Exercise 1 Solutions

Problem 1.1. (Semisimplification of the reduction is well-defined) Let L be a finite extension of $\mathbb{Q}_\ell$ with ring of integers $\mathcal{O}$, uniformizer ϖ, and residual field κ. Let Γ be a compact topological group, and let $\rho : \Gamma \to \mathrm{GL}_n(L) = \mathrm{GL}(V)$ be a representation. So there exists an $\mathcal{O}$-lattice Λ that is stable under Γ-action, and define $\bar{\rho}_\Lambda$ to be the representation given by the Γ-action on $\Lambda/\varpi\Lambda$.

(1) Show that the semisimplification of $\bar{\rho}_\Lambda$ does not depend on the choice of the Γ-stable $\mathcal{O}$-lattice Λ. (Hint: consider two such lattices Λ and Λ'; first reduce to the case when $\varpi \cdot \Lambda \subseteq \Lambda' \subseteq \Lambda$.)

(2) When $\bar{\rho}^{\mathrm{ss}}$ is irreducible, show that for every two Γ-stable lattices Λ_1 and Λ_2, $\Lambda_1 = \varpi^n \cdot \Lambda_2$ for some $n \in \mathbb{Z}$.

Solution. (1) (Method 1) As multiplication by ϖ defines an isomorphism between $\varpi\Lambda/\varpi^2\Lambda$ and $\Lambda/\varpi\Lambda$, we may replace Λ by $\varpi^n\Lambda$ for some $n \in \mathbb{Z}$ and thus assume that $\varpi^n\Lambda' \subseteq \Lambda \subseteq \Lambda'$ for some $n \in \mathbb{Z}$. Consider lattices

$$M_n = \Lambda \subseteq M_{n-1} = \Lambda + \varpi^{n-1}\Lambda' \subseteq M_{n-2} = \Lambda + \varpi^{n-2}\Lambda' \subseteq \cdots \subseteq M_0 = \Lambda + \Lambda' = \Lambda'.$$

Then we have $\varpi \cdot M_i \subseteq M_{i-1} \subseteq M_i$ for each i. We may then reduce (1) to the case $\varpi\Lambda \subseteq \Lambda' \subseteq \Lambda$. In this case, we consider two exact sequences:

$$0 \to \Lambda'/\varpi\Lambda \to \Lambda/\varpi\Lambda \to \Lambda/\Lambda' \to 0$$
$$0 \to \varpi\Lambda/\varpi\Lambda' \to \Lambda'/\varpi\Lambda' \to \Lambda'/\varpi\Lambda \to 0$$

From this, we deduce that

$$\big(\Lambda/\varpi\Lambda\big)^{\mathrm{ss}} \cong \big(\Lambda'/\varpi\Lambda\big)^{\mathrm{ss}} \oplus \big(\Lambda/\Lambda'\big)^{\mathrm{ss}} \cong \big(\Lambda'/\varpi\Lambda\big)^{\mathrm{ss}} \oplus \big(\varpi\Lambda/\varpi\Lambda'\big)^{\mathrm{ss}} \cong \big(\Lambda'/\varpi\Lambda'\big)^{\mathrm{ss}}.$$

(1) (Method 2) Note that the characteristic polynomial $\overline{\mathrm{char}(\gamma)}$ of each element $\gamma \in \Gamma$ acting on $\Lambda/\varpi\Lambda$ is the reduction of the characteristic polynomial $\mathrm{char}(\gamma)$ of γ on V (which belongs to $\mathcal{O}[x]$) modulo ϖ. But for two different lattices Λ and Λ', $\mathrm{char}(\gamma)$ are the same, and thus $\overline{\mathrm{char}(\gamma)}$ are the same for $\Lambda/\varpi\Lambda$ and $\Lambda'/\varpi\Lambda'$. By Brauer–Nesbitt theorem, we see that $\big(\Lambda/\varpi\Lambda\big)^{\mathrm{ss}} \cong \big(\Lambda'/\varpi\Lambda'\big)^{\mathrm{ss}}$. (Note that for this, we need only to use the theorem for finite groups, as the image of Γ in $\Lambda/\varpi\Lambda$ and $\Lambda'/\varpi\Lambda'$ is finite.)

(2) As in (1), we may assume that $\varpi^n\Lambda_2 \subseteq \Lambda_1 \subseteq \Lambda_2$ for some $n \geq \mathbb{Z}_{\geq 0}$. We may take n to be minimal. Suppose that $n \neq 0$, Then

$$\Lambda_1 \subsetneq \Lambda_1 + \varpi^{n-1}\Lambda_2 = M \subsetneq \varpi^{-1}\Lambda_1.$$

Then as in (1), we have

$$0 \to M/\Lambda_1 \to \varpi^{-1}\Lambda_1/\Lambda_1 \to \varpi^{-1}\Lambda_1/M \to 0$$

But $\bar{\rho}^{\mathrm{ss}}$ is assumed to be irreducible. Yet M/Λ_1 and $\varpi^{-1}\Lambda_1/M$ are non-trivial. We arrive at a contradiction. □

Problem 1.2. ($\mathbb{Z}_p$-extensions of local fields and global fields) For a field k, let $k^{p\text{-ab}}$ denote its maximal pro-p-abelian extension, i.e. the union of all abelian Galois extensions of k whose Galois groups are pro-p-groups. Under the Galois theory, this corresponds to the maximal pro-p quotient of G_k^{ab}. Then $G_k^{p\text{-ab}} := \mathrm{Gal}(k^{p\text{-ab}}/k)$ is a $\mathbb{Z}_p$-module, and we write $r_{p\text{-ab}}(k)$ for its rank over $\mathbb{Z}_p$ (possibly infinite), or equivalently $r_{p\text{-ab}}(k) = \dim_{\mathbb{Q}_p} G_k^{p\text{-ab}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Answer the following questions on the computation of $r_{p\text{-ab}}$ for different fields.

