
Problem 1.1. Let $d \in \mathbb{Z}$ be a square-free integer. Show that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$ for $\zeta_n = e^{2\pi i/n}$ where

$$n = \begin{cases} |d| & \text{if } d \equiv 1 \pmod 4, \\ 4|d| & \text{if } d \not\equiv 1 \pmod 4. \end{cases}$$

Show moreover that this n is the smallest natural number for which such an inclusion holds.

Problem 1.2. Let K/k be an extension of number fields.

(a) Let $p \in \mathbb{N}$ be a prime number which is unramified in k, and let $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spm}(\mathcal{O}_k)$ be two prime ideals above p. Show that if $K \subset k(\zeta_m)$ for some m, then we have:

$$\mathfrak{p} \text{ ramifies in } K/k \quad \Longleftrightarrow \quad \mathfrak{q} \text{ ramifies in } K/k$$

(b) Deduce that if $k \neq \mathbb{Q}$, then there exists an extension K/k of degree $[K:k] = 2$ such that

$$K \not\subset \bigcup_{m \in \mathbb{N}} \mathbb{Q}(\zeta_m).$$

Problem 1.3. Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$.

(a) Show that in $K/\mathbb{Q}$ only the places $2, 5, \infty$ are ramified.

(b) Compute the group $\operatorname{Gal}(K/\mathbb{Q})$, and determine the Frobenii σ_p for all primes $p \neq 2, 5$.

(c) Show that $K \subset \mathbb{Q}(\zeta_{20})$. Deduce that the Artin map gives an isomorphism

$$\operatorname{Cl}(\mathfrak{m})/H \xrightarrow{\sim} \operatorname{Gal}(K/\mathbb{Q})$$

for $\mathfrak{m} = (20)\infty$ and some subgroup $H \subset \operatorname{Cl}(\mathfrak{m})$, and determine this subgroup explicitly.

For a number field K denote by Cl_K its ideal class group and by $H(K)$ its Hilbert class field.

Problem 2.1. Let $K, L \subset \overline{\mathbb{Q}}$ be two number fields.

(a) Show that if $K \subset L$, then $H(K) \subset H(L)$ and $|\mathrm{Cl}_K|$ divides $|\mathrm{Cl}_L| \cdot [L : K]$.

(b) Back to the general case, show that if $\mathrm{Cl}_K = \mathrm{Cl}_L = 1$, then also $\mathrm{Cl}_{K \cap L} = 1$.

Problem 2.2.

(a) Let E/K be an abelian extension of number fields and $L \subset E$ the maximal subextension which is unramified over K. Show that the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to the cokernel of the norm

$$N_{E/K}\colon \quad \mathrm{Cl}_E \longrightarrow \mathrm{Cl}_K.$$

(b) Show that for $n \in \mathbb{N}$ the class number of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ divides the class number of $\mathbb{Q}(\zeta_n)$.

Problem 2.3. The *Hilbert class field tower* of a number field K is the sequence of number fields

$$H_0(K) \subset H_1(K) \subset H_2(K) \subset \cdots \quad \text{defined by} \quad H_0(K) := K \quad \text{and} \quad H_{i+1}(K) := H(H_i(K)).$$

Show that this tower is finite if and only if there exists a finite extension L/K with $\mathrm{Cl}_L = 1$.

Problem 2.4. Let $\alpha \in \overline{\mathbb{Q}}$ be a zero of the polynomial $X^3 - X - 1 \in \mathbb{Z}[X]$, and $K = \mathbb{Q}(\sqrt{-23})$.

(a) Prove that

- $L = K(\alpha)$ is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$,
- $K \subset L$ is an abelian extension of degree three.

(b) Prove that only two primes of $\mathbb{Q}(\alpha)$ ramify over $\mathbb{Q}$, and that they lie over 23 and ∞.

(c) Prove that $K \subset L$ is totally unramified.

(d) Prove that L is the Hilbert class field of K.

Problem 3.1. Show that the category $\mathrm{Mod}(G)$ has enough injectives:

(a) To deal with the case where $G = 1$ is trivial, show first that an abelian group A is injective iff it is *divisible* in the sense that the map $[n]\colon A \to A, a \mapsto n \cdot a$ is surjective for all $n \in \mathbb{N}$. Then show that every abelian group embeds in a divisible group.

