\tau(\chi)$ *the Gauss sum. Note that* $|W(\chi)| = 1$.

Proof. We simply check that the Mellin principle applies. Note that

$$\theta(\chi, iy) = \chi(0) + O(e^{-\pi y/m}).$$

We see that $\chi(0) = 0$ when $m > 1$. The nontrivial step is studying the behavior of $\theta(\chi, i/y)$. Recall that $\mathrm{SL}_2(\mathbb{R})$ acts on the Poincaré upper half plane by $z \mapsto \frac{az+b}{cz+d}$. Given some

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

a modular form is an $f : \mathbb{H} \longrightarrow \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)f(z).$$

In particular, if we consider the function $\mathbb{H} \to \mathbb{H}$ taking $z \mapsto -1/z$ (on the imaginary axis, this is $iy \mapsto i/y$), then $f(-1/z) = if(z)$.

To apply the Mellin principle, set

$$f(y) = \frac{1}{2}\left(\frac{\pi}{m}\right)^{\epsilon/2} \theta(\chi, iy)$$

and

$$g(y) = \frac{1}{2}\left(\frac{\pi}{m}\right)^{\epsilon/2} \theta(\overline{\chi}, iy),$$

and note that this proves the theorem. □

15. Tuesday March 26

15.1. **Dedekind Zeta Function.**

Definition 15.1. Let K be a number field. The *Dedekind Zeta function* is defined as

$$\zeta_K(s) = \sum_{0 \neq I \subset O_K} \frac{1}{N(I)^s} = \sum_{0 \neq I \subset O_K} \frac{1}{|O_K/I|^s}.$$

Proposition 15.2. *We have that ζ_K is absolutely convergent and uniformly so on* $\mathrm{Re}(s) \geq 1 + \delta$. *Moreover,*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Proof due to Marcus. Let $i(n) = \#\{I \subset O_K \mid |O_K/I| = n\}$, and recall that $\varphi(n) = \sum_{k=1}^{n} i(k) = O(n^{1+\delta})$. We can write

$$\zeta_K(s) = \sum_{n \geq 1} \frac{1}{n^s} i(n) \sim \sum_{n \geq 1} \varphi(n) \left(\frac{1}{n^s} - \frac{1}{n^{s+1}}\right);$$

some more work gives the result. □

Theorem 15.3. *The Dedekind zeta function admits a meromorphic continuation to* $\mathbb{C} \setminus \{1\}$. *At 1, ζ_K has a simple pole such that*

$$\mathrm{Res}_{s=1}(\zeta_K) = \frac{2^{r_1}(2\pi)^{r_2} h_k |\mathrm{Reg}(O_K)|}{\sqrt{|\mathrm{Disc}(O_K)}\omega_K},$$

where r_1 and r_2 are the number of real and complex embeddings of K (modulo conjugacy, so that $[K : \mathbb{Q}] = r_1+2r_2$), h_K is the class number, and ω_K is the number of roots of unity in K. Recall that O_K^* maps into $\mathbb{R}^{r_1+r_2}$ via the logarithm; its image Λ, which lies in $\mathbb{R}^{r_1+r_2-1} = \{(x_1, \dots, x_k) \mid \sum_i x_i = 0\}$ is discrete and cocompact and thus a lattice. The regulator is the volume of the fundamental domain in the resulting lattice $|\mathrm{Reg}(O_K)| = \mathrm{vol}(\mathbb{R}^{r_1+r_2-1}/\Lambda)$.

Moreover, ζ_K has a functional equation relating s with $1 - s$, *which relies on integral formulas and the Mellin transform.*

More generally, let $\mathfrak{m} \subset O_K$ be an integral ideal, and let $J^{\mathfrak{m}}$ be the set of ideals of K coprime to $\mathfrak{m}$. Let $\chi : J^{\mathfrak{m}} \to S^1$ be a character and associate to χ the Dirichlet L-series

$$L(\chi, s) = \sum_{0 \neq I \subset O_K} \frac{\chi(I)}{N(I)^s}$$

(if $(I, \mathfrak{m}) > 1$, then we set $\chi(I) = 0$).

Question 15.4. (Hecke) When does $L(\chi, s)$ have an analytic continuation and functional equation?

Definition 15.5. A *Größencharakter* modulo $\mathfrak{m}$ is a character $\chi : J^{\mathfrak{m}} \longrightarrow S^1$ such that there exist $\chi_f : (O_K/\mathfrak{m})^* \longrightarrow S^1$ and $\chi_\infty : K_{\mathbb{R}}^* \longrightarrow S^1$, where

$$K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{\tau} K_\tau = \mathbb{R}^{r_1} \times \mathbb{C}^{r_s},$$

such that $\chi((a)) = \chi_f(a)\chi_\infty(a)$ for all $a \in O_K$ with $(a, \mathfrak{m}) = 1$.

15.2. **Idèles and Characters.**

Definition 15.6. A *Hecke character* is a character of $C_K = I/K$, where I is the group of idèles of K. In other words, it is a continuous homomorphism $\chi : I \longrightarrow S^1$ taking $K \subset I \mapsto 1$. Equivalently, χ is a continuous homomorphism $\chi : C_K \longrightarrow S^1$.

Let $\mathfrak{m} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{n_\mathfrak{p}}$, where $n_\mathfrak{p} \geq 0$ and $n_\mathfrak{p} = 0$ for $\mathfrak{p}|\infty$. Let $\overline{I}^{\mathfrak{m}} = I_f^{\mathfrak{m}} \times I_\infty$ where $I_f^{\mathfrak{m}} = \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}^{(n_\mathfrak{p})}$ and $I_\infty = \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^* = K_{\mathbb{R}}^*$. We call $\mathfrak{m}$ a *module of definition* of χ if $\chi(I_f^{\mathfrak{m}}) = 1$.

Lemma 15.7. *Every Hecke character admits a module of definition.*

Proof. Restrict χ to $\prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}$, which, recall, is compact and totally disconnected. We see that its image in S^1 is compact and totally disconnected and therefore finite. Thus, $\ker(\chi) \subset \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}^{(n_\mathfrak{p})}$ where $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$, and we may take $\mathfrak{m} = \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}^{(n_\mathfrak{p})}$ as our module of definition. □

Hence, $\chi : C_K = I/K^* \longrightarrow S^1$ has $\chi(I_f^{\mathfrak{m}}) = 1$, which descends to $\chi : C(\mathfrak{m}) = I/I_f^{\mathfrak{m}}K^* \longrightarrow S^1$. We construct a Großencharakter mod $\mathfrak{m}$. For every $\mathfrak{p} \nmid \infty$, let $\pi_\mathfrak{p}$ be a uniformizer of $K_\mathfrak{p}$. Let $c : J^{\mathfrak{m}} \longrightarrow C(\mathfrak{m})$ take $\mathfrak{p} \mapsto \langle \pi_\mathfrak{p} \rangle = (1, \ldots, 1, \pi_\mathfrak{p}, 1, \ldots)$. Note that because $I_f^{\mathfrak{m}}$ contains the group of units for all $\mathfrak{p} \nmid \mathfrak{m}$, we have that c is independent from the choice of $\pi_\mathfrak{p}$.

Theorem 15.8. *The composition $\chi \circ c : J^{\mathfrak{m}} \longrightarrow C(\mathfrak{m}) \longrightarrow S^1$ yields a one-to-one correspondence between Hecke characters modulo $\mathfrak{m}$ and Größencharakters modulo $\mathfrak{m}$.*

Proof. We rely on the following exact sequence

$$1 \longrightarrow K^{(\mathfrak{m})}/O^{\mathfrak{m}} \to J^{\mathfrak{m}} \times (O/\mathfrak{m})^* \times K_{\mathbb{R}}^*/O^{\mathfrak{m}} \xrightarrow{f} C(\mathfrak{m}) \longrightarrow 1,$$

where $O^{\mathfrak{m}} = \{a \in O^* \mid a \equiv 1 \mod \mathfrak{m}\}$, $K^{(\mathfrak{m})} = \{c/d \mid c \equiv d \mod \mathfrak{m}\}$, and the map $K^{(\mathfrak{m})}/O^{\mathfrak{m}} \to J^{\mathfrak{m}} \times (O/\mathfrak{m})^* \times K_{\mathbb{R}}^*/O^{\mathfrak{m}}$ is given by

$$a \mapsto ((a)^{-1}, a \mod \mathfrak{m}, a \mod O^{\mathfrak{m}}).$$

To see exactness in the middle, suppose that $(I, b, c) \mapsto bcI = 1$. It suffices to show that I is principal.

Given a Hecke character $\chi : C(\mathfrak{m}) \to S^1$, we have $\chi \circ f : J^{\mathfrak{m}} \times (O/\mathfrak{m})^* \times K_{\mathbb{R}}^*/O^{\mathfrak{m}} \to S^1$ is a character vanishing on $K^{(\mathfrak{m})}/O^{\mathfrak{m}}$. If the components of these characters are $\chi' : J^{\mathfrak{m}} \to S^1$, $\chi_f : (O/\mathfrak{m})^* \to S^1$, and $\chi_\infty : K_{\mathfrak{m}}^*/O^{\mathfrak{m}} \to S^1$, then $\chi'((a)^{-1})\chi_f(a)\chi_\infty(a) = 1$ if and only if $chi'((a)) = \chi_f(a)\chi_\infty(a)$. Hence, χ' is a Größencharakter modulo $\mathfrak{m}$.

For the other direction, $\chi : J^{\mathfrak{m}} \longrightarrow S^1$ can be written as the product of $\chi_\infty : (O/\mathfrak{m})^* \longrightarrow S^1$ and $\chi_f : K_{\mathbb{R}}^*/C^{\mathfrak{m}} \longrightarrow S^1$. Then we have a map $(\chi, \chi_\infty, \chi_f) : J^{\mathfrak{m}} \times (O/\mathfrak{m})^* \times K_{\mathbb{R}}^*/O^{\mathfrak{m}} \longrightarrow S^1$; this gives us our desired Hecke character. □

Theorem 15.9. *If χ is a Hecke character, then $L(\chi, s)$ admits a meromorphic continuation to $\mathbb{C}$ with a functional equation.*

16. Thursday March 28

The following presentation of Hecke's approach to proving the functional equation for the Dedekind zeta function is adapted from Neukirch.

For K a number field and $\zeta_K(s)$ the corresponding Dedekind zeta function, we can consider $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, which can be written as $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where r_1 and r_2 give the number of real and complex embeddings of K, respectively. This further maps into $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}^{r_1} \times (\mathbb{C}^2)^{r_2}$, where $\mathbb{R} \hookrightarrow \mathbb{C}$ in the usual way and $\mathbb{C} \to \mathbb{C}^2$ by $z \mapsto (z, \overline{z})$. The maps

$$K \longrightarrow K_{\mathbb{R}} \longrightarrow K_{\mathbb{C}}$$

restrict to give maps

$$\mathcal{O}_K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{C}^{r_1} \times (\mathbb{C}^2)^{r_2},$$

where recall that the image of $\mathcal{O}_K$ is discrete and cocompact (and hence a lattice).

