2023 Fall — *Algebra and Number Theory 2*

SOLUTION TO PROBLEM SET 2

LECTURER: KOJI SHIMIZU

TA: WENHAN DAI

Problem 1. Prove that the multiplicative group $K^\times$ of the non-archimedean local field $K = \mathbb{F}_p(\!(t)\!)$ has a non-closed subgroup of finite index.

Solution. Since t is a uniformizer we have an isomorphism

$$K^\times \cong \mathbb{F}_p^\times \times U \times t^{\mathbb{Z}}, \qquad U = 1 + t\mathbb{F}_p[\![t]\!].$$

We first claim that the map

$$\prod_{\mathbb{Z}>0} \{0, 1, \ldots, p-1\} \longrightarrow U, \quad (a_n)_{n>0} \longmapsto \prod_{n>0} (1+t)^{a_n}$$

is a bijection of sets. To see this, note that since $\prod_{n>0}(1+t)^{a_n}$ becomes a finite product modulo $1 + t^m\mathbb{F}_p[\![t]\!]$ for every m, the infinite product converges in U, and thus the above map is well-defined. Conversely, any $f(t) \in U$ is written uniquely of the above form $\prod_{n>0}(1+t)^{a_n}$. Namely, write $f(t) = 1 + b_1^{(1)}t + b_2^{(1)}t^2 + \cdots$ with $b_i^{(1)} \in \{0, 1, \ldots, p-1\}$ and set $a_1 = b_1^{(1)}$. Then $f(t)(1+t)^{-a_1}$ is of the form $1 + b_2^{(2)}t^2 + b_3^{(2)}b^3 + \cdots$ with $b_i^{(2)} \in \{0, 1, \ldots, p-1\}$, and thus set $a_2 = b_2^{(2)}$. Repeating this gives $(a_n) \in \prod_{\mathbb{Z}>0}\{0, 1, \ldots, p-1\}$ with $\prod(1+t^n)^{a_n} = f(t)$ and the uniqueness can be seen by induction on n. Next we see that the subgroup

$$U^p := \{x^p \mid x \in U\} = 1 + t^p\mathbb{F}_p[\![t^p]\!]$$

since $x \mapsto x^p$ is a ring endomorphism of K. Regard U/U^p as an $\mathbb{F}_p$-vector space. The above claim gives an isomorphism of $\mathbb{F}_p$-vector spaces

$$\prod_{\mathbb{Z}_{>0} \backslash p\mathbb{Z}_{>0}} \mathbb{F}_p \xrightarrow{\sim} U/U^p, \quad (a_n) \longmapsto \prod_{n>0} (1+t^n)^{a_n} \bmod U^p.$$

Since $\bigoplus_{\mathbb{Z}_{>0} \backslash p\mathbb{Z}_{>0}} \mathbb{F}_p$ is a proper $\mathbb{F}_p$-vector subspace of $\prod_{\mathbb{Z}_{>0} \backslash p\mathbb{Z}_{>0}} \mathbb{F}_p$, take an $\mathbb{F}_p$-linear surjection

$$\alpha \colon \prod_{\mathbb{Z}_{>0} \backslash p\mathbb{Z}_{>0}} \mathbb{F}_p \longrightarrow \mathbb{F}_p, \qquad \operatorname{Ker}\alpha \supset \bigoplus_{\mathbb{Z}_{>0} \backslash p\mathbb{Z}_{>0}} \mathbb{F}_p.$$

Set

$$U' := \operatorname{Ker}(U \to U/U^p \xrightarrow{\alpha} \mathbb{F}_p).$$

Then U' is a subgroup of U of index p. We claim that U' is not a closed subgroup of U, equivalently, $1 + t^m\mathbb{F}_p[\![t]\!] \not\subset U'$ for every m. In fact, take $f(t) \in U \backslash U'$ and write $f(t) = \prod_{n>0}(1+t^n)^{a_n}$ as above. Then $f(t)\prod_{0<n<m}(1+t^n)^{-a_n} = \prod_{n \geqslant m}(1+t^n)^{-a_n} \in 1 + t^m\mathbb{F}_p[\![t]\!]$. Since $\prod_{0<n<m}(1+t^n)^{-a_n} \in U'$, we conclude $f(t)\prod_{0<n<m}(1+t^n)^{-a_n} \in (1 + t^m\mathbb{F}_p[\![t]\!]) \backslash U'$. Consider

$$N := \mathbb{F}_p^\times \times U' \times t^{\mathbb{Z}} \subset K^\times.$$

By construction, N is a subgroup of $K^\times$ of index p. Since $U' = N \cap U$ is not closed, N is not a closed subgroup of $K^\times$.