(b) In general, for a given $M \in \mathrm{Mod}(G)$, embed the underlying abelian group into a divisible group N. Show that we then have an embedding $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], N)$ of G-modules where the target is an injective G-module as required.

Problem 3.2. Let G be a group and $A \in \mathrm{Mod}(G)$.

(a) Show that we have an isomorphism $Z^1(G, A) \xrightarrow{\sim} \mathrm{Hom}_G(I_G, A), f \mapsto ((g-1) \mapsto f(g))$.

(b) Consider the semidirect product $E = A \rtimes G$ with the projection $p\colon E \to G$. Show that we have
$$Z^1(G, A) \xrightarrow{\sim} \{ s \in \mathrm{Hom}(G, E) \mid p \circ s = \mathrm{id} \}$$

Problem 3.3. Let $G = \mathbb{Z}/2\mathbb{Z}$ act on $A = \mathbb{Z}$ either trivially or by multiplication by ± 1. In both of the two cases, compute the cohomology group $H^2(G, A)$ by hand in terms of cocycles and coboundaries. Use your result to determine up to isomorphism all extensions
$$0 \longrightarrow \mathbb{Z} \longrightarrow E \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Problem 3.4. Let G be a group and $A \in \mathrm{Mod}(G)$. In the lecture we have seen that $H^2(G, A)$ can be identified with the set of isomorphism classes of extensions of G by A.

(a) Fill in the missing details in the proof.

(b) Describe the group structure on $H^2(G, A)$ in terms of extensions.

(c) Now fix an extension $\epsilon\colon [1 \to A \to E \to G \to 1]$. Conjugation by $a \in A$ gives rise to an automorphism
$$\varphi_a \in \mathrm{Aut}(\epsilon), \quad \varphi_a(e) = aea^{-1}$$
where $\mathrm{Aut}(\epsilon)$ denotes the group of automorphisms of the extension as defined in the lecture, i.e. its elements are the group automorphisms $\varphi\colon E \to E$ such that $\varphi|_A = \mathrm{id}_A$ and $\overline{\varphi} = \mathrm{id}_G$ for the induced morphism $\overline{\varphi} \in \mathrm{End}(G)$. Put
$$\mathrm{Out}(\epsilon) = \mathrm{Aut}(\epsilon)/\sim \quad \text{for the equivalence relation } f \sim g \iff \exists a \in A\colon f = c_a \circ g.$$
Show that we have an isomorphism
$$H^1(G, A) \xrightarrow{\sim} \mathrm{Out}(\epsilon).$$

Problem 4.1. Let K/k be a finite Galois extension of fields with Galois group G.

(a) Show that the elements of G are linear independent as elements of the K-vector space of maps $\sigma \colon K \to K$, where the vector space structure is given by pointwise addition and scalar multiplication (you may have seen this in Galois theory). Deduce from this that
$$H^1(G, K^\times) = 0.$$

(b) Use this to find an explicit parametrization for the set $S = \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\}$.

Problem 4.2. Let $G = \mathrm{Gal}(L/K)$ for the field extension $L = \mathbb{Q}_p(\sqrt{p})/K = \mathbb{Q}_p$. Compute the Herbrand quotient
$$h(A) \;=\; \frac{|H^0_T(G, A)|}{|H^1_T(G, A)|}$$
for $A = L^\times \in \mathrm{Mod}(G)$ by looking at the short exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$.

Problem 4.3. Let G be a group, X a free $\mathbb{Z}[G]$-module of finite rank, and $A \in \mathrm{Mod}(G)$. Show that we have a natural isomorphism of abelian groups
$$\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} \mathrm{Hom}_G(X, A).$$
What does this say about the Tate cohomology of $M = \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} A \in \mathrm{Mod}(G)$?

Problem 4.4. Let G be a finite group. We say that an embedding $i \colon A \hookrightarrow B$ of G-modules is *admissible* if on the level of the underlying abelian groups it splits as the inclusion of a direct summand. A module $I \in \mathrm{Mod}(G)$ is called *relatively injective* if the map
$$i^* \colon \mathrm{Hom}_G(B, I) \to \mathrm{Hom}_G(A, I)$$
is surjective for any admissible embedding $i \colon A \hookrightarrow B$ of G-modules.

(a) Show that any free $\mathbb{Z}[G]$-module of finite rank is relatively injective.