(1) If $k = K$ is a finite extension of $\mathbb{Q}_p$, show that $r_{p\text{-ab}} = [K : \mathbb{Q}_p] + 1$.
(2) If $k = \mathbb{F}_q((t))$ is a function field, with q a power of p, show that $r_{p\text{-ab}} = \infty$. (Hint: the structure of $\mathbb{F}_q((t))^\times$ is discussed in, for example, Neukirch, Algebraic Number Theory, Page 140, Proposition II.5.7 (ii).)
Remark: Philosophically, one can understand this difference as: in the function field case, all fields look like $\mathbb{F}_{q'}((t'))$ for some uniformizer t'. So there is no "base field" like $\mathbb{Q}_p$. Because of this, we can always make $\mathbb{F}_q((t))$ an as large as possible extension of another $\mathbb{F}_{q'}((t'))$. So $r_{p\text{-ab}}(\mathbb{F}_q((t)))$ is infinite.
(3) If $k = F$ a global number field, then Dirichlet unit theorem says that the rank of the unit group $\mathrm{rank}(\mathcal{O}_F^\times) = r_1 + r_2 - 1$, where r_1 and r_2 are number of real embeddings and number of pairs of complex embeddings. Show that

$$r_{\mathrm{ab}}(F) \geq [F : \mathbb{Q}] - (r_1 + r_2 - 1) = r_2 + 1.$$

Remark: It is conjectured that this is an equality, so-called the Leopoldt Conjecture. This is known when $F/\mathbb{Q}$ is an abelian extension, but open in general.

Solution. (1) and (2) Let K be a local field. The local class field theory shows that there is a canonical isomorphism

$$\mathrm{Art}_K : \widehat{K}^\times \xrightarrow{\cong} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

As pro-abelian groups, we have isomorphisms

$$\widehat{K}^\times = \varpi_K^{\widehat{\mathbb{Z}}} \times \mu(K) \times \begin{cases} \mathbb{Z}_p^{[K:\mathbb{Q}_p]} & \text{when } K \text{ is finite over } \mathbb{Q}_p \\ \mathbb{Z}_p^{\mathbb{N}} & \text{when } K = \mathbb{F}_q((t)), \end{cases}$$

as discussed in Neukirch's book, for example. So

$$r_{p\text{-ab}}(K) = \begin{cases} 1 + [K : \mathbb{Q}_p] & \text{when } K \text{ is finite over } \mathbb{Q}_p \\ \infty & \text{when } K = \mathbb{F}_q((t)). \end{cases}$$

(3) Let F be a global field. The global class field theory gives a canonical isomorphism

$$\mathrm{Art}_F : \mathbb{A}_F^\times / (F^\times F_{\mathbb{R}}^{\times,\circ})^{\mathrm{cl}} \xrightarrow{\cong} \mathrm{Gal}(F^{\mathrm{ab}}/F),$$

where $(-)^{\mathrm{cl}}$ is the closure of the corresponding set in the ambient spaces. To solve our problem, it is enough to consider the subextension $F_{(p)}^{\mathrm{ab}}/F$, the maximal abelian extension of F that is unramified outside p-adic places. Then

$$\mathrm{Gal}(F_{(p)}^{\mathrm{ab}}/F) \cong \mathbb{A}_F^\times / \left(F^\times F_{\mathbb{R}}^\times \textstyle\prod_{v \nmid p} \mathcal{O}_{F_v}^\times\right)^{\mathrm{cl}} \cong \mathbb{A}_{F,f}^\times / \left(F^\times \textstyle\prod_{v \nmid p\infty} \mathcal{O}_{F_v}^\times\right)^{\mathrm{cl}}.$$

Consider the following exact sequence:

$$1 \to \frac{\prod_{v|p} \mathcal{O}_{F_v}^\times}{(\mathcal{O}_F^\times)^{\mathrm{cl}}} \to \frac{\mathbb{A}_{F,f}^\times}{\left(F^\times \prod_{v \nmid p\infty} \mathcal{O}_{F_v}^\times\right)^{\mathrm{cl}}} \to \frac{\mathbb{A}_{F,f}^\times}{F^\times \prod_{v \nmid \infty} \mathcal{O}_{F_v}^\times} \cong \mathrm{Cl}(F) \to 1.$$

As the ideal class group $\mathrm{Cl}(F)$ is finite, it is enough to show the $\mathbb{Z}_p$-rank of the maximal pro-p quotient of $(\prod_{v|p} \mathcal{O}_{F_v}^\times)/(\mathcal{O}_F^\times)^{\mathrm{cl}}$ is $\geq r_2 + 1$. As we seen in (1), for each $v|p$, the $\mathbb{Z}_p$-rank of the maximal pro-p quotient of $\mathcal{O}_{F_v}^\times$ is $[F_v : \mathbb{Q}_p]$. By Dirichlet unit theorem, $\mathcal{O}_F^\times$ has $\mathbb{Z}$-rank $r_1 + r_2 - 1$, so the closure of its image in $\prod_{v|p} \mathcal{O}_{F_v}^\times$ has $\mathbb{Z}_p$-rank $\leqslant r_1 + r_2 - 1$. Hence we conclude that

$$r_{p\text{-ab}}(F) \geqslant \sum_{v|p} [F_v : \mathbb{Q}_p] - (r_1 + r_2 - 1) = n - (r_1 + r_2 - 1) = r_2 + 1.$$

□

Problem 1.3. (Restriction of a Galois representation) Let F be a number field and let $\bar{\rho} : G_F \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ be a continuous residual Galois representation. Let S be a finite set of places of F at which $\bar{\rho}$ is unramified. Show that there exists a finite solvable Galois extension E over F such that

(1) letting $\bar{\rho}|_{G_E}$ denote the restriction of $\bar{\rho}$ to G_E, then $\mathrm{Im}(\bar{\rho}) = \mathrm{Im}(\bar{\rho}|_{G_E})$,
(2) $\bar{\rho}|_{G_E}$ is everywhere unramified, and
(3) every $v \in S$ splits completely in E/F.

