COURSEWORK FOR ALGEBRAIC NUMBER THEORY II (FALL 2023)

LECTURER — KOJI SHIMIZU
TEACHING ASSISTANT — WENHAN DAI

This document is about the course *Algebraic Number Theory II* offered by Qiuzhen College, Tsinghua University, during the Fall 2023 semester. The following contains two sheets of homework problems together with the (closed-book) final exam. All problems are proposed by the lecturer and are attached with solutions. The TA is responsible for any mistakes in this document.

CONTENTS

HOMEWORK 1

Problem 1.1. For each of the following, give one example and explains briefly why your example works.

(1) A local ring A such that its maximal ideal is generated by a non-nilpotent element but A is not a discrete valuation ring.

(2) A finite separable extension L/K of complete discrete valuation fields whose residue field extension k_L/k is not separable.

Solution. (1) We propose two remarkable examples. For the first example, we work with a natural object in p-adic geometry.

(a) Let C be an algebraically closed complete p-adic field with residue field $\overline{\mathbb{F}}_p$ (for example, C can be the p-adic completion of $\overline{\mathbb{Q}}_p$). Let v be the normalized p-adic valuation on C and write $\mathcal{O}_C$ for the ring of integers of C. Fix a real number $0 < r < 1$ such that $r = v(\pi)$ for some $\pi \in \mathcal{O}_C$. Consider the ideal

$$I \coloneqq \{x \in \mathcal{O}_C \colon v(x) \geqslant r\} \subset \mathcal{O}_C.$$

We take $A \coloneqq \mathbb{Z}_p + I$. Then A is a ring and I is an ideal of A. Since both $\mathbb{Z}_p$ and I are complete and I is characterized by the closed condition $v(\pi) \geqslant r$, A is closed complete in $\mathcal{O}_C$.

We verify that A satisfies the desired local properties as follows. For this, we first claim that I is a maximal ideal of A. Indeed, we have natural maps $A \to \mathcal{O}_C$ and $\mathcal{O}_C \to \overline{\mathbb{F}}_p$. Let $f \colon A \to \overline{\mathbb{F}}_p$ be their composite. Then from the construction $f(I) = 0$ and $f(\mathbb{Z}_p) = \mathbb{F}_p$. It follows that the surjection $A \twoheadrightarrow \mathbb{F}_p$ has kernel equal to I. Thus

$$A/I = (\mathbb{Z}_p + I)/I \simeq \mathbb{F}_p,$$

which proves our claim. Further, note that each $x \in A - I$ must satisfy $v(x) = 0$, and is thus invertible. So I is the unique maximal ideal of A.

Then A is a local ring; its unique maximal ideal I is generated by the non-nilpotent element $\pi \in \mathcal{O}_C$. Clearly, $v(A)$ is not discrete in $\mathbb{R}_{\geqslant 0} \cup \{\infty\}$.

Last updated on January 3, 2024.

For another example, recall that each discrete valuation ring is by definition a noetherian local ring. It is thus natural to consider dropping the noetherian condition and create a localization.

(b) Consider the ring

$$R = \mathbb{Z}[X_1, X_2, \ldots]$$

with infinitely many variables. Fix a prime $p \in \mathbb{Z}$. Then (p) is a principal prime ideal in R. We can localize R at (p) to get

$$A \coloneqq R_{(p)} = (R - (p))^{-1}R = \{f/g \in \mathbb{Z}(X_1, X_2, \ldots) \colon p \nmid g\}.$$

Clearly, A is a local ring. We verify other desired properties on A. By a property of localization, the maximal ideal of A is $pR_{(p)}$, generated by one non-nilpotent element $p \in R_{(p)}$. On the other hand, let $\varphi\colon R \to A,\ r \mapsto r/1$ be the natural localization map. Notice that in R each ideal in the infinite strictly ascending chain $p(X_1) \subsetneq p(X_1, X_2) \subsetneq \cdots$ is contained in pR. So $\varphi((pX_1)) \subsetneq \varphi((pX_1, pX_2)) \subsetneq \cdots$ is also an infinite strictly ascending chain of ideals in A. It follows that A is not noetherian.

There could also be other examples at work. But note that (a) and (b) above reveal the two essential points that A fails to be a discrete valuation ring under our assumption.

(2) Over the local function field $\mathbb{F}_p(\!(t)\!)$, the ring of Laurent power series

$$K = \mathbb{F}_p(\!(t)\!)(\!(T)\!)$$

is a complete discrete valuation field. Its ring of integers and its residue field are respectively $\mathcal{O}_K = \mathbb{F}_p(\!(t)\!)[\![T]\!]$ and $k = \mathbb{F}_p(\!(t)\!)$. Consider the polynomial

$$f(X) = X^p + TX - t \in \mathcal{O}_K[X].$$

We make the following observations:

(i) After modulo T, we have $f(X) \equiv X^p - t \in k[X]$, where k is a complete discrete valuation ring with uniformizer t. Then $X^p - t$ is irreducible by the Eisenstein criterion.

(ii) By computing the derivative $f'(X) = T \neq 0$, we see $f(X)$ is separable over K.

Thus, $L \coloneqq K[X]/(f(X))$ is a finite separable extension of K. Then L is also a discrete valuation field, complete with respect to the induced topology from K, with the residue field

$$k_L = k[X]/(\overline{f}(X)) = \mathbb{F}_p(\!(t)\!)[X]/(X^p - t) = k(t^{1/p}).$$

Consequently, $k_L/k = k(t^{1/p})/k$ is not separable, because the minimal polynomial $\overline{f}(X) = X^p - t$ satisfies $\overline{f}'(X) = 0$ over k. □

Problem 1.2. Let K be a field. A *non-trivial non-archimedean absolute value* on K is a function $|\cdot|\colon K \to \mathbb{R}_{\geqslant 0}$ satisfying for $x, y \in K$: (i) $|xy| = |x| \cdot |y|$; (ii) $|x + y| \leqslant \max\{|x|, |y|\}$; (iii) $|x| = 0$ if and only if $x = 0$; (iv) $|K| \supsetneq \{0, 1\}$. An absolute value defines a topology on K in a usual way. Now let $|\cdot|_1$ and $|\cdot|_2$ be two non-trivial non-archimedean absolute values on K. Show that they give the same topology if and only if there exists $\rho > 0$ such that $|x|_2 = |x|_1^\rho$ for every $x \in K$.

Solution. Suppose $|\cdot|_2 = |\cdot|_1^\rho$ for $\rho > 0$. For $i = 1, 2$, the neighborhood base of the topology induced by $|\cdot|_i$ consists of open neighborhoods of 0 of form

$$\{x \in K \colon |x - y|_1 < r\} = \{x \in K \colon |x - y|_2 < r^\rho\}$$

for all $0 < r \ll 1$ (and, alternatively, $0 < r^\rho \ll 1$), as well as their translates. So $|\cdot|_1$ and $|\cdot|_2$ give the same topology, which proves the "if" part.

