GESAMTSKRIPT

zur Vorlesung ALGEBRA I

Kapitel III

Prof. Dr. Salma Kuhlmann

Wintersemester 2020 - 2021

Inhaltsverzeichnis Kapitel III zur Vorlesung: Algebra 1 (WiSe 2020-2021)

Prof. Dr. Salma Kuhlmann

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 $< x >= \{x^i ; i = 0, \ldots, n-1\}$ (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).

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

Prof. Dr. Salma Kuhlmann

In diesem skript werden wir Abschnitt 15 beenden, indem wir die zyklische Untergruppen studieren. Im Abschnitt 16 werden wir Homomorphismen und Faktorgruppen untersuchen, dabei werden wir normale Untergruppen kennenlernen.

Notation: Seien K, H und G stets Gruppen. Wir schreiben $K \leq H$ für: K ist eine Untergruppe von H.

Satz 15.1.
Sei $H =< x >$ zyklisch

(1) Sei $K \leq H$, dann ist K zyklisch.

(2) Wenn $|H| = \infty$, dann sind $< x^j > \neq < x^i >$ für $i \neq j$ und $\{< x^i > ; \, i \in \mathbb{N}_0\}$ ist die Menge aller Teilgruppen von H.

(3) Wenn $|H| = n$ und $a \in \mathbb{N}$ mit $a \,|\, n$, dann gibt es eine eindeutige Teilgruppe der Ordnung a, nämlich $< x^{n/a} >$. Die Menge aller nicht-trivialen Teilgruppen von H ist $\{< x^d >; d \in \mathbb{N}, d|n\}$.

Beweis:

(1) $K = \{1\}$ ist zyklisch, also ohne Einschränkung $K \neq \{1\}$.
Sei $k \in \mathbb{N}$ die kleinste, so dass $x^k \in K$. Also ist $< x^k > \leq K$.
Sei $x^a \in K; DA \Rightarrow a = qk + r$ mit $0 \leq r < k$ und $x^r = x^a x^{-qk} \in K$.
Da k minimal gewählt ist, muss $r = 0$ sein. Also $a = qk$ und $x^a = (x^k)^q \in < x^k >$.
Also $K \leq < x^k >$.

(2) ÜA.

(3) Sei $d := \frac{n}{a}$, also $d|n$ und $|x^d| = \frac{n}{ggT(n,d)} = n/d = n/(n/a) = a$. Somit ist $| < x^d > | = a$.
Eindeutigkeit: Sei $K \leq H$ mit $|K| = a$ und $b \in \mathbb{N}$ kleinste, so dass $K = < x^b >$. Wir berechnen $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{ggT(n,b)}$. Daraus folgt $d = ggT(n, b)$, insbesondere $d|b$. Also $x^b \in < x^d >$ und $K = < x^b > \leq < x^d >$.
Da aber $|K| = a = | < x^d > |$, folgt nun $K = < x^d >$. □

§16: Faktorgruppen

Proposition 15.2.
Sei $\mathcal{A}$ eine nichtleere Menge von Teilgruppen von H, dann ist $\bigcap \mathcal{A}$ auch eine Teilgruppe.

Beweis:
Setze $K := \bigcap \mathcal{A}; a, b \in K \Rightarrow ab^{-1} \in A$, für alle $A \in \mathcal{A}$ (weil $A \leq H$), also $ab^{-1} \in K$ und damit $K \leq H$. □

Definition 15.3.
Sei $S \subseteq H$ eine Untermenge; $\mathcal{A} := \{K \leq H; S \subseteq K\}$.
Definiere $< S >= \bigcap \mathcal{A}$. Dann ist $< S >$ die (für die Inklusion) kleinste Teilgruppe von H, die S enthält. $< S >$ heißt die *Teilgruppe, die von S erzeugt ist.*
Konvention: $< \varnothing >= \{1\}$
Notation: $S = \{a_1, \ldots, a_n\}; < S >=< a_1, \ldots, a_n >$ (wenn S endlich ist).

Proposition 15.4.
Sei $S \neq \varnothing$. Dann ist $< S >= \{a_1^{\varepsilon_1} \ldots a_n^{\varepsilon_n}; n \in \mathbb{N}; a_i \in S; \varepsilon_i = \pm 1\}$.

Beweis:
Diese Menge ist eine Teilgruppe (ÜA). Sie enthält S und muss in jeder Teilgruppe, die S enthält enthalten sein. □

Der Beweis dieser Proposition ist analog wie für Ringhomomorphismen und wird als ÜA überlassen:

Proposition 15.5.
Sei $\varphi : G \to H$ ein Homomorphismus. Es gelten
(1) $\varphi(1) = 1$
(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$
(3) $\varphi(g^n) = \varphi(g)^n$ für alle $n \in \mathbb{Z}$
(4) $\ker \varphi := \{g \in G; \varphi(g) = 1\} \leq G$
(5) $\text{im } \varphi := \{h \in H; \exists g \in G : \varphi(g) = h\} \leq H$

Wir wollen Faktorengruppen definieren.

Definition 15.6.
Sei $H \leq G$ und $g \in G$. Dann ist $gH := \{gh \mid h \in H\}$ ist die *linke Nebenklasse von g bezüglich H* und $Hg := \{hg \mid h \in H\}$ ist die *rechte Nebenklasse von g bezüglich H.*
Additive Notation: $g + H$ und $H + g$

Proposition 15.7.
Sei $H \leq G$. Es gelten:

(1) Die Menge der linken Nebenklassen bilden eine Partition von G i.e. $G = \bigcup_{g \in G} gH$ und $uH \cap vH \neq \varnothing \Rightarrow uH = vH$.
(2) Für alle $u, v \in G : uH = vH \Leftrightarrow v^{-1}u \in H$.

Beweis:
(1) $1 \in H$, also $g \in gH$ für alle $g \in G$. Also $G = \bigcup gH$. Sei $uH \cap vH \neq \varnothing$. Sei $x \in uH, x \in vH$, also $x = uh_1 = vh_2$ für geeignete $h_1, h_2 \in H$. Also $u = v \underbrace{h_2 h_1^{-1}}_{\in H}$.
Sei $t \in H$. Es gilt also $ut = v(h_2 h_1^{-1})t = v(h_2 h_1^{-1} t) \in vH$, somit $uH \subseteq vH$.
Analog: $uH \supseteq vH$.
(2) $uH = vH$ genau dann, wenn $u \in vH$ genau dann, wenn $u = vh$ für ein $h \in H$ genau dann, wenn $v^{-1}u \in H$. □

Proposition 15.8.
Sei $N \leq G$. Die Verknüpfung

$$(uN)(vN) := (uv)N$$

ist wohldefiniert genau dann, wenn

(*) $$gng^{-1} \in N \text{ für alle } g \in G; \text{ für alle } n \in N$$

Beweis:
"⇒" Wohldefiniert →

$$\left.\begin{array}{l} u, u_1 \in uN \\ v, v_1 \in vN \end{array}\right\} \Rightarrow (uv)N = (u_1v_1)N$$

Sei $g \in G, n \in N$, dann setze $u = 1, v = g^{-1}, u_1 = n, v_1 = g^{-1} \Rightarrow 1g^{-1}N = ng^{-1}N$ i.e. $g^{-1}N = ng^{-1}N$.

Nun: $ng^{-1} \in ng^{-1}N$, also $ng^{-1} \in g^{-1}N$. Also $ng^{-1} = g^{-1}n_1$ für geeignetes $n_1 \in N$. Also $gng^{-1} = n_1 \in N$.

"⇐" Sei $u, u_1 \in uN, v, v_1 \in vN$. Zu zeigen: $(uv)N = (u_1v_1)N$.
Schreibe $u_1 = un, v_1 = vm; n, m \in N$. Wir zeigen: $u_1v_1 \in (uv)N$.
Wir berechnen: $u_1v_1 = (un)(vm) = u(vv^{-1})nvm = uv(\underbrace{v^{-1}nv}_{:=n_1 \in N})m = uvn_1m = uv(\underbrace{n_1m}_{\in N})$ □

Zusatz zu Proposition 15.8.
Wenn wohldefiniert, dann definiert die Verknüpfung $(uN)(vN) := (uv)N$ eine Gruppenoperation auf die Menge der linken Nebenklassen. (ÜA).

Definition 15.9.
1. Sei $N \leq G$. N ist *normal*, falls $(*)$ in Proposition 15.8. gilt. Wir schreiben dafür: $N \trianglelefteq G$.
2. Für $N \trianglelefteq G$ bezeichnen wir G/N *die Gruppe der linken Nebenklassen* .

Beispiel:
Sei φ ein Homomorphismus, $N := \ker\varphi$ ist normal, weil

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = 1\,.$$

Also $gng^{-1} \in N$ für alle $g \in G$ und $n \in N$.

Die Umkehrung gilt auch (ÜA):

Proposition 15.10.
Für $N \trianglelefteq G$ ist die kanonische Projektion $\begin{array}{rccc} \varphi: & G & \longrightarrow & G/N \\ & g & \mapsto & gN \end{array}$
ein surjektiver Gruppenhomomorphismus mit $\ker\varphi = N$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript wollen wir die Menge der Nebenklassen, normale Teilgruppen, sowie Faktorgruppen weiter untersuchen. Im Abschnitt 17 werden wir zunächst die Anzahl der Nebenklassen allgemein berechnen; insbesondere bestimmen wir die Kardinalität einer Faktorgruppe. Im Abschnitt 18 werden wir diesbezüglich den ersten von insgesamt vier Isomorphiesätze studieren.

