Algebraische Zahlentheorie

WS 2011/12

Christoph Baxa

1) Es sei G eine abelsche Gruppe und $m \in \mathbb{Z}$. Zeigen Sie:

a) $mG = \{mg \mid g \in G\}$ ist eine Untergruppe von G.

b) Ist $G \cong G_1 \oplus \cdots \oplus G_n$, so gelten

$$mG \cong mG_1 \oplus \cdots \oplus mG_n \text{ und } G/mG \cong G_1/mG_1 \oplus \cdots \oplus G_n/mG_n.$$

2) Es sei F eine freie abelsche Gruppe vom Rang n. Zeigen Sie:

a) Es ist nicht richtig, dass jede linear unabhängige Teilmenge von F mit n Elementen eine Basis von F ist.

b) Es ist nicht richtig, dass jede linear unabhängige Teilmenge von F zu einer Basis von F erweitert werden kann.

c) Es ist nicht richtig, dass jede Teilmenge von F, die F erzeugt, eine Basis von F enthält.

3) Eine abelsche Gruppe G heißt freie abelsche Gruppe, wenn sie eine Basis $B \subseteq G$ besitzt. (Das verallgemeinert den entsprechenden Begriff aus der Vorlesung, da B unendlich sein kann.) Es sei $G := \{x \in \mathbb{Q} \mid x > 0\}$. Zeigen Sie, dass $(G, \cdot)$ eine freie abelsche Gruppe ist und finden Sie eine Basis.

4) a) Beweisen Sie, dass $(\mathbb{Q}, +)$ nicht endlich erzeugt ist.

b) Beweisen Sie, dass $(\mathbb{Q}, +)$ keine freie abelsche Gruppe ist.

5) Es sei R ein Integritätsbereich. Beweisen Sie, dass die Menge

$$\{A \mid A \text{ ist } n \times n\text{-Matrix mit Eintragungen aus } R \text{ und } \det A \in R^*\}$$

mit der Matrizenmultiplikation eine Gruppe bildet.

6) a) Es sei G eine endlich erzeugte abelsche Gruppe, in der 0 das einzige Element endlicher Ordnung ist. Beweisen Sie, dass G eine freie abelsche Gruppe ist.

b) Zeigen Sie, dass diese Aussage nicht richtig bleibt, wenn man nur voraussetzt, dass G eine abelsche Gruppe ist, in der 0 das einzige Element endlicher Ordnung ist.

7) a) Die drei Polynome $f, g, h \in \mathbb{Z}[X]$ sollen die Relation $f = g \cdot h$ erfüllen. Beweisen Sie: Teilt die Primzahl p alle Koeffizienten von f, so teilt sie entweder alle Koeffizienten von g oder sie teilt alle Koeffizienten von h.
b) Die Polynome $f \in \mathbb{Z}[X]$ und $g, h \in \mathbb{Q}[X]$ sollen die Relation $f = g \cdot h$ erfüllen. Beweisen Sie die Existenz eines $\lambda \in \mathbb{Q}$, derart dass $\lambda g, \lambda^{-1} h \in \mathbb{Z}[X]$.

8) (Irreduzibilitätskriterium von Eisenstein) Es sei

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

und es existiere eine Primzahl p, die die folgenden drei Eigenschaften besitzt: $p \nmid a_n$, $p \mid a_i$ für $0 \leq i < n$ und $p^2 \nmid a_0$. Beweisen Sie, dass f in $\mathbb{Q}[X]$ irreduzibel ist.

9) Beweisen Sie die Irreduzibilität der folgenden Polynome in $\mathbb{Q}[X]$ mit Hilfe des Eisensteinkriteriums:

a) $X^3 + 6X + 2$
b) $3X^4 + 15X^2 + 10$
c) $2X^5 - 6X^3 + 9X^2 - 15$
d) $X^{11} - 7X^6 + 21X^5 + 49X - 56$

10) a) Welches der beiden Polynome $X^2 + 4$ und $X^2 - 4$ ist reduzibel bzw. irreduzibel in $\mathbb{Q}[X]$? Kann man das Eisensteinkriterium anwenden?
b) Es sei $n \in \mathbb{N}$. Für welche $d \in \mathbb{Z}$ kann man mit Hilfe des Eisensteinkriteriums beweisen, dass das Polynom $X^n - d$ in $\mathbb{Q}[X]$ irreduzibel ist?