(b) Deduce that for any two complete resolutions $X_\bullet, Y_\bullet$ of the trivial G-module $\mathbb{Z}$ with free $\mathbb{Z}[G]$-modules X_i, Y_i of finite rank for $i \in \mathbb{Z}$, there exists a morphism $f \colon X_\bullet \to Y_\bullet$ of complete resolutions and that this morphism is unique up to chain homotopy.

Problem 5.1. Let G be a finite group and $H \subset G$ a subgroup.

(a) Let $s\colon H \setminus G \to G$ be a map giving a coset decomposition $G = \bigsqcup_{x \in H \setminus G} Hs(x)$. Show that the Verlagerung

$$\mathrm{Ver}\colon \quad G^{ab} \longrightarrow H^{ab} \quad \text{is given by} \quad g \mapsto \sum_{x \in H \setminus G} s(x) \cdot g \cdot s(gx)^{-1}$$

(b) Show that if $H = \{\pm 1\} \subset G = \mathbb{F}_p^\times$ for a prime $p > 2$, then the Verlagerung is given by the Legendre symbol (you may use Gauss' lemma about quadratic residues).

Problem 5.2. Consider the symmetric group $G = \mathrm{Sym}_3$.

(a) Use the Hochschild-Serre spectral sequence to compute $H^i_T(G, \mathbb{Z})$ for all $i \in \mathbb{Z}$.

(b) Now let G act on $M = \mathbb{Z}^3$ by permutation of the coordinates, and let $A = M/M^G$ be the quotient modulo the invariants. Compute $H^i_T(G, A)$ for $i = 1, 2$.

Problem 5.3. Let G be a finite group and $A \in \mathrm{Mod}(G)$. We say A is *cohomologically trivial* if $H^i_T(H, A) = 0$ for all subgroups $H \subset G$ and all degrees $i \in \mathbb{Z}$. Find an example of G and A such that

- $H^i_T(G, A) = H^{i+1}_T(G, A) = 0$ for some $i \in \mathbb{Z}$, but
- nevertheless $A \in \mathrm{Mod}(G)$ is not cohomologically trivial.

For instance, you may consider the group $G = \mathbb{Z}/6\mathbb{Z}$ with a suitable action on $A = \mathbb{Z}/3\mathbb{Z}$.

Problem 5.4. Suppose we are given the following diagram whose terms are complexes in an abelian category and whose rows and columns are exact in each degree:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Y' & \longrightarrow & Y & \longrightarrow & Y'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Z' & \longrightarrow & Z & \longrightarrow & Z'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Verify the claim from the lecture that the boundary operators anticommute, i.e. they fit into the commutative diagram:

$$\begin{array}{ccc}
H^{i-1}(Z'') & \xrightarrow{\delta} & H^i(Z') \\
{\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle -\delta} \\
H^i(X'') & \xrightarrow{\delta} & H^{i+1}(X')
\end{array}$$

Problem 6.1. Let G be a profinite group. We say that a closed subgroup $H \leq G$ is *p-Sylow* if for every open normal subgroup $N \trianglelefteq G$ the quotient HN/N is a p-Sylow subgroup of the finite group G/N. Show:

(a) For every prime number p, there exists a p-Sylow subgroup of G.

(b) Every pro-p-subgroup of G is contained in a p-Sylow subgroup. Here by a *pro-p-group* we mean a profinite group that is an inverse limit of finite p-groups.

(c) Any two p-Sylow subgroups of G are conjugate.

Problem 6.2. Find all p-Sylow subgroups of $\widehat{\mathbb{Z}}$ and of $\mathbb{Z}_p^\times$. How about those of $\mathrm{GL}_2(\mathbb{Z}_p)$?

Problem 6.3. Consider the group $\mathrm{GL}_2(\mathbb{Q}_p)$ with its natural topology

(a) Show that $\mathrm{GL}_2(\mathbb{Q}_p)$ is a totally disconnected, locally compact Hausdorff group.

(b) Show that the subgroup $\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$ is open and compact.

(c) More generally, show that any compact subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ lies in a maximal compact subgroup and that the maximal compact subgroups are precisely the subgroups of the form
$$\mathrm{Stab}(L) \;=\; \big\{g \in \mathrm{GL}_2(\mathbb{Q}_p) \mid gL = L\big\}$$
where $L \subset \mathbb{Q}_p^2$ is a *lattice*, i.e. a free $\mathbb{Z}_p$-submodule of rank two.