§17: Satz von Lagrange

Definition 16.1. Der *Index* einer Teilgruppe H in einer Gruppe G, bezeichnet mit $[G : H]$, ist die Anzahl der Linksnebenklassen von H in G
($[G : H]$ ist entweder eine natürliche Zahl oder unendlich).

Satz 16.2 (Lagrange)**.** Seien G eine endliche Gruppe und H eine Teilgruppe von G. Dann:

1. $|H|$ teilt $|G|$
2. Es gilt $[G : H] = \frac{|G|}{|H|}$.
3. Insbesondere für $H \trianglelefteq G$ ist $|G/H| = \frac{|G|}{|H|}$.

Beweis. Die Menge der linken Nebenklassen bilden eine Partition von G (Proposition 15.7). Da G endlich ist, ist also $n := [G : H]$ eine natürliche Zahl und es existieren $g_1, \ldots, g_n \in G$ mit

- $G = \bigcup_{i=1}^{n} g_i H$
- für alle $1 \leq i < j \leq n$ gilt $g_i H \cap g_j H = \varnothing$.

Es genügt also zu zeigen, dass jede Nebenklasse von H in G Kardinalität $|H|$ hat.
Sei also $g \in G$. Die Abbildung

$$\phi_g : H \to gH; \quad h \mapsto gh$$

ist surjektiv, nach Definition. Sie ist auch injektiv, denn, wenn für $h_1, h_2 \in H$ gilt

$$gh_1 = \phi_g(h_1) = \phi_g(h_2) = gh_2$$

dann ergibt Multiplikation mit g^{-1} die Gleichheit $h_1 = h_2$. Es folgt, dass für alle Nebenklassen gH von H

$$|gH| = |H|$$

gilt. Daher

$$|G| = \sum_{i=1}^{n} |g_i H| = \sum_{i=1}^{n} |H| = [G : H]|H|$$

woraus (i) und (ii) folgen. □

Bemerkung: Im obigen Beweis hätten wir auch mit Rechtsnebenklassen arbeiten können. Daher, die Anzahl der Linksnebenklassen von H ist gleich wie die von Rechtsnebenklassen. Allgemeiner, die Abbildung $gH \mapsto Hg^{-1}$ ist eine Bijektion zwischen die Menge der Links- und Rechtsnebenklassen von H in G. (ÜA)

Korollar 16.3. Sei G eine endliche Gruppe. Für alle $x \in G$ teilt $|x|$ die Ordnung $|G|$. Insbesondere gilt für alle $x \in G$: $x^{|G|} = 1$.

Beweis. Nach Proposition 14.3. und Satz 16.2 gilt $|x| = |\langle x \rangle| \mid |G|$. □

Beispiel: Die Umkehrung des Satzes von Lagrange gilt nicht. Es gibt endliche Gruppen G und $m \in \mathbb{N}$ so dass $m \mid |G|$, jedoch besitzt G keine Teilgruppe der Ordnung m: Sei $G = A_4$. Die Elemente von A_4 sind alle gerade Permutationen auf 4 Elementen:

$$A_4 = \{e,\ (123),\ (132),\ (234),\ (243),\ (134),\ (143), (124),\ (142),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Es gilt $|A_4| = 12$, und $6 \mid 12$, aber A_4 hat keine Teilgruppe der Ordnung 6. (ÜA)

Korollar 16.4. Jede Gruppe primer Ordnung ist zyklisch.

Beweis. Sei G eine endliche Gruppe mit $|G|$ prim. Sei $x \in G\,, x \neq 1$. Nach Korollar 16.3 teilt $|x|$ die Ordnung $|G|$. Da $|G|$ prim ist, folgt entweder $|x| = |G|$ oder $|x| = 1$. Aus $x \neq 1$ folgt $|x| \neq 1$ also $|x| = |G|$ und somit $\langle x \rangle = G$. □

Wir betrachten nun weitere Gruppenkonstruktionen, die wir später im §18 für die Isomorphiesätze brauchen.

Bezeichnung 16.5. Sei G eine Gruppe und seien S, T Teilmenge von G. Schreibe:

$$ST := \{st : s \in S,\ t \in T\}.$$

Proposition 16.6. Sei G eine endliche Gruppe und seien H, K Teilgruppe. Dann gilt

$$|HK||H \cap K| = |H||K|.$$

Beweis. Definiere eine Abbildung

$$\phi\colon H \times K \to HK,\ (h,k) \mapsto hk.$$

Nach Definition ist ϕ surjektiv.

Behauptung: für alle $(h,k) \in H \times K$ gilt $\phi^{-1}(hk) = \{(hd^{-1}, dk) : d \in H \cap K\}$.
Beweis der Behauptung:
"$\supseteq$": offensichtlich, wenn $d \in H \cap K$ dann auch $d^{-1} \in H \cap K$ somit $h' = hd^{-1} \in H$ und $k' = dk \in K$ und $h'k' = hk$.
"$\subseteq$": seien $h' \in H$ und $k' \in K$ mit $h'k' = hk$. Dann $d := k'k^{-1} = h'^{-1}h \in H \cap K$ und $h' = hd^{-1}$ und $k' = dk$. Die Behauptung ist damit bewiesen.

Es folgt, dass für alle $x \in HK$, $|\phi^{-1}(x)| = |H \cap K|$ gilt und somit

$$|HK||H \cap K| = |H \times K| = |H||K|.$$

□

Proposition 16.7. Sei G eine Gruppe und seien H, K Teilgruppen. Die Menge HK ist genau dann eine Teilgruppe wenn $HK = KH$.

Beweis. Wir bemerken die folgende allgemeine Tatsache: Seien $h \in H$ und $k \in K$. Dann $hk \in HK$ und $(hk)^{-1} = k^{-1}h^{-1} \in KH$. Also $g \in HK \iff g^{-1} \in KH$.

Sei nun HK eine Teilgruppe und sei $g := hk \in HK$. Dann ist $g^{-1} \in HK$, und somit $g = (g^{-1})^{-1} \in KH$. Somit $HK \subseteq KH$. Die Inklusion $KH \subseteq HK$ wird analog bewiesen.

Umgekehrt sei nun $HK = KH$. Bemerke dass $HK \neq \varnothing$. Seien $h_1, h_2 \in H$ und $k_1, k_2 \in K$. Betrachte $h_1k_1h_2k_2$. Da $k_1h_2 \in KH = HK$ gilt, dann existieren $h_3 \in H$ und $k_3 \in K$ mit $k_1h_2 = h_3k_3$. Daher $h_1(k_1h_2)k_2 = (h_1h_3)(k_3k_2) \in HK$. Also HK ist bezüglich Multiplikation abgeschlossen. Wir haben weiterhin oben gemerkt, dass $g \in HK$ impliziert $g^{-1} \in KH$. Da $KH = HK$ ist also HK auch bezüglich Inversen abgeschlossen, und somit eine Teilgruppe. □

Definition 16.8. Sei A eine Teilgruppe von G. Der *Normalisator* von A in G, bezeichnet $N_G(A)$, ist die Menge

$$N_G(A) = \{x \in G : xAx^{-1} = A\}$$

Bemerkung 16.9. $N_G(A)$ ist eine Teilgruppe von G die A enthält, A ist genau dann normal in G wenn $G = N_G(A)$ (ÜA).

Korollar 16.10. Seien H, K Teilgruppen von G mit $H \leq N_G(K)$. Dann ist HK eine Teilgruppe von G. Insbesondere, wenn $K \trianglelefteq G$ dann $HK \leq G$ für alle $H \leq G$.

Beweis. Es genügt zu zeigen, dass $HK = KH$. Seien $h \in H$ und $k \in K$. Dann $h^{-1}kh, hkh^{-1} \in K$ weil $H \leq N_G(K)$. Daher $hk = (hkh^{-1})h \in KH$ und $kh = h(h^{-1}kh) \in HK$. Somit $HK = KH$. □

§18: Isomorphiesätze

Satz 16.11 (Erster Isomorphiesatz)**.** Sei $\phi: G \to H$ ein Gruppenhomomorphismus. Dann $\ker\phi \trianglelefteq G$ und

$$G/\ker\phi \simeq \operatorname{Im}\,\phi.$$

Beweis. Es wurde bereits bewiesen, dass der Kern eines Gruppenhomomorphismus normal ist (s. Skript 15; Beispiel nach Definition 15.9).
Definiere $f: G/\ker\phi \to H$ durch $f(a\ker\phi) = \phi(a)$.

- f ist wohldefiniert, denn wenn $a\ker\phi = b\ker\phi$ dann $ab^{-1} \in \ker\phi$ also $1 = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1}$ und somit $\phi(a) = \phi(b)$.
- f ist ein Gruppenhomomorphismus, denn

$$f((a\ker\phi)(b\ker\phi)) = f(ab\ker\phi) = \phi(ab) = \phi(a)\phi(b) = f(a\ker\phi)f(b\ker\phi).$$

- $\operatorname{Im} f = \operatorname{Im}\phi$. Klar.
- f ist injektiv: Seien $f(a\ker\phi) = f(b\ker\phi)$. Dann $\phi(a) = \phi(b) \Rightarrow \phi(ab^{-1}) = 1 \Rightarrow ab^{-1} \in \ker\phi \Rightarrow a\ker\phi = b\ker\phi$.