11) a) Es sei $p(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ und $c \in \mathbb{Z}$. Beweisen Sie: $p(X)$ ist genau dann irreduzibel wenn $p(X + c)$ irreduzibel ist (jeweils in $\mathbb{Q}[X]$).
b) Zeigen Sie mit Hilfe des Eisensteinkriteriums, dass $p(X) = X^2 + X + 2$ irreduzibel ist (in $\mathbb{Q}[X]$). (Hinweis: Betrachten Sie $p(X + 3)$.)

12) Es sei p eine Primzahl. Das p-te Kreisteilungspolynom $\Phi_p(X)$ hat die Gestalt

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

Zeigen Sie mit Hilfe des Eisensteinkriteriums, dass $\Phi_p(X)$ in $\mathbb{Q}[X]$ irreduzibel ist. (Hinweis: Verwenden Sie $\Phi_p(X) = (X^p - 1)/(X - 1)$, betrachten Sie $\Phi_p(X + 1)$ und wenden Sie den binomischen Lehrsatz an.) Welche Nullstellen hat $\Phi_p(X)$? Wie sieht seine Faktorisierung in Linearfaktoren aus?

13) Es sei p eine Primzahl.

a) Beweisen Sie, dass die folgende Abbildung ein Ringhomomorphismus ist.

$$\mathbb{Z}[X] \to \mathbb{Z}_p[X], \quad f(X) = \sum_{i=0}^{n} a_i X^i \mapsto \bar{f}(X) = \sum_{i=0}^{n} \bar{a}_i X^i$$

Dabei bezeichnet $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ die Restklassen modulo p und $\bar{a}_i = a_i \bmod p$.

b) Beweisen Sie: Gilt $\operatorname{grad} \bar{f} = \operatorname{grad} f$ und ist $\bar{f}$ irreduzibel in $\mathbb{Z}_p[X]$, so ist f irreduzibel in $\mathbb{Q}[X]$.

c) Verwenden Sie Teil b) um zu zeigen, dass $f(X) = X^2 + X + 2$ in $\mathbb{Q}[X]$ irreduzibel ist.

14) Es sei R ein Ring.

a) Für jedes $j \in \mathcal{J} (\neq \varnothing)$ sei I_j ein Ideal von R. Zeigen Sie, dass $\bigcap\limits_{j \in \mathcal{J}} I_j$ ein Ideal von R ist.

b) Für jedes $j \in \mathcal{J} (\neq \varnothing)$ sei I_j ein Ideal von R. Zeigen Sie, dass

$$\sum_{j \in \mathcal{J}} I_j = \left\{ \sum_{j \in \mathcal{J}} a_j \;\middle|\; a_j \in I_j \text{ und } a_j = 0 \text{ für alle bis auf endlich viele } j \right\}$$

ein Ideal von R ist. Was erhält man im Spezialfall $|\mathcal{J}| = 2$?

c) Es seien I_1, I_2 und I_3 Ideale von R. Zeigen Sie

$$(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3) \quad \text{und} \quad I_1 + I_2 = I_2 + I_1.$$

15) Es sei R ein Ring. Zeigen Sie die folgenden Behauptungen:

a) Wenn I und J Ideale sind, ist

$$I \cdot J = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in I \text{ und } b_i \in J \text{ für } 1 \leq i \leq n \right\}$$

ebenfalls ein Ideal von R.

b) Sind I und J Ideale von R, so gilt $I \cdot J \subseteq I \cap J$.

c) Ist I ein Ideal von R, so gilt $I \cdot R = I$.

16) Es sei R ein Ring und I_1, I_2 und I_3 Ideale von R. Zeigen Sie

a) $I_1 \cdot I_2 = I_2 \cdot I_1$,

b) $I_1 \cdot (I_2 \cdot I_3) = (I_1 \cdot I_2) \cdot I_3$,

c) $I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3$ und $(I_1 + I_2) \cdot I_3 = I_1 \cdot I_3 + I_2 \cdot I_3$.

