Westfälische Wilhelms-Universität Münster

Fachbereich 10 Mathematik und Informatik

Einführung in die Algebra

Aufarbeitung der Vorlesungsnotizen

Tobias Wedemeier

25. November 2014

gelesen von

Prof. Dr. Kramer

Hierbei handelt es sich um eine Aufarbeitung der Vorlesungsnotizenvon **Prof. Dr. Kramer**, WWU Münster, aus der Vorlesung **Einführung in die Algebra** im Wintersemester 2014/15. Dies ist kein Skript der Vorlesung und keine eigene Arbeit des Autors.

Für Fehler in der Aufarbeitung wird keine Haftung übernommen. Hinweise auf Fehler sind gerne gesehen, hierfür kann man mich in der Uni ansprechen oder alternativ eine e-Mail an:
tobias.wedemeier@gmx.de
Auch ist eine Mitarbeit über Github möglich.

Wenn Teile aus der Vorlesung selber fehlen, können diese gerne an meine e-Mail versandt werden. Ich werde diese dann einarbeiten.

Eine Aufarbeitung der Übungen ist ebenfalls existent, diese sind auch in der Dropbox oder bei Github zu finden.

Inhaltsverzeichnis

1 Elementare Gruppentheorie

Erinnerung: eine **Verknüpfung** auf einer nicht leeren Menge X ist eine Abbildung

$$X \times X \to X, (x,y) \mapsto m(x,y).$$

Häufig schreibt man $m(x,y) = x \cdot y$ oder $m(x,y) = x + y$, je nach Kontext. Die Schreibweise $m(x,y) = x + y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn $\forall x, y \in X$ gilt $m(x,y) = m(y,x)$.

1.1 Definition Gruppe

Eine **Gruppe** $(G, \cdot)$ besteht aus einer Verknüpfung $\cdot$ auf einer nicht leeren Menge G, mit folgenden Eigenschaften:

(G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt $\forall x, y, z \in G$.
(Folglich darf man Klammern weglassen.)

(G2) Es gibt ein neutrales Element $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x \forall x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $xy = e = yx$.
man schreibt dann auch $y = x^{-1}$ für das Inverse zu x.

Fordert man von der Verknüpfung nur (G1) und (G2), so spricht man von einer Halbgruppe mit Eins oder einem **Monoid**. Fordert man nur (G1), so spricht man von einer **Halbgruppe**.

1.2 Beispiel 1

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind kommutative Gruppen.
- $(\mathbb{Z}, \cdot), (\mathbb{N}, \cdot), (\mathbb{N}, +)$ sind Monoide.

1.3 Beobachtungen

a) Das Neutraleelement (einer Verknüpfung) ist eindeutig bestimmt: sind e, e' beides Neutralelemente, so folgt: $e = ee' = e'$

b) Das Inverse zu x ist eindeutig bestimmt:
$xy = e = xy' = y'x \Rightarrow y' = y'e = y'xy = ey = y$

1.4 Lemma 1 (Sparsame Definition von Gruppen)

Sei $G \times G \to G$ eine assoziative Verknüpfung. Dann ist G schon eine Gruppe, wenn gilt:

(i) es gibt $e \in G$ so, dass $ex = x \ \forall x \in G$ gilt.

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$

Beweis
Sei $yx = e$, es folgt $yxy = y$. Wähle z mit $zy = e$, es folgt $z \underbrace{yx}_{=e} y = zy = e \Rightarrow xy = e$

Weiter gilt $xe = xyx = ex = x$. □

1.5 Beispiel 2

Sei X eine nicht leere Menge, sei $X^X = \{f : X \to X\}$ die Menge aller Abbildungen von X nach X. Als Verknüpfung auf X nehmen wir die Komposition von Abbildungen. Dann gilt wegen $f = \mathrm{id}_X \circ f = f \circ \mathrm{id}_X$, dass id_X ein Neutralelement ist.
Damit haben wir ein Monoid $(X_X, \circ)$.
Sei $\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ bijektiv}\}$. Zu jedem $f \in \mathrm{Sym}(X)$ gibt es also eine Umkehrabbildung $g : X \to X$ mit $f \circ g = g \circ f = \mathrm{id}_X$. Folglich ist $(\mathrm{Sym}(X), \circ)$ eine Gruppe, die **Symmetrische Gruppe**.
Wenn X endlich ist mit n Elementen, so gibt es genau $n! = n(n-1)(n-2)\cdot \dots \cdot 2 \cdot 1$ Permutationen, also hat $\mathrm{Sym}(X)$ dann genau $n!$ Elemente.
Für $X = \{1, 2, 3, \dots, n\}$ schreibt man auch $\mathrm{Sym}(X) = \mathrm{Sym}(n)\big(= S_n\big)$.

1.6 Definition zentralisieren

Sei $G \times G \to G$ eine Verknüpfung. Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder x **zentralisiert** y, wenn gilt $xy = yx$.
Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder **abelsch**.

1.7 Beispiel 3

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdot)$ sind abelsche Gruppen.

(b) K Körper, $G = Gl_2(K) = \{X \in K^{2\times 2} \mid \det(X) \neq 0\}$ Gruppe der invertierbaren 2×2 Matrizen.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$\Rightarrow$ nicht abelsch, genauso $Gl_n(K)$ für $n \geq 2$.

(c) $\mathrm{Sym}(2)$ ist abelsch, aber $\mathrm{Sym}(3)$ nicht. Allgemein ist $\mathrm{Sym}(X)$ nicht abelsch, falls $\#X \geq 3$ gilt.

1.8 Definition Untergruppe

Sei G eine Gruppe, sei $H \subseteq G$. Wir nennen H **Untergruppe** von G, wenn gilt:

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offensichtlich ist eine Untergruppe dann wieder eine Gruppe, mit der von G vererbten Verknüpfung.

Bsp

(a) $(\mathbb{Q}, +)$. $\mathbb{Z}$ ist Untergruppe, denn $0 \in \mathbb{Z}, m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}$ und $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

(b) $(\mathbb{Q}^*, \cdot)$. $\mathbb{Z}^*$ ist keine Untergruppe, kein Inverses.

1.9 Lemma 2

Sei G eine Gruppe und sei U eine nicht leere Menge von Untergruppen von G. Dann ist auch
$\bigcap U = \{g \in G \mid \forall H \in U \text{ gilt } g \in H\}$
eine Untergruppe von G.

Beweis
Für alle $H \in U$ gilt $e \in H$, also $e \in \bigcap U$. Angenommen $x, y \in \bigcap U$. Dann gilt für alle $H \in U$, dass $xy \in H$ sowie $x^{-1} \in H$. Es folgt $xy \in \bigcap U$ sowie $x^{-1} \in \bigcap U$. $\square$

1.10 Definition $\langle X \rangle$

Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Wir setzen:

$$\langle X \rangle = \bigcap \{H \subseteq G | H \text{ Untergruppe und } X \subseteq H\}$$

Ist nicht leer, da mindestens G enthalten ist.

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insb. also $\langle H \rangle = H$.

Satz

Sei $X \subseteq G$ und sei $W = \{x_1 \cdot x_2, \cdots x_s | s \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \ \forall i = 1, \ldots, s\}$.
Dann gilt: $\langle X \rangle = \{e\} \cup W$.

Beweis
Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $fg \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von G, mit $X \subseteq H$. Es folgt $\langle X \rangle \subseteq H = \{e\} \cup W$. $\square$

1.11 Definition zyklische Gruppe

Sei G eine Gruppe und sei $g \in G$. Für $n \geq 1$ setze $g^n = \underbrace{g \cdots g}_{n-mal}$ sowie $g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{n-mal}$ und $g^0 = e$.

Dann gilt $\forall k, l \in \mathbb{Z}$, dass $g^k \cdot g^l = g^{k+l}$.
Sei $\langle g \rangle = \langle \{g\} \rangle \overset{1.10}{=} \{g^n | n \in \mathbb{Z}\}$. Man nennt $\langle g \rangle$ die von g erzeugte **zyklische Gruppe**. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt n ein **Exponent** von g. Die **Ordnung** von g ist der kleinste Exponent von g,

$$o(g) = \min\left(\{n \geq 1 | g^n = 1\} \cup \{\infty\}\right)$$

$o(g) = \infty$ bedeutet: $g^n \neq e \ \forall n \geq 1$
$o(g) = 1$ bedeutet: $g^n = g = e$

1.12 Zyklische Gruppen

Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: zyklische Gruppen sind abelsch.

Satz

Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^1, g^2, g^3, \dots, g^n\}$.

Beweis
Jedes $m \in \mathbb{Z}$ lässt sich schreiben als $m = kn+l$ mit $0 \leq l < n$ (Teilen mit Rest), also $g^m = \underbrace{g^{kn}}_{=e}.g^l = g^l$.

Es folgt $G \subseteq \{g, g^2, \dots, g^n\}, g^n = g^0$. Ist $g^k = g^l$ für $0 \leq k \leq l < n$, so gilt $e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen $l < n$), also $\#\{g, g^2, \dots, g^n = g^0\} = n$. □

Folgerung

Ist G endlich mit $\#G = n$ und ist $h \in G$ mit $o(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann G eine zyklische Gruppe.

1.13 Nebenklassen

Sei G eine Gruppe und sei H eine Untergruppe. Sei $a \in G$. Wir definieren:

$$aH = \{ah | h \in H\} \subseteq G$$

$$Ha = \{ha | h \in H\} \subseteq G$$

Man nennt aH die **Linksnebenklassen** von a bzgl. H (und Ha die **Rechtsnebenklassen**). In nicht abelschen Gruppen gilt im allgemeinen $aH \neq Ha$.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G und $a, b \in G$.
Dann sind äquivalent:

(i) $b \in aH$

(ii) $bH = aH$

(iii) $bH \cap aH \neq \emptyset$

Beweis

- $(i) \Rightarrow (ii):\ b \in aH \Rightarrow b = ah$ für ein $h \in H \Rightarrow bH = \{ahh' | h' \in H\}$ $\overset{H \text{ Untergruppe}}{=} \{ah'' | h'' \in H\} = aH$
- $(ii) \Rightarrow (iii)$: klar
- $(iii) \Rightarrow (i)$: Sei $g \in bH \cap aH,\ g = bh = ah' \Rightarrow b = ah'h^{-1} \in aH$, da H Untergruppe

□

Folgerung

Jedes $g \in G$ liegt in genau einer Linksnebenklasse bzgl. H, nämlich $g \in gH$. Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt:
${}^{G}/_{H} = \{gH \mid g \in G\}$ Menge der Linksnebenklasse, Rechtsnebenklassen analog.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G, sei $a \in G$.
Dann ist die Abbildung $H \to gH, h \mapsto gH$ bijektiv.

Beweis
'Surjektiv' ist klar nach Definition von gH. Angenommen, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$ $\square$

1.14 Satz 1, Satz von Lagrange

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wenn zwei der drei Mengen $G, H, G/H$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt:

$$\#G = \#H \cdot \#G/H$$

Insbesondere ist dann $\#H$ eine **Teiler** von $\#G$.