Problem 6.4. For a topological group G and a continuous G-module A, define the continuous cohomology by
$$H^i(G,A) \;:=\; Z^i_{cont}(G,A)/B^i_{cont}(G,A)$$
where $B^i_{cont}(G,A) \subset Z^i_{cont}(G,A)$ denotes the group of continuous coboundaries resp. cochains.

(a) Show that for G profinite we have a natural isomorphism
$$H^i(G,A) \;\xrightarrow{\sim}\; \varinjlim H^i(G/N, A^N)$$
where the limit is taken over the collection of all open normal subgroups $N \trianglelefteq G$.

(b) The abstract group cohomology is recovered as the continuous cohomology $H^i(G_d, A)$ where G_d denotes the abstract group G endowed with the discrete topology. Show that in general
$$H^i(G_d, A) \;\not\simeq\; H^i(G,A),$$
for example by taking $G = \widehat{\mathbb{Z}}$ with the trivial action on the discrete G-module $A = \widehat{\mathbb{Z}}$.

Can you also find an example where the module $A \in \mathrm{Mod}(G)$ is finite?

Problem 7.1. Let K be a field of characteristic $\mathrm{char}(K) \neq 2$. For $a, b \in K^\times$ let $\mathcal{H}(a,b)$ denote the K-algebra with a K-basis $1, i, j, k$ and multiplication given by $i^2 = a, j^2 = b, ij = -ji = k$.

(a) Show that $\mathcal{H}(a,b)$ is a four-dimensional central simple algebra over K, and that every four-dimensional central simple algebra over K arises like this for some a, b.

(b) Show that $\mathcal{H}(a,b)$ is either a division algebra or isomorphic to $\mathrm{Mat}_{2\times 2}(K)$, and show that

$$\begin{aligned} \mathcal{H}(a,b) \simeq \mathrm{Mat}_{2\times 2}(K) \quad &\Longleftrightarrow \quad \exists (x,y,w) \in K^3 \setminus \{0\}\colon \quad ax^2 + by^2 = w^2 \\ &\Longleftrightarrow \quad a \in N_{K(\sqrt{b})/K}(K(\sqrt{b})^\times) \end{aligned}$$

(c) Observe that

- $\mathcal{H}(1,b) \simeq \mathcal{H}(a,-a) \simeq \mathrm{Mat}_{2\times 2}(K)$
- $\mathcal{H}(a,b) \simeq \mathcal{H}(ax^2, by^2)$ for all $x, y \in K^\times$
- $\mathcal{H}(a, 1-a) \simeq \mathrm{Mat}_{2\times 2}(K)$ if $a, 1-a \in K^\times$

(d) Show that $\mathcal{H}(a,b)^{\mathrm{op}} \simeq \mathcal{H}(a,b)$, hence we have $2 \cdot [\mathcal{H}(a,b)] = 0$ in $\mathrm{Br}(k)$.

Problem 7.2. Let L/K be a cyclic Galois extension of degree n, and $\sigma \in G = \mathrm{Gal}(L/K)$ a generator of its Galois group. Show that we have an isomorphism

$$K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Br}(L/K), \quad b \mapsto [\,\mathcal{A}(\sigma, b)\,]$$

where $\mathcal{A}(\sigma, b)$ denotes the K-algebra whose underlying vector space is $\mathcal{A}(\sigma,b) := \bigoplus_{i=0}^{n-1} L \cdot \beta^i$ for formal basis vectors β^i with multiplication defined by

$$\beta^n := b \quad \text{and} \quad \beta \cdot z := \sigma(z) \cdot \beta \quad \text{for} \quad z \in K.$$

Problem 7.3. Let K be a field containing a primitive root of unity $\zeta \in K$, and let $L = K(\sqrt[n]{a})$ for some $a \in K$. Show that if $[L : K] = n$, then for the automorphism $\sigma \in \mathrm{Gal}(L/K)$ defined by

$$\sigma(\sqrt[n]{a}) = \zeta \cdot \sqrt[n]{a}$$

the algebra $\mathcal{A}(\sigma, 1-a)$ splits, i.e. its class in the Brauer group $\mathrm{Br}(L/K)$ is trivial.

