Théorie des Nombres TD7

M2 AAG 2021-2022

Exercice 1. Let E/F be a finite extension of number fields.

1. Explain why there exists an infinite number of primes of F totally split in E.

2. Show that if E/F isn't cyclic, there is no prime of F inert in E. What happens when E/F is cyclic?

Exercice 2. We assume the local statement for local class field theory as given in the course. Let F be a local field and $\overline{F}$ an algebraic closure. We denote

$$G_F := \mathrm{Gal}(\overline{F}/F) = \varprojlim_{F \subset L \subset \overline{F}} \mathrm{Gal}(L/F).$$

1. Show that there exists a (unique) continuous map

   $$r_F : F^\times \longrightarrow G_F^{ab},$$

   such that for all finite abelian extension L/F,

   $$\pi_L \circ r_F : F^\times \longrightarrow G_F^{ab} \longrightarrow \mathrm{Gal}(L/F)$$

   factor through $F^\times / N_{L/F}(L^\times)$ and coincides with $r_{L/F}$.

2. Show that r_F has dense image.

3. Show that we have the commutative diagram

$$\begin{array}{ccc} F^\times & \xrightarrow{\quad r_F \quad} & G_F^{ab} \\ \Big\downarrow v & & \Big\downarrow \\ \mathbb{Z} & \xrightarrow{1 \mapsto \mathrm{Frob}_q} & \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \end{array}$$

4. Show that r_F induces an homeomorphism from $\mathcal{O}_F^\times$ to I_F^{ab}, the inertia subgroup.

5. Show that r_F is injective and induces and isomorphism

$$r_F : \widehat{F^\times} \longrightarrow G_F^{ab}.$$

Remark 1. Sometimes we denote by W_F the preimage of $\mathbb{Z} \subset \widehat{\mathbb{Z}} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ in G_F. This is the Weil group of F, and r_F is an homeomorphism from $F^\times$ to W_F (but careful that W_F ***does not*** have the subspace topology of G_F !).

Exercice 3 (Local CFT implies Kronecker-Weber). Assume that $F = \mathbb{Q}_p$ here, and that all statement of the previous exercise are true.

1. Show that the map

$$G_{\mathbb{Q}_p}^{ab} \longrightarrow \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p),$$

induces an isomorphism when restricted to $I_{\mathbb{Q}_p}^{ab}$. *Hint : Show that the cyclotomic extension is totally ramified with Galois group* $\mathbb{Z}_p^\times$.

2. Show the local Kronecker-Weber theorem :

Theorem 1. *Any finite abelian extension* L *of* $\mathbb{Q}_p$ *is included in* $\mathbb{Q}_p(\zeta_n)$ *for some* n.

Hint : Consider $\mathbb{Q}_p^{ab}$ *the maximal abelian extension and* $E = \bigcup_n \mathbb{Q}_p(\zeta_n)$, *and show that they both contain* $\mathbb{Q}_p^{nr}$

3. Deduce the global Kronecker-Weber theorem :

Theorem 2. *Let* K *be a finite abelian extension of* $\mathbb{Q}$. *There exists* n *such that* $K \subset \mathbb{Q}(\zeta_n)$.

Hint : use the local Kronecker Weber at ramified places for K *to find a suitable field* $L = K(\zeta_n)$. *Look at the local intertia subgroups and prove they are small enough. Let* I *be the generated subgroup in* $\mathrm{Gal}(L/\mathbb{Q})$ *and estimate* $[L : \mathbb{Q}]$.

Exercice 4.

1. What are the Hilbert class field and extended/narrow Hilbert class field of $\mathbb{Q}$?

2. Let $m \in \mathbb{N}_{\geqslant 1}$ and $\mathfrak{m}_1 = m$ and $\mathfrak{m}_2 = m(\infty)$. What are the Ray class fields for $\mathfrak{m}_1$ and $\mathfrak{m}_2$?

3. Let $K/\mathbb{Q}$ be an abelian extension, and let $\mathrm{Art}_{K/\mathbb{Q}} : \mathbb{A}_{\mathbb{Q}}^{\times} \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$ be the Artin Reciprocity map. Find the smallest modulus $\mathfrak{m}$ such that $\mathrm{Art}_{K/\mathbb{Q}}$ factors through $\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}V_{\mathfrak{m}}$. What is the smallest n such that $K \subset \mathbb{Q}(\zeta_n)$?

