

Mathematics GR6657 Algebraic Number Theory

Assignment # 2

Benjamin Church

July 4, 2018

1. Let $G \subset H$ be a pair of locally compact (Hausdorff) abelian groups with H/G finite cyclic of order n . Consider the restriction map $r : \hat{H} \rightarrow \hat{G}$ defined by $r(\chi)(g) = \chi(g)$ for $g \in G$. Given any continuous character $\chi \in \hat{G}$ we can lift χ to one of n continuous characters in \hat{H} . Since H/G is cyclic, $H/G = \langle aH \rangle$ so any element of H can be written uniquely as $a^k g$ for some $g \in G$. Write $\chi(a) = e^{i\theta}$ for $\theta \in [0, 2\pi)$. Therefore, define the lift,

$$\tilde{\chi}_r(a^k g) = \chi(g) e^{i(2\pi r + \theta)k/n}$$

This character is well-defined because $a^n \in G$ but,

$$\begin{aligned} \tilde{\chi}_r(a^{k+zn} g) &= \chi(g) e^{i(2\pi r + \theta)(k+zn)/n} = \chi(g) e^{i(2\pi r + \theta)k/n} e^{i(2\pi r + \theta)z} = \chi(g) e^{i\theta z} e^{i(2\pi r + \theta)k/n} \\ &= \chi(g) \chi(a^n)^z e^{i(2\pi r + \theta)k/n} = \chi(a^{nz} g) e^{i(2\pi r + \theta)k/n} = \tilde{\chi}_r(a^k a^{zn} g) \end{aligned}$$

We must show that this character is a continuous homomorphism. Take $h_1 = a^{k_1} g_1$ and $h_2 = a^{k_2} g_2$ then $h_1 h_2 = a^{k_1+k_2} g_1 g_2$ because H is abelian. Then,

$$\tilde{\chi}_r(h_1 h_2) = \chi(g_1 g_2) e^{i(2\pi r + \theta)(k_1+k_2)/n} = \chi(g_1) e^{i(2\pi r + \theta)k_1/n} \chi(g_2) e^{i(2\pi r + \theta)k_2/n} = \tilde{\chi}_r(h_1) \tilde{\chi}_r(h_2)$$

Furthermore, let $U \subset S^1$ be open. I claim that,

$$\tilde{\chi}_r^{-1}(U) = \bigcup_{k=0}^{n-1} a^k \cdot \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U)$$

To prove this claim, suppose that $h \in \tilde{\chi}_r^{-1}(U)$ with $h = a^k g$ then,

$$\tilde{\chi}_r(a^k g) = \chi(g) e^{i(2\pi r + \theta)k/n} \in U \implies \chi(g) \in e^{-i(2\pi r + \theta)k/n} \cdot U \implies g \in \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U)$$

and thus, $h = a^k \chi(g) \in a^k \cdot \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U)$ so h is an element of the RHS. Conversely, suppose,

$$h \in \bigcup_{k=0}^{n-1} a^k \cdot \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U)$$

Then for some k , we know that,

$$h \in a^k \cdot \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U) \implies a^{-k} h \in \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U) \implies e^{i(2\pi r + \theta)k/n} \chi(a^{-k} h) \in U$$

but $\chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U) \subset G$ so $a^{-k} h = g$ and therefore, $h = a^k g$ which implies that $\tilde{\chi}_r(h) = e^{i(2\pi r + \theta)k/n} \chi(a^{-k} h) \in U$ so $h \in \tilde{\chi}_r^{-1}(U)$. Thus, we have proven the claim. However,

$$\tilde{\chi}_r^{-1}(U) = \bigcup_{k=0}^{n-1} a^k \cdot \chi^{-1}(e^{-i(2\pi r + \theta)k/n} \cdot U)$$

is a union of open sets because $\chi^{-1}(U)$ is open by continuity and multiplication by a group element is a homeomorphism. Thus, $\tilde{\chi}_r$ is continuous. In particular, the reduction map r is surjective because for any $\chi \in \hat{G}$ we have, $r(\tilde{\chi}_r)(g) = \tilde{\chi}_r(g) = \chi(g)$. Furthermore, we have constructed n distinct lifts of χ because $\tilde{\chi}_r(ag) = \chi(g)e^{2\pi i k/n}$ which are distinct elements of S^1 for $0 \leq k \leq n-1$. Also, if any $\tilde{\chi}$ is a lift of χ then $\tilde{\chi}(a^k g) = \tilde{\chi}(a^k)\chi(g) = \chi(g)\tilde{\chi}(a)^k$. Thus, $\tilde{\chi}$ is determined by the image of a . However, $a^n \in G$ so $\tilde{\chi}(a^n) = \tilde{\chi}(a)^n = \chi(a^n)$ so $\tilde{\chi}(a)$ is an n^{th} -root of $\chi(a^n)$ which immediately leads to the formula,

$$\tilde{\chi}_r(a^k g) = \chi(g)e^{i(2\pi r + \theta)k/n}$$

Thus, there are exactly n lifts of χ .

