Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der jeweils nächsten Übungsgruppe besprochen. Für jede richtig gelöste Aufgabe gibt es 4 Punkte.

Aufgabe 1. Diese Aufgabe setzt die in der Vorlesung begonnene Untersuchung von Quadratsummen fort:

(a) Wir haben gesehen, dass jede Primzahl $p \equiv 1 \pmod 4$ in dem Ring $\mathbb{Z}[i]$ als Produkt zweier irreduzibler Faktoren zerfällt. Man überlege sich, dass jede Primzahl $p \equiv 3 \pmod 4$ in diesem Ring irreduzibel bleibt.

(b) Jede natürliche Zahl ist ein Produkt $n = \prod_{p\,\mathrm{prim}} p^{\nu_p}$ von Primzahlen $p \in \mathbb{Z}$ mit Vielfachheiten $\nu_p \geq 0$. Man finde hiervon ausgehend ein notwendiges und hinreichendes Kriterium für die Existenz einer Darstellung $n = x^2 + y^2$ als Summe von Quadraten ganzer Zahlen $x, y \in \mathbb{Z}$.

Aufgabe 2. Sei R ein faktorieller Ring. Zwei Elemente $a, b \in R$ heißen teilerfremd, wenn sie außer Einheiten keine gemeinsamen Teiler besitzen. Man zeige: Ist in diesem Fall $ab = x^n$ für ein $x \in R$ und $n \in \mathbb{N}$, so folgt

$$a \;=\; \epsilon u^n \quad \text{und} \quad b \;=\; \epsilon^{-1} v^n \quad \text{mit} \quad \epsilon \;\in\; R^\times \quad \text{und} \quad u, v \;\in\; R.$$

Als Anwendung finde man alle ganzzahligen Lösungen der Gleichung $y^2 = x^3 - 1$, indem man $R = \mathbb{Z}[i]$ setzt.

Aufgabe 3. Sei $p \in \mathbb{Z}$ eine Primzahl, sodass das Polynom $x^2 + 2$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ eine Nullstelle hat. Man übertrage die Argumente aus der Vorlesung auf den faktoriellen Ring $R = \mathbb{Z}[\sqrt{-2}]$, um zu zeigen, dass dann

$$p \;=\; x^2 + 2y^2 \quad \text{mit} \quad x, y \;\in\; \mathbb{Z}$$

ist, und formuliere ohne Beweis eine Vermutung, für welche Primzahlen p dies gilt!

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der jeweils nächsten Übungsgruppe besprochen. Für jede richtig gelöste Aufgabe gibt es 4 Punkte.

Aufgabe 4. (a) Welche der Ringe $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Q}[x,y]$ sind Hauptidealringe?

(b) Man prüfe nach, dass für $d \equiv 1 \pmod 4$ das Minimalpolynom von $\alpha = \frac{1+\sqrt{d}}{2}$ ganzzahlige Koeffizienten hat und

$$\mathbb{Z}[\alpha] \;=\; \{\, m + n\alpha \mid m, n \in \mathbb{Z}\,\}$$

gilt. Man zeige weiter, dass der Ring $\mathbb{Z}[\alpha]$ für $d \in \{-3, -7, -11\}$ Euklidisch, für $d = -15$ aber nicht faktoriell ist.

Im Folgenden wollen wir den Ring $R = \mathbb{Z}[\alpha]$ für $\alpha = \frac{1+\sqrt{-19}}{2}$ betrachten.

Aufgabe 5. (a) Man zeige $R^\times = \{\pm 1\}$ und berechne das Minimalpolynom von α.

(b) Welche der Primzahlen $p = 2, 3, 5, 7, 11$ und 13 sind in R irreduzibel?

Aufgabe 6. Man zeige, dass der Ring R bezüglich keiner Funktion $N : R \longrightarrow \mathbb{N}_0$ Euklidisch sein kann. Dazu nehme man das Gegenteil an und finde zunächst ein Ringelement $m \in R \setminus (R^\times \cup \{0\})$, sodass jedes $a \in R$ bei Division durch m einen Rest

$$r \;\in\; \{0, \pm 1\}$$

lässt. Was folgt hieraus über den Quotientenring $R/(m)$? Man führe dies zu einem Widerspruch, indem man zeigt, dass das Minimalpolynom aus Aufgabe 5(a) in diesem Quotientenring keine Nullstelle hat.

