

Körper- und Galoistheorie

Anhang 4

SATZ 4.1. *Sei G eine endlich erzeugte kommutative Gruppe. Dann ist G das Produkt von zyklischen Gruppen. D.h. es gibt eine Isomorphie*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_s).$$

Beweis. Für einen Beweis siehe Storch/Wiebe, Lineare Algebra, 8.C.12. □

KOROLLAR 4.2. *Sei G eine endliche kommutative Gruppe. Dann ist G das Produkt von endlichen zyklischen Gruppen. D.h. es gibt eine Isomorphie*

$$G \cong \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_s).$$

Beweis. Dies folgt direkt aus Satz Anhang 4.1. □

In diesem Zusammenhang sollte auch der chinesische Restsatz erwähnt werden, der eine weitere Produktzerlegung der zyklischen Gruppen erlaubt, wenn die Primfaktorzerlegung bekannt ist.

SATZ 4.3. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(p_i^{r_i})$ einen Isomorphismus*

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k}).$$

Zu einer gegebenen ganzen Zahl (a_1, a_2, \dots, a_k) gibt es also genau eine natürliche Zahl $a < n$, die die simultanen Kongruenzen

$$a = a_1 \pmod{p_1^{r_1}}, \quad a = a_2 \pmod{p_2^{r_2}}, \quad \dots, \quad a = a_k \pmod{p_k^{r_k}}$$

löst.

Beweis. Da die Ringe links und rechts beide endlich sind und die gleiche Anzahl von Elementen haben, nämlich n , genügt es, die Injektivität zu zeigen. Sei x eine natürliche Zahl, die im Produktring (rechts) zu null wird, also modulo $p_i^{r_i}$ den Rest null hat für alle $i = 1, 2, \dots, k$. Dann ist x ein Vielfaches von $p_i^{r_i}$ für alle $i = 1, 2, \dots, k$, d.h. in der Primfaktorzerlegung von x muss p_i zumindest mit Exponent r_i vorkommen. Also muss x

ein Vielfaches des Produktes sein muss, also ein Vielfaches von n . Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv. □

Für die Einheitengruppe ergibt dies das folgende Korollar.

KOROLLAR 4.4. Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann gibt es einen kanonischen Gruppenisomorphismus

$$(\mathbb{Z}/(n))^\times \cong (\mathbb{Z}/(p_1^{r_1}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times.$$

Insbesondere ist eine Zahl a genau dann eine Einheit modulo n , wenn sie eine Einheit modulo $p_i^{r_i}$ ist für $i = 1, \dots, k$.