Let X be a finite set with an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (eventually we will set $X = \mathrm{Hom}(K, \mathbb{C})$). Write $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, i\}$, where $i(z) = \overline{z}$. Let $n = \#X$ (in our example, $n = r_1 + 2r_2$). Let

$$\mathcal{C} = \prod_{\tau \in Z} \mathbb{C}_\tau = \{z = (z_\tau)_{\tau \in X} \mid z_\tau \in \mathbb{C}\},$$

where each $\mathbb{C}_\tau \simeq \mathbb{C}$. Note that $\mathcal{C} = \mathbb{C}^{r_1} \times (\mathbb{C}^2)^{r_2}$ and that an arbitrary element of this space can be written as $z = (z)_{r_1} \times (z_1, z_2)_{r_2}$. There is a conjugation action (i.e., action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$) on $\mathcal{C}$ given by $\overline{z} = (\overline{z})_{r_1} \times (\overline{z_1}, \overline{z_2})_{r_2}$. For $z \in \mathcal{C}$, we define

$$\overline{z} = (\overline{z}_{\overline{\tau}}),$$
$$z^* = (z_{\overline{\tau}}),$$
$${}^*z = (\overline{z}_\tau).$$

Note that $\overline{z} = {}^*z^*$. Let

$$\mathcal{R} = \left[\prod_\tau \mathbb{C}_\tau\right]^\dagger = \{z \in \mathcal{C} \mid z = \overline{z}\}.$$

It is straightforward to check that an element in this space is of the form $(z)_{r_1} \times (z_1, z_2)_{r_2}$, where $z \in \mathbb{R}$ and $z_1 = \overline{z_2}$, so $\mathcal{R} = K_{\mathbb{R}}$ is a Minkowski space. We define trace $\mathrm{tr} : \mathcal{C} \to \mathbb{C}$ and norm $N : \mathcal{C} \to \mathbb{C}$ maps $(z_\tau) \mapsto \sum_\tau z_\tau$ and $(z_\tau) \mapsto \prod_\tau z_\tau$, respectively. There is also a Hermitian product on $\mathcal{C}$ given by

$$\langle x, y\rangle = \sum_\tau x_\tau \overline{y_\tau} = \mathrm{tr}(x\,{}^*y);$$

this restricts to a scalar product on $\mathcal{R}$. We remark that $\langle xz, y\rangle = \langle x, {}^*zy\rangle$ for $z \in \mathcal{C}$. Define $\mathcal{R}_\pm = \{x \in \mathcal{R} \mid x = x^*\} = \mathbb{R}^{r_1} \times (\Delta_{\mathbb{R}})^{r_2}$, where $\Delta_{\mathbb{R}}$ is the diagonal embedding of $\mathbb{R}$ into $\mathbb{C}^2$. Finally, define $\mathcal{R}_+ = \{x \in \mathcal{R}_\pm \mid x_\tau > 0\}$. Let $|\cdot| : \mathcal{R}^* \to \mathcal{R}_+^*$ be given by $x = (x_\tau) \mapsto |x| = (|x_\tau|)$. We also have a map $\log : \mathbb{R}^* \to \mathbb{R}_\pm$ given by $x = (x_\tau) \mapsto \log(x) = (\log(x_\tau))$.

We also have a notion of Poincaré Half Space $\mathcal{H} = \mathbb{R}_\pm + i\mathbb{R}_+^* = \mathbb{H}^{r_1} \times (\Delta_{\mathbb{H}})^{r_2}$. Let $\mathrm{Re}(z) = (z + \overline{z})/2$ and $\mathrm{Im}(z) = (z - \overline{z})/(2i)$. Let $\mathcal{H} = \{z \in \mathcal{C} \mid z = z^*, \mathrm{Im}(z) > 0\}$. As an exercise, prove that $z \in \mathcal{H}$ if and only if $-1/z \in \mathcal{H}$. If $z = (z_\tau)$, $\rho = (\rho_\tau)$ with $\rho_\tau \in \mathbb{C}$, then

$$z^\rho = (z_\tau^{\rho_\tau}) = (e^{\rho_\tau \log z_\tau}),$$

where we take the usual branch of the logarithm $\log : \mathbb{C} \setminus \mathbb{R} \to \mathbb{C}$ with $\log(1) = 0$.

In a sense, most integral formulas rely on the Poisson summation formula. Let $f : \mathbb{R}^n \to \mathbb{C}$ a Schwarz function (recall that the space of Schwarz functions $\mathcal{S}(\mathbb{R}^n)$ is the set of f such that

$\sum_{x\in\mathbb{R}^n} |P(x)\frac{\partial^\alpha f}{\partial x^\alpha}| < \infty$ for all $\alpha = (\alpha_1, \dots, \alpha_n)$ and all polynomials P). The Fourier transform of f is given by

$$\widehat{f}(y) = \int_{\mathbb{R}^n} f(x)e^{-2\pi i\langle x,y\rangle}dx,$$

and $\widehat{f} \in \mathcal{S}(\mathbb{R}^n)$. The usual example is $h(x) = e^{-\pi\langle x,x\rangle}$; here $h = \widehat{h}$. For $A : \mathbb{R}^n \to \mathbb{R}^n$ linear and invertible, we can set $f_A(x) = f(Ax)$; here

$$\widehat{f_A}(x) = \frac{1}{\det(A)}\widehat{f}((A^t)^{-1}x).$$

Let $\Gamma \subset \mathbb{R}^n$ be a lattive (i.e., a discrete abelian subgroup that is cocompact; equivalently, $\Gamma \simeq \mathbb{Z}^n$ and $\mathbb{R}^n = \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$). Optionally, we can also require the inner product on $\mathbb{R}^n$ to restrict to a $\mathbb{Z}$-valued pairing on $\Gamma \times \Gamma$.

Theorem 16.1 (Poisson formula). *For $f \in \mathcal{S}(\mathbb{R}^n)$, we have*

$$\sum_{\lambda\in\Gamma} f(\lambda) = \frac{1}{|\mathrm{vol}(\Gamma)|}\sum_{\lambda\in\Gamma^\vee}\widehat{f}(\lambda)$$

where $\Gamma^\vee = \{y \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z} \text{ for all } x \in \Gamma\}$ is the dual lattice.

Proof. Identify $\Gamma = \mathbb{Z}^n$ and let

$$g(x) = \sum_{\lambda\in\mathbb{Z}^n} f(\lambda + x).$$

Note that g is $\mathbb{Z}^n$-periodic; moreover, g is the sum of its Fourier series. Precisely, we have, for $n = 1$,

$$g(x) = \sum_{n\in\mathbb{Z}} \widehat{g}(n)e^{2\pi inx},$$

where

$$\widehat{g}(n) = \int_0^1 g(x)e^{-2\pi inx}dx.$$

For arbitrary n, this becomes

$$g(x) = \sum_{\lambda\in\mathbb{Z}^n} \widehat{g}(y)e^{2\pi i\langle\lambda,x\rangle},$$

where

$$\widehat{g}(\lambda) = \int_{(\mathbb{R}^n/\Lambda)} g(y)e^{-2\pi i\langle\lambda,y\rangle}dy.$$

We may rewrite the above as

$$\widehat{g}(y) = \sum_{\beta\in\mathbb{Z}^n}\int_{\mathbb{R}^n/\Lambda} f(\beta + y)e^{-2\pi i\langle\lambda,y\rangle}dy = \sum_{\beta\in\mathbb{Z}^n}\int_{\lambda+\mathbb{R}^n/\Lambda} f(y)e^{-2\pi i\langle\lambda,y\rangle}e^{2\pi i\langle\lambda,\beta\rangle}dy.$$

Since $\langle\lambda, \beta\rangle \in \mathbb{Z}$, the above simplifies to

$$\int_{\mathbb{R}^n} f(y)e^{-2\pi i\langle\lambda,y\rangle}dy = \widehat{f}(\lambda);$$

we may conclude the theorem (at least in the case $\Lambda = \mathbb{Z}^n$). □

Let $\Gamma \subset \mathcal{R} = K_{\mathbb{R}}$ be a lattice. We can define the theta function

$$\Theta_\Gamma(z) = \sum_{\lambda \in \Gamma} e^{i\pi\langle \lambda z, \lambda \rangle},$$

where $z \in \mathcal{H}$. More generally, for $a, b \in \mathcal{R}$ and $p \in \prod_\tau \mathbb{Z}$, we can define

$$\Theta_\Gamma^p(a, b, z) = \sum_{\lambda \in \Gamma} N((a+\lambda)^p) e^{i\pi\langle (a+\lambda)z, a+\lambda \rangle + 2\pi i \langle b, \lambda \rangle}.$$

Let $f_p(a, b, x) = N((x+a)^p) e^{-\pi\langle a+x, a+x \rangle + 2\pi i \langle b, x \rangle}$ for $a, b \in \mathcal{R}$ and p admissible. In other words, $p_\tau \in \{0, 1\}$ if $\tau = \overline{\tau}$ and $p_\tau p_{\overline{\tau}} = 0$ if $\tau \neq \overline{\tau}$.

Proposition 16.2. *With notation as above, we have $f_p \in \mathcal{S}(\mathcal{R})$ and*

$$\widehat{f}(y) = \left[i^{\mathrm{tr}(p)} e^{2\pi i \langle a, b \rangle} \right]^{-1} f_p(-b, a, y).$$

Theorem 16.3. *With notation as above, we have that $\Theta^p(a, b, z)$ converges absolutely and uniformly on compact subsets of $\mathcal{R} \times \mathcal{R} \times \mathcal{H}$.*

Moreover,

$$\Theta_\Gamma(-1/z) = \frac{\sqrt{N(z/i)}}{\mathrm{vol}(\Gamma)} \Theta_{\Gamma'}(z).$$

Proof. Apply Poisson summation to $f_0(0, 0)$. □

16.1. **Gamma Factors.** Let

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}$$

for $s \in \mathbb{C}$ and $\mathrm{Re}(s) > 0$. In general,

$$\mathcal{R}_+^* = (\mathbb{R}_+^*)^{r_1} \times (\Delta_{\mathbb{R}_+^*})^{r_2},$$

which is contained in $(\mathbb{R}_+^*)^{r_1} \times (\mathbb{R}_+^*)^{r_2}$ by the map $(y, y) \mapsto y^2$. Since R_+^* is endowed with a Haar measure, we can pull back the product Haar measure to $\mathcal{R}_+^*$, which we denote using $\frac{dy}{y} = \prod_{(r_1, r_2)} \frac{dt}{t}$.

Definition 16.4. For $s = (s_t) \in C$ with $\mathrm{Re}(s_\tau) > 0$, define

$$\Gamma_X(s) = \int_{\mathcal{R}_+^*} N(e^{-y} y^s) \frac{dy}{y} = \prod_{r_1} \Gamma(s_\rho) \times \prod_{r_2} 2^{1 - s_p + s_{\overline{p}}} \Gamma(s_p + s_{\overline{p}}),$$

where $\rho = \{\tau, \overline{\tau}\}$.

17. Tuesday April 2

Let K be a number field. Rewrite the Dedekind zeta function as

$$\zeta_K(s) = \sum_{0 \neq I \subset O_K} \frac{1}{N(I)^s} = \sum_{b \in \mathrm{Cl}(K)} \sum_{\substack{I \subset O_K \\ [I] = b}} \frac{1}{N(I)^s}$$

for $\mathrm{Re}(s) > 1$. We introduce, for each $b \in \mathrm{Cl}(K)$,

$$\zeta_K(b, s) = \sum_{\substack{I \subset O_K \\ [I] = b}} \frac{1}{N(I)^s},$$

and note that $\sum_K(s) = \sum_{b \in \mathrm{Cl}(K)} \zeta_K(b, s)$.