As for the "only if" part, since $x^n \to 0$ if and only if $|x|_i < 1$ for $i = 1, 2$, we see

$$\{x \colon |x|_1 < 1\} = \{x \colon |x|_2 < 1\}.$$

As $|\cdot|_1$ is nontrivial, we can fix some $y \in K$ so that $|y|_1 > 1$. Set $\rho \coloneqq \log|y|_2/\log|y|_1$. We aim to show that $|x|_1^\rho = |x|_2$ for every $x \in K$. Indeed, if we have $m, n \in \mathbb{Z}_{\geqslant 1}$ such that $n/m > s = \log|x|_1/\log|y|_1$, then $|y|_1^{n/m} > |y|_1^s = |x|_1$ holds, which further implies $|x^m/y^n|_1 < 1$; in this case, by assumption

$|x^m/y^n|_2 < 1$ as well, and hence $|x|_2 < |y|_2^{n/m}$. Notice that this argument holds for arbitrary $n/m \in \mathbb{Q}$, so we deduce that

$$|y|_2^s \geqslant |x|_2$$

for any $s \in \mathbb{R}_{>0}$. Similarly, we also have $|y|_2^s \leqslant |x|_2$. Combining these, the equality holds and

$$|y|_1^\rho = |x|_1^{\rho/s} = |x|_2^{1/s} = |y|_2.$$

Therefore, we have proved $|x|_1^\rho = |x|_2$ for arbitrary $x \in K$. □

Problem 1.3. Let K be a complete discrete valuation field with valuation v and let L/K be a finite field extension of degree n. Then we showed that L admits a unique valuation w such that $w|_K = v$ (here we normalize so that w prolongs v with index 1, not index $e_{L/K}$).

This exercise outlines another proof of this result by an explicit formula. Define $w\colon L \to \mathbb{R} \cup \{\infty\}$ by

$$w(x) = \frac{1}{n} v(N_{L/K}(x)) \quad (x \in L).$$

It is easy to see w is non-trivial, $w|_K = v$, and $w(xy) = w(x) + w(y)$. We are going to show

$$w(x+y) \geqslant \min\{w(x), w(y)\} \quad \text{for} \quad x, y \in L.$$

Note that the uniqueness of the prolonged norm follows from the property of topological vector spaces as we saw in the class.

(1) Show that it suffices to prove, for $x \in L$, $w(x) \geqslant 0$ implies $w(x+1) \geqslant 0$.
(2) Take any $x \in L$ with $w(x) \geqslant 0$. Show $w(x+1) \geqslant 0$.

Solution. Denote A and B the valuation rings of K and L, respectively.

(1) Note that $w(ab) = w(a) + w(b)$ for all $a, b \in L$. Given $y, z \in L$, we may assume without loss of generality that $w(y) \geqslant w(z)$, which implies $w(yz^{-1}) \geqslant 0$. In this case, the desired inequality is equivalent to

$$w(y+z) \geqslant \min\{w(y), w(z)\} = w(z).$$

Further, through dividing by z on both variables, this becomes

$$w(yz^{-1} + 1) \geqslant 0.$$

By taking $x = yz^{-1} \in L$, it suffices to show that $w(x) \geqslant 0$ implies $w(x+1) \geqslant 0$.

(2) Fix $x \in L$ satisfying $w(x) \geqslant 0$. Then we have $x \in B$. Let $f(X) = X^m + \cdots + a_1 X + a_0 \in K[X]$ be the minimal polynomial of x over K, with degree $m = [K(x) : K]$ dividing $n = [L : K]$.

To compute $N_{L/K}(x)$, let $\alpha_1, \ldots, \alpha_m$ be all m roots of $f(X)$ in the algebraic closure of K. So we have $(X - \alpha_1) \cdots (X - \alpha_m) = X^m + \cdots + a_1 X + a_0$. Comparing the coefficients we obtain $(-1)^m (\alpha_1 \cdots \alpha_m) = a_0$. Thus, by definition of norm,

$$N_{L/K}(x) = (\alpha_1 \cdots \alpha_m)^{n/m} = ((-1)^m a_0)^{n/m} = (-1)^n a_0^{n/m}.$$

It follows from $w(x) \geqslant 0$ that $v(N_{L/K}(x)) \geqslant 0$, and hence $v(a_0) \geqslant 0$, namely $a_0 \in A$. Observe that $f(X-1)$ is the minimal polynomial of $x+1$.

If $a_1, \ldots, a_m \in A$, then the constant term of $f(X-1)$ lies in A, which further implies $w(x+1) \geqslant 0$. So it boils down to showing $f(X) \in A[X]$. Choose a uniformizer ϖ of A and write $A/(\varpi)$ for the residue field. Then there exists some integer $r \geqslant 0$ such that $g(X) := \varpi^r f(X) \in A[X]$, and along the modulo ϖ quotient map $A[X] \to (A/(\varpi))[X]$ the image $\bar{g}(X)$ of $g(X)$ is nonzero.

Assume $r \geqslant 1$ for the sake of contradiction. In this case $\bar{g}(X)$ has a zero constant term. Hence we can write $\bar{g}(X) = X^s \overline{h}(X)$ for some $s \geqslant 1$. Note that $g(X)$ is primitive. By Hensel's lemma [Lan94, p.43] there are lifts $t(X), h(X) \in A[X]$ of $X^s, \overline{h}(X)$ such that $g(X) = t(X)h(X)$. So $g(X)$ must be reducible, which contradicts the irreducibility of $f(X)$. It then forces $r = 0$ and $f(X) \in A[X]$. It thus follows that $x \in B$, and hence $x + 1 \in B$. Therefore,

$$w(x+1) = \frac{1}{n} v(N_{L/K}(x+1)) \geqslant 0.$$

This completes the proof. □

Problem 1.4 (Conductor, [Ser79, p.53, Exercise])**.** Let C be a subring of B containing A, and having the same field of fractions as B.

(1) Show that among all the ideals of B contained in C, there is a largest one, and that it is the annihilator of the C-module B/C; it is denoted $\mathfrak{f}_{C/B}$, the *conductor* of B in C.
(2) Show that $\mathfrak{f}_{C/B} = (B^* : C^*)$, i.e., that $\mathfrak{f}_{C/B}$ is the set of all $x \in L$ such that $xC^* \subset B^*$.
(3) Suppose that C^*, considered as a fractional C-ideal, is invertible; let $\mathfrak{c}$ be its inverse (so that $\mathfrak{c}C^* = C$). Deduce from part (2) the formula
$$\mathfrak{f}_{C/B} = \mathfrak{c} \cdot \mathfrak{D}_{B/A}^{-1}.$$

Solution. Let K and L be the fields of fractions of A and B, respectively. By assumption L is also the field of fraction of C.

(1) Let $I \subset B$ be an ideal such that $I = I \cdot B \subset C$. Then
$$\mathrm{Ann}_C(B/C) = \{b \in B \colon bB \subset C\} \supset I.$$
Since $\mathrm{Ann}_C(B/C)$ is an ideal of C, it is the largest ideal $\mathfrak{f}_{C/B}$ with the desired property.

(2) For each $x \in \mathfrak{f}_{C/B}$ we have $bx \in C$ for every $b \in B$. Thus, for each $c^* \in C^*$,
$$\mathrm{Tr}_{L/K}((bx)c^*) = \mathrm{Tr}_{L/K}(b(xc^*)) \in B.$$
It follows that $xc^* \in B^*$ and then $xC^* \subset B^*$, which implies $\mathfrak{f}_{C/B} \subset (B^* : C^*)$. Conversely, take any $x \in (B^* : C^*)$ and we have $xC^* \subset B^*$. So
$$\mathrm{Tr}_{L/K}(C^*(xB)) = \mathrm{Tr}_{L/K}((xC^*)B) \subset \mathrm{Tr}_{L/K}(B^*B) \subset A.$$
Therefore, $xB \subset C$ and $x \in \mathfrak{f}_{C/B}$. This proves $\mathfrak{f}_{C/B} = (B^* : C^*)$.

