Student seminar solutions Week 12

Exercise 1. *a)* Since $v \notin S$, the extension K/F is unramified at v.

- The invariants are $A_v^G = A_v \cap F_v = \mathcal{U}_v$.
- The map $s(G)$ acts as the norm $N_{K/F}$. A key property of unramified extensions of local fields is that the norm map on units is surjective, i.e., $N_{K_w/F_v}(\mathcal{U}_w) = \mathcal{U}_v$.

Thus, $s(G)A_v = \mathcal{U}_v = A_v^G$, which implies $\hat{H}^0(G, A_v) = 1$.

b) The index $[\ker_{A_v} s(G) : (\sigma - 1)A_v]$ represents the order of the cohomology group $H^1(G, A_v)$. By Shapiro's Lemma, $H^1(G, A_v) \cong H^1(G_w, \mathcal{U}_w)$, where G_w is the decomposition group. Consider the cohomology sequence derived from $1 \to \mathcal{U}_w \to K_w^\times \xrightarrow{v} \mathbb{Z} \to 0$. Since the extension is unramified, the valuation map on invariants $F_v^\times \to \mathbb{Z}$ is surjective. Combined with Hilbert's Theorem 90 ($H^1(G_w, K_w^\times) = 1$), the exact sequence implies that $H^1(G_w, \mathcal{U}_w) = 1$. Therefore, the index is 1.

c) Let $A = \prod_{v \notin S} A_v$. Cohomology commutes with direct products. From parts (a) and (b), we have $\hat{H}^0(G, A_v) = 1$ and $H^1(G, A_v) = 1$ for all $v \notin S$. It follows that:

$$A^G / s(G)A \cong \prod (\hat{H}^0) = 1 \implies A^G = s(G)A$$

$$\ker_A s(G) / (\sigma - 1)A \cong \prod (H^1) = 1 \implies \ker_A s(G) = (\sigma - 1)A$$

Consequently, the Herbrand quotient is $\mathcal{Q}_G(A) = 1$.

Exercise 2. *a)* Since $\mathcal{L}$ is a lattice in V, the $\mathbb{Q}$-span $\mathbb{Q}\mathcal{L}$ is dense in $V \cong \mathbb{R}^n$. Let $\{w_1, \ldots, w_r\}$ be a complete set of representatives for the orbits of S. For each i, since $\mathbb{Q}\mathcal{L}$ is dense, we can choose an element $X'_{w_i} \in \mathbb{Q}\mathcal{L}$ arbitrarily close to the basis vector X_{w_i}. Specifically, we choose X'_{w_i} such that:

$$\left\| X'_{w_i} - X_{w_i} \right\|_0 < \frac{1}{\dim V}.$$

b) First, observe that the norm $\|\cdot\|_0$ is G-invariant. That is, for any $v \in V$ and $\sigma \in G$, $\|\sigma v\|_0 = \|v\|_0$, because σ merely permutes the coefficients corresponding to the basis $\{X_w\}$.

Also, note that for any $\sigma \in G_{w_i}$, we have $\sigma(X_{w_i}) = X_{\sigma w_i} = X_{w_i}$. Now, we estimate the

distance:

$$\begin{aligned}
\left\|X''_{w_i} - X_{w_i}\right\|_0 &= \left\| \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \sigma(X'_{w_i}) - X_{w_i} \right\|_0 \\
&= \left\| \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} (\sigma(X'_{w_i}) - \sigma(X_{w_i})) \right\|_0 \\
&\leq \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \left\|\sigma(X'_{w_i} - X_{w_i})\right\|_0 \\
&= \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \left\|X'_{w_i} - X_{w_i}\right\|_0 \quad \text{(by } G\text{-invariance)} \\
&< \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \frac{1}{\dim V} = \frac{1}{\dim V}.
\end{aligned}$$

c) **Well-definedness:** We need to ensure that the definition $X''_w = \sigma(X''_{w_i})$ does not depend on the choice of σ. Suppose $\sigma w_i = \tau w_i = w$. Then $\tau^{-1}\sigma w_i = w_i$, so $\rho := \tau^{-1}\sigma \in G_{w_i}$.

We must show that X''_{w_i} is invariant under G_{w_i}. Let $\rho \in G_{w_i}$:

$$\rho(X''_{w_i}) = \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \rho\sigma(X'_{w_i}) = \frac{1}{|G_{w_i}|} \sum_{\mu \in G_{w_i}} \mu(X'_{w_i}) = X''_{w_i}.$$

Thus, $\tau^{-1}\sigma X''_{w_i} = X''_{w_i} \implies \sigma X''_{w_i} = \tau X''_{w_i}$. So X''_w is well-defined.