□

Date: December 19, 2023.

Problem 2. Let K be a non-archimedean local field with $\operatorname{char} K \neq 2$ and let $(-,-)_v \colon K^\times \times K^\times \to \{\pm 1\}$ denote the local symbol defined in the class and [Ser79, p. 208] for $n = 2$. Show that for each $a, b \in K^\times$, $(a,b)_v = 1$ if and only if there exists $x, y, z \in K$ such that $z^2 = ax^2 + by^2$.[1] (Hint: Use [Ser79, p. 208, Prop. 7(iii)].)

Solution. By [Ser79, p. 208, Prop. 7(iii)], $(a,b)_v = 1$ if and only if b is a norm in $K(\sqrt{a})/K$. Observe that the norm of $s + t\sqrt{a} \in K(\sqrt{a})$ with $s, t \in K$ is $s^2 - at^2$. So if b is a norm, write $b = s^2 - at^2$. Then $x = t,\ y = 1$, and $z = s$ satisfy $z^2 = ax^2 + by^2$. Conversely, if there exists $x, y, z \in K$ such that $z^2 = ax^2 + by^2$, set $s = z/y \in K$ and $t = x/y \in K$. Then b is the norm of $s + t\sqrt{a}$.

□

Problem 3. Let $p \geqslant 3$. For each $n \geqslant 1$, let $\mu_n := \{\zeta \in \overline{\mathbb{Q}}_p \mid \zeta^n = 1\}$.

(a) Show $\mu_{p-1} \subset \mathbb{Q}_p$.

(b) Show $\mathbb{Q}_p(\mu_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$, where $\sqrt[p-1]{-p}$ denotes a root of $x^{p-1} + p = 0$ in $\overline{\mathbb{Q}}_p$.

(c) Consider the following isomorphisms

$$\overline{\sigma}\colon (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\cong} \operatorname{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p); \quad a \longmapsto (\overline{\sigma}_a \colon \zeta_p \mapsto \zeta_p^a)$$

with $\zeta_p \in \mu_p$, and

$$\theta_0 \colon \operatorname{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times; \quad g \longmapsto g(\pi)/\pi,$$

with $\pi \in \mathbb{Z}_p[\mu_p]$ a uniformizer. Here the second map θ_0 is defined in [Ser79, p. 67, Prop. 7] and is an isomorphism since $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$ is a tamely ramified extension of degree $p-1$. Show $\theta_0 \circ \overline{\sigma} = \mathrm{id}$.

Solution. (a) Notice that all p solutions of $T^p - T$ are exactly all p elements of the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$. It follows that the primitive polynomial $T^{p-1} - 1$ splits in $\mathbb{F}_p$. On the other hand, it has derivative $(p-1)T^{p-2} \neq 0$, and hence is separable over $\mathbb{F}_p$. By Hensel's lemma [Lan94, p. 43], each root in $\mathbb{F}_p$ lifts to $\mathbb{Z}_p$ and then $T^{p-1} - 1$ splits in $\mathbb{Q}_p$. Therefore, $\mu_{p-1} \subset \mathbb{Q}_p$.