Also $f: G/\ker\phi \to \operatorname{Im}\phi$ ist also ein bijektiver Gruppenhomomorphismus (ein Isomorphismus). □

Korollar 16.12. Sei $\phi: G \to H$ ein Gruppenhomomorphismus. Dann

1. ϕ ist genau dann injektiv wenn $\ker \phi = 1$;
2. $[G : \ker \phi] = |\text{Im } \phi|$.

Beweis. 1. Die Hinrichtung folgt direkt aus der Definition von Injektivität.

Für die Rückrichtung, sei $\ker \phi = 1$ und seien $a, b \in G$ mit $\phi(a) = \phi(b)$. Dann $\phi(ab^{-1}) = 1 \Rightarrow ab^{-1} \in \ker \phi \Rightarrow ab^{-1} = 1 \Rightarrow a = b$.

2. Aus dem ersten Isomorphiesatz, folgt $[G : \ker \phi] = |G/\ker \phi| = |\text{Im } \phi|$.

□

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

Prof. Dr. Salma Kuhlmann

In diesem Skript wollen wir weitere Isomorphiesätze kennenlernen, und damit §18 beenden.

Wir ergänzen Bemerkung 16.9:

Bemerkung 17.1. Seien $A \leq B \leq G$ Gruppen. Der Normalisator $N_G(A)$ von A in G ist die größte Teilgruppe von G in der A normal ist; A ist genau dann normal in B wenn $B \leq N_G(A)$. (siehe ÜB).

Satz 17.2 (Zweiter Isomorphiesatz)**.** Sei G eine Gruppe und seien A, B Teilgruppen mit $A \leq N_G(B)$. Dann ist AB eine Teilgruppe von G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ und $AB/B \simeq A/(A \cap B)$.

Beweis. Aus $A \leq N_G(B)$ folgt $AB \leq G$ (Korollar 16.10). Aus $B \leq N_G(B)$ folgt $AB \leq N_G(B)$, also $B \trianglelefteq AB$ (Bemerkung 17.1).

Sei nun $\pi\colon AB \to (AB)/B$ die kanonische Projektion, und betrachte die Einschränkung $\pi|_A$ von π auf A. Für $a \in A$ mit $\pi(a) = 1$ gilt auch $a \in B$, daher $a \in A \cap B$. Also ist $\ker(\pi|_A) = A \cap B$, und daher $A \cap B \trianglelefteq A$.

Seien nun $a \in A$ und $b \in B$. Es gilt $\pi(a) = \pi(ab)$. Also ist $\pi|_A$ surjektiv, d.h., Im $(\pi|_A) = (AB)/B$. Der erste Isomorphiesatz (Satz 16.11) ergibt nun $A/(A \cap B) \simeq (AB)/B$. □

Satz 17.3 (Dritter Isomorphiesatz)**.** Sei G eine Gruppe und seien $H, K \trianglelefteq G$ normale Teilgruppen mit $H \leq K$. Dann $K/H \trianglelefteq G/H$ und

$$(G/H)/(K/H) \simeq G/K.$$

Beweis. Definiere die Abbildung $f\colon G/H \to G/K$ durch $f(gH) = gK$.

- f ist wohldefiniert, da für $g_1, g_2 \in G$ mit $g_1H = g_2H$ gilt $g_1^{-1}g_2 \in H$ und $g_1^{-1}g_2 \in K$. Also $g_1K = g_2K$ (s. Proposition 15.7).
- f ist ein Gruppenhomomorphismus:

$$f(aHbH) = f(abH) = abK = aKbK = f(aH)f(bH).$$

- f ist surjektiv: klar.
- Bemerke dass $H \trianglelefteq K$, so dass K/H eine Gruppe ist, also $K/H \leq G/H$ ist eine Untergruppe (s. Proposition 15.8). Wir behaupten dass $\ker f = K/H$. In der Tat, sei $a \in G$. Dann $f(aH) = 1K \iff aK = 1K \iff a \in K$. Daher $K/H = \ker f$. Also $K/H \trianglelefteq G/H$ und (s. Satz 16.11) es folgt:

$$(G/H)/(K/H) \simeq G/K.$$

□

Satz 17.4. (Gitter Isomorphiesatz / Korrespondenzsatz) Sei G eine Gruppe und N eine normale Teilgruppe von G. Für eine Teilgruppe A die N enthält, sei $\bar{A} := A/N$. Sei $\pi: G \to G/N$ die kanonische Projektion.

Die Abbildung $A \mapsto \pi(A) = \bar{A}$ ist eine Bijektion zwischen der Menge der Teilgruppen von G die N enthalten und der Menge der Teilgruppen von G/N.

Weiter, für $A, B \leq G$ mit $N \leq A$ und $N \leq B$ gelten:

1. $A \leq B \iff \bar{A} \leq \bar{B}$; in diesem Fall, gilt $[B : A] = [\bar{B} : \bar{A}]$.
2. $A \trianglelefteq B \iff \bar{A} \trianglelefteq \bar{B}$; in diesem Fall, gilt $B/A \simeq \bar{B}/\bar{A}$.
3. $\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$.
4. $\overline{A \cap B} = \bar{A} \cap \bar{B}$.

Beweis. Siehe ÜB. □

Satz 17.5. (Schmetterlingslemma / Lemma von Zassenhaus) Seien $a \trianglelefteq A$ und $b \trianglelefteq B$ Teilgruppen einer Gruppe G. Dann

1. $a(A \cap b) \trianglelefteq a(A \cap B)$
2. $b(B \cap a) \trianglelefteq b(B \cap A)$
3. $(A \cap b)(B \cap a) \trianglelefteq A \cap B$
4. $$\frac{a(A \cap B)}{a(A \cap b)} \simeq \frac{A \cap B}{(A \cap b)(B \cap a)} \simeq \frac{b(B \cap A)}{b(B \cap a)}$$

Beweis. Aus $A \leq N_G(a)$ beziehungsweise $B \leq N_G(b)$ folgen :

$$A \cap b \leq A \cap B \leq N_G(a) \quad \text{beziehungsweise} \quad B \cap a \leq A \cap B \leq N_G(b).$$

(s. Bemerkungen 16.9 und 17.1).

• Daher sind $a(A \cap b), a(A \cap B), b(B \cap a)$ und $b(A \cap B)$ Teilgruppen von G (s. Korollar 16.10).

Zunächst zeigen wir 3.

• Bemerke, dass $A \cap b$ und $B \cap a$ normale Teilgruppen von $A \cap B$ sind. Wir führen den Beweis für $A \cap b$ (der Beweis für $B \cap a$ ist analog): Für $g \in A \cap B$ und $c \in A \cap b$ gelten $gcg^{-1} \in b$ (weil $b \trianglelefteq B$) und $gcg^{-1} \in A$ weil $c, g \in A$.

• Also ist $(A \cap b)(B \cap a) \leq A \cap B$ (s. Korollar 16.10). Es folgt übrigens dass $(A \cap b)(B \cap a) = (B \cap a)(A \cap b)$ (s. Proposition 16.7).

• Jetzt prüfen wir dass $(A \cap b)(B \cap a)$ eine normale Teilgruppe von $A \cap B$ ist: für $c \in A \cap b$ und $d \in B \cap a$ gilt $gcdg^{-1} = gcg^{-1}gdg^{-1} \in (A \cap b)(B \cap a)$.

Jetzt zeigen wir 4 (und zugleich 1. beziehungsweise 2.).

Ein Element $x \in a(A \cap B)$ lässt sich als $x = \alpha\gamma$ darstellen mit $\alpha \in a$ und $\gamma \in A \cap B$. Definiere

$$f: a(A \cap B) \to \frac{A \cap B}{(A \cap b)(B \cap a)}$$

durch

$$x \mapsto \gamma(A \cap b)(B \cap a).$$

• f ist wohldefiniert: sei $\alpha\gamma = \alpha'\gamma'$. Dann $\gamma'\gamma^{-1} = (\alpha')^{-1}\alpha \in a \cap B \cap A = a \cap B \leq (A \cap b)(B \cap a)$, d.h.:

$$\gamma'(A \cap b)(B \cap a) = \gamma(A \cap b)(B \cap a).$$

• f ist ein Gruppenhomomorphismus: seien $\alpha, \alpha' \in a$ und $\gamma, \gamma' \in A \cap B$. Dann $\alpha, \gamma\alpha'\gamma^{-1} \in a$ weil $a \lhd A$. Also

$$f(\alpha\gamma\alpha'\gamma') = f((\alpha\gamma\alpha'\gamma^{-1})\gamma\gamma') = \gamma\gamma'(A \cap b)(B \cap a)$$

und da $(A \cap b)(B \cap a) \lhd A \cap B$ folgt

$$f(\alpha\gamma)f(\alpha'\gamma') = \gamma(A \cap b)(B \cap a)\gamma'(A \cap b)(B \cap a) = \gamma\gamma'(A \cap b)(B \cap a).$$

• f ist surjektiv: nach Definition.

