

# EINFÜHRUNG IN DIE ALGEBRA

## BLATT 10

Jendrik Stelzner

8. Januar 2014

### Aufgabe 10.2.

**Bemerkung 1.** Sei  $p \in \mathbb{N}$  eine Primzahl und  $k \in \mathbb{N}, k \geq 1$ . Dann gibt es in  $\mathbb{Z}/p^k\mathbb{Z}$  genau  $p$  Elemente  $g \in \mathbb{Z}/p^k\mathbb{Z}$  mit  $pg = 0$ .

*Beweis.* Es bezeichne  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/p^k\mathbb{Z}$  die kanonische Projektion und  $\bar{n} = \pi(n)$  für alle  $n \in \mathbb{Z}$ . Für alle  $n \in \mathbb{Z}$  ist

$$\begin{aligned} p \cdot \bar{n} = 0 &\Leftrightarrow \overline{np} = 0 \Leftrightarrow np \in \text{Ker } \pi = p^k\mathbb{Z} \Leftrightarrow n \in p^{k-1}\mathbb{Z} \\ &\Leftrightarrow \bar{n} \in \{0, \overline{p^{k-1}}, \dots, \overline{(p-1)p^{k-1}}\}. \end{aligned}$$

□

**Bemerkung 2.** Seien  $G_1, \dots, G_n$  Gruppen. Für  $(g_1, \dots, g_n) \in G_1 \times \dots \times G_n$  ist

$$\text{ord}(g_1, \dots, g_n) = \text{kgV}(\text{ord } g_1, \dots, \text{ord } g_n).$$

*Beweis.* Wir schreiben  $k = \text{kgV}(\text{ord } g_1, \dots, \text{ord } g_n)$  und  $l = \text{ord}(g_1, \dots, g_n)$ . Es ist offenbar

$$(g_1, \dots, g_n)^k = (g_1^k, \dots, g_n^k) = (0, \dots, 0),$$

also  $l \mid k$ . Da

$$(0, \dots, 0) = (g_1, \dots, g_n)^l = (g_1^l, \dots, g_n^l)$$

ist  $\text{ord } g_i \mid l$  für alle  $i = 1, \dots, n$ , also auch  $k \mid l$ . □

Es bezeichne  $P \subsetneq \mathbb{N}$  die Menge der Primzahlen. Sei  $G$  eine abelsche Gruppe mit  $\text{ord } G = 15625 = 5^6$ . Aus dem Hauptsatz über endlich erzeugte abelsche Gruppen folgt, dass

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{p \in P} \bigoplus_{n \geq 1} (\mathbb{Z}/p^n\mathbb{Z})^{\nu(p,n)},$$

wobei die  $\nu(p, n)$  eindeutig bestimmt sind und  $\nu(p, n) = 0$  für fast alle  $(p, n) \in P \times (\mathbb{N} \setminus \{0\})$ . Da  $G$  endlich ist, ist in diesem Fall  $d = 0$ , und da  $\text{ord } G = 5^6$  ist  $\nu(p, n) = 0$  für alle  $p \in P, p \neq 5$ , und  $\sum_{n \geq 1} n \cdot \nu(5, n) = 6$ . Übersichtlich ausgedrückt ist also

$$G \cong (\mathbb{Z}/5\mathbb{Z})^{\nu_1} \times \dots \times (\mathbb{Z}/5^6\mathbb{Z})^{\nu_6}$$

mit eindeutig bestimmten  $\nu_1, \dots, \nu_6 \in \mathbb{N}$  und  $\nu_1 + 2\nu_2 + \dots + 6\nu_6 = 6$ . Da wir nur die Zahl der Isomorphieklassen ermitteln wollen, können wir im Folgenden o.B.d.A. davon ausgehen, dass  $G$  von der obigen Form ist. Für

$$(g_1, \dots, g_n) \in (\mathbb{Z}/5\mathbb{Z})^{\nu_1} \times \dots \times (\mathbb{Z}/5^6\mathbb{Z})^{\nu_6}$$