Consider the map $\iota : \widehat{H/G} \rightarrow \hat{H}$ given by $\iota(\chi) = \tilde{\chi}$ where $\tilde{\chi}(h) = \chi(hG)$. If $\tilde{\chi} = 1$ then take any coset hG in H which gives $\chi(hG) = \tilde{\chi}(h) = 1$ so χ is trivial. Thus, ι is an injection. Furthermore, suppose that $\tilde{\chi} \in \text{Im}(\iota)$ then $\tilde{\chi}$ is constant on G -cosets and, in particular, $\tilde{\chi}(g) = \chi(gG) = 1$ so $r(\tilde{\chi})(g) = \tilde{\chi}(g) = 1$. Thus, $\text{Im}(\iota) \subset \ker r$. Likewise, if $\tilde{\chi} \in \ker r$ then $\tilde{\chi}(g) = 1$ so if $h' \in hG$ then $\tilde{\chi}(h') = \tilde{\chi}(hg) = \tilde{\chi}(h)\tilde{\chi}(g) = \tilde{\chi}(h)$ so $\tilde{\chi}$ is constant on G -cosets. Thus, $\tilde{\chi}$ descends to a map on the quotient space $\chi : H/G \rightarrow S^1$ with the property that $\chi(hG) = \tilde{\chi}(h)$ which means that $\tilde{\chi} = \iota(\chi)$. Therefore, $\ker r \subset \text{Im}(\iota)$ and thus $\ker r = \text{Im}(\iota)$. In summary, the following sequence is exact,

$$1 \longrightarrow \widehat{H/G} \xhookrightarrow{\iota} \hat{H} \twoheadrightarrow \hat{G} \longrightarrow 1$$

2. I will follow the discussion in Ramakrishnan's book: Fourier Analysis on Number Fields (§7.5). First, we will find the volume of \mathbb{I}_K/K^\times in terms of $\mathbb{I}_{K,S}^1$ for any finite set S of places.

Lemma 0.1. *The following sequence is exact,*

$$1 \longrightarrow \mathbb{I}_{K,S}^1/(K^\times \cap \mathbb{I}_{K,S}^1) \hookrightarrow \mathbb{I}_K^1/K^\times \twoheadrightarrow \mathbb{I}_K^1/(K^\times \cdot \mathbb{I}_{K,S}^1) \longrightarrow 1$$

Proof. The natural map $\mathbb{I}_{K,S}^1/(K^\times \cap \mathbb{I}_{K,S}^1) \rightarrow \mathbb{I}_K^1/K^\times$ is a well defined injection because it is an inclusion of the restricted quotient¹. Likewise, the map $\mathbb{I}_K^1/K^\times \rightarrow \mathbb{I}_K^1/(K^\times \cdot \mathbb{I}_{K,S}^1)$ is surjective because $K^\times \subset K^\times \cdot \mathbb{I}_{K,S}^1$. It suffices to show that the image of,

$$f : \mathbb{I}_{K,S}^1/(K^\times \cap \mathbb{I}_{K,S}^1) \rightarrow \mathbb{I}_K^1/K^\times \quad \text{equals the kernel of} \quad g : \mathbb{I}_K^1/K^\times \rightarrow \mathbb{I}_K^1/(K^\times \cdot \mathbb{I}_{K,S}^1)$$

The kernel of g consists of $[K^\times \cdot \mathbb{I}_{K,S}^1]$ where the brackets denotes cosets with respect to K^\times . However, multiplication by an element of K^\times does not affect the coset. Therefore,

$$\ker g = [K^\times \cdot \mathbb{I}_{K,S}^1] = [\mathbb{I}_{K,S}^1] = \text{Im}(f)$$

□

¹If $A, H \subset G$ then $A/(H \cap A) \hookrightarrow G/H$ by $a + (H \cap A) \mapsto a + H$. This is a well-defined injection because $a \in A$ so $a \in (H \cap A) \iff a \in H$