Solution. Since G_F is compact and $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ is discrete, the image of $\bar{\rho}$ is finite and $\mathrm{Ker}(\bar{\rho})$ is an open subgroup of G_F, corresponding to a finite Galois extension H of F. There are only finitely places of F that ramify in H/F; let T be the set of such places (which is disjoint from T). We specify the following local extensions:

- for each $v \in S$, set $F'_v = F_v$;
- for each $v \in T$, $\bar{\rho}|_{G_{F_v}} : G_{F_v} \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ has an open kernel, corresponding a finite extension F'_v of F_v;
- for each $\sigma \in \mathrm{Gal}(H/F)$, Chebotarev density theorem implies that there exists a place $v_\sigma \notin S \cup T$ such that the Frobenius element at v lies in the same conjugacy class as σ in $\mathrm{Gal}(H/F)$. Set $F'_{v_\sigma} := F_v$.

Applying a theorem from the class, there exists a finite solvable Galois extension E/F such that, for each $v \in S \cup T$ or $v = v_\sigma$ above and each place w of E above v, $E_w \cong F'_v$ as extensions of F_v. We may instantly verify (2) and (3) by our construction. For (1), we note that, each $\sigma \in \mathrm{Gal}(H/F) \cong \mathrm{Im}(\bar{\rho})$, $\sigma = \bar{\rho}(\mathrm{Frob}_v)$ (after we properly choose the embedding $G_{F_v} \hookrightarrow G_F$). Thus, for some place w of E above v, $\bar{\rho}|_{G_E}(\mathrm{Frob}_w) = \bar{\rho}(\mathrm{Frob}_v) = \rho$. Thus $\mathrm{Im}(\bar{\rho}) = \mathrm{Im}(\bar{\rho}|_{G_E})$. □

Remark: A typical mistake here is try to find a place v of F that is nonsplit in H. Such place may not exists in general, because the set of places above v is the index of the local Galois group in the global Galois group. The local Galois group is always solvable, yet the global Galois group can be (conjecturally?) arbitrary.

Problem 1.4. (Compatibility of corestriction map and Shapiro's lemma under cup product) Let G be a finite group and H a subgroup. Let A and B be two finite H-modules and C a finite G-module. Assume that we are given a natural H-module homomorphism

$$\psi : A \otimes B \to C,$$

i.e. $\psi(ha \otimes hb) = h\psi(a \otimes b)$ for $h \in H$, $a \in A$, and $b \in B$.

(1) Show that ψ induces a natural well-defined G-module homomorphism

$$\tilde{\psi} : \mathrm{Ind}_H^G A \otimes \mathrm{Ind}_H^G B \to C$$

$$\tilde{\psi}(f_A \otimes f_B) := \sum_{g \in H\backslash G} g^{-1}\psi(f_A(g) \otimes f_B(g)). \tag{1.4.1}$$

(Here $\mathrm{Ind}_H^G A := \{f : G \to V; \mid f(hg) = h(f(g)) \text{ for } h \in H, g \in G\}$ is the standard induced representation; G acts on it by $(g \star f)(x) := f(xg)$ for $g, x \in G$.)

(2) Show that, for any $i, j \geq 0$, the following diagram of cup products commutes:

$$\begin{array}{ccccc} H^i(H,A) & \times & H^j(H,B) & \xrightarrow{\cup_\psi} & H^{i+j}(H,C) \\ {\scriptstyle \text{Shapiro}\atop\text{Lemma}}\downarrow\cong & & {\scriptstyle \text{Shapiro}\atop\text{Lemma}}\downarrow\cong & & \downarrow{\scriptstyle \text{corestriction}} \\ H^i(G,\mathrm{Ind}_H^G A) & \times & H^j(G,\mathrm{Ind}_H^G B) & \xrightarrow{\cup_{\tilde\psi}} & H^{i+j}(G,C). \end{array} \tag{1.4.2}$$

(Hint: use dimension shifting to reduce to $i = j = 0$, and then make an explicit computation.)

Proof. (1) We fist check that the expression (1.4.1) does not depend on the choice of representatives g of the coset $H\backslash G$: for $g \in G$ and $h \in H$,

$$(hg)^{-1}\psi(f_A(hg) \otimes f_B(hg)) = g^{-1}h^{-1}\psi(hf_A(g) \otimes hf_B(g)) = g^{-1}\psi(f_A(g) \otimes f_B(g)).$$

Next, we check that (1.4.1) is G-equivariant: for $x \in G$

$$\tilde\psi(xf_A \otimes xf_B) = \sum_{g\in H\backslash G} g^{-1}\psi(xf_A(g) \otimes xf_B(g)) \tag{1.4.3}$$

$$= \sum_{g\in H\backslash G} g^{-1}\psi(f_A(gx) \otimes f_B(gx)) \tag{1.4.4}$$

$$\overset{g'=gx}{=} \sum_{g'\in H\backslash G} xg'^{-1}\psi(f_A(g') \otimes f_B(g')) \tag{1.4.5}$$

$$= x\tilde\psi(f_A \otimes f_B). \tag{1.4.6}$$

Here in the third equality, x acts (from the right) on all cosets in $H\backslash G$ to permute these cosets.

