Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Arbeitsblatt 9

Aufgaben

Aufgabe 9.1.*

Betrachte die Quadratrestgruppe

$$\mathbb{Q}^\times / \mathbb{Q}^{\times 2} \, ,$$

wobei $\mathbb{Q}^{\times 2}$ die Untergruppe der Quadrate bezeichne. Zeige, dass es zu jeder Restklasse $x \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ einen Repräsentanten aus $\mathbb{Z}$ gibt.

Aufgabe 9.2. Für einen Körper K bezeichnet $K^{\times 2} \subseteq K^\times$ die Untergruppe aller Quadrate. Bestimme für die folgenden Körper die Restklassengruppe

$$K^\times / K^{\times 2} \, .$$

(1) K ist ein endlicher Körper.
(2) $K = \mathbb{R}$.
(3) $K = \mathbb{C}$.
(4) $K = \mathbb{Q}$.

Aufgabe 9.3. Zeige, dass die Konjugation auf $\mathbb{Q}[\sqrt{D}]$ ein Körperautomorphismus und auf A_D ein Ringautomorphismus ist. Zeige, dass der Invariantenring gleich $\mathbb{Q}$ bzw. gleich $\mathbb{Z}$ ist.

Aufgabe 9.4. Es sei R ein quadratischer Zahlbereich. Zeige, dass die 1 Teil einer Ganzheitsbasis von R ist.

Aufgabe 9.5. Bestimme die Konjugation für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.6. Bestimme die Spur für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.7. Bestimme die Norm für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.8.*

Berechne explizit die Diskriminante des quadratischen Zahlbereichs A_{-7}. Stelle die Multiplikationsmatrix bezüglich einer geeigneten Basis für das Element

$$f = \frac{3}{2} + \frac{5}{2}\sqrt{-7}$$

auf und berechne damit die Spur und die Norm von f.

Aufgabe 9.9. Bestimme den (Isomorphietyp des) Ganzheitsringes der quadratischen Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}[X]/\left(X^2 + \frac{3}{2}X - \frac{5}{7}\right).$$

Aufgabe 9.10. Seien D und E zwei verschiedene quadratfreie Zahlen und seien A_D und A_E die zugehörigen quadratischen Zahlbereiche. Zeige

$$A_D \cap A_E = \mathbb{Z}.$$

Aufgabe 9.11.*

Bestimme ein Element aus $\mathbb{Z}[\sqrt{-11}]$, das unter allen Nichteinheiten minimale Norm besitzt. Begründe, dass dieses Element irreduzibel ist.

Aufgabe 9.12. Es sei $D \neq 0, 1$ quadratfrei. Bestimme die Restklassengruppe $A_D/\mathbb{Z}[\sqrt{D}]$.

Aufgabe 9.13. Sei D eine quadratfreie Zahl mit $D = 1 \mod 4$, und sei A_D der zugehörige quadratische Zahlbereich. Man gebe eine Ganzheitsgleichung für $\frac{1+\sqrt{D}}{2}$ über $\mathbb{Z}$ an. Man zeige, dass es keine echten Zwischenringe $\mathbb{Z}[\sqrt{D}] \subset R \subset A_D$ gibt.

Aufgabe 9.14. Es sei $D \neq 0, 1$ eine quadratfreie Zahl, sei $R = \mathbb{Z}[\sqrt{D}]$ und sei A_D der zugehörige Ganzheitsring. Zeige, dass nach Nenneraufnahme an 2 ein Ringisomorphismus

$$R_2 \longrightarrow (A_D)_2$$

vorliegt.

Aufgabe 9.15. Bestimme für die quadratischen Zahlbereiche A_D mit negativem D sämtliche Einheiten.

Aufgabe 9.16.*

Für welche quadratfreien Zahlen mit

$$D = 1 \mod 4$$

ist $\frac{1+\sqrt{D}}{2}$ eine Einheit?