Beweis
Wenn G endlich ist, dann sind auch H und G/H endlich.
Angenommen, G/H und H sind endlich. Dann ist auch $G = \bigcup G/H = \bigcup\{gH \mid gH \in G/H\}$ endlich, da $\#gH = \#H$ nach 1.13.
Jetzt zählen wir genauer: sei $\#G/H = m; \#H = n$ etwa $G/H = \{g_1H, g_2H, \dots g_mH\}$.
$g_iH \overset{1.13}{=} n \qquad g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach 1.13.
$G = g_1 \cap g_2H \cap \dots \cap g_mH \Rightarrow \#G = m \cdot n$ $\square$

Bemerkung

(1) Eine entsprechende Aussage gilt für Rechtsnebenklassen.

(2) Die Abbildung $G \to G, \quad g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} \overset{\text{Achtung!}}{=} \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1} \qquad \text{(ÜA)}$$

Korollar A (Lagrange)

Sei G eine endliche Gruppe und sei $g \in G$. Dann teilt $o(g)$ die Zahl $\#G$.

Beweis
Da G endlich ist, folgt $o(g) < \infty$. Nach dem Satz von Lagrange ist $\#\langle g\rangle = o(g)$ ein Teiler von $\#G$. $\square$

Korollar B

Sei G eine endliche Gruppe, sei p eine **Primzahl** (d.h. die einzigen Teiler von p sind 1 und p) und $p > 1$. Wenn gilt $\#G = p$, dann ist G zyklisch. Für jedes $g \in G \backslash \{e\}$ gilt $\langle g\rangle = G$.

Beweis
Sei $g \in G\backslash\{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt p. Es folgt $o(g) = p$, also $G = \langle g\rangle$ vgl. 1.12. $\square$
Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.
Die Zahl $\#G/H := [G : H]$ nennt man auch den **Index von H in G**.

Wichtige Rechenregeln in Gruppen

(a) Man darf kürzen

$$ax = ay \Rightarrow x = y$$
$$xa = ya \Rightarrow x = y$$

(multipliziere beide Seiten von links/rechts mit a^{-1})

(b) Es gilt $(x^{-1})^{-1} = x$ $(x^{-1}x = e = xx^{-1} \Rightarrow (x^{-1})^{-1} = x)$

(c) Beim Invertieren darf die Reihenfolge umgedreht werden:

$$(ab)^{-1} = b^{-1}a^{-1} \left(ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab \Rightarrow (ab)^{-1} = b^{-1}a^{-1}\right)$$

(in abelschen Gruppen gilt natürlich damit $(ab)^{-1} = a^{-1}b^{-1}$)

1.15 Homomorphismen

Seien G, K Gruppen. Eine Abbildung $\varphi : G \to K$ heißt **(Gruppen-)Homomorphismus**, wenn $\forall x, y \in G$ gilt

$$\varphi \underbrace{(x \cdot y)}_{\text{Verküpfung in G}} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verknüpfung in K}}$$

Bsp

(a) $id_G : G \to G$ ist Homomorphismus

(b) $H \subseteq G$ Untergruppe $i : H \hookrightarrow G, \quad h \mapsto h$ Inklusion, ist Homomorphismus.

(c) $(G, \cdot) = (\mathbb{Z}, +)$ $m \in \mathbb{Z}$ $\varphi : \mathbb{Z} \to \mathbb{Z}, x \mapsto mx$ ist Homomorphismus, denn $\phi(x + y) = m(x + y) = mx + my = \varphi(x) + \varphi(y)$

(d) G Gruppe, $a \in G,\ a \neq e,\ \ \lambda_a(x) = ax$.
$\lambda : G \to G$ ist kein Homomorphismus, denn $\lambda_a(e) = a, \lambda(ee) = a$, aber $\lambda_a(e)\lambda_a(e) = aa \neq a$

Lemma

Sei $\varphi : G \to K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1}$ $\forall x \in G$. (e_G Neutralelement in G und e_K Neutralelement in K)

Beweis

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \overset{\text{kürzen}}{\Rightarrow} e_K = \varphi(e_G)$$

$$e_K = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$$

□

Achtung: $\varphi(x)^{-1}$ ist das Inverse in K von $\varphi(x)$ nicht die Umkehrabbildung!

Das **Bild** eines Homomorphismus $\varphi : G \to K$ ist $\varphi(G) \subseteq K$,
der **Kern** ist $ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\} \subseteq G$

1.16 Satz 2, Gruppenhomomorphismen

Bild und Kern von Gruppenhomomorphismen sind Untergruppen.

Beweis
Setze $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ gilt $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist H Untergruppe. Betrachte jetzt $ker(\varphi) \subseteq G$. Es gilt $\varphi(e_G) = e_K$, also $e_G \in ker(\varphi)$. Ist $x, y \in ker(\varphi)$, so folgt

$$\varphi(xy) = \varphi(x)\varphi(y) = e_K \cdot e_K = e_K \text{ , also } xy \in ker(\varphi)$$

$$\varphi(x^{-1}) = \varphi(x)^{-1} = e_K^{-1} = e_K \text{ , also } x^{-1} \in ker(\varphi)$$

□

Bemerkung:
Jede Untergruppe von $H \subseteq G$ ist Bild eine geeigneten Homomorphismus (nämlich der Inklusion $H \hookrightarrow G$). Wir werden sehen, dass im allgemeinen nicht jede Untergruppe $H \subseteq G$ Kern eines Homomorphismus ist.

1.17 Normalteiler

Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Wir nennen N **normal** in G oder **Normalteiler** in G, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) für alle $a \in G$ gilt $aN = Na$ (Rechtsnebenklassen sind Linksnebenklassen)

(ii) für alle $a \in G$ gilt $aNa^{-1} = N(aNa^{-1} = \{ana^{-1} \mid n \in N\})$

(iii) für alle $a \in G$ gilt $aN \subseteq Na$

(iv) für alle $a \in G$ gilt $aNa^{-1} \subseteq N$

Beweis:
(i) und (ii) sind äquivalent: multipliziere von rechts mit a^{-1} bzw. a. Genauso sind (iii) und (iv) äquivalent.
Klar: (ii) $\Rightarrow$ (iv) (✓)
Zeige (iv) $\Rightarrow$ (ii): Setze $b = a^{-1}$, es folgt aus (iv), dass $bNb^{-1} \subseteq N \rightsquigarrow N \subseteq b^{-1}Nb = aNa^{-1}$. Also gilt für alle $a \in G$, dass $N \subseteq aNa^{-1}$ und $aNa^{-1} \subseteq N$, damit gilt (ii) □

Lemma

Ist $\varphi : G \to K$ ein Homomorphismus von Gruppen, dann ist $ker(\varphi)$ ein Normalteiler in G.

Beweis:
Sei $N = ker(\varphi) = \{n \in G \mid \varphi(n) = e\}$, sei $a \in G$. Dann gilt

$$\varphi(ana^{-1}) = \varphi(a)\underbrace{\varphi(n)}_{=e}\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e$$

also gilt $aNa^{-1} \subseteq N \quad \forall a \in G$. □

Achtung:
Bilder von Homomorphismen sind nicht immer Normalteiler, nach Beispiel 1.15 (b) ist jede Untergruppe Bild eines Homomorphismus, aber nicht jede Untergruppe ist normal.

Beispiel:
$G = Sym(3)$, $g = (1,2)$ Transposition, die 1 und 2 vertauscht. $g^2 = id$, $\langle g\rangle = \{g, id\} \subseteq \mathrm{Sym}(3)$ ist Untergruppe, aber für $h = (2,3)$ gilt

$$h\langle g\rangle h^{-1} = \{hgh^{-1}, h\ id\ h^{-1}\} = \{\underbrace{(2,3)(1,2)(2,3)}_{=(3,1)}, id\} \not\subseteq \langle g\rangle$$

also ist $\langle g\rangle$ kein Normalteiler in $\mathrm{Sym}(3)$.

<u>**Schreibweise:**</u> Ist $N \subseteq G$ ein Normalteiler, schreibt man kurz $N \trianglelefteq G$

<u>**Beachte:**</u> Ist G <u>abelsch</u>, dann sind alle Untergruppen $H \subseteq G$ automatisch normal.

1.18 Definition Teilmengen assoziativ

Für Teilmengen $X, Y, Z \subseteq G$ in einer Gruppe schreibe kurz:

$$XY = \{xy \mid x \in X,\ y \in Y\} \subseteq G$$
$$X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G$$

Es gilt dann $(XY)Z = X(YZ)$, (weil die Verknüpfung assoziativ ist).

Satz

Sei $N \trianglelefteq G$ Normalteiler in der Gruppe G. Dann ist $G/N = \{gN \mid g \in G\}$ eine Gruppe mit der Verknüpfung $(gN) \cdot (hN) = ghN$
Das Neutralelement ist $eN = N$, das Inverse zu gN ist $g^{-1}N$.
<u>**Beweis:**</u>
Da N Normalteiler ist, gilt für $g, h \in G$

$$gNhN = g(Nh)N \overset{1.17}{=} g(hN)N = ghNN \overset{N\ \text{Gruppe}}{=} ghN$$

Die Verknüpfung ist also einfach gegeben durch

$$gN \cdot hN = gNhN = ghN$$

und damit assoziativ nach obiger Bemerkung. Es gilt $NgN = gNN = gN = gNN$, also ist N ein Neutralelement. Weiter gilt:

$$gNg^{-1}N = gg^{-1}N = N = g^{-1}gN = g^{-1}NgN$$

□

1.19 Definition π_H

Ist G eine Gruppe und H eine Untergruppe, so definieren wir $\pi_H : G \to G/H$ durch $\pi_H(g) = gH$.

Satz

Ist $N \trianglelefteq G$ ein Normalteiler, dann ist $\pi_N : G \to G/N$ ein surjektiver Homomorphismus mit Kern $N = ker(\pi_N)$.
<u>**Beweis:**</u>
π_N ist nach Definition surjektiv und

$$\pi_N(gh) = ghN = gNhN = \pi_N(g)\pi_N(h)$$

Weiter gilt

$$\pi_N(g) = N \Longleftrightarrow gN = N \overset{1.13}{\Longleftrightarrow} g \in N$$

$\square$

Folgerung:
Jeder Normalteiler ist auch ein Kern eines Homomorphismus.

1.20 Der Homomorphiesatz

Sei $G \xrightarrow{\varphi} K$ ein Homomorphismus von Gruppen, sei $N \trianglelefteq G$ ein Normalteiler. Wenn gilt $N \subseteq ker(\varphi)$, dann gibt es <u>genau einen</u> Homomorphismus $\overline{\varphi} : {}^{G}/_{H} \to K$ mit $\overline{\varphi} \circ \pi_H = \varphi$.

$$\begin{tikzcd}
G \arrow[rr, "\varphi"] \arrow[dr, "\pi_N"'] & & K \\
& {}^{G}/_{N} \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

Abbildung 1: Homomorphiesatz

<u>**Beweis:**</u>
<u>Existenz von $\overline{\varphi}$:</u>
Für $g \in G$ setze $\overline{\varphi}(gN) = \varphi(g)$. Das ist eine wohldefinierte Abbildung, denn angenommen,

$$gN = g'N \Rightarrow g^{-1}g' \in N \subseteq ker(\varphi) \Rightarrow \varphi(g^{-1}g') = e \Rightarrow \varphi(g) = \varphi(g')$$

Es gilt damit

$$\overline{\varphi}(gNhN) = \overline{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(gN)\overline{\varphi}(hN)$$

also ist $\overline{\varphi}$ ein Homomorphismus.