Lemma 17.1. *Let $a \subset \mathcal{O}_K$ be an integral ideal such that $[a^{-1}] = b$. Then $\{I \subset \mathcal{O}_K \mid [I] = b\}$ is in bijection with $a^*/\mathcal{O}_K^*$, where $a^* = a \setminus \{0\}$ and $\mathcal{O}_K^*$ is the group of units of $\mathcal{O}_K^*$.*

Proof. If $[I] = b = [a^{-1}]$, then $aI = (\alpha) \subset a$, implying that $\alpha \in a \setminus \{0\}$ and $I = \alpha a^{-1}$. Since $I = \alpha' a^{-1}$, it follows that $\alpha\alpha' \in a^*/\mathcal{O}_K^*$. The other direction is similarly straightforward as is left as an exercise for the reader. □

Using this lemma, we may write

$$\zeta_K(b,s) = \sum_{\alpha \in a^*/\mathcal{O}^*} \frac{1}{N(\alpha a^{-1})^s} = N(a)^s \sum_{\alpha \in a^*/\mathcal{O}_K^*} \frac{1}{|N(\alpha)|^s}.$$

We have $\mathcal{O}_K \hookrightarrow K_\mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathcal{R}$; the image of $\mathcal{O}_K$ under this embedding is a lattice, since it is discrete and cocompact. Similarly, the image of $a \subset \mathcal{O}_K$ in $\mathcal{R}$ is a lattice. We would like to determine $\operatorname{vol}(\mathcal{R}/\mathcal{O}_K) = \operatorname{vol}(\mathcal{O}_K)$ and $\operatorname{vol}(\mathcal{R}/a) = \operatorname{vol}(a)$. Since $\operatorname{vol}(\mathcal{O}_K)$ is the determinant of the images of a $\mathbb{Z}$-basis for $\mathcal{O}_K$ in $\mathcal{R}$, we see that $\operatorname{vol}(\mathcal{O}_K) = |\operatorname{Disc}(\mathcal{O}_K)| = d_K$. Moreover, since $a \subset \mathcal{O}_K$, we have that $\operatorname{vol}(\mathcal{R}/a) = \operatorname{vol}(a) = N(a)^2 d_K = d_a$. Consider the Theta series

$$\Theta(a,z) = \Theta_a(z/d_a^{1/n}) = \sum_{x \in a} e^{\pi i \langle 2z/d_a^{1/n}, x\rangle}.$$

Recall that

$$\Gamma_K(s) = \int_{\mathcal{R}_+^*} N(e^{-y}y^s)\frac{dy}{y}.$$

For each $x \in a \subset \mathcal{O}_K$, we have

$$|d_K|^s \pi^{-ns}\Gamma_K(s)\frac{N(a)^{2s}}{N(x)^{2s}} = \int_{\mathcal{R}_+^*} e^{-\pi\langle xy/d_a^{1/n}, x\rangle} N(y)^s \frac{dy}{y}$$

by making the change of variables $y \mapsto \pi|x|^2 y/d_a^{1/n}$. Summing over $x \in a$, we obtain

$$|d_K|\pi^{-ns}\Gamma_K(s)\zeta_K(b,2s) = \int_{\mathcal{R}_+^*} g(y)N(y)^s\frac{dy}{y},$$

where

$$g(y) = \sum_{x \in a^*/\mathcal{O}^*} e^{-\pi\langle xy/d_a^{1/n}, x\rangle}.$$

Let $Z_\infty(s) = |d_K|^{s/2}\pi^{-ns/2}\Gamma_K(s/2)$ be the Euler factor at infinity, and let

$$Z(b,x) = Z_\infty(s)\zeta_K(b,s).$$

Then

$$Z(b,2s) = \int_{\mathcal{R}_+^*} g(y)N(y)^s\frac{dy}{y}.$$

This is almost what we need to apply the Mellin transform; the only issue is that g is a sum only over $a^*/\mathcal{O}^*$. Note that $\mathcal{O}_K^* \subset \mathcal{R}^* \subset \mathcal{R}_+^*$ is sent to the norm-1 hypersurface $S = \{x \in \mathcal{R}_+^* \mid N(x) = 1\}$. Composing with log embeds $\mathcal{O}_K^*$ as a hyperplane in $\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$. Every $y \in \mathcal{R}_+^*$ can be written as $y = xt^{1/n}$, where $t = N(y)$ and $n \in S$. Then $\mathcal{R}_+^* = S \times \mathbb{R}_+^*$, which induces a Haar measure on $\mathcal{R}_+^*$ $dy/y = d^*x \times dt/t$, where d^*x is the Haar measure on S that makes the equality valid. Choose F a fundamental domain for the action of $|\mathcal{O}_K^*|^2$ in the following

$$\log : \mathcal{R}_+^* \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2},$$

under which S is mapped to a hyperplane $H = \{\sum_i x_i = 0\}$. A theorem of Dirichlet tells us that $\log(|\mathcal{O}_K^*|)$ is a lattice in H, and we see that F is the preimage of 2 times the fundamental domain for $\log(|\mathcal{O}_K^*|)$ in H.

Proposition 17.2. *With notation as above,*

$$Z(b, 2s) = L(f, s)$$

and

$$f(t) = f_F(a, t) = \frac{1}{\#\mu(K)} \int_F \Theta(a, ixt^{1/n}) d^*x,$$

where $\mu(K)$ is the roots of unity in $\mathcal{O}_K$.

Proof. Decompose $\mathcal{R}_+^* = S \times \mathbb{R}_*^+$ and write

$$Z(b, 2s) = \int_{S \times \mathbb{R}_*^+} g(y) N(y)^s d^*x \frac{dt}{t} = \int_0^\infty \left(\int_S \sum_{v \in a^*/\mathcal{O}^*} e^{-\pi \langle vy/d_a^{1/n}, v \rangle} d^*x \right) t^s \frac{dt}{t}.$$

Writing

$$\int_S \sum_{v \in a^*/\mathcal{O}^*} e^{-\pi \langle vy/d_a^{1/n}, v \rangle} d^*x = \frac{1}{\#\mu(K)} \int_F \sum_{\epsilon \in \mathcal{O}_K^*} \sum_{v \in a^*/\mathcal{O}^*} e^{-\pi \langle v \epsilon x (t/d_a)^{1/n}, v\epsilon \rangle} = \frac{1}{\#\mu(K)} \int_F \sum_{v \in a^*} e^{-\pi \langle vs(t/d_a)^{1/n}, v \rangle} d^*x,$$

we see that this is

$$\frac{1}{\#\mu(K)} \int_F \Theta(a, ixt^{1/n}) - 1 d^*x = f(t) - f(\infty,$$

as desired. □

What's left? We still need to show that

$$\mathrm{vol}(F) = 2^{r-1} \mathrm{Reg}(\mathcal{O}_K),$$

where recall that the regulator is the volume of $|\mathcal{O}_K^*|$ in $\mathbb{R}^{r_1 + r_2 - 1}$. We also need to show that

$$f_F(a, 1/t) = t^{1/2} f_{F^{-1}}((a\mathcal{D})^{-1}, t),$$

where $\mathcal{D}$ is the different ideal $\mathcal{D} = \{x \in K \mid \mathrm{tr}(xy) \in \mathbb{Z}, y \in \mathcal{O}_K\}$ and $|\mathcal{D}^{-1}/\mathcal{O}| = |\mathrm{Disc}(\mathcal{O}_K)|$. This allows us to apply the Mellin principle.

Theorem 17.3. *With notation as above, $Z(b, s)$ admits an analytic continuation to $\mathbb{C} \setminus \{0, 1\}$ with functional equation $Z(b, s) = Z(b', 1 - s)$, where $bb' = \mathrm{Diff}(\mathcal{O}_K)$. The function has simple poles at $s = 0$ and $s = 1$ with residues $2^r R/\#\mu(K)$.*

18. Thursday April 4

18.1. **Tate's Thesis.** A good reference for the following is the paper *Théorie de la dualité et analyse harmonique* by Canton–Godement (1947). The first input is the local theory. Let K be the completion of a number field at a prime so that K is either $\mathbb{R}$ or $\mathbb{C}$ in the archimedean case or K is a finite extension of $\mathbb{Q}_p$ (i.e., a local field of characteristic 0) in the nonarchimedean case. Recall that in the nonarchimedean case, K has finite residue field. In this case, we write $\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}$, which has maximal ideal $\mathfrak{p} = \{x \in K \mid v(x) > 1\}$. For $\alpha \in K$, let

$$|\alpha| = \begin{cases} |\alpha| & \text{if } \alpha \in \mathbb{R}; \\ |\alpha\overline{\alpha}| & \text{if } \alpha \in \mathbb{C}; \\ N(\mathfrak{p})^{-v(\alpha)} = |\mathcal{O}/\mathfrak{p}|^{-v(\alpha)} & \text{if } K \text{ is local.} \end{cases}$$

Note that K is a locally compact abelian group; as is K^*.

Next we study additive characters of $K = (K, +)$, i.e., continuous $\chi : K \longrightarrow S^1$ with $\chi(x + y) = \chi(x)\chi(y)$.

Lemma 18.1. *Let χ be a nontrivial character of K taking $\zeta \mapsto \chi(\zeta)$. Then, for each $\eta \in K$, the map χ_η taking $\zeta \mapsto \chi(\eta\zeta)$ is also a character, and the map $\varphi : K \longrightarrow \operatorname{Hom}(K, S^1) = K^\vee$ taking $\eta \mapsto \chi_\eta$ is an isomorphism.*

Proof. It is straightforward to verify that χ_η is clearly a character. To see injectivity, note that $\chi_\eta = 0$ implies that $\chi(\eta\zeta) = 0$ for all $\zeta \in K$. Hence, $\chi(\eta\zeta) = 0$ for all $\zeta \in K$, which forces $\eta = 0$.

Next, we would like to prove that $\operatorname{im}(\varphi)$ is dense in $K^\vee$. This relies on the fact that $(K^\vee)^\vee \simeq K$, since K is a locally compact abelian group. If $\operatorname{im}(\varphi)$ is contained in some closed subgroup $A \subset K^\vee$, then there exists nontrivial $f : K^\vee/A \longrightarrow S^1$, where f takes $\chi \mapsto \chi(\alpha)$ for some nonzero $\alpha \in K$. Since $f|_A = 1$, we have that $\chi(\eta\alpha) = 0$ for all $\eta \in K$, which forces $\alpha = 0$.

The rest is left to the reader. □

We need to fix a special nontrivial character of K to complete the identification $K \simeq K^\vee$. For $p > 0$ prime, let $\lambda : \mathbb{Q}_p \longrightarrow \mathbb{R}/\mathbb{Z}$ be the principal part of x, i.e., the $\lambda(x) \in \mathbb{Q}$ such that $x - \lambda(x) \in \mathbb{Z}_p$. We remark that $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Since $\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{R}/\mathbb{Z}[p^n]$, there is a natural containment $\mathbb{Q}_p/\mathbb{Z}_p \subset \mathbb{R}/\mathbb{Z}$; λ factors through $\mathbb{Q}_p/\mathbb{Z}_p$ (note that λ is just the natural quotient map $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$). For $\mathbb{R}$, let $\lambda : \mathbb{R} \longrightarrow \mathbb{R}/\mathbb{Z}$ be given by $x \mapsto -x \bmod 1$. For $\mathbb{C}$, we have $[\mathbb{C} : \mathbb{R}] = 2$; let $\Lambda(\zeta) = \lambda(\alpha + \overline{\alpha})$.

If $[K : \mathbb{Q}_p] < \infty$, then let

$$\Lambda(\zeta) = \lambda(\operatorname{tr}_{K/\mathbb{Q}_p}(\zeta)).$$

Then the character $K \longrightarrow S^1$ taking $\zeta \mapsto e^{2\pi i\Lambda(\zeta)}$ is a nontrivial additive character.

Theorem 18.2. *We have that $K \simeq K^\vee$ via*

$$\zeta \mapsto \left(\eta \mapsto e^{2\pi i n(\eta\zeta)}\right).$$

Definition 18.3. The *different* of K (nonarchimedean) is the ideal $\mathcal{D}_K$ of $\mathcal{O}_K$ such that $\mathcal{D}_K^{-1} = \{x \in K \mid \operatorname{tr}_{K/\mathbb{Q}_p}(xy) \in \mathbb{Z}_p \text{ for all } y \in \mathcal{O}_K\}$.

Then we see that $\eta \mapsto e^{2\pi i n(\zeta\zeta)}$ is trivial on $\mathcal{O}_K$ if and only if $\zeta \in \mathcal{D}_K^{-1}$. Let μ be a Haar measure on $(K, +)$. For K a locally compact abelian group, we have the following theorem).

