SOLUTION TO PROBLEM SET 1

LECTURER: KOJI SHIMIZU

TA: WENHAN DAI

Problem 1. For each of the following, give one example and explains briefly why your example works.

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

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

Solution. There would be various examples for (a) and we propose two of them below.

(a) The following comes a natural object from p-adic geometry.

(a1) Let C be an algebraically closed complete p-adic field with residue field $\overline{\mathbb{F}}_p$ (for example, $C = \widehat{\overline{\mathbb{Q}}}_p$). 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

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

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.

- 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. So

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

  In other words, I is a maximal ideal of A.
- 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 $\mathbb{R}_{\geqslant 0} \cup \{\infty\}$.

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.

(a2) 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

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

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 $p \in R_{(p)}$.

Date: October 31, 2023.

- 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.

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

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

is a complete discrete valuation field. We have the ring of integers and the residue field

$$\mathcal{O}_K = \mathbb{F}_p(\!(t)\!)[\![T]\!], \quad k = \mathbb{F}_p(\!(t)\!),$$

respectively. Consider the polynomial

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

We make the following observations:

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

Thus, $L := K[X]/(f(X))$ 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 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

$$\rho = \log|y|_2 / \log|y|_1.$$

We aim to show that $|x|_1^\rho = |x|_2$ for every $x \in K$. Note that for $m, n \in \mathbb{N}$,

$$\frac{n}{m} > s = \frac{\log|x|_1}{\log|y|_1} \implies |y|_1^{n/m} > |y|_1^s = |x|_1 \implies \left|\frac{x^m}{y^n}\right|_1 < 1$$
$$\implies \left|\frac{x^m}{y^n}\right|_2 < 1 \implies |x|_2 < |y|_2^{n/m}.$$

Since $n/m \in \mathbb{Q}$ is arbitrary, we get $|y|_2^s \geqslant |x|_2$ for $s \in \mathbb{R}_{>0}$. 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 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.

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

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

(a) Note that $w(ab) = w(a) + w(b)$ for all $a, b \in L$. We fix $y, z \in L$ and assume without loss of generality that $w(y) \geqslant w(z)$. Then $w(yz^{-1}) \geqslant 0$. Moreover, the desired inequality is equivalent to

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

or alternatively, through dividing by z on both variables,

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

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

(b) 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

$$\begin{array}{ccc} A[X] & \xrightarrow{\text{mod } \varpi} & (A/(\varpi))[X] \\ g(X) & \longmapsto & \overline{g}(X) \neq 0. \end{array}$$

Assume $r \geqslant 1$ for the sake of contradiction. In this case $\overline{g}(X)$ has a zero constant term. Hence we can write $\overline{g}(X) = X^s \overline{h}(X)$ 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,

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

□

Problem 4 (Conductor, [Ser79, p. 53, Exercise])**.** Let C be a subring of B containing A, and having the same field of fractions as B.

(a) 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.
(b) 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 $xC^* \subset B^*$.
(c) 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 (b) 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.

(a) 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.

(b) 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 $\mathfrak{f}_{C/B} = (B^* : C^*)$.

(c) Using (b) together with the relation $\mathfrak{c}C^* = C$, we see that

$$x \in \mathfrak{f}_{C/B} \iff xC^* \subset B^* \iff x\mathfrak{c}^{-1} \subset \mathfrak{D}_{B/A}^{-1} \iff x \in \mathfrak{c} \cdot \mathfrak{D}_{B/A}^{-1}.$$

This proves $\mathfrak{f}_{C/B} = \mathfrak{c} \cdot \mathfrak{D}_{B/A}^{-1}$.

□

Problem 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.

(a) Let $\overline{K}_{\mathrm{s}}$ be the separable closure of $\overline{K}$. Show that $G/G_0 = \mathrm{Gal}(\overline{K}_{\mathrm{s}}/\overline{K})$.
(b) 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}).
   (i) Show that G_0/G_1 is (canonically) isomorphic to μ.
   (ii) 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 $\overline{K}$.
   (iii) 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.