<u>Eindeutigkeit von $\overline{\varphi}$:</u>
Sei $\psi : {}^{G}/_{N} \to K$ ein Homomorphismus mit $\psi \circ \pi_N = \varphi$.
Es folgt

$$\psi(gN) = \psi(\pi_N(g)) = \varphi(g) = \overline{\varphi}(gN) \quad \forall g \in G$$

Bemerkung:
In der Situation vom Homomorphiesatz gilt:

(i) $ker(\varphi) = \pi_N^{-1}\ ker(\overline{\varphi})$

(ii) $ker(\overline{\varphi}) = \pi_N\ ker(\varphi)$

(iii) $\varphi(G) = \overline{\varphi}({}^{G}/_{N})$

<u>**Beweis:**</u>
(iii) ist klar nach Konstruktion, $\overline{\varphi}(gN) = \varphi(g)$
(ii) $\overline{\varphi}(gN) = e = \varphi(g) \Leftrightarrow g \in ker(\varphi)$, also $ker(\overline{\varphi}) = \pi_N(ker(\varphi))$
(i) $\varphi(g) = e \Rightarrow g \in ker(\varphi) \Rightarrow \pi_N(g) \in ker(\overline{\varphi}) \Rightarrow \varphi(g) = e$ $\square$

1.21 Definition Isomorphismus

Ein Gruppenhomomorphismus $\varphi : G \to K$ heißt <u>**Mono/Epi/Isomorphismus**</u>, wenn φ <u>injektiv/surjektiv/bijektiv</u> ist.
(Klar: φ Epimorphismus $\Leftrightarrow \varphi(G) = K$)
Für einen Mono / Epi / Isomorphismus schreibt man auch:
$\overset{\varphi}{\rightarrowtail}$ $\overset{\varphi}{\twoheadrightarrow}$ und $\overset{\cong}{\to}$.

Lemma

Ein Gruppenhomomorphismus $G \xrightarrow{\varphi} K$ ist genau dann injektiv, wenn gilt $ker(\varphi) = \{e_G\}$.

Beweis:
Wenn φ injektiv ist, dann ist $ker(\varphi) = \{e_G\}$ (klar). Angenommen, $ker(\varphi) = \{e_G\}$ und $a, b \in G$ mit $\varphi(a) = \varphi(b) \rightsquigarrow \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = e_K \Rightarrow ab^{-1} = e_G \Rightarrow a = b$ $\square$

1.22 Satz 3, Eigenschaften von Gruppenhomomorphismen

Sei $G \xrightarrow{\varphi} K$ ein Gruppenhomomorphismus. Dann gilt folgendes:

(i) Ist $H \subseteq G$ Untergruppe, so ist $\varphi(H) \subseteq G$ Untergruppe. Wenn $H \trianglelefteq G$, so gilt $\varphi(H) \trianglelefteq \varphi(G)$

(ii) Ist $L \subseteq K$ Untergruppe, so ist $\varphi^{-1}(L) \subseteq G$ Untergruppe. Ist $L \trianglelefteq K$, so gilt $\varphi^{-1}(L) \trianglelefteq G$.

Beweis:

(i) Sei $a, b \in H$ und $g \in G$. Es gilt $\varphi(a)\varphi(b) = \varphi(ab) \in H$, $\quad \varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$. $\varphi(e_G) = e_K \in \varphi(H) \Rightarrow \varphi(H)$ Untergruppe.
Ist $H \trianglelefteq G$, so folgt $\varphi(g)\varphi(H)\varphi(g)^{-1} = \varphi(gHg^{-1}) \overset{H \trianglelefteq G}{=} \varphi(H)$ $\square$

(ii) Sei $a, b \in \varphi^{-1}(L)$, $\quad g \in G$ (also $\varphi(a), \varphi(b) \in L$). Es folgt $\varphi(ab) \in L$, $\quad \varphi(a^{-1}) = \varphi(a)^{-1} \in L$ und $\varphi(e_G) = e_K \Rightarrow ab, a^{-1}, e_G \in \varphi^{-1}(L) \rightsquigarrow$ Untergruppe.
Angenommen, $L \trianglelefteq K$.
Es folgt $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) \in L$, also $g\varphi^{-1}(L)g^{-1} \subseteq \varphi^{-1}(L)$. $\square$

Beispiele
Gruppe $(\mathbb{Z}, +)$, $\varphi : \mathbb{Z} \to \mathbb{Z}$ Homomorphismus, $\varphi(z) = m \cdot z$, $m \in \mathbb{Z}$ fest.
$\varphi(\mathbb{Z}) = m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\} = (-m)\mathbb{Z}$
z.B. $m = 2 \;\rightsquigarrow 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ gerade Zahlen
$ker(\varphi) = \begin{cases} \{0\}, & \text{wenn } m \neq 0 \\ \mathbb{Z}, & \text{wenn } m = 0. \end{cases}$ $\quad \varphi$ surjektiv $\Leftrightarrow \quad m = \pm 1$
φ injektiv $\Leftrightarrow \quad m \neq 0$

Angenommen, $m > 0$, $a, b \in \mathbb{Z}$
$a + m\mathbb{Z} = b + m\mathbb{Z}$ Nebenklassen $\overset{1.13}{\Leftrightarrow} a \in b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$
Folglich $\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$ insbesondere $\#\mathbb{Z}/m\mathbb{Z} = m$.
Schreibe $\overline{k} = k + m\mathbb{Z}$ **Kongruenzklasse** von k **modulo** m.
$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ wird erzeugt von $\overline{1} \rightsquigarrow \mathbb{Z}/m\mathbb{Z} = \langle \overline{1} \rangle$ zyklische Gruppe der Ordnung m. $o(\overline{1}) = m$.
Später mehr dazu.

1.23 Die Isomorphiesätze

Lemma

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen. Wenn $N \trianglelefteq G$ gilt, dann ist $HN = NH \subseteq G$ eine Untergruppe.

Beweis:
Es gilt $e = e \cdot e \in N \cdot H$. Weiter gilt für $h_1, h_2 \in H$, $\quad n_1, n_2 \in N$, dass

$$h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{h_2^{-1} n_1 h_2}_{\in N} n_2 \in HN$$

$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}\underbrace{h_1n_1^{-1}h_1^{-1}}_{\in N} \in HN$$

$$(HN)^{-1} = N^{-1}H^{-1} = NH \subseteq HN \text{ genauso } HN \subseteq NH$$

□

Satz

Sei $G \overset{\varphi}{\to} K$ ein Epimorphismus von Gruppen. Sei $N = ker(\varphi)$. Dann ist die Abbildung $\overline{\varphi} : G/N \to K$ aus dem Homomorphisatz 1.20 ein Isomorphismus.

Beweis:
$\overline{\varphi}(G/N) = \varphi(G)$ und $ker(\overline{\varphi}) = \{N\}$ nach dem Beweis von 1.20. Den Isomorphismus $\overline{\varphi} : G/ker(\varphi) \overset{\cong}{\to} K$ nennt man **kanonisch** oder **natürlich**.

Theorem: 1. Isomorphiesatz

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen mit $N \trianglelefteq G$. Dann gilt $H \cap N \trianglelefteq H$, $N \trianglelefteq NH$ und die Abbildung

$$H/H\cap N \to NH/N$$
$$aH \mapsto aNH$$

ist ein Isomorphismus. ("Kürzungsregel")

Beweis:
Für alle $h \in H$ gilt $h(H \cap N)h^{-1} \subseteq N \cap H$ weile $N \trianglelefteq G$ und $hHh^{-1} = H$. $\Rightarrow N \cap H \trianglelefteq H$. Für alle $g \in NH$ gilt $gNg^{-1} \subseteq N \Rightarrow N \trianglelefteq NH$ □

Lemma

Sei $G \overset{\varphi}{\to} K$ ein Gruppenhomomorphismus. Dann sind äquivalent:

(i) φ ist bijektiv

(ii) es gibt ein Homomorphismus $\psi : K \to G$ mit $\varphi \circ \psi = \mathrm{id}_K$ und $\psi \circ \varphi = \mathrm{id}_G$.

Beweis:
(ii)⇒(i): klar, aus $\varphi \circ \psi = \mathrm{id}_K$ folgt, dass φ surjektiv ist und aus $\varphi \circ \psi = \mathrm{id}_G$ folgt, dass φ injektiv ist.

(i)⇒(ii): Sei $\psi : K \to G$ die eindeutig bestimmte Umkehrabbildung, also $\varphi \circ \psi = \mathrm{id}_K$ und $\psi \circ \varphi = \mathrm{id}_G$. Für $a, b \in K$ folgt $\psi(ab) = \psi(\varphi\psi(a)\varphi\psi(b)) \overset{\varphi \text{ Homo.}}{=} \underbrace{\psi(\varphi}_{\mathrm{id}}(\psi(a)\psi(b))) = \psi(a)\psi(b)$ □ Betrachte die

Abbildung $\varphi : H \to HN/N \subseteq G/N,\ h \mapsto hN$ das ist ein Homomorphismus, weil $H \overset{i}{\to} G \overset{\pi_N}{\to} G/N$ einer ist. Für $hn \in HN$ gilt $\varphi(h) = hN = hnN$, also ist φ ein Epimorphismus. Der Kern ist $ker(\varphi) = \{h \in H \mid hN = N\} = H \cap N$. Also gilt nach dem vorigem Satz

$$H/n\cap H \xrightarrow[\cong]{\overline{\varphi}} HN/N$$

□

Theorem: 2. Isomorphiesatz

Sei G Gruppe, seien $M, N \trianglelefteq G$ Normalteiler mit $M \subseteq N \subseteq G$. Dann gilt ${}^{N}/_{M} \trianglelefteq {}^{G}/_{M}$ und

$$ {}^{{}^{G}/_{M}}/_{{}^{N}/_{M}} \cong {}^{G}/_{N} \qquad \text{'Kürzungsregel'} $$

Beweis:
Es gilt ${}^{N}/_{M} = \{nM \mid n \in N\} = \pi_M(N) \subseteq {}^{G}/_{M}$
Nach1.22(i) gilt ${}^{N}/_{M} \trianglelefteq {}^{G}/_{M}$.
Jetzt Homomorphiesatz 1.20

$$\begin{tikzcd} G \arrow[rr, "\pi_N"] \arrow[dr, "\pi_M"'] & & K \\ & {}^{G}/_{N} \arrow[ur, "\overline{\pi_N}\leftarrow\text{surjektiv}"'] & \end{tikzcd}$$

Abbildung 2: 2. Isomorphiesatz

Nach dem vorigen Satz gilt:

$$ {}^{{}^{G}/_{M}}/_{ker(\overline{\pi_N})} \overset{\cong}{\to} {}^{G}/_{N} $$
$$ ker(\overline{\pi_N}) \overset{1.20}{=} \pi_M(N) = {}^{N}/_{M} $$

□

1.24 Produkte von Gruppen

Seien G, K zwei Gruppen. Dann ist das Produkt $G \times K$ wieder eine Gruppe das **direkte Produkt**, mit Verknüpfung

$$ (g_1, k_1) \cdot (g_2, k_2) = (g_1 g_2, k_1 k_2) $$
$$ \text{Neutralelement } e = (e_G, e_K) $$
$$ \text{Das Inverse zu } (g,k) \in G \times K \text{ ist } (g,k)^{-1} = (g^{-1}, k^{-1}) $$

Den Beweis lassen wir weg, die Gruppenaxiome (G1)-(G3) sind leicht zu prüfen.
Wir haben kanonische Homomorphismen:

$$ \begin{aligned} i_G : G &\to G \times K \\ g &\mapsto (g, e_K) \end{aligned} \qquad\qquad \begin{aligned} i_K : K &\to G \times K \\ k &\mapsto (e_G, k) \end{aligned} $$

sowie

$$ pr_G : G \times K \to G, \quad (g,k) \mapsto g $$
$$ pr_K : G \times K \to K, \quad (g,k) \mapsto k $$

mit

$$ pr_G \circ i_G = \mathrm{id}_G \qquad pr_K \circ i_K = \mathrm{id}_K $$
$$ ker(pr_G) = \{e_G\} \times K \cong K \qquad ker(pr_K) = G \times \{e_K\} \cong G $$

Das geht auch mit Familien von (endliche vielen) Gruppen: ist $(G_i)_{i \in I}$ eine Familie von Gruppen, so ist $\prod\limits_{i \in I} G_i$ wieder eine Gruppe, das **direkte Produkt** der G_i. Die Elemente sind Folgen $(g_i)_{i \in I},\ g_i \in G_i$ mit Verknüpfung $(g_i)_{i \in I} \cdot (g_i')_{i \in I} = (g_i g_i')_{i \in I}$ usw.

