

Lösungsblatt 11 zur Zahlentheorie

**Aufgabe 1.**

- (a) Wir zeigen zunächst, dass ein  $t \in \mathbb{N}$  existiert mit  $tG \subseteq \mathcal{O}_K$ . Ist  $x \in G$ , so gibt es  $a_1, \dots, a_r \in \mathbb{Z}$  mit  $a_1 > 0$  und

$$a_1 x^r + \dots + a_{r-1} x + a_1^{r-1} a_r = 0.$$

Multiplikation mit  $(a_1)^{r-1}$  liefert eine Ganzheitsgleichung

$$(a_1 x)^r + \dots + a_{r-1} a_1^{r-2} (a_1 x) + a_1 a_r = 0$$

für  $a_1 x$ . Daher ist  $a_1 x \in \mathcal{O}_K$ . Insbesondere gibt es  $t_1, \dots, t_n \in \mathbb{N}$  mit  $t_i x_i \in \mathcal{O}_K$  für  $i = 1, \dots, n$ . Für  $t := t_1 \cdots t_n$  erhält man  $tG \subseteq \mathcal{O}_K$ . Da  $x_1, \dots, x_n$  linear unabhängig über  $\mathbb{Z}$  sind, sind diese auch über  $\mathbb{Q}$  linear unabhängig. Daher ist  $x_1, \dots, x_n$  auch eine  $\mathbb{Q}$ -Basis von  $K$ . Ist  $y_1, \dots, y_n$  eine  $\mathbb{Z}$ -Basis von  $\mathcal{O}_K$ , so gibt es  $\alpha_{ij} \in \mathbb{Q}$  mit

$$y_i = \sum_{j=1}^n \alpha_{ij} x_j,$$

für  $1 \leq i \leq n$ . Multipliziert man jeweils mit dem Hauptnenner folgt die Existenz eines  $u_i \in \mathbb{N}$  mit  $u_i y_i \in G$ . Setzt man  $u := u_1 \cdots u_n$  so ist  $u\mathcal{O}_K \subseteq G$ . Die natürliche Zahl  $s := ut$  erfüllt demnach  $s\mathcal{O}_K \subseteq G$  und  $sG \subseteq \mathcal{O}_K$ .

- (b) Sei  $z_1, \dots, z_n$  eine weitere Basis von  $G$ . Dann gibt es  $s_{ij} \in \mathbb{Z}$  mit  $1 \leq i, j \leq n$  mit

$$x_i = \sum_{j=1}^n s_{ij} y_j.$$

Bezeichne  $S$  die Matrix mit den Einträgen  $s_{ij}$ , dann ist  $\det(S) = \pm 1$ . Für  $1 \leq k, l \leq n$  folgt

$$\begin{aligned} \operatorname{tr}_{K|\mathbb{Q}}(x_l x_k) &= \operatorname{tr}_{K|\mathbb{Q}} \left( \sum_{j=1}^n s_{lj} y_j \sum_{i=1}^n s_{ki} y_i \right) \\ &= \operatorname{tr}_{K|\mathbb{Q}} \left( \sum_{j=1}^n \sum_{i=1}^n s_{lj} s_{ki} y_j y_i \right) \\ &= \sum_{j=1}^n \sum_{i=1}^n s_{lj} s_{ki} \operatorname{tr}_{K|\mathbb{Q}}(y_j y_i). \end{aligned}$$

Daher ist

$$\det \begin{pmatrix} \operatorname{tr}_{K|\mathbb{Q}}(x_1 x_1) & \cdots & \operatorname{tr}_{K|\mathbb{Q}}(x_1 x_n) \\ \vdots & \ddots & \vdots \\ \operatorname{tr}_{K|\mathbb{Q}}(x_n x_1) & \cdots & \operatorname{tr}_{K|\mathbb{Q}}(x_n x_n) \end{pmatrix} = \det \left( S \cdot \begin{pmatrix} \operatorname{tr}_{K|\mathbb{Q}}(y_1 y_1) & \cdots & \operatorname{tr}_{K|\mathbb{Q}}(y_1 y_n) \\ \vdots & \ddots & \vdots \\ \operatorname{tr}_{K|\mathbb{Q}}(y_n y_1) & \cdots & \operatorname{tr}_{K|\mathbb{Q}}(y_n y_n) \end{pmatrix} \cdot S^T \right).$$

Also  $d_{K|\mathbb{Q}}(x_1, \dots, x_n) = \det(S)^2 d_{K|\mathbb{Q}}(y_1, \dots, y_n)$ . Wegen  $\det(S)^2 = 1$  ist  $d(G)$  unabhängig von der Wahl der Basis von  $G$ .

(c) Sei  $u_1, \dots, u_n$  eine Basis von  $H$  und  $\alpha_{ij} \in \mathbb{Z}$  mit

$$u_i = \sum_{j=1}^n \alpha_{ij} x_j$$

für  $i = 1, \dots, n$ . Eine analoge Rechnung wie in Teil (b.) zeigt

$$d(H) = \det(A)^2 d(G).$$

Auf der anderen Seite ist  $G/H \cong G/\text{im}(A)$  und daher  $|G/H| = \det(A)$  (vgl. Aufgabe 1 auf Blatt 9). Dies zeigt die Behauptung.