Why it fails for X': The element X'_{w_i} was chosen arbitrarily in $\mathbb{Q}\mathcal{L}$ near X_{w_i} and is not necessarily fixed by G_{w_i}. Thus, $\sigma X'_{w_i}$ could differ from $\tau X'_{w_i}$, making the definition ambiguous.

d) First, we show $\{X''_w\}_{w \in S}$ is a basis. For any $w \in S$, let $w = \sigma w_i$. Then:

$$\|X''_w - X_w\|_0 = \left\|\sigma(X''_{w_i}) - \sigma(X_{w_i})\right\|_0 = \left\|X''_{w_i} - X_{w_i}\right\|_0 < \frac{1}{\dim V}.$$

Since this holds for all $w \in S$, by Lemma 5.8, $\{X''_w\}_{w \in S}$ is a basis for V.

Next, regarding containment: Since $\mathcal{L}$ is preserved by G and $X'_{w_i} \in \mathbb{Q}\mathcal{L}$, any linear combination/action by G keeps the element in $\mathbb{Q}\mathcal{L}$. Thus $X''_w \in \mathbb{Q}\mathcal{L}$. To find a basis in $\mathcal{L}$, let m be the common denominator of the coefficients of all X''_w expressed in a basis of $\mathcal{L}$. Then let $Y_w = mX''_w$. Then $\{Y_w\}_{w \in S}$ is a basis for V contained in $\mathcal{L}$.

e) Let $\{Y_w\}_{w \in S}$ be the basis found in (d) (where $Y_w = mX''_w$ for some scalar m). For any $\sigma \in G$ and $w \in S$, let $w = \tau w_i$. Then $\sigma w = \sigma\tau w_i$. Using the definition from (c):

$$\sigma(Y_w) = \sigma(mX''_w) = m\sigma(\tau(X''_{w_i})) = m(\sigma\tau)(X''_{w_i}).$$

By definition, $Y_{\sigma w} = mX''_{\sigma w} = m(\sigma\tau)(X''_{w_i})$. Hence, $\sigma(Y_w) = Y_{\sigma w}$. This concludes the proof.

Exercise 3. *a)* The condition $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$ implies that $\mathfrak{m}$ is a defining modulus for the abelian extension K/F. By the definition of the conductor $\mathfrak{f}$ (as the greatest common divisor of all such moduli), we must have $\mathfrak{f} \mid \mathfrak{m}$.

Since $\mathfrak{f} \mid \mathfrak{m}$, any prime ideal $\mathfrak{p}$ that divides $\mathfrak{f}$ must also divide $\mathfrak{m}$. Consequently, if an ideal $\mathfrak{a}$ is coprime to $\mathfrak{m}$ (i.e., $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$), it is coprime to any factor of $\mathfrak{m}$, and thus coprime to $\mathfrak{f}$. Therefore, $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$.

b) The statement is true. We utilize the Artin map from Class Field Theory. Let $\psi_\mathfrak{m} : \mathcal{I}_F(\mathfrak{m}) \to \mathrm{Gal}(K/F)$ be the Artin map defined modulo $\mathfrak{m}$. By the main theorems of Class Field Theory, the kernel of this map is:

$$\ker(\psi_\mathfrak{m}) = \mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}).$$

Similarly, for the conductor $\mathfrak{f}$, the kernel of $\psi_\mathfrak{f} : \mathcal{I}_F(\mathfrak{f}) \to \mathrm{Gal}(K/F)$ is:

$$\ker(\psi_\mathfrak{f}) = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}).$$

Since $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$, the map $\psi_\mathfrak{m}$ is simply the restriction of $\psi_\mathfrak{f}$ to the subgroup $\mathcal{I}_F(\mathfrak{m})$. Therefore, the kernel of $\psi_\mathfrak{m}$ must be exactly the intersection of the kernel of $\psi_\mathfrak{f}$ with the domain $\mathcal{I}_F(\mathfrak{m})$:

$$\ker(\psi_\mathfrak{m}) = \ker(\psi_\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

Substituting the explicit forms of the kernels gives the desired equality:

$$\mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}) = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

c) Let $H_\mathfrak{m} = \mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m})$ and $H_\mathfrak{f} = \mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f})$. Consider the inclusion map $i : \mathcal{I}_F(\mathfrak{m}) \hookrightarrow \mathcal{I}_F(\mathfrak{f})$. From part (b), we established that $H_\mathfrak{m} = H_\mathfrak{f} \cap \mathcal{I}_F(\mathfrak{m})$. This implies that $H_\mathfrak{m} \subseteq H_\mathfrak{f}$.

Since $H_\mathfrak{m}$ maps to the identity in the quotient $\mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}$, the inclusion map induces a well-defined homomorphism between the quotients:

$$\varphi : \mathcal{I}_F(\mathfrak{m})/H_\mathfrak{m} \hookrightarrow \mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}.$$

The map is injective because the kernel of the map from $\mathcal{I}_F(\mathfrak{m})$ to the quotient $\mathcal{I}_F(\mathfrak{f})/H_\mathfrak{f}$ is exactly $H_\mathfrak{f} \cap \mathcal{I}_F(\mathfrak{m})$, which equals $H_\mathfrak{m}$.

d) The embedding in part (c) is **always an isomorphism** (under the assumption from (a) that $\mathfrak{m}$ is a valid modulus, i.e., $\mathfrak{f} \mid \mathfrak{m}$).