(2) It is enough to deal with the tautological case when $C = A \otimes B$. We first check the diagram when $i = j = 0$. The natural Shapiro isomorphism is given by

$$\begin{array}{ccc} \mathcal{S}_A : H^0(H,A) = A^H & \xrightarrow{\text{Shapiro Lemma}} & (\mathrm{Ind}_H^G A)^G = H^0(G,\mathrm{Ind}_H^G A) \\ a & \longmapsto & \big(g \mapsto a\big). \end{array}$$

Thus we compute $\cup_{\tilde\psi}$ as follows: for $a \in A$ and $b \in B$

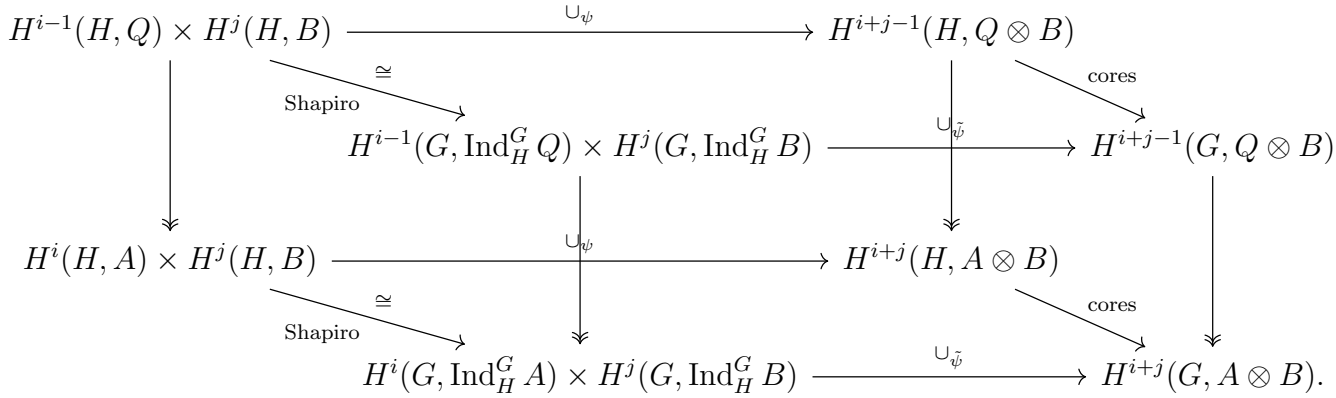
$$\mathcal{S}_A(a) \cup_{\tilde\psi} \mathcal{S}_B(b) = \sum_{g\in H\backslash G} g^{-1}\psi(a \otimes b) = \mathrm{cores}_H^G(a \otimes b).$$

Next, assume that we have proved (1.4.2) for $i-1$ and j. We consider the natural injective map $A \hookrightarrow \mathrm{Ind}_{\{1\}}^H A$ given by $a \mapsto (h \mapsto ha)$. Let Q denote its cokernel. Then we have

$$H^{i-1}(H,\mathrm{Ind}_{\{1\}}^H A) \to H^{i-1}(H,Q) \to H^i(H,A) \to H^i(H,\mathrm{Ind}_{\{1\}}^H A) = 0.$$

$$H^{i-1}(G,\mathrm{Ind}_H^G \mathrm{Ind}_{\{1\}}^H A) \to H^{i-1}(G,\mathrm{Ind}_H^G Q) \to H^i(G,\mathrm{Ind}_H^G A) \to H^i(G,\mathrm{Ind}_H^G \mathrm{Ind}_{\{1\}}^H A) = 0.$$

From this, we see that the two boundary homomorphisms are surjective. Consider the following diagram:



The commutativity of the top diagram implies the commutativity of the bottom diagram due to the vertical surjective maps.

We may run a similar argument of dimension shifting to show deduce the case of (i,j) from that of $(i,j-1)$. This completes the proof of the problem. □

Problem 1.5. (Lattices in a representation by example) Let $\ell \geq 3$ be a prime number Let Γ be a compact topological group. Let $\chi_1, \chi_2 : \Gamma \to \mathbb{Z}_\ell^\times$ be two continuous characters, whose reductions modulo ℓ are different. Let $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{Q}_\ell) = \mathrm{GL}(V)$ be an *irreducible* representation.

(1) Prove (by abstract nonsense) that for every $g \in \Gamma$, $\mathrm{Tr}(\rho(g)) \in \mathbb{Z}_\ell$, and that the associated semisimple residual Galois representation $\bar\rho^{\mathrm{ss}} \cong \bar\chi_1 \oplus \bar\chi_2$ if and only if, for every $g \in \Gamma$,
$$\mathrm{Tr}(\rho(g)) \equiv \chi_1(g) + \chi_2(g) \mod \ell.$$

(2) Assume the equivalent conditions in (1) hold. Show that there exists a lattice Λ_1 admitting a basis for which the associated residual Galois representation $\bar\rho_{\Lambda_1}$ takes the form of
$$\bar\rho_{\Lambda_1}(g) = \begin{pmatrix} \bar\chi_1(g) & \bar b(g) \\ 0 & \bar\chi_2(g) \end{pmatrix}$$
for some nonzero map $\bar b : \Gamma \to \mathbb{F}_\ell$. Show that such Λ_1 is unique up scalar. (This is not hard; but I believe that such an argument first appeared in Ribet's famous converse to Herbrand theorem, in K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

(3) We may reverse the role of $\bar\chi_1$ and $\bar\chi_2$ in (2) to get a lattice Λ_2 (canonical up to a unique scalar), so that $\bar\rho_{\Lambda_2}$ is a non-trivial extension of $\bar\chi_1$ by $\bar\chi_2$. By possibly rescaling Λ_2, we may assume that $\Lambda_1 \subseteq \Lambda_2 \subseteq \ell^{-n}\Lambda_1$, with subquotients for each inclusion is isomorphic to $\mathbb{Z}_\ell/\ell^n$. This n can be viewed as an invariant that describes how similar this ρ is to a direct sum of two characters. Show that there exists two characters $\chi_i^{(n)} : \Gamma \to (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times$ with $i = 1, 2$, such that for every $g \in \Gamma$,
$$\mathrm{Tr}(\rho(g)) \equiv \chi_1^{(n)}(g) + \chi_2^{(n)}(g) \mod \ell^n.$$

(4) Assume $\ell \geq 3$ and that Γ contains an element $\mathbf{c}$ of order 2 (e.g. a complex conjugation in $G_\mathbb{Q}$) for which $\bar\chi_1(\mathbf{c}) = 1$ and $\bar\chi_2(\mathbf{c}) = -1$. Prove that the converse to (3) holds, namely, if there exists characters $\chi_1, \chi_2 : \Gamma \to \mathbb{Z}_\ell^\times$ such that
$$\chi_1(\mathbf{c}) = 1, \quad \chi_2(\mathbf{c}) = -1, \quad \text{and} \quad \mathrm{Tr}(\rho(g)) \equiv \chi_1(g) + \chi_2(g) \bmod \ell^m,$$
then the invariant n from (3) satisfies $n \geq m$.

