14. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller

WS 2016/2017: 13. Dezember 2016

Definition

(1) G ist eine Gruppe mit $x \in G$.

$$|x| := \begin{cases} \text{kleinste } n \in \mathbb{N} \text{ mit } x^n = 1 \text{ falls vorhanden} \\ \infty \qquad \text{sonst} \end{cases}$$

$|x|$ ist die *Ordnung von x*, per Konvention $|x^0| = 1$.

(2) H ist *zykisch*, wenn ein $x \in H$ existiert mit

$$H =< x >:= \{x^n \mid n \in \mathbb{Z}\}$$

und x heißt *Erzeuger* der Gruppe H (additiv $H =< x >= \{nx \mid n \in \mathbb{Z}\}$).

Bemerkung

Eine zyklische Gruppe ist abelsch.

Proposition 1

$H =< x >\Rightarrow |x| = |H|$, das heißt

(1) $|H| = n < \infty$ für $n \in \mathbb{N}_0 \Leftrightarrow x^n = 1$ und $x^i \neq x^j$ für $i \neq j; i, j \in \{0, \ldots, n-1\}$

(2) $|H| = \infty$ genau dann, wenn $x^i \neq x^j$ für alle $i, j \in \mathbb{N}_0$ mit $i \neq j$.

Beweis

(1) $|x| = n < \infty$, wenn $x^i = x^j$ mit $0 \leq i < j < n \Rightarrow x^{j-i} = 1$ mit $0 < j - i < n$ - Widerspruch.
Sei $x^k \in< x >; k = qn + r$ mit $0 \leq r < n$, also $x^k = x^{nq+r} = (x^n)^q x^r = x^r$.

(2) $|x| = \infty$ und $x^i = x^j$ mit $i \neq j \Rightarrow x^{j-i} = 1$. Also $|x| \leq j - i$ - Widerspruch. □

Proposition 2

Sei G eine Gruppe mit $x \in G$ und $m, n \in \mathbb{Z}$. Es gelten $x^n = 1$ und $x^m = 1 \Rightarrow x^d = 1$ für $d =$ ggT (m, n). Insbesondere $x^m = 1$ mit $m \in \mathbb{Z} \Rightarrow |x| | m$.

Beweis

$d = mr + ns$. Also $x^d = (x^m)^r (x^n)^s = 1$. Sei nun $x^m = 1$. Setze $|x| = n$. Schreibe $m = qn + r$ mit $0 \leq r < n$. $x^m = (x^n)^q x^r \Rightarrow x^r = 1$ - Widerspruch. Also $r = 0$. □

Proposition 3
Zyklische Gruppen derselben Ordnung sind isomorph.

Beweis

(1) Sei $|G| = |H| = n, G =< x >$ und $H =< y >$. Betrachte

$$\begin{array}{rccc} \varphi: & G & \to & H \\ & x^k & \mapsto & y^k \end{array}$$

φ ist wohldefiniert, weil $x^r = x^s \Rightarrow x^{r-s} = 1 \Rightarrow n|r-s \Rightarrow nt = (r-s)$
$\Rightarrow y^{(r-s)} = (y^n)^t = 1 \Rightarrow y^r y^{-s} = 1 \Rightarrow y^r = y^s$.
Es ist klar, dass φ ein Homomorphismus und auch surjektiv ist. Da beide Gruppen die gleiche Ordnung haben und endlich sind, folgt das φ injektiv ist.
(Eine Abbildung $\varphi : S \to S$ (S ist eine endliche Menge) ist injektiv $\Leftrightarrow$ sie ist surjektiv $\Leftrightarrow$ sie ist bijektiv).

(2) Sei nun $|G| = |H| = \infty$.

$$\begin{array}{rccc} \varphi: & G & \to & H \\ & x^k & \mapsto & y^k \end{array}$$

ist ein surjektiver Homomorphismus und ferner injektiv, weil $x^i \neq x^j \Leftrightarrow i + j \Leftrightarrow y^i \neq y^j$.
$\square$

Beispiel

(1) $|G| = n$ und G ist zyklisch $\Rightarrow G \simeq \mathbb{Z}_n$

(2) $|G| = \infty$ und G ist zyklisch $\Rightarrow G \simeq \mathbb{Z}$

Erzeuger

Proposition 4 (Übungsblatt)
Sei G eine Gruppe mit $x \in G$ und $j \in \mathbb{Z}$ mit $j \neq 0$. Es gelten

(1) $|x| = \infty \Rightarrow |x^j| = \infty$

(2) $|x| = n < \infty \Rightarrow |x^j| = \frac{n}{ggT(n,j)}$

(3) $|x| = n < \infty$ und $j|n \Rightarrow |x^j| = \frac{n}{j}$.

Proposition 5
Sei $H =< x >$ und $j \in \mathbb{N}$.

(1) $|x| = \infty$, dann ist x^j Erzeuger genau dann, wenn $j = \pm 1$

(2) $|x| < \infty$, dann ist x^j Erzeuger genau dann, wenn $|x| = n$ und ggT $(j, n) = 1$.

Beweis

(1) Übungsaufgabe

(2) x^j Erzeuger $\Leftrightarrow |H| = |x^j|$. Also $\Leftrightarrow |x^j| = |x| \Leftrightarrow \frac{n}{ggT(j,n)} = n \Leftrightarrow ggT(j, n) = 1$. $\square$

Korollar 6

$|H| = n; H$ist zyklisch, dann ist die Anzahl der Erzeuger von $H = \phi(n)$ (Euler).

Satz 7

Sei $H =< x >$ zyklisch.

(1) $K \leq H \Rightarrow K$ zyklisch, das heißt $K =< x^d >$ (oder $K = \{1\}$), wobei d die kleinste $d \in \mathbb{N}$ mit $x^d \in K$.

(2) $|H| = \infty \Rightarrow < x^j > \neq < x^i >$ für $i \neq j; i, j \in \mathbb{N}_0$.

(3) $|H| = n < \infty; j \in \mathbb{N}_0; j|n \Rightarrow \exists! K \leq H; K$ zyklisch; $|K| = j$ und $K =< x^{\frac{n}{j}} >$