From the above lemma,

$$\text{vol}(\mathbb{I}_K^1/K^\times) = \text{vol}(\mathbb{I}_K^1/(K^\times \cdot \mathbb{I}_{K,S}^1)) \cdot \text{vol}(\mathbb{I}_{K,S}^1/(K^\times \cap \mathbb{I}_{K,S}^1)) \quad (1)$$

However, we proved in class that $\text{vol}(\mathbb{I}_K^1/(K^\times \cdot \mathbb{I}_{K,S}^1)) = h_S$ is finite. In fact, when $S = S_\infty$ then $h_S = h_K$ the class number. In particular, we will want to consider the case where $S = S_\infty$. In that case, $K^\times \cap \mathbb{I}_{K,S_\infty}^1 = \mathcal{O}_K^\times$. This equality holds since every norm of a unit is 1 so $\mathcal{O}_K^\times \subset K^\times \cap \mathbb{I}_{K,S_\infty}^1$. Furthermore, if there were some element $x \in K^\times \cap \mathbb{I}_{K,S_\infty}^1$ with $x \notin \mathcal{O}_K^\times$ then $(x) \neq \mathcal{O}_K$ so in particular it must be a power of prime (possibly fractional) ideals and thus could not have norm 1 with respect to the valuation of any prime in its factorization. Thus, $x \in \mathcal{O}_K^\times$. Rewriting the volume formula,

$$\text{vol}(\mathbb{I}_K^1/K^\times) = h_K \cdot \text{vol}(\mathbb{I}_{K,S}^1/\mathcal{O}_K^\times) \quad (2)$$

Now, we need to define the logarithmic and regulator maps, $\lambda : \mathbb{I}_{K,S_\infty}^1 \rightarrow \mathbb{R}^{r_1+r_2}$ given by,

$$\lambda(x) = (\log |x_\nu|_\nu)_\nu$$

and its restriction to $K^\times \cap \mathbb{I}_{K,S_\infty}^1$ called the regulator map $\text{reg} : K^\times \cap \mathbb{I}_{K,S_\infty}^1 \rightarrow \mathbb{R}^{r_1+r_2}$.

Lemma 0.2. *Properties of the logarithmic map,*

- $\text{Im}(\lambda) = H = \{(t_\nu) \mid \sum_{\text{real } \nu} t_\nu + 2 \sum_{\text{complex } \nu} t_\nu = 0\}$
- $\ker \lambda = \mathbb{I}_{K,\emptyset}^1$

Proof. The first statement is clear from the fact that the domain of λ is $\mathbb{I}_{K,S_\infty}^1$. From the definition of the unit ideles,

$$\prod_{\nu \in S_\infty} |x_\nu|_\nu = 1 \quad \text{and thus} \quad \sum_{\nu \in S_\infty} \log |x_\nu|_\nu = 0$$

which sums twice over each pair of complex embeddings. Furthermore, $\lambda(x) = 0$ if and only if $|x_\nu|_\nu = 1$ for each $\nu \in S_\infty$. This is exactly the definition of $x \in \mathbb{I}_{K,\emptyset}^1$. \square

In particular, $\ker \text{reg} = K^\times \cap \mathbb{I}_{K,\emptyset}^1 = \mu_K$ because if every absolute value of x is 1 then the field norm must be 1 which implies that x is a unit on the unit circle and thus a root of unity. Also, define $w_K = |\mu_K|$ and $L = \text{reg}(\mathcal{O}_K^\times)$. Now, consider the commutative diagram,

$$\begin{array}{ccccccc} & & 1 & & 1 & & 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mu_K & \longrightarrow & \mathcal{O}_K^\times & \xrightarrow{\text{reg}} & L \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathbb{I}_{K,\emptyset}^1 & \longrightarrow & \mathbb{I}_{K,S_\infty}^1 & \xrightarrow{\lambda} & H \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathbb{I}_{K,\emptyset}^1/\mu_K & \longrightarrow & \mathbb{I}_{K,S_\infty}^1/\mathcal{O}_K^\times & \xrightarrow{\lambda_*} & H/L \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 1 & & 1 & & 1 \end{array}$$