• Es gilt $\ker f = a(A \cap b)$. In der Tat, seien $\alpha \in a$ und $\gamma \in A \cap B$ mit $f(\alpha\gamma) = 1(A \cap b)(B \cap a)$, d.h., $\gamma \in (A \cap b)(B \cap a)$. Seien $x \in (A \cap b)$ und $y \in (B \cap a)$ mit $\gamma = xy$. Dann $\alpha\gamma = (\alpha x)y \in a(A \cap b)$. Umgekehrt, seien $\alpha \in a$ und $\gamma \in A \cap B$ mit $\alpha\gamma \in a(A \cap b)$. Dann existieren $t \in a,\ s \in A \cap b$ mit $\alpha\gamma = ts$. Nun $\alpha^{-1}t \in a$ und aus $\gamma, s \in B$ folgt $\alpha^{-1}t = \gamma s^{-1} \in B$. Also $\alpha^{-1}ts = \gamma \in (B \cap a)(A \cap b) = (A \cap b)(B \cap a)$ und somit $\alpha\gamma \in \ker f$.

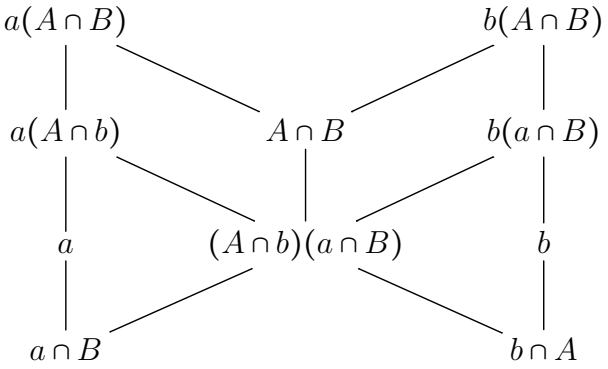
• Nach dem ersten Isomorphiesatz ist $a(A \cap b)$ normal in $a(A \cap B)$ (was 1. zeigt) und

$$\frac{a(A \cap B)}{a(A \cap b)} \simeq \frac{(A \cap B)}{(A \cap b)(B \cap a)}.$$

• Wenn wir nun A und B und, entsprechend, a und b umtauschen und den gleichen Beweis durchführen bekommen wir 2. und

$$\frac{b(A \cap B)}{b(B \cap a)} \simeq \frac{(A \cap B)}{(A \cap b)(B \cap a)}.$$

Das Schmetterlingsdiagramm:



□

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Abschnitt §19 beginnen; Normalreihen einführen, Satz 17.5 benutzen um den Verfeinerungssatz von Schreier sowie den Satz von Jordan-Hölder zu beweisen.

§19: Einfache und auflösbare Gruppen

Definition 18.1. Sei G eine Gruppe.

1. Eine normale Teilgruppe $N \trianglelefteq G$ heißt auch *Normalteiler* von G. Wir schreiben auch $G \trianglerighteq N$ dafür.
2. G ist *einfach* falls G nicht-trivial ist (i.e. $G \neq 1$) und 1 und G die einzige Normalteiler von G sind.

Proposition 18.2. Eine nicht-triviale abelsche Gruppe G ist genau dann einfach wenn $G \simeq \mathbb{Z}_p$ für eine Primzahl p (i.e. G ist zyklisch von primer Ordnung p).

Beweis. 1. Sei G eine abelsche Gruppe. Dann ist jede Teilgruppe N von G normal (weil die Bedingung $(*)$ in Proposition 15.8 stets für N erfüllt ist, wenn G abelsch ist). G ist also genau dann einfach wenn ihre einzige Teilgruppen 1 und G sind. (Insbesondere ist $\mathbb{Z}_p$ einfach, wegen Lagrange's Satz).

2. Sei nun G einfach. Aus 1. folgt, dass G von jedem nicht-trivialen Element erzeugt ist, also G ist zyklisch. Wenn G zyklisch und unendlich ist, und x ein Erzeuger von G, dann ist z.B. x^2 kein Erzeuger von G (s. Proposition 14.11). Es folgt: G ist endlich und zyklisch und jedes Element $x \neq 1$ erzeugt G.

   Sei nun $x \neq 1$ ein Erzeuger von G, $p \in \mathbb{N}$ eine Primzahl die $|x|$ teilt. Dann ist $|x^p| < |x|$ (s. Proposition 14.11) und daher ist x^p kein Erzeuger, also ist $x^p = 1$. Daraus folgt $|G| = p$.

□

Definition 18.3. Sei G eine Gruppe.

1. Eine Kette von Teilgruppen

$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$

   heißt *Normalreihe* falls $G_i \trianglelefteq G_{i+1}$ für alle $i = 0, \cdots, s$ gilt.

2. Die Quotienten G_{i+1}/G_i für $i = 0, \ldots, s-1$ heißen *Faktorgruppen*, oder die *Faktoren* oder die *Quotienten* der Normalreihe.
3. Eine Normalreihe heißt *Kompositionsreihe* falls alle Faktorgruppen einfach sind.
4. In diesem Fall heißen die Faktorgruppen *Kompositionsfaktoren* von G.

5. Eine Normalreihe
$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$
heißt *Verfeinerung* einer anderen Normalreihe
$$1 = H_0 \leq H_2 \leq \ldots \leq H_r = G$$
falls $H_0, \ldots, H_r$ eine Teilkette von $G_0, \ldots, G_s$ ist.

Beispiel: Die Gruppe A_4 ist normal in S_4, weil $[S_4 : A_4] = 2$ (s. ÜB). Im ÜB wird ferner gezeigt, dass die Teilgruppe (die *kleinsche Vierergruppe*)
$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$
ein Normalteiler von A_4 ist. Somit ist
$$\{1\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$$
eine Normalreihe für S_4.

Definition 18.4. Zwei Normalreihen heißen *äquivalent* falls es eine Bijektion zwischen ihren Faktorgruppen gibt, und entsprechende Faktorgruppen isomorph sind. Das heißt zwei Reihen
$$H_0 \trianglelefteq \cdots \trianglelefteq H_i \trianglelefteq H_{i+1} \trianglelefteq \cdots \trianglelefteq G$$
und $\quad K_0 \trianglelefteq \cdots \trianglelefteq K_j \trianglelefteq K_{j+1} \trianglelefteq \cdots \trianglelefteq G$
sind äquivalent, wenn es eine Bijektion $i \to j$ gibt, so dass die korrespondierenden Faktoren isomorph sind: $H_{i+1}/H_i \simeq K_{j+1}/K_j$.

Beispiel: Betrachte die folgende Kompositionsreihen für $\mathbb{Z}_{30}$:
$$\mathbb{Z}_{30} \geq \langle 5\rangle \geq \langle 10\rangle \geq \{0\}$$
$$\mathbb{Z}_{30} \geq \langle 3\rangle \geq \langle 6\rangle \geq \{0\}.$$
Die Kompositionsfaktoren der ersten Reihe sind $\mathbb{Z}_{30}/\langle 5\rangle \simeq \mathbb{Z}_5$, $\langle 5\rangle/\langle 10\rangle \simeq \mathbb{Z}_2$ und $\langle 10\rangle/\langle 0\rangle \simeq \mathbb{Z}_3$.
Die Kompositionsfaktoren der ersten Reihe sind $\mathbb{Z}_{30}/\langle 3\rangle \simeq \mathbb{Z}_3$, $\langle 3\rangle/\langle 6\rangle \simeq \mathbb{Z}_2$ und $\langle 6\rangle/\langle 0\rangle \simeq \mathbb{Z}_5$.
Daher sind die zwei Kompositionsreihen äquivalent.

Satz 18.5 (Verfeinerungssatz von Schreier)**.** Zwei Normalreihen einer Gruppe G haben äquivalente Verfeinerungen.

Beweis. Seien

(1) $$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

und

(2) $$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = G$$

Normalreihen. Sei $G_{i,j} := G_i(G_{i+1} \cap H_j)$ für $0 \leq j \leq r$. Dann
$$G_{i,0} = G_i\{1\} = G_i \quad \text{und} \quad G_{i,r} = G_i(G_{i+1} \cap G) = G_{i+1}.$$
(also haben wir r weitere Glieder zwischen G_i und G_{i+1} eingefügt).
Da $G_i \trianglelefteq G_{i+1}$ und $H_j \trianglelefteq H_{j+1}$, aus dem Lemma von Zassenhaus (mit $a = G_i$, $A = G_{i+1}$, $b = H_j$ und $B = H_{j+1}$) folgt
$$G_{i,j} = G_i(G_{i+1} \cap H_j) \trianglelefteq G_i(G_{i+1} \cap H_{j+1}) = G_{i,j+1}.$$

Somit ist die folgende Normalreihe eine Verfeinerung von (1):

$$\{1\} \trianglelefteq G_{0,0} \trianglelefteq G_{0,1} \trianglelefteq \ldots \trianglelefteq G_{0,r} = G_{1,0} \trianglelefteq G_{1,1} \trianglelefteq \ldots \trianglelefteq G_{s-1,r} = G_s = G.$$

Sei nun $H_{i,j} := H_i(H_{i+1} \cap G_j)$ für $0 \leq j \leq s$. Ähnlich wie oben, ist

$$\{1\} \trianglelefteq H_{0,0} \trianglelefteq H_{0,1} \trianglelefteq \ldots \trianglelefteq H_{0,s} = H_{1,0} \trianglelefteq H_{1,1} \trianglelefteq \ldots \trianglelefteq H_{r-1,s} = H_r = G.$$

eine Verfeinerung von (2). Nun, aus dem Lemma von Zassenhaus (mit $a = G_i$, $A = G_{i+1}$, $b = H_j$ und $B = H_{j+1}$) folgt

$$\frac{G_i(G_{i+1} \cap H_{j+1})}{G_i(G_{i+1} \cap H_j)} \simeq \frac{H_j(H_{j+1} \cap G_{i+1})}{H_j(H_{j+1} \cap G_i)}$$

das heißt:

$$G_{i,j+1}/G_{i,j} \simeq H_{j,i+1}/H_{j,i}.$$

□

Satz 18.6 (Satz von Jordan-Hölder)**.** Sei G eine endliche Gruppe mit $G \neq 1$. Dann gelten

1. G hat eine Kompositionsreihe
2. alle Kompositionsreihen von G sind äquivalent.

Beweis. 1. Wenn G einfach ist, dann ist $\{1\} \trianglelefteq G$ bereits eine Kompositionsreihe.

