June 11th, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 9[1]

Exercise 1. Let K be a number field. Prove that there is a finite field extension L of K such that any ideal $\mathfrak{a} \subseteq O_K$ becomes principal in O_L (i.e. $\mathfrak{a}O_L$ becomes principal). (Hint: for any $\mathfrak{a} \subseteq O_K$, use the fact that $\mathrm{Cl}(O_K)$ is finite to construct a principal ideal $(a) \subseteq O_K$ which equals to some power of $\mathfrak{a}$, then use a to construct a finite extension L of K in which $\mathfrak{a}$ becomes principal, then repeat.)

Exercise 2. Let K be a number field and $\mathfrak{a}$ an ideal in $\mathcal{O}_K$. Show that if $\mathbb{N}(\mathfrak{a}) = p$ with p a prime number, then $\mathfrak{a}$ is a prime ideal and $p \in \mathfrak{a}$.

Exercise 3. Let L/K be a finite Galois extension of number fields. Let $\mathfrak{q}$ be a maximal ideal of O_L, $\mathfrak{p} := O_K \cap \mathfrak{q}$. Any $\sigma \in \mathrm{Gal}(L/K)$ induces an automorphism of the O_K-algebra O_L. Let $D_\mathfrak{q}$ be the subgroup of $\mathrm{Gal}(L/K)$ consisting of elements which send $\mathfrak{q}$ to itself via the induced automorphism of O_L. If $\sigma \in D_\mathfrak{q}$, then σ induces an automorphism of the field $\kappa(\mathfrak{q}) := O_L/\mathfrak{q}$ and this automorphism fixes the subfield

$$\kappa(\mathfrak{p}) := O_K/\mathfrak{p} \subseteq O_L/\mathfrak{q} = \kappa(\mathfrak{q}).$$

Let $I_\mathfrak{q}$ be the subgroup of $D_\mathfrak{q}$ consisting of elements which induces the identity field automorphism of $\kappa(\mathfrak{q})$.

(1) Show that there is an exact sequence of groups

$$1 \to I_\mathfrak{q} \to D_\mathfrak{q} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \to 1.$$

(2) Show that $I_\mathfrak{q}$ is trivial if and only if $\mathfrak{q}$ is unramified.

Now suppose that L/K is a finite abelian extension, i.e. $\mathrm{Gal}(L/K)$ is a finite abelian group.

(3) Show that if $\mathfrak{q}' \subseteq O_L$ is another maximal ideal lying over $\mathfrak{p}$, then $D_\mathfrak{q} = D_{\mathfrak{q}'}$ as subgroups of $\mathrm{Gal}(L/K)$.

(4) Show that for any unramified maximal ideal $\mathfrak{q}$ of L lying over $\mathfrak{p}$ there is a unique element $\sigma \in G_\mathfrak{q} \subseteq \mathrm{Gal}(L/K)$ having the effect

$$\sigma\alpha \equiv \alpha^q \pmod{\mathfrak{q}} \qquad \alpha \in O_L$$

where q is the cardinality of the residue field $\kappa(\mathfrak{p})$, and this element $\sigma \in \mathrm{Gal}(L/K)$ depends only on $\mathfrak{p}$ and L/K but not on

[1] If you want your solutions to be corrected, please hand them in just before the lecture on June 18. If you have any questions concerning these exercises you can contact Lei Zhang via l.zhang@fu-berlin.de or come to Arnimallee 3 112A.

$\mathfrak{q}$. This element σ is usually denoted by $(\mathfrak{p}, L/K)$, and is called *the Artin Symbol*.

(5) Show that if L/K is unramified, i.e. each maximal ideal of O_L is unramified, then the Artin symbol defines a group homomorphism $\phi : \mathrm{Id}(O_K) \to \mathrm{Gal}(L/K)$.

(6) If L/K is unramified, and if each principal ideal $(a) \subseteq O_K$ goes to the trivial element of $\mathrm{Gal}(L/K)$ under ϕ, then ϕ induces a map

$$\mathrm{Cl}(O_K) \to \mathrm{Gal}(L/K).$$

If the map is an isomorphism then we call L the *Hilbert Class Field* of K. Show that if L is the Hilbert class field of K, then a maximal ideal $\mathfrak{p}$ of O_K is principal if and only if it splits completely in O_L.

Remark 1. In fact, for any number field K, the Hilbert class field does exist. It is the maximal unramified abelian extension of K. We have seen that the Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself (Theorem 4.9. in `http://jmilne.org/math/CourseNotes/ANT.pdf`). But unlike $\mathbb{Q}$, for arbitrary number field K, whenever $\mathrm{Cl}(O_K)$ is non-trivial the Hilbert class field provides a non-trivial extension which is unramified everywhere.

Exercise 4. Let $L = \mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$, $K = \mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$.

(1) Compute $\mathrm{disc}(L/K)$ and $\mathrm{disc}(K/\mathbb{Q})$.

(2) Conclude that the ring of integers of L is $\mathbb{Z}[i, \frac{1+\sqrt{5}}{2}]$. (Hint: recall that if A is a PID with fraction field K, L/K be a finite separable extension of degree m, $(\alpha_1, \cdots, \alpha_m)$ be elements contained in the integral closure B of A in L. If the discriminant of $(\alpha_1, \cdots, \alpha_m)$ from B to A is square free, then it is an integral basis of B over A, so in particular $B = A[\alpha_1, \cdots, \alpha_m]$.)

(3) Find all the ramified primes for the extension $L/\mathbb{Q}$ and determine their ramification indices.

(4) Deduce that L is the Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$. (Hint we have seen that $\mathrm{Cl}(O_{\mathbb{Q}[\sqrt{-5}]})$ is of order 2 in Ex.8.4..)