Algebraic Number Theory

WS 2022/23

Christoph Baxa

1) Prove that $(\mathbb{Q}^+, \cdot)$ has a basis (where $\mathbb{Q}^+$ denotes the set of positive rational numbers).

2) a) Prove that $(\mathbb{Q}, +)$ is not a finitely generated group.
b) Prove that $(\mathbb{Q}, +)$ does not have a basis.

3) Let $G_1, \dots, G_k$ be groups and $N_i \trianglelefteq G_i$ normal subgroups for $1 \le i \le k$. Prove

$$N_1 \times \cdots \times N_k \trianglelefteq G_1 \times \cdots \times G_k$$

and

$$(G_1 \times \cdots \times G_k)/(N_1 \times \cdots \times N_k) \cong (G_1/N_1) \times \cdots \times (G_k/N_k).$$

Hint. Consider the map

$$\varphi : G_1 \times \cdots \times G_k \to (G_1/N_1) \times \cdots \times (G_k/N_k),\ \varphi(a_1, \dots, a_k) = (a_1N_1, \dots, a_kN_k).$$

4) Let R be an integral domain. Prove that the set

$$\{A \mid A \text{ is an } n \times n \text{ matrix with entries in } R \text{ and } \det A \in R^*\}$$

is a group with matrix multiplication.

5) Let F be free abelian group of rank n. Prove the following:

a) It is not true that every linearly independent subset of F with n elements is a basis of F.
b) It is not true that every linearly independent subset of F can be extended to a basis of F
c) It is not true that every subset of F which generates F contains a basis of F.

6) a) Let G be a finitely generated abelian group in which 0 is the only element of finite order. Prove that G is a free abelian group.

b) Prove that part a) is no longer true if one only assumes G to be an abelian group in which 0 is the only element of finite order.

7) Let K be a field with characteristic $\operatorname{char} K = p > 0$ and $f \in K[X]$ an irreducible polynomial. Prove that the following are equivalent:

(i) f is not separable (i.e., $f' = 0$),
(ii) There is a $g \in K[X]$ such that $f(X) = g(X^p)$.

8) Let K be field with $\operatorname{char} K = p > 0$ and $\sigma : K \to K$, $\sigma(x) = x^p$. Prove that

a) σ is a monomorphism,

b) If K is finite σ is an isomorphism.

Definition. The map σ described in Exercise 8 is called Frobenius endomorphism.

9) Let K be a finite field. Prove that

a) Every irreducible $f \in K[X]$ is separable,

b) If L/K is a finite field extension then L/K is a separable extension.

10) Let K be a field with $\operatorname{char} K = p > 0$ and L/K a finite field extension with $p \nmid [L : K]$. Prove that L/K is a separable extension.

11) Let p be prime and $f(X) = X^p - T \in \mathbb{F}_p(T)[X]$ (i.e., f is a polynomial with coefficients in the quotient field of the polynomial ring $\mathbb{F}_p[T]$). Prove that f is irreducible but not separable. *Hint.* Use Eisenstein's criterion.

12) Find a primitive element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ for the following algebraic number fields:

a) $K = \mathbb{Q}(\sqrt{2}, i)$ b) $K = \mathbb{Q}(\sqrt{2}, i\sqrt{2})$ c) $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$

13) Let p be a prime and let L/K be a finite field extension such that $[L : K] = p$. Prove that $L = K(\alpha)$ for all $\alpha \in L \setminus K$.

14) Let L/K be a field extension and let $\alpha \in L$ be algebraic over K. Prove the following:

a) If $\deg m_{K,\alpha}$ is odd then $K(\alpha^2) = K(\alpha)$. (Is this also true if $\deg m_{K,\alpha}$ is even?)

b) Let m, n be positive integers with mn squarefree. Then $\mathbb{Q}\big(\sqrt[3]{mn^2}\big) = \mathbb{Q}\big(\sqrt[3]{m^2n}\big)$.