which I claim is exact in each row and column. The columns are simply inclusions and projections onto the corresponding quotients which are trivially exact. The first row is exact because $\ker \text{reg} = \mu_K$ under the inclusion into \mathcal{O}_K^\times . The second row is exact again because $\ker \lambda = \mathbb{I}_{K,\emptyset}^1$ included into $\mathbb{I}_{K,S_\infty}^1$. The third row is exact by the snake lemma where the bottom row forms the cokernels of the downward maps and the top row of trivial groups forms the kernels of the downwards maps by the exactness of the columns. That is,

$$\begin{array}{ccccccc}
& & 1 & \longrightarrow & 1 & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mu_K & \longrightarrow & \mathcal{O}_K^\times & \xrightarrow{\text{reg}} & L \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathbb{I}_{K,\emptyset}^1 & \longrightarrow & \mathbb{I}_{K,S_\infty}^1 & \xrightarrow{\lambda} & H \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \mathbb{I}_{K,\emptyset}^1/\mu_K & \longrightarrow & \mathbb{I}_{K,S_\infty}^1/\mathcal{O}_K^\times & \xrightarrow{\lambda_*} & H/L \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 1 & & 1 & & 1
\end{array}$$

Using the properties of quotient measures, we arrive at formulas for various groups in this diagram by noting that the center group is isomorphic to the quotient of the last over the first. In particular,

$$\text{vol}(\mathbb{I}_{K,S_\infty}^1/\mathcal{O}_K^\times) = \text{vol}(\mathbb{I}_{K,\emptyset}^1/\mu_K) \cdot \text{vol}(H/L) \quad (3)$$

where $R_K = \text{vol}(H/L)$ is the regulator of K i.e. the volume of the fundamental domain H/L with respect to the quotient measure induced by λ_* . Furthermore,

$$\text{vol}(\mathbb{I}_{K,\emptyset}^1/\mu_K) = \text{vol}(\mathbb{I}_{K,\emptyset}^1) / \text{vol}(\mu_K) \quad (4)$$

where the measure on μ_K is the discrete measure so $\text{vol}(\mu_K) = |\mu_K| = w_K$ by definition. Putting equations 2, 3, and 4 together we get,

$$\text{vol}(\mathbb{I}_K^1/K^\times) = \frac{h_K}{w_K} R_K \cdot \text{vol}(\mathbb{I}_{K,\emptyset}^1) \quad (5)$$

Therefore, we have reduced the task of computing $\text{vol}(\mathbb{I}_K^1/K^\times)$ to that of computing $\text{vol}(\mathbb{I}_{K,\emptyset}^1)$ which I claim is easier.

Lemma 0.3.

$$\text{vol}(\mathbb{I}_{K,\emptyset}^1) = 2^{r_1} (2\pi)^{r_2} |d_K|^{-1/2}$$

Proof. $\mathbb{I}_{K,\emptyset}^1$ admits the product decomposition,

$$\mathbb{I}_{K,\emptyset}^1 = \prod_{\text{real } \nu} U_\nu \times \prod_{\text{complex } \nu} U_\nu \times \prod_{\text{non arch. } \nu} U_\nu$$

where U_ν denotes the subset of K_ν with absolute value 1. Ramakrishnan classifies how the Haar measure on $\mathbb{I}_{K,\emptyset}^1$ restricts to these sets:

- For real ν , the measure on $\{\pm 1\}$ is the counting measure.
- For complex ν , the measure on $S^1 \subset \mathbb{C}^\times$ is the standard Lebesgue measure.
- For non archimedean ν , the measure on \mathcal{O}_ν^\times is the standard self-dual Haar measure.

Therefore,

$$\text{vol}(U_\nu) = \begin{cases} 2 & \nu \text{ is real} \\ 2\pi & \nu \text{ is complex} \\ N(\mathcal{D}_\nu)^{-1/2} & \nu \text{ is non archimedean} \end{cases} \quad (6)$$

where \mathcal{D}_ν is the different for the place ν . Then, using the fact that,

$$|d_K| = \prod_{\text{non arch. } \nu} N(\mathcal{D}_\nu) \quad (7)$$

we find that the total measure becomes,

$$\text{vol}(\mathbb{I}_{K,\emptyset}^1) = 2^{r_1} (2\pi)^{r_2} |d_K|^{-1/2} \quad (8)$$

□

Combining the above lemma and equation 5 we arrive at the final result,

$$\text{vol}(\mathbb{I}_K^1/K^\times) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}} \quad (9)$$