Hinweis zu Teil b): Zeigen Sie

$$I_1 \cdot (I_2 \cdot I_3) = (I_1 \cdot I_2) \cdot I_3 = \left\{ \sum_{i=0}^{n} a_i b_i c_i \;\middle|\; a_i \in I_1,\, b_i \in I_2 \text{ und } c_i \in I_3 \text{ für } 1 \leq i \leq n \right\}.$$

Definition. Eine Teilmenge S eines Rings R heißt *multiplikativ* (oder *multiplikativ abgeschlossen*) wenn $1 \in S$ und $xy \in S$ $\forall x, y \in S$.

17) Es sei R ein Ring und P ein Ideal von R. Zeigen Sie die Äquivalenz der folgenden drei Aussagen:

(i) P ist ein Primideal,
(ii) $R \setminus P$ ist multiplikativ,
(iii) $P \subsetneqq R$ und für Ideale I, J von R gilt: Wenn $I \cdot J \subseteq P$ dann $I \subseteq P$ oder $J \subseteq P$.

18) Es sei R ein Integritätsbereich und $\pi \in R$. Beweisen Sie:

a) π ist prim $\iff (\pi) \neq (0)$ und (π) ist ein Primideal von R.
b) π ist irreduzibel $\iff (\pi)$ ist maximal in der Menge aller echten Hauptideale von R.
c) Ist R ein faktorieller Ring, so gilt π ist irreduzibel $\iff \pi$ ist prim.

19) Finden Sie ein primitives Element $\alpha \in K$, derart dass $K = \mathbb{Q}(\alpha)$ für

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

20) Es seien $K \subseteq L$ zwei algebraische Zahlkörper, $\alpha \in L$ und $\varphi_\alpha : L \to L$, $\varphi_\alpha(x) = \alpha x$. Beweisen Sie:

a) φ_α ist eine K-lineare Abbildung (wobei man L als K-Vektorraum auffasst).
b) Das charakteristische Polynom $\det(X \operatorname{id}_L - \varphi_\alpha)$ von φ_α zerfällt gemäß

$$\det(X \operatorname{id}_L - \varphi_\alpha) = \prod_{i=1}^{[L:K]} \big(X - \sigma_i(\alpha)\big)$$

in Linearfaktoren, wobei $\sigma_i : L \to \mathbb{C}$ (mit $1 \leq i \leq [L : K]$) alle Einbettungen mit $\sigma_i|_K = \operatorname{id}_K$ durchläuft.
c) $\mathrm{N}_{L/K}(\alpha) = \det(\varphi_\alpha)$
d) $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Spur}(\varphi_\alpha)$

Hinweis: Verwenden Sie die folgende Tatsache: Ist $\{\beta_1, \ldots, \beta_{[L:K(\alpha)]}\}$ eine Basis von L (aufgefasst als $K(\alpha)$-Vektorraum), so ist (nach dem Beweis des Gradsatzes)

$$\big\{\beta_i \alpha^j \,\big|\, 1 \leq i \leq [L : K(\alpha)], 0 \leq j < [K(\alpha) : K]\big\}$$

eine Basis von L (aufgefasst als K-Vektorraum). Die Verwendung dieser Basis erleichtert die Rechnung.

21) a) Berechnen Sie $\mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha)$ und $\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(\alpha)$ für beliebiges $\alpha \in \mathbb{Q}(\sqrt{3})$.
b) Berechnen Sie $\mathrm{N}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})}(\alpha)$ und $\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})}(\alpha)$ für beliebiges $\alpha \in \mathbb{Q}(\sqrt[4]{3})$.
c) Berechnen Sie $\mathrm{N}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}}(\alpha)$ und $\mathrm{Tr}_{\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}}(\alpha)$ für beliebiges $\alpha \in \mathbb{Q}(\sqrt[4]{3})$ sowohl mittels Satz 2.11 als auch direkt.

22) Berechnen Sie $\Delta_{\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}}\big(1, \sqrt{2}, \sqrt{3}, \sqrt{2}+\sqrt{3}\big)$ ausgehend von der Definition der Diskriminante. Gibt es einen schnelleren Weg?