4. Show that the abelian inverse Galois problem holds for $\mathbb{Q}$, i.e. any finite abelian group is the Galois group of some finite extension $K/\mathbb{Q}$.

Exercice 5. 1. Let $K = \mathbb{Q}(\sqrt{3})$. Show that $h_K = 1$. What is the Hilbert class field of K ?

2. Let $L = K(i) = \mathbb{Q}(i, \sqrt{3})$. Show that L/K is unramified everywhere. Why is it not a contradiction with the previous question ?

3. Let $K = \mathbb{Q}(i\sqrt{5})$. What is the Hilbert class field and narrow/extended Hilbert class field for K ?

4. Let $d > 0$ and $K = \mathbb{Q}(\sqrt{d})$. We denote by C and $C_{\mathfrak{m}}$, with $\mathfrak{m} = (\infty)$[1] the Class group and Extended/Narrow class group. Show that we have an exact sequence

$$0 \longrightarrow Ker \longrightarrow C_{\mathfrak{m}} \longrightarrow C \longrightarrow 0,$$

with Ker of cardinal at most 2.

5. Fix τ_1 one real embedding of K, and denote τ_2 the other one. We say that an element x of K is positive if $\tau_1(x) > 0$ and totally positive if moreover $\tau_2(x) > 0$. Show that Ker is non-trivial iff all units which are positive are totally positive.

6. Recall why $\mathcal{O}_K^{\times} = \{\pm 1\} \times < u >$ for some positive fundamental unit. Show that the Hilbert class field of K coincides with the extended Hilbert class field iff $Nm(u) = -1$.

7. Calculate for $\mathbb{Q}(\sqrt{d})$, with $d = 2, 3, 5, 6$ the extended Hilbert class fields and Hilbert class fields.

Exercice 6 (A counter example to Hasse's principle). Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Denote $N = N_{E/\mathbb{Q}}(E^{\times})$.

1. What is the Galois group of $E/\mathbb{Q}$? What are the intermediate extensions $E/K_i/\mathbb{Q}$?

[1] or $\mathfrak{m} = (\tau_1)$ one real embedding, it doesn't change anything as $-1 \in K^{\times}$

2. Let p be a prime, show that p splits completely in one of the three intermediate extension.

3. Show that every square (in $\mathbb{Q}$) is a local norm everywhere.

4. Denote $N_i = N_{K_i/\mathbb{Q}}(K_i^\times)$. Show that $N_1N_2N_3 = \{ x \in \mathbb{Q}^\times | \, x^2 \in N\}$.

Recall the Hilbert Symbol for $a, b \in \mathbb{Q}_v^\times$, $(a,b)_{\mathbb{Q}_v}$, which takes value 1 if $ax^2 + by^2 = z^2$ has a non zero solution in $\mathbb{Q}_v$. We denote $(a,b)_v$ for $a, b \in \mathbb{Q}^\times$ for $(a,b)_{\mathbb{Q}_v}$.

5. Show that $(a,b)_{\mathbb{Q}_v} = 1$ iff b is a norm for the extension $\mathbb{Q}_v(\sqrt{a})/\mathbb{Q}_v$.

6. Show that if $a, b \in \mathbb{Q}^\times$, then
$$\prod_v (a,b)_v = 1.$$

7. Denote $K_i = \mathbb{Q}(\sqrt{a_i})$ and S_i the set of (rational) primes which splits in K_i. Define
$$\phi_{1,2}(x) = \prod_{v \in S_1} (a_2, x)_v.$$
Show that $\phi_{1,2} = \phi_{1,3} = \phi_{2,1} = \phi_{2,3} = \phi_{3,1} = \phi_{3,2} =: \phi$.

8. Show that $N_1N_2N_3 = \ker \phi$.

9. Show that if x is a product of primes p such that $\left(\frac{p}{13}\right) = -1$ then
$$\phi(x) = \left(\frac{x}{17}\right).$$

10. Show that 5^2 is not a global norm.