Sei nun G nicht einfach. Da G endlich ist, hat sie einen maximalen echten Normalteiler N. Dann ist G/N einfach, nach dem Korrespondenzsatz 17.4. Nach Induktion auf $|G|$ hat G eine Kompositionsreihe. ÜA.

2. Nach dem Korrespondenzsatz 17.4 haben Kompositionsreihen keine echte Verfeinerungen; wenn $G_i \trianglelefteq N \trianglelefteq G_{i+1}$ dann $N/G_i \trianglelefteq G_{i+1}/G_i$ und wenn G_{i+1}/G_i einfach ist, dann gilt $N = G_i$ oder $N = G_{i+1}$. Nun, nach dem Verfeinerungssatz von Schreier haben zwei beliebige Kompositionsreihen äquivalente Verfeinerungen. Somit sind zwei beliebige Kompositionsreihen bereits äquivalent.

□

Definition 18.7.
G heißt *auflösbar*, wenn es eine *Normalreihe mit abelschen Faktoren hat.*

Bemerkung 18.8.
Jede abelsche Gruppe ist trivialerweise auflösbar. Betrachte $G \triangleright \{1\}$.

Erinnerung (s. LA II, Kapitel II, § 6; Skripte 6 und 7.) Sei $n \geq 3$, dann ist

1. $|S_n/A_n| = 2$
2. S_n ist nicht abelsch
3. A_n ist nicht abelsch für $n > 3$
   (Begründung: (123) und (234) kommutieren nicht!)

Beispiel 18.9.
S_n ist auflösbar für $n \leq 4$: S_1 und S_2 sind abelsch also auflösbar. Wir betrachten nun:

1. $S_3 \trianglerighteq A_3 \trianglerighteq \{1\}$

   $| S_3/A_3 | = 2$ $| A_3/\{1\} | = 3$: Diese zwei Gruppen haben als Ordnung eine Primzahl. Es folgt aus Lagrange, dass die Gruppen zyklisch sind, also abelsch.

2. $S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq W \trianglerighteq \{1\}$, wobei V die kleinsche Vierergruppe ist und $W := \{1, (12)(34)\}$.

   $| S_4/A_4 | = 2$ $| A_4/V | = 3$ $| V/W | = 2$.

   Die Faktorgruppen sind also $\mathbb{Z}_2$ und $\mathbb{Z}_3$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir auflösbare Gruppen weiter untersuchen, und eine Charakterisierung erzielen in Satz 19.6. Dafür werden wir neue Definitionen und Begriffe (z.B. iterierte Kommutatoren) benötigen. Auflösbare Gruppen spielen in Kapitel 4 eine wesentliche Rolle.

Sei $G \neq \{1\}$ stets eine Gruppe.

Definition 19.1.

1. Für $g, h \in G$ definiere $(g,h) := g^{-1}h^{-1}gh \in G$; (g,h) heißt *Kommutator* von g und h.
2. $G' := (G,G)$ ist die *Kommutatorgruppe* von G und ist die Untergruppe, die durch
$$S := \{(g,h); g,h \in G\}$$
erzeugt wird.
3. Wir definieren die iterierte Kommutatoren per Induktion über $k \in \mathbb{N}, k \geq 2$:
$G'' := (G')'$, $G^{(k)} := (G^{(k-1)})'$.

Bemerkung 19.2.

1. G ist abelsch genau dann, wenn $(G,G) = \{1\}$.
2. $gh = hg(g,h)$
3. $(g,h) = (h,g)^{-1}$, also ist $< S >= \{s_1 \cdots s_n \mid n \in \mathbb{N};\ s_i \in S\}$.
4. Wenn $H \leq G$, dann ist $H^{(l)} \leq G^{(l)}$ für alle $l \in \mathbb{N}$.

Beweis: ÜA.

Wir werden nun die iterierte Kommutatoren genauer untersuchen, und sie für unsere Charakterisierung für auflösbare Gruppen ausnutzen.

Proposition 19.3.
Seien G, K Gruppen und $\eta : G \to K$ ein Homomorphismus. Es gelten

1. $\eta(g,h) = (\eta(g), \eta(h))$
2. $\eta(G') \subseteq K'$
3. Wenn η surjektiv ist, gilt ferner: $\eta(G') = K'$
4. Insbesondere für einen beliebigen Homomorphismus η gilt: $\eta(G') = \eta(G)'$ und
5. Allgemeiner gilt $\eta(G^{(k)}) = \eta(G)^{(k)}$ für alle $k \in \mathbb{N}$

Beweis:

1. Wir berechnen: $\eta(g,h) = \eta(g^{-1}h^{-1}gh) = \eta(g)^{-1}\eta(h)^{-1}\eta(g)\eta(h) = (\eta(g),\eta(h))$.
2. Aus 1. folgt unmittelbar $\eta(G') \subseteq K'$.
3. Wenn η surjektiv ist, folgt aus 1. dass für alle $x, y \in K : (x,y) \in \eta(G')$. Es folgt also auch $\eta(G') \supseteq K'$, und damit ist die Gleichheit bewiesen.
4. Klar, da $\eta : G \to \eta(G)$ surjektiv ist.
5. Für $k = 1$ gilt die Behauptung wie in 4.

   Nun betrachte $\eta : G' \to K$ und 4. nochmal angewendet ergibt:

   $$\begin{array}{lrcl} & \eta((G')') & = & \eta(G')' \\ \text{i.e.} & \eta(G'') & = & (\eta(G)')' = \eta(G)'' . \end{array}$$

   (Usw. per Induktion fortsetzen, ÜA). □

Proposition 19.4.
Wenn $K \trianglelefteq G$, dann ist $K' \trianglelefteq G$. Insbesondere ist $G' \trianglelefteq G$.

Beweis:
Sei $a \in G$ fest und betrachte die Abbildung $\eta_a : K \to K$, $k \mapsto aka^{-1}$.
Da K ein Normalteiler ist, ist η_a wohldefiniert. Außerdem ist η_a ein Homomorphismus (ÜA).
Aus Proposition 19.3 folgt: $\eta_a(K') \subseteq K'$ für alle $a \in G$, i.e. $K' \trianglelefteq G$. □

Wir erhalten also eine Kette:

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq G^{(k+1)} \trianglerighteq \cdots .$$

Für den Beweis von Satz 19.6 brauchen wir noch:

Lemma 19.5.
Sei $K \trianglelefteq G$. Es gilt G/K ist abelsch $\Leftrightarrow K \geq G'$. Insbesondere ist G/G' abelsch.
(In der Tat ist G' ist die kleinste normale Untergruppe mit dieser Eigenschaft).
Allgemeiner gilt: $G^{(k)}/G^{(k+1)}$ ist abelsch für alle $k \in \mathbb{N}$.

Beweis:
Aus Bemerkung 19.2 folgt: G/K ist abelsch $\Leftrightarrow (G/K)' = \{1\} \Leftrightarrow (gK, hK) = 1$ für alle $g, h \in G$.
Aber $(gK,hK) = (gK)^{-1}(hK)^{-1}gKhK = (g^{-1}h^{-1}gh)K = (g,h)K$. Also ist G/K abelsch $\Leftrightarrow$ $(g,h)K = K$ für alle $g,h \in G \Leftrightarrow (g,h) \in K$ für alle $g,h \in G \Leftrightarrow G' \leq K$.
Die letzte Aussage folgt per Induktion nach $k \in \mathbb{N}$. □

Satz 19.6.
G ist auflösbar $\Leftrightarrow \exists k \in \mathbb{N}$ mit $G^{(k)} = 1$.

Beweis:
"$\Leftarrow$" Folgt unmittelbar aus Lemma 19.5: Die Normalreihe $G \trianglerighteq G' \trianglerighteq \cdots \trianglerighteq G^{(k)} = 1$ hat abelsche Faktoren.

"⇒" Sei $G = G_1 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$ eine Normalreihe mit abelschen Faktoren G_i/G_{i+1}.