Problem 7.4. Let K be a field that contains a primitive root of unity $\zeta \in K$. Show that for all $a, b \in K^\times$ we have:

$$a \in N_{K(\sqrt[n]{b})/K}(K(\sqrt[n]{b})^\times) \quad \Longleftrightarrow \quad b \in N_{K(\sqrt[n]{a})/K}(K(\sqrt[n]{a})^\times)$$

Problem 8.1. Let L/K be an extension of local fields. In local class field theory we have used that if the extension is unramified, then $H^i(\mathrm{Gal}(L/K), \mathscr{O}_L^*) = 0$ for all $i > 0$. Give an example of a cyclic ramified extension of local fields with

$$H^i(\mathrm{Gal}(L/K), \mathscr{O}_L^*) \neq 0 \quad \text{for some} \quad i > 0.$$

Problem 8.2. Let $K/\mathbb{Q}_p$ be a finite extension.

(a) A Galois extension L/K is called a $\mathbb{Z}_p$-extension if $\mathrm{Gal}(L/K) \simeq \mathbb{Z}_p$. Show that for the field

$$M := (\text{composite of all } \mathbb{Z}_p\text{-extensions } L/K) \subset \overline{K}$$

the group $\mathrm{Gal}(M/K)$ is a free $\mathbb{Z}_p$-module, and determine the rank of this free module.

(b) Show that there is a unique unramified $\mathbb{Z}_p$-extension L/K, and describe this extension explicitly by adjoining certain roots of unity to the base field K.

Problem 8.3. Let $K/\mathbb{Q}_p$ be a finite extension and $\Gamma = \mathrm{Gal}(K^{\mathrm{ur}}/K)$. Show that

(a) $H^1(\Gamma, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$,

(b) $H^1(\Gamma, \mu_n(\overline{K})) \simeq (\mathscr{O}_K^* \cdot K^{*n})/K^{*n}$ if $p \nmid n$.

Problem 8.4. Let $K/\mathbb{Q}_p$ be a finite extension, and let $G_K = \mathrm{Gal}(\overline{K}/K)$ act on $\mu_n = \mu_n(\overline{K})$.

(a) Show that the local norm residue symbol $(-, K)\colon K^* \to G_K^{ab}$ induces a nondegenerate pairing

$$\beta_K\colon \quad H^1(G_K, \mathbb{Z}/n\mathbb{Z}) \times H^1(G_K, \mu_n) \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad (\chi, a) \mapsto \chi((a, K)).$$

(b) Show that for $p \nmid n$, the orthocomplement of $H^1(\mathrm{Gal}(K^{\mathrm{ur}}/K), \mathbb{Z}/n\mathbb{Z}) \subset H^1(G_K, \mathbb{Z}/n\mathbb{Z})$ with respect to this pairing is

$$H^1(\mathrm{Gal}(K^{\mathrm{ur}}/K), \mu_n) \subset H^1(G_K, \mu_n).$$

(c) Show that for any finite extension L/K and for all $\chi \in H^1(G_K, \mathbb{Z}/n\mathbb{Z})$, $a \in H^1(G_L, \mu_n)$ we have

$$\beta_L(\mathrm{res}(\chi), a) = \beta_K(\chi, N_{L/K}(a))$$

for the maps

$$\mathrm{res}\colon H^1(G_K, \mathbb{Z}/n\mathbb{Z}) \to H^1(G_L, \mathbb{Z}/n\mathbb{Z}) \quad \text{and} \quad N_{L/K}\colon H^1(G_L, \mu_n) \to H^1(G_K, \mu_n).$$

(d) Show that analogous statements hold if $\mathbb{Z}/n\mathbb{Z}$ is replaced by any finite G_K-module A and μ_n is replaced by

$$A' = \mathrm{Hom}(A, \overline{K}^*).$$

Problem 9.1. Let F be a formal group law over a commutative ring R.

(a) Show that $F(X,0) = X$ and $F(0,Y) = Y$.

(b) Show that there is a unique power series $i \in TR[[T]]$ with $F(X, i(X)) = 0$.

(c) Check that the set $\mathrm{End}(F)$ is a ring for the addition and multiplication

$$(\phi +_F \psi)(T) := F(\phi(T), \psi(T)) \quad \text{and} \quad (\phi \cdot_F \psi)(T) := \phi(\psi(T)).$$

Problem 9.2. Let R be a commutative $\mathbb{Q}$-algebra.

(a) Show that for any formal group law F over R, there is a unique isomorphism of formal group laws

$$\log_F\colon \quad F \xrightarrow{\sim} \widehat{\mathbb{G}}_a \quad \text{such that} \quad \log_F(T) \equiv T \pmod{T^2}.$$

(b) Write down this isomorphism explicitly for the formal group law $F = \widehat{\mathbb{G}}_m$ over R.