(3) Using part (2) together with the relation $\mathfrak{c}C^* = C$, we see the following are equivalent:
$$x \in \mathfrak{f}_{C/B} \iff xC^* \subset B^* \iff x\mathfrak{c}^{-1} \subset \mathfrak{D}_{B/A}^{-1} \iff x \in \mathfrak{c} \cdot \mathfrak{D}_{B/A}^{-1}.$$
This proves $\mathfrak{f}_{C/B} = \mathfrak{c} \cdot \mathfrak{D}_{B/A}^{-1}$. □

Problem 1.5 (Structure of separable closures, [Ser79, p.71, Exercise 2])**.** Suppose that $\overline{K}$ is a perfect field.[1] Let K_{s} be the separable closure of K, and let $G = \mathrm{Gal}(K_{\mathrm{s}}/K)$ be its Galois group. Let G_0 and G_1 be the inertia subgroup and the wild inertia subgroup in G, respectively.

(1) Let $\overline{K}_{\mathrm{s}}$ be the separable closure of $\overline{K}$. Show that $G/G_0 = \mathrm{Gal}(\overline{K}_{\mathrm{s}}/\overline{K})$.
(2) For every integer $n \geqslant 1$, let μ_n be the group of n-th roots of unity in $\overline{K}_{\mathrm{s}}$. If m divides n, let $f_{mn} \colon \mu_n \to \mu_m$ be the homomorphism $x \mapsto x^{n/m}$, and let μ be the projective limit of the system (μ_n, f_{mn}). Show that G_0/G_1 is (canonically) isomorphic to μ. Deduce that it is (non-canonically) isomorphic to the product $\prod \mathbb{Z}_\ell$ of the groups of ℓ-adic integers, ℓ running through the set of primes distinct from the characteristic of $\overline{K}$. Show that the isomorphism $G_0/G_1 = \mu$ is compatible with the operations of G/G_0 on G_0/G_1 and on μ.
(3) Deduce from the above the structure of the group G/G_1 when $\overline{K}$ is a finite field.

Solution. For every finite Galois extension L/K in K_{s}, write $G'_L \coloneqq \mathrm{Gal}(L/K)$.

(1) By [Ser79, p.71, Exercise 1], we have $G_0 = \varprojlim_L G'_{L,0}$ under the identification $G = \varprojlim_L G'_L$, where both limits are taken over all finite Galois extensions L/K in K_{s}. In particular, we see
$$K_{\mathrm{s}}^{G_0} = \bigcup_L L^{G'_{L,0}}.$$
Since $G'_{L,0}$ is the inertia subgroup for L/K, $L^{G'_{L,0}}$ is the maximal unramified extension of K inside L. It follows that $K_{\mathrm{s}}^{G_0}$ is the maximal unramified extension K_{ur} of K (in K_{s}). Hence $G/G_0 = \mathrm{Gal}(K_{\mathrm{s}}^{G_0}/K) = \mathrm{Gal}(K_{\mathrm{ur}}/K) = \mathrm{Gal}(\overline{K}_{\mathrm{s}}/\overline{K})$ by [Ser79, p.54, Corollary 1].

(2) We use the notation p that $p = \mathrm{char}\,\overline{K}$ if $\mathrm{char}\,\overline{K} > 0$, and $p = 1$ if $\mathrm{char}\,\overline{K} = 0$. So the product in the problem is written as $\prod_{\ell \neq p} \mathbb{Z}_\ell$. We start with the following two observations.

[1] Unlike the modern notations, in Problem 1.5 we assume K is a local field and denote $\overline{K}$ its residue field (rather than the algebraically closure).

- For each $n \geqslant 1$, if we write $n = mn'$ with m a power of p and $(m, n') = 1$, we have $\mu_n = \mu_{n'}$. In particular, μ is the project limit of the system $(\mu_n, f_{mn})_{(n,p)=1}$. Moreover, if $(n, p) = 1$, we can identify $\mu_n = \mu_n(\overline{K}_{\mathrm{s}})$ with $\mu_n(K_{\mathrm{ur}})$ by Hensel's lemma.[2]
- Let M be a finite extension of K_{ur} and let $u \in \mathcal{O}_M$ be a unit. Then for each $n \geqslant 1$ with $(n, p) = 1$, there exists $\alpha \in \mathcal{O}_M$ such that $\alpha^n = u$; to show this, since the residue field of M is separably closed, the polynomial $X^n - u$ has a (simple) root in the residue field, and every such root lifts to a root of $X^n - u$ in $\mathcal{O}_M$ by Hensel's lemma (as in the footnote of the preceding paragraph).

Now we are ready to tackle with the three tasks in (2) through the following steps.

Step I. We first construct the canonical isomorphism between G_0/G_1 and μ. As in part (1),

$$K_{\mathrm{s}}^{G_1} = \bigcup_L L^{G'_{L,1}},$$

where L runs over all finite Galois extensions L/K in K_{s}. Fix such L and write $L_1 = L^{G'_{L,1}}$. Note that L_1 is the maximal tamely ramified extension of K inside L, and thus the ramification index for $L^{G'_{L,1}}/K$, say m, is prime to $\operatorname{char} \overline{K}$. It follows that the composite $K_{\mathrm{ur}}L_1$ is a finite tamely ramified extension over K_{ur} of degree m. We claim

$$K_{\mathrm{ur}}L_1 = K_{\mathrm{ur}}(\varpi_K^{1/m})$$

for any uniformizer ϖ_K of K. In fact, take any uniformizer ϖ_K of K and ϖ' of L_1, respectively. Then $K_{\mathrm{ur}}L_1 = K_{\mathrm{ur}}(\varpi')$ and $u \coloneqq \varpi_K/\varpi'^m$ is a unit of $\mathcal{O}_{K_{\mathrm{ur}}L_1}$. Since $(m, p) = 1$, the second observation at the beginning implies that there exists $\alpha \in \mathcal{O}_{K_{\mathrm{ur}}L_1}$ such that $\alpha^m = u$. In particular, $\alpha\varpi'$ gives an m-th root of ϖ_K and $K_{\mathrm{ur}}L_1 = K_{\mathrm{ur}}(\varpi') = K_{\mathrm{ur}}(\varpi_K^{1/m})$.

Moreover, since $X^a - \varpi_K$ has no root in K_{ur} for every $a > 1$, the Kummer theory gives an isomorphism of groups

$$\mathrm{Gal}(K_{\mathrm{ur}}(\varpi_K^{1/m})/K) \xrightarrow{\sim} \mu_m(K_{\mathrm{ur}}), \quad g \longmapsto g(\varpi_K^{1/m})/\varpi_K^{1/m}$$

that is independent of the choice of a uniformizer ϖ_K and an m-th root $\varpi_K^{1/m}$. By considering finite Galois extensions containing $K(\varpi_K^{1/m})$ for $(m, p) = 1$, we conclude

$$K_{\mathrm{s}}^{G_1} = \bigcup_{(m,p)=1} K_{\mathrm{ur}}(\varpi_K^{1/m}).$$

It follows that, there are canonical isomorphisms

$$G/G_0 = \mathrm{Gal}(K_{\mathrm{s}}^{G_1}/K_{\mathrm{ur}}) = \varprojlim_{(m,p)=1} \mathrm{Gal}(K_{\mathrm{ur}}(\varpi_K^{1/m})/K_{\mathrm{ur}}) = \varprojlim_{(m,p)=1} \mu_m(K_{\mathrm{ur}}) = \mu,$$

where we have combined the result before with the canonical isomorphisms $\mathrm{Gal}(K_{\mathrm{ur}}(\varpi_K^{1/m})/K) \cong \mu_m(K_{\mathrm{ur}}) \cong \mu_m$. In the last equality above, we used the first observation at the beginning and an easy comparison of the transition maps. Note that $K_{\mathrm{t}} \coloneqq K_{\mathrm{s}}^{G_1}$ is the maximal tamely ramified extension and the above argument (together with [Ser79, p.89, Lemma 6]) shows that every finitely tamely ramified extension of K_{ur} is of the form $K_{\mathrm{ur}}(\varpi_K^{1/m})$ for a uniformizer ϖ_K of K and $(m, p) = 1$.