(I do not know if (4) holds without the additional assumption on the existence of the element $\mathbf{c}$. In applications, $\mathbf{c}$ is the complex conjugation in the Galois group.)

Remark: In the aforementioned paper of Ribet, he considered the representation ρ associated to a cuspidal eigenform that is congruent to an Eisenstein series modulo p.

Solution. (1) We may conjugate the representation ρ to have image in $\mathrm{GL}_2(\mathbb{Z}_\ell)$; this way, we see that $\mathrm{Tr}(\rho)$ takes values in $\mathbb{Z}_\ell$. The statement in (1) follows from Brauer–Nesbitt theorem.

(2) We first prove the existence of such lattice Λ_1'. Then $(\Lambda_1'/\ell\Lambda_1')^{\mathrm{ss}} \cong \bar{\chi}_1 \oplus \bar{\chi}_2$. Lifting an eigenbasis of $\Lambda_1'/\ell\Lambda_1'$ to a basis $\{e_1', e_2'\}$ of Λ_1, we may assume that the representation ρ' is given by

$$\rho'(g) = \begin{pmatrix} a'(g) & b'(g) \\ c'(g) & d'(g) \end{pmatrix}$$

such that $a'(g) \pmod{\ell} = \bar{\chi}_1(g)$, $d'(g) \pmod{\ell} = \bar{\chi}_2(g)$, and either b' or c' is constantly zero modulo ℓ.

We know that $b'(g)$ cannot be constantly zero, otherwise V would be reducible; let ℓ^n be the maximal power such that $b'(g) \in \ell^n\mathbb{Z}_\ell$ for every $g \in \Gamma$. Then with respect to the basis $\{e_1 = \ell^n e_1', e_2 = e_2'\}$, the representation V becomes

$$\rho(g) = \begin{pmatrix} \ell^n & 0 \\ 0 & 1 \end{pmatrix}^{-1} \rho'(g) \begin{pmatrix} \ell^n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a'(g) & \ell^{-n}b'(g) \\ \ell^n c'(g) & d'(g) \end{pmatrix} =: \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix},$$

which satisfies the condition that $a(g) \pmod{\ell} = \bar{\chi}_1(g)$, $d(g) \pmod{\ell} = \bar{\chi}_2(g)$, and $b \bmod \ell : \Gamma \to \mathbb{F}_\ell$ is nonzero. Moreover, when $n \geq 1$, $c(g) \in \ell\mathbb{Z}_\ell$; and when $n = 0$, our earlier condition also implies that $c(g) \in \ell\mathbb{Z}_\ell$.

We now show that such lattice is unique. Before any discussion, we note that $\Lambda/\varpi\Lambda$ has a unique subrepresentation $\bar{\chi}_1$ and a unique quotient representation $\bar{\chi}_2$. Let Λ_1' be another such lattice; after multiplying an appropriate power of ϖ, we may assume that $\Lambda_1' \subset \Lambda_1$ and $\Lambda_1/\Lambda_1' \cong \mathbb{Z}_\ell/\ell^m\mathbb{Z}_\ell$ for some $m \in \mathbb{Z}_{\geq 0}$. If $m = 0$, our statement already holds. So assume that $m \geq 1$. In this case, we have

$$\frac{\Lambda_1' + \varpi\Lambda_1}{\varpi\Lambda_1} \hookrightarrow \frac{\Lambda_1}{\varpi\Lambda_1} \quad \text{and} \quad \frac{\Lambda_1'}{\varpi\Lambda_1'} \twoheadrightarrow \frac{\Lambda_1'}{\Lambda_1' \cap \varpi\Lambda_1} \cong \frac{\Lambda_1' + \varpi\Lambda_1}{\varpi\Lambda_1}$$

By the first injection, the Γ-action on $\frac{\Lambda_1'+\varpi\Lambda_1}{\varpi\Lambda_1}$ is $\bar{\chi}_1$, but by the second surjective map, the Γ-action on $\frac{\Lambda_1'+\varpi\Lambda_1}{\varpi\Lambda_1}$ is $\bar{\chi}_2$. This is a contradiction.

(3) Suppose that we are placed in the situation as described. We choose

- an element $\tilde{e}_1$ lifting a basis of the rank 1 $\mathbb{Z}_\ell/\ell^n$-module $\ell^n\Lambda_2/\ell^n\Lambda_1 \subseteq \Lambda_1/\ell^n\Lambda_1$, and
- an element $\tilde{e}_2$ lifting a basis of the rank 1 $\mathbb{Z}_\ell/\ell^n$-module $\Lambda_1/\ell^n\Lambda_2 \subseteq \Lambda_2/\ell^n\Lambda_2$

It is clear from our construction that Λ_1 has a basis given by $\{\tilde{e}_1, \tilde{e}_2\}$ and Λ_2 has a basis given by $\{\ell^{-n}\tilde{e}_1, \tilde{e}_2\}$. Moreover, for $i = 1, 2$, the Γ-action on $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell \cdot \tilde{e}_i$ is given by a character $\chi_i^{(n)} : \Gamma \to (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times$. From this, we see that if we write, for $g \in \Gamma$

$$\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

for the representation of Γ with respect to the basis $\{e_1, e_2\}$. Then $a(g) \pmod{\ell^n} = \chi_1^{(n)}$, $d(g) \pmod{\ell^n} = \chi_2^{(n)}$, $c(g) \in \ell^n\mathbb{Z}_\ell$. So we must have

$$\mathrm{Tr}(\rho(g)) = a(g) + d(g) \equiv \chi_1^{(n)}(g) + \chi_2^{(n)}(g) \mod \ell^n.$$

