May 28, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 7[1]

Exercise 1. Let d be a square-free integer, $K := \mathbb{Q}(\sqrt{d})$.

(a) If $d \equiv 2$ or $3 \mod 4$, show that the discriminant δ of K is $4d$.
(b) If $d \equiv 1 \mod 4$, show that $\delta = d$.
(c) Conclude that in both cases $\{1, \frac{(\delta+\sqrt{\delta})}{2}\}$ is a $\mathbb{Z}$-basis for the ring of integers $\mathcal{O}_K$ of K. This is a uniform formula for a $\mathbb{Z}$-basis of $\mathcal{O}_K$. (*Hint:* You already know a $\mathbb{Z}$-basis for $\mathcal{O}_K$; compare it with the one given in this exercise.)

Exercise 2. Let p be a prime number.

(a) Show that the polynomial $f := X^p + tX^{p-1} - t \in \mathbb{F}_p(t)[X]$ is irreducible, and define $L := \mathbb{F}_p(t)[X]/(f)$.
(b) Let A be the integral closure of $\mathbb{F}_p[t]$ in L. Compute the ramification behaviour of the prime ideal (t) in A.
(c) If $p = 3$, compute the discriminant of $L/\mathbb{F}_3(t)$ with respect to the basis $1, X, X^2$.

Exercise 3. Let $p > 2$ be an odd prime number, and let $\zeta \in \mathbb{C}$ a primitive p-th root of unit (i.e. $\zeta^p = 1$, and $\zeta^r \neq 1$ for all $0 < r < p$).

(a) Write

$$\Phi_p(X) := X^{p-1} + X^{p-2} + \ldots + X + 1.$$

Show that Φ_p is irreducible, and the minimal polynomial of ζ in $\mathbb{Q}(\zeta)$. Show that the roots of $\Phi_p(X)$ are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. (*Hint*: It is easier to show that $\Phi_p(X+1)$ is irreducible.)

(b) Let A be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta)$. Show that for every $1 \leq i \leq p-1$ there exists a unit $u_i \in A^\times$, such that $(1-\zeta^i) = u_i(1-\zeta)$. Conclude that $p = u(1-\zeta)^{p-1}$ with $u = u_1 \cdot \ldots \cdot u_{p-1}$, and that $(1-\zeta)A \cap \mathbb{Z} = p\mathbb{Z}$.

(c) For $x \in A$, there exist unique $a_0, \ldots, a_{p-2} \in \mathbb{Q}$, such that

$$x = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},$$

show by induction that the a_i lie in $\mathbb{Z}$, and hence that $A = \mathbb{Z}[\zeta]$. (*Hint*: Show that $\mathrm{Tr}(\zeta) = \mathrm{Tr}(\zeta^2) = \ldots = \mathrm{Tr}(\zeta^{p-2})$. From this compute $\mathrm{Tr}(x(1-\zeta)) = a_0 p$ and that $\mathrm{Tr}(x(1-\zeta)) \in (1-\zeta)A \cap \mathbb{Z}$, which is $p\mathbb{Z}$ by (b). Then conclude by induction).

[1] If you want your solutions to be corrected, please hand them in just before the lecture on June 4th. If you have any questions concerning these exercises you can contact Lars Kindler via kindler@math.fu-berlin.de or come to Arnimallee 3 112A.

Exercise 4. Let K be a number field with ring of integers $\mathcal{O}_K$, and $x_1, \ldots, x_n$ a $\mathbb{Q}$-basis of K with $x_1, \ldots, x_n \in \mathcal{O}_K$. Assume that $K/\mathbb{Q}$ is Galois. Prove that

$$\operatorname{discr}_{K/\mathbb{Q}}(x_1, \ldots, x_n) \equiv 0 \text{ or } 1 \mod 4.$$

(*Hint*: Use that the discriminant of $x_1, \ldots, x_n$ is equal to $\det\left((\sigma_i(x_j))\right)^2$, if $\sigma_1, \ldots, \sigma_n$ are the distinct $\mathbb{Q}$-automorphisms of K, and write this determinant as $A^2 + 4B$, where $A, B \in \mathcal{O}_K$ are Galois invariant, hence $\in \mathbb{Z}$.)