5. Teil: Körper

20. Endliche Untergruppen der multiplikativen Gruppe eines Körpers

Lemma 188: Es sei G eine abelsche Gruppe und $a, b \in G$ mögen endliche Ordnung besitzen. Sind $\operatorname{ord}(a)$ und $\operatorname{ord}(b)$ relativ prim, so besitzt auch ab endliche Ordnung und $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b)$.

Beweis: Es bezeichne $m = \operatorname{ord}(a)$, $n = \operatorname{ord}(b)$ und $k = \operatorname{ord}(ab)$. Es ist

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e.$$

Daher besitzt ab endliche Ordnung und aus Satz 15 (iii) folgt $k \mid mn$. Umgekehrt ist

$$e = e^m = \big((ab)^k\big)^m = (a^m)^k b^{km} = e^k b^{km} = b^{km}$$

und wieder nach Satz 15 (iii) gilt $n \mid km$. Da $\operatorname{ggT}(m, n) = 1$ folgt $n \mid k$. Völlig analog zeigt man $m \mid k$. Daraus folgt $\operatorname{kgV}(m, n) \mid k$, d.h. $mn \mid k$. Daher ist

$$\operatorname{ord}(ab) = k = mn = \operatorname{ord}(a) \cdot \operatorname{ord}(b).$$

Bemerkung: Ohne die Voraussetzung, dass G abelsch ist, wäre Lemma 188 nicht richtig. Das haben wir in Übungsbeispiel 30a) gesehen.

Korollar 189: Es sei G eine abelsche Gruppe und $a_1, \dots, a_n \in G$ mögen endliche Ordnung besitzen. Sind $\operatorname{ord}(a_1), \dots, \operatorname{ord}(a_n)$ paarweise relativ prim, so besitzt auch $a_1 \cdots a_n$ endliche Ordnung und $\operatorname{ord}(a_1 \cdots a_n) = \operatorname{ord}(a_1) \cdots \operatorname{ord}(a_n)$.

Beweis: Wir verwenden Induktion nach n. Für $n = 1$ ist die Behauptung trivial und der Fall $n = 2$ wurde in Lemma 188 bewiesen. Nach der Induktionsvoraussetzung ist

$$\operatorname{ggT}\big(\operatorname{ord}(a_1 \cdots a_n), \operatorname{ord}(a_{n+1})\big) \overset{\text{IV}}{=} \operatorname{ggT}\big(\operatorname{ord}(a_1) \cdots \operatorname{ord}(a_n), \operatorname{ord}(a_{n+1})\big) = 1$$

da $\operatorname{ord}(a_1), \dots, \operatorname{ord}(a_{n+1})$ paarweise relativ prim sind und daher wegen Lemma 188

$$\begin{aligned} \operatorname{ord}(a_1 \cdots a_{n+1}) &= \operatorname{ord}\big((a_1 \cdots a_n) a_{n+1}\big) = \operatorname{ord}(a_1 \cdots a_n) \cdot \operatorname{ord}(a_{n+1}) \\ &\overset{\text{IV}}{=} \operatorname{ord}(a_1) \cdots \operatorname{ord}(a_n) \operatorname{ord}(a_{n+1}). \end{aligned}$$

Satz 190: Es sei K ein Körper und G eine endliche Untergruppe von $(K^*, \cdot) = (K \setminus \{0\}, \cdot)$. Dann ist G eine zyklische Gruppe.

Beweis: Die Ordnung $|G|$ habe Primfaktorzerlegung $|G| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, d.h. $p_1, \dots, p_n$ sind paarweise verschiedene Primzahlen und $\alpha_1, \dots, \alpha_n \in \mathbb{N} \setminus \{0\}$.

Wir zeigen zunächst: Ist $p \in \{p_1, \dots, p_n\}$ und P eine p-Sylowgruppe von G, so ist P zyklisch. Ist also $p = p_i$ (für ein $i \in \{1, \dots, n\}$), so bezeichne $\alpha = \alpha_i$, d.h. $|P| = p^\alpha$. Wegen Satz 103 gibt es $\beta_1, \dots, \beta_k \in \mathbb{N} \setminus \{0\}$ mit den Eigenschaften $\beta_1 + \cdots + \beta_k = \alpha$ und

$$(P, \cdot) \cong \left(\mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_k}}, +\right).$$

Offensichtlich ist $\max\{\operatorname{ord}(a) \mid a \in P\} = p^\beta$, wobei $\beta = \max\{\beta_1, \dots, \beta_k\}$ und daher $a^{p^\beta} = 1 (\in K)$ für alle $a \in P$. Daher sind alle $a \in P$ Nullstelle des Polynoms

$$f(X) = X^{p^\beta} - 1 \in K[X].$$

Wäre $k > 1$, so wäre $\alpha > \beta$ und f hätte $p^\alpha > p^\beta = \operatorname{grad} f$ verschiedene Nullstellen, was Satz 168 (ii) widersprechen würde. Also ist $k = 1$, $\alpha = \beta_1$ und daher $(P, \cdot) \cong (\mathbb{Z}_{p^\alpha}, +)$.
Es bezeichne nun P_i die p_i-Sylowgruppe von G (für $1 \le i \le n$). (Da G abelsch ist, ist jede Untergruppe von G Normalteiler von G und wegen Korollar 119 (ii) gibt es genau eine p_i-Sylowgruppe in G.) Da P_i zyklisch ist, gibt es ein $a_i \in P_i$ mit der Eigenschaft $\langle a_i \rangle = P_i$, d.h. $\operatorname{ord}(a_i) = |P_i| = p_i^{\alpha_i}$ (für $1 \le i \le n$). Aus Korollar 189 folgt nun

$$\operatorname{ord}(a_1 \cdots a_n) = \operatorname{ord}(a_1) \cdots \operatorname{ord}(a_n) = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = |G|,$$

woran man sofort erkennt, dass G zyklisch ist.

Korollar 191: Es sei K ein endlicher Körper. Dann ist $(K^*, \cdot) = (K \setminus \{0\}, \cdot)$ eine zyklische Gruppe.

Beweis: Folgt sofort aus Satz 190.

Beispiel: Ist p eine Primzahl, so ist $(\mathbb{Z}_p^*, \cdot)$ eine zyklische Gruppe der Ordnung $|\mathbb{Z}_p^*| = p - 1$ (deren Erzeuger Primitivwurzeln genannt werden).