(4) By our assumption, the element $\mathbf{c}$ has two eigenvalues 1 and -1. Let v_+ and v_- denote two nonzero eigenvectors with the given eigenvalues. Write

$$\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_\ell)$$

for the representation with respect to the basis $\{v_+, v_-\}$. Note that

$$\rho(\mathbf{c}g) = \begin{pmatrix} a(g) & -b(g) \\ c(g) & -d(g) \end{pmatrix}$$

Then we have

$$\begin{cases} a(g) + d(g) = \mathrm{Tr}(\rho(g)) \equiv \chi_1(g) + \chi_2(g) \pmod{\ell^n} \\ a(g) - d(g) = \mathrm{Tr}(\rho(\mathbf{c}g)) \equiv \chi_1(\mathbf{c}g) + \chi_2(\mathbf{c}g) = \chi_1(g) - \chi_2(g) \pmod{\ell^n} \end{cases}$$

So we must have $a(g) \equiv \chi_1(g),\ d(g) \equiv \chi_2(g) \pmod{\ell^n}$.

Next, from the upper-left entry of $\rho(g)\rho(h) = \rho(gh)$, we get

$$a(gh) = a(g)a(h) + b(g)c(h)$$

So $b(g)c(h) \equiv 0 \pmod{\ell^n}$ for every $g, h \in \Gamma$. So if m_1 and m_2 are the maximal integers such that $b(g) \in \ell^{m_1}\mathbb{Z}_\ell$ and $c(g) \in \ell^{m_2}\mathbb{Z}_\ell$ for every $g \in \Gamma$. Then we must have $m_1 + m_2 \geq n$. Then with respect to the new basis $\{v_1' = \ell^{m_1}v_1,\ v_2' = v_2\}$

$$\rho'(g) = \begin{pmatrix} \ell^{m_1} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \rho(g) \begin{pmatrix} \ell^{m_1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a(g) & \ell^{-m_1}b(g) \\ \ell^{m_1}c(g) & d(g) \end{pmatrix} =: \begin{pmatrix} a'(g) & b'(g) \\ c'(g) & d'(g) \end{pmatrix}$$

satisfies conditions for (2) with invariant $m_1 + m_2 \geq n$. □

Problem 1.6. (Extensions of groups)

(1) If H is a normal subgroup of a finite group G and H is abelian, show that the quotient group $\Gamma := G/H$ acts naturally on H by conjugation, i.e. for $\gamma \in \Gamma$, pick a lift $\tilde{\gamma}$ of γ in G, then we let γ acts on H by

$$\gamma \star h := \tilde{\gamma} h \tilde{\gamma}^{-1}.$$

Show that this action is well-defined.

(In this situation, we call G an extension of Γ by H.)

(2) Given a finite group Γ acting on a finite abelian group H, then the set of isomorphism classes of extensions of Γ by H can be identified with $H^2(\Gamma, H)$. The identification is given as follows: for G an extension of Γ by H as in (1), for each $\gamma \in \Gamma$, we fix a lift $g(\gamma) \in G$, and set

$$f_{\gamma,\gamma'} := g(\gamma) \cdot g(\gamma') \cdot g(\gamma\gamma')^{-1} \in H.$$

Show that this defines a 2-cocycle in $Z^2(\Gamma, H)$, and a different choice of $g(\gamma)$ amounts to chancing the above 2-cocycle by a 2-coboundary.

(3) Show that G is a semi-direct product $H \rtimes \Gamma$ if and only if the corresponding class of G in $H^2(\Gamma, H)$ is trivial.

Solution. (1) A different lift $\tilde{\gamma}$ is of the form $\tilde{\gamma}' = \tilde{\gamma}h'$ for some $h' \in H$. Then

$$\tilde{\gamma}' h \tilde{\gamma}'^{-1} = \tilde{\gamma} h' h h'^{-1} \tilde{\gamma}^{-1} = \tilde{\gamma} h \tilde{\gamma}^{-1}.$$

So the action $\gamma \star h$ is well-defined.

(2) We first show that $(f_{\gamma,\gamma'})_{\gamma,\gamma'\in\Gamma}$ is a 2-cocycle. We first rewrite the definite of $f_{\gamma,\gamma'}$ as

$$g(\gamma)\cdot g(\gamma') = f_{\gamma,\gamma'}g(\gamma\gamma').$$

Now we consider, for $\gamma,\gamma',\gamma''\in\Gamma$,

$$\begin{aligned} g(\gamma)\cdot g(\gamma')\cdot g(\gamma'') &= f_{\gamma,\gamma'}g(\gamma\gamma')\cdot g(\gamma'') \\ &= f_{\gamma,\gamma'}\cdot f_{\gamma\gamma',\gamma''}g(\gamma\gamma'\gamma''); \\ g(\gamma)\cdot g(\gamma')\cdot g(\gamma'') &= g(\gamma)\cdot f_{\gamma',\gamma''}g(\gamma'\gamma'') \\ &= (\gamma\star f_{\gamma',\gamma''})\cdot g(\gamma)\cdot g(\gamma'\gamma'') \\ &= (\gamma\star f_{\gamma',\gamma''})\cdot f_{\gamma',\gamma''}g(\gamma\gamma'\gamma''). \end{aligned}$$

This implies (by reverting to additive convention as H is abelian)

$$f_{\gamma,\gamma'} + f_{\gamma\gamma',\gamma''} = \gamma\star f_{\gamma',\gamma''} + f_{\gamma',\gamma''},$$

which is precisely the condition that says that $(f_{\gamma,\gamma'})_{\gamma,\gamma'\in\Gamma}$ is a 2-cocycle.

If we make different choices of $g(\gamma)$, say $g'(\gamma) = h_\gamma g(\gamma)$ for $h_\gamma\in H$, then

$$\begin{aligned} g'(\gamma)\cdot g'(\gamma')\cdot g'(\gamma\gamma') &= h_\gamma g(\gamma)\cdot h_{\gamma'}g'(\gamma')\cdot g(\gamma\gamma')^{-1}h_{\gamma\gamma'}^{-1} \\ &= h_\gamma\cdot(\gamma\star h_{\gamma'})\cdot g(\gamma)g(\gamma')g(\gamma\gamma')^{-1}h_{\gamma\gamma'}^{-1} \\ &= h_\gamma\cdot(\gamma\star h_{\gamma'})\cdot f_{\gamma,\gamma'}h_{\gamma\gamma'}^{-1}. \end{aligned}$$

So the so-defined 2-cocycle is differed by a boundary. This implies that extensions of Γ by H (as groups) is classified by $H^2(\Gamma,H)$.