Satz
Sei G eine Gruppe mit Untergruppe $H, K \subseteq G$.Angenommen, es gilt folgendes

(i) $G = HK$

(ii) $H \cap K = \{e\}$

(iii) $hk = kh \quad \forall h \in H,\ k \in K$

Dann ist die Abbildung $H \times K \stackrel{\varphi}{\to} G$, $(h,k) \mapsto hk$ ein Isomorphismus, d.h. G 'ist' das direkte Produkt aus H und K.
Beweis:
Wegen (iii) gilt

$$\varphi((h_1,k_1)(h_2,k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2$$
$$\varphi(h_1,k_1)\varphi(h_2,k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2$$

also ist φ ein Homomorphismus. Wegen (i) ist φ surjektiv.

$$(h,k) \in ker(\varphi) \Leftrightarrow hk = e \Leftrightarrow \underbrace{h}_{\in H} = \underbrace{k^{-1}}_{\in K} \Leftrightarrow h = k = e \text{ wegen (ii)}$$

□

Beispiel
$G = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \ldots, \overline{5}\}$ vgl. 1.22.Dann sind $H = \{\overline{0}, \overline{3}\}$ sowie $K = \{\overline{0}, \overline{2}, \overline{4}\}$ Untergruppen (nachrechnen!), $H \cong \mathbb{Z}/2\mathbb{Z},\ K \cong \mathbb{Z}/3\mathbb{Z}$ und (i),(ii),(iii) aus dem vorigen Satz sind erfüllt. Es folgt

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

2 Gruppenwirkungen und Sylow-Sätze

2.1 Gruppenwirkungen

Sei G eine Gruppe und X eine nicht leere Menge. Eine **Wirkung** von G auf X (auch: G-**Wirkung**, **'G-Aktion'**) ist ein Homomorphismus $\alpha : G \to \mathrm{Sym}(X)$. Für $g \in G$ und $x \in X$ schreibe kurz

$$g(x) = \alpha(g)(x)$$

(wenn klar ist welches α gemeint ist). Die Abbildung $G \times X \to X, \quad (g, x) \mapsto g(x)$ erfüllt folgende Eigenschaften:

(W1) $e(x) = x \; \forall x \in X$ ($e \in G$ Neutralelement)

(W2) $(a \circ b)(x) = a(b(x)) \; \forall a, b \in G, \; x \in X$

Ist umgekehrt eine Abbildung $G \times X \to X$ gegeben die (W1) und (W2) erfüllt, so erhalten wir eine Wirkung $\alpha : G \to Sym(X)$ durch

$$\alpha(g) = [x \mapsto g(x)]$$

denn aus (W2) folgt: $\alpha(g^{-1})$ ist Inverse zu $\alpha(g)$, also ist die Abbildung $\alpha(g) : X \to X$ bijektiv und $\alpha : G \to Sym(X)$ ist ein Homomorphismus nach (W2).

2.2 Mehrere Definitionen

Gegeben sei eine G-Wirkung $G \times X \to X$. Für $x \in X$ ist der **Stabilisator** (die **Standgruppe**)

$$G_x = \{g \in G \mid g(x) = x\} \subseteq G$$

Die **Bahn** (der **Orbit**) von x ist

$$G(x) = \{g(x) \mid g \in G\} \subseteq X$$

Der Kern der Wirkung ist $\bigcap\limits_{x \in X} G_x \subseteq G$.

Satz

Der Stabilisator G_x ist eine Untergruppe und der Kern ist ein Normalteiler.

Beweis:
Es gilt $e(x) = x \rightsquigarrow e \in G_x$. Für $a, b \in G_x$ gilt

$$(ab)(x) = a(\underbrace{b(x)}_{=x}) = a(x) = x \rightsquigarrow ab \in G_x$$

$$a^{-1}(x) = a^{-1}(\underbrace{a(x)}_{=x}) = (a^{-1}a)(x) = e(x) = x \rightsquigarrow a^{-1} \in G_x$$

Also ist $G_x \subseteq G$ Untergruppe.
Es gilt:

$$\bigcap_{x \in X} G_x = \{g(x) = x \mid \forall x \in X\}$$

Das ist genau der Kern der zugehörigen Homomorphie $\alpha : G \to \mathrm{Sym}(X)$, also ein Normalteiler. $\square$

2.3 Beispiele Wirkungen

(a) Sei G eine Gruppe. Für $g \in G$ definiere eine Abbildung $\lambda_g : G \to G$ durch $\lambda_g(x) = gx$. Es folgt

$$\lambda_g \circ \lambda_h = \lambda_{gh} \quad \lambda_e = \mathrm{id}_G \rightsquigarrow \lambda_g \lambda_{g^{-1}} = \mathrm{id}_G = \lambda_{g^{-1}} \lambda_g$$

also $\lambda_g \in \mathrm{Sym}(G)$. Die Gruppe G wirkt also auf der Menge $G = X$. Es gilt für die Wirkung:

$$G_x = \{g \in G \mid \lambda_g(x) = x\} = \{g \in G \mid gx = x\} = \{e\}$$

Zu $x, y \in G$ gibt es genau ein $g \in G$ mit $\lambda_g(x) = y$, nämlich $g = yx^{-1}$.
Man nennt das die **<u>Linksreguläre Wirkung</u>** von G auf sich.

(b) Sei G eine Gruppe und $H \subseteq G$ Untergruppe. Sei $X = {}^G/_H = \{aH \mid a \in G\}$. Die Gruppe G wirkt auf X durch

$$\lambda_g : {}^G/_H \to {}^G/_H, \ aH \mapsto gaH$$

Es gilt wieder $\lambda_g \lambda_h = \lambda_{gh}, \ \lambda_e = \mathrm{id}_{G/H}$.
Der Stabilisator von $x = H \in X$ ist

$$G_x = \{g \in G \mid gH = H\} = H$$

Zu $x = aH, y = bH \in X$ gibt es wieder $g \in G$ mit $g(x) = y$, nämlich $g = ba^{-1}$. Anders als im Bsp(a) ist g nicht eindeutig, falls $H \neq \{e\}$ gilt (für $H = \{e\}$ erhalten wir wieder Bsp(a)).

2.4 Satz 4, Satz von Cayley

Zu jeder Gruppe G gibt es eine Menge X und ein injektiven Homomorphismus $\alpha : G \to \mathrm{Sym}(X)$.

<u>Beweis:</u>
Setze $G = X$ und $\lambda : G \to \mathrm{Sym}(X)$ wie in Beispiel 2.3(a) □
Eine Untergruppe von $\mathrm{Sym}(X)$ nennt man auch eine **<u>Permutationsgruppe</u>**. Der Satz von Cayley wird auch so formuliert:
<u>Jede</u> Gruppe 'ist' (bis auf Isomorphie) eine Permutationsgruppe.

2.5 Definition transitiv

Eine G-Wirkung $G \times X \to X$ heißt **<u>transitiv</u>**, wenn es für alle $x, y \in G$ ein $g \in G$ gibt mit $g(x) = y$.
Die in Bsp. 2.3(a)(b) betrachteten Wirkungen sind also transitiv.

Satz

Gegeben sei ein transitive G-Wirkung $G \times X \to X$. Sei $x \in X$ und $H = G_x$. Dann ist die Abbildung ${}^G/_H \to X, \ gH \mapsto g(x)$ wohldefiniert und bijektiv. Für jedes $y \in X$ mit $y = g(x)$ gilt $G_y = gG_xg^{-1}$.

<u>Beweis:</u>
Betrachte die Abbildung $\epsilon : G \to X, \epsilon(g) = g(x)$. Es gilt

$$\epsilon(g) = \epsilon(g') \Leftrightarrow g(x) = g'(x) \Leftrightarrow g^{-1}g' = x \Leftrightarrow g^{-1}g' \in G_x = H \overset{1.13}{\Leftrightarrow} g'H = gH$$

Damit ist die erste Behauptung gezeigt.
Für $y = g(x)$ gilt

$$a(y) = y \Leftrightarrow ag(x) = g(x) \Leftrightarrow g^{-1}ag(x) = x \Leftrightarrow g^{-1}ag \in G_x \Leftrightarrow a \in gG_xg^{-1}$$

□

2.6 Bahnen

Gegeben sei eine G-Wirkung $G \times X \to X$.

Lemma

Für **Bahnen** $G(x),\ G(y) \subseteq X$ gilt stets:

$$\text{Ist } G(x) \cap G(y) \neq \emptyset, \text{ so gilt } G(x) = G(y)$$

Bahnen sind entweder disjunkt oder gleich.

Beweis:
Angenommen, $z \in G(x) \cap G(y)$, also $z = a(x) = b(y)$ für $a, b \in G$. Es folgt $b^{-1}a(x) = y$, also $y \in G(x)$, also $G(y) \subseteq G(x)$. Genauso folgt auch $G(y) \supseteq G(x)$, also $G(x) = G(y)$. □

Bemerkung

Für jedes $x \in X$ wirkt G transitiv auf der Bahn $G(x) \subseteq X$. Denn: $y, z \in G(x),\ y = a(x)$ und $z = b(x) \rightsquigarrow x = a^{-1}(y) \rightsquigarrow z = ba^{-1}(x)$. Weiter gilt $g(y) = ga(x) \in G(x)$.

Definition Bahnenraum

Die Menge der Bahnen bezeichnen wir mit ${}_{G}\backslash^{X} = \{G(x) \mid x \in X\}$ 'Bahnenraum'

Bemerkung

Das passt zur Notation für Nebenklassen: Gegeben sei eine Untergruppe $H \subseteq G$. Setze $X = G$, dann wirkt H auf $G = X$ durch $H \times X \to X,\ (h, x) \mapsto hx$
Die **Länge** einer Bahn $G(x)$ ist $\#G(x)$. Ist $\{x\} = \{G\}$ (Bahn der Länge 1), so sagt man,dass $x \in X$ ein **Fixpunkt** der G-Wirkung auf X ist. Für alle $g \in G$ gilt dann $g(x) = x$.
Die Bahnen der Wirkung von H auf G sind dann genau die Rechtsnebenklassen, $H(x) = Hx$ für $x \in X = G$, die Bahnenmenge ist also ${}_{H}\backslash^{G} = \{Hx \mid x \in G\}$

2.7 Satz 5, Die Bahnengleichung

Gegeben sei eine G-Wirkung $G \times X \to X$. Ein **Schnitt** (ein **Transversale**) ist eine Teilmenge $S \subseteq X$ mit folgender Eigenschaft: für jedes $x \in X$ gilt $\#(s \cap G(x)) = 1$, jede Bahn trifft S genau einmal. Es folgt $\#S = \#\left({}_{G}\backslash^{X}\right)$. Mit Hilfe des Auswahlaxioms sieht man, dass Schnitte stets existieren.

