ÉNS Lyon
2017-2018

Number Theory
M1

Exercise sheet 2
Dedekind rings

Exercise 1. [Ring of integers of a biquadratic extension]

Let $m, n > 1$ be two distinct squarefree integers congruent to 1 modulo 4 and $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

(a) Prove that $\alpha \in K$ is an algebraic integer if and only if its trace and norm relatively to $\mathbb{Q}(\sqrt{m})$ belong to $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

(b) By considering the relative traces, prove that all $\alpha \in \mathcal{O}_K$ is of the shape

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn}}{4}, \qquad a, b, c, d \in \mathbb{Z},\ a \equiv b \equiv c \equiv d \mod 2.$$

(c) For such an α, prove that up to an integer multiple of $(1+\sqrt{m})(1+\sqrt{n})/4$, it can be written as

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n}}{4}$$

with a, b, c even numbers in $\mathbb{Z}$.

(d) After adding an integer multiple of $(1+\sqrt{n})/2$, deduce that an integral basis of $\mathcal{O}_K$ is given by

$$\left(1, \left(\frac{1+\sqrt{m}}{2}\right), \left(\frac{1+\sqrt{n}}{2}\right), \left(\frac{1+\sqrt{m}}{2}\right) \cdot \left(\frac{1+\sqrt{n}}{2}\right)\right).$$

Exercise 2. [Non-monogenous ring of integers]

Let $K = \mathbb{Q}(\alpha)$ with α a fixed root of $P(X) = X^3 - X^2 - 2X - 8$.

(a) Prove that P is irreducible in $\mathbb{Q}[X]$ by showing that α cannot be an integer.

(b) For $\beta = (\alpha^2 + \alpha)/2$, prove that $\beta^3 - 3\beta^2 - 10\beta - 8 = 0$ and deduce that $\beta \in \mathcal{O}_K$.

(c) Prove that $\operatorname{disc}(1, \alpha, \alpha^2) = -4 \cdot 503$ hence $\operatorname{disc}(1, \alpha, \beta) = -503$. Deduce that $(1, \alpha, \beta)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

(d) Prove that for all $x \in \mathcal{O}_K$, $\operatorname{disc}(1, x, x^2)$ is even. Deduce $\mathcal{O}_K \neq \mathbb{Z}[x]$.

Exercise 3. [Ring of integers of cyclotomic fields]

Let p be a prime number, $m \in \mathbb{N}^*$ and $\zeta_{p^m} = e^{2i\pi/p^m}$. The aim of this exercise is to compute the discriminant of $\mathbb{Q}(\zeta_{p^m})$ and to prove that its ring of integers is $\mathbb{Z}[\zeta_{p^m}]$, as was done for the prime case in the lectures.

(a) Let $K = \mathbb{Q}(a)$ where a is an algebraic number whose minimal polynomial $P \in \mathbb{Z}[X]$ of degree n satisfies Eisenstein criterion for some prime p. Consider an element $x \in \mathcal{O}_K \cap \frac{1}{p}\mathbb{Z}[a]$. Write

$$x = \frac{m_0 + m_1 a + \cdots + m_{n-1}a^{n-1}}{p}$$

Prove that p divides a^n but not a^{n-1} (in $\mathcal{O}_K$), and use it by induction to prove that p divides $m_0, \cdots, m_{n-1}$. We have thus established that $\frac{1}{p}\mathbb{Z}[a] \cap \mathcal{O}_K = \mathbb{Z}[a]$.

(b) Under the same hypotheses, prove that the p-adic valuations of $\mathrm{disc}(K)$ and $\mathrm{disc}(1, a, \cdots, a^{n-1})$ are the same.

(c) Consider the p^m-th cyclotomic polynomial Φ_{p^m}. Prove that the polynomial $\Phi_{p^m}(X+1)$ satisfies Eisenstein criterion, and compute the discriminant of

$$(1, \zeta_{p^m}, \cdots, \zeta_{p^m}^{p^m(p-1)-1}).$$

(d) Use the previous questions to conclude that $\mathrm{disc}(K) = \pm p^{p^{m-1}(pm-m-1)}$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^m}]$.

Exercise 4. [Principal ideal domains and Dedekind domains]

Let A be an integral domain.

(a) Assume that A is a principal ideal domain. Recall why A is then noetherian and a unique factorisation domain. What can we say about the generators of prime (resp. maximal) ideals ?

(b) Prove that all unique factorisation domains are integrally closed. Deduce with question (a) that all principal ideal domains are Dedekind domains.

(c) Give an example of a (noetherian) unique factorisation domain which is not a Dedekind domain.