14 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Kapitel 3

GRUPPEN

In LA I und II haben wir schon Gruppen studiert. Insbesondere haben wir die symmetrische und alternierende Gruppen S_n in Zusammenhang mit Determinanten kennengelernt. In diesem Kapitel, setzen wir das Studium der Gruppentheorie fort, mit Schwerpunkt endliche Gruppen. Die Gruppentheorie die wir entfalten ist für die Grundlagen der Galoistheorie in Kapitel 4 unerlässig. Wir fangen damit an in diesem Skript und studieren Zyklische Gruppen.

§15: Zyklische Gruppen

Definition 14.1.
Sei G eine Gruppe. Eine Untermenge $H \subseteq G$ ist eine *Untergruppe*, oder *Teilgruppe*, falls H (versehen mit der Verknüpfung von G) eine Gruppe ist, das heißt:
$H \neq \varnothing$; und $\forall x, y \in G : x, y \in H \Rightarrow xy \in H$ und $x^{-1} \in H$.

Notation: Sei G eine gruppe, $x \in G$.

1. $< x >:= \{x^k \mid k \in \mathbb{Z}\}$ (additiv geschrieben $< x >:= \{kx \mid k \in \mathbb{Z}\}$) bezeichnet die Untergruppe die von x erzeugt ist.
2. $|G| := \begin{cases} \text{Anzahl} & \text{der Elemente in } G, \text{ falls } G \text{ endlich} \\ \infty & \text{sonst} \end{cases}$

Definition 14.2.

Sei G eine Gruppe und $x \in G$. Die *Ordnung von x*, die wir mit $|x|$ bezeichnen, ist so definiert:

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

Proposition 14.3.
Sei G eine Gruppe, $x \in G$. Es gilt $|x| = |< x >|$.

Beweis:

1. Sei $n \in \mathbb{N}$, und $|x| = n$. Wir behaupten dass $< x >= \{x^i ; i = 0, \dots, n-1\}$ (und damit ist $|< x >| = n$). Wenn $x^i = x^j$ mit $0 \leq i < j < n$, dann $x^{j-i} = 1$ mit $0 < j - i < n$. Widerspruch. Sei nun $k \in \mathbb{Z}$ und $x^k \in < x >$; schreibe $k = qn + r$ mit $0 \leq r < n$. Berechne $x^k = x^{nq+r} = (x^n)^q x^r = x^r$.
   Analog zeigt man dass wenn $|< x >| = n$, dann ist $|x| = n$ (ÜA).

2. Sei nun $|x| = \infty$. Wir behaupten dass $x^i \neq x^j$ für alle $i, j \in \mathbb{Z}$ mit $i \neq j$ (und damit ist $|< x >| = \infty$): wenn $x^i = x^j$ mit $i < j \in \mathbb{Z}$, dann ist $x^{j-i} = 1$, also $|x| \leq j - i$. Widerspruch.
   Analog zeigt man dass wenn $|< x >| = \infty$, dann ist $|x| = \infty$ (ÜA).

□

Proposition 14.4.
Sei G eine Gruppe, $x \in G$ und $m, n \in \mathbb{Z}$, setze $d := \text{ggT}(m, n)$. Es gilt:

$$x^n = 1 \text{ und } x^m = 1 \Rightarrow x^d = 1 .$$

Insbesondere gilt für $m \in \mathbb{Z} : x^m = 1 \Rightarrow |x| \,|\, m$.

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

Definition 14.5.

G ist *zykisch*, wenn ein $x \in G$ existiert mit $G =< x >$, in diesem Fall ist x ein *Erzeuger* der Gruppe G.

Bemerkung 14.6.
Eine zyklische Gruppe ist abelsch. (ÜA)

Definition 14.7.
(*i*) Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ ist ein *Gruppenhomomorphismus*, wenn $\varphi(xy) = \varphi(x)\varphi(y)$ ist für alle $x, y \in G$.
(*ii*) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

Proposition 14.8.
Zyklische Gruppen derselben Ordnung sind isomorph.

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

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

• 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 (ÜA).

(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 $x^i \neq x^j \Leftrightarrow i \neq j \Leftrightarrow y^i \neq y^j$. □

Beispiel 14.9.

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

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

Die folgende Proposition wird im Übungsblatt bearbeitet:

Proposition 14.10. 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 14.11.
Sei $H = < x >$ und $j \in \mathbb{N}$.

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

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

Beweis:

(1) ÜA.

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

Korollar 14.12.
Sei H zyklisch mit $|H| = n$; dann ist die Anzahl der Erzeuger von $H = \phi(n)$ (Euler).