(3) When $G\cong H\rtimes\Gamma$, we may choose the lifting $g:\Gamma\to G$ to be a homomorphism (this is the meaning of semi-direct product). Then $f_{\gamma,\gamma'}=0$ and thus the class of G is zero in $H^2(\Gamma,H)$ is trivial. Conversely, if the class of G is trivial, we may modify it by a boundary, which amounts to changing the lifts $g:\Gamma\to G$, such that $f_{\gamma,\gamma'}$ is the zero cycle. This precisely means that the lift $g:\Gamma\to G$ is a group homomorphism, and thus G is a semi-direct product of H with Γ. □

Problem 1.7. (Ramification filtration for Lubin–Tate tower) In this problem, for a Galois extension L/K, we write $G_{L/K}$ for its Galois group. This is a slight generalization of the cyclotomic case we did in class. Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$, uniformizer ϖ and residue field $k_K=\mathbb{F}_q$. Consider the Lubin–Tate formal group $\mathcal{F}_\varpi$ associated to the polynomial $f(x)=\varpi x+x^q$. Then adjoining the ϖ^∞-torsion of the formal group defines a tower of extension $K_n=K(\pi_n)$ with π_n a generator of $\mathcal{F}_\varpi[\varpi^n]$, i.e. $\pi_1\in K^{\mathrm{alg}}$ is a nonzero root of $f(x)=0$ and $f(\pi_i)=\pi_{i-1}$ for $i\geq 2$. Set $K_\infty:=\bigcup_{n\geq 1}K_n$. Write $K_n^{\mathrm{unr}}:=K_nK^{\mathrm{unr}}$ for $n\geq 1$. Then under the Artin map, we have a canonical isomorphism

$$\mathrm{Art}_K:\mathcal{O}_K^\times/(1+\varpi^n\mathcal{O}_K)^\times\cong G_{K_n^{\mathrm{unr}}/K^{\mathrm{unr}}},\quad\text{and}\quad \mathrm{Art}_K:\mathcal{O}_K^\times\cong G_{K_\infty^{\mathrm{unr}}/K^{\mathrm{unr}}}$$

For each K_n/K, compute the lower numbering ramification filtration and the upper numbering ones, and check that when $m\geq n$,

$$G^v_{K_m/K}G_{K_m/K_n}/G_{K_m/K_n}=G^v_{K_n/K},\qquad\text{for every } v>0.$$

Show that when taking the inverse limit, we get when $v>0$

$$G^v_{K_\infty^{\mathrm{unr}}/K^{\mathrm{unr}}}\cong(1+\varpi^{\lceil v\rceil}\mathcal{O}_K)^\times.$$

Solution. We write $\mathcal{O}_K^{\times,(n)} := 1 + \varpi^n \mathcal{O}_K$, and $f^{[n]}(x) := \underbrace{f \circ \cdots \circ f}_{n \text{ times}}(x)$.

We use the following facts from Lubin–Tate theory:

- The minimal polynomial of π_n over K is
$$f^{[n]}(X)/f^{[n-1]}(X) = X^{q^{n-1}(q-1)} + \cdots + \varpi \in \mathcal{O}_K[X],$$
which is an Eisenstein polynomial. So K_n/K is a totally ramified extension of degree $q^{n-1}(q-1)$, with uniformizer π_n.
- K_n/K is an abelian extension with Galois group
$$G_{K_n/K} \cong (\mathcal{O}_K/\varpi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K/\mathcal{O}_K^{\times,(n)}.$$
Under the LCFT correspondence, K_n/K corresponds to $\varpi^{\mathbb{Z}} \times \mathcal{O}_K^{\times,(n)}$. Moreover, for any $\sigma \in G_{K_n/K}$ corresponding to $u \in \mathcal{O}_K$, we have
$$\sigma(\pi_n) = [u^{-1}]_{\mathcal{F}_\varpi}(\pi_n).$$

We now compute the higher ramification groups. First, $G_{K_n/K,-1} = G_{K_n/K,0} = G_{K_n/K} \cong \mathcal{O}_K/\mathcal{O}_K^{\times,(n)}$ and $G_{K_n/K,1}$ is the p-Sylow group of G_0, i.e. $G_{K_n/K,1} \cong \mathcal{O}_K^{\times,(1)}/\mathcal{O}_K^{\times,(n)}$.