(b) We know that $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$ is a ramified extension of degree $p-1$ with ring of integers $\mathbb{Z}_p[\mu_p]$ and a uniformizer $\pi \colon \zeta_p - 1$ for a primitive p-th root of unity ζ_p. Since the image of p in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{p-1}$ is of order $p-1$, we have $[\mathbb{Q}_p(\sqrt[p-1]{-p}) : \mathbb{Q}_p] = p-1$ by Kummer theory. Hence it suffices to show $\sqrt[p-1]{-p} \in \mathbb{Q}_p(\mu_p)$. The minimal polynomial of π over $\mathbb{Q}_p$ is given by $((X+1)^p - 1)/X$, which is written of the form

$$X^{p-1} + p(a_{p-2}X^{p-2} + \cdots + a_1 X + a_0), \quad a_i \in \mathbb{Z}_p,\ a_0 = 1.$$

Consider the polynomial

$$f(X) = X^{p-1} - (a_{p-2}\pi^{p-2} + \cdots + a_1\pi + a_0) \in \mathbb{Z}_p[\mu_p][X].$$

Its image to the residue field $\mathbb{Z}[\mu_p]/(\pi) = \mathbb{F}_p$ is $X^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^\times}(X - a)$. Hence by Hensel's lemma, there exists $u \in \mathbb{Z}_p[\mu_p]$ such that $f(u) = 0$ and $u \not\equiv 0 \bmod \pi$. The latter condition implies $u \in \mathbb{Z}_p[\mu_p]^\times$. Set $\pi' = \pi/u \in \mathbb{Z}_p[\mu_p]$. By construction,

$$(\pi')^{p-1} = \frac{-p(a_{p-2}\pi^{p-2} + \cdots + a_1\pi + a_0)}{a_{p-2}\pi^{p-2} + \cdots + a_1\pi + a_0} = -p.$$

This means $\sqrt[p-1]{-p} \in \mathbb{Q}_p(\mu_p)$.

[1] This holds in a more general setup if we use the symbol $(-,-)$ instead (see [Ser79, p. 207, Remark 3]).

(c) For the computation of θ_0, we will use the uniformizer $\pi = \zeta_p - 1$ for a primitive p-th root of unity ζ_p. For $n \geqslant 1$, we compute

$$\frac{\zeta_p^n - 1}{\zeta_p - 1} = 1 + \zeta_p + \cdots + \zeta_p^{n-1} \equiv 1 \bmod \pi.$$

This implies for $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ that $\overline{\sigma}_a(\pi)/\pi = a \in (\mathbb{Z}/p\mathbb{Z})^\times$, namely, $\theta_0 \circ \overline{\sigma} = \mathrm{id}$.

□

Problem 4. Keep the assumption and notation as in Problem 3. Consider the local Artin map (reciprocity map)

$$\mathrm{Art}_p = (\ ,*/\mathbb{Q}_p)\colon \mathbb{Q}_p^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$$

with the arithmetic normalization as in [Ser79]. Write $\mathbb{Q}_p(\mu_{p^\infty}) := \bigcup_{m\geqslant 1} \mathbb{Q}_p(\mu_{p^m})$ and fix the identification

$$\mathbb{Z}_p^\times \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p); \quad a \longmapsto (\sigma_a\colon \zeta_{p^m} \mapsto \zeta_{p^m}^{a \bmod p^m}).$$

Let $u \in \mathbb{Z}_p^\times$ be a primitive $(p-1)$st root of unity (which exists by Problem 3(a)). We are going to show $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_{u^{-1}}$.

(a) Let $(-,-)_v\colon \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \mu_{p-1}$ denote the local symbol defined in the class and [Ser79, p. 208] for $n = p-1$. Show $(u,-p)_v = u$.

(b) Deduce $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)} = \overline{\sigma}_{u^{-1}}$.

(c) Show $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_{u^{-1}}$.