Lemma 19.5 $\Rightarrow G_{i+1} \supseteq G_i'$ für alle i.

Wir prüfen per Induktion dass $G_i \supseteq G^{(i)}$ für alle i:

- für $i = 1$ gilt $G = G_1 \supseteq G'$ ✓
- Induktionsannahme für k ✓
- Induktionsschritt für $k+1$: $G_{k+1} \supseteq (G_k)' \supseteq (G^{(k)})' = G^{(k+1)}$

Schließlich, da $G_{s+1} = \{1\}$ folgt insbesondere $G^{(s+1)} = \{1\}$ □

Satz 19.7.
Sei G auflösbar.

(1) Sei $H \leq G$. Dann ist H auflösbar.

(2) Sei $\eta : G \twoheadrightarrow H$ ein surjektiver Homomorphismus, dann ist H auflösbar.

(3) Sei G eine beliebige Gruppe und $K \trianglelefteq G$, so dass K und G/K auflösbar sind, dann ist G auch auflösbar.

Beweis: Für den Beweis, benutzen wir stillschweigend Proposition 19.3 und Satz 19.6:

(1) $H \leq G \Rightarrow H^{(i)} \leq G^{(i)}$, also $G^{(k)} = \{1\} \Rightarrow H^{(k)} = \{1\}$.

(2) $\eta(G^{(i)}) = \eta(G)^{(i)}$. Also $G^{(k)} = \{1\} \Rightarrow \eta(G)^{(k)} = \{1\}$. Also $H^{(k)} = \{1\}$.

(3) Sei $\pi : G \twoheadrightarrow G/K$ die kanonische Projektion. Es gilt $\pi(G^{(i)}) = (G/K)^{(i)}$.

Nun G/K auflösbar $\Rightarrow \exists k$ mit $\pi(G^{(k)}) = (G/K)^{(k)} = \{1\}$. Also: für alle $x \in G^{(k)}$ gilt $xK = K$. Es folgt: für alle $x \in G^{(k)}$ gilt $x \in K$, i.e. $G^{(k)} \subseteq K$.

Nun ist aber auch K auflösbar, also existiert ℓ mit $K^{(\ell)} = \{1\}$. Wir berechnen: $G^{(k+\ell)} = (G^{(k)})^{\ell} \subseteq K^{(\ell)} = \{1\}$. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir eine Charakterisierung für endliche auflösbare Gruppen beweisen. Wir werden ferner (ergänzend zu Beispiel 18.9) die Gruppen A_n und S_n für $n \geq 5$ untersuchen, damit werden wir Abschnitt §19 beenden. Im Abschnitt §20 werden wir die Sylow Sätze aussagen, und die notwendige Begriffe und Werkzeug für deren Beweise einführen.

Sei $G \neq \{1\}$ stets eine Gruppe.

Bemerkung 20.1.
G ist auflösbar und einfach $\Rightarrow G$ ist abelsch (weil $G \trianglerighteq \{1\}$ die einzig mögliche Normalreihe ist).

Satz 20.2.
Sei G eine endliche Gruppe. Dann ist G auflösbar $\Leftrightarrow$ jeder (nicht-trivialer) Kompositionsfaktor einer Kompositionsreihe ist zyklisch mit Primordnung.

Beweis:

"$\Rightarrow$" Sei G auflösbar; und $G = G_1 \trianglerighteq \cdots \trianglerighteq G_{s+1} = \{1\}$ eine Kompositionsreihe. Per Definition ist G_i/G_{i+1} einfach, für alle i. Außerdem ist G_i/G_{i+1} auch auflösbar, für alle i (s. Satz 19. 7). Es folgt: G_i/G_{i+1} ist abelsch, für alle i (s. Bemerkung 20.1), also entweder trivial oder zyklisch mit Primordnung (s. Proposition 18.2).

"$\Leftarrow$" Da G endlich ist, existiert wegen Jordan Hölder eine Kompositionsreihe

$$(*) \qquad G = G_1 \trianglerighteq \cdots \trianglerighteq G_{s+1} = \{1\}$$

Per Annahme sind die (nicht-triviale) G_i/G_{i+1} zyklisch mit Primordnung. Dann ist insbesondere G_i/G_{i+1} abelsch und damit ist die Reihe $(*)$ sogar eine auflösbare Reihe. $\square$.

Satz 20.3.
A_n ist einfach für $n \geq 5$.

Beweis:
Aus Lineare Algebra II, ÜB5 Aufgabe 5.3 (b) wissen wir dass A_n von 3-Zykeln erzeugt ist, für $n \geq 3$. Sei $K \neq \{1\}, K \trianglelefteq A_n$. Zu zeigen: $K = A_n$.

Behauptung 1: Wenn K ein 3-Zykel enthält, dann enthält K alle 3-Zykeln.

Beweis: Sei OE $(123) \in K$ und (ijk) beliebig. Betrachte γ darunter (OE ist $\gamma \in A_n$ sonst ersetze durch $(lm)\gamma$):

$$\gamma := \begin{pmatrix} 1\,2\,3\,4\,5\cdots \\ i\,j\,k\,l\,m\cdots \end{pmatrix}. \quad \text{Wir berechnen: } \gamma(123)\gamma^{-1} = (ijk) \qquad (*)$$

Da K normal ist folgt nun wegen $(*)$ dass $(ijk) \in K$. $\square$

Behauptung 2: K enthält ein 3-Zykel.

Beweis: • Sei $\alpha \in K\,; \alpha \neq 1$. Wähle α mit maximaler Anzahl von Fixpunkten. Bemerke dass α keine Transposition ist. Wir zeigen: α ist ein 3-Zykel. Sonst schreibe:

(a) $\alpha = (123\cdots)\cdots$

oder

(b) $\alpha = (12)(34)\cdots$

als Produkt disjunkter Zykeln.

• Beobachte, dass im Fall (a) α noch zwei Zahlen bewegen muss (ohne Einschränkung 4, 5), sonst ist $\alpha = (123k)$ eine ungerade Permutation - Widerspruch.

• Setze $\beta := (345)$ und $\alpha_1 := \beta\alpha\beta^{-1}$. Dann ist $\alpha_1 \in K$, weil $\alpha \in K$ und $K \trianglelefteq A_n$.

Direktes Rechnen zeigt:
$\alpha_1 = (124\cdots)\cdots$ im Fall (a) und $\alpha_1 = (12)(45)\cdots$ im Fall (b).

Auf jeden Fall ist $\alpha_1 \neq \alpha$ und damit $\alpha_2 := \alpha_1\alpha^{-1} \neq 1$ und $\alpha_2 \in K$.

Nun ist jede $\ell > 5$ durch β fixiert. Beobachte, dass falls ℓ auch durch α fixiert ist, ℓ auch durch α_2 fixiert ist. Also sind die Fixpunkte von α und α_2 die größer als 5 sind, identisch.

Direktes Rechnen im Fall (a) zeigt $\alpha_2(2) = 2$ und außerdem bewegt α in diesem Fall $1, 2, 3, 4, 5$ (wie oben beobachtet). Also hat α_2 einen extra Fixpunkt (nämlich 2). Da $\alpha_2 \in K$ ist es ein Widerspruch.

Direktes Rechnen im Fall (b) zeigt $\alpha_2(1) = 1$ und $\alpha_2(2) = 2$ - Widerspruch. □

Korollar 20.4.
S_n ist **nicht** auflösbar für $n \geq 5$.

Beweis:
Sonst wäre wegen Satz 19.7 auch A_n auflösbar. Da aber A_n einfach ist folgt wegen Bemerkung 20.1 dass A_n abelsch ist - Widerspruch (s. Erinnerung, S. 3 Skript 18). □

§20: Die Sylow Sätze.

Unser nächstes Ziel ist es, die Sylow Sätze zu beweisen. Diese sind Sonderfälle, für die die Umkehrung von Lagrange gilt. Die Sylow Sätze werden wir für die Galoistheorie in Kapitel 4 benötigen.

Sei G stets eine endliche Gruppe.

Sylow 1:

Sei p Primzahl und $k \in \mathbb{N}$, so dass $p^k \,||G|$, dann hat G eine Teilgruppe H der Ordnung p^k.

Definition 20.5.
Eine solche Teilgruppe H mit $H = p^m$, wobei m maximal ist, heißt eine *Sylow-p-Untergruppe.*

Sylow 2:

1. Sylow-p-Untergruppen H_1 und H_2 sind zueinander konjugiert, das heißt es existiert $a \in G$ mit $H_2 = aH_1a^{-1}$.
2. Die Anzahl der Sylow-p-Untergruppen ist ein Divisor von $[G : H]$ für eine (jede) Sylow-p-Untergruppe H und ist $\equiv 1 \mod p$.
3. Jede Untergruppe der Ordnung p^k ist enthalten in einer Sylow-p-Untergruppe.

Für die Beweise der Sylow-Sätze brauchen wir Gruppenaktionen:

Definition 20.6.
Sei G eine Gruppe und $S \neq \varnothing$ eine Menge. Eine Abbildung

$$\begin{array}{ccc} G \times S & \to & S \\ (g, x) & \mapsto & gx \end{array}$$

so dass

(i) $1x = x$ für alle $x \in S$

(ii) $g_1g_2x = g_1(g_2x)$ für alle $x \in S$ und für alle $g_1, g_2 \in G$

heißt *Gruppenaktion*. Wir sagen G *operiert auf* S.

