May 21st, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 6[1]

Exercise 1. Let K be a number field, i.e. a finite field extension of $\mathbb{Q}$, and O_K be its ring of integers, i.e. the integral closure of $\mathbb{Z}$ in K. Show that O_K is a Dedekind domain with infinitely many prime ideals.

Exercise 2. Let A be a Dedekind domain with fraction field K. Let $K \subseteq L$ be a finite separable extension, B be the integral closure of A in L.

(1) Let $S := A \setminus \{0\}$. Show that $S^{-1}B = L$.
(2) Show that there is an element $\alpha \in B$ such that $L = K[\alpha]$. (Hint: you can use the primitive element theorem.)
(3) Let α be as in (2), $f(X) \in K[X]$ be the minimal polynomial of α in K. Show that $f(X) \in A[X]$.
(4) Let $\alpha, f(X)$ be as in (3). Suppose $B = A[\alpha]$, then show that $B \cong A[X]/(f(X))$.
(5) Notations and assumptions being as in (4), let $\mathfrak{p}$ be a maximal ideal in A and denote by $\bar{f}(X) \in (A/\mathfrak{p})[X]$ the reduction modulo $\mathfrak{p}$ of $f(X)$, and let

$$\bar{f}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_g(X)^{e_g} \text{ in } (A/\mathfrak{p})[X], \text{ with } e_i \geq 1,$$

be the factorization of $\bar{f}(X)$ into distinct irreducible monic polynomials $\bar{f}_i(X) \in (A/\mathfrak{p})[X]$. Show that the distinct prime ideals in B lying over $\mathfrak{p}$ are exactly given by

$$\mathfrak{q}_i := \mathfrak{p}B + f_i(x)B, \quad i = 1, \dots g,$$

where $f_i(X) \in A[X]$ is some lift of $\bar{f}_i(X)$. Further, the residue class degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is given by the degree of $\bar{f}_i(X)$ and the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ is given by e_i, i.e.

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \quad \text{and} \quad [B/\mathfrak{q}_i : A/\mathfrak{p}] = \deg(\bar{f}_i(X)).$$

Exercise 3. Let $K := \mathbb{Q}[X]/(X^3 - 2)$, $O_K = \mathbb{Z}[\sqrt[3]{2}]$ its ring of integers (You can accept this as a fact!), $(3) \subseteq \mathbb{Z}$ be the ideal generated by $3 \in \mathbb{Z}$.

(1) Is K a Galois extension of $\mathbb{Q}$?

[1] If you want your solutions to be corrected, please hand them in just before the lecture on May 28th. 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.

(2) How many prime ideals of O_K are lying over (3)? (Hint: use Ex.6.2 (5).)
(3) What are the ramification indices and the residue class degrees of primes of O_K lying over (3)? (Hint: use Ex.6.2 (5).)

Exercise 4. Let $m \neq 1 \in \mathbb{Z}$ be a square free integer and A be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{m}]$. Let p be a prime number. Denote by g the number of prime ideals in A over p, by $e_1, \ldots, e_g$ their ramification indices and by $f_1, \ldots, f_g$ their residue class degrees.

(1) Show that the triple (g, e_i, f_i) is one of the following 3.
  (a) $g = 1$, $e_1 = 1$, $f_1 = 2$;
  (b) $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$;
  (c) $g = 1$, $e_1 = 2$, $f_1 = 1$.
(2) Show that if p is an odd prime not dividing m then
  (a) pA is a product of two distinct prime ideals iff m is a square mod p, i.e. there exists $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a^2 = m \in \mathbb{Z}/p\mathbb{Z}$, and
  (b) pA is a prime ideal in A iff m is a not square mod p.
(3) Show that if $m \equiv 1 \bmod 4$ and $p|m$ or if $m \equiv 2, 3 \bmod 4$ and $p|2m$, then p is ramified in A.
(4) Show that if $m \equiv 1 \bmod 4$ and $p = 2$ then
  (a) pA is a product of two distinct prime ideals iff $m \equiv 1 \bmod 8$;
  (b) pA is a prime ideal in A iff $m \equiv 5 \bmod 8$.