Let $\sigma \neq 1 \in G_{K_n/K,1}$ corresponds to $u \in \mathcal{O}_K^{(1)}$. Suppose $u^{-1} = 1 + \varepsilon\varpi^m$ where $\varepsilon \in \mathcal{O}_K^\times$ and $0 < m < n$. Then
$$\sigma(\pi_n) = [1 + \varepsilon\varpi^m]_{\mathcal{F}_\varpi}(\pi_n) = F_\varpi(\pi_n, [\varepsilon\varpi^m]_{\mathcal{F}_\varpi}(\pi_n)),$$
where $F_\varpi \in \mathcal{O}_K[[X,Y]]$ is the Lubin–Tate formal group law. Since $[\varepsilon\varpi^m]_{\mathcal{F}_\varpi}(\pi_n) \in \mathcal{F}_\varpi[\varpi^{n-m}] \setminus \mathcal{F}_\varpi[\varpi^{n-m-1}]$, $[\varepsilon\varpi^m]_{\mathcal{F}_\varpi}(\pi_n)$ is a uniformizer of K_{n-m}, which has precise valuation $v_{K_n}([\varepsilon\varpi^m]_{\mathcal{F}_\varpi}(\pi_n)) = q^m$. Note that
$$F_\varpi(X,Y) = X + Y + XY \cdot G(X,Y)$$
for some $G(X,Y) \in \mathcal{O}_K[[X,Y]]$. So
$$\sigma(\pi_n) - \pi_n = [\varepsilon\varpi^m](\pi_n) + \text{terms with higher valuations}$$
Hence $v_{K_n}(\sigma(\pi_n) - \pi_n) = q^m$. It follows that
$$G_{K_n/K,i} \cong \mathcal{O}_K^{\times,(k)}/\mathcal{O}_K^{\times,(n)}$$
for $q^{k-1} \leqslant i \leqslant q^k - 1$. By exactly the same argument as in the cyclotomic case from the lecture, we may draw the graph of Herbrand function and see that
$$G^k_{K_n/K} = G_{K_n/K,q^k-1} = \mathcal{O}_K^{\times,(k)}/\mathcal{O}_K^{\times,(n)},$$
for any $1 \leq k \leq n$. Composing with K^{unr}, we get a canonical isomorphism, for any $v > 0$,
$$G^v_{K_n^{\mathrm{unr}}/K} \cong \mathcal{O}_K^{\times,(\lceil v \rceil)}/\mathcal{O}_K^{\times,(n)}.$$
For $m \geqslant n$ and any $v > 0$, the image of $G^v_{K_m/K}$ in $G_{K_n/K}$ is $G^v_{K_n/K}$. Taking the inverse limit, we get when $v > 0$
$$G^v_{K_\infty^{\mathrm{unr}}/K^{\mathrm{unr}}} \cong \mathcal{O}_K^{\times,(\lceil v \rceil)}. \qquad \square$$

Problem 1.8. Decide whether there exists an abelian extension of $K = \mathbb{Q}(\sqrt{3})$ of degree 3, ramified only at the primes of $\mathcal{O}_K$ above 5.

Remark: This is just a very explicit example. It is important to be able to apply abstract heavy theory to a concrete example.

Solution. We first list basic data we need for the field K.

- $K = \mathbb{Q}[\sqrt{3}]$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, $\mathrm{Disc}(K) = 2^2 \cdot 3$, $r_1 = 2$, $r_2 = 0$.
- The rank of $\mathcal{O}_K^\times$ is $r_1 + r_2 - 1 = 1$. The roots of unity contained in K are precisely ± 1. Note that $(x, y) = (2, 1)$ is a minimal solution for the Pell's equation $x^2 - 3y^2 = \pm 1$. So
$$\mathcal{O}_K^\times = \{\pm 1\} \times (2 + \sqrt{3})^{\mathbb{Z}}.$$
- 2 and 3 are ramified in $\mathcal{O}_K$: $2 = (2 + \sqrt{3})(\sqrt{3} - 1)^2$, $3 = (\sqrt{3})^2$.
- For prime $p \neq 2, 3$, p splits in $\mathcal{O}_K$ if and only if $X^2 - 3$ splits in $\mathbb{F}_p$. In particular, 5 and 7 are inert in $\mathcal{O}_K$.
- The class number of K is 1. In other words, $\mathcal{O}_K$ is a PID.

To determine degree 3 abelian extensions that are ramified only at $5\mathcal{O}_K$, we only need to determine the following quotient:
$$G^{\mathrm{ab}}_{K,\{\text{tame at } (5)\}} \cong K^\times \backslash \mathbb{A}_K^\times / \big(K_{\mathbb{R}}^\times (1 + 5\mathcal{O}_{K_{(5)}})^\times \textstyle\prod_{\mathfrak{p} \nmid 5} \mathcal{O}_{K_\mathfrak{p}}^\times\big).$$
Note that the part of the field which is wildly ramified at 5 is always pro-5, which is irrelevant to our discussion. In a same way, the ramification at infinity has degree 2, which is also irrelevant.

As $\mathrm{Cl}(K) = 1$, we can write $\mathbb{A}_K^\times$ as $K^\times \cdot K_{\mathbb{R}}^\times \prod_{\mathfrak{p}} \mathcal{O}_{K_\mathfrak{p}}^\times$. So
$$\begin{aligned} G^{\mathrm{ab}}_{K,\{\text{tame at } (5)\}} &\cong \frac{K^\times \cdot K_{\mathbb{R}}^\times \prod_{\mathfrak{p}} \mathcal{O}_{K_\mathfrak{p}}^\times}{K^\times \cdot \big(K_{\mathbb{R}}^\times (1 + 5\mathcal{O}_{K_{(5)}})^\times \prod_{\mathfrak{p} \nmid 5} \mathcal{O}_{K_\mathfrak{p}}^\times\big)} \\ &\cong \frac{\mathcal{O}_{K_{(5)}}^\times / (1 + 5\mathcal{O}_{K_{(5)}})^\times}{\mathrm{Image}\big(\mathcal{O}_K^\times \to \mathcal{O}_{K_{(5)}}^\times / (1 + 5\mathcal{O}_{K_{(5)}})^\times\big)} \end{aligned} \tag{1.8.1}$$
The quotient $\mathcal{O}_{K_{(5)}}^\times / (1 + 5\mathcal{O}_{K_{(5)}})^\times \cong \mathbb{F}_{25}^\times$ has order 24. Recall that $\mathcal{O}_K$ is generated by -1 and $2 + \sqrt{3}$. -1 is clearly mapped to an element of order 2. For $2 + \sqrt{3}$, note that
$$(2 + \sqrt{3})^3 = 26 + 10\sqrt{3} \in 1 + 5\mathcal{O}_K.$$
So $2 + \sqrt{3}$ is mapped to an element of order 3 in $(\mathcal{O}_K / 5\mathcal{O}_K)^\times \cong \mathbb{F}_{25}^\times$. It follows that the quotient (1.8.1) has order relatively prime to 3. So there does not exist an abelian extension of $K = \mathbb{Q}(\sqrt{3})$ of degree 3, ramified only at the primes of $\mathcal{O}_K$ above 5. □