ist wegen Bemerkung 2 genau dann

$$5 = \text{ord}(g_1, \dots, g_n) = \text{kgV}(\text{ord } g_1, \dots, \text{ord } g_n),$$

wenn  $\text{ord } g_1, \dots, \text{ord } g_n \in \{1, 5\}$  und  $\text{ord } g_i = 5$  für (mindestens) ein  $i \in \{1, \dots, n\}$ . (Denn man bemerke, dass  $\text{ord } g_i = 5^k$  für ein  $k \in \mathbb{N}$  für alle  $i = 1, \dots, n$ .) Da es genau 124 Elemente der Ordnung 5 in  $G$  gibt, gibt es genau  $125 = 5^3$  Elemente der Ordnung 1 oder 5 in  $G$ ; dies sind genau die Element  $(g_1, \dots, g_n) \in G$  mit  $\text{ord } g_i \in \{1, 5\}$  für alle  $i = 1, \dots, n$ . Aus Bemerkung 2 folgt damit, dass

$$G = \mathbb{Z}/5^{\mu_1}\mathbb{Z} \times \mathbb{Z}/5^{\mu_2}\mathbb{Z} \times \mathbb{Z}/5^{\mu_3}\mathbb{Z},$$

mit  $\mu_1, \mu_2, \mu_3 \geq 1$  und  $\mu_1 + \mu_2 + \mu_3 = 6$ . Die Isomorphieklassen dieser Gruppen entsprechen offenbar gerade den Partitionen von 6 in drei natürliche, positive Zahlen. Diese sind  $(1, 1, 4)$ ,  $(1, 2, 3)$  und  $(2, 2, 2)$ , d.h.  $G$  ist isomorph zu einer der drei Gruppen

$$(\mathbb{Z}/5\mathbb{Z})^2 \times \mathbb{Z}/5^4\mathbb{Z} \text{ oder } \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5^3\mathbb{Z} \text{ oder } (\mathbb{Z}/2\mathbb{Z})^3,$$

die zueinander paarweise nicht isomorph sind. Offenbar erfüllt auch jede dieser drei Gruppen die geforderten Bedingungen. Also gibt es genau drei Isomorphieklassen.

### Aufgabe 10.3.

(i)

Es ist  $\text{char } K = p$ : Ist  $P \cong \mathbb{F}_q$  der Primkörper von  $K$ , so besitzt  $K$  als endlichdimensionaler  $P$ -Vektorraum genau  $q^m$ ,  $m \geq 1$ , Elemente. Wegen  $p^n = q^m$  muss  $p = q$  und  $n = m$ . Also ist  $P \cong \mathbb{F}_p$  und daher  $\text{char } K = \text{char } P = p$ .

Da  $\text{char } K = p$  ist für alle  $\alpha, \beta \in K$

$$\sigma(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \sigma(\alpha) + \sigma(\beta).$$

Auch ist  $\sigma(1) = 1^p = 1$  und

$$\sigma(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \sigma(\alpha)\sigma(\beta).$$

Also ist  $\sigma$  ein Ringendomorphismus. Da  $K$  ein Körper ist, ist  $\sigma : K \rightarrow K$  injektiv. Da  $K$  endlich ist, ist  $\sigma$  damit auch surjektiv. Also ist  $\sigma$  ein Körperautomorphismus.

(ii)

Da  $K$  genau  $p^n$  Elemente hat, ist  $\alpha^{(p^n)} = \alpha$  für alle  $\alpha \in K$  (denn  $K^*$  hat  $p^n - 1$  Elemente, und 0 ist ein Fixpunkt von  $\sigma$ ). Es ist also  $\sigma^n = \text{id}_K$  und daher  $\text{ord } \sigma \mid n$ . Für  $t \geq 1$  mit

$$\alpha = \sigma^t(\alpha) = \alpha^{(p^t)} \text{ für alle } \alpha \in K$$

ist jedes  $\alpha \in K$  eine Nullstelle des Polynoms  $X^{(p^t)} - 1 \in K[X]$ , weshalb

$$p^n \geq \deg(X^{(p^t)} - 1) = p^t,$$

also  $n \geq t$ . Insbesondere ist  $n \geq \text{ord } \sigma$ . Also ist  $\text{ord } \sigma = n$ .