23) Es seien $a, b \in \mathbb{N}$, wobei $a > 1$ und ab quadratfrei sei. Es sei $m = ab^2$. Berechnen Sie $\Delta_{\mathbb{Q}(\sqrt[3]{m})/\mathbb{Q}}\big(1, \sqrt[3]{m}, \sqrt[3]{m^2}\big)$ sowohl ausgehend von der Definition der Diskriminante als auch mittels Korollar 2.18. Warum sind die Voraussetzungen an a und b keine Einschränkungen?

24) Es sei $p > 2$ eine Primzahl und $\zeta = e^{2\pi i/p}$. Beweisen Sie:

a) $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$
Hinweis: Verwenden Sie die Faktorisierung von $\Phi_p(X)$ in Linearfaktoren aus Bsp. 12.

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

25) (Division mit Rest für Polynome mit Koeffizienten in einem Ring) Es sei R ein Ring und $f, g \in R[X] \setminus \{0\}$. Weiters sei der Leitkoeffizient von g eine Einheit von R, d.h. g besitze eine Darstellung

$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 \quad \text{mit } b_m \in R^*.$$

Beweisen Sie die Existenz eindeutig bestimmter Polynome $q, r \in R[X]$ mit den Eigenschaften $f = qg + r$ und $\operatorname{grad} r < \operatorname{grad} g$.

26) Es seien R und S Ringe, $\varphi : R \to S$ ein Ringhomomorphismus mit der Eigenschaft $\varphi(1) = 1$ und M ein S-Modul. Beweisen Sie, dass M durch $R \times M \to M$, $(a, m) \mapsto \varphi(a)m$ zu einem R-Modul wird.

27) Es sei R ein Ring, M und N zwei R-Moduln und $\varphi : M \to N$ ein R-Modulhomomorphismus. Beweisen Sie:

a) Ist M' ein Untermodul von M, so ist $\varphi(M')$ ein Untermodul von N.
b) Ist N' ein Untermodul von N, so ist $\varphi^{-1}(N')$ ein Untermodul von M.
c) $\ker \varphi$ ist ein Untermodul von M.
d) $\operatorname{Im} \varphi$ ist ein Untermodul von N.

28) Es sei R ein Ring, M und N zwei R-Moduln und $\varphi : M \to N$ ein R-Modulhomomorphismus. Beweisen Sie, dass φ genau dann injektiv ist wenn $\ker \varphi = \{0\}$.

29) Es sei R ein Ring und M_1, M_2 zwei R-Moduln. Weiters bezeichne

$$\mathrm{Hom}_R(M_1, M_2) = \{\varphi : M_1 \to M_2 \mid \varphi \text{ ist } R\text{-Modulhomomorphismus}\}.$$

Beweisen Sie: Setzt man

$$(\varphi_1 + \varphi_2)(m) := \varphi_1(m) + \varphi_2(m) \text{ (für } \varphi_1, \varphi_2 \in \mathrm{Hom}_R(M_1, M_2),\ m \in M_1)$$
$$\text{und} \quad (a\varphi)(m) := a\varphi(m) \text{ (für } a \in R,\ \varphi \in \mathrm{Hom}_R(M_1, M_2),\ m \in M_1),$$

so wird $\mathrm{Hom}_R(M_1, M_2)$ ein R-Modul.

30) Es sei R ein Ring und M_1, M_2, M_3 drei R-Moduln. Zeigen Sie: Ist $\varphi \in \mathrm{Hom}_R(M_1, M_2)$ und $\psi \in \mathrm{Hom}_R(M_2, M_3)$, dann ist $\psi \circ \varphi \in \mathrm{Hom}_R(M_1, M_3)$.

31) Es sei R ein Ring, M ein R-Modul und N ein Untermodul von M. Beweisen Sie:

a) M/N ist ein R-Modul.

b) $\varphi : M \to M/N$, $\varphi(m) = m + N$ ist ein R-Modulepimorphismus.