Aufgabe 7. Dennoch ist R ein Hauptidealring: Ist $\mathfrak{a} \trianglelefteq R$ ein von Null verschiedenes Ideal und $b \in \mathfrak{a} \setminus \{0\}$ ein Element minimalen Absolutbetrags, so ist $\mathfrak{a} = (b)$. Um dies zu sehen, nehme man die Existenz eines $a \in \mathfrak{a} \setminus (b)$ an und suche nach $r, s \in R$ mit

$$0 \;<\; |ar + bs| \;<\; |b|.$$

Dabei reduziere man zunächst auf den Fall von Imaginärteilen $|\mathrm{Im}(a/b)| \leq \sqrt{19}/4$ und unterscheide zwischen

$$|\mathrm{Im}(a/b)| \;\in\; [0, \sqrt{3}/2) \quad \text{bzw.} \quad |\mathrm{Im}(a/b)| \;\in\; [\sqrt{3}/2, \sqrt{19}/4].$$

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der jeweils nächsten Übungsgruppe besprochen. Für jede richtig gelöste Aufgabe gibt es 4 Punkte.

Aufgabe 8. Sei $d < 0$ eine quadratfreie ganze Zahl, welche durch mindestens zwei Primzahlen teilbar ist. Man überlege sich, dass $\mathbb{Z}[\sqrt{d}]$ kein Hauptidealring ist. Man zeige andererseits, dass $\mathbb{Z}[\sqrt{6}]$ sogar ein Euklidischer Ring ist bezüglich der üblichen Norm

$$N(x + y\sqrt{6}) \; = \; |x^2 - 6y^2|.$$

Aufgabe 9. Welche der Ringerweiterungen

$$\mathbb{Z} \; \subset \; \mathbb{Z}[\sqrt{5}] \; \subset \; \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \; \subset \; \mathbb{Z}[\tfrac{1}{2}, \sqrt{5}] \; \subset \; \mathbb{Q}(\sqrt{5})$$

sind ganz? Welche der auftretenden Integritätsringe sind ganz abgeschlossen?

Aufgabe 10. Sei K/k eine endliche separable Körpererweiterung. Es ist $K = K(\alpha)$ für ein geeignet gewähltes Element $\alpha \in K$, und wir bezeichnen die Nullstellen des Minimalpolynoms von α in einem algebraischen Abschluß mit $\alpha_1, \ldots, \alpha_n \in \overline{k}$. Man zeige

$$d_{K/k}(\alpha) \; = \; \prod_{i<j} (\alpha_i - \alpha_j)^2$$

und folgere: Für $n = 3$ ist K/k eine Galoiserweiterung genau dann, wenn $\sqrt{d} \in K$.

Bonusaufgabe. Für kommutative Ringe R und $A = (a_{ij})_{1 \leq i,j \leq n} \in Mat_{n \times n}(R)$ beweise man die Identität

$$A^* \cdot A = \det(A) \cdot \mathbb{I}_n.$$

Hierbei ist $\mathbb{I}_n$ die Einheitsmatrix und

$$\begin{aligned} \det(A) \;\; &= \;\; \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} \cdots a_{n\sigma(n)} \; \in \; R, \\ A^* \;\; &= \;\; \big((-1)^{j+k} \cdot \det(A_{jk})\big)_{1 \leq j,k \leq n} \; \in \; \mathrm{Mat}_{n \times n}(R), \end{aligned}$$

wobei A_{jk} aus A durch Streichen der j-ten Spalte und k-ten Zeile hervorgeht.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der jeweils nächsten Übungsgruppe besprochen. Für jede richtig gelöste Aufgabe gibt es 4 Punkte.

Aufgabe 8. Sei $d < 0$ eine quadratfreie ganze Zahl, welche durch mindestens zwei Primzahlen teilbar ist. Man überlege sich, dass $\mathbb{Z}[\sqrt{d}]$ kein Hauptidealring ist. Man zeige andererseits, dass $\mathbb{Z}[\sqrt{6}]$ sogar ein Euklidischer Ring ist.

Aufgabe 9. Welche der Ringerweiterungen

$$\mathbb{Z} \;\subset\; \mathbb{Z}[\sqrt{5}] \;\subset\; \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \;\subset\; \mathbb{Z}[\tfrac{1}{2}, \sqrt{5}] \;\subset\; \mathbb{Q}(\sqrt{5})$$

sind ganz? Welche der auftretenden Integritätsringe sind ganz abgeschlossen?

Aufgabe 10. Man berechne den Ganzheitsring $\mathfrak{o}_K$ und die Diskriminante d_K für die beiden Zahlkörper

$$K \;=\; \mathbb{Q}(\sqrt[3]{2}) \qquad \text{und} \qquad K \;=\; \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Aufgabe 11. Für eine endliche separable Körpererweiterung K/k mit $[K : k] = 3$ betrachte man die Galoisoperation auf einer Quadratwurzel von

$$d \;=\; \det\Big(tr_{K/k}(\alpha_i\alpha_j)\Big)_{i,j}$$

wobei $\alpha_1, \alpha_2, \alpha_3$ eine k-Basis des Vektorraumes K seien. Man beweise: K/k ist eine Galoiserweiterung genau dann, wenn $\sqrt{d} \in K$ ist.