### Aufgabe 2.

(a) Da  $R$  insbesondere ein  $\mathbb{Z}$ -Untermodul des freien  $\mathbb{Z}$ -Moduls  $\mathcal{O}_K$  ist, ist auch  $R$  selbst ein freier  $\mathbb{Z}$ -Modul vom Rang  $k \leq n$ . Sei daher  $y_1, \dots, y_k$  eine  $\mathbb{Z}$ -Basis von  $R$ . Da die  $y_1, \dots, y_k$  linear unabhängig über  $\mathbb{Z}$  sind, sind sie auch über  $\mathbb{Q}$  linear unabhängig. Sei  $V$  der  $\mathbb{Q}$ -Vektorraum aufgespannt von  $y_1, \dots, y_k$ . Wegen  $y_i y_j \in R \subseteq V$  für  $1 \leq i, j \leq k$ , ist  $V$  ein Zwischenring von  $\mathbb{Q} \subsetneq R \subseteq K$ . Da jeder Zwischenring einer algebraischen Körpererweiterung selbst ein Körper ist, ist auch  $V$  ein Körper. Schließlich folgt aus  $R \subseteq V$  auch  $K = \text{qf}(R) \subseteq V$  und daher  $V = K$ . Es ist also  $k = \dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}} K = n$ . Dies zeigt, dass  $R$  ein freier  $\mathbb{Z}$ -Modul vom Rang  $n$  ist.

(b) Aus Aufgabe 1 folgt  $[\mathcal{O}_K : R]^2 d(\mathcal{O}_K) = d(R)$ . Nach Voraussetzung gibt es keine Primzahl  $p$ , für die  $p^2 \mid d(R)$  gilt. Daher gibt es auch keine Primzahl  $p$  mit  $p \mid [\mathcal{O}_K : R]$ . Dies ist nur möglich, wenn  $[\mathcal{O}_K : R] = 1$  gilt, also  $\mathcal{O}_K = R$  ist. (Man beachte, dass man verwendet, dass  $[\mathcal{O}_K : R]$  endlich ist, was ebenfalls in Aufgabe 1 gezeigt wurde).

### Aufgabe 3.

(a) Können wir zeigen, dass das Polynom  $f(X) = X^3 - X + 3$  irreduzibel ist, so folgt, dass  $[K : \mathbb{Q}] = 3$ . Betrachten wir  $f$  in  $\mathbb{Z}/(2)$  so ist  $\bar{f} = X^3 + X + 1$  und es ist  $\bar{f}(0) = 1$  und  $\bar{f}(1) = 1$ , was zeigt, dass  $\bar{f}$  keine Nullstellen in  $\mathbb{F}_2$  hat und daher wegen  $\deg(\bar{f}) = 3$  irreduzibel ist. Nach dem Reduktionskriterium ist somit auch  $f$  irreduzibel über  $\mathbb{Q}$  und wir haben  $[K : \mathbb{Q}] = 3$ .

(b) Eine beliebige Vermutung ist, dass  $\mathcal{O}_K = \mathbb{Z}[z]$ . Dies soll im Folgenden gezeigt werden. Wir setzen  $R := \mathbb{Z}[z]$ . Offensichtlich ist  $z \in K$  ganz über  $\mathbb{Z}$  und daher ist  $R \subseteq \mathcal{O}_K$ ; desweiteren ist  $\text{qf}(R) = K$ . Kann man schließlich noch zeigen, dass kein Primzahlquadrat die Diskriminante von  $R$  teilt, dann sind alle Voraussetzungen aus Aufgabe 2.(b) erfüllt und es ist in der Tat  $\mathcal{O}_K = R$ . Zu bestimmen ist also noch  $d(R)$ . Wegen  $z^3 = z - 3$  ist  $R = \mathbb{Z} \oplus z\mathbb{Z} \oplus z^2\mathbb{Z}$ . Daher genügt es, die Spuren von  $z^k$  für  $k = 0, \dots, 4$  zu berechnen. Es ist  $\text{tr}(1) = [K : \mathbb{Q}] = 3$  und  $\text{tr}(z) = 0$ . Wegen  $z^2 \cdot z = z^3 = z - 3$  und  $z^2 \cdot z^2 = z^4 = z^2 - 3z$  ist

$$\begin{pmatrix} 0 & -3 & 0 \\ 0 & 1 & -3 \\ 1 & 0 & 1 \end{pmatrix}$$

eine Darstellungsmatrix der Linksmultiplikation mit  $z^2$ . Daher ist  $\text{tr}(z^2) = 2$ . Weiter folgt  $\text{tr}(z^3) = \text{tr}(z - 3) = -9$ . und  $\text{tr}(z^4) = \text{tr}(z^2 - 3z) = \text{tr}(z^2) = 2$ . Daher ist

$$d(R) = \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & -9 \\ 2 & -9 & 2 \end{pmatrix} = (-13) \cdot 19,$$

woraus die Behauptung folgt.