Aufgabe 9.17. Finde ein quadratfreies D derart, dass die natürliche Inklusion

$$\mathbb{Z}[\sqrt{D}] \subseteq A_D$$

die Eigenschaft besitzt, dass es zwei verschiedene Primideale $\mathfrak{q}$ und $\mathfrak{q}'$ in A_D gibt, die beide über dem gleichen Primideal $\mathfrak{p} \subset \mathbb{Z}[\sqrt{D}]$ liegen. Was ist $\mathfrak{p} \cap \mathbb{Z}$?

Aufgabe 9.18.*

Es sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Zeige, dass es für eine Primzahl p die folgenden drei Möglichkeiten:

(1) p ist prim in A_D.
(2) Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}^2$ ist.
(3) Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ mit $\mathfrak{p} \neq \overline{\mathfrak{p}}$ ist.

Aufgabe 9.19. Es sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Zeige, dass für eine ungerade Primzahl p, die kein Teiler von D ist, folgende Aussagen äquivalent sind.

(1) D ist ein Quadrat in $\mathbb{Z}/(p)$.
(2) Es gibt zwei Primideale in A_D oberhalb von (p).

Aufgabe 9.20. Es sei R ein quadratischer Zahlbereich. Zeige, dass es nur endlich viele Primzahlen mit der Eigenschaft gibt, dass der Faserring über $\mathbb{Z}/(p)$ nicht reduziert ist.

Aufgabe 9.21. Es sei R ein quadratischer Zahlbereich. Zeige, dass die Konjugation zu jeder Primzahl p einen $\mathbb{Z}/(p)$-Algebraisomorphismus des Faserringes über p in sich selbst induziert. Beschreibe diesen in den drei möglichen Fällen im Sinne von Aufgabe 5.29 bzw. Aufgabe 9.16.

Aufgabe 9.22. Sei $D \neq 0, 1$ eine quadratfreie Zahl und betrachte die quadratische Erweiterung $\mathbb{Z} \subset \mathbb{Z}[\sqrt{D}]$. Es sei p ein Primfaktor von D und es sei vorausgesetzt, dass weder p noch $-p$ ein Quadratrest modulo D/p ist. Dann ist p irreduzibel in $\mathbb{Z}[\sqrt{D}]$, aber nicht prim.

Aufgabe 9.23. Es sei $R = \mathbb{Z}[\sqrt{7}]$. Bestimme die Primideale in R, die über $p = 29$ liegen und zeige, dass es sich um Hauptideale handelt.

Aufgabe 9.24. Es sei $R = \mathbb{Z}[\sqrt{15}]$. Bestimme die Primideale in R, die über $p = 17$ liegen (man gebe Idealerzeuger an). Handelt es sich um Hauptideale?

Aufgabe 9.25. Zeige, dass 2 im Ring $\mathbb{Z}[\sqrt{5}]$ irreduzibel, aber nicht prim ist. Wie sieht es in A_5 aus?

Aufgabe 9.26.*

Es sei p ein ungerade Primzahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.
(2) p ist die Norm eines Elementes aus $\mathbb{Z}[\mathrm{i}]$.
(3) p ist zerlegbar (nicht prim) in $\mathbb{Z}[\mathrm{i}]$.
(4) -1 ist ein Quadrat in $\mathbb{Z}/(p)$.
(5) Es ist $p = 1 \mod 4$.

Aufgabe 9.27.*

Es sei n eine positive natürliche Zahl. Wir schreiben $n = r^2 m$, wobei jeder Primfaktor von m nur einfach vorkomme. Zeige, dass dann n genau dann die Summe von zwei Quadraten ist, wenn in der Primfaktorzerlegung von m nur 2 und Primzahlen vorkommen, die modulo 4 den Rest 1 haben.

Aufgabe 9.28.*

Zeige, dass -3 genau dann ein Quadratrest modulo einer Primzahl $p \neq 2$ ist, wenn $p = 0, 1 \mod 3$ ist.