Bonusaufgabe. Für kommutative Ringe R und $A = (a_{ij})_{1\leq i,j\leq n} \in Mat_{n\times n}(R)$ beweise man die Identität

$$A^* \cdot A = \det(A) \cdot \mathbb{I}_n.$$

Hierbei ist $\mathbb{I}_n$ die Einheitsmatrix und

$$\begin{aligned} \det(A) \;&=\; \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma)\cdot a_{1\sigma(1)}\cdots a_{n\sigma(n)} \;\in\; R, \\ A^* \;&=\; \big((-1)^{j+k}\cdot\det(A_{jk})\big)_{1\leq j,k\leq n} \;\in\; \mathrm{Mat}_{n\times n}(R), \end{aligned}$$

wobei A_{jk} aus A durch Streichen der j-ten Spalte und k-ten Zeile hervorgeht.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der jeweils nächsten Übungsgruppe besprochen. Für jede richtig gelöste Aufgabe gibt es 4 Punkte.

Aufgabe 11. Man zeige

$$\mathfrak{o}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\sqrt{3} \oplus \mathbb{Z}\frac{\sqrt{2}+\sqrt{6}}{2} \quad \text{für} \quad K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Hinweis: Die Norm und Spur für Erweiterungen von Zahlkörpern erhalten Ganzheit, insbesondere ist $N_{K/k}(\mathfrak{o}_K), tr_{K/k}(\mathfrak{o}_K) \subseteq \mathfrak{o}_k$ für $k = \mathbb{Q}(\sqrt{d})$ mit $d \in \{2, 3, 6\}$.

Aufgabe 12. Sei $\alpha = \alpha_1$ eine algebraische Zahl mit Minimalpolynom $f(x) \in \mathbb{Q}[x]$, dessen Nullstellen wir im Folgenden mit $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ bezeichnen. Man zeige, dass

$$d_{K/\mathbb{Q}}(\alpha) \; = \; (-1)^{\binom{n}{2}} \prod_i f'(\alpha_i)$$

für $K = \mathbb{Q}(\alpha)$ gilt, wobei $f'(x) \in \mathbb{Q}[x]$ die formale Ableitung von $f(x)$ sei.

Aufgabe 13. Man zeige:

(a) Das Polynom $f(x) = x^3 + 2x + 1$ ist in $\mathbb{Q}[x]$ irreduzibel.

(b) Für seine Nullstellen $\alpha = \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ gilt $f'(\alpha_i) = \frac{4}{\alpha_i}(-\frac{3}{4} - \alpha_i)$.

(c) Für $K = \mathbb{Q}(\alpha)$ folgt aus Aufgabe 12, dass $d_{K/\mathbb{Q}}(\alpha) = -59$ und $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ ist.

Bonusaufgabe. Für $K = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[3]{2}$ zeige man, dass $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ ist:

(a) Man berechne $d_K(1, \alpha, \alpha^2)$ und folgere: Wäre $\mathfrak{o}_K \neq \mathbb{Z}[\alpha]$, so läge in $\mathfrak{o}_K \setminus \mathbb{Z}[\alpha]$ ein Element

$$\tfrac{1}{p}(c_0 + c_1\alpha + c_2\alpha^2) \quad \text{mit} \quad c_0, c_1, c_2 \in \mathbb{Z},\; p \in \{2, 3\},\; p \nmid c_i \text{ für ein } i \in \{0, 1, 2\}.$$

(b) Durch Multiplikation mit α-Potenzen und Subtraktion von Elementen in $\mathbb{Z}[\alpha]$ reduziere man zunächst auf den Fall $c_0 = 0$, $c_1, c_2 \in \{0, 1\}$ für $p = 2$ bzw. auf den Fall $c_0 = 1$, $c_1, c_2 \in \{0, \pm 1\}$ für $p = 3$. In beiden Fällen führe man durch Betrachten der Norm und/oder Spur einen Widerspruch herbei.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 14. Sei R ein Integritätsring. Man zeige:

(a) Ein Hauptideal $(a) \lhd R$ ist prim genau dann, wenn a prim oder Null ist.

(b) Ist ein von Null verschiedenes Hauptideal $(a) \lhd R$ maximal, dann ist a ein irreduzibles Element. Die Umkehrung hiervon gilt in Hauptidealringen, ist aber ansonsten im Allgemeinen falsch; man finde ein Gegenbeispiel.

Aufgabe 15. Sei R ein Dedekind-Ring. Für Ideale $\mathfrak{a}, \mathfrak{b} \unlhd R$ definiert man den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache durch

$$\mathfrak{d} \;:=\; \mathfrak{a} + \mathfrak{b} \;=\; \big\{ a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b} \big\} \quad \text{und} \quad \mathfrak{m} \;:=\; \mathfrak{a} \cap \mathfrak{b}.$$

Man zeige:

- Es ist $\mathfrak{d} \mid \mathfrak{a}$ und $\mathfrak{d} \mid \mathfrak{b}$. Für alle $\mathfrak{c} \unlhd R$ mit $\mathfrak{c} \mid \mathfrak{a}$ und $\mathfrak{c} \mid \mathfrak{b}$ gilt $\mathfrak{c} \mid \mathfrak{d}$.
- Es ist $\mathfrak{a} \mid \mathfrak{m}$ und $\mathfrak{b} \mid \mathfrak{m}$. Für alle $\mathfrak{n} \unlhd R$ mit $\mathfrak{a} \mid \mathfrak{n}$ und $\mathfrak{b} \mid \mathfrak{n}$ gilt $\mathfrak{m} \mid \mathfrak{n}$.