Step II. We then describe G_0/G_1 in terms of the product of $\mathbb{Z}_\ell$'s. For each prime $\ell \neq p$, fix a compatible system $(\zeta_\ell, \zeta_{\ell^2}, \zeta_{\ell^3}, \ldots)$ where each ζ_{ℓ^n} is a primitive ℓ^n-th root of unity satisfying $(\zeta_{\ell^{n+1}})^\ell = \zeta_{\ell^n}$. For each integer r with $(r, p) = 1$, write $r = \prod_{i=1}^t \ell_i^{k_i}$ for distinct primes $\ell_i \neq p$ and $k_i \in \mathbb{Z}_+$, and set

$$\zeta_r = \prod_{i=1}^t \zeta_{\ell_i^{k_i}}.$$

[2] Since $\mathcal{O}_{K_{\mathrm{ur}}}$ is the direct limit of $\mathcal{O}_{K'}$'s for finite unramified extensions K'/K and each $\mathcal{O}_{K'}$ is complete, Hensel's lemma also holds for $\mathcal{O}_{K_{\mathrm{ur}}}$. By a similar argument, Hensel's lemma holds for $\mathcal{O}_M$ for every finite extension M of K_{ur} (see also [Ser79, p.89, Lemma 6]).

Then ζ_r is a generator of the cyclic group μ_r and $\zeta_r^{r/r'} = \zeta_{r'}$ for every r' dividing r. Hence these choices $\{\zeta_r\}_{(r,p)=1}$ give isomorphisms

$$\mu_r \cong \mathbb{Z}/r\mathbb{Z} \cong \mathbb{Z}/\ell_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell_t^{k_t}\mathbb{Z}$$

that are compatible with transition maps when r varies. Therefore,

$$G_0/G_1 \cong \mu \simeq \varprojlim_{(r,p)=1} (\mathbb{Z}/\ell_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell_t^{k_t}\mathbb{Z}) = \prod_{\ell \neq p} \mathbb{Z}_\ell.$$

Here the second isomorphism is non-canonical as it depends on choices of primitive roots of unity.

Step III. Now it remains to check the compatibility under the G/G_0-action. Indeed, for any $\sigma \in G/G_0$ and $g \in G_0/G_1$, the action of σ on g is defined as $\sigma.g = \sigma g \sigma^{-1}$. With the notation in Step I, note that $\sigma^{-1}(\varpi_K)^{1/m}$ is an m-th root of ϖ_K, and thus $g(\sigma^{-1}(\varpi_K^{1/m}))/\sigma^{-1}(\varpi_K^{1/m}) = g(\varpi_K^{1/m})/\varpi_K^{1/m}$. Hence we compute

$$\frac{\sigma g \sigma^{-1}(\varpi_K^{1/m})}{\varpi_K^{1/m}} = \frac{\sigma\big(g(\varpi_K^{1/m})\sigma^{-1}(\varpi_K^{1/m})\big)}{\sigma(\varpi_K^{1/m})} \cdot \frac{1}{\varpi_K^{1/m}} = \sigma\Big(\frac{g(\varpi_K^{1/m})}{\varpi_K^{1/m}}\Big).$$

Since $g(\varpi_K^{1/m})/\varpi_K^{1/m}$ is an m-th root of unity, this equality yields the desired compatibility by taking the inverse limit over m with $(m,p) = 1$.

(3) Since $\overline{K}$ is a finite field, write $\overline{K} = \mathbb{F}_q$ for some p-power integer q. By part (1) we have

$$G/G_0 \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}},$$

where the topological generator $1 \in \hat{\mathbb{Z}}$ corresponds to the arithmetic Frobenius $\sigma\colon x \mapsto x^q$ in $G/G_0 = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Using the compatibility of part (2)(iii), the action of G/G_0 on G_0/G_1 is defined by the group homomorphism $\varphi\colon G/G_0 \to \mathrm{Aut}(G_0/G_1)$; this can be determined by the image of σ, which sends any $g \in G_0/G_1$ to g^q, because σ acts on $\mu_m = \mu_m(\overline{\mathbb{F}}_q)$ by the q-th power map and thus

$$\frac{\sigma g \sigma^{-1}(\varpi_K^{1/m})}{\varpi_K^{1/m}} = \sigma\Big(\frac{g(\varpi_K^{1/m})}{\varpi_K^{1/m}}\Big) = \Big(\frac{g(\varpi_K^{1/m})}{\varpi_K^{1/m}}\Big)^q = \frac{g^q(\varpi_K^{1/m})}{\varpi_K^{1/m}}.$$

This gives the semi-direct product

$$G/G_1 = (G/G_0) \ltimes_\varphi (G_0/G_1) \simeq \hat{\mathbb{Z}} \ltimes \prod_{\ell \neq p} \mathbb{Z}_\ell,$$

for which $1 \in \hat{\mathbb{Z}}$ acts on $\prod_{\ell \neq p} \mathbb{Z}_\ell$ by multiplication-by-q.

To summarize, if we assume $\overline{K}$ is finite, then we have the following tower.

$$\begin{tikzcd}
K_{\mathrm{s}} \arrow[d, dash, "G_1\ (\text{pro-}p\ \text{wild inertia})"] \arrow[dd, dash, bend right=60, "G_0"'] \\
K_{\mathrm{t}} = \bigcup_{(m,p)=1} K_{\mathrm{ur}}(\varpi_K^{1/m}) \arrow[d, dash, "\mu"] \\
K_{\mathrm{ur}} = \bigcup_{(m,p)=1} K(\mu_m) \arrow[d, dash, "\hat{\mathbb{Z}}"] \\
K
\end{tikzcd}$$

In the picture, K_{ur} (resp. K_{t}) is the maximal unramified (resp. tamely ramified) extension of K in K_{s}. □

Problem 1.6 (Artin–Schreier extension, [Ser79, p.72, Exercise 5]). Let e_K be the absolute ramification index of K, and let n be a positive integer prime to p and (strictly) less than $pe_K/(p-1)$; let y be an element of valuation $-n$.

(1) Show that the *Artin–Schreier equation*

$$x^p - x = y$$

is irreducible over K, and defines an extension L/K which is cyclic of degree p.

(2) Let $G = \mathrm{Gal}(L/K)$. Show that $G_n = G$ and $G_{n+1} = \{1\}$.

Solution. Let α be a root of $x^p - x - y$ in the algebraic closure of K. Take $f(x)$ to be an irreducible factor of $x^p - x - y$ such that $f(\alpha) = 0$ and then set $L = K[x]/(f(x))$. Denote A_L the valuation ring of L. Choose ϖ_K and ϖ_L as uniformizers in K and L, respectively. Write v for the normalized ϖ_K-adic valuation on K and v_L the prolonging of v to L of index 1. By assumption $v(y) = -n < 0$ and $v(p) = e_K$.

(1) We need to use the following claim.

Claim. Suppose α is a root of $x^p - x - y$ in L. Then the other $p-1$ roots in L are exactly $\alpha + z_i$ for $1 \leqslant i \leqslant p-1$ with $z_i \in A_L$, satisfying that $z_i \equiv i \bmod \varpi_L$.