Definition 20.7.
Angenommen G operiert auf S und S'. Die Aktionen heißen *äquivalent*, wenn es eine Bijektion

$$\nu : S \to S'$$

gibt so dass

$$\nu(gx) = g\nu(x)$$

für alle $g \in G$ und $x \in S$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Gruppenaktionen genauer untersuchen, einige wichtige Beispiele und Begriffe dazu lernen, und eine Charakterisierung von transitiven Aktionen beweisen in Satz 21.12. Der Satz ergibt mehrere Korollare, u.a. die wichtige Bahngleichung in Skript 22.

Seien stets $S \neq \varnothing$ eine Menge, G eine Gruppe.

Notation: $Sym\ S$ bezeichnet die Gruppe der Permutationen von S.

Definition 21.1.
$H \leq Sym\ S$ heißt Permutationsgruppe.

Proposition 21.2. Sei G eine Gruppe. Angenommen G operiert auf S. Sei $g \in G$.

1. Definiere die Abbildung
$$\begin{array}{rccc} T(g): & S & \longrightarrow & S \\ & x & \mapsto & gx \end{array}$$
Dann ist $T(g) \in Sym\ S$.

2. Die Abbildung
$$\begin{array}{rccc} T: & G & \longrightarrow & SymS \\ & g & \mapsto & T(g) \end{array}$$
ist ein Gruppenhomomorphismus.

Beweis: ÜA. □

Definition 21.3.
Ansatz wie in Proposition 21.2, $\ker T \trianglelefteq G$ heißt der *Kern der Aktion von G auf S*. Die Aktion heißt *effektiv*, wenn $\ker T = \{1\}$.

Bemerkung 21.4.

1. G operiert auf S und $H \leq G \Rightarrow H$ operiert auf S (durch Einschränkung).
2. G operiert auf S und $\varnothing \neq \mathcal{O} \subseteq S \Rightarrow G$ operiert auf $\mathcal{O}$
(wann immer die Einschränkung wohldefiniert ist.)

Beweis: (ÜA) □

Beispiel 21.5 (samt Definitionen).

(i) Nehme $S = G$. Definiere die effektive Aktion "*linke Multiplikation*" μ_L :
$(g, x) \mapsto \underbrace{gx}_{\text{Produkt in } G}$, für alle $g, x \in G$.

(ii) Dual dazu μ_R: "*rechte Multiplikation*".

(iii) Nehme $S = G$. Definiere die Aktion "*Konjugation*" κ_j:
$(g, x) \mapsto gxg^{-1}$, für alle $g, x \in G$.

Der Kern dieser Aktion ist die normale Untergruppe $C_G \trianglelefteq G$ und heißt *Zentrum von* G:
$$\begin{aligned} C_G &= \{g \mid \forall x \in G : gxg^{-1} = x\} \\ &= \{g \mid \forall x \in G : gx = xg\} \end{aligned}$$

Satz 21.6. (Satz von Cayley)
Jede Gruppe ist isomorph zu einer Permutationsgruppe.

Beweis:
Setze $S = G$, G operiert auf S mit μ_L. Betrachte den Gruppenhomomorphismus T wie in Proposition 21.2 : $\begin{array}{rccc} T: & G & \longrightarrow & Sym\ G \\ & g & \mapsto & T(g) \end{array}$.
Dann ist offensichtlich $\ker T = \{1\}$. Also $G \simeq T(G) \leq Sym\ G$. □

Aktionen induzieren Äquivalenzrelation. Wir nehmen an: G operiert auf S.

1. Seien $x, y \in S$. Setze $x \underset{G}{\sim} y$, wenn es ein $g \in G$ gibt, s.d. $y = gx$.
   $\underset{G}{\sim}$ ist eine Äquivalenzrelation auf S.
2. $[x] := Gx := \{gx \mid g \in G\}$ heißt die *Orbit* oder *Bahn von* x in S.
3. Es folgt: $S = \bigsqcup_{x \in S} Gx$.

Beispiel 21.7 (samt Definitionen).

(iv) Sei $H \leq G$, setze $S = G$. Dann operiert H auf G durch μ_L (s. Bemerkung 21.4). Wir berechnen für $x \in G$:
$$[x] = \{hx \mid h \in H\} = Hx\,,$$
also die rechte Nebenklasse von x bezüglich H.

(v) Analog für μ_R . Hier bekommen wir $[x] = xH$, die linke Nebenklasse von x bezüglich H.

(vi) Für die Aktion κ_j , und $x \in G$ ist $[x] = \{gxg^{-1} \mid g \in G\}$ die *Konjukationsklasse* von x.

Proposition 21.8.
(i) Die Konjugationsklasse von x ist $\{x\}$ genau dann, wenn $x \in C_G$.

(ii) Also ist das Zentrum von G die Vereinigung solcher Konjugationsklassen.

Beweis: ÜA

□

Wir nehmen an: G operiert auf S.

Definition 21.9.
1. *G operiert transitiv auf S*, oder *die Aktion von G auf S ist transitiv* wenn es nur eine Bahn gibt, das heißt für alle $x, y \in S : x \underset{G}{\sim} y$.
2. Sei $x \in S$, der *Stabilisator von x in G* ist die Untergruppe von G
$$Stab_x := \{g \in G\ ;\ gx = x\ .\}$$

3. Für die Aktion κ_j von G auf G und $x \in G$ heißt

$$Stab_x = \{g \in G \mid gxg^{-1} = x\} = C(x) = \{g \in G \mid gx = xg\} ,$$

der *Zentralisator von x in G.*

Bemerkung 21.10.

(i) Wir nehmen an: G operiert auf S. Seien $x, y \in S$ und $g \in G$. Es gilt:

$$y = gx \Rightarrow Stab_x = g^{-1}(Stab_y)g .$$

(ii) Es folgt: wenn G auf S transitiv operiert, dann gilt:

$$\forall x, y \in S \exists g \in G : Stab_y = g(Stab_x)g^{-1} .$$

Beweis: ÜA □

Beispiel 21.11. [**Transitive Aktion:**]
Sei $H \leq G$ und setze $\overline{G} := \{xH \mid x \in G\}$ die menge der linken Nebenklassen von H in G. Dann operiert G auf $\overline{G}$ durch linke Multiplikation: $g(xH) := (gx)H$. Die Aktion ist transitiv: seien xH und $yH \in \overline{G}$, setze $g = yx^{-1}$. Dann ist $g(xH) = (gx)H = (yx^{-1}x)H = yH$.

Wir zeigen nun, dass bis auf Äquivalenz von Aktionen, alle transitive Aktionen von G auf eine Menge $S \neq \varnothing$ diese Gestalt haben:

Satz 21.12.
Wir nehmen an dass G transitiv auf S operiert. Sei $s \in S$ fest und setze $H := Stab_s$. Dann ist die angegebene transitive Aktion von G auf S äquivalent zur Aktion von G auf $\overline{G} := \{xH \mid x \in G\}$ durch linke Multiplikation.

Beweis:
Definierte $\nu : \overline{G} \to S$ mit $\nu(xH) := xs$. Laut Definition 20.7 müssen wir Folgendes prüfen:

- ν ist wohldefiniert weil $xH = yH$ gdw $y^{-1}x \in H$ gdw $(y^{-1}x)s = s$ gdw $xs = ys$ (*)
- Die Aktion ist transitiv $\Rightarrow \nu$ ist surjektiv.
- ν ist injektiv (auch wegen (*)).
- Wir berechnen: $\nu(g(xH)) = \nu((gx)H) = (gx)s = g(xs) = g\nu(xH)$.

□

Korollar 21.13.
Es sei G eine endliche Gruppe und $S \neq \varnothing$ eine Menge so dass G auf S transitiv operiert. Dann ist $|S| = [G : Stab_s]$ für ein (jedes) $s \in S$. Insbesondere ist S endlich und $|S| \mid |G|$.

Beweis:
Es folgt nun aus Satz 21.12 und Satz 16.2. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir die Bahn Gleichung und die Sylow Sätze beweisen. Damit beenden wir Kapitel 3.

Seien $S \neq \varnothing$ eine Menge, G eine Gruppe, so dass G auf S operiert.