Wie liest man die Primfaktorzerlegung der Ideale $\mathfrak{d}$ und $\mathfrak{m}$ aus der von $\mathfrak{a}$ und $\mathfrak{b}$ ab?

Aufgabe 16. In $R = \mathbb{Z}[\sqrt{-5}]$ finde man vier Primideale $\mathfrak{p}_i \lhd R$ mit

$$(2) = \mathfrak{p}_1\mathfrak{p}_2, \quad (3) = \mathfrak{p}_3\mathfrak{p}_4, \quad (1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3 \quad \text{und} \quad (1-\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4.$$

Bonusaufgabe. Sei $K = \mathbb{Q}(\alpha)$ für eine algebraische Zahl α, deren Minimalpolynom ein Eisenstein-Polynom[1] bezüglich einer Primzahl p ist. Man folgere $p \nmid [\mathfrak{o}_K : \Lambda]$ für das Gitter $\Lambda = \mathbb{Z}[\alpha]$. Dazu überlege man sich zunächst, dass es andernfalls $a_\nu \in \mathbb{Z}$ gäbe mit

$$\tfrac{1}{p} \cdot (a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \;\in\; \mathfrak{o}_K \setminus \Lambda,$$

reduziere unter Benutzung des Minimalpolynoms auf den Fall $a_\nu = 0$ für $\nu \neq n-1$ und erhalte durch Bilden der Norm einen Widerspruch.

[1] Ein *Eisenstein-Polynom* bezüglich p ist ein Polynom $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{Z}[x]$ mit $p \mid c_i$ für alle i, aber $p^2 \nmid c_0$. Solche Polynome sind insbesondere irreduzibel.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 17. Für ganze Erweiterungen von Integritätsringen $R \subseteq S$ zeige man:

(a) Es ist S ein Körper genau dann, wenn R ein Körper ist.

(b) Ein Primideal $\mathfrak{m} \lhd S$ ist maximal genau dann, wenn $R \cap \mathfrak{m} \lhd R$ maximal ist.

Aufgabe 18. Sei $R = \mathbb{Z}[\sqrt{d}]$ für eine quadratfreie Zahl $d \equiv 1 \pmod 4$. Man zeige am folgenden Beispiel, dass in diesem Ring keine eindeutige Faktorisierung von Idealen möglich ist:

$$(2, 1+\sqrt{d}) \cdot (2, 1+\sqrt{d}) \;=\; (2) \cdot (2, 1+\sqrt{d}), \quad \text{aber} \quad (2) \;\neq\; (2, 1+\sqrt{d}).$$

Welche Teile der Definition von Dedekind-Ringen sind für R erfüllt, welche nicht?

Aufgabe 19. Es sei K ein quadratischer Zahlkörper und $z \mapsto \overline{z}$ das nichttriviale Element seiner Galoisgruppe. Man beweise, dass dann für jedes Ideal $\mathfrak{a} = (\alpha, \beta)$ mit $\alpha, \beta \in \mathfrak{o}_K$ gilt:

$$\mathfrak{a} \cdot \overline{\mathfrak{a}} \;=\; \big(N_{K/\mathbb{Q}}(\alpha),\, tr_{K/\mathbb{Q}}(\alpha\overline{\beta}),\, N_{K/\mathbb{Q}}(\beta)\big).$$

Dazu schreibe man den Durchschnitt des rechten Ideals mit dem Teilring $\mathbb{Z} \subset \mathfrak{o}_K$ in der Form

$$\big(N_{K/\mathbb{Q}}(\alpha),\, tr_{K/\mathbb{Q}}(\alpha\overline{\beta}),\, N_{K/\mathbb{Q}}(\beta)\big) \cap \mathbb{Z} \;=\; d\mathbb{Z}$$

mit $d \neq 0$ und zeige durch Betrachten der Norm und Spur, dass $\alpha\overline{\beta}/d \in \mathfrak{o}_K$ ist.

Bonusaufgabe. Man zeige für den Ring $S = \{\alpha \in \mathbb{C} \mid \alpha \text{ ist ganz über } \mathbb{Z}\}$:

(a) Der Ring S ist ganz abgeschlossen und hat Krull-Dimension $\dim(S) = 1$.