Proof of Claim. Motivated by this, begin with the equation $(\alpha + z)^p - (\alpha + z) = y$, for which we can replace y with $\alpha^p - \alpha$ to get

$$(*) \qquad z^p - z + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i z^{p-i} = 0.$$

If one assumes $v(\alpha) \geqslant 0$, then $v(y) = v(\alpha^p - \alpha) \geqslant \min\{v(\alpha^p), v(\alpha)\} \geqslant 0$, contradicting to the given condition $v(y) = -n < 0$. So $v(\alpha) < 0$ (namely $\alpha \notin A_L$) and hence

$$v(y) = v(\alpha^p - \alpha) = v(\alpha^p) = pv(\alpha).$$

It follows that $v(\alpha) = -n/p$, and then

$$v\left(\binom{p}{i}\alpha^i\right) = v\left(\binom{p}{i}\right) + iv(\alpha) = v(p) - \frac{in}{p}.$$

By assumption $n < pe_K/(p-1)$, so for each $i \in \{1, \ldots, p-1\}$,

$$v\left(\binom{p}{i}\alpha^i\right) > e_K - \frac{ie_K}{p-1} = \frac{p-1-i}{p-1} e_K > 0.$$

Therefore, after modulo ϖ_K on both sides of $(*)$, the coefficients $\binom{p}{i}\alpha^i$ vanish; this equation further becomes

$$z^p - z \equiv 0 \bmod \varpi_L.$$

Clearly, all p solutions of this equation are exactly $0, 1, \ldots, p-1 \in A_L/\varpi_L$. By Hensel's lemma, these solutions respectively lift to $z_0, z_1, \ldots, z_{p-1} \in A_L$ such that $z_i \equiv i \bmod \varpi_L$. From the assumption that α is already a root, $z_0 = 0$. This proves the claim.

From the argument above we have $v(\alpha) = -n/p$, and $\alpha \notin K$ by $p \nmid n$. But

$$v_L(\alpha) = e(L/K)v(\alpha) = -\frac{ne(L/K)}{p} \in \mathbb{Z},$$

where $e(L/K)$ is the ramification index of L over K. Again, $p \nmid n$ shows that $p \mid e(L/K)$. On the other hand, by construction $f(x)$ is the minimal polynomial of α, so

$$p = \deg(x^p - x - y) \geqslant \deg f(x) = [L : K] \geqslant e(L/K).$$

These can deduce $p = [L : K] = e(L/K)$. Then $f(x) = x^p - x - y$, and hence the Artin–Scherier equation is irreducible.

Therefore, L is the splitting field of $x^p - x - y \in K[x]$. Since $x^p - x - y$ has nonzero derivative in K, it must be separable. So L/K is Galois and $\mathrm{Gal}(L/K)$ has order p. Since each group of prime order is cyclic, we complete the proof.

(2) As $p \nmid n$, there is a pair of integers (r, s) such that $rp - sn = 1$ by elementary number theory. We may assume $0 \leqslant s < p$ by replacing s with its mod p residue if necessary. For α a root as in part (1),

$$v(\varpi_K^r \alpha^s) = rv(\varpi_K) + sv(\alpha) = r - \frac{sn}{p} = \frac{1}{p}.$$

Thus, the uniformizer ϖ_L of L can be taken as $\varpi_K^r \alpha^s$, and we have $A_L = A_K[\varpi_L]$. It remains to compute $v_L(\sigma(\varpi_L) - \varpi_L)$. By part (1), L/K is totally ramified of index p. We obtain for $\sigma\colon \alpha \mapsto \alpha + z_i$ that

$$\begin{aligned} v_L(\sigma(\varpi_L) - \varpi_L) &= pv(\sigma(\varpi_K^r \alpha^s) - \varpi_K^r \alpha^s) \\ &= p(v(\varpi_K^r) + v((\alpha + z_i)^s - \alpha^s)) \\ &= p(r + v((\alpha + z_i)^s - \alpha^s)). \end{aligned}$$

To proceed on, one makes the following observation:

$$(\alpha + z_i)^s - \alpha^s = z_i^s + \sum_{k=1}^{s-1} \binom{s}{k} \alpha^k z_i^{s-k},$$

with $v(z_i) = 0$, $v(\alpha) < 0$; from the assumption $0 \leqslant s < p$, we also have $v\left(\binom{s}{k}\right) = v(s) = 0$ when $1 \leqslant k \leqslant s - 1$. Hence $v((\alpha + z_i)^s - \alpha^s) = v(s\alpha^{s-1} z_i) = v(\alpha^{s-1})$, and then

$$v_L(\sigma(\varpi_L) - \varpi_L) = p(r + v(\alpha^{s-1})) = pr - (s-1)n = n + 1.$$

By definition, we get $G_n = G$ and $G_{n+1} = \{1\}$. □

Problem 1.7 (Shapiro's lemma, [Ser79, p.116, Exercise])**.** Let H be a subgroup of G, and let B be an H-module.

(1) Let B^* be the group of maps φ of G into B such that $\varphi(hs) = h\varphi(s)$ for all $h \in H$; show that $B^* = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$.

Make B^* into a G-module by setting $(s\varphi)(g) = \varphi(gs)$. Let $\theta\colon B^* \to B$ be the homomorphism defined by $\theta(\varphi) = \varphi(1)$.

(2) Show that θ is compatible with the inclusion $H \to G$.

(3) Show that the homomorphisms

$$H^q(G, B^*) \longrightarrow H^q(H, B)$$

associated to this pair of maps are isomorphisms.

Solution. (1) We aim to show the map

$$\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B) \longrightarrow B^*, \quad \phi \longmapsto \phi|_G$$

is an isomorphism of groups. This can be done through the following verifications. First, for each $h \in H \subset \mathbb{Z}[H]$ and $\phi \in \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$, as functions on $s \in G$,

$$\phi|_G(hs) = \phi(hs) = h\phi(s) = h\phi|_G(s).$$

Hence the above map is a well-defined group homomorphism, compatible with the H-action from the right side. On the other hand, given $\varphi \in B^*$ and $n \in \mathbb{Z}$, we define

$$\phi\colon \mathbb{Z}[G] \longrightarrow B, \quad \sum n_g g \longmapsto \sum n_g \varphi(g),$$

where $n_g \in \mathbb{Z}$ for each $g \in G$. For any $\sum m_h h \in \mathbb{Z}[H]$ with $m_h \in \mathbb{Z}$, we use the homomorphism property and $\phi(hg) = h\phi(g)$ to deduce that

$$\begin{aligned} \phi\left(\sum_{h\in H} m_h h \cdot \sum_{g \in G} n_g g\right) &= \sum_{h \in H} m_h \cdot \phi\left(h \cdot \sum_{g\in G} n_g g\right) \\ &= \sum_{h\in H} m_h h \cdot \phi\left(\sum_{g \in G} n_g g\right). \end{aligned}$$

So ϕ is an element of $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$ with $\varphi = \phi|_G \in B^*$. Since G generates $\mathbb{Z}[G]$ as a $\mathbb{Z}$-module, if $\phi|_G = 0$ for some $\phi \in \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$, then $\phi = 0$ as well. Therefore, the given map is a well-defined bijective homomorphism of groups, and hence an isomorphism.

(2) It suffices to compute the image of H-action on B^* along θ. For each $h \in H$,

$$\theta(h\varphi) = (h\varphi)(1) = \varphi(1 \cdot h) = \varphi(h \cdot 1) = h\varphi(1) = h\theta(\varphi),$$

and the compatibility follows from this.