15) Find all homomorphisms $\sigma : \mathbb{Q}(\sqrt[4]{2}) \hookrightarrow \mathbb{C}$ such that a) $\sigma|_{\mathbb{Q}(\sqrt{2})} = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$ and b) $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

16) Find all homomorphisms $\sigma : \mathbb{Q}(\sqrt{2}, i) \hookrightarrow \mathbb{C}$ such that

a) $\sigma|_{\mathbb{Q}(i)} = \mathrm{id}_{\mathbb{Q}(i)}$, b) $\sigma|_{\mathbb{Q}(\sqrt{2})} = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$, c) $\sigma|_{\mathbb{Q}(\sqrt{2}i)} = \mathrm{id}_{\mathbb{Q}(\sqrt{2}i)}$ and d) $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

17) Prove the results of Lemma 22 (i) – (vi) once more, this time using the results of Theorem 23 (ii) and (iii) as the definition of the norm $\mathrm{N}_{L/K}$ and the trace $\mathrm{Tr}_{L/K}$, i.e., let

$$\mathrm{N}_{L/K}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha),$$

where L/K is a finite, separable field extension with $[L : K] = n$ and $\sigma_i : L \hookrightarrow \overline{K}$ are the different homomorphisms with $\sigma|_K = \mathrm{id}_K$.

18) Let L/K be a field extension with $[L:K]=2$. Prove that L/K is a normal extension.

19) a) Prove that the field extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are both normal, but the field extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not.

b) Let $\zeta := e^{2\pi i/3} = \frac{1}{2}(-1+\sqrt{3}i)$. Show that the field extensions $\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}(\sqrt[3]{2})$ are both normal, but the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

20) a) Calculate $\mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha)$ for $\alpha \in \mathbb{Q}(\sqrt{3})$.
b) Calculate $\mathrm{N}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})}(\alpha)$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})}(\alpha)$ for $\alpha \in \mathbb{Q}(\sqrt[4]{3})$.
c) Calculate $\mathrm{N}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}}(\alpha)$ for $\alpha \in \mathbb{Q}(\sqrt[4]{3})$ both directly and with the help of Theorem 28.

21) Calculate $\Delta_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}}\big(1,\sqrt{2},\sqrt{3},\sqrt{2}+\sqrt{3}\big)$ using the definition of the discriminant. Is there a faster way of doing this?

22) Let a and b be positive integers with $a>1$ and ab squarefree. Let $m=ab^2$. Calculate $\Delta_{\mathbb{Q}(\sqrt[3]{m})/\mathbb{Q}}\big(1,\sqrt[3]{m},\sqrt[3]{m^2}\big)$ both using the definition of the discriminant and with the help of Theorem 34.

23) Let p be a prime. The p^{th} cyclotomic polynomial $\Phi_p(X)$ is

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

Use Eisenstein's criterion to show that $\Phi_p(X)$ is irreducible (in $\mathbb{Q}[X]$). (*Hint.* Use $\Phi_p(X) = (X^p-1)/(X-1)$, consider $\Phi_p(X+1)$ and employ the binomial theorem.) Find all roots of $\Phi_p(X)$ and its factorization into linear factors.

24) Let $p>2$ be a prime and $\zeta = e^{2\pi i/p}$. Prove the following:

a) $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$

Hint. Use the factorization of $\Phi_p(X)$ into linear factors from the previous exercise.

b) $\Delta_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1,\zeta,\zeta^2,\ldots,\zeta^{p-2}) = (-1)^{(p-1)/2}p^{p-2}$.

25) Let R be a commutative ring with identity and M an R-module. Prove the following:

a) $(-a)m = -(am) = a(-m)$ for all $a\in R$ and all $m\in M$,
b) $k(am) = a(km)$ for all $k\in\mathbb{Z}$, all $a\in R$ and all $m\in M$.

26) Let R and S be commutative rings with identity, $\varphi: R\to S$ a ring homomorphism with the property $\varphi(1_R)=1_S$ and M an S-module. Prove that M becomes an R-module by setting $R\times M\to M$, $(a,m)\mapsto \varphi(a)\cdot m$.

27) Let R be a commutative ring with identity, M an R-module and I an ideal of R with the property that $am = 0$ for all $a \in I$ and all $m \in M$. Prove the following:

a) $bm = cm$ if $b - c \in I$,

b) M becomes an R/I-Modul by setting $(a + I) \cdot m := a \cdot m$.

28) Let R be an integral domain, K its quotient field, L/K a finite field extension and $S = \bar{R}^L$. Prove that for every $\beta \in L$ there is a $a \in R \setminus \{0\}$ such that $a\beta \in S$.