(b) Die Kette

$$(2) \;\subsetneq\; (\sqrt{2}) \;\subsetneq\; (\sqrt[4]{2}) \;\subsetneq\; (\sqrt[8]{2}) \;\subsetneq\; \cdots$$

von Hauptidealen wird nicht stationär und somit ist S nicht Noethersch.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 20.

(a) Für welche Zahlkörper K ist die Einheitengruppe $\mathfrak{o}_K^\times$ endlich? Man berechne diese endliche Gruppe in allen Fällen.

(b) Man finde für $K = \mathbb{Q}(\sqrt{61})$ die Fundamentaleinheit und bestimme mit einem Taschenrechner die kleinste Lösung $(x, y) \in \mathbb{N}^2$ von $x^2 = 61y^2 + 1$.

Aufgabe 21. Sei K ein Zahlkörper. Wir sagen, ein gegebenes Ideal $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ werde in einer endlichen Körpererweiterung L/K ein Hauptideal, wenn das hiervon erzeugte Ideal

$$\mathfrak{a} \cdot \mathfrak{o}_L \;=\; \Big\{ \sum_{i=1}^{N} \alpha_i \beta_i \mid \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{o}_L \Big\} \;\trianglelefteq\; \mathfrak{o}_L$$

ein Hauptideal ist. Man zeige:

(a) Ist $\mathfrak{a}^n = (a)$ ein Hauptideal von $\mathfrak{o}_K$, dann wird $\mathfrak{a}$ ein Hauptideal in $K(\sqrt[n]{a})$.

(b) Insbesondere existiert wegen der Endlichkeit der Klassengruppe eine endliche Erweiterung L/K, in der jedes Ideal $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ ein Hauptideal wird.

Aufgabe 22. Für $K = \mathbb{Q}(\sqrt{-13})$ zeige man:

(a) Das Hauptideal $(2) \trianglelefteq \mathfrak{o}_K$ ist Quadrat eines Primideals.

(b) Das Hauptideal $(3) \trianglelefteq \mathfrak{o}_K$ ist ein Primideal.

(c) Für die Klassengruppe gilt $C_K \simeq \mathbb{Z}/2\mathbb{Z}$.

Bonusaufgabe. Man benutze die obige Klassengruppe, um alle Lösungen $(x, y) \in \mathbb{N}^2$ für die Gleichung $x^2 + 13 = y^3$ zu finden:

(a) Man zeige, dass y ungerade und teilerfremd zu x ist, und folgere hieraus, dass die beiden Ideale

$$(x + \sqrt{-13}), (x - \sqrt{-13}) \;\trianglelefteq\; \mathfrak{o}_K$$

teilerfremd sind. Hinweis: Die Summe dieser Ideale enthält y^3 und $2x$.

(b) Man folgere, dass $(x + \sqrt{-13}) = \mathfrak{a}^3$ die dritte Potenz eines Ideals $\mathfrak{a} \trianglelefteq \mathfrak{o}_K$ ist.

(c) Wegen $|C_K| = 2$ muß dabei $\mathfrak{a}$ ein Hauptideal sein. Was folgt für die Zahl x?

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 23. Sei R ein Dedekind-Ring, $\mathfrak{a} \trianglelefteq R$ ein Ideal und $0 \neq \alpha \in \mathfrak{a}$ ein beliebig gewähltes Element. Man zeige

$$\mathfrak{a} \;=\; (\alpha, \beta) \quad \text{für ein} \quad \beta \;\in\; \mathfrak{a}.$$

Dazu schreibe man die Primfaktorzerlegung des Ideals in der Form $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ mit $e_i \in \mathbb{N}$, zeige $(\alpha) = \mathfrak{b} \cdot \mathfrak{c}$ mit $\mathfrak{a} \mid \mathfrak{b}$ und $\operatorname{ggT}(\mathfrak{a}, \mathfrak{c}) = (1)$ und wähle nach dem Chinesischen Restsatz

$$\beta \;\in\; \bigcap_{i=1}^{n} \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1} \quad \text{mit} \quad \beta - 1 \;\in\; \mathfrak{c}.$$

Aufgabe 24. Sei $K = \mathbb{Q}(\sqrt{-14})$.

(a) Man finde Primideale $\mathfrak{p}, \mathfrak{q}_1, \mathfrak{q}_2 \trianglelefteq \mathfrak{o}_K$ mit $(2) = \mathfrak{p}^2$ und $(3) = \mathfrak{q}_1\mathfrak{q}_2$ und prüfe nach, dass keines dieser drei Primideale ein Hauptideal ist.

(b) Durch Betrachten von Normen zeige man

$$(2 + \sqrt{-14}) \;=\; \mathfrak{p} \cdot \mathfrak{q}_i^2 \quad \text{für ein} \quad i \;\in\; \{1, 2\}.$$

(c) Man berechne die Minkowski-Schranke M_K und die Klassengruppe C_K.