(3) If B is co-induced from an abelian group A for H, i.e., $B = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], A)$. By part (1), we compute

$$\begin{aligned} B^* &= \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B) \\ &= \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], A)) \\ &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}[H], A) \\ &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A). \end{aligned}$$

Here we have used the tensor–Hom adjoint property to deduce the third equality.[3] Hence B^* is co-induced as well. This implies $H^q(G, B^*) = H^q(H, B) = 0$ for $q \geqslant 1$. From $\theta\colon B^* \to B$ we have the induced homomorphism

$$\theta^G\colon (B^*)^G = H^0(G, B^*) \longrightarrow H^0(H, B) = B^H,$$

sending each function in $(B^*)^G$ to its valuation at 1. Take $\varphi \in (B^*)^G$ such that $\varphi(1) = 0$. By G-invariance, $0 = \varphi(1) = (g\varphi)(1) = \varphi(1 \cdot g) = \varphi(g)$ for all $g \in G$. This implies $\varphi = 0$ and shows the injectivity. For surjectivity, given any $b \in B^H$ we define $\varphi_b\colon G \to B$, $g \mapsto b$. Then $(s\varphi_b)(g) = \varphi_b(gs) = b = \varphi_b(g)$ for all $s \in G$. This shows that φ_b is G-invariant, and it lies in $(B^*)^G$ (after a $\mathbb{Z}$-linear extension to the $\mathbb{Z}[H]$-invariant map $\varphi_b\colon \mathbb{Z}[G] \to B$). So the surjectivity follows. Thus, θ^G is an isomorphism.

Therefore, for $q \geqslant 0$, we can identify the universal δ-functors $H^q(G, (-)^*)$ and $H^q(H, (-))$, from Mod_H to Mod_G, with each other. This completes the proof. □

Problem 1.8 ([Ser79, p.119, Exercise 1])**.** Grant the following fact from [Ser79, p.119, Proposition 6] that

$$H^q(G, A) \xrightarrow{\mathrm{Res}} H^q(H, A) \xrightarrow{\mathrm{Cor}} H^q(G, A)$$

equals the multiplication-by-n map, where $n = \#(G/H)$. Let q be such that $H^q(H, A) = 0$. Show that $nx = 0$ for all $x \in H^q(G, A)$.

Solution. The map $[n]\colon H^q(G, A) \to H^q(G, A)$, $x \mapsto nx$, factors through $\mathrm{Cor}\colon 0 \to H^q(G, A)$. So the result follows. □

[3] The adjoint formalism [Eis95, §2.2, §A5.2.2] is as follows. Let R be a ring. Let M, N be R-modules. Let A be an abelian group. Then there is an isomorphism of R-modules

$$\varphi\colon \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, A)) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, A), \quad f \longmapsto \varphi(f),$$

with $\varphi(f)(m \otimes n) = f(m)(n)$. Here the target of φ is an R-module via the R-action $(r\psi)(m \otimes n) = \psi(m \otimes nr)$. In practice we are taking $R = \mathbb{Z}[H]$ as a group ring, together with R-modules $M = \mathbb{Z}[G]$, $N = \mathbb{Z}[H]$, and A the same as in the problem.

Homework 2

Problem 2.1. 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

$$K^\times \cong \mathbb{F}_p^\times \times U \times t^{\mathbb{Z}},$$

where $U = 1 + t\mathbb{F}_p[\![t]\!]$. In the following, denote $\mathbb{Z}_+$ the set of all positive integers. We first claim that the map

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

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

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

We then construct a subgroup U' of U with index p as follows. Notice that, since $\bigoplus_{\mathbb{Z}_+ \backslash p\mathbb{Z}_+} \mathbb{F}_p$ is a proper $\mathbb{F}_p$-vector subspace of $\prod_{\mathbb{Z}_+ \backslash p\mathbb{Z}_+} \mathbb{F}_p$, we can take an $\mathbb{F}_p$-linear surjection

$$\alpha \colon \prod_{\mathbb{Z}_+ \backslash p\mathbb{Z}_+} \mathbb{F}_p \longrightarrow \mathbb{F}_p$$

whose kernel contains $\bigoplus_{\mathbb{Z}_+ \backslash p\mathbb{Z}_+} \mathbb{F}_p$. Set

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

Then U' is a subgroup of U of index p. The claim is that U' is not a closed subgroup of U, or 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 that

$$f(t) \prod_{0<n<m} (1+t^n)^{-a_n} \in (1 + t^m\mathbb{F}_p[\![t]\!]) \backslash U'.$$

This proves our claim about U' above.

Finally, we consider the following subgroup

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

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

Problem 2.2. 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 $z^2 = ax^2 + by^2$.[4]

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

Solution. By [Ser79, p.208, Proposition 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 2.3. Let $p \geqslant 3$. For each $n \geqslant 1$, let $\mu_n \coloneqq \{\zeta \in \overline{\mathbb{Q}}_p \mid \zeta^n = 1\}$.

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

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

(3) Consider the following isomorphisms

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

with $\zeta_p \in \mu_p$, and

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

with $\pi \in \mathbb{Z}_p[\mu_p]$ a uniformizer. Here the second map θ_0 is defined in [Ser79, p.67, Proposition 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. (1) 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, $\mu_{p-1} \subset \mathbb{Q}_p$.

(2) 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 $\pi \coloneqq \zeta_p - 1$ 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 $[\mathbb{Q}_p((-p)^{1/(p-1)}) : \mathbb{Q}_p] = p-1$ by Kummer theory. Hence it suffices to show $(-p)^{1/(p-1)} \in \mathbb{Q}_p(\mu_p)$. The minimal polynomial of π over $\mathbb{Q}_p$ is given by $((X+1)^p - 1)/X$, which is written of the form

$$X^{p-1} + p(a_{p-2}X^{p-2} + \cdots + a_1X + a_0), \quad a_i \in \mathbb{Z}_p,\ a_0 = 1.$$

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 $(-p)^{1/(p-1)} \in \mathbb{Q}_p(\mu_p)$.

(3) 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 2.4. Keep the assumption and notation as in Problem 2.3. 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 $\mathbb{Q}_p(\mu_{p^\infty}) \coloneqq \bigcup_{m \geqslant 1} \mathbb{Q}_p(\mu_{p^m})$ 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 2.3(a)). We are going to show $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_{u^{-1}}$ through the following steps.

(1) 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 $(u,-p)_v = u$.
(2) Deduce $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)} = \overline{\sigma}_{u^{-1}}$.
(3) Show $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_{p^\infty})} = \sigma_{u^{-1}}$.

Solution. (1) 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, Proposition 6], we compute

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

(2) With the notation as in Problem 2.3, it follows from [Ser79, p.208, Proposition 6] and part (1) that

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

By Problem 2.3(c), we conclude $\mathrm{Art}_p(u)|_{\mathbb{Q}_p(\mu_p)} = \overline{\sigma}_{u^{-1}}$.

(3) 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 part (2). 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 2.3(a), the composite

$$\mu_{p-1} \hookrightarrow \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

is actually a bijection. 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

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

This completes the proof of the main result. □

Problem 2.5. 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

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

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 $P_1, \dots, P_k$ be all the irreducible monic polynomials such that $v_i(x_{v_i}) < 0$ where $v_i := v_{P_i}$. 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 2.6. 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, inside $\mathbb{A}_K$, all the subsets

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

form an open neighborhood basis of 0; here 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 2.7. Recall that $K^\times$ embeds into $\mathbb{I}_K$ diagonally for every global field K.

(1) Show that $\mathbb{Q}^\times$ and $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$ generate $\mathbb{I}_\mathbb{Q}$, and $\mathbb{Q}^\times \cap (\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}) = \{1\}$.

(2) 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. (1) 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 $\mathrm{sgn}(x_\infty) = x_\infty / |x_\infty| \in \{\pm 1\}$. 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, $\mathbb{Q}^\times \cap \big(\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}\big) = \{1\}$.

