Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie

SoSe 2019

Exercise Sheet 4

If you want your solutions to be corrected, you should hand them in by Monday, May 13.
Please write your name and immatriculation number on top of every exercise

IMPORTANT: Try to do Exercise 4.4, even if you do not wish to hand your solution in.

Exercise 4.1 (6 points) Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. Let $m_\alpha(X)$ be the minimal polynomial of α and let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \overline{\mathbb{Q}}$ be the embeddings of $K/\mathbb{Q}$. Prove that

$$\operatorname{disc}(\alpha) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m'_\alpha(\alpha)).$$

Hint: Vandermonde.

Exercise 4.2 (2+2+2+4 points) Let $a, b \in \mathbb{Z}$.Assume that the polynomial $f(X) = X^3 + aX + b$ is irreducible over $\mathbb{Q}$, let α be a root of $f(X)$ and $K = \mathbb{Q}(\alpha)$.

a) Show that $f'(\alpha)\alpha = -(2a \cdot \alpha + 3b)$.

b) Observe that $2a \cdot \alpha + 3b$ is a root of $g(X) = f\left(\frac{X-3b}{2a}\right)$. Compute $N_{K/\mathbb{Q}}(2a\alpha + 3b)$.

c) Show that $\operatorname{disc}(\alpha) = -(4a^3 + 27b^2)$.

d) Assume $f(X) = X^3 - X - 1$. Compute an integral basis of $\mathcal{O}_K$.

Exercise 4.3 (1+3+5+5+1 points) Let m, n be two distinct squarefree integers, $m, n \neq 1$. Consider the field $K := \mathbb{Q}(\sqrt{m}, \sqrt{n})$ and denote by $\mathcal{O}_K$ its ring of integers.

a) Let $k = \frac{mn}{\gcd(m,n)^2} \in \mathbb{Z}$. Check that $\mathbb{Q}(\sqrt{k}) \subset K$.

b) Let $F \subset K$ be a subfield with $[K : F] = 2$. Show that $\alpha \in \mathcal{O}_K$ if and only if $N_{K/F}(\alpha) \in \mathcal{O}_F$ and $Tr_{K/F}(\alpha) \in \mathcal{O}_F$.

c) Show that every $\alpha \in \mathcal{O}_K$ can be written in the form

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2},$$

where $a, b, c, d \in \mathbb{Z}$. (*Hint*: consider the trace of such an expression with rational coefficents, with respect to the three obvious quadratic subfields).

d) Assume $m \equiv 3 \pmod 4$ and $n \equiv k \equiv 2 \pmod 4$. Show that in the previous expression a, b are even and $c \equiv d \pmod 2$. (*Hint*: for the congruence between c and d, consider the norm with respect to $\mathbb{Q}(\sqrt{m})$).

e) With the same assumptions of the previous point, conclude that an integral basis of $\mathcal{O}_K$ is given by

$$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}.$$

Turn the sheet.

Exercise 4.4 (1+1+1+2+3+2+2+2) Let A be a ring and $S \subseteq A$ a multiplicatively closed subset. Recall that the fraction ring $S^{-1}A$ is defined as the set of symbols

$$S^{-1}A = \left\{ \frac{a}{s} \,|\, a \in A, s \in S \right\},$$

where the symbols are subject to the relation

$$\frac{a}{s} = \frac{b}{t} \text{ in } S^{-1}A \overset{\text{def}}{\iff} \exists\, u \in S \text{ s. t. } uat = ubs \text{ in } A.$$

Then $S^{-1}A$ is a ring with the usual definitions of sums and products for fractions. Prove the following properties:

a) The map $A \to S^{-1}A, a \mapsto \frac{a}{1}$ defines a canonical ring homomorphism.

b) Every element $\frac{s}{t} \in S^{-1}A$ with, $s, t \in S$ is invertible in $S^{-1}A$.

c) If $I \subseteq A$ is an ideal, then define $S^{-1}I = \{\frac{a}{s} \,|\, a \in I, s \in S\}$. Prove that $S^{-1}I$ is an ideal in $S^{-1}A$, and show that $S^{-1}I = S^{-1}A$ if and only if $I \cap S \neq \emptyset$.

d) Let $J \subseteq S^{-1}A$ be a proper ideal. Define $I = \{a \in A \,|\, \frac{a}{1} \in J\}$, show that I is an ideal in A and that $J = S^{-1}I$. Hence any proper ideal in $S^{-1}A$ is of the form $S^{-1}I$, for an ideal in A.

e) Suppose that $P \subseteq A$ is a prime ideal such that $P \cap S = \emptyset$. Prove that $S^{-1}P$ is prime in $S^{-1}A$. Show that if $P, Q \subseteq A$ are both primes such that $P \cap S = Q \cap S = \emptyset$, then $P \subseteq Q$ if and only if $S^{-1}P \subseteq S^{-1}Q$. Conclude that the map

$$\{\text{ prime ideals } P \subseteq A \,|\, P \cap S = \emptyset\} \longrightarrow \left\{ \text{ prime ideals in } S^{-1}A \right\}, \qquad P \mapsto S^{-1}P$$

is a bijection.

f) Let $I \subseteq A$ be an ideal such that $I \cap S = \emptyset$ and in A/I consider the set $\overline{S} = \{s + I \in A/I \,|\, s \in S\}$. Show that $\overline{S}$ is a multiplicatively closed subset in A/I, and that the map

$$(S^{-1}A)/(S^{-1}I) \longrightarrow \overline{S}^{-1}(A/I), \qquad \frac{a}{s} + S^{-1}I \mapsto \frac{a+I}{s+I}$$

is well-defined and an isomorphism of rings.

Now, let $\mathfrak{p} \subseteq A$ be a prime and let $S = A \setminus \mathfrak{p}$. It is customary to denote $A_{\mathfrak{p}} := S^{-1}A$, and $I_{\mathfrak{p}} := S^{-1}I$ for any ideal $I \subseteq A$.

h) Show that the primes ideal of $A_{\mathfrak{p}}$ are in bijection with the prime ideals of A contained in $\mathfrak{p}$. Conclude that $A_{\mathfrak{p}}$ is local, with unique maximal ideal $\mathfrak{p}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$.

To conclude, we observe that when A is a domain, the $S^{-1}A$ are just subrings of the field of fractions:

i) Suppose that A is a domain and let $S \subseteq A$ be a multiplicatively closed subset. Prove that $\frac{a}{s} = \frac{b}{t}$ in $S^{-1}A$ if and only if $ta = bs$ in A. Conclude that we can look at $S^{-1}A$ as an intermediate extension

$$A \subseteq S^{-1}A \subseteq \operatorname{Frac} A.$$