Aufgabe 25. Sei $K = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[3]{2}$. Für die Primzahlen $p = 2, 3, 5, 7, 11, 31$ zerlege man das Polynom

$$x^3 - 2 \;\in\; \mathbb{F}_p[x]$$

modulo p in irreduzible Faktoren, finde die Primfaktorzerlegung der Ideale $(p) \trianglelefteq \mathfrak{o}_K$ und gebe die Verzweigungsindices und Restklassengrade an.

Zusatzfrage. Gibt es für den Zahlkörper der vorigen Aufgabe eine Primzahl p mit einer Zerlegung $(p) = \mathfrak{p}\mathfrak{q}^2$ für Primideale $\mathfrak{p} \neq \mathfrak{q}$ in $\mathfrak{o}_K = \mathbb{Z}[\alpha]$?

Die folgenden Fragen sind als Wiederholung im Stil von Klausuraufgaben gedacht, können aber wie gewohnt schriftlich abgegeben und in der nächsten Übungsgruppe besprochen werden. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 1. Wann nennt man eine Zahl $\alpha \in \mathbb{C}$ algebraisch, wann ganz? Welche der Zahlen

$$\alpha_1 \;=\; \sqrt{2}+\sqrt{3}, \quad \alpha_2 \;=\; \frac{1}{\sqrt{2}}, \quad \alpha_3 \;=\; \frac{1+i}{\sqrt{2}} \quad \text{und} \quad \alpha_4 \;=\; \frac{\sqrt{2}+\sqrt{6}}{2}$$

sind ganze algebraische Zahlen, und wie sehen jeweils die Minimalpolynome aus?

Aufgabe 2. Für welche $d \in \{2,3,5\}$ ist der Ring $\mathbb{Z}[\sqrt{-d}]$

(a) Euklidisch bezüglich der Norm,

(b) faktoriell,

(c) ein Dedekind-Ring?

Aufgabe 3. Wann bezeichnet man einen kommutativen Ring als Noethersch? Man zeige, dass sich in Noetherschen Integritätsringen jedes Element als ein endliches Produkt von irreduziblen Elementen schreiben lässt.

Aufgabe 4. Für $K = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[4]{2}$ berechne man die Diskriminante $d_{K/\mathbb{Q}}(\alpha)$.

Aufgabe 5. Welche der Untergruppen

$$\begin{aligned}
\Lambda_1 &= \big\{12a + 8b \mid a, b \in \mathbb{Z}\big\} &&\subset \mathbb{R}\\
\Lambda_2 &= \big\{\, a + b\sqrt{2} \mid a, b \in \mathbb{Z}\big\} &&\subset \mathbb{R}\\
\Lambda_3 &= \big\{(a,\, b\sqrt{2}) \mid a, b \in \mathbb{Z}\big\} &&\subset \mathbb{R}^2
\end{aligned}$$

sind Gitter in dem jeweils auf der rechten Seite stehenden reellen Vektorraum, und was besagt in diesem Fall der Minkowski'sche Gitterpunktsatz?

Aufgabe 6. Sei $K = \mathbb{Q}(\sqrt{-43})$.

(a) Man berechne das Minimalpolynom von $\alpha = \frac{1+\sqrt{-43}}{2}$ über $\mathbb{Q}$.

(b) Man zeige, dass das Ideal $(p) \trianglelefteq \mathfrak{o}_K$ für $p = 2, 3$ ein Primideal ist.

(c) Man berechne die Minkowski-Schranke M_K und folgere, dass $\mathfrak{o}_K$ faktoriell ist.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 26. Sei K/k eine Erweiterung von Zahlkörpern und $\mathfrak{P} \mid \mathfrak{p}$ ein Paar darin übereinanderliegender Primideale. Man zeige:

(a) Ist $k \subseteq K' \subseteq K$ ein Zwischenkörper, so gilt für das Primideal $\mathfrak{P}' = \mathfrak{P} \cap K'$ die Formel

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{P}'} \cdot e_{\mathfrak{P}'|\mathfrak{p}} \quad \text{und} \quad f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{P}'} \cdot f_{\mathfrak{P}'|\mathfrak{p}}.$$

(b) Sind K', K'' zwei Zwischenkörper und ist $\mathfrak{p}$ im ersten der beiden voll verzweigt, im zweiten jedoch unverzweigt, dann ist notwendigerweise $K' \cap K'' = k$.

Aufgabe 27. Man bestimme die Galoishülle $K/\mathbb{Q}$ des Zahlkörpers $K' = \mathbb{Q}(\sqrt[3]{2})$ und zeige, dass sie genau einen quadratischen Zahlkörper enthält. Welchen? Man finde die Verzweigungsindices und Restklassengrade für die Primideale

$$\mathfrak{P} \in \mathrm{Spm}(\mathfrak{o}_K) \quad \text{über} \quad p = 2, 3, 5$$

und gebe ihre Zerlegungs- und Trägheitskörper an, ohne die Primideale explizit zu berechnen. Zur Erinnerung: In K' sind $2, 3$ voll verzweigt und $(5) = \mathfrak{p}\mathfrak{q}$ mit $\mathfrak{p} \neq \mathfrak{q}$.