Theorem 18.4 (Bourbaki, Topology 3; Folland Abstract Harmonic Analysis)**.** *For K a locally compact group, there exists a unique measure, up to scalar multiplication, such that the following hold.*

(1) *$\mu(T) < \infty$ for T compact;*

(2) *for $x \in K$ and $U \subset K$ measurable, we have $\mu(xU) = \mu(U)$ (i.e., μ is left-translation invariant; similarly, there exists a right Haar measure as well).*

Lemma 18.5. *For every nonzero $\alpha \in K$ and every measurable U, define $\mu_\alpha(U) = \mu(\alpha U)$. Then there exists $\varphi : K^* \longrightarrow \mathbb{R}_+^*$ such that $\mu_\alpha = \varphi(\alpha)\mu$. In fact, $\varphi(\alpha) = |\alpha|$.*

Proof. We see that μ_α is also a Haar measure. By the uniqueness of the Haar measure, we must have $\mu_\alpha = \varphi(\alpha)\mu$. If $K = \mathbb{R}$ or $\mathbb{C}$, then we may use the usual formula for the Lebesgue measure. For a p-adic field K, let π be a uniformizer. Then $\alpha = \pi^n u$ for a unit $u \in \mathcal{O}_K^*$. For simplicity, suppose $n \geq$, and note that $\alpha \mathcal{O}_K = \pi^n \mathcal{O}_K \subset \mathcal{O}_K$. Note that $|\mathcal{O}_K/\pi^n\mathcal{O}_K| = |\mathcal{O}_K/\pi\mathcal{O}_K|^n$, so $\mathcal{O}_K = \sqcup_{i\in I}(\pi^n\mathcal{O}_K + v_i)$, where $|I| = |\mathcal{O}_K/\pi\mathcal{O}_K|^n$. Thus, we see that

$$\mu(\mathcal{O}_K) = |\mathcal{O}_K/\pi\mathcal{O}_K|^n \mu(\pi^n\mathcal{O}_K);$$

therefore, $\mu(\alpha\mathcal{O}_K) = |\alpha|\mu(\mathcal{O}_K)$. □

If $f \in L^1(K)$, then

$$\int f(\zeta)d\mu(\zeta) = |\alpha| \int f(\alpha\zeta)d\mu(\zeta).$$

In condensed form, $d\mu(\alpha\zeta) = |\alpha|d\mu(\zeta)$. We pin down unique choices of Haar measures in the following way: $d\zeta$ is just the ordinary Lebesgue measure on $K = \mathbb{R}$, so this is just the Haar measure with $\mu([0,1]) = 1$. If $K = \mathbb{C}$, then $d\zeta$ is twice the usual Lebesgue measure on $\mathbb{C}$, so $\mu([0,1]^2) = 2$. If $K/\mathbb{Q}_p$ is p-adic and $[K : \mathbb{Q}_p] < \infty$, then $d\zeta$ is the unique Haar measure such that $\mu(\mathcal{O}_K) = (N(\mathcal{D}_K))^{-1/2}$.

Theorem 18.6. *The Fourier transform of $f \in L^1(K)$ is*

$$\widehat{f}(\eta) = \int f(\zeta)e^{-2\pi i\Lambda(\eta\zeta)}d\zeta.$$

Moreover, if f is continuous and $\hat{f} \in L^1(K)$, then

$$f(\zeta) = \int \hat{f}(\eta)e^{2\pi i\Lambda(\zeta\eta)}d\eta = \hat{\hat{f}}(-\zeta).$$

18.2. **Multiplicative characters.** There is an obvious character $v : K^* \longrightarrow \mathbb{R}_+^*$ taking $\alpha \mapsto |\alpha|$. Note that $U = \ker(v)$ is a compact subgroup of K^*. More generally, we are interested in continuous group homomorphisms $c : K^* \longrightarrow C^*$. These are called *quasi-characters*.

Definition 18.7. We say that c is unramified if $c|_U = 1$.

Lemma 18.8. *The unramified quasi-characters are exactly the maps of the form $c(\alpha) = |\alpha|^s$ for $s \in \mathbb{C}$. (If K is archimedean, then s is unique; if K is nonarchimedean, then s is determined up to $2\pi i/q$.)*

Proof. If K is $\mathbb{R}$ or $\mathbb{C}$, then $c : K^* \longrightarrow C^*$ is equivalent to a map $c : \mathbb{R}_+^* \longrightarrow \mathbb{C}^*$, since $K = U \times \mathbb{R}_+^*$. Using exp, we can lift to the universal cover and get a diagram

$$\begin{tikzcd}
\mathbb{R} \arrow[r] \arrow[d, "\exp"] & \mathbb{C} \arrow[d, "\exp"] \\
\mathbb{R} \arrow[r] & \mathbb{C}.
\end{tikzcd}$$

This diagram gives us the result.

For K a p-adic field, $K^* = U \times \pi^{\mathbb{Z}}$, so $c : \pi^{\mathbb{Z}} \longrightarrow \mathbb{C}^*$. Let β be the image of π; note that $\pi^n = \beta^n$ □

19. Tuesday April 9

We continue our discussion of unramified quasi-characters.

Theorem 19.1. *The quasi-characters of K^* are of the form $\alpha \mapsto c(\alpha) = \tilde{c}(\tilde{\alpha})|\alpha|^s$, where $\alpha = \tilde{\alpha}\rho$, $\tilde{\alpha} \in U$, and $\tilde{U} = \{\alpha \mid |\alpha| = 1\} \longrightarrow S^1$ is a character.*

We determine U for each possible K. If $K = \mathbb{R}$, then $U = \{\pm 1\}$ and $\tilde{c} : U \longrightarrow S^1$ takes $\alpha \mapsto 1$ or $\alpha \mapsto \alpha$. If $K = \mathbb{C}$, then $U = S^1$, and $\tilde{c} : U \longrightarrow S^1$ takes $\alpha \mapsto \alpha^n$ for some $n \in \mathbb{Z}$ by elementary Fourier analysis. If K is some p-adic field, then let O_K be the ring of integers and $\mathfrak{p} \subset O_K$ the maximal ideal. We have $U = O_K^*$, and $1 + \mathfrak{p}^\nu$ for $\nu > 0$ form a system of neighborhoods of 1. For $\tilde{c} : U \longrightarrow S^1$ a continuous character, then $\tilde{c}(1 + \mathfrak{p}^n) = 1$ for n sufficiently large. Choose n minimally such that $\tilde{c}(1 + \mathfrak{p}^n) = 1$ and $\tilde{c}(1 + \mathfrak{p}^{n-1}) \neq 1$. Then $f = \mathfrak{p}^n$ is called the conductor of $\tilde{c}$, and thus $\tilde{c}$ descends to $\tilde{c} : U/(1 + f) \longrightarrow S^1$, where $U/(1 + f)$ is a finite abelian group. Recall that $U = O_K^* = (1 + \mathfrak{p}) \times \mathbb{F}_q^*$ and that $1 + \mathfrak{p}^n/(1 + \mathfrak{p}^{n+1}) \simeq \mathbb{F}_q$. For a quasi-character $c : K^* \longrightarrow C^*$, we define the *exponent* of c to be $\sigma = \mathrm{Re}(s)$, where $|c(\alpha)| = |\alpha|^\sigma$ and $c = \tilde{c}(-)| - |^s$ for $s \in \mathbb{C}$ or $s \in \mathbb{C}/2\pi i/q\mathbb{Z}$. Note that c is a character if and only if $\sigma = 0$.

Now, we would like a Haar measure on K^*. We have a Haar measure $d\xi$ on K; changing variables gives us $d(\alpha\xi) = |\alpha| d\xi$. For $\alpha \in k^*$, we define $d^*\alpha = d\alpha/|\alpha|$. Since

$$d^*(\beta\alpha) = \frac{d(\beta\alpha)}{|\beta\alpha|} = d^*\alpha,$$

it follows that $d^*\alpha$ is a Haar measure on K^*. This works for $K = \mathbb{R}$ or $K = \mathbb{C}$. If K is a p-adic field, then we normalize differently and set $d^*\alpha = \frac{q}{q-1}\frac{d\alpha}{|\alpha|}$.

Lemma 19.2. *If K is a p-adic field, then*

$$\int_U d^*\alpha = (N(\mathcal{D}))^{1/2}$$

Proof. We have that

$$\int_U d^*\alpha = \frac{q}{q-1}\int_U \frac{d\alpha}{|\alpha|} = \int_U d\alpha.$$

Recall that $\int_{O_K} d\xi = N(\mathcal{D})^{-1/2}$. Moreover, we know that

$$O_K = O_K^* \times \pi^{\mathbb{N}} = \bigsqcup_{n \geq 0} O_K^* \pi^n.$$

Therefore,

$$\mathrm{vol}(O_K) = \sum_{n \geq 0} \mathrm{vol}(O_K^*) q^{-n} = \frac{q}{q-1}\mathrm{vol}(O_K^*);$$

putting this all together gives the result. □

19.1. **The Local ζ-function and the Functional Equation.** Let $f : K \longrightarrow \mathbb{C}$ take $\xi \mapsto f(\xi)$, and denote its restriction to K^* by $\alpha \mapsto f(\alpha)$. Let

$$Z = \{f : K \longrightarrow \mathbb{C} \mid f, \hat{f} \in L^1(K) \text{ continuous and } f(\alpha)|\alpha|^\sigma, \hat{f}(\alpha)|\alpha|^\sigma \in L^1(K) \text{ for any } \sigma > 0\}.$$

Let c be a quasi-character of positive exponent. Define

$$\zeta(f, c) = \int_{K^*} f(\alpha)c(\alpha)d^*\alpha.$$

We call ζ a ζ-function of K.

Lemma 19.3. *We have that ζ is a holomorphic function in s when* $\mathrm{Re}(s) > 0$.

Remark 19.4. Recall that $c(\alpha) = \tilde{c}(\tilde{\alpha})|\alpha|^s$. There is an equivalence relation on quasi-characters $c_1 \sim c_2$ if and only if c_1/c_2 is unramified. The equivalence classes are given as follows: fix $\tilde{c} : U \longrightarrow S^1$; the quasi-characters equivalent to $\tilde{c}$ are given by $\tilde{c}(-)| - |^s$.

Proof. Differentiate under the integral; this is left as an exercise to the reader. □

We would like to show that the ζ-functions of K have meromorphic continuations and functional equations.

Lemma 19.5. *Let C be a quasi-character of exponent $\sigma \in (0,1)$. Let $\hat{c}(\alpha) = |\alpha| c^{-1}(\alpha)$ for $\alpha \in K^*$.*

Theorem 19.6. *For all $f, g \in Z$, we have that*

$$\zeta(f,c)\zeta(\hat{g},\hat{c}) = \zeta(\hat{f},\hat{c})\zeta(g,c).$$

(I.e., $\zeta(f,c)/\zeta(\hat{f},\hat{c})$ is independent of f.)

Proof of lemma. We have that

$$\zeta(f,c)\zeta(\hat{g},\hat{c}) = \int_{K^*} f(\alpha)c(\alpha)d^*\alpha \int_{K^*} \hat{g}(\beta)c(\beta)d^*\beta = \int_{K^*\times K^*} f(\alpha)\hat{g}(\beta)c(\alpha\beta^{-1})|\beta|d^*(\alpha,\beta).$$

Make the change of variables $(\alpha,\beta) \mapsto (\alpha,\alpha\beta)$, which yields

$$\int_{K^*\times K^*} f(\alpha)\hat{g}(\alpha\beta)c(\beta^{-1})|\alpha\beta|d^*(\alpha,\beta) = \int_{K^*}\int_{K^*} f(\alpha)\hat{g}(\alpha\beta)|\alpha|d^*\alpha c(\beta^{-1})|\beta|d^*\beta.$$

The goal is to show that the inner integral in the above is symmetric. We have

$$\int_{K^*} f(\alpha)\hat{g}(\alpha\beta)|\alpha|d^*\alpha = \int_{K^*\times K^*} f(\alpha)g(\eta)e^{-2\pi i\Lambda(\alpha\beta\eta)}d\alpha d\eta,$$

which is clearly symmetric. □

Theorem 19.7 (Main Theorem)**.** *Any ζ-function has an analytic continuation to $\mathbb{C}$ and a functional equation*

$$\zeta(f,c) = \rho(c)\zeta(\hat{f},\hat{c}),$$

where $\rho(c)$ is independent of f and meromorphic in c.