Solution. (a) Choose a primitive $(p-1)^2$-th root of unity $\zeta \in \overline{\mathbb{Q}}_p$ such that $\zeta^{p-1} = u$. Since $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is unramified of degree $p-1$,

$$\mathrm{Art}_{\mathbb{Q}_p}(-p)|_{\mathbb{Q}_p(\zeta)} = \mathrm{Frob}_p^{v_p(-p)} = \mathrm{Frob}_p,$$

where $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ is the pth power Frobenius map. By [Ser79, p. 208, Prop. 6], we compute

$$(u,-p)_v = \frac{\mathrm{Art}(-p)(\zeta)}{\zeta} = \frac{\mathrm{Frob}_p(\zeta)}{\zeta} = \frac{\zeta^p}{\zeta} = \zeta^{p-1} = u.$$

(b) With the notation as in Problem 3, it follows from [Ser79, p. 208, Prop. 6] and (a) that

$$\theta_0(\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)}) = \frac{\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)}(\sqrt[p-1]{-p})}{\sqrt[p-1]{-p}} = (-p,u)_v = (u,-p)^{-1} = u^{-1}.$$

By Problem 3(c), we conclude $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)} = \overline{\sigma}_{u^{-1}}$.

(c) Since $u^{p-1} = 1$, the order of $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} \in \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ divides $p-1$. However, the order of $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)}$ is $p-1$ by (b). Hence the order of $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})}$ is exactly $p-1$. By Hensel's lemma as the proof of Problem 3(a), $\mu_{p-1} \subset \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ is bijective. Hence there is a unique element of order $p-1$ in $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ whose image in $\mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ is $\overline{\sigma}_{u^{-1}}$. Since both $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})}$ and $\sigma_{u^{-1}}$ satisfy this property, we conclude $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_{u^{-1}}$.

□

Problem 5. Let $K = \mathbb{F}_p(t)$ and let $\mathbb{A}_K$ denote its adèle ring. Show that K is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K/K$ is compact (with respect to the quotient topology).

Solution. Note that $\mathbb{A}_K$ is a locally compact topological ring. For this, one can first show that $\mathbb{A}$ is a Hausdorff space. Let S be a finite subset of places containing all non-archimedean places. For any distinct $x, x' \in K$, there exists a place w such that $x_w \neq x'_w$. Since K_w is Hausdorff, there exists an open neighborhood $\mathcal{U} = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v \ni x$ and $\mathcal{U}' = \prod_{v\in S} U'_v \times \prod_{v\notin S} \mathcal{O}_v \ni x'$, such that $w \in S$ and $U_w \cap U'_w = \emptyset$, where U_v, U'_v are open subsets of K_v. It follows that $\mathcal{U} \cap \mathcal{U}' = \emptyset$. Next, since each $\mathcal{O}_v$ is a subring of K_v, the addition and multiplication on $\mathbb{A}_K$ are continuous, and hence $\mathbb{A}_K$ is a topological ring. As for local compactness, note that each $\mathcal{O}_v$ is compact, and thus each K_v is locally compact, and so also is $\mathbb{A}_K$ by Tychonoff's theorem.

We first show that the diagonal map $K \to \mathbb{A}_K,\ x \mapsto (x)_v$ makes K a discrete subring of $\mathbb{A}_K$. The diagonal map is well-defined, because each $x \in K$ lies in $\mathcal{O}_v$ for almost all places v, and then $(x)_v \in \prod'_v K_v = \mathbb{A}_K$.

Step I. Set $R \coloneqq \mathbb{F}_p[t] \subset K$. Recall that the places of K correspond exactly to the maximal ideals of R and the valuation $v_\infty \coloneqq -\deg\colon f(t)/g(t) \mapsto \deg g - \deg f$. To see this, note that the maximal ideals of R and $-\deg$ define inequivalent valuations of K. Conversely, let v be a normalized valuation of K and let R_v (resp. $\mathfrak{m}_v$) be its valuation ring (resp. maximal ideal). Then $R \cap R_v$ is a subring of R containing $\mathbb{F}_p$.

- If $R \cap R_v = \mathbb{F}_p$, then $v(t^{-1}) > 0$. For $f(t) = a_n t^n + \cdots + a_1 t + a_0 \in R$ with $a_n \neq 0$, write $f(t) = t^n(a_n + \cdots + a_1 t^{-(n-1)} + a_0 t^{-n})$. Then $v(a_n + \cdots + a_1 t^{-(n-1)} + a_0 t^{-n}) = \min\{a_n, \ldots, a_0 t^{-n}\} = v(a_n) = 0$, and thus $v(f) = nv(t)$. By the multiplicativity of v, we see $v(f/g) = (\deg g - \deg f)v(t^{-1})$ for $f, g \in R$. Since v is normalized, we conclude $v = -\deg$.
- If $\mathbb{F}_p \subsetneq R \cap R_v$, then $t \in R \cap R_v$ since R_v is integrally closed. Hence $R \subset R_v$ and $R \cap \mathfrak{m}_v$ is a nonzero prime ideal, namely, a maximal ideal of R.