3. Let K/\mathbb{Q} be a finite Galois extension with a complex embedding $\tau : K \rightarrow \mathbb{C}$ such that $\bar{\tau} \neq \tau$. Because τ is an embedding, $K \cong \tau(K)$. Therefore, we can consider the field $\mathbb{Q} \subset \tau(K) \subset \mathbb{C}$. I claim that $\tau(K)/\mathbb{Q}$ is normal. For any $\alpha \in \tau(K)$ there exists a $\beta \in K$ such that $\tau(\beta) = \alpha$. Now consider the minimal polynomial $q \in \mathbb{Q}[X]$ of α . Because $\tau(1) = 1$ we know that τ preserves \mathbb{Q} . Therefore, $q(\alpha) = q(\tau(\beta)) = \tau(q(\beta)) = 0$ so because τ is injective we know that β is a root of q . Since q is irreducible over \mathbb{Q} we know that q is the minimal polynomial of β . Because K/\mathbb{Q} is Galois, q splits in K . Therefore, the image of q must also split in $\tau(K)$. Thus, $\tau(K)/\mathbb{Q}$ is normal.

Now, for $\alpha \in \tau(K)$ take the minimal polynomial of q over \mathbb{Q} ,

$$q(X) = a_n X^n + \cdots + a_0$$

Because the coefficients are real, $\overline{q(\alpha)} = q(\bar{\alpha}) = 0$. Therefore, α is a root of q . However, $\tau(K)$ is normal over \mathbb{Q} so q splits completely in $\tau(K)$ so $\bar{\alpha} \in \tau(K)$. Therefore, complex conjugation, $\sigma : \tau(K) \rightarrow \tau(K)$ is an automorphism of $\tau(K)$. However, $\tau \neq \bar{\tau}$ so $\exists \beta \in K$ such that $\tau(\beta) \neq \bar{\tau}(\beta)$. Therefore, $\sigma \neq \text{id}$ but $\sigma^2 = \text{id}$ so σ has order 2 in the group $\text{Gal}(\tau(K)/\mathbb{Q})$. Thus, $\text{Gal}(K/\mathbb{Q}) \cong \text{Gal}(\tau(K)/\mathbb{Q})$ must have even order and thus $[K : \mathbb{Q}]$ is even.

4. Let K/\mathbb{Q} be real with $r_1 = d$ and $r_2 = 0$ and let L/K have degree two with L having complex embeddings, $r_1 = 0$ and $r_2 = d$. Take $c \in \text{Gal}(L/K)$ with $c \neq \text{id}$. By Dirichlet's unit theorem, we know that $\mathcal{O}_K^\times \cong \mathbb{Z}^{d-1} \times \mu(\mathcal{O}_K)$ and likewise, $\mathcal{O}_L^\times \cong \mathbb{Z}^{d-1} \times \mu(\mathcal{O}_L)$ because $r_1 + r_2 - 1$ is equal in both cases. Let u_1, \dots, u_{d-1} be a basis for the free abelian part of \mathcal{O}_K^\times . However, \mathcal{O}_L^\times

has free abelian part of equal rank so u_1, \dots, u_k with $k = d - 1$, must also be a basis for the units of infinite order in \mathcal{O}_L . Thus, any unit $u \in \mathcal{O}_L^\times$ can be written as,

$$u = u_1^{n_1} \cdots u_k^{n_k} \omega$$

where $\omega \in \mu(\mathcal{O}_L)$ is a root of unity in \mathcal{O}_L . However, $u_i \in \mathcal{O}_K \subset K$ so $c \in \text{Gal}(L/K)$ fixes u_i for each i . Therefore, suppose that $c(u) = u^{-1}$, then,

$$c(u) = c(u_1^{n_1} \cdots u_k^{n_k})c(\omega) = u_1^{n_1} \cdots u_k^{n_k} c(\omega) = u^{-1} = u_1^{-n_1} \cdots u_k^{-n_k} \omega^{-1}$$

In this case,

$$u_1^{2n_1} \cdots u_k^{2n_k} c(\omega) \omega = 1$$

but since $c(\omega)\omega$ has finite order and $u_1 \cdots u_k$ is a basis of a free abelian group, this implies that $n_1 = \cdots = n_k = 0$ and thus $c(\omega)\omega = 1$. Therefore, $u = \omega \in \mu(\mathcal{O}_L)$. However, L/\mathbb{Q} is a finite extension so it has a finite number of roots of unity and thus, $\mu(\mathcal{O}_L)$ is finite. However, the set of units such that $c(u) = u^{-1}$ is a subset of $\mu(\mathcal{O}_L)$ and is therefore finite.