32) Es sei R ein ganzabgeschlossener Integritätsbereich, K der Quotientenkörper von R, L/K eine endliche Körpererweiterung und $S = \bar{R}^L$. Beweisen Sie, dass es für jedes $\beta \in L$ ein $a \in R$ gibt, derart dass $a\beta \in S$.

33) Es sei R ein ganzabgeschlossener Integritätsbereich, K der Quotientenkörper von R, L/K eine endliche Körpererweiterung und $S = \bar{R}^L$. Beweisen Sie:

a) Der Quotientenkörper von S ist (isomorph zu) L.

b) Der Ring S ist ganzabgeschlossen.

34) Es sei K ein algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$ und $\{\alpha_1, \dots, \alpha_n\}$ eine Basis von K (als $\mathbb{Q}$-Vektorraum), die nur Elemente von O_K enthält. Beweisen Sie: Gilt $\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = d_K$, so ist $\{\alpha_1, \dots, \alpha_n\}$ eine Ganzheitsbasis.

35) Es sei $K = \mathbb{Q}(\sqrt{3})$. Beweisen Sie, dass $O_K^* = \mathbb{Z}[\sqrt{3}]^* = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}$.

36) Beweisen Sie, dass $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ normeuklidisch sind.

37) a) Zeigen Sie, dass $O_{\mathbb{Q}(i\sqrt{6})} = \mathbb{Z}[i\sqrt{6}]$ nicht faktoriell ist.
b) Zeigen Sie, dass $O_{\mathbb{Q}(i\sqrt{10})} = \mathbb{Z}[i\sqrt{10}]$ nicht faktoriell ist.
Hinweis. Verwenden Sie die Gleichungen

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

38) Wieso widerspricht die Gleichung $10 = 2 \cdot 5 = (3+i) \cdot (3-i)$ nicht der Tatsache, dass $O_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ faktoriell ist?

39) Es sei $p \equiv 3 \pmod 4$ eine Primzahl und $a, b \in \mathbb{Z}$. Zeigen Sie, dass aus $p \mid (a^2 + b^2)$ folgt, dass $p \mid a$ und $p \mid b$.

40) Die Zahl $n \in \mathbb{N} \setminus \{1\}$ habe Primfaktorzerlegung $n = 2^\alpha p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_\ell^{\gamma_\ell}$ (mit $k, \ell, \alpha \geq 0$, $\beta_1, \ldots, \beta_k, \gamma_1, \ldots, \gamma_\ell \geq 1$, $p_i \equiv 1 \pmod 4$ für $1 \leq i \leq k$ und $q_i \equiv 3 \pmod 4$ für $1 \leq i \leq \ell$). Beweisen Sie die Äquivalenz der folgenden beiden Aussagen:

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

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

Hinweis: Verwenden Sie die Gleichung $(x^2+y^2)(u^2+v^2) = (xu - yv)^2 + (xv + yu)^2$.

41) Beweisen Sie, dass die diophantische Gleichung $X^2 + 1 = Y^3$ nur die Lösung $(X, Y) = (0, 1)$ in $\mathbb{Z}^2$ besitzt.

42) Beweisen Sie, dass die diophantische Gleichung $Y^2 + 2 = X^3$ nur die Lösungen $(X, Y) = (3, \pm 5)$ in $\mathbb{Z}^2$ besitzt. Folgern Sie, dass 26 die einzige ganze Zahl ist, die zwischen einem (kleineren) Quadrat und einer (größeren) dritten Potenz liegt.

43) a) Es seien $a, b \in \mathbb{Z}$, $p(X) = X^3 + aX + b \in \mathbb{Z}[X]$ sei irreduzibel und α eine Nullstelle von p. Zeigen Sie die folgende Behauptung: Ist $-4a^3 - 27b^2 = 4m$ für ein quadratfreies $m \in \mathbb{Z}$ mit $m \equiv 2 \pmod 4$ oder $m \equiv 3 \pmod 4$, so ist $\{1, \alpha, \alpha^2\}$ Ganzheitsbasis von $K = \mathbb{Q}(\alpha)$ und $d_K = -4a^3 - 27b^2$.
b) Wenden Sie Teil a) auf das Polynom $p(X) = X^3 - X - 2$ an.