Each maximal ideal of R is generated by a unique irreducible monic polynomial $P \in R$, so write $v_P\colon K \to \mathbb{Z} \cup \{\infty\}$ for the corresponding normalized valuation. Observe that if $x \in K$ satisfies $v_P(x) \geqslant 0$ for every such P, then $x \in R$.

Step II. We show that K is discrete in $\mathbb{A}_K$. Consider an open subset

$$U = \mathcal{O}_{K_{v_\infty}} \times (t\mathcal{O}_{K_{v_t}}) \times \prod_{P \neq t} \mathcal{O}_{K_{v_P}} \subset \mathbb{A}_K.$$

The preceding observation shows

$$K \cap U = \{f \in R \mid \deg f \leqslant 0,\ f \in tR\} = \{0\}.$$

Since $\mathbb{A}_K$ is a topological ring, we conclude $K \cap (x + U) = \{x\}$ for every $x \in K$ with $x + U$ open in $\mathbb{A}_K$. This means that K is discrete in $\mathbb{A}_K$.

Step III. Finally, we show that $\mathbb{A}_K/K$ is compact. Since K is a discrete subgroup of $\mathbb{A}_K$, the quotient $\mathbb{A}_K/K$ is Hausdorff. Set

$$Z = \prod_v \mathcal{O}_{K_v} \subset \mathbb{A}_K,$$

where v runs over all the places of K. Since each $\mathcal{O}_{K_v}$ compact, so is Z by Tychonoff's theorem. We claim $K + Z = \mathbb{A}_K$. For this, take any $(x_v) \in \mathbb{A}_K$. By definition, there are only finitely many v's with $v(x_v) < 0$. Let $P_1, \ldots, P_k$ be all the irreducible monic polynomials such that $v_i(x_{v_i}) < 0$ where $v_i \coloneqq v_{P_i}$. Since P_i is a uniformizer of $\mathcal{O}_{v_i}$, there exists $f_i \in R$ such that $x_{v_i} - f_i P_i^{v_i(x_{v_i})} \in \mathcal{O}_{v_i}$. Set $f = \sum_{i=1}^k f_i P_i^{v_i(x_{v_i})} \in K$. Since $P_i \in \mathcal{O}_{v_P}^\times$ for $P \neq P_i$, we see $x_{v_P} - f \in \mathcal{O}_{K_{v_P}}$ for every irreducible monic polynomial P. Consider $x_{v_\infty} - f \in K_{v_\infty} = \mathbb{F}_p(\!(t^{-1})\!)$. Choose $g \in R$ such that $x_{v_\infty} - f - g \in \mathcal{O}_{K_{v_\infty}} = \mathbb{F}_p[\![t]\!]$. Since $x_{v_P} - f - g \in \mathcal{O}_{K_{v_P}}$, we conclude $(x_v) - f - g \in Z$ with $f + g \in K$. This means $K + Z = \mathbb{A}_K$. Since $Z \mapsto \mathbb{A}_K/K$ is continuous and surjective with Z compact, we conclude that $\mathbb{A}_K/K$ is compact.

□

Problem 6. Let K be a global field and let $\mathbb{I}_K$ denote its idèle group. Show that the inverse map $\mathbb{I}_K \to \mathbb{I}_K; x \mapsto x^{-1}$ is not continuous if $\mathbb{I}_K$ is equipped with the induced topology $\mathbb{I}_K \subset \mathbb{A}_K$ from the adèle ring.