Aufgabe 28. Sei k ein Körper. Man zeige, dass für irreduzible Polynome $f(x) \in k[x]$ folgende Bedingungen äquivalent zueinander sind:

(a) Es ist $f'(x) = 0$.

(b) Es ist $char(k) = p > 0$, und $f(x) = g(x^p)$ für ein Polynom $g(y) \in k[y]$.

(c) Im algebraischen Abschluß $\overline{k}$ von k besitzt $f(x)$ eine mehrfache Nullstelle.

(d) Es ist $\mathrm{ggT}(f(x), f'(x)) \neq 1$ in $\overline{k}[x]$ und somit auch in $k[x]$.

Zusatzfrage. Ein irreduzibles Polynom $f(x) \in k[x]$ heißt *inseparabel*, wenn es die obigen Eigenschaften besitzt. Man zeige, dass es genau dann ein solches Polynom gibt, wenn $char(k) = p > 0$ ist und $\Phi : k \to k, \alpha \mapsto \alpha^p$ nicht surjektiv ist. Man finde ein Beispiel für einen Körper mit diesen Eigenschaften.

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 29. Für $n \in \mathbb{N}$ bezeichne $\Phi_n(x)$ das n-te Kreisteilungspolynom.

(a) Man zeige $\Phi_{2n}(x) = \Phi_n(-x)$ für ungerades $n > 1$.

(b) Man zeige $\Phi_{np^\nu}(x) = \Phi_{np}(x^{p^{\nu-1}})$ für $\nu \in \mathbb{N}$ und Primzahlen $p \nmid n$.

(c) Man berechne das Polynom $\Phi_{144}(x)$.

Aufgabe 30. Sei $n \in \mathbb{N}$. Man zeige:

(a) Wenn $\Phi_n(x)$ modulo einer Primzahl irreduzibel ist, so ist $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch.

(b) Für $n \in \{12, 15, 16\}$ berechne man $(\mathbb{Z}/n\mathbb{Z})^\times$ und folgere, dass $\Phi_n(x)$ modulo jeder Primzahl reduzibel ist.

(c) Man finde eine Primzahl, modulo der alle drei Polynome $\Phi_n(x)$ aus Teil (b) komplett in Linearfaktoren zerfallen.

Aufgabe 31. Sei $K = \mathbb{Q}(\zeta)$ der von $\zeta = e^{2\pi i/9}$ erzeugte Kreisteilungskörper.

(a) Man zeige, dass die Gruppe $Gal(K/\mathbb{Q})$ zyklisch ist, und finde einen Erzeuger.

(b) Man folgere, dass K genau zwei echte Teilkörper $k \neq \mathbb{Q}$ enthält — welche?

(c) Man finde für alle Primideale $\mathfrak{P} \trianglelefteq \mathfrak{o}_K$ über den Primzahlen $p = 2, 3, 5, 19$ die Verzweigungsindices, Restklassengrade, Zerlegungs- und Trägheitsgruppen sowie im unverzweigten Fall den Frobenius $\mathrm{Fr}_p \in Gal(K/\mathbb{Q})$.

Bonusaufgabe. Man beweise in folgenden Schritten, dass es für jedes $n \in \mathbb{N}$ unendlich viele Primzahlen $p \equiv 1 \pmod{n}$ gibt:

(a) Für je endlich viele vorgegebene Primzahlen $p_1, \dots, p_r \equiv 1 \pmod{n}$ zeige man, dass die Zahl

$$N \;=\; \Phi_n(mn \cdot p_1 \cdots p_r) \quad \text{für} \quad m \;\gg\; 0$$

durch mindestens eine weitere Primzahl $p \neq p_1, \dots, p_r$ teilbar ist.

(b) Man folgere, dass $\mathbb{F}_p$ alle n-ten Einheitswurzeln enthält. Was gilt dann für p?

Übungen zur Algebraischen Zahlentheorie — Blatt 12

Dr. T. Krämer — Abgabe: 11. Juli 2017

Die Lösungen zu den Aufgaben sind Dienstags *vor* der Vorlesung abzugeben und werden in der folgenden Übung besprochen. Für jede Aufgabe gibt es 6 Punkte.

Aufgabe 32. (a) Modulo welcher Primzahlen p ist 21 ein quadratischer Rest?

(b) Besitzt die Kongruenz $x^2 \equiv 6 \pmod{215}$ eine Lösung $x \in \mathbb{Z}$?

Aufgabe 33. Sei $d = n^2 - 2$ mit $n \in \mathbb{N}$. Man zeige:

(a) Für jede ungerade Primzahl p mit $p \mid d$ gilt $p \equiv \pm 1 \pmod 8$.