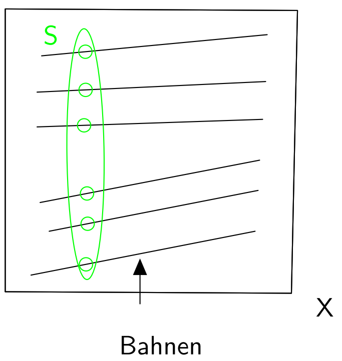

Abbildung 3: Die Bahnengleichung

Satz

Sei $S \subseteq X$ ein Schnitt der G-Wirkung $G \times X \to X$. Wenn X endlich ist, dann gilt

$$\#X = \sum_{s \in S} [G : G_s]$$

Beweis:
Sei $\#S = m$, $S = \{s_1, \dots, s_m\} \rightsquigarrow X = G(s_1) \dot\cup G(s_2) \dot\cup \cdots \dot\cup G(s_m)$

$$\#G(s_i) \overset{2.5}{=} \#^G/_{G_{s_i}} \overset{1.14}{=} [G : G_{s_i}]$$

2.8 Automorphismen und Konjugationswirkungen

Sei G Gruppe. Ein bijektiver Homomorphismus $\alpha : G \to G$ heißt **Automorphismus** von G. Die Menge

$$\mathrm{Aut}(G) = \{\alpha : G \to G \mid \alpha \text{ Automorphismus}\}$$

ist eine Gruppe, mit der Komposition von Automorphismus als Verknüpfung und id_G als Neutralelement.

Beispiel

Sei $a \in G$. Dann ist die Abbildung $\gamma_a : G \to G,\ g \mapsto aga^{-1}$ ein Automorphismus. Denn:

$$\begin{aligned}
&\gamma_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \gamma_a(g)\gamma_a(h)\\
&\rightsquigarrow \gamma_a \text{ Homomorphismus}\\
&\gamma_a(g) = e \Leftrightarrow aga^{-1} = e \Leftrightarrow g = a^{-1}ea = e\\
&\rightsquigarrow \gamma_a \text{ Monomorphismus},\ ker(\gamma_a) = \{e\}\\
&\text{Gegeben } g \in G \text{ folgt } \gamma_a(aga^{-1}) = g\\
&\rightsquigarrow \gamma_a \text{ Epimorphismus}\\
&\Rightarrow \gamma_a \text{ Automorphismus}
\end{aligned}$$

oder: $\gamma_a \circ \gamma_a = \mathrm{id}_G = \gamma_{a^{-1}} \circ \gamma_a$

Satz

Die Abbildung $G \overset{\gamma}{\to} \mathrm{Aut}(G),\ a \mapsto \gamma_a$ ist ein Homomorphismus.

Beweis:
Es gilt

$$\gamma_a \circ \gamma_b(g) = abgb^{-1}a^{-1} = abg(ab)^{-1} = \gamma_{ab}(g)$$

also $\gamma_a \circ \gamma_b = \gamma_{ab}$, □

Weil $\mathrm{Aut}(G) \subseteq \mathrm{Sym}(G)$ eine Untergruppe ist, ist $\gamma : G \to \mathrm{Aut}(G)$ eine Wirkungvon G auf G, die **Konjugationswirkung**.
Beachte den Unterschied zu 2.3(a):

$$\lambda_a(g) = ag \qquad\qquad \gamma_a(g) = aga^{-1}$$

λ_a ist kein Homomorphismus (für $a \neq e$)

$$\lambda_a(gh) = agh \neq \lambda_a(g)\lambda_a(h) = agah$$

Der Kern von $\gamma : G \to \mathrm{Aut}(G)$ ist

$$\begin{aligned}
Z(G) &= \{a \in G \mid \forall g \in G \text{ gilt } aga^{-1} = g\}\\
&= \{a \in G \mid \forall g \in G \text{ gilt } ag = ga\}
\end{aligned}$$

Man nennt diesen Normalteiler das **Zentrum** von G. Das Zentrumvon G ist also abelsch (und G ist genau dann abelsch, wenn $Z(G) = G$ gilt).

Bemerkung

Im Allgemeinen ist die Abbildung $\gamma : G \to \mathrm{Aut}(G)$ weedr injektiv und surjektiv. Das Bild $\gamma(G) \subseteq \mathrm{Aut}(G)$ ist die Gruppe der **inneren Automorphismen**, $\gamma(G) = \mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$.
Mit dem Homomorphiesatz also:

$$G/Z(G) \cong \mathrm{Inn}(G)$$

Wie sehen die Stabilisatoren in der Konjugationswirkung aus? Der Stabilisator von $g \in G$ ist der **Zentralisator** von g (vgl. 1.6)

$$\begin{aligned} Z_G(g) &= \{a \in G \mid aga^{-1} = g\} \\ &= \{a \in G \mid ag = ga\} \end{aligned}$$

Beachte: es gilt stets $\langle g \rangle \subseteq Z_G(g)$,denn

$$ggg^{-1} = g \rightsquigarrow g \in Z_G(g) \rightsquigarrow \langle g \rangle \subseteq Z_G(g)$$

Die Bahnen $G(g) = \{aga^{-1} \mid a \in G\}$ nennt man **Klassen** oder **Konjugiertenklassen** in G.

2.9 Satz 6, Die Klassengleichung

Sei G eine endliche Gruppe, sei $S \subseteq G$ ein Schnitt der Konjugationswirkung γ. Sei $\mathcal{K} = S - Z(G)$. Dann gilt

$$\#G = \#Z(G) + \sum_{s \in \mathcal{K}} [G : Z_G(s)]$$

Beweis:
Nach der Bahnengleichung gilt

$$\#G = \sum_{s \in S} [G : Z_G(s)]$$

Für jedes $z \in Z(G)$ gilt $G(z) = \{aza^{-1} \mid a \in G\} = \{z\}$, also $Z(G \subseteq S$ und $\#G(z) = 1 \ \forall z \in Z$. □

2.10 Korollar über das Zentrum

Sei p eine Primzahl und G eine endliche Gruppe mit $\#G = p^m,\ m \geq 1$.
Dann gilt $Z(G) \neq \{e\}$.

Beweis:
Für $g \in G \backslash Z(G)$ ist $Z_G(g) \neq G$. Nach dem Satz von Lagrange 1.14 folgt $\#Z_G(g) = p^l,\ l < m$. Insbesondere ist dann p ein Teiler von $[G : Z_G(g)] = p^{m-l} \neq 1$. Folglich ist p ein Teiler von $\#Z(G)$, also $\#Z(G) \geq p$. □
Wenn G eine endliche Gruppe ist, dann nennt man ihre Kardinalität $\#G$ die **Ordnung** von G. Das passt zu 1.11: die Ordnung eines Elements $g \in G$ ist die Ordnung der von g erzeugten zyklischen Gruppe, $o(g) = \#\langle g \rangle$, vgl. 1.12.

Definition p-Gruppe

Eine endliche Gruppe G heißt **p-Gruppe**, für eine Primzahl p, wenn gilt $\#G = p^m$ für ein $m \geq 1$. Das vorige Korollar besagt also: jede p-Gruppe hat ein nicht-triviales Zentrum.

Beispiel
$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in K^{3 \times 3} \right\}$ mit $K = \mathbb{F}_p$ (Körper mit p Elementen)

$\#G = p^3 \rightsquigarrow G$ ist p-Gruppe. Das Zentrum ist $\left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \in K^{3 \times 3} \right\}$

Unser nächstes Ziel ist der Beweis der Sylow-Sätze. Das braucht etwas Vorbereitung.

2.11 Definition Normalisator

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Der **Normalisator** von H in G ist

$$N_G(H) = \{n \in G \mid nHn^{-1} = H\}$$

Satz

Der Normalisator $N_G(H)$ ist eine Untergruppe von G und es gilt

$$H \trianglelefteq N_G(H)$$

Insbesondere gilt $H \subseteq N_G(H)$

Beweis:
Setze $X = \{aHa^{-1} \mid a \in G\}$. Dann wirkt G auf der Menge X durch Konjugation,

$$\begin{aligned} G \times X &\to X \\ (g, aHa^{-1}) &\mapsto gaHa^{-1}g^{-1} = (ga)H(ga)^{-1} \end{aligned}$$

Der Stabilisator von $H \in G$ ist genau $N_G(H)$, also eine Untergruppe.
Weiter gilt $H \subseteq N_G(H)$ (klar) und nach Definition gilt für alle $n \in N_G(H)$, dass $nHn^{-1} = H$, also $H \trianglelefteq N_G(H)$. □
Die Menge $X = \{aHa^{-1} \mid a \in G\}$ nennt man auch die **Konjugationsklasse** der Untergruppe H in G.
Folgerung aus dem Satz: Ist $K \subseteq N_G(H)$ eine Untergruppe, dann ist $KH \subseteq N_G(H)$ eine Untergruppe, denn $H \trianglelefteq N_G(H)$, das folgt aus 1.23 Lemma.

2.12 Satz 7, Cauchys Satz

Sei G eine endliche Gruppe und sei p eine Primzahl. Wenn p ein Teiler von $\#G$ ist , dann enthält G (mindestens) ein Element der Ordnung p.

Beweis:
Setze $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e\}$. Da $g_1, \ldots, g_{p-1} \in G$ frei gewählt werden können und $g_p = (g_1, \cdots, g_{p-1})^{-1}$, gilt, $\#X = (\#G)^{p-1}$ und p teilt $\#X$. Gesucht ist ein Element $g \in G$ mit $g \neq e$ und $(g, \ldots, g) \in X$ (d.h. $g^p = e \neq g$).
Setze $K = \mathbb{Z}/p\mathbb{Z}$. Diese Gruppe K wirkt auf X wie folgt: sei $\overline{k} \in K$, setze $\overline{k}(g_{\overline{1}}, \ldots, g_{\overline{p}}) = (g_{\overline{1+k}}, \ldots, g_{\overline{p+k}})$
Das ist wirklich eine K-Wirkung: $0 < k \leq p$wirkt durch

$$\overline{k} : (g_{\overline{1}}, \ldots, g_{\overline{p}}) \mapsto (g_{\overline{1+k}}, \ldots, g_{\overline{p}}, g_{\overline{1}}, \ldots, g_{\overline{k}})$$

$g_{\overline{1}} \cdots g_{\overline{k}} = a \quad g_{\overline{k+1}} \cdots g_{\overline{p}} = b \qquad ab = e$ nach Voraussetzung $\Rightarrow b = a^{-1}$

$$g_{\overline{1+k}} \cdots g_{\overline{p}} \cdot g_{\overline{1}} \cdots g_{\overline{k}} = ba = e \Rightarrow (g_{\overline{1+k}}, \ldots, g_{\overline{p}}) \in X$$

Die Fixpunkte dieser K-Wirkung sind genau die Tupel $(g, \ldots, g) \in X$. Also ist $(e, \ldots, e)$ ein Fixpunkt.
Da $\#K = p$ hat jede K-Bahn $K(x)$ Länge $\#K(x) = [K : K_x] \in \{1, p\}$ und die der Länge 1 sind die Fixpunkte. Nach der Bahnengleichung gilt (für ein Schnitt $S \subseteq X$)

$$\#X = \#G^{p-1} = \sum_{s \in S} [K : K_s]$$

Die Primzahl p teilt beide Seiten, es gilt $[K : K_s] \in \{1, p\}$ und für $s = (e, \ldots, e)$ gilt $[K : K_s] = 1$.
Also gibt es ein $s \neq (e, \ldots, e)$ mit $[K : K_s] = 1$ □

Wir brauchen noch das folgende technische Hilfsmittel.