Solution. Let S_K (resp. $S_{K,\infty}$, resp. $S_{K,\mathrm{fin}}$) denote the set of places (resp. infinite places, resp. finite places) of K. Recall that the following subsets of $\mathbb{A}_K$ form an open neighborhood basis of 0:

$$U = \prod_{v\in S_{K,\infty}} U_v \times \prod_{v\in S} \mathfrak{p}_v^n \times \prod_{v\in S_{K,\mathrm{fin}}\setminus S} \mathcal{O}_{K_v},$$

where U_v is an open neighborhood of $0 \in K_v$ and $S \subset S_{K,\mathrm{fin}}$ is a finite subset. In particular, the sets of the form $V := (1+U)\cap \mathbb{I}_K$ for such U's form an open neighborhood basis of $1 \in \mathbb{I}_K$ with respect to the induced topology $\mathbb{I}_K \subset \mathbb{A}_K$. To show that the inverse map on $\mathbb{I}_K$ is not continuous with respect to the induced topology, it suffices to see that V^{-1} is not open in $\mathbb{I}_K$ with respect to the induced topology. Assume the contrary. Since $1 \in V^{-1}$, there exists an open neighborhood $U' = \prod_{v\in S_{K,\infty}} U_v \times \prod_{v\in S'} \mathfrak{p}_v^{n'} \times \prod_{v\in S_{K,\mathrm{fin}}\setminus S'} \mathcal{O}_{K_v}$ of $0 \in \mathbb{A}_K$ of the above form such that $(1+U')\cap\mathbb{I}_K \subset V^{-1}$. Take $v \in S_{K,\mathrm{fin}}\setminus(S\cup S')$ and set $x = (1,\dots,1,\pi_v,1,\dots) \in \mathbb{I}_K$, where π_v is the uniformizer of K_v placed in the v-component. Then $x \in 1+U'$ but $x^{-1} = (1,\dots,1,\pi_v^{-1},1,\dots) \notin 1+U$ since $\pi_v^{-1} \notin \mathcal{O}_{K_v}$. This shows $x \in (1+U')\cap\mathbb{I}_K\setminus V^{-1}$, and we obtain contradiction.

□

Problem 7. Recall that $K^\times$ embeds into $\mathbb{I}_K$ diagonally for every global field K.

(a) Show that $\mathbb{Q}^\times$ and $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$ generate $\mathbb{I}_\mathbb{Q}$, and $\mathbb{Q}^\times \cap (\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}) = \{1\}$.
(b) Let $K = \mathbb{Q}(\sqrt{-5})$. Show that $\mathbb{I}_K$ is not generated by $K^\times$ and $\prod_{v\in S_{K,\mathrm{fin}}} \mathcal{O}_{K_v}^\times \times \mathbb{C}^\times$.

Solution. (a) Take any $(x_v) \in \mathbb{I}_\mathbb{Q}$. By definition, there are only finitely many primes p with $v_p(x_p) \neq 0$. Hence $q' = \mathrm{sgn}(x_\infty)\cdot q' \in \mathbb{Q}^\times$, where $\mathrm{sgn}(x_\infty) = x_\infty/|x_\infty| \in \{\pm1\}$. Then by construction,

$$q\cdot(x_v) \in \prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}.$$

This means that $\mathbb{Q}^\times$ and $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$ generate $\mathbb{I}_\mathbb{Q}$. Next take $q \in \mathbb{Q}^\times$ with $q \in \prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$. Since $v_p(q) = 0$ for every prime p, we see $q \in \mathbb{Z}^\times$ must be equal to ±1. Since $q \in \mathbb{R}_{>0}$, we conclude $q = 1$, namely, $\mathbb{Q}^\times \cap \left(\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}\right) = \{1\}$.