Reasoning: The Artin map $\psi_\mathfrak{f}$ induces an isomorphism:

$$\mathcal{I}_F(\mathfrak{f})/\mathcal{P}^+_{F,\mathfrak{f}} \mathrm{N}_{K/F}(\mathfrak{f}) \xrightarrow{\sim} \mathrm{Gal}(K/F).$$

Similarly, since $\mathfrak{f} \mid \mathfrak{m}$, the Artin map $\psi_\mathfrak{m}$ is surjective (by Chebotarev's Density Theorem, every conjugacy class in the Galois group contains infinitely many primes, so we can always find primes coprime to $\mathfrak{m}$ representing any $\sigma \in \mathrm{Gal}(K/F)$). Thus, it induces an isomorphism:

$$\mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} \mathrm{N}_{K/F}(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(K/F).$$

Since both the domain and codomain of the embedding φ are finite groups isomorphic to $\mathrm{Gal}(K/F)$, they have the same order. An injective homomorphism between two finite groups of the same order must be an isomorphism.

Exercise 4. *a)* We determine the Artin symbol $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)$ by analyzing the action of p on i and $\sqrt{5}$.

The action on i is determined by $p \pmod 4$:

$$\sigma_p(i) = i \iff p \equiv 1 \pmod 4, \quad \sigma_p(i) = -i \iff p \equiv 3 \pmod 4.$$

The action on $\sqrt{5}$ is determined by the Legendre symbol $\left(\frac{p}{5}\right)$:

$$\sigma_p(\sqrt{5}) = \sqrt{5} \iff p \equiv 1, 4 \pmod 5, \quad \sigma_p(\sqrt{5}) = -\sqrt{5} \iff p \equiv 2, 3 \pmod 5.$$

Combining these congruences modulo 20:

- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = 1 \iff \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1, 4 \pmod 5 \end{cases} \implies p \equiv 1, 9 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \tau \iff \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 2, 3 \pmod 5 \end{cases} \implies p \equiv 13, 17 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \sigma \iff \begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 1, 4 \pmod 5 \end{cases} \implies p \equiv 11, 19 \pmod{20}.$
- $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \sigma\tau \iff \begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 2, 3 \pmod 5 \end{cases} \implies p \equiv 3, 7 \pmod{20}.$

b) A prime p splits completely in $K/\mathbb{Q}$ if and only if its Artin symbol is the identity. From part (a), this corresponds to:

$$p \equiv 1, 9 \pmod{20}.$$

This matches the condition from Theorem 0.1, as these are precisely the primes p such that $p \equiv 1 \pmod m$ for the subfield $\mathbb{Q}(\zeta_m)$ containing K. Wait, specifically, $K \subset \mathbb{Q}(\zeta_{20})$. Primes splitting completely in $\mathbb{Q}(\zeta_{20})$ are $p \equiv 1 \pmod{20}$. However, K is a proper subfield. The primes splitting in K form the subgroup of $(\mathbb{Z}/20\mathbb{Z})^\times$ corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/K)$, which is $\{1, 9\}$.

c) Suppose $p\mathbb{Z}$ is inert in $\mathbb{Q}(i)/\mathbb{Q}$. This implies $p \equiv 3 \pmod 4$. Let $\mathfrak{P} = p\mathbb{Z}[i]$. The residue degree of $\mathfrak{P}$ over p is $f = 2$. Using the property of the Artin symbol under restriction/lifting:

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right) = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^f = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^2.$$

From part (a), if $p \equiv 3 \pmod 4$, the symbol $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)$ is either σ or $\sigma\tau$. Since $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$, the square of any element is the identity.

$$\sigma^2 = 1, \quad (\sigma\tau)^2 = 1.$$

Thus, the Artin symbol is trivial:

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right) = 1.$$

(This implies $p\mathbb{Z}[i]$ splits completely in $K/\mathbb{Q}(i)$).

d) Suppose $p\mathbb{Z}$ splits in $\mathbb{Q}(i)/\mathbb{Q}$, so $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}'$. This implies $p \equiv 1 \pmod 4$. The residue degree is $f = 1$. Thus:

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}(i)}\right) = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right)^1 = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right).$$

Since $p \equiv 1 \pmod 4$, we know from part (a) that the symbol is either 1 or τ. We distinguish the cases using the Legendre symbol $\left(\frac{p}{5}\right)$:

- If $\left(\frac{p}{5}\right) = 1$ (i.e., $p \equiv 1, 4 \pmod 5$), then the symbol is 1.
- If $\left(\frac{p}{5}\right) = -1$ (i.e., $p \equiv 2, 3 \pmod 5$), then the symbol is τ.

In terms of mod 20 congruences:

$$\left(\frac{\mathfrak{p}}{K/\mathbb{Q}(i)}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 9 \pmod{20} \\ \tau & \text{if } p \equiv 13, 17 \pmod{20} \end{cases}$$