29) Let R be an integral domain, K its quotient field, L/K a finite field extension and $S = \bar{R}^L$. Prove the following:

a) The quotient field of S is (isomorphic to) L,

b) S is an integrally closed integral domain.

30) Let R be an integrally closed integral domain, K its quotient field, L/K a field extension and $S = \bar{R}^L$. Prove $S \cap K = R$.

31) Let K be an algebraic number field with $[K : \mathbb{Q}] = n$ and $\{\alpha_1, \dots, \alpha_n\}$ a basis of K (as a $\mathbb{Q}$-vector space) consisting only of elements of O_K. Prove that $\{\alpha_1, \dots, \alpha_n\}$ is an integral basis for K if $\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = d_K$.

32) Prove that the groups $(\mathbb{Z}[\sqrt{2}]^*, \cdot)$ and $(\mathbb{Z}_2 \times \mathbb{Z}, +)$ are isomorphic.

33) Let $K = \mathbb{Q}(\sqrt{3})$. Prove that $O_K^* = \mathbb{Z}[\sqrt{3}]^* = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}$.

34) Show that both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are norm-euclidean.

35) a) Show that $O_{\mathbb{Q}(i\sqrt{6})} = \mathbb{Z}[i\sqrt{6}]$ is not a unique factorization domain.
b) Show that $O_{\mathbb{Q}(i\sqrt{10})} = \mathbb{Z}[i\sqrt{10}]$ is not a unique factorization domain.
Hint. Use the equations

$$6 = 2 \cdot 3 = i\sqrt{6} \cdot (-i\sqrt{6}) \text{ and } 14 = 2 \cdot 7 = (2 + i\sqrt{10}) \cdot (2 - i\sqrt{10}).$$

36) Does not the equation $10 = 2 \cdot 5 = (3 + i) \cdot (3 - i)$ contradict the fact that $O_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ is a unique factorization domain?

37) Let $p \equiv 3 \pmod 4$ be a prime and $a, b \in \mathbb{Z}$. Show that $p \mid (a^2 + b^2)$ implies $p \mid a$ and $p \mid b$.

38) Let $n \geq 2$ be an integer with prime factorization $n = 2^\alpha p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_\ell^{\gamma_\ell}$ (where $k, \ell, \alpha \geq 0$, $\beta_1, \dots, \beta_k, \gamma_1, \dots, \gamma_\ell \geq 1$, $p_i \equiv 1 \pmod 4$ for $1 \leq i \leq k$ and $q_i \equiv 3 \pmod 4$ for $1 \leq i \leq \ell$). Prove that the following are equivalent:

(i) $\exists\, x, y \in \mathbb{Z} : n = x^2 + y^2$

(ii) $\gamma_1 \equiv \cdots \equiv \gamma_\ell \equiv 0 \pmod 2$

Hint. Use the identity $(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2$.

39) a) Is the ring $R = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continous}\}$ noetherian?

Hint. Consider $I_n = \left\{f \in R \;\middle|\; f(x) = 0 \text{ for all } x \in [0, \frac{1}{n}]\right\}$ with $n \in \mathbb{N}$.

b) Find a finitely generated module with a submodule that is not finitely generated.

40) Present the following proof of the **Hilbert basis theorem** (i.e., if R is a noetherian ring then $R[X]$ is a noetherian ring).

Proof. Let I be an ideal of $R[X]$ that is not finitely generated. Then $I \setminus (0) \neq \varnothing$. Choose a $p_1 \in I \setminus (0)$ with minimal degree. As I is not finitely generated, we have $I \setminus (p_1) = I \setminus (p_1 R[X]) \neq \varnothing$. Choose a $p_2 \in I \setminus (p_1)$ with minimal degree. Continue this way: if $p_1, \dots, p_k \in I$ have already been chosen, then

$$I \setminus (p_1, \dots, p_k) = I \setminus (p_1 R[X] + \cdots + p_k R[X]) \neq \varnothing$$

as I is not finitely generated. Choose a $p_{k+1} \in I \setminus (p_1, \dots, p_k)$ with minimal degree. This yields a sequence $(p_k)_{k \geq 1}$ in I. Let $n_i := \deg p_i$ and let a_i be the leading coefficient of p_i. By construction we have $n_1 \leq n_2 \leq n_3 \leq \cdots$.