(b) Let I_K denote the ideal group and consider

$$f\colon \mathbb{I}_K \longrightarrow I_K, \quad (x_v) \longmapsto \prod_v \mathfrak{p}_v^{v(x_v)},$$

where $\mathfrak{p}_v$ is the maximal ideal of $\mathcal{O}_K$ corresponding to the finite place v. By definition of $\mathbb{I}_K$, f is well-defined and surjective. Moreover, $\operatorname{Ker} f = \prod_{v\in S_{K,\mathrm{fin}}} \mathcal{O}_{K_v}^\times \times \mathbb{C}^\times$ and $f(K^\times)$ is the subgroup P_K of principal ideals. In particular, f induces an isomorphism

$$\frac{\mathbb{I}_K}{K^\times \prod_{v\in S_{K,\mathrm{fin}}} \mathcal{O}_{K_v}^\times \times \mathbb{C}^\times} \xrightarrow{\sim} I_K/P_K.$$

Since $(2, 1+\sqrt{-5}) \in I_K$ is not principal, $I_K/P_K \neq 0$. This means that $\mathbb{I}_K$ is not generated by $K^\times$ and $\prod_{v\in S_{K,\mathrm{fin}}} \mathcal{O}_{K_v}^\times \times \mathbb{C}^\times$.

□

Problem 8. For $n \geqslant 1$, let $\mathbb{Q}(\mu_n)$ denote the cyclotomic field generated by nth roots of unity and let $N\colon \mathbb{I}_{\mathbb{Q}(\mu_n)} \to \mathbb{I}_\mathbb{Q}$ be the norm map. Construct explicitly a group isomorphism

$$\mathbb{I}_\mathbb{Q}/(\mathbb{Q}^\times N(\mathbb{I}_{\mathbb{Q}(\mu_n)})) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times.$$

Moreover, describe the image in $(\mathbb{Z}/n\mathbb{Z})^\times$ of the following idèles:

(a) $\pi_p = (1,\dots,1,p,1,\dots,1)$ (p sits in the $\mathbb{Q}_p$-component) for $(p,n) = 1$;
(b) $c = (1,1,\dots,-1)$ (-1 sits in the $\mathbb{R}$-component and the other entries are 1).

You may use any result on the image of the local norm map $N_{\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p}\colon \mathbb{Q}_p(\mu_n) \to \mathbb{Q}_p$ as long as you state it correctly.

Solution. Set $K = \mathbb{Q}(\mu_n)$. If $n = 1, 2$, then $K = \mathbb{Q}$, and hence there exists a unique isomorphism $\mathbb{I}_{\mathbb{Q}}/(\mathbb{Q}^\times N(\mathbb{I}_{\mathbb{Q}(\mu_n)})) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$ as both are the trivial group. Assume $n \geqslant 3$ and write $n = q_1^{e_1} \cdots q_r^{e_r}$ for distinct primes with $e_i > 0$. Then K has no real places and is unramified outside $Q \coloneqq \{q_1, \ldots, q_r\}$. Let v be a place of $\mathbb{Q}$ and w a place of K above v. From what we know about $N_{K/\mathbb{Q}_p}$, we have the following.

(i) If $v = \infty$, we have

$$N_{K_w/\mathbb{R}}(K_v^\infty) = \mathbb{R}_{>0}.$$

(ii) If $v = p$ is a prime, we have

$$N_{K_w/\mathbb{Q}_p}(\mathcal{O}_{K_v}^\times) = \begin{cases} \mathbb{Z}_p^\times, & p \notin Q, \\ 1 + q_i^{e_i}\mathbb{Z}_{q_i}, & p = q_i. \end{cases}$$

By Problem 7(a), the inclusion $\prod_p \mathbb{Z}_p^\times \times 1 \to \mathbb{I}_{\mathbb{Q}}$ induces an isomorphism

$$\alpha \colon \frac{\mathbb{I}_{\mathbb{Q}}}{\mathbb{Q}^\times \prod_p 1 \times \mathbb{R}_{>0}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p^\times.$$

Under this isomorphism, we see

$$\beta \colon \mathbb{I}_{\mathbb{Q}}/(\mathbb{Q}^\times N(\mathbb{I}_{\mathbb{Q}(\mu_n)})) \xrightarrow{\sim} \prod_{p \notin Q} \mathbb{Z}_p^\times/\mathbb{Z}_p^\times \times \prod_{i=1}^{k} \mathbb{Z}_{q_i}^\times/(1 + q_i^{e_i}\mathbb{Z}_{q_i}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Let us determine the images of π_p and c under

$$\gamma \colon \mathbb{I}_{\mathbb{Q}} \longrightarrow \mathbb{I}_{\mathbb{Q}}/(\mathbb{Q}^\times N(\mathbb{I}_{\mathbb{Q}(\mu_n)})) \xrightarrow{\beta} (\mathbb{Z}/n\mathbb{Z})^\times.$$