Proof. It is enough to construct for each equivalence class of quasi-characters of exponent in $(0,1)$ an explicit function $f_c \in Z$ such that

$$\rho(c) = \frac{\zeta(f_c,c)}{\zeta(\hat{f}_c,c)}$$

for all c with $\exp(c) \in (0,1)$. Moreover, $\rho(c)$ has analytic continuation to $\mathbb{C}$ or $\mathbb{C}/2\pi i/q\mathbb{Z}$. Then this implies the theorem. Indeed, for any $f \in Z$, we have

$$\zeta(f,c)\zeta(\hat{f}_c,\hat{c}) = \zeta(\hat{f},\hat{c})\zeta(f_c,c),$$

implying that

$$\zeta(f,c) = \rho(c)\zeta(\hat{f},\hat{c}),$$

where the left-hand side is analytic for $\exp(\sigma) > 0$ and the right-hand side is analytic for $\exp(\sigma) < 1$. □

Lemma 19.8. *We have*

$$\rho(\hat{c}) = \frac{c(-1)}{\rho(c)}$$

and

$$\rho(\overline{c}) = c(-1)\overline{\rho(c)},$$

and $|\rho(c)| = 1$ if c has exponent 1/2.

Proof. We know that

$$\zeta(f,c)=\rho(c)\zeta(\hat{f},\hat{c})=\rho(c)\rho(\hat{c})\zeta(\hat{\hat{f}},\hat{\hat{c}}).$$

Now, $\hat{\hat{c}}(\alpha)=|\alpha|\hat{c}^{-1}(\alpha)=c(\alpha)$ and $\hat{\hat{f}}(\alpha)=f(-\alpha)$. The result follows. □

20. Thursday March 11

Proof. We prove that $\rho(c)$ (for $c=c_0|\cdot|^s$) as defined previously has analytic continuation for $s\in\mathbb{C}$ (K archimedean) and for $s\in\mathbb{C}/2\pi i/q\mathbb{Z}$.

In the case where $K=\mathbb{R}$ is real, we have $\Lambda(\xi)=-\xi$ for $\xi\in\mathbb{R}$. The equivalence classes of quasi-characters of $\mathbb{R}^*$ are

$$\operatorname{sgn}(\alpha)|\alpha|^s \quad\text{and}\quad |\alpha|^s$$

for $s\in\mathbb{C}$. Let $f(\xi)=e^{-\pi\xi^2}$ (corresponds to $|\alpha|^s$) and let $f_\pm(\xi)=\xi e^{-\pi\xi^2}$ (corresponds to $\operatorname{sgn}(\alpha)|\alpha|^s$). It is not difficult to compute that $\hat{f}(\xi)=f(\xi)$ and $\widehat{f_\pm}(\xi)=if_\pm(\xi)$. We compute the zeta function

$$\zeta(f,|\cdot|^s)=\int_{\mathbb{R}^*}f(x)|x|^s\frac{dx}{x}=2\int_0^\infty e^{-\pi x^2}|x|^s\frac{dx}{x}=2\int_0^\infty e^{-t}\frac{t^{s/2}}{\pi^{s/2}}\frac{dt}{2\sqrt{\pi t}}=\frac{1}{\pi^{s/2}}\Gamma(s/2),$$

and

$$\zeta(f_\pm,c_0|\cdot|^s)=\int_{-\infty}^0 xe^{-\pi x^2}(-|x|^s)\frac{dx}{x}+\int_0^\infty 2e^{-\pi x^2}|x|^s\frac{dx}{|x|}=2\int_0^\infty e^{-\pi x^2}|x|^s dx=\pi^{-(s+1)/2}\Gamma((s+1)/2).$$

Moreover, we compute that

$$\zeta(\hat{f},\widehat{|\cdot|^s})=\zeta(f,|\cdot|^{1-s})=\pi^{(s-1)/2}\Gamma((1-s)/2)$$

and

$$\zeta(\widehat{f_\pm},\widehat{|\cdot|^s})=i\zeta(f_\pm,|\cdot|^{1-s})=i\pi^{-(1-s+1)/2}\Gamma((1-s+1)/2).$$

Hence,

$$\rho(|\cdot|^s)=\frac{\pi^{-2/s}\Gamma(s/2)}{\pi^{(s-1)/2}\Gamma((1-s)/2)}=2\pi^{-s}\cos(\pi s/2)\Gamma(s)$$

and

$$\rho(\pm|\cdot|^s)=\frac{i\pi^{-(s+1)/2}\Gamma((s+1)/2)}{\pi^{-(1-s+1)/2}\Gamma((1-s+1)/2)}=-i2^{1-s}\pi^{-s}\sin(\pi s/2)\Gamma(s).$$

Both of these functions have analytic continuations to $\mathbb{C}$.

For the case $K=\mathbb{C}$, the equivalence classes of quasi-characters are $c_n(\alpha)=\alpha^n$ for $c_n:S^1\longrightarrow S^1$ and $n\mathbb{Z}$. We define corresponding functions to be

$$f_n(\xi)=\begin{cases}(x-iy)^{|n|}e^{-2\pi(x^2+y^2)} & \text{if } n\geq 0\\ (x+iy)^{|n|}e^{-2\pi(x^2+y^2)} & \text{if } n\leq 0\end{cases},$$

and note that the Fourier transform of f_n is

$$\widehat{f_n}(\xi)=i^{|n|}f_n(\xi)$$

for all n. Recall the Lebesgue meausure on $\mathbb{C}$ $d\xi=2dxdy$ in addition to the multiplicative measure $d^*\alpha=\frac{2}{r}drd\theta$, where $\alpha=re^{i\theta}$ and $|\alpha|=r^2$. We have that

$$\zeta(f_n,c_n|\cdot|^s)=\int_{\mathbb{C}^*}f_n(\alpha)c_n(\alpha)|\alpha|^s d^*\alpha=\int_0^\infty\int_0^{2\pi}r^n e^{-i\theta n}e^{-2\pi r^2}e^{i\theta n}r^{2s}\frac{2drd\theta}{r},$$

which simplifies to

$$2\int_0^\infty \int_0^{2\pi} e^{-2\pi r^2} r^{2s+n-1} dr d\theta = 4\pi \int_0^\infty e^{-2\pi r^2} r^{2s+1} dr.$$

Changing variables gives us that the the above is equal to $(2\pi)^{1-s+|n|/2}\Gamma(s+|n|/2)$. Similarly, we have that

$$\zeta(\hat{f_n}, \widehat{c_n|\cdot|^s}) = \zeta(i^{|n|} f_{-n}, c_{-n}|\cdot|^{1-s}) = i^{|n|}(2\pi)^{s+|n|/2}\Gamma(1-s+|n|/2),$$

so

$$\rho(c_n|\cdot|^s) = \frac{(-1)^{|n|}(2\pi)^{1-s}\Gamma(s+|n|/2)}{(2\pi)^2\Gamma(1-s+|n|/2)},$$

which has analytic continuation to $\mathbb{C}$.

The final case is for K a p-adic field. For $\xi \in K$, recall that $\Lambda(\xi) = \lambda(\mathrm{tr}_{K/\mathbb{Q}_p}(\xi))$. We fix some notation: $q = |\mathcal{O}_K/\mathfrak{p}|$ and $d^*\alpha = \frac{q}{q-1}\frac{d\alpha}{|\alpha|}$; recall that $\mathrm{vol}(\mathcal{O}_K) = (N(\mathcal{D}))^{-1/2}$. Now, what are the equivalence classes of quasi-characters? For $n \geq 0$, let c_n be a character of conductor π^n such that $c_n(\pi) = 1$ (so $c_n|_{(1+\pi^n)} = 1$). Let

$$f_n(\xi) = \begin{cases} e^{2\pi i\Lambda(\xi)} & \text{if } \xi \in \mathcal{D}^{-1}\mathfrak{p}^{-n} \\ 0 & \text{otherwise.} \end{cases}$$

We next show the following helpful claim:

$$\hat{f_n}(\xi) = \begin{cases} N(\mathcal{D})^{1/2}N(\mathfrak{p})^n & \text{if } \zeta \equiv 1 \mod \mathfrak{p}^n \\ 0 & \text{otherwise.} \end{cases}$$

Begin by noting that

$$\hat{f_n}(\xi) = \int f_n(\eta) e^{-2\pi i\Lambda(\xi\eta)} d\eta = \int_{\mathcal{D}^{-1}\mathfrak{p}^{-n}} e^{-2\pi i\Lambda((\xi-1)\eta)} d\eta.$$

Now, $\mathcal{D}^{-1}\mathfrak{p}^{-n}$ is a compact subgroup of K, and the map taking $\eta \mapsto e^{-2\pi i\Lambda((\xi-1)\eta)}$ is a character of $\mathcal{D}^{-1}\mathfrak{p}^{-n}$. Recall that if H is a compact abelian group with Haar meausre μ, then

$$\int_H \chi(h) d\mu = \begin{cases} 0 & \text{if } \chi \neq 1; \\ \mathrm{vol}(H) & \text{if } \chi = 1, \end{cases}$$

where $\chi : H \longrightarrow S^1$ is a character. To see this, note that if χ is nontrivial, then there exists $g \in H$ with $\chi(g) \neq 1$, and we can make the change of variables

$$\int_H \chi(h) dh = \int_H \chi(gh) gh = \chi(g) \int_H \chi(h) dh,$$

which forces the integral to be 0, since $\chi(g) \neq 1$. Returning to our integral of $\mathcal{D}^{-1}\mathfrak{p}^{-n}$, the character $\eta \mapsto e^{-2\pi i\Lambda((\xi-1)\eta)}$ is trivial if and only if $\xi \equiv 1 \bmod \mathfrak{p}^n$. Hence,

$$\hat{f_n}(\xi) = \mathrm{vol}(\mathcal{D}^{-1}\mathfrak{p}^{-n}) = \mathrm{vol}(\pi^{-n-d}\mathcal{O}_K) = |\pi^{-n-d}|N(\mathcal{D})^{-1/2} = q^{n+s}q^{-d/2} = q^{n+d/2}.$$

Now, we can compute the ζ-function. If $n = 0$, then $c_0 = 1$. It follows that

$$\zeta(f_n, |\cdot|^s) = \int_{\mathcal{D}^{-1}} |\alpha|^s d^*\alpha.$$

Let $A_v = \{x \in K^* \mid v(x) = v\} = \pi^v \mathcal{O}_K^* = \{x \mid 1/q < |x| < q\}$ (think of A_v as some sort of annulus). Note that

$$\mathcal{D}^{-1} = \bigcup_{v=-d}^{\infty} A_v$$

and that, excluding 0, this union is disjoint. Now,

$$\zeta(f_0, |\cdot|^s) = \sum_{v=-d}^{\infty} \int_{A_v = \pi^v \mathcal{O}_K^*} q^{-vs} d^*\alpha = \sum_{v=-d}^{\infty} q^{-vs} \mathrm{vol}_{d^*}(\mathcal{O}_K^*) = \frac{q^{ds}}{1-q^{-s}} N(\mathcal{D})^{-1/2} = \frac{q^{d(s-1/2)}}{1-q^{-s}}.$$

On the other hand, $\hat{f}_0 = N(\mathcal{D})^{1/2} \mathbb{1}_{\mathcal{O}_K}$, so

$$\zeta(\hat{f}_0, \widehat{|\cdot|^s}) = q^{d/2} \int_{\mathcal{O}_K} |\alpha|^{1-s} d^*\alpha = q^{d/2} \sum_{v=0}^{\infty} q^{-v(1-s)} q^{-d/2} = \frac{1}{1-q^{s-1}}.$$

It follows that

$$\rho(|\cdot|^s) = q^{d(s-1/2)} \frac{1-q^{s-1}}{1-q^{-s}}$$

has an analytic continuation to $\mathbb{C}$. □

21. Tuesday April 16

Proof. We continue from where we left off previously. Let K be a p-adic field. For c_n a character of conductor n (where $c_n(\pi) = 1$), recall that

$$f_n(\xi) = \begin{cases} e^{2\pi i \Lambda(\xi)} & \text{if } \xi \in \mathcal{D}^{-1}\mathfrak{p}^{-n} \\ 0 & \text{otherwise,} \end{cases}$$

and that

$$\hat{f}_n(\xi) = \begin{cases} N(\mathcal{D})^{1/2} N(\mathfrak{p})^n & \text{if } \zeta \equiv 1 \mod \mathfrak{p}^n \\ 0 & \text{otherwise.} \end{cases}$$

We consider the ramified case for $n > 0$. Note that

$$\zeta(f_n, c_n |\cdot|^s) = \int_{\mathcal{D}^{-1}\mathfrak{p}^{-n}} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) |\alpha|^s d^*\alpha.$$

Let $\mathcal{D} = (\pi^d)$, and note that $(\pi^{-d-n}) = \mathcal{D}^{-1}\mathfrak{p}^{-n} = \bigcup_{v=-d-n}^{\infty} A_v$, where $A_v = \{x \in \mathcal{O}_K \mid v(x) = v\}$. Thus, we may write the integral in the above as

$$\zeta(f_n, c_n |\cdot|^s) = \int_{\mathcal{D}^{-1}\mathfrak{p}^{-n}} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) |\alpha|^s d^*\alpha = \sum_{v=-d-n}^{\infty} q^{-vs} \int_{A_v} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d^*\alpha.$$

We claim that

$$\int_{A_v} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d^*\alpha = 0$$

for $v > -d - n$.