Problem 9.3. Let $K/\mathbb{Q}_p$ be finite. Fix a uniformizer $\pi \in \mathscr{O}_K$ and put $q = |\mathscr{O}_K/\pi\mathscr{O}_K|$. Show that the series $f(t) = \sum_{n\geq 0} \pi^{-n} \cdot t^{q^n} \in K[[t]]$ has an inverse $f^{-1}(t)$ with respect to composition and that

$$\begin{aligned} F(x,y) &= f^{-1}(f(x) + f(y)), \\ [a]_F(t) &= f^{-1}(af(t)) \quad \text{for} \quad a \in \mathscr{O}_K \end{aligned}$$

defines a Lubin-Tate module whose logarithm in the sense of the problem 9.2(a) is $\log_F = f$.

Problem 9.4. Let $K/\mathbb{Q}_p$ be finite. Show that if F_1, F_2 are two Lubin-Tate modules over $\mathscr{O}_K$ for *different* uniformizers $\pi_1 \neq \pi_2 \in \mathscr{O}_K$, then they are not isomorphic.

Problem 9.5. For a finite extension $K/\mathbb{Q}_p$, denote by $\widehat{K}$ the completion of K^{ur}/K.

(a) Show that the Frobenius extends to a continuous automorphism $\varphi\colon \widehat{K} \to \widehat{K}$ and that we have exact sequences

$$0 \longrightarrow \mathscr{O}_K \longrightarrow \mathscr{O}_{\widehat{K}} \xrightarrow{f} \mathscr{O}_{\widehat{K}} \longrightarrow 0 \qquad \text{where } f(x) = \varphi(x) - x,$$

$$1 \longrightarrow \mathscr{O}_K^* \longrightarrow \mathscr{O}_{\widehat{K}}^* \xrightarrow{g} \mathscr{O}_{\widehat{K}}^* \longrightarrow 1 \qquad \text{where } g(x) = \varphi(x)/x.$$

(b) Use this to fill in the details in the proof of the following claim from the lecture: Given two uniformizers $\pi, \tilde{\pi} \in \mathscr{O}_K$ and Lubin-Tate polynomials $e \in \mathscr{E}_\pi, \tilde{e} \in \mathscr{E}_{\tilde{\pi}}$, there exists a power series

$$\theta(T) = \epsilon T + \cdots \in \mathscr{O}_{\widehat{K}}[[T]]$$

with $\epsilon \in \mathscr{O}_{\widehat{K}}^*$ such that $\theta^\varphi(e(T)) = \tilde{e}(\theta(T))$ and $\theta^\varphi(T) = \theta([u]_e(T))$ for $u = \tilde{\pi}/\pi$.

Problem 10.1. Fill in the online evaluation[1] for the lecture *before January 21.*

Problem 10.2. Let L/K be a Galois extension of number fields with group $G = \mathrm{Gal}(L/K)$.

(a) Find an example where the natural map $\mathrm{Cl}_K \longrightarrow (\mathrm{Cl}_L)^G$ is not injective.

(b) Find an example where the natural map $\mathrm{Cl}_K \longrightarrow (\mathrm{Cl}_L)^G$ is not surjective.

Problem 10.3. Let K be a number field. As an additive version of the idèles one defines the ring of adèles by

$$\mathbb{A}_K \;:=\; \Big\{ (a_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p} \mid a_\mathfrak{p} \in \mathscr{O}_{K_\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p} \nmid \infty \Big\} \;\subset\; \prod_\mathfrak{p} K_\mathfrak{p}.$$

Show:

(a) $\mathbb{A}_K$ is a topological ring for the topology where a basis of open subsets is defined by the subsets

$$\prod_{\mathfrak{p} \in S} W_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} \mathscr{O}_{K_\mathfrak{p}} \;\subset\; \mathbb{A}_K \qquad \text{for } S \supset S_\infty \text{ finite and } W_\mathfrak{p} \subset K_\mathfrak{p} \text{ open.}$$

(b) We have a natural embedding $\mathbb{I}_K \hookrightarrow \mathbb{A}_K$ but the topology on the idèles is *not* induced by the one on adèles via this embedding. However, it is induced by the topology on $\mathbb{A}_K^2$ via the embedding

$$\mathbb{I}_K \;\hookrightarrow\; \mathbb{A}_K^2, \quad x \;\mapsto\; (x, x^{-1}).$$

In other words: The idèle topology comes from the identification $\mathbb{I}_K = \mathrm{GL}_1(\mathbb{A}_K) \subset \mathbb{A}_K^2$.