For any place v of $\mathbb{Q}$, let $i_v \colon \mathbb{Q}_v = \mathbb{Q}_v \times \prod_{v' \neq v} 1 \hookrightarrow \mathbb{I}_{\mathbb{Q}}$ denote the inclusion. So

$$\pi_p = i_p(p), \quad c = i_\infty(-1).$$

Similarly, for any subset $S \subset S_{\mathbb{Q},\mathrm{fin}}$ of the primes, let $i_S \colon \prod_{p \in S} \mathbb{Z}_p^\times = \prod_{p \in S} \mathbb{Z}_p^\times \times \prod_{v \notin S} 1 \hookrightarrow \mathbb{I}_{\mathbb{Q}}$ denote the inclusion.

(a) For p with $(n, p) = 1$, namely, $p \notin Q$, we have

$$p = i_p(p) \cdot i_Q(p) \cdot i_{S_{\mathbb{Q},\mathrm{fin}} \setminus (Q \cup \{p\})}(p) \cdot i_\infty(p)$$

as elements of $\mathbb{I}_{\mathbb{Q}}$ since $p \in \mathbb{Z}_q^\times$ for $q \neq p$. By definition, as $p > 0$,

$$\gamma(p) = 1, \quad \gamma(i_{S_{\mathbb{Q},\mathrm{fin}} \setminus (Q \cup \{p\})}(p)) = 1, \quad \gamma(i_\infty(p)) = 1.$$

Hence

$$\gamma(\pi_p) = \gamma(i_p(p)) = \gamma(i_Q(p))^{-1} = p^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

(b) Similarly to (a),

$$-1 = i_Q(-1) \cdot i_{S_{\mathbb{Q},\mathrm{fin}} \setminus Q}(-1) \cdot i_\infty(-1),$$

and we compute

$$\gamma(c) = \gamma(i_\infty(-1)) = \gamma(i_Q(-1))^{-1} = -1 \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Note that the global Artin map

$$\mathrm{Art}_{\mathbb{Q}} \colon \mathbb{I}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

induces an isomorphism

$$\mathrm{Art}_{\mathbb{Q}(\mu_n)/\mathbb{Q}} \colon \mathbb{I}_{\mathbb{Q}}/(\mathbb{Q}^\times N(\mathbb{I}_{\mathbb{Q}(\mu_n)})) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$$

and the cyclotomic theory gives an isomorphism

$$\sigma \colon (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}), \quad a \longmapsto (\sigma \colon \zeta_n \mapsto \zeta_n^a).$$

Consider the diagram

$$\begin{array}{ccc} \mathbb{I}_{\mathbb{Q}} & \xrightarrow{\mathrm{Art}_{\mathbb{Q}}} & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \\ \Big\downarrow{\scriptstyle \gamma} & & \Big\downarrow{\scriptstyle g\mapsto g|_{\mathbb{Q}(\mu_n)}} \\ (\mathbb{Z}/n\mathbb{Z})^{\times} & \underset{\sim}{\xrightarrow{\sigma}} & \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}). \end{array}$$

By the above computation, we see this diagram is commutative if the local Artin map $\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ satisfies $\mathrm{Art}_{\mathbb{Q}_p}(p)|_{\mathbb{Q}_p^{\mathrm{ur}}} = (x \mapsto x^{-p})$ under the identification $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, namely, if one uses the geometric normalization for $\mathrm{Art}_{\mathbb{Q}_p}$.

□

References

[Lan94] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 1994.

[Ser79] Jean-Pierre Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York–Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

Qiuzhen Colledge, Shuangqing, Tsinghua University, 100084, Beijing, China
Email address: dwh23@mails.tsinghua.edu.cn