To see this claim, consider the case where $v \geq -d$. Then $A_v \subset \mathcal{D}^{-1}$, and $\Lambda(\alpha) = \lambda(\mathrm{tr}_{K/\mathbb{Q}_p}(\alpha)) = 0$, since $\mathrm{tr}_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$. Hence, we get

$$\int_{A_v} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d^*\alpha = \int_{\pi^v \mathcal{O}_K^*} c_n(\alpha) d^*\alpha = \int_{\mathcal{O}_K^*} c_n(\pi^v \alpha) d^*\alpha = \int_{\mathcal{O}_K^*} c_n(\alpha) d^*\alpha = 0,$$

since c_n is nontrivial on $\mathcal{O}_K^*$ (we are in the ramified case).

Next, consider the case where $-d-n < \nu < -d$. Recall that $\mathcal{D}^{-1} = (\pi^{-d})$ and that $A_\nu = \pi^\nu \mathcal{O}_K^*$. Write $A_\nu = \bigsqcup(\alpha_0 + \mathcal{D}^{-1})$ (take a set of representatives of the quotient by $\mathcal{D}^{-1}$). If $x \in \alpha_0 + \mathcal{D}^{-1}$, then $\Lambda(x) = \Lambda(\alpha_0)$. Thus,

$$\int_{\alpha_0+\mathcal{D}^{-1}} e^{2\pi i\Lambda(\alpha)} c_n(\alpha) d^*\alpha = e^{2\pi i\Lambda(\alpha_0)} \int_{\alpha_0(1+\mathfrak{p}^{-\nu-d})} c_n(\alpha) d^*\alpha.$$

Now, changing variables gives us that

$$\int_{\alpha_0(1+\mathfrak{p}^{-\nu-d})} c_n(\alpha) d^*\alpha = \int_{\alpha_0(1+\mathfrak{p}^{-\nu-d})} c_n(\alpha_0\alpha) d^*\alpha = c_n(\alpha_0) \int_{\alpha_0(1+\mathfrak{p}^{-\nu-d})} c_n(\alpha) d^*\alpha.$$

The above is 0 as long as c_n is a nontrivial character on $1+\mathfrak{p}^{-\nu-d}$. This follows from the fact that $0 < -\nu - d < n$, since $c_n|_{1+\mathfrak{p}^{-\nu-d}}$ is a nontrivial character of conductor n.

Hence, we are left with

$$\zeta(f_n, c_n|\cdot|^s) = q^{(d+n)s} \int_{A_{-d-n}} e^{2\pi i\Lambda(\alpha)} c_n(\alpha) d^*\alpha.$$

Let $\mathcal{E}$ be a set of representatives of $\mathcal{O}_K^*/(1+\mathfrak{p}^n)$ so that $\mathcal{O}_K^* = \bigsqcup_{\epsilon\in\mathcal{E}} \epsilon(1+\mathfrak{p}^n)$. Then

$$A_{-d-n} = \bigsqcup_{\epsilon\in\mathcal{E}} \epsilon\pi^{-d-n}(1+\mathfrak{p}^n) = \bigsqcup_{\epsilon\in\mathcal{E}} (\epsilon\pi^{-d-n} + \mathcal{D}^{-1}).$$

On $\epsilon\pi^{-d-n}(1+\mathfrak{p}^n)$, we have that c_n is equal to $c_n(\epsilon)$. Moreover, on $\epsilon\pi^{-d-n}+\mathcal{D}^{-1}$, we have that Λ is equal to $\Lambda(\epsilon\pi^{-d-n})$. Thus,

$$\zeta(f_n, c_n|\cdot|^s) = q^{(d+n)s} \left(\sum_{\epsilon\in\mathcal{E}} \int_{\epsilon\pi^{-d-n}+\mathcal{D}^{-1}} c_n(\epsilon) e^{2\pi i\Lambda(\epsilon\pi^{-d-n})} \right) = q^{(d+n)s} \left(\sum_{\epsilon\in\mathcal{E}} c_n(\epsilon) e^{2\pi i\Lambda(\epsilon\pi^{-d-n})} \right) \int_{1+\mathfrak{p}^n} d^*\alpha.$$

Now, we compute

$$\zeta(\hat{f}_n, \widehat{c_n|\cdot|^s}) = \zeta(\hat{f}_n, c_n^{-1}|\cdot|^{1-s}) = q^{n+d/2} \int_{1+\mathfrak{p}^n} c_n(\alpha)^{-1} |\alpha|^{1-s} d^*\alpha = q^{n+d/2} \int_{1+\mathfrak{p}^n} d^*\alpha.$$

This gives us explicit expressions for $\rho(c)$:

$$\rho(|\cdot|^s) = q^{s-1/2} \frac{1-q^{s-1}}{1-q^{-s}} \quad \text{and} \quad \rho(c, |\cdot|^s) = q^{(d+n)(s-1/2)} \rho_0(c),$$

where

$$\rho_0(c) = q^{-n/2} \sum_{\epsilon\in\mathcal{E}} c(\epsilon) e^{2\pi i\Lambda(\epsilon/\pi^{d+n})}.$$

The above is called a *root number.* As an exercise, prove that $|\rho_0(c)| = 1$. We see that ρ is meromorphic and admits an analytic continuation to the whole complex plane; this completes our analysis of the local case. □

21.1. **Restricted Products.** Let $\{\mathfrak{p}\}$ be a set of indices. For each $\mathfrak{p}$, let $G_\mathfrak{p}$ be a locally compact abelian group, with $H_\mathfrak{p} \subset G_\mathfrak{p}$ an open compact subgroup. Let $G = \prod_\mathfrak{p}' G_\mathfrak{p}$, and recall that G is a locally compact abelian group. The topology on G is given by viewing G as the inductive limit

$$G = \varinjlim_{\substack{S\subset\{\mathfrak{p}\} \\ |S|<\infty}} \prod_{\mathfrak{p}\in S} G_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p},$$

where the individual terms in the limits are endowed with the product topology.

Now, what are the characters of G? Let $c : G \longrightarrow \mathbb{C}^*$ be a continuous quasi-character; denote its restriction to $G_\mathfrak{p}$ by $c_\mathfrak{p}$.

Lemma 21.1. *For almost all $\mathfrak{p}$, we have $c_\mathfrak{p}|_{H_\mathfrak{p}} = 1$ and*

$$c(\alpha) = \prod_\mathfrak{p} c_\mathfrak{p}(\alpha_\mathfrak{p})$$

for $\alpha \in G$. Conversely, if $c_\mathfrak{p} : G_\mathfrak{p} \longrightarrow \mathbb{C}^*$ is a quasi-character for all $\mathfrak{p}$ and $c_\mathfrak{p}|_{H_\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$, then $c = \prod_\mathfrak{p} c_\mathfrak{p}$ defines a continuous quasi-character of G.

Proof. Let $U = D(1/2, 1) \subset \mathbb{C}^*$. Note that $c^{-1}(U)$ is an open subset of G. Thus, there exists a finite set S such that

$$\prod_\mathfrak{p} N_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} H_\mathfrak{p} \subset c^{-1}(U)$$

for $N_\mathfrak{p} \subset G_\mathfrak{p}$ open. It follows that $c_\mathfrak{p}(H_\mathfrak{p}) \subset U$ for $\mathfrak{p} \notin S$, but $c_\mathfrak{p}(H_\mathfrak{p})$ is a subgroup of $\mathbb{C}^*$, which forces $c_\mathfrak{p}(H_\mathfrak{p}) = 1$.

For the other direction, the only nontrivial issue is the continuity of $c = \prod_\mathfrak{p} c_\mathfrak{p}$. Let $S = \{\mathfrak{p} \mid c_\mathfrak{p}|_{H_\mathfrak{p}} \neq 1\}$; suppose $|S| = n$. Let $U \subset \mathbb{C}^*$ be a neighborhood of 1; let V be another neighborhood of 1 such that $V^n \subset U$. For $\mathfrak{p} \in S$, there exists $N_\mathfrak{p} \subset G_\mathfrak{p}$ such that $c_\mathfrak{p}(N_\mathfrak{p}) \subset V$, so $c(\prod_\mathfrak{p} N_\mathfrak{p}) \subset V^n \subset U$. Thus,

$$\prod_{\mathfrak{p} \in S} N_\mathfrak{p} \times \prod_\mathfrak{p} H_\mathfrak{p} \subset c^{-1}(U),$$

implying $c^{-1}(U)$ is open, as desired. □

Let $\widehat{G}_\mathfrak{p}$ denote the dual of $G_\mathfrak{p}$. Let $H_\mathfrak{p}^* = \{\chi \in \widehat{G}_\mathfrak{p} \mid \chi|_{H_\mathfrak{p}} = 1\}$, and note that $\widehat{G}_\mathfrak{p}/H_\mathfrak{p}^* \simeq \widehat{H}_\mathfrak{p}$ is discrete. Hence, $H_\mathfrak{p}^* \subset \widehat{G}_\mathfrak{p}$ is open (recall that $H_\mathfrak{p}$ open implies $G_\mathfrak{p}/H_\mathfrak{p}$ is discrete, so $H_\mathfrak{p}^* = \widehat{G_\mathfrak{p}/H_\mathfrak{p}}$ is compact).

Theorem 21.2. *The restricted product $\prod_\mathfrak{p}{}' \widehat{G}_\mathfrak{p}$ with respect to $H_\mathfrak{p}^*$ is isomorphic to $\widehat{G}$ as locally compact abelian groups.*

Proof. By the previous lemma, the map $\widehat{G} \longrightarrow \prod_\mathfrak{p}{}' \widehat{G}_\mathfrak{p}$ given by $c \mapsto (c|_{G_\mathfrak{p}})$ is a bijection. It is left as an exercise to check compatibility. □

21.2. **Measure Theory.** We relate the Haar measure on $\prod_\mathfrak{p}{}' G_\mathfrak{p}$ to the Haar measures on each $G_\mathfrak{p}$. We will show that the Haar measure on the restricted product is the restricted product of the individual Haar measures. Let $da_\mathfrak{p}$ be a Haar measure on $G_\mathfrak{p}$ such that

$$\int_{H_\mathfrak{p}} da_\mathfrak{p} = 1$$

for almost all $\mathfrak{p}$.