[1] Hint: Click on the link *Diesen Kurs jetzt evaluieren* or *Evaluate this course now* at the right upper corner of the moodle page. This is very important even if you feel that you don't have to say much: If < 5 students participate, I won't receive any of their evaluations. The evaluation form seems to be in German only, but you are allowed to use `www.deepl.com` or any other device of your choice. Thanks for your feedback!

Problem 11.1. Let L/K be an extension of number fields.

(a) Show that for any place $\mathfrak{p}$ of K we have $L \otimes_K K_\mathfrak{p} \xrightarrow{\sim} \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$.

(b) Deduce that for the ring of adèles we have a natural isomorphism $\mathbb{A}_K \otimes_K L \xrightarrow{\sim} \mathbb{A}_L$.

Problem 11.2. Let K be a number field. Show:

(a) $\mathscr{O}_K \subset \mathbb{A}_K$ maps to a lattice in the $\mathbb{R}$-vector space $\mathbb{A}_{K,\infty} = \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}$.

(b) $K \subset \mathbb{A}_K$ is a discrete subgroup.

(c) $\mathbb{A}_{K,\infty} \times \prod_{\mathfrak{p}\nmid\infty} \mathscr{O}_{K_\mathfrak{p}} \subset \mathbb{A}_K$ surjects onto the quotient $\mathbb{A}_K/K$.

Deduce from this that the quotient $\mathbb{A}_K/K$ is a compact Hausdorff group.

Problem 11.3. Let $\mathbb{S} := (\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ for the embedding $\mathbb{Z} \hookrightarrow \mathbb{R} \times \widehat{\mathbb{Z}}, n \mapsto (n, n)$. Show:

(a) $\mathbb{S}$ is a connected compact Hausdorff group.

(b) We have an isomorphism $\mathbb{S} \simeq \mathbb{A}_\mathbb{Q}/\mathbb{Q}$ of topological groups.

(c) There is a non-split short exact sequence $0 \to \widehat{\mathbb{Z}} \to \mathbb{S} \to \mathbb{R}/\mathbb{Z} \to 0$.

Problem 11.4. Show that as a topological group the idèle class group of the field $\mathbb{Q}$ is given by

$$C_\mathbb{Q} \;\simeq\; \widehat{\mathbb{Z}}^\times \times \mathbb{R}.$$

Determine the connected component of the identity in this group, and the subgroup $C_\mathbb{Q}^0 \subset C_\mathbb{Q}$ of idèles of absolute norm one. Can you give a similar description for the idèle class groups of the number fields

$$K \;=\; \mathbb{Q}(i) \quad \text{and} \quad L \;=\; \mathbb{Q}(\sqrt{2})?$$

Problem 12.1. Solve problems 11.3 and 11.4 that we haven't discussed last time.

Problem 12.2. Let L/K be a Galois extension of number fields. We say that a prime ideal of $\mathcal{O}_K$ *does not split* in the extension if there is a unique prime ideal of $\mathcal{O}_L$ above it. Show that the following statements hold:

(a) If L/K is not cyclic, there are only finitely primes that do not split in L/K.

(b) If L/K is cyclic of degree a prime power, there are infinitely many such primes.

Problem 12.3. Let L/K be a Galois extension of number fields. Show that its Galois group is generated by the Frobenii of unramified primes, i.e.

$$\mathrm{Gal}(L/K) \;=\; \big\langle \; \mathrm{Frob}_{\mathfrak{P}} \mid \mathfrak{P} \trianglelefteq \mathcal{O}_L \text{ prime ideal which is unramified in } L/K \; \big\rangle.$$

Problem 12.4. Let K be a number field. Let $L_1, \ldots, L_n$ be cyclic extensions of K which all have the same prime degree $[L_i : K] = p$ and which are pairwise linearly disjoint in the sense that $L_i \cap L_j = K$ for all $i \neq j$. Show that there exist infinitely many prime ideals $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ such that

- $\mathfrak{p}$ does not split in L_1, but
- $\mathfrak{p}$ splits completely in L_i for all $i > 1$.