We claim that $(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3) \subsetneqq \cdots$ is an ascending chain of ideals of R that does not terminate.

Suppose there is an $r \in \mathbb{N}$ such that $(a_1, \dots, a_r) = (a_1, \dots, a_{r+1})$. This just says

$$Ra_1 + \cdots + Ra_r = Ra_1 + \cdots + Ra_{r+1}$$

and there would be $b_1, \dots, b_r \in R$ such that $a_{r+1} = b_1 a_1 + \cdots + b_r a_r$. Consider the polynomial

$$q(X) := p_{r+1}(X) - \sum_{i=1}^{r} b_i p_i(X) X^{n_{r+1} - n_i}.$$

Clearly $q \in I \setminus (p_1, \dots, p_r)$ (as $p_{r+1} \notin (p_1, \dots, p_r)$) and $\deg q \leq n_{r+1}$. Because of $a_{r+1} - (b_1 a_1 + \cdots + b_r a_r) = 0$ the coefficient of $X^{n_{r+1}}$ in q is zero and thus $\deg q < n_{r+1}$. This, however, contradicts the minimality of $\deg p_{r+1}$.

41) Prove Lemma 89 (i) – (v) and Lemma 89 (vii) – (ix).

42) Let R be a commutative ring with identity and I_1, I_2 and I_3 ideals of R. Prove

$$I_1 \cdot (I_2 \cdot I_3) = (I_1 \cdot I_2) \cdot I_3 = \left\{ \sum_{i=1}^{n} a_i b_i c_i \;\middle|\; a_i \in I_1,\ b_i \in I_2 \text{ and } c_i \in I_3 \text{ for } 1 \leq i \leq n \right\}.$$

43) Let R be a commutative ring with identity and P an ideal of R. Prove that the following are equivalent:

(i) $P \subsetneqq R$ and $a \cdot b \in P$ implies $a \in P$ or $b \in P$ (for $a, b \in R$),

(ii) $P \subsetneqq R$ and $I \cdot J \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ (for ideals I, J of R).

44) Let D be a Dedekind domain, K its quotient field, I and J two ideals of D and $\alpha, \beta \in D \setminus \{0\}$. Prove that

a) $\alpha^{-1}I + \beta^{-1}J = (\alpha\beta)^{-1}(\beta I + \alpha J)$ and b) $\alpha^{-1}I \cdot \beta^{-1}J = (\alpha\beta)^{-1}I \cdot J$

are fractional ideals of K.

45) Prove Lemma 92 (iii).

46) Let K be an algebraic number field and $P \neq (0)$ a prime ideal of O_K. Prove the following generalization of Fermat's little theorem:

a) If $\alpha \in O_K \setminus P$ then $\alpha^{N(P)-1} \equiv 1 \pmod{P}$,
b) If $\alpha \in O_K$ then $\alpha^{N(P)} \equiv \alpha \pmod{P}$.

47) Let K be an algebraic number field and $I \neq (0)$ an ideal of O_K. Prove that:

a) If $\alpha \in I$ satisfies $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$ then $I = (\alpha) = \alpha O_K$,
b) If p, q are two different primes such that $pq \mid N(I)$ then I is not a prime ideal.

48) Let K be an algebraic number field, $P \neq (0)$ a prime ideal of O_K and p the prime lying below P. Prove that $P \cap \mathbb{Z} = p\mathbb{Z}$.

49) Let $K = \mathbb{Q}(i\sqrt{5})$. Find pairwise different prime ideals P_1, P_2 and P_3 of the ring $O_K = \mathbb{Z}[i\sqrt{5}]$ such that

$$(2) = P_1^2,\ (3) = P_2P_3,\ (1 + i\sqrt{5}) = P_1P_2 \text{ and } (1 - i\sqrt{5}) = P_1P_3$$

and prove that these assertions hold.

50) Let $K = \mathbb{Q}(i\sqrt{6})$. Find different prime ideals P_1 and P_2 of the ring $O_K = \mathbb{Z}[i\sqrt{6}]$ such that

$$(2) = P_1^2,\ (3) = P_2^2 \text{ and } (i\sqrt{6}) = (-i\sqrt{6}) = P_1P_2$$

and prove that these assertions hold.