Theorem 21.3. *The restricted product*

$$G = \prod_\mathfrak{p}{}' G_\mathfrak{p}$$

has a unique Haar meausre da such that for any finite subset $S \subset \{\mathfrak{p}\}$ and

$$G_S = \prod_{\mathfrak{p} \in S} G_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} H_\mathfrak{p},$$

we have

$$da|_{G_S} = \prod_{\mathfrak{p}\in S} da_{\mathfrak{p}} \times da^S,$$

where da^S *is the Haar measure on* $\prod_{\mathfrak{p}\notin S} H_{\mathfrak{p}}$ *such that*

$$\int_{G^S} da^S = \prod_{\mathfrak{p}\notin S}\left(\int_{H_{\mathfrak{p}}} da_{\mathfrak{p}}\right)$$

(here we are letting $H^S = \prod_{\mathfrak{p}\notin S} H_{\mathfrak{p}}$*).*

Proof. See page 325 of Section 3.3 in Cassels and Frölich. □

22. Thursday April 18

22.1. Computing Integrals in Restricted Products.

Let $G = \prod'_{\mathfrak{p}} G_{\mathfrak{p}}$ with respect to open compact subgroups $H_{\mathfrak{p}} \subset G_{\mathfrak{p}}$. We have $da = \prod' da_{\mathfrak{p}}$ and

$$\int_{H_{\mathfrak{p}}} da_{\mathfrak{p}} = 1$$

for almost all $\mathfrak{p}$.

Definition 22.1. Let $T = \{\mathfrak{p}\}$ be the index set, and let φ be a function taking finite subsets of T into $\mathbb{C}$ (or, more generally, any topological space). We let $\varphi_0 = \lim_S \varphi(S)$. If for every open V_0 containing φ_0, there exists a finite set $S(V_0)$ such that for all $S \supset S(v_0)$ we have $\varphi(S) \in V_0$.

Lemma 22.2. *Let* $f : G \longrightarrow \mathbb{R}$ *be a function that is either measurable and nonnegative (*$f \geq 0$*) or in* $L^1(G)$*. Then*

$$\int_G f(a)da = \lim_S \int_{G_S} f(a)da.$$

Lemma 22.3. *For each* $\mathfrak{p}$*, let* $f_{\mathfrak{p}} \in L^1(G_{\mathfrak{p}})$ *be a continuous function such that* $f_{\mathfrak{p}}(x) = 1$ *for all* $x \in H_{\mathfrak{p}}$ *for almost all* $\mathfrak{p}$*. Let* $f = \prod_{\mathfrak{p}} f_{\mathfrak{p}}$*. Then* f *is continuous. Moreover, if* S *is a finite set of primes containing* $\{\mathfrak{p} \mid f_{\mathfrak{p}}|_{H_{\mathfrak{p}}} \neq 1\}$*, then*

$$\int_{G_S} f(a)da = \prod_{\mathfrak{p}\in S}\left(\int_{G_{\mathfrak{p}}} f_{\mathfrak{p}}(a_{\mathfrak{p}})da_{\mathfrak{p}}\right).$$

Lemma 22.4. *If*

$$\prod_{\mathfrak{p}}\left(\int_{G_{\mathfrak{p}}} |f_{\mathfrak{p}}(a_{\mathfrak{p}})|da_{\mathfrak{p}}\right) < \infty,$$

then $f \in L^1(G)$ *and*

$$\int_G f(a)da = \lim_S \int_{G_S} f(a)da = \prod_{\mathfrak{p}}\left(\int_{G_{\mathfrak{p}}} f_{\mathfrak{p}}(a_{\mathfrak{p}})da_{\mathfrak{p}}\right).$$

22.2. **Fourier Analysis on Restricted Products.** Recall that $\widehat{G} = \prod'_\mathfrak{p} \widehat{G}_\mathfrak{p}$, where the restricted product is taken with respect to $H_\mathfrak{p}^* = H_\mathfrak{p}^\perp = \{c \in \widehat{G}_\mathfrak{p} \mid c|_{H_\mathfrak{p}} = 1\} = \widehat{G/H_\mathfrak{p}}$. Denote an arbitrary element of $\widehat{G}$ by $c = (c_\mathfrak{p})_\mathfrak{p}$, and let $dc_\mathfrak{p}$ denote the measure on $\widehat{G}_\mathfrak{p}$ dual to $da_\mathfrak{p}$. As an exercise, check that

$$\int_{H_\mathfrak{p}^*} dc_\mathfrak{p} = 1$$

for almost all $\mathfrak{p}$. Hint: use the following inversion formula

$$\left(\int_{H_\mathfrak{p}} da_\mathfrak{p}\right)\left(\int_{H_\mathfrak{p}^*} dc_\mathfrak{p}\right) = 1.$$

Let $dc = \prod'_\mathfrak{p} dc_\mathfrak{p}$.

Lemma 22.5. *Let $f_\mathfrak{p} \in L^1(G)$ and $\hat{f}_\mathfrak{p} \in L^1(\widehat{G}_\mathfrak{p})$ be continuous. Suppose that $f_\mathfrak{p}|_{H_\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$. Then $f = \prod f_\mathfrak{p}$ has Fourier transform $\hat{f} = \prod'_\mathfrak{p} \hat{f}_\mathfrak{p}$, and dc is the measure dual to da.*

22.3. **Return to Global Theory.** Let K be a number field with ring of integers $\mathcal{O}_K$. If $\mathfrak{p}$ is a prime (finite or infinite), then as usual let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$. Likewise, let $\mathcal{O}_{K,\mathfrak{p}}$ be the ring of integers in $K_\mathfrak{p}$. Recall from the beginning of the course the ring of adèles $\mathbb{A}_K$ and the group of idèles I_K.

For each $\mathfrak{p}$, we have an isomorphism $K_\mathfrak{p} \longrightarrow \widehat{K}_\mathfrak{p}$ given by $\xi \mapsto (x \mapsto e^{2\pi i \Lambda_\mathfrak{p}(x\xi)})$. For $x \in \mathbb{A}_K$, we have that $\Lambda_\mathfrak{p}(x) = 0$ for almost all $\mathfrak{p}$. Thus,

$$\Lambda(x) = \sum_\mathfrak{p} \Lambda_\mathfrak{p}(x)$$

is a well-defined expression.

Theorem 22.6. *The map $\mathbb{A}_K \longrightarrow \widehat{\mathbb{A}}_K$ taking*

$$\xi \mapsto \left(x \mapsto e^{2\pi i \Lambda(x\xi)}\right)$$

is an isomorphism. Moreover, $f \in L^1(\mathbb{A}_K)$, and

$$\widehat{f}(\eta) = \int_{\mathbb{A}_K} f(x) e^{-2\pi i \Lambda(\eta x)} dx.$$

If $\hat{f} \in L^1(\mathbb{A}_K)$, then $\hat{\hat{f}}(x) = f(-x)$.

Proof. The map $\mathbb{A}_K \longrightarrow \widehat{\mathbb{A}}_K$ is simply the product of the isomorphisms $K_\mathfrak{p} \longrightarrow \widehat{K}_\mathfrak{p}$ taking $\xi \mapsto (x \mapsto e^{2\pi i \Lambda_\mathfrak{p}(\xi x)})$ (note that this map takes $\mathcal{O}_{K,\mathfrak{p}}$ to $\mathcal{O}_{K,\mathfrak{p}}^*$, so the product of these local maps is indeed well-defined on the restricted product). The local isomorphisms give us the global one. □

Recall that we have a norm map $|\cdot| : I_K \longrightarrow \mathbb{R}_{\geq 0}$ given by $(x_\mathfrak{p}) \mapsto \prod_\mathfrak{p} |x_\mathfrak{p}|$. Thus, we see that if $x \in I_K$, we have $d(xa) = |x| da$ (this follows from the local situation, where $d(x_\mathfrak{p} a_\mathfrak{p}) = |x_\mathfrak{p}| da_\mathfrak{p}$).

We also recall that K embeds into $\mathbb{A}_K$ via the diagonal map; its image is a cocompact subgroup. Also, for all $x \in K$, we have $\Lambda(x) = 0$. Indeed, we may write

$$\Lambda(x) = \sum_\mathfrak{p} \Lambda_\mathfrak{p}(x) = \sum_p \left(\sum_{\mathfrak{p}|p} \Lambda_\mathfrak{p}(x)\right) = \sum_p \Lambda_p(y),$$

where $y \in \mathbb{Q}$. The last equality follows from assuming that K is Galois (which we may do without loss of generality) and noting the following. We have

$$\sum_{\mathfrak{p}|\infty} \Lambda_{\mathfrak{p}}(x) = \Lambda_\infty \left(\sum_\sigma \sigma(x) \right),$$

where $\Lambda_\infty : \mathbb{Q} \longrightarrow \mathbb{R}/\mathbb{Z}$ takes $y \mapsto -y$; a similar argument works for

$$\sum_{\mathfrak{p}|p} \Lambda_{\mathfrak{p}}(x).$$

Thus, we may rewrite the above as

$$\sum_p \Lambda_p(y) = \sum_p \lambda_p(y).$$

Fixing a finite prime q, we have

$$\sum_{p \neq q, p < \infty} \lambda_p(y) + \lambda_q(y) - y.$$

Since $\lambda_q(y) - y \in \mathbb{Z}_q$ and since $\lambda_p(y) \in \mathbb{Z}_q$ for $p \neq q$, it follows that

$$\sum_p \lambda_p(y) \in \mathbb{Q} \cap \mathbb{Z}_q = \mathbb{Z},$$

so $\sum_p \lambda_p(y) = 0$.

We conclude that under the isomorphism $\mathbb{A}_K \simeq \widehat{\mathbb{A}}_K^*$, we have that K is sent to K^*. To see why this is the case, note that $K^* = \widehat{\mathbb{A}_K/K}$ is discrete. Since $K \subset K^*$, it follows that K^*/K is discrete; $K^*/K \subset V/K$, some compact set. Thus, we have that K^* is a K-vector space such that K^*/K is finite. Thus, $K = K^*$, as desired.

We move on to discuss the multiplicative theory of idèles. We have that

$$K^* \hookrightarrow I_K \longrightarrow \mathbb{R}_{>0},$$

where the first map is the diagonal embedding and the second one the norm $|\cdot| : I_K \longrightarrow \mathbb{R}_{>0}$. Note that the first map factors through $J_K = \{x \in I_K \mid |x| = 1\}$. We have the following product formula: for all $x \in K$, we have $|x| = \prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1$. We now choose a decomposition $I_K = J_K \times T$ in the following way. Let $\mathfrak{p}_0$ be archimedean, and let

$$T = \{a \in I_K \mid a_{\mathfrak{p}_0} > 0, a_{\mathfrak{p}} = 1 \text{ for } \mathfrak{p} \neq \mathfrak{p}_0\}.$$

If $\mathfrak{p}_0 = \mathbb{R}$, set $s(t) = (t, 1, 1, \ldots)$; if $\mathfrak{p}_0 = \mathbb{C}$, set $s(t) = (\sqrt{t}, 1, \ldots)$. Let dt/t be the Haar measure on T. On J_K we choose the measure db such that $da = db \times dt/t$. If $f \in L^1(I_K)$, then

$$\int_{I_K} f(a)da = \int_0^\infty \left(\int_{J_K} f(tb)db \right) \frac{dt}{t} = \int_{J_K} \int_0^\infty f(tb)\frac{dt}{t}db.$$

Recall K^*/J_K is cocompact, so

$$\mathrm{vol}(J_K/K^*) = \frac{2^{r_1}(2\pi)^{r_2} h_K \mathrm{Reg}(K)}{\sqrt{\mathrm{disc}_K}\omega_K}.$$

We will be interested only in quasi-characters that are trivial on K^*. Given such a quasi-character $c : I_K \longrightarrow \mathbb{C}^*$, we can consider its restriction to J_K; this descends to a quasi-character on J_K/K^*, which is a compact group. Hence, c is a character on J_K/K^*.

Definition 22.7. Such a character $c : I_K \longrightarrow \mathbb{C}^*$ trivial on K^* is said to be unramified if $C|_{J_K} = 1$.

Note that if c is unramified, then $c = |\cdot|^s$ for $s \in \mathbb{C}$. If $c : I_K \longrightarrow \mathbb{C}^*$, then $|c(x)| = |x|^\sigma$ for $\sigma \in \mathbb{R}$, where σ is called the exponent of c. Note that c is a character if and only if $\sigma = 0$.