(2) 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, $\ker f = \prod_{v \in S_{K,\mathrm{fin}}} \mathcal{O}_{K_v}^\times \times \mathbb{C}^\times$ 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 2.8. 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) $\pi_p = (1, \ldots, 1, p, 1, \ldots, 1)$ (p sits in the $\mathbb{Q}_p$-component) for $(p, n) = 1$;
(b) $c = (1, 1, \ldots, -1)$ (-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. (1) We first construct the desired isomorphism. 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 groups are trivial. 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 $Q := \{q_1, \ldots, q_r\}$. 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 2.7(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

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

(2) We now 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. By definition, we have $\pi_p = i_p(p)$ and $c = i_\infty(-1)$. Also, for any subset $S \subset S_{\mathbb{Q},\mathrm{fin}}$ of the primes, we define the inclusion $i_S\colon \prod_{p \in S} \mathbb{Z}_p^\times = \prod_{p \in S} \mathbb{Z}_p^\times \times \prod_{v \notin S} 1 \hookrightarrow \mathbb{I}_\mathbb{Q}$ similarly. Now the desired images are given as follows.

(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 $p > 0$, we have $\gamma(p) = 1$, and $\gamma(i_{S_{\mathbb{Q},\mathrm{fin}} \setminus (Q \cup \{p\})}(p)) = 1$ at finite places as well as $\gamma(i_\infty(p)) = 1$ at infinity. 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
$$\begin{tikzcd}
\mathbb{I}_\mathbb{Q} \arrow[r, "\mathrm{Art}_\mathbb{Q}"] \arrow[d, "\gamma"'] & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \arrow[d, "g \mapsto g|_{\mathbb{Q}(\mu_n)}"] \\
(\mathbb{Z}/n\mathbb{Z})^\times \arrow[r, "\sigma", "\sim"'] & \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}).
\end{tikzcd}$$

By the above computation, this diagram commutes if the local Artin map $\mathrm{Art}_{\mathbb{Q}_p} \colon \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ satisfies $\mathrm{Art}_{\mathbb{Q}_p}(p)|_{\mathbb{Q}_p^{\mathrm{ur}}}(x) = x^{-p}$ 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 $\mathrm{Art}_{\mathbb{Q}_p}$. □

Appendix A. Final Exam

Problem A.1 (50 points)**.** Consider the polynomial

$$f(X) \coloneqq X^3 - X - 1 \in \mathbb{Q}[X]$$

and let $L/\mathbb{Q}$ denote the (smallest) splitting field of f. Note that the discriminant of f is -23. Let v be a place of $\mathbb{Q}$ (a prime or ∞) and let w be a place of L above v. Set $G \coloneqq \mathrm{Gal}(L/\mathbb{Q})$ and $G_v \coloneqq \mathrm{Gal}(L_w/\mathbb{Q}_v)$.

(1) Show that $f(X) \in \mathbb{Q}[X]$ is irreducible. (Using this irreducibility and $\sqrt{\Delta} \notin \mathbb{Q}$, one can conclude $[L:\mathbb{Q}] = 6$.)
(2) Let $K \coloneqq \mathbb{Q}(\sqrt{-23})$. It turns out that $K \subset L$. Granting this fact, show that L/K is unramified at every place. (By this and $h_K = 3$, one can see that L is the Hilbert class field of K.)
(3) Determine $\#G_v$ for $v = 2, 23, \infty$ with proof.
(4) Let $\mathbb{I}_L$ denote the idèle group of L and let $\mathcal{C}_L \coloneqq \mathbb{I}_L/L^\times$ denote the idèle class group of L. Consider the induced map

$$\varepsilon \colon H^2(G, \mathbb{I}_L) \longrightarrow H^2(G, \mathcal{C}_L).$$

Determine with an explanation whether ε is surjective or not.

Solution. Since $f(X) \in \mathbb{Z}[X]$, we can consider its mod p reduction $f_p \in \mathbb{F}_p[X]$. This notation is used in the following.

(1) Notice that $f_2 \in \mathbb{F}_2[X]$ is irreducible since f_2 has no root in $\mathbb{F}_2$; this holds because f_2 has degree 3. By Gauss's lemma, f is irreducible in $\mathbb{Z}[X]$ and thus in $\mathbb{Q}[X]$.

(2) Since K is totally imaginary, it has no real place, so L/K is unramified at every archimedean place. For non-archimedean places, since L/K is a Galois extension, it suffices to show that for every non-archimedean place of K there exists one unramified place of L above it. Set $M \coloneqq \mathbb{Q}[X]/(f)$. By part (a), $[L:\mathbb{Q}] = 2$ and M is a degree 3 subextension of $L/\mathbb{Q}$. On the other hand, we have $[K:\mathbb{Q}] = 2$ and M, K are linearly disjoint over $\mathbb{Q}$. It follows that $L = KM$. Thus, for our purpose, it is enough to show that for every prime p, there exists an unramified prime of $\mathcal{O}_M$ above p. For each p, the discriminant of f_p is $-23 \in \mathbb{F}_p$. This is nonzero unless $p = 2$, so f_p is separable whenever $p \neq 23$.

(i) In case of $p \neq 23$, the set of irreducible factors of f_p corresponds to the set of primes of $\mathcal{O}_M$ above p. Since each irreducible factor appears only once in f_p, all primes above $p \neq 23$ in $\mathcal{O}_M$ is unramified.
(ii) As for $p = 23$, we compute $f_{23}(X) = (X-3)(X-10)^2 \in \mathbb{F}_{23}[X]$. By Hensel's lemma, there exists $\alpha \in \mathbb{Z}_{23}$ such that $f(\alpha) = 0$ and $\alpha \equiv 3 \bmod 23$. So $M = \mathbb{Q}[X]/(f) \to \mathbb{Q}_{23},\ X \mapsto \alpha$ defines an unramified prime of $\mathcal{O}_M$ above 23.

This completes the proof that L/K is unramified at every place.

(3) By definition, $G_v \coloneqq \mathrm{Gal}(L_w/\mathbb{Q}_v)$. If $v = 2$, then w above v in L is unramified in $L/\mathbb{Q}$, because L is the Hilbert class field of K by (2) and that $v = 2$ is unramified in $K/\mathbb{Q}$. So G_2 is a cyclic subgroup of G. On the other hand, we have seen f_2 is irreducible in (1). Thus, $2\mathcal{O}_M$ is a prime ideal with residue field $\mathbb{F}_8$ of degree 3 over $\mathbb{F}_2$. It follows that $3 \mid \#G_2$. From this, we conclude that $\#G_2 = 3$.

(4) The map ε is described as

$$H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(G_v, (L_w)^\times) = \bigoplus_v \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sum_v} \frac{1}{\#G}\mathbb{Z}/\mathbb{Z} = H^2(G, \mathcal{C}_L),$$

where v runs over all the places of $\mathbb{Q}$, and the arrow is defined by taking sum along all v's. Since the least common multiple of $\#G_v$'s is 6 by (3), which equals $\#G$, we conclude that ε is surjective. □

Problem A.2 (50 points)**.** Fix a prime p. Let K be a number field and let K_∞/K be an infinite Galois extension with

$$\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p.$$

We call such an extension a $\mathbb{Z}_p$-extension. All the nonzero closed subgroups of $\mathbb{Z}_p$ are precisely $p^n\mathbb{Z}_p$ for some $n \geqslant 0$. For each $n \geqslant 0$, let K_n be the unique subextension of K_∞/K with $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}_p$; in particular, $K = K_0$.

Let $v = v_0$ be a place of K and choose a place v_n of K_n inductively such that v_{n+1} lies above v_n. Let L_n denote the completion $(K_n)_{v_n}$ of K_n with respect to v_n-adic topology. Set $L_\infty \coloneqq \bigcup_{n\geqslant 0} L_n$. In particular, $\mathrm{Gal}(L_\infty/L_0) \subset \mathrm{Gal}(K_\infty/K)$ is the decomposition group at v. Let $I_v \subset \mathrm{Gal}(L_\infty/L_0)$ denote the inertia group at v.