2.13 Lemma 3

Sei $G \times X \to X$ eine Wirkung einer endlichen Gruppe G auf einer endlichen Menge X. Sei p eine Primzahl. Angenommen, es gilt folgendes:
(i) zu jedem $x \in X$ gibt es eine p-Gruppe $P \subseteq G$ mit $P(x) = \{x\}$.
Dann gilt $\#X = kp + 1$ für ein $k \geq 0$ und G wirkt transitiv auf X.

Beweis:
Sei $S \subseteq X$ ein Schnitt. Für jedes $s \in S$ wirkt G also transitiv auf $G(s)$. Sei $s \in S$. Sei $P \subseteq G$ p-Gruppe mit $P(s) = \{s\}$. Für jedes $x \in X \backslash \{s\}$ teilt p die Länge der Bahn $P(x)$ $\big($weil P p-Gruppe ist und $P(x) \neq \{x\}$ nach (i)$\big)$. Es folgt $\#G(s) = kp + 1$.
Angenommen, $S \neq \{s\}$. Für $t \in S \backslash \{s\}$ folgt $\#G(t) = lp$, weil P in $G(t)$ kein Fixpunkt hat. Anderseits zeigt das gleiche Argument, dass $G(t) = mp + 1 \lightning$
Es folgt $S = \{s\}$ und $X = G(s)$ $\square$

Jetzt beweisen wir Sylows Sätze. Peter Sylow war ein norwegischer Mathematiker und Lehrer. Seine Sätze sind in der endlichen Gruppentheorie ganz wesentlich.

2.14 Definition Sylow-Gruppe

Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r$, wobei $m \geq 1$ sei und p kein Teiler von r ist. Eine Untergruppe $U \subseteq G$ heißt **Sylow-p-Gruppe** in G, wenn gilt $\#U = p^m$.
Die Menge aller Sylow-p-Gruppen in G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.
(Im Moment ist nicht klar, dass $\mathrm{Syl}_p(G) \neq \emptyset$, aber das beweisen wir gleich.)

Sylows Sätze

Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r,\ m \geq 1$, p kein Teiler von r. Dann gilt folgendes:

(1) $\mathrm{Syl}_p(G) \neq \emptyset$

(2) G wirkt transitiv auf $\mathrm{Syl}_p(G)$: zu $U, V \in \mathrm{Syl}_p(G)$ gibt es stets $g \in G$ mit $gUg^{-1} = V$

(3) $\#\,\mathrm{Syl}_p(G) = kp + 1$ für ein $k \geq 0$

(4) Ist $P \subseteq G$ ein p-Gruppe, so gibt es $U \in \mathrm{Syl}_p(G)$ mit $P \subseteq U$.

Beweis:
Sei Γ die Menge aller p-Gruppen in G. Nach Cauchys Satz ist $\Gamma \neq \emptyset$. Sei $\Omega \subseteq \Gamma$ die Menge aller maximalen p-Gruppen in Γ (weil G endlich ist, ist jede p-Gruppe $P \subseteq G$ ein einer maximalen p-Gruppe enthalten).
Die Gruppe G wirkt durch Konjugation auf der Menge Γ und Ω. Nach Definition gilt $\mathrm{Syl}_p(G) \subseteq \Omega$.

1. Schritt: G wirkt transitiv auf Ω und es gilt $\#\Omega = kp + 1$ für ein $k \geq 0$.
Beweis 1. Schritt: Wir benutzen das Lemma 2.13. Für $U \in \Omega$ ist U der einzige Fixpunkt der Wirkung von U auf der Menge Ω. Denn: wenn U das Element $V \in \Omega$ fixiert, so folgt $U \subseteq N_G(V) \overset{2.11}{=} UV \subseteq G$ Untergruppe, $V \trianglelefteq UV$. Es gilt

$$\#UV \overset{1.14}{=} \#V \cdot [UV : V] = \#V \cdot \#^{UV}/_{V}$$

sowie

$$^{UV}/_{V} \overset{1.23}{\cong} {}^{U}/_{U\cap V} = \frac{\#U}{\#(U\cap V)} \text{ also ist } \#^{UV}/_{V} \text{ eine } p\text{-Potenz}$$

denn $\#U$ und $\#U \cap V$ sind p-Potenzen. Folglich ist $UV \subseteq G$ eine p-Gruppe. Da U und V maximale p-Gruppen sind und $U, V \subseteq UV$ folgt

$$U = UV = V$$

Mit Lemma 2.13 folgt nun: G wirkt transitiv auf Ω und $\#\Omega = kp + 1$ □

<u>2. Schritt:</u> Es gilt $\Omega = \mathrm{Syl}_p(G)$

<u>Beweis 2. Schritt:</u> Sei $U \in \Omega,\ \#U = p^l$. Wir müssen zeigen, dass $p^l = p^m$ gilt.
Wegen Schritt 1 gilt jedenfalls

$$\#G = p^m \cdot r = \#N_G(U) \cdot \#\Omega = \#N_G(U)(kp+1) \qquad (*)$$

und folglich

$$\#N_G(U) = p^m \cdot s \quad \text{für ein } s \geq 1 \qquad (**)$$

Angenommen, es gilt $l < m$. Betrachte

$$N_G(U) \overset{\pi_U}{\twoheadrightarrow} {}^{N_G(U)}/_{U} = K$$

Es folgt $\#N_G(U) = p^m \cdot s = \underbrace{\#U}_{=p^e}$, also ist p ein Teiler von $\#K$. Nach Cauchys Satz 2.12 gibt es eine p-Gruppe $P \subseteq K$. Setze $V = \pi_U^{-1}(P) \subseteq N_G(U)$. Es folgt mit $P = {}^{V}/_{U}$, dass

$$\#V = \#U \cdot \#P$$

also ist V eine p-Gruppe.
Da p ein Teiler von $\#P$ ist, folgt $V \supsetneq U$, ein Widerspruch zur Maximalität von U.
Folglich gilt $\#U = p^m$ für alle $U \in \Omega$ und damit $\Omega = \mathrm{Syl}_p(G)$. □

Damit sind (1),(2) und (3) bewiesen. Wegen $\mathrm{Syl}_p(G) = \Omega$ folgt (4). □

Addendum zu Sylows Theorem

Es gilt (mit den Bezeichnungen von oben)

$$r = s \cdot (kp + 1)$$

Das folgt aus $(*)$ und $(**)$.

2.15 Beispiel einer Anwendung

Lemma

Seien p, q Primzahlen mit $p < q$. Wenn G eine Gruppe ist mit $\#G = p \cdot q$ und wenn p kein Teiler von $q - 1$ ist, dann ist G abelsch.

<u>**Beweis:**</u>
Setze $\#\mathrm{Syl}_p(G) = kp + 1$ und $\#\mathrm{Syl}_q(G) = lq + 1$, dann folgt $q = s(kp + 1)$.
1.Fall: $s = 1 \rightsquigarrow q = kp + 1$ Widerspruch zur Annahme, dass p kein Teiler von $q - 1$ ist.
2.Fall: $kp + 1 = 1 \rightsquigarrow$ es gibt genau eine Sylow-p-Gruppe $U \subseteq G \rightsquigarrow G = N_G(U)$, d.h. $U \trianglelefteq G$.
Jetzt $p = s' \cdot (lq + 1)$ wegen $q > p$ folgt $s' = p$ und $lq + 1 = 1 \rightsquigarrow$ es gibt genau eine Sylow-q-Gruppe $Q \subseteq G \rightsquigarrow Q \trianglelefteq G$.

Weiter gilt: $\#P = p \qquad \#Q = q$ und $\#(P \cap Q)$ teilt nach Lagrange p und $q \Rightarrow P \cap Q = \{e\}$. Weil $P \trianglelefteq G$ und $Q \trianglelefteq G$ gilt für $a \in P$ und $b \in Q$, dass

$$\underbrace{\underbrace{aba^{-1}}_{\in Q}\underbrace{b^{-1}}_{\in Q}}_{\in P} \in Q \cap P \text{ d.h. } ab = ba$$

Nach 1.23 haben wir ein Monomorphismus $P \times Q \xrightarrow{\varphi} G,\ (a,b) \mapsto ab$. Wegen $\#(P \times Q) = p \cdot q = \#G$ ist φ surjektiv, also ein Isomorphismus.
Wegen $\#P = p$ und $\#Q = q$ sind P und Q abelsch: ist $a \in P,\ a \neq e$, so gilt $o(a) > 1$ und $o(a)$ teilt p

$$\Rightarrow o(a) = p \Rightarrow \langle a \rangle = P \Rightarrow P \text{ zyklisch } \Rightarrow P \text{ abelsch, vgl. 1.12.}$$

Gleiches gilt für Q (mit ÜA 4.3 einfügen folgt jetzt sogar: G ist <u>zyklisch</u>) □

Beispiel

Die Gruppe $\mathrm{Sym}(3)$ ist nicht abelsch, vgl 1.7. Es gilt $\#\,\mathrm{Sym}(3) = 2 \cdot 3$ (aber 2 teilt 3-1 !). Was sind die Sylowgruppen in $\mathrm{Sym}(3)$? (ÜA)

Bemerkung

Im Beweis vom obigen Lemma haben wir einige <u>nützliche Fakten</u> bewiesen, die auch sonst hilfreich sein können:

(1) Jede endliche Gruppe, deren Ordnung eine Primzahl ist, ist ablesch.

(2) Wenn $\varphi : K \to G$ ein Monomorphismus von endlichen Gruppen ist und wenn gilt $\#K = \#G$, dann ist φ ein Isomorphismus.

(3) Wenn $N, M \subseteq G$ Normalteiler sind und wenn gilt $N \cap M = \{e\}$, dann ist die Abbildung $N \times M \to G,\ (n,m) \mapsto n \cdot m$ ein Monomorphismus.

(4) Wenn G endlich ist und p eine Primzahl und wenn p ein Teiler von $\#G$ ist mit $\mathrm{Syl}_p(G) = 1$, dann ist die (eindeutige) Sylow-p-Gruppe $U \in \mathrm{Syl}_p(G)$ ein Normalteiler in G, $U \trianglelefteq G$.

2.16 Satz 8

Sei G eine endliche Gruppe mit $\#G = pq,\ p \neq q$ Primzahlen. Dann gilt es gibt einen Normalteiler $N \trianglelefteq G,\ \{e\} \neq N \neq G$.