22.4. **The ζ-function and the Functional Equation.** Let $f : \mathbb{A}_K \to \mathbb{C}$ be continuous. Let Z

23. Tuesday April 23

23.1. **The global ζ-function.** Recall the following from last time. Let Z be the set of functions $f : \mathbb{A}_K \longrightarrow \mathbb{C}$ such that $f, \hat{f} \in L^1(\mathbb{A}_K)$ are continuous; the functions

$$\sum_{\xi \in K} f(a(x+\xi)) \quad \text{and} \quad \sum_{\xi \in K} \hat{f}(a(x+\xi))$$

converge absolutely for all $a \in I_K$ and $x \in \mathbb{A}_K$ and uniformly in (a, x) for $a \in C \subset I_K$ compact and $x \in \mathbb{A}_K/K$; and the functions $a \mapsto f(a)|a|^\sigma$ and $a \mapsto \hat{f}(a)|a|^\sigma$ are in $L^1(I_K)$ for all $\sigma > 1$. For $f \in Z$, let c be a quasi-character of exponent greater than 1 (i.e., $c(x) = 1$ for all $x \in K^*$). Recall that a quasi-character $c : I_K \longrightarrow \mathbb{C}^*$ is unramified if $C/J_K = 1$, where $J_K = \{x \in I_K \mid |x| = 1\}$, where $|x| = \prod_{\mathfrak{p}} |x|_{\mathfrak{p}}$. Also recall that there is an equivalence relation on the quasi-characters given by $c_1 \sim c_2$ if c_1/c_2 is unramified, or, equivalently, if $c_1 = c_2|\cdot|^s$ for $x \in \mathbb{C}$. To $f \in Z$ and a quasi-character c, we associate the ζ-function

$$\zeta(f, c) = \int_{I_K} f(a)c(a)da.$$

Fix c_0 such that $c = c_0|\cdot|^s$ for $s \in \mathbb{C}$. Let $\zeta(f, c) = \zeta(f, c_0|\cdot|^s)$.

Lemma 23.1. *The function $\zeta(f, c)$ is holomorphic in s for $\operatorname{Re}(s) = \exp(c) > 1$.*

Proof. We sketch a proof. Write

$$f(a)c(a) = f(a)c_0(a)e^{s\log|a|}.$$

Then

$$\frac{\partial}{\partial s}(f(a)c(a)) = f(a)c_0(a)\log|a||a|^s \in L^1(I_K);$$

from this the result follows. □

The following is the main theorem.

Theorem 23.2. *The ζ-function admits an analytic continuation for all c with simple poles at $c = 1$ ($s = 0$ and $c_0 = 1$) or $c(a) = |a|$ ($s = 1$ and $c_0 = 1$) with residues $-\kappa f(0)$ and $\kappa\hat{f}(0)$, respectively. Here,*

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\sqrt{\operatorname{Disc}(\mathcal{O}_K)}\omega_K}.$$

The ζ-function satisfies the functional equation

$$\zeta(f, c) = \zeta(\hat{f}, \hat{c}),$$

where $\hat{c}(a) = |a|c^{-1}(a)$.

Proof. Let c be a quasi-character of greater than 1. Then

$$\zeta(f,c)=\int_{I_K} f(a)c(a)da=\int_0^\infty\int_J f(tb)c(tb)db\frac{dt}{t}=\int_0^\infty \zeta_t(f,c)\frac{dt}{t},$$

where

$$\zeta_t(f,c)=\int_{J_K} f(tb)c(tb)db.$$

Since $|c(tb)|=t^\sigma$ (notably, $c(tb)$ is independent of b), we know that $\zeta_t(f,c)$ is convergent for all c. We interrupt this proof to prove a short lemma.

Lemma 23.3. *We have*

$$\zeta_t(f,c)+f(0)\int_E c(tb)db=\int_{1/t}(\hat{f},\hat{c})+\hat{f}(0)\int_E \hat{c}(b/t)db,$$

where E is a fundamental domain for the action of K^* on J_K.

Proof. Recall that J_K/K^* is compact. We can write $J_K=\bigcup_{\alpha\in K^*}\alpha E$ and split

$$\zeta_t(f,c)+f(0)\int_E c(tb)db=\sum_{\alpha\in K^*}\int_{\alpha E} f(tb)c(tb)db+f(0)\int_E c(tb)db.$$

Rewrite this as

$$\sum_{\alpha\in K^*}\int_{\alpha E} f(\alpha tb)c(\alpha tb)db+f(0)\int_E c(tb)db=\int_E\sum_{\alpha\in K^*} f(\alpha tb)c(tb)db+f(0)\int_E c(tb)db,$$

where the first equality follows because c is trivial on K^*. Thus,

$$\zeta_t(f,c)+f(0)\int_E c(tb)db=\int_E\sum_{\alpha\in K} f(atb)c(tb)db.$$

Now, we need the following complex-analytic version of Riemann–Roch (we refer the reader to Tate's thesis for a proof):

Theorem 23.4 (Riemann–Roch)**.** *We have*

$$\sum_{\alpha\in K} f(\alpha tb)=\frac{1}{|tb|}\sum_{\alpha\in K}\hat{f}(\alpha/tb)$$

Applying Riemann–Roch, the above can be rewritten as

$$\int_E\sum_{\alpha\in K}\hat{f}(\alpha/tb)\frac{c(tb)}{|tb|}db=\int_E\sum_{\alpha\in K}\hat{f}(\alpha b/t)\frac{c(t/b)}{|t|}db,$$

where the equality follows from making the change of variables $b\mapsto b^{-1}$. Now, it is not difficult to verify that $c(t/b)/|t|=\hat{c}(b/t)$, which tells us that the above is

$$\int_E\sum_{\alpha\in K}\hat{f}(\alpha b/t)\hat{c}(b/t)db,$$

which gives us the result of the lemma. □

We next need the following lemma:

Lemma 23.5. *We have that*

$$\int_E c(tb)db = \begin{cases} Kt^s & \textit{if } c(a) = |a|^s \\ 0 & \textit{if } c|_{J_K} \neq 1. \end{cases}$$

Proof. Recall that $c(tb) = |t|^s c(b)$. Hence,

$$\int_E c(tb)db = t^s \int_E c(b)db = t^s \int_{J_K/K^*} c(b)db,$$

where $c : J_K/K^* \to S^1$. The above is

$$t^s \mathrm{vol}(J_K/K^*)$$

if $c|_{J_K} = 1$ and 0 otherwise. Also, $\mathrm{vol}(J_K/K^*) = \kappa$. For a proof of this last statement, see Marcus's *Number Fields.* □

We can now continue with our proof of the main theorem. We have

$$\zeta(f,c) = \int_0^1 \zeta_t(f,c)\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t} = \int_1^\infty \zeta_{1/t}(f,c)\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t},$$

and

$$\zeta_{1/t}(f,c) = \zeta_t(\hat{f},\hat{c}) + \hat{f}(0)\int_E \hat{c}(tb)db - f(0)\int_E c(b/t)db.$$

Integrating both sides of the above, we have that

$$\int_1^\infty \zeta_{1/t}(f,c)\frac{dt}{t} = \int_1^\infty \zeta_t(\hat{f},\hat{c})\frac{dt}{t} + \int_1^\infty \hat{f}(0)\int_E \hat{c}(tb)db - f(0)\int_E c(b/t)db\frac{dt}{t}.$$

If $c|_{J_K} \neq 1$, then

$$\int_1^\infty \hat{f}(0)\int_E \hat{c}(tb)db - f(0)\int_E c(b/t)db\frac{dt}{t} = 0,$$

implying that

$$\zeta(f,c) = \int_1^\infty \zeta_t(\hat{f},\hat{c})\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t}. \tag{2}$$

If $c|_{J_K} = 1$, then

$$\zeta(f,c) = \int_1^\infty \zeta_t(\hat{f},\hat{c})\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t} + \kappa\left(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}\right). \tag{3}$$

Notice that

$$\int_1^\infty \zeta_t(f,c)\frac{dt}{t} = \int_{I_K, |a|\geq 1} f(a)c(a)da$$

and $|c(a)| = |a|^\sigma$. For $\sigma' < \sigma$ and c' such that $|c'(a)| = |a|^{\sigma'}$, we have $|f(a)c'(a)| \leq |f(a)c(a)|$. The function $f(a)c'(a)$ is L^1, so for all $s \in \mathbb{C}$,

$$\int_1^\infty \zeta_t(f,c)\frac{dt}{t}$$

is holomorphic. This applied to (2) and (3) implies the analytic continuation and the functional equation. □

23.2. **Comparison with the classical theory.** Let $c : I_K \longrightarrow \mathbb{C}^*$ be a quasi-character with $c|_{K^*} = 1$. Let S be a finite set of primes that contain the infinite primes. We suppose that c is unramified outside of S. Recall that we can write $c = \prod_{\mathfrak{p}} c_{\mathfrak{p}}$. For each $\mathfrak{p} \in S$, we have

$$c_{\mathfrak{p}}(a_{\mathfrak{p}}) = \tilde{c}_{\mathfrak{p}}(a_{\mathfrak{p}})|a_{\mathfrak{p}}|_{\mathfrak{p}}^{it_{\mathfrak{p}}}$$

for $t_{\mathfrak{p}} \in \mathbb{R}$. For $\mathfrak{p} \notin S$, set

$$c^*(a) = \prod_{\mathfrak{p} \notin S} c_{\mathfrak{p}}(a_{\mathfrak{p}}),$$

and note that c^* is a character on the ideals $I \subset K$ coprime to S. Hence, c^* induces a character $\chi : \{I \subset K \mid (I,S) = 1\} \longrightarrow S^1$, and we may write

$$c(a) = \prod_{\mathfrak{p} \in S} \tilde{c}_{\mathfrak{p}}(\tilde{a}_{\mathfrak{p}})|a|_{\mathfrak{p}}^{it_{\mathfrak{p}}} \chi(\varphi_S(a)).$$

We have a corresponding function in Z: for $\mathfrak{p} \in S$ take $f_{\mathfrak{p}}$ from the local theory; for $\mathfrak{p} \notin S$, set $f_{\mathfrak{p}} = \mathbb{1}_{\mathcal{O}_K^*}$. Set $f = \prod_{\mathfrak{p}} f_{\mathfrak{p}}$, and note that $\hat{f} = \prod_{\mathfrak{p}} \hat{f}_{\mathfrak{p}}$. For $\mathfrak{p} \notin S$, we have

$$\int_{K_{\mathfrak{p}}^*} |f_{\mathfrak{p}}(a_{\mathfrak{p}})||a_{\mathfrak{p}}|_{\mathfrak{p}}^{\sigma} da_{\mathfrak{p}} = \frac{N(\mathcal{D}_{\mathfrak{p}})^{-1/2}}{1 - N(\mathfrak{p})^{-\sigma}},$$

and $\prod_{\mathfrak{p}}(1/(1 - N(\mathfrak{p})^{-\sigma}))$ is convergent for $\sigma > 1$. Thus,

$$\zeta(f,c) = \prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}(f_{\mathfrak{p}}, c_{\mathfrak{p}}).$$

For $\mathfrak{p} \notin S$, we have

$$\zeta_{\mathfrak{p}}(f_{\mathfrak{p}}, c_{\mathfrak{p}}| \cdot |_{\mathfrak{p}}^s) = \frac{N(\mathcal{D}_{\mathfrak{p}})^{-1/2}}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}.$$

Hence,

$$\zeta(f, c| \cdot |^s) = \zeta(s,\chi) \prod_{\mathfrak{p} \notin S} N(\mathcal{D}_{\mathfrak{p}})^{-1/2} \prod_{\mathfrak{p} \in S} \zeta_{\mathfrak{p}}(f_{\mathfrak{p}}, c_{\mathfrak{p}}| \cdot |_{\mathfrak{p}}^s),$$

which implies the results from before—that the Hecke ζ-function $\zeta(s,\chi)$ has analytic continuation and functional equation.