44) Tragen Sie den folgenden Beweis vor:

Hilbertscher Basissatz: Es sei R ein noetherscher Ring. Dann ist auch $R[X]$ ein noetherscher Ring.

Beweis: Es sei I ein Ideal von $R[X]$, das nicht endlich erzeugt ist. Dann ist $I \setminus (0) \neq \varnothing$. Wähle $p_1 \in I \setminus (0)$ mit minimalem Grad. Da I nicht endlich erzeugt ist, ist $I \setminus (p_1 R[X]) \neq \varnothing$. Wähle $p_2 \in I \setminus (p_1 R[X])$ mit minimalem Grad. Verfahre weiter so, d.h. sind $p_1, \ldots, p_n \in I$ schon gewählt, so ist $I \setminus (p_1 R[X] + \cdots + p_n R[X]) \neq \varnothing$, da I nicht endlich erzeugt ist. Wähle $p_{n+1} \in I \setminus (p_1 R[X] + \cdots + p_n R[X])$ mit minimalem Grad. Man erhält auf diese Weise eine Folge $(p_n)_{n \geq 1}$ in I. Es sei $n_i := \operatorname{grad} p_i$ und a_i der führende Koeffizient von p_i. Nach Konstruktion gilt $n_1 \leq n_2 \leq n_3 \leq \cdots$.

Wir behaupten, dass $Ra_1 \subsetneqq Ra_1 + Ra_2 \subsetneqq Ra_1 + Ra_2 + Ra_3 \subsetneqq \cdots$ eine aufsteigende Kette von Idealen ist, die nicht stationär wird. Angenommen, es wäre

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

für ein $r \in \mathbb{N}$. Dann würde es $b_1, \ldots, b_r \in R$ mit der Eigenschaft $a_{r+1} = b_1 a_1 + \cdots + b_r a_r$ geben. Betrachte

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

Es wäre $q \in I$ und $q \notin p_1 R[X] + \cdots + p_r R[X]$ (da $p_{r+1} \notin p_1 R[X] + \cdots + p_r R[X]$). Offensichtlich ist $\operatorname{grad} q \leq n_{r+1}$. Wegen $a_{r+1} - (b_1 a_1 + \cdots + b_r a_r) = 0$ ist der Koeffizient von $X^{n_{r+1}}$ in q aber 0 und daher $\operatorname{grad} q < n_{r+1}$, was der Minimalität des Grades von p_{r+1} widerspricht.

45) a) Es sei R ein noetherscher Ring und I ein Ideal von R. Zeigen Sie, dass R/I noethersch ist.
b) Es sei R ein noetherscher Ring und I ein Ideal von $R[X_1, \ldots, X_n]$. Zeigen Sie, dass $R[X_1, \ldots, X_n]/I$ noethersch ist.

46) Ist der Ring $R = \{f : [0,1] \to \mathbb{R} \mid f \text{ ist stetig}\}$ noethersch? Hinweis: Betrachten Sie $I_n = \left\{ f \in R \;\middle|\; f(x) = 0 \text{ für alle } x \in [0, \tfrac{1}{n}] \right\}$ für $n \in \mathbb{N}$.

47) Es sei K ein algebraischer Zahlkörper und P ein Primideal von O_K. Beweisen Sie:

a) Ist $\alpha \in O_K \setminus P$, so gilt $\alpha^{N(P)-1} \equiv 1 \pmod{P}$.
b) Für alle $\alpha \in O_K$ gilt $\alpha^{N(P)} \equiv \alpha \pmod{P}$.

48) Es sei $K = \mathbb{Q}(i\sqrt{6})$ und $P_1 = (2, i\sqrt{6})$ und $P_2 = (3, i\sqrt{6})$ seien Ideale von $O_K = \mathbb{Z}[i\sqrt{6}]$. Beweisen Sie

a) $(2) = P_1^2$, $(3) = P_2^2$, $(i\sqrt{6}) = (-i\sqrt{6}) = P_1 P_2$ und $(6) = P_1^2 P_2^2$,
b) P_1 und P_2 sind Primideale von O_K und $P_1 \neq P_2$.