<u>**Beweis:**</u>
Œ$p < q,\ \#\,\mathrm{Syl}_q(G) = lq + 1$

$$\begin{aligned} &\overset{2.14}{\Rightarrow} p = s(lq+1) \Rightarrow lq + 1 = 1 \text{ wegen } p < q \\ &\Rightarrow \text{ es gibt genau eine Sylow-}q\text{-Gruppe } U \subseteq G \\ &\Rightarrow U \trianglelefteq G \text{ und } \#U = p \end{aligned}$$

□

Wir betrachten als nächstes p-Gruppen genauer.

2.17 Lemma 4

Sei G eine Gruppe. Dann ist jede Untergruppe $H \subseteq Z(G)$ Normalteiler in G.

Beweis:
Sei $g \in G$ und $h \in H \subseteq Z(G)$. Es folgt $ghg^{-1} = h$, also $gHg^{-1} = H$. □

Satz

Sei p Primzahl und G eine p-Gruppe, $\#G = p^m$, $m \geq 1$. Dann gibt es Normalteiler $G_k \trianglelefteq G$ mit $\#G_k = p^k$ für $0 \leq k \leq m$ und mit

$$G_m \trianglelefteq G_{m-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = \{e\}$$

Beweis:
Induktion nach m. Für $m = 1$ ist nichts zu zeigen. Sei jetzt $\#G = p^m$, $m \geq 1$.
Nach 2.10 ist $Z(G) \neq \{e\}$, also $Z(G) = p^s$ für ein $s > 1$ (Lagrange). Nach Cauchys Satz 2.12 gibt es $g \in Z(G)$ mit $o(g) = p$. Setze $G_1 = \langle g \rangle$ und $G \overset{\pi}{\to} \tilde{G} = G/G_1$ (nach dem Lemma gilt $G_1 \trianglelefteq G$).
Es folgt $\#\tilde{G} = p^{m-1}$ nach Induktionannahme gibt es $\tilde{G}_k \trianglelefteq \tilde{G}$ mit $\#\tilde{G}_k = p^k$, $\tilde{G} \supseteq \tilde{G}_{m-2} \supseteq \cdots \supseteq \tilde{G}_0$.
Setze $G_{k+1} = \pi^{-1}(G_k)$, es folgt nach 1.22, dass $G_{k+1} \trianglelefteq G$, sowie $G_m \supseteq G_{m-1} \supseteq \cdots \supseteq G_0 = \{e\}$.
Wegen $G_1 \subseteq G_{k+1}$ folgt $\tilde{G}_k \cong G_{k+1}/G_1$, also

$$\#G_{k+1} = p \cdot \#\tilde{G}_k = p^{k+1}$$

□

Folgerung

Ist G eine endliche Gruppe, p eine Primzahl und ist p^k ein Teiler von $\#G$, dann hat G eine Untergruppe der Ordnung p^k.

Beweis:
Sei $U \in \mathrm{Syl}_p(G)$, $\#U = p^m$.
Dann gilt $k \leq m$ und nach dem vorigen Satz gibt es eine Untergruppe $H \subseteq U$ mit $\#H = p^k$ □

2.18 Definition Normalreihe

Sei G eine Gruppe, sei $G = G_m \supseteq G_{m-1} \supseteq \cdots \supseteq G_0 = \{e\}$ Untergruppen. Wenn gilt

$$G_{k-1} \trianglelefteq \mathcal{G}_k,$$

dann heißt $G_m \supseteq \cdots \supseteq G_0$ **Normalreihe** in G. Die Quotienten G_k/G_{k+1} heißen **Faktoren** der Normalreihe.
Eine Gruppe, die eine Normalreihe mit ableschen Faktoren hat, heißt **auflösbare Gruppe**.

Beispiele

(a) G abelsch $\Rightarrow$ G auflösbar, setze $G_1 = GG \supseteq G_0 = \{e\}$

(b) $G = \mathrm{Sym}(3)$, $\#G = 6$, $\tau : \{1,2,3\} \to \{1,2,3\}$ $\tau : \begin{array}{c} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{array}$
$o(\tau) = 3$, $G_1 = \langle \tau \rangle \trianglelefteq G$ (weil $[G : G_1] = 2$,ÜA 3.2 oder 2.16)
$\#G/G_1 = 2 \rightsquigarrow$ abelsch, also ist $\mathrm{Sym}(3)$ auflösbar.

(c) Nach Satz 2.17 ist jede p-Gruppe auflösbar.

Wir betrachten jetzt abelsche p-Gruppen.

2.19 Lemmata 5,6,7

Lemma A

Sei G abelsche p-Gruppe. Wenn G genau eine Untergruppe $H \subseteq G$ der Ordnung p hat, dann ist G zyklisch.

Beweis:
Setze $\#G = p^m,\ m \geq 1$. Induktion nach m. Für $m = 1$ ist nichts zu zeigen. Sei jetzt $m > 1$. Betrachte den Homomorphismus $\varphi : G \to G,\ g \mapsto g^p$ (das ist ein Homomorphismus, weil G abelsch ist: $(gh)^p = g^p h^p$).
Es gilt $\ker(\varphi) = \{g \in G \mid g^p = e\} = \{g \in G \mid o(g) \in \{1, p\}\}$.Ist $o(g) = p$,so folgt aus der Annahme $g \in H$, also $H = \ker(\varphi)$, denn $h \in H \rightsquigarrow o(h) \in \{1, p\}$.
Setze $K = \varphi(G)$. Nach dem Homomorphiesatz 1.20 gilt $K \cong G/H$, also $\#K = p^{m-1}$. Wegen $m > 1$ folgt aus Cauchys Satz 2.12, dass K ein Element der Ordnung p enthält. Folglich gilt $H \subseteq K$. Also hat K genau eine Untergruppe der Ordnung p und ist deswegen nach Induktionsannahme zyklisch, $K = \langle k \rangle$ für ein $k \in K = \varphi(G)$. Wähle $g \in G$ mit $\varphi(g) = g^p = k$. Wegen $o(g) = p \cdot r$ folgt $o(g^r) = p \rightsquigarrow H \subseteq \langle g \rangle$ (wegen der Eindeutigkeit von H), also

$$\langle g \rangle / H \cong K \Rightarrow \#\langle g \rangle = \#K \cdot \#H = \#G \Rightarrow G = \langle g \rangle$$

□

Lemma B

Sei Gzyklisch mit $\#G = k \cdot l$. Dann hat G genau eine Untergruppe $H \subseteq G$ mit $\#H = k$ (ÜA 4.1).

Beweis:
Betrachte $\varphi : G \to G,\ g \mapsto g^k$, das ist ein Homomorphismus. Der Kern ist $K = \{g \in G \mid g^k = e\}$. Ist $H \subseteq G$ Untergruppe mit $\#H = k$,so folgt $H \subseteq K$. Sei $u \in G$ Erzeuger, $G = \langle u \rangle$. Das Bildvon φ ist dann $\varphi(G) = \langle u^k \rangle$ und $o(u^k) = l$. Also folgt

$$l = \#\varphi(G) = \frac{\#G}{\#K} \Rightarrow \#K = k \Rightarrow H = K.$$

□

Lemma C

Sei G eine abelsche p-Gruppe, sei $u \in G$ eine Element maximaler Ordnung in G und sei $U = \langle u \rangle$. Dann gibt es eine Untergruppe $H \subseteq G$ mit

$$H \cap U = \{e\} \text{ und } G = HUs,\ \text{d.h. } H \times UU \cong G.$$

Beweis:
Setze $\#G = p^m$. Für $m = 1$ist G zyklisch, setze $U = G$ und $H = \{e\} \rightsquigarrow$ fertig.
Sei jetzt $m > 1$, Induktion nach m.
1. Fall: G zyklisch, $G = U,\ H = \{e\} \rightsquigarrow$ fertig.
2. Fall: G nicht zyklisch. Da U genau eine Untergruppe der Ordnung p hat (Lemma B) gibt es nach Lemma A und Cauchys Satz 2.12 ein Element $w \in G \backslash U$ mit $o(w) = p$. Setze $W = \langle w \rangle$.
Es folgt $U \cap W = \{e\}$,weil $w \notin U$ ($\#U \cap W$ ist p-Potenz). Betrachte $\pi : G \to G/W$. Wegen $\ker(\pi) = W$ ist die Einschränkung von π auf U injektiv, d.h. $o(\pi(u)) = o(u)$. Folglich ist $\pi(u)$ ein Element maximaler Ordnung in $L = G/H$, und $\#G/W = p^{m-1}$.

Nach Induktionsannahme gibt es eine Untergruppe $H' \subseteq L$ mit $H' \cap \pi(U) = \{e_L\}$ und $L = \pi(U)H' \cong \pi(U) \times H'$.
Setze $H = \pi^{-1}(H')$. Es folgt $H \cap U = \{e\}$, denn:

$$h \in H,\ \pi(h) \in \pi(U) \rightsquigarrow \pi(h) = e_L \rightsquigarrow h \in W.$$

Weiter gilt für $g \in G$, dass

$$\begin{aligned} &\pi(g) = \pi(u^k)\pi(h) && \text{für ein } k \geq 0,\ h \in H \\ &\rightsquigarrow g = u^k(h \cdot w^l) && \text{für ein } l \geq 0,\ \text{aber } w \in H \\ &\Rightarrow G = UH \end{aligned}$$

□

Korollar

Sei G eine abelsche p-Gruppe, $\#G = p^m$ mit $m \geq 1$. Dann gibt es Zahlen $n_1 \geq \cdots \geq n_r \geq 1$ mit $m = n_1 + \cdots + n_r$ und

$$G \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$

Beweis:
Wähle $u_1 \in G$ mit maximaler Ordnung $o(u_1) = p^{n_1}$, $U_1 = \langle u_1 \rangle \cong \mathbb{Z}/p^{n_1}\mathbb{Z}$ und eine Untergruppe $G_1 \subseteq G$ wie in Lemma C mit $U_1 \cap G_1 = \{e\},\ G = U_1G_1 \cong U_1 \times G_1$. Wähle $u_2 \in G_1$ mit maximaler Ordung $o(u_2) = p^{n_2},\ U_2 = \langle u_2 \rangle \cong \mathbb{Z}/p^{n_2}\mathbb{Z},\ G_1 = U_2G_2$ usw. Nach endlich vielen Schritten

$$G = U_1U_2 \cdots U_r \cong U_1 \times \cdots \times U_r$$

Zur Eindeutigkeit der Zahlen $n_1, \ldots, n_r$:
Für $l \geq 1$ sei $\varphi_l : G \to G,\ g \mapsto g^{p^l}$.
Da G abelsch ist, ist φ_l ein Homomorphismus mit

$$\ker(\varphi_l) = \{g \in G \mid o(g) \text{ teilt } p^l\},$$

insbesondere

$$\left.\begin{array}{ll} \varphi_l(u_i) = e & \text{für } l \geq n_i \\ \varphi_l(u_i) \neq & \text{sonst} \end{array}\right\} \Rightarrow \#\varphi_l(U_i) = \begin{cases} \{1\} & l \geq n_i \\ \mathbb{Z}/p^{n_i - l}\mathbb{Z} & l < n_i \end{cases}$$

$\Rightarrow\ \#\varphi_l(G) = \prod_{n_i > l} p^{n_i - l} = p^{N_l}$,aus den Zahlen $N_1, N_2, \ldots$ lassen sich die n_i berechnen, $N_l = \sum_{n_i > l}(n_i - l)$ □

2.20 Satz 9

Sei G eine endliche abelsche Gruppe,$\#G = p_1^{l_1} \cdots p_s^{l_s},\ 2 \leq p_1 < p_2 < \cdots < p_s$ Primzahlen, $l_1, \ldots, l_s \geq 1$. Dann gilt

$$G \cong P_1 \times \cdots \times P_s$$

wobei $P_j$eine abelsche p_j-Gruppe der Ordnung $p_j^{l_j}$ ist wie im vorigen Korollar.
Insbesondere ist jede endliche abelsche Gruppe eine Produkt von zyklischen Gruppen.