[1] Unlike the modern notations, in Problem 5 we assume K is a local field and denote by $\overline{K}$ its residue field (rather than the algebraically closure).

(c) 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 $G'_L \coloneqq \mathrm{Gal}(L/K)$.

(a) 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].

(b) Let p denote $\operatorname{char}\overline{K}$ if $\operatorname{char}\overline{K} > 0$ and 1 if $\operatorname{char}\overline{K} = 0$. We start with two observations.

- 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 identified with 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 $\alpha^n = u$: 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).

(i) As in (a), we see

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

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 $a > 1$, Kummer theory tells

$$\begin{array}{ccc} \mathrm{Gal}(K_{\mathrm{ur}}(\varpi_K^{1/m})/K) & \xrightarrow{\ \sim\ } & \mu_m(K_{\mathrm{ur}}) \\ g & \longmapsto & g(\varpi_K^{1/m})/\varpi_K^{1/m} \end{array}$$

is a group isomorphism which 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

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

Combining this with the canonical isomorphisms $\mathrm{Gal}(K_{\mathrm{ur}}(\varpi_K^{1/m})/K) \cong \mu_m(K_{\mathrm{ur}}) \cong \mu_m$, we obtain the canonical isomorphisms

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

Here, in the last equality, 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

[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]).

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 $(m,p)=1$.

(ii) 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 $k_i \in \mathbb{Z}_{>0}$, and set $\zeta_r = \prod_{i=1}^t \zeta_{\ell_i^{k_i}}$. 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 varying r. 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.

(iii) 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 as in (i), note $\sigma^{-1}(\varpi_K)^{1/m}$ 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

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

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 $(m,p)=1$.

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

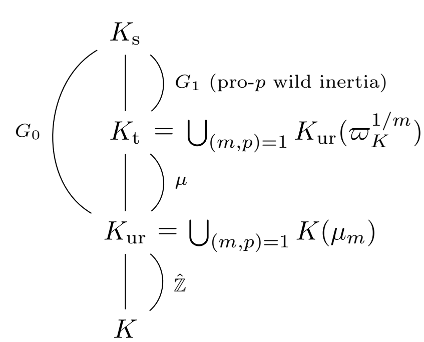
$$\frac{\sigma g \sigma^{-1}(\varpi_K^{1/m})}{\varpi_K^{1/m}} = \sigma\Big(\frac{g(\varpi_K^{1/m})}{\varpi_K^{1/m}}\Big) = \Big(\frac{g(\varpi_K^{1/m})}{\varpi_K^{1/m}}\Big)^q = \frac{g^q(\varpi_K^{1/m})}{\varpi_K^{1/m}}.$$

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.



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

□

Problem 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 $-n$.

(a) 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.

(b) 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 by 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 $v(p) = e_K$.

(a) Following the hint, we consider:

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.

(b) 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 (a),

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

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 (a), 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 7 (Shapiro's lemma, [Ser79, p. 116, Exercise])**.** Let H be a subgroup of G, and let B be an H-module.

(a) 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 $\theta(\varphi) = \varphi(1)$.

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

(c) Show that the homomorphisms

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

associated to this pair of maps are isomorphisms.

Solution. (a) We aim to show the map

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

is an isomorphism of groups. This can be done through the following verifications.

- 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.
- Given $\varphi \in B^*$ and $n \in \mathbb{Z}$, we define

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

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.

(b) 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.

(c) If B is co-induced from an abelian group A for H, i.e.,

$$B = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], A),$$

then by (a),

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

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

$$\begin{aligned} \theta^G\colon (B^*)^G = H^0(G, B^*) &\longrightarrow H^0(H, B) = B^H \\ \varphi &\longmapsto \varphi(1). \end{aligned}$$

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.

□

[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.

Problem 8 ([Ser79, p. 119, Exercise 1])**.** Granting the fact (cf. [Ser79, p. 119, Proposition 6]) that

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

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 $\text{Cor} \colon 0 \to H^q(G,A)$. So the result follows. □

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