## Aufgabe 10.4.

Für einen beliebigen Körper  $K$  und beliebiges  $g \in K[X]$  mit  $\deg g \geq 1$  gilt, da  $K[X]$  ein Hauptidealring ist, bekanntermaßen

$$K[X]/(g) \text{ ist ein Körper} \Leftrightarrow (g) \text{ ist maximal} \Leftrightarrow g \text{ ist irreduzibel.}$$

Da das Polynom  $f = X^3 - 2$  irreduzibel in  $\mathbb{Q}[X]$  ist, nicht jedoch in  $\mathbb{R}[X]$ , ist  $\mathbb{Q}[X]/(f)$  ein Körper,  $\mathbb{R}[X]/(f)$  jedoch nicht.

## Aufgabe 10.5.

(i)

Da  $\alpha$  und  $\beta$  algebraisch über  $K$  sind, ist die Körpererweiterung  $K(\alpha, \beta)/K$  algebraisch und  $K(\alpha, \beta) = K[\alpha, \beta]$ . Insbesondere ist daher  $(\alpha^k \beta^l)_{k,l \in \mathbb{N}}$  ein  $K$ -Erzeugendensystem von  $K(\alpha, \beta)$ .

Sei nun  $x_1, \dots, x_m \in K(\alpha)$  eine  $K$ -Basis von  $K(\alpha)$  und  $y_1, \dots, y_n \in K(\beta)$  eine  $K$ -Basis von  $K(\beta)$ . Es ist  $(x_i y_j)_{i=1, \dots, m, j=1, \dots, n}$  ein  $K$ -Erzeugendensystem von  $K(\alpha, \beta)$ , und damit insbesondere

$$K[(\alpha, \beta) : K] = \dim_K(K(\alpha, \beta)) \leq mn$$

Für alle  $k, l \in \mathbb{N}$  gibt es nämlich (eindeutige)  $\lambda_1^k, \dots, \lambda_m^k \in K$  mit  $\alpha^k = \sum_{i=1}^m \lambda_i^k x_i$  und  $\mu_1^l, \dots, \mu_n^l \in K$  mit  $\beta^l = \sum_{j=1}^n \mu_j^l y_j$ , weshalb

$$\alpha^k \beta^l = \left( \sum_{i=1}^m \lambda_i^k x_i \right) \left( \sum_{j=1}^n \mu_j^l y_j \right) = \sum_{i=1}^m \sum_{j=1}^n \lambda_i^k \mu_j^l x_i y_j.$$

da  $(\alpha^k \beta^l)_{k,l \in \mathbb{N}}$  ein  $K$ -Erzeugendensystem von  $K(\alpha, \beta)$  ist, ist es daher auch  $(x_i y_j)_{i,j}$ .

(ii)

Aus der Kette von Körpererweiterungen

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$$

ergibt sich durch den Gradsatz, dass

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K],$$

also

$$m = [K(\alpha) : K] \mid [K(\alpha, \beta) : K]$$

Analog ergibt sich, dass auch  $n \mid [K(\alpha, \beta) : K]$ . Folglich ist auch

$$\text{kgV}(m, n) \mid [K(\alpha, \beta) : K].$$

Dabei ist  $\text{kgV}(m, n) = mn$ , da  $m$  und  $n$  teilerfremd sind. Mit  $[K(\alpha, \beta) : K] \geq 1$  ergibt sich damit, dass  $mn \leq [K(\alpha, \beta) : K]$ . Da auch  $[K(\alpha, \beta) : K] \leq mn$  ist also

$$[K(\alpha, \beta) : K] = mn.$$