Wir wollen nun Korollar 21.13 für eine beliebige Aktion verallgemeinern:

Korollar 22.1. [Bahngleichung]
Sei S endlich; wähle ein Vertretersystem $\{x_1, \ldots, x_r\}$ der Bahnen. Es gilt

$$|S| = \sum_{i=1}^{r} [G : Stab_{x_i}] .$$

Beweis:
Seien $\mathcal{O}_1, \ldots, \mathcal{O}_r$ alle Bahnen. Es ist leicht zu sehen (s. Bemerkung 21.4), dass die Aktion von G auf $\mathcal{O}_i$ transitiv ist für jedes $i = 1, \ldots, r$. Es folgt aus Korollar 21.13 dass $|\mathcal{O}_i| = [G : Stab_{x_i}]$. Nun ist $S = \bigsqcup_{i=1}^{r} \mathcal{O}_i$, also $|S| = \sum_{i=1}^{r} |\mathcal{O}_i|$. □

Korollar 22.2. [Klassengleichung I]
Sei G endlich; wähle ein Vertretersystem $\{x_1, \ldots, x_k\}$ der Konjugationsklassen von G. Es gilt

$$|G| = \sum_{i=1}^{k} [G : C(x_i)] .$$

Beweis:
G operiert auf G durch die Konjugation κ_j und $Stab_{x_i} = C(x_i)$ per Definition 21.9. Wir können Korollar 22.1 also direkt anwenden. □

Korollar 22.3. [Klassengleichung II]
Sei G endlich; wähle ein Vertretersystem $\{y_1, \ldots, y_\ell\}$ für die Konjugationsklassen in $G \backslash C_G$. Es gilt:

$$|G| = |C_G| + \sum_{i=1}^{\ell} [G : C(y_i)] \qquad (*)$$

Beweis:
Die Konjugationsklasse von x ist $\{x\}$ gdw $x \in C_G$ genau dann, wenn $C(x) = G \quad (**)$
(s. Proposition 21.8). In Korollar 22.2 wird also in der Formel $1 = [G : G] = [G : C(x_i)]$ so oft summiert wie es Elemente in C_G gibt. Also erhalten wir $|C_G|$ als ersten Summand. □

Korollar 22.4.
Sei G endlich, $|G| = p^k, p$ ist Primzahl und $k \in \mathbb{N}$. Es gilt $C_G \neq \{1\}$.

Beweis: Siehe ÜB.

Proposition 22.5. Sei G eine endliche abelsche Gruppe, $p \in \mathbb{N}$ eine Primzahl und $p \mid |G|$. Dann existiert ein $x \in G$ mit $|x| = p$.

Beweis: Siehe ÜB.

Beweise der Sylow-Sätze.

Beweis von Sylow 1:
Sei p Primzahl und $k \in \mathbb{N}$, so dass $p^k \mid |G|$. Wir werden per Induktion nach $|G|$ zeigen dass G eine Teilgruppe H der Ordnung p^k hat.

• $|G| = 2$ ist klar.

• Induktionsannahme: Sylow 1 gilt für alle Gruppen der Ordnung $< |G|$.

• Induktionsschritt: Wir werden Lagrange's Satz, die Klassengleichung II, und Proposition 22.5 (für die abelsche Gruppe $C := C_G$) anwenden.

Zwei Fälle sind zu betrachten:

Fall 1: $p \nmid |C|$. In diesem Fall wegen $(*)$ $\exists j$ mit $p \nmid [G : C(y_j)]$.
Aber $p^k \mid |G|$ und $|G| = [G : C(y_j)] \mid C(y_j) \mid$.
Also $p^k \mid |C(y_j)|$. Wegen $(**)$ ist $|C(y_j)| < |G|$, da $y_j \notin C$ ist.
Induktionsannahme $\Rightarrow C(y_j)$ besitzt eine Teilgruppe der Ordnung p^k. $\square_{Fall1}$

Fall 2: $p \mid |C|$. In diesem Fall liefert Proposition 22.5 ein Element $c \in C$ der Ordnung p.
Nun ist $< c > \trianglelefteq C, | < c > | = p$. Betrachte die Gruppe $G/ < c >$ der Ordnung $\frac{|G|}{|<c>|} = \frac{|G|}{p}$.
Also $p^{k-1} \mid |\frac{G}{<c>}|$. Induktionsannahme $\Rightarrow \exists$ eine Teilgruppe von $G/ < c >$ der Ordnung p^{k-1}.

Nun haben wegen Satz 17.4 die Teilgruppen von $G/ < c >$ die Gestalt $H/ < c >$, wobei $H \leq G$ und $< c > \leq H$. Also existiert $H \leq G$ mit $|\frac{H}{<c>}| = p^{k-1}$. Wir berechnen:
$|H| = |\frac{H}{<c>}| \ | < c > | = p^{k-1} \, p = p^k$. $\square_{Fall2}$ $\square_{Sylow1}$

Wir wollen nun Sylow 2 beweisen.

Bemerkung 22.6. Sei $H \leq G$ und $g \in G$. Dann ist $gHg^{-1} \leq G$. G operiert also durch Konjugation auf $\Gamma :=$ die Menge der Teilgruppen von G. Wir müssen diese Aktion besser verstehen. Für $H \in \Gamma$ berechnen wir:

(i) $Stab_H = \{g \in G \,;\, gHg^{-1} = H\}$. Somit erkennen wir dass $Stab_H = N_G(H)$ der Normalisator von H in G (s. Definition 16.8). Zur Erleichterung der Notation schreiben wir hier $N(H)$ anstatt $N_G(H)$. Wir erinnern dass $H \trianglelefteq N(H)$ (s. Bemerkung 17.1).

(ii) Die Bahnn von H : $\mathcal{O}_H = \{gHg^{-1} \ ; \ g \in G\}$. Korollar 21.13 liefert $|\mathcal{O}_H| = [G : N(H)]$. Da $[G : H] = [G : N(H)][N(H) : H]$, so ist $|\mathcal{O}_H| \mid [G : H]$.

(iii) Wir betrachten diese Aktion auf die Mengen $\Pi \subseteq \Gamma$ der Sylow-p-Untergruppen von G. Die Aktion auf Π ist wohldefiniert, weil $gHg^{-1} \in \Pi$, wenn $H \in \Pi$. (s. Bemerkung 21.4)

Wir bekommen ein Hilfslemma.

Lemma 22.7. (i) Sei $P \in \Pi, H \leq N(P)$ so dass $|H| = p^j$ für ein $j \in \mathbb{N}$. Dann ist $H \leq P$.

(ii) P ist die einzige Sylow-p-Untergruppe von $N(P)$.

Beweis:

$$\left.\begin{array}{ll} H \leq N(P) & \text{und} \\ P \trianglelefteq N(P) & \end{array}\right\} \Rightarrow HP \text{ ist Untergruppe und } HP/P \simeq H/(H \cap P)$$

(Isomorphie-Satz 17.2). Also ist HP/P isomorph zu einer Faktorgruppe von H und damit hat sie die Ordnung $|HP| = p^k$ für ein geeignetes $k \in \mathbb{N}$. Da aber P eine Sylow-p-Untergruppe ist, folgt: $HP = P$, so dass $H \leq P$. Damit haben wir (i) bewiesen, (ii) folgt unmittelbar aus (i). □

Beweis von Sylow 2:
Betrachte eine Bahn $\sum$ für die Aktion in Bemerkung 22.6. Sei $P \in \Pi$, dann operiert P auf die Bahn $\sum$ (s. Bemerkung 21.4). Wir bekommen eine Partition von $\sum$ in P-Bahnen (i.e. Äquivalenzklassen bezüglich dieser Aktion von P auf $\sum$).

Fall 1: Sei $P \in \sum$.

- Betrachte die P-Bahn von P. Die ist offensichtlich $\{P\}$ (weil $xPx^{-1} = P$ für alle $x \in P$).
- Wir behaupten, dass $\{P\}$ die einzige P-Bahn der Kardinalität 1 ist:
  Sei $\{P'\}$ eine P-Bahn. Dann gilt $xP'x^{-1} = P'$ für alle $x \in P$, das heißt $P \leq N(P')$ und Lemma 22.7(ii) liefert $P = P'$ (weil P' die einzige Sylow-p-Untergruppe von $N(P')$ ist und P ist eine Sylow-p-Untergruppe von $N(P')$).
- Beachte, dass jede P-Bahn Kardinalität eine Potenz von p hat, da diese Kardinalität die Kardinalität $|P|$ teilen muss (siehe Korollar 21.13). Also ist $|\sum| \equiv 1 \mod p$.

Dieses beweist die zweite Aussage von Sylow 2 (2).

Nun beweisen wir Sylow 2 (1). Wir müssen zeigen, dass $\sum$ die einzige Bahn für die Aktion in Bemerkung 22.6. Sonst gibt es $P \in \Pi$ mit

Fall 2: $P \notin \sum$.

Analog wie Fall 1 sehen wir, dass es überhaupt keine P-Bahnen der Kardinalität 1 gibt (die einzige Möglichkeit, nämlich $\{P\}$ scheidet nun aus, weil $P \notin \sum$ ist). Also ist $|\sum| \equiv 0 \mod p$ - Widerspruch. So $\sum = \Pi$ und damit ist Sylow 2 (1) bewiesen.

Es ist $|\Pi| = [G : N(P)]$ für alle $P \in \Pi$ (Korollar 21.13). Also ist die Anzahl der Sylow-p-Untergruppen ein Divisor (s. Bemerkung 22.6). Das beweist die erste Aussage in Sylow 2 (2).

Nun beweisen wir Sylow 2 (3). Sei $H \leq G, |H| = p^k$. Betrachte die Aktion von H auf Π. Die H-Bahnen haben Kardinalität ein Divisor von $|H|$ (Korollar 21.13), also haben die H-Bahnen Kardinalität eine Potenz von p.
Nun ist aber $|\Pi| \equiv 1 \mod p$, also gibt es eine H-Bahn $\{P\}$ mit nur einem Element, das heißt $H \leq N(P)$ und damit $H \leq P$ (s. Lemma 22.7 (i)). □