(1) Show that there exists at least one place of K that is ramified in K_∞/K.
(2) Show that if v is an infinite place, then K_∞/K is unramified at v (i.e. $L_\infty = L_0$).
(3) Assume that v is a finite place that is above a rational prime $\ell \neq p$. Show that K_∞/K is unramified at v.
(4) Show that there exists $n \geqslant 0$ such that if a place of K_n is ramified in K_∞, then it is totally ramified in K_∞.
(5) Assume that K_∞/K is a cyclotomic $\mathbb{Z}_p$-extension, i.e., $K_\infty \subset K(\mu_{p^\infty}) \coloneqq \bigcup_m K(\mu_{p^m})$. Show that if v is a finite place, v does not split completely in K_∞/K.

Solution. (1) Assume the contrary. Then K_∞/K is an abelian extension in which every place is unramified, so it should be contained in the Hilbert class field H of K. Since $[K_\infty : K] = \infty$ and $[H : K] < \infty$, we get the contradiction.

(2) If v is an infinite place, then $\#\,\mathrm{Gal}(L_\infty/L_0)$ is 1 or 2, depending on that v lies above $\mathbb{R}$ or $\mathbb{C}$. On the other hand, $\mathbb{Z}_p$ is torsion-free. So we deduce $\mathrm{Gal}(L_\infty/L_0) = 1$ and $L_\infty = L_0$.

(3) Write k_n for the residue field of L_n and set $k_\infty \coloneqq \bigcup_{n\geqslant 0} k_n$. Since L_∞/L_0 is is abelian, the local Artin map induces the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_{L_0}^\times \arrow[r] \arrow[d, "\alpha"] & L_0^\times \arrow[r, "v_K"] \arrow[d, "\mathrm{Art}_{L_\infty/L_0}"] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & I_v \arrow[r] & \mathrm{Gal}(L_\infty/L_0) \arrow[r] & \mathrm{Gal}(k_\infty/k_0) \arrow[r] & 0.
\end{tikzcd}$$

Here, we claim that the restriction

$$\alpha \coloneqq (\mathrm{Art}_{L_\infty/L_0})|_{\mathcal{O}_{L_0}^\times} : \mathcal{O}_{L_0}^\times \longrightarrow I_v$$

is continuous and surjective. Indeed, at a finite level, if we write $I(L_n/L_0)$ for the inertia group for L_n/L_0, then the restriction of Art_{L_n/L_0} to $\mathcal{O}_{L_0}^\times$, mapping to $I(L_n/L_0)$, is surjective. Since $I_v = \varprojlim_n I(L_n/L_0)$ and that $\mathcal{O}_{L_0}$ is complete with respect to the norm topology, we deduce that α is surjective.

To show that K_∞/K is unramified at v, it suffices to show that $I_v = 0$. Assume $I_v \neq 0$ for the sake of contradiction. Since I_v is a closed subgroup of $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$, we can write $I_v = p^n\mathbb{Z}_p$ for some $n \geqslant 0$. Take an open subgroup $H \subset \mathcal{O}_{L_0}^\times$ that is topologically isomorphic to $\mathcal{O}_{L_0}$. Note that for each $m \geqslant 0$ we always have $p^m\mathcal{O}_{L_0} = \mathcal{O}_{L_0}$, because the assumption $p \neq \ell$ implies that p is invertible in $\mathcal{O}_{L_0}$. It follows that the composite

$$H \hookrightarrow \mathcal{O}_{L_0}^\times \xrightarrow{\alpha} I_v = p^n\mathbb{Z}_p \longrightarrow p^n\mathbb{Z}_p/p^{n+m}\mathbb{Z}_p = \mathbb{Z}/p^m\mathbb{Z}$$

is the zero map for every $m \geqslant 0$. In particular, we have $H \subset \ker\alpha$ and α induces a surjection $\mathcal{O}_{L_0}^\times/H \twoheadrightarrow I_v = p^n\mathbb{Z}_p$. But $\mathcal{O}_{L_0}^\times/H$ is finite, which leads to a contradiction. So we conclude $I_v = 0$.

(4) Since K is a number field, there are only finitely many places of K above p. This together with (2) and (3) implies that there are only finitely many places of K that are ramified in K_∞/K. Let $v_1, \ldots, v_s$ be those places of K. For $1 \leqslant i \leqslant s$, the inertia group I_{v_i} is a nonzero closed subgroup of $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$, so we can write $I_{v_i} = p^{n_i}\mathbb{Z}_p \subset \mathbb{Z}_p$ for some n_i. Set $n \coloneqq \max\{n_1, \ldots, n_s\}$. We claim that such n is exactly the desiderata.

To check the claim, suppose v' is a place of K_n that is ramified K_∞, and then v' lies above v_i for some i. If we write I' for the inertia subgroup of $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}_p$ at v', then we get

$$I' = I_{v_i} \cap \mathrm{Gal}(K_\infty/K_n) = p^{n_i}\mathbb{Z}_p \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}_p = \mathrm{Gal}(K_\infty/K_n).$$

This means that v' is totally ramified in K_∞/K_n.

(5) Set $M \coloneqq K \cap \mathbb{Q}(\mu_{p^\infty})$. Then we have

$$\mathrm{Gal}(K_\infty/K) \subset \mathrm{Gal}(K(\mu_{p^\infty})/K) = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/M) \subset \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$$

with $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$ and $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Since $\mathbb{Z}_p^\times$ contains an open subgroup that is topologically isomorphic to $\mathbb{Z}_p$, we see that $\mathrm{Gal}(K_\infty/K)$ has finite index in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and thus in $\mathrm{Gal}(K(\mu_{p^\infty})/K)$. In particular, we have $[K(\mu_{p^\infty}) : K_\infty] < \infty$.

If v is a finite place, then $K_v = L_0$ is a non-archimedean local field and thus contains only finitely many roots of unity. In particular, $[K_v(\mu_{p^\infty}) : K_v] = \infty$. Since $[K_v(\mu_{p^\infty}) : L_\infty] \leqslant [K(\mu_{p^\infty}) : K_\infty] < \infty$, we conclude $[L_\infty : L_0] = \infty$. In particular, $L_0 \subsetneq L_\infty$. This means that the decomposition group of K_∞/K at v is nontrivial, namely, v does not split completely in K_∞/K. □

Problem A.3 (Bonus, 10 points)**.**

1. Write down the statement of the existence and uniqueness (i.e., characterizing properties) of the local Artin map Art_K in local class field theory for a non-archimedean local field K. You may write "There exists a unique ... such that ... ."
2. Write down the fundamental exact sequence in class field theory (i.e., the exact sequence involving the Brauer groups) for a global field K.

Solution. (1) There exists a unique continuous group homomorphism

$$\mathrm{Art}_K \colon K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that

- for every uniformizer π, we have $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K$ (where Frob_K is a fixed topological generator of $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \hat{\mathbb{Z}}$);
- for every finite abelian extension L/K, we have $\mathrm{Art}_K(N_{L/K}(L^\times))|_L = 1$ and $\mathrm{Art}_K|_L$ induces an isomorphism $K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

(2) The restrictions and the local invariant maps induce an exact sequence

$$0 \longrightarrow \mathrm{Br}_K \xrightarrow{(\mathrm{Res}_v)_v} \bigoplus_{v \in S_K} \mathrm{Br}_{K_v} \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z},$$

where S_K denotes the set of places of K. □

Photograph — December 24, 2023; at the Summer Palace, Beijing, China.
A peaceful winter scene at a corner of the palace after a heavy snow.

References

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 1995.

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