Beweis:
Da G abelsch ist,ist jede Sylow-p_j-gruppe in G normal, also gibt es (wegen 2.14(2)) genau eine Sylow-p_j-Gruppe$P_j \subseteq G$, und P_j enthält alle Elemente $g \in G$, deren Ordnung eine p_j-Potenz ist.
Betrachte

$$\varphi : P_1 \times \cdots \times P_s \to G$$
$$(g_1, \dots, g_s) \mapsto g_1 g_2 \cdots g_s$$

Weil G abelsch ist, ist φ ein Homomorphismus (oder: weil für alle $i < j$ gilt $P_i \cap P_j = \{e\} \rightsquigarrow$ B6 A($*$)).
Es genügt zu zeigen, dass φ injektiv ist, dann folgt aus Kardinalitätsgründen, dass φ bijektiv ist.
ZZ $\ker(\varphi) = \{e\}$.
Angenommen, $g_1 \cdots g_s = e,\ g_i \in P_i$.
Setze $r_i = \frac{\#G}{p_i^{l_i}}$.Für $i \neq j$ folgt $g_j^{r_i} = e$, weil $\#P_j$ ein Teiler von r_i ist. Also gilt

$$(g_1 \cdot g_s)^{r_i} = g_1^{r_i} \cdot g_s^{r_i} = g_i^{r_1} = e^{r_i} = e$$

Also ist $o(g_i)$ ein Teiler von r_i. Weil $o(g_i)$ eine p_i-Potenz ist, folgt $o(g_i) = 1$, d.h. $g_i = 1$.
Es folgt $\ker(\varphi) = \{(e, \dots, e)\}$. □

2.21 Satz 10

Sei G eine endliche auflösbare Gruppe mit einer Normalreihe $G = G_m \trianglelefteq \dots \trianglelefteq G_0$ mit abelschen Faktoren. Dann gibt es für jedes $1 \leq k \leq m$ Untergruppe H_j mit

$$G_k \trianglelefteq H_l \trianglelefteq \dots \trianglelefteq H_0 = \mathcal{G}_{k-1}$$

mit ${}^{H_j}/_{H_{j-1}} \cong {}^{\mathbb{Z}}/_{p_j\mathbb{Z}}, \quad p_j$ Primzahl.
Insbesondere hat jede endliche auflösbare Gruppe eine Normalreihe, in der alle Faktoren zyklisch von Primzahlordnung sind.

Beweis:
Betrachte die abelsche Gruppe $A = {}^{G_k}/_{G_{k-1}}$.
Nach Satz 2.20 und 2.17, angewandt auf die Sylowgruppen von A, gibt es Untergruppen

$$A = A_l \supseteq \cdots \supseteq A_0 = \{e\} \text{ mit } {}^{A_j}/_{A_{j-1}} \cong {}^{\mathbb{Z}}/_{p_j\mathbb{Z}},\ p_j \text{ Primzahl}$$

Setze $\pi : \mathcal{G}_k \to {}^{G_k}/_{G_{k-1}} = A$ kanonischee Epimorphismus und $H_j = \pi^{-1}(A_j) \rightsquigarrow H_j \trianglelefteq G_k$ und

$$G_k \trianglelefteq H_l \trianglelefteq \dots H_0 = G_{k-1}$$

$${}^{H_j}/_{H_{j-1}} \overset{\text{2.Iso-satz}}{\cong} {}^{A_j}/_{A_{j-1}} \cong {}^{\mathbb{Z}}/_{p_j\mathbb{Z}}$$

□

2.22 Komutatoren

Sei G eine Gruppe, $a, b \in G$. Der **Komutator** von a und b ist

$$[a, b] = aba^{-1}b^{-1} = ab(ba)^{-1} \rightsquigarrow ab = [a, b]ba$$

Offensichtlich gilt $[a, b]^{-1} = [b, a]$ und

$$[a, b] = e \Leftrightarrow a \text{ zentralisiert } b \Leftrightarrow b \text{ zentralisiert } a \Leftrightarrow a \text{ und } b \text{ vertauschen}$$

Die **Kommutatorengruppe** von G ist

$$\mathcal{D}G = \langle [a, b] \,|\, a, b \in G \rangle \,,$$

die von allen Komutatoren erzeugte Gruppe.

Satz

Sei G eine Gruppe. Dann gilt

(i) $\mathcal{D}G \trianglelefteq G$

(ii) $G/\mathcal{D}G$ ist abelsch

(iii) Ist A abelsche Gruppe und $\varphi : G \to A$ ein Homomorphismus, so gilt $\mathcal{D}G \subseteq \ker(\varphi)$.

Beweis:

(i) Für $g, a, b \in G$ gilt $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$ (nachrechnen), also gilt für alle $g \in G,\ a_1, \dots, a_s, b_1, \dots, b_s \in G$, dass
$$g[a_1, b_1] \cdots [a_s, b_s]g^{-1} \in \mathcal{D}G$$
also $g\mathcal{D}Gg^{-1} \subseteq \mathcal{D}G$ für alle $g \in G \Rightarrow \mathcal{D}G \trianglelefteq G$.

(ii) Sei $g, h \in G$. Es folgt wegen $gh = [g,h]hg$, dass
$$gh\mathcal{D}G = \underbrace{[g,h]}_{\in \mathcal{D}G} hg\mathcal{D}G = hg\mathcal{D}G$$
und damit, dass $G/\mathcal{D}G$ abelsch ist.

(iii) Für alle $g, h \in G$ gilt
$$\varphi([g,h]) = [\varphi(g), \varphi(h)] = e_A, \text{ weil } A \text{ abelsch ist,}$$
also
$$\{[g,h] \mid g, h \in G\} \subseteq \ker(\varphi) \Rightarrow \mathcal{D}G \subseteq \ker(\varphi)$$
□

Man definiert rekursiv
$$\mathcal{D}^0 G = G,\ \mathcal{D}^1 G = G,\ \mathcal{D}^{k+1} G = \mathcal{D}(\mathcal{D}^k G)$$
Es folgt $D^{k+1}G \trianglelefteq G$.
Genauer: $D^{k+1}G \trianglelefteq G$ mit Induktion
$$a, b \in \mathcal{D}^k G \Rightarrow g[a,b]g^{-1} = [\underbrace{gag^{-1}}_{\in \mathcal{D}^k G}, \underbrace{gbg^{-1}}_{\in \mathcal{D}^k G}] \in D^{k+1}G$$
also $g(D^{k+1}G)g^{-1} \subseteq D^{k+1}G$.

2.23 Satz 11

Eine Gruppe G ist auflösbar genau dann, wenn gilt $D^m G = \{e\}$ für ein $m \geq 0$.

Beweis:
Angenommmen, $D^m G = \{e\}$ für ein $m \geq 0$. Dann ist $\mathcal{D}^0 G \supseteq \mathcal{D}^1 G \supseteq \cdots \supseteq \mathcal{D}^m G = \{e\}$ eine Normalreihe und $\mathcal{D}^k G/\mathcal{D}^{k+1}G = \mathcal{D}^k G/\mathcal{D}(\mathcal{D}^k G)$ ist abelsch nach 2.22(ii), also ist G auflösbar.
Ist umgekehrt G auflösbar und $G = G_m \trianglelefteq \ldots \trianglelefteq G_0 = \{e\}$ eine Normalreihe mit abelschen Faktoren, so folgt aus 2.22(iii), dass $\mathcal{D}G_k \subseteq G_{k+1}$, also iteriert auch
$$D^{l+1} G_k \subseteq D^l G_{k-1}$$
$$\Rightarrow \mathcal{D}^m G = \mathcal{D}^m G_m \subseteq \mathcal{D}^{m-1} G_{m-1} \subseteq \cdots \subseteq \mathcal{D}^0 G_0 = \{e\}$$
□

Korollar

Bilder und Untergruppen von auflösbaren Gruppen sind wieder auflösbar.

Beweis:
Sei $\varphi : G \to K$ Homomorphismus und G auflösbar, $D^m G = \{e\}$. Wegen

$$\varphi([a, b]) = \varphi(aba^{-1}b^{-1}) = [\varphi(a), \varphi(b)]$$

folgt

Bilder von Komutatoren sind Komutatoren

$$\mathcal{D}^m(\varphi(G)) = \varphi(\mathcal{D}^m G) = \varphi(e_G) = \{e_K\}$$

Ist $H \subseteq G$, so folgt $\mathcal{D}^k H \subseteq \mathcal{D}^k G$ für alle $k \geq 0$, also

$$\mathcal{D}^m G\{e_g\} \Rightarrow D^m H = \{e_G\}$$

Also folgt mit dem Satz von oben, dass H auflösbar ist. □

2.24 Definition perfekt

Eine Gruppe G heißt **perfekt**, wen gilt $\mathcal{D}G = G$.
Eine Gruppe, die gleichzeitig perfekt und auflösbar ist, ist trivial.

2.25 Die symmetrischen und alternierenden Gruppen

Sei $\mathrm{Sym}(n)$ die Gruppe aller Permutationen der Menge $\{1, \ldots, n\}$. Es gilt $\#\,\mathrm{Sym}(n) = n! = n(n-1)(n-2)\cdots 2 \cdot 1$, denn $\mathrm{Sym}(n)$ wirkt transitiv auf der n-elementigen Menge $\{1, \ldots, n\}$.
Der Stabilisator von n ist isomorph zu $\mathrm{Sym}(n-1)$.

$$\overset{\text{Bahnengl.}}{\Rightarrow} \#\,\mathrm{Sym}(n) = n \cdot \mathrm{Sym}(n-1) \text{ und } \#\,\mathrm{Sym}(1) = 1$$

Erinnerung an LAII, Kapitel über Determinanten, 4.6.

abelsche Gruppe der ordnung 2 bzgl. Multiplikation

Für $\pi \in \mathrm{Sym}(n)$ setze $\mathrm{sign}(\pi) = \prod_{i<j} \frac{\pi(i)-\pi(j)}{i-j} \in \{\pm 1\} = C_2$.
$\mathrm{sign} : \mathrm{Sym}(n) \to C_2$ ist ein Homomorphismus.
Der kern von sign ist die alternierende Gruppe

$$\mathrm{Alt}(n) = \{\pi \in \mathrm{Sym}(n) \mid \mathrm{sign}(\pi) = 1\}$$

Aus 2.22 folgt $\mathcal{D}\,\mathrm{Sym}(n) \subseteq \mathrm{Alt}(n)$, weil C_2 abelsch ist.

Satz

Es gilt $\mathcal{D}\,\mathrm{Sym}(n) = \mathrm{Alt}(n)$. Für $n \geq 5$ ist $\mathrm{Alt}(n)$ perfekt.

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar!*

Abbildungsverzeichnis