(b) Im Fall $4 \mid n$ ist d durch mindestens eine Primzahl $p \equiv -1 \pmod 8$ teilbar.

(c) Es gibt unendlich viele Primzahlen der Form $p = 8k + 7$ mit $k \in \mathbb{N}$.

Aufgabe 34. Seien $K_1, K_2 \subset \mathbb{C}$ zwei Zahlkörper, Galois'sch über $k = K_1 \cap K_2$. Wir haben ein Diagramm

$$\begin{tikzcd}[column sep=small] & K \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\ & k & \end{tikzcd}$$

wobei $K = K_1K_2 \subset \mathbb{C}$ das Kompositum der zwei Zahlkörper sei, also der kleinste beide enthaltende Zahlkörper. Man zeige:

(a) Jede Basis der Körpererweiterung K_1/k ist auch eine Basis von K/K_2.

(b) Es ist $tr_{K/K_2}(\alpha) = tr_{K_1/k}(\alpha)$ für alle $\alpha \in K_1$.

(c) Im Fall $k = \mathbb{Q}$ wende man Teil (a) auf eine Ganzheitsbasis von $\mathfrak{o}_{K_1}$ an und folgere

$$d_{K_1} \cdot \mathfrak{o}_K \;\subseteq\; \mathfrak{o}_{K_1}\mathfrak{o}_{K_2} \;:=\; \Big\{ \sum_i \alpha_1^{(i)}\alpha_2^{(i)} \;\Big|\; \alpha_\nu^{(i)} \in \mathfrak{o}_{K_\nu} \text{ für } \nu = 1, 2 \Big\}.$$

(d) Gilt für die Diskriminanten $\mathrm{ggT}(d_{K_1}, d_{K_2}) = 1$, dann folgt $\mathfrak{o}_K = \mathfrak{o}_{K_1}\mathfrak{o}_{K_2}$.

Bonusaufgabe. Für $K = \mathbb{Q}(\zeta_n)$ mit $n \in \mathbb{N}$, $\zeta_n = e^{2\pi i/n}$ folgere man aus Teil (d) der letzten Aufgabe

$$\mathfrak{o}_K \;=\; \mathbb{Z}[\zeta_n].$$

Die Lösungen zu diesem ergänzenden Aufgabenblatt können zu einem beliebigen Zeitpunkt abgegeben und in der Übung am 17. Juli besprochen werden.

Aufgabe 35. Sei K ein Körper und $v : K \to \mathbb{R} \cup \{\infty\}$ eine Bewertung.

(a) Man prüfe nach, dass $R = \{\alpha \in K \mid v(\alpha) \geq 0\}$ ein lokaler Ring ist.

(b) Man beweise die folgenden Äquivalenzen:

$$v \text{ ist diskret} \iff R \text{ ist ein Hauptidealring} \iff R \text{ ist Noethersch.}$$

(c) Ist v diskret und $\pi \in R$ ein Erzeuger des maximalen Ideals, so zeige man, dass genau eine Fortsetzung zu einer Bewertung $v : K(\sqrt{\pi}) \to \mathbb{R} \cup \{\infty\}$ existiert.

(d) Man finde ein Beispiel einer nicht-diskreten Bewertung.

Aufgabe 36. Sei $R = \mathbb{Z}[\sqrt{-6}]$.

(a) Man überlege sich, dass die abelsche Gruppe $M = \{\, a\sqrt{2} + b\sqrt{-3} \mid a, b \in \mathbb{Z} \,\}$ eine natürliche R-Modulstruktur trägt.

(b) Man zeige, dass für jedes Primideal $\mathfrak{p} \trianglelefteq R$ die Lokalisierung $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul vom Rang 1 ist, und finde einen Erzeuger.

(c) Man zeige andererseits, dass M kein freier R-Modul ist.

Bonusaufgabe. Man zeige, dass auch der R-Modul $N = R \oplus M$ nicht frei ist, indem man einen Isomorphismus

$$M \;\simeq\; \wedge^2 N \;=\; N \otimes_R N \,/\, \big\{ \textstyle\sum_i r_i n_i \otimes n_i \mid n_i \in N, r_i \in R \big\}$$

von M mit der zweiten äußeren Potenz des R-Moduls N findet.

Aufgabe 37. Man zeige mittels Aufgabe 34, dass der Zahlkörper $K = \mathbb{Q}(\sqrt{2}, \sqrt{-6})$ den Ganzheitsring

$$S \;=\; \left\{ \frac{a + b\sqrt{-3} + c\sqrt{2} + d\sqrt{-6}}{2} \;\middle|\; a, b, c, d \in \mathbb{Z},\ a \equiv b \pmod 2, c \equiv d \pmod 2 \right\}$$

besitzt, und folgere aus der Bonusaufgabe, dass S nicht frei über $R = \mathbb{Z}[\sqrt{-6}]$ ist.