49) Es sei $K = \mathbb{Q}(i\sqrt{10})$. Finden Sie die Zerlegung der Hauptideale (2), (7), $(2 + i\sqrt{10})$, $(2 - i\sqrt{10})$ und (14) in Primideale von $O_K = \mathbb{Z}[i\sqrt{10}]$.

Definition. Es seien $G_0, \dots, G_n$ Gruppen und für $1 \leq i \leq n$ sei $\varphi_i : G_{i-1} \to G_i$ ein Gruppenhomomorphismus. Man nennt

$$G_0 \xrightarrow{\varphi_1} G_1 \xrightarrow{\varphi_2} G_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} G_n$$

eine exakte Sequenz, wenn $\operatorname{Im} \varphi_i = \ker \varphi_{i+1}$ für $1 \leq i < n$.

50) Beweisen Sie die folgenden Aussagen, wobei G und H Gruppen sein sollen und φ ein Gruppenhomomorphismus.

a) $\varphi : G \to H$ ist genau dann injektiv, wenn $\{1\} \longrightarrow G \xrightarrow{\varphi} H$ exakt ist.

b) $\varphi : G \to H$ ist genau dann surjektiv, wenn $G \xrightarrow{\varphi} H \longrightarrow \{1\}$ exakt ist.

c) $\varphi : G \to H$ ist genau dann bijektiv (d.h. ein Isomorphismus), wenn

$$\{1\} \longrightarrow G \xrightarrow{\varphi} H \longrightarrow \{1\}$$

exakt ist.

d) Ist H ein Normalteiler von G, so ist

$$\{1\} \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \longrightarrow \{1\}$$

eine exakte Sequenz, wobei ι die Einbettung von H in G bezeichnen soll und π den kanonischen Epimorphismus.

51) Es sei K ein algebraischer Zahlkörper. Beweisen Sie, dass

$$\{1\} \longrightarrow O_K^* \xrightarrow{\iota} K^* \xrightarrow{\varphi} \mathcal{F}_K \xrightarrow{\pi} \mathcal{H}_K \longrightarrow \{1\}$$

eine exakte Sequenz ist. Dabei bezeichnen ι die Einbettung von O_K^* in K^*, π den kanonischen Epimorphismus und es sei $\varphi : K^* \to \mathcal{F}_K$, $\varphi(\alpha) = \langle \alpha \rangle = \alpha O_K$.

52) Es sei $K = \mathbb{Q}(i\sqrt{43})$. Zeigen Sie $h_K = 1$, d.h. $O_K = \mathbb{Z}\big[\frac{1}{2}(1 + i\sqrt{43})\big]$ ist faktoriell.

53) Es sei $K = \mathbb{Q}(i\sqrt{67})$. Zeigen Sie $h_K = 1$ d.h. $O_K = \mathbb{Z}\big[\frac{1}{2}(1 + i\sqrt{67})\big]$ ist faktoriell.

54) Es sei $K = \mathbb{Q}(\sqrt{5})$. Zeigen Sie $h_K = 1$, d.h. $O_K = \mathbb{Z}\big[\frac{1}{2}(1 + \sqrt{5})\big]$ ist faktoriell.

55) Es sei $K = \mathbb{Q}(\sqrt{6})$. Zeigen Sie $h_K = 1$, d.h. $O_K = \mathbb{Z}[\sqrt{6}]$ ist faktoriell.

56) Es sei $K = \mathbb{Q}(i\sqrt{6})$. Zeigen Sie $\mathcal{H}_K = \big\{\big[(1)\big], \big[(2, i\sqrt{6})\big]\big\} = \big\{\big[(1)\big], \big[(3, i\sqrt{6})\big]\big\}$, $h_K = 2$ und $\mathcal{H}_K \cong \mathbb{Z}/2\mathbb{Z}$.

57) Es sei $\mathbb{P}$ die Menge der Primzahlen und $|x|_\infty$ bezeichne den gewöhnlichen Absolutbetrag von $x \in \mathbb{Q}$. Beweisen Sie

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1 \quad \text{für alle } x \in \mathbb{Q} \setminus \{0\}.$$