Aufgabe 9.29. Es sei $\mathbb{Z}[\omega]$ der Ring der Eisenstein-Zahlen und p eine ungerade Primzahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) Es gibt eine Darstellung $p = x^2 + xy + y^2$ mit $x, y \in \mathbb{Z}$.
(2) p ist die Norm eines Elementes aus $\mathbb{Z}[\omega]$.
(3) p ist zerlegbar (nicht prim) in $\mathbb{Z}[\omega]$.

(4) -3 ist ein Quadrat in $\mathbb{Z}/(p)$.
(5) Es ist $p = 0, 1 \mod 3$.

AUFGABE 9.30. Es sei D eine quadratfreie positive Zahl mit $D = 3 \mod 4$. Zeige, dass der Zahlbereich zur Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}, \sqrt{D}]$ echt größer als $\mathbb{Z}[\mathrm{i}, \sqrt{D}]$ ist.

AUFGABE 9.31.*

Sei R ein noetherscher, kommutativer Ring. Zeige, dass dann auch jeder Restklassenring $R/\mathfrak{a}$ noethersch ist.

AUFGABE 9.32. Zeige: Ein kommutativer Ring R ist noethersch genau dann, wenn es in R keine unendliche echt aufsteigende Idealkette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$$

gibt.

AUFGABE 9.33. Zeige, dass das Produkt $R \times S$ zu noetherschen Ringen R und S wieder noethersch ist.

AUFGABE 9.34. Es sei K ein Körper. Zeige, dass es in $K[X, Y]$ keine obere Schranke für die Anzahl der Erzeuger von Idealen (in einem minimalen Erzeugendensystem) gibt.

Tipp: Betrachte die Potenzen $(X, Y)^m$.

AUFGABE 9.35. Sei R ein noetherscher Integritätsbereich. Zeige, dass sich jedes Element aus R als ein Produkt von irreduziblen Elementen schreiben lässt.

AUFGABE 9.36. Es sei R ein kommutativer Ring und seien $f_1, \ldots, f_n \in R$ Elemente, die das Einheitsideal erzeugen. Es sei vorausgesetzt, dass die Nenneraufnahmen R_{f_i} für $i = 1, \ldots, n$ noethersch sind. Zeige, dass dann auch R noethersch ist.

AUFGABE 9.37. Sei K ein Körper und sei

$$K[X_n, \, n \in \mathbb{N}]$$

der Polynomring über K in unendlich vielen Variablen. Man beschreibe darin ein nicht endlich erzeugtes Ideal und eine unendliche, echt aufsteigende Idealkette.

Aufgabe 9.38. Man gebe ein Beispiel eines nicht-noetherschen Ringes, dessen Reduktion ein Körper ist.

Aufgabe 9.39.*

Zeige, dass ein Unterring $R \subseteq S$ eines noetherschen Ringes nicht noethersch sein muss.

Aufgabe 9.40. Es sei R ein faktorieller Zahlbereich und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung. Zu einer Primzahl p sei

$$p = q_1^{r_1} \cdots q_k^{r_k}$$

die Primfaktorzerlegung von p in R (die q_i seien also paarweise nicht assoziiert). Zeige, dass die Primideale $\mathfrak{p}$ von R mit der Eigenschaft $\mathfrak{p} \cap \mathbb{Z} = (p)$ genau die Primideale der Form $\mathfrak{p} = (q_i)$ sind.

Aufgabe 9.41. Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ verschiedene Primideale $\neq 0$. Dann gibt es einen Ringisomorphismus

$$R/\mathfrak{p} \cap \mathfrak{q} \longrightarrow R/\mathfrak{p} \times R/\mathfrak{q}.$$

Aufgabe 9.42. Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene Primideale. Dann ist

$$\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}.$$

Aufgabe 9.43. Man gebe ein Beispiel für einen Dedekindbereich, wo jeder Restklassenring $\neq 0$ unendlich ist, und für einen Dedekindbereich, der einen Körper enthält und wo alle echten Restklassenringe endlich sind.

Abbildungsverzeichnis