KAPITEL 4

Nebenklassen, Normalteiler und Faktorgruppen

1. Produkte von Teilmengen einer Gruppe

Sei G eine multiplikativ geschriebene Gruppe. Für nichtleere Teilmengen $A, B \subseteq G$ definieren wir

$$AB = \{ab : a \in A, b \in B\}.$$

Hat A nur ein Element, d.h. $A = \{a\}$, so schreiben wir auch aB statt $\{a\}B$, also

$$aB = \{ab : b \in B\},$$

und analog $Ab = A\{b\}$.
Ist C eine weitere nichtleere Teilmenge von G, so gilt

$$(AB)C = A(BC) = \{abc : a \in A, b \in B, c \in C\}.$$

LEMMA. *Ist H eine Untergruppe einer Gruppe G, so gilt*

$$HH = H.$$

Beweis:

- $\subseteq$ Da mit $h_1, h_2 \in H$ natürlich $h_1 h_2 \in H$ gilt, folgt
$$HH = \{h_1 h_2 : h_1, h_2 \in H\} \subseteq \{h : h \in H\} = H.$$
- $\supseteq$ Ist e das neutrale Element von G, so gilt auch $e \in H$, und damit für jedes $h \in H$
$$h = e \cdot h \in HH, \text{ also } \quad H \subseteq HH.$$

Insgesamt ergibt sich

$$HH = H,$$

wie behauptet. ■

2. Kongruenz modulo einer Untergruppe und Nebenklassen

DEFINITION. *Ist G eine (multiplikativ geschriebene) Gruppe und H eine Untergruppe, so definieren wir für $x, y \in G$*

$$x \equiv y \bmod H \quad \Longleftrightarrow \quad x^{-1}y \in H,$$

und sagen x **ist kongruent zu** *y* **modulo** *H.*
Schreibt man G additiv, so lautet die Bedingung

$$x \equiv y \bmod H \quad \Longleftrightarrow \quad -x + y \in H.$$

Beispiel: Wir betrachten $(\mathbb{Z}, +)$ und eine Untergruppe $\mathbb{Z}\,d$ mit $d \in \mathbb{Z}$. Dann gilt:

$$x \equiv y \bmod \mathbb{Z}\,d \quad \Longleftrightarrow \quad -x + y \in \mathbb{Z}\,d \quad \Longleftrightarrow \quad x - y \in \mathbb{Z}\,d \quad \Longleftrightarrow \quad d \mid x - y.$$

LEMMA. *Sei G eine (multiplikativ geschriebene) Gruppe und H eine Untergruppe.*

(1) *Die Kongruenz modulo H definiert eine Äquivalenzrelation auf G, d.h. für $x, y \in G$ gilt:*
   - *(Transitivität)* $x \equiv y \bmod H, \quad y \equiv z \bmod H, \quad \Longrightarrow \quad x \equiv z \bmod H.$
   - *(Reflexivität)* $x \equiv x \bmod H.$

- *(Symmetrie)* $x \equiv y \bmod H \quad \Longrightarrow \quad y \equiv x \bmod H$.

(2) *Äquivalent sind folgende Aussagen für* $x, y \in G$*:*
   (a) $x \equiv y \bmod H$.
   (b) $y^{-1}x \in H$.
   (c) $x \in yH$*, d.h. es gibt ein* $h \in H$ *mit* $x = yh$.
   (d) $xH = yH$.
   (e) $xH \cap yH \neq \emptyset$.

(3) *Die Äquivalenzklasse von* x *ist* xH*, d.h.*

$$\{y \in G : y \equiv x \bmod H\} = xH.$$

Beweis:

(1)
- (Transitivität) $x \equiv y \bmod H$ und $y \equiv z \bmod H$ bedeutet $x^{-1}y \in H$ und $y^{-1}z \in H$. Als Untergruppe ist H abgeschlossen unter Multiplikation, woraus $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, und damit $x \equiv z \bmod H$ folgt.
- (Reflexivität) Ist 1 das neutrale Element von G, so gilt auch $1 \in H$, und damit für $x \in G$ natürlich $x^{-1}x = 1 \in H$, also $x \equiv x \bmod H$.
- (Symmetrie) Gilt $x \equiv y \bmod H$, so ist $x^{-1}y \in H$. Da H als Untergruppe abgeschlossen unter Inversenbildung ist, folgt $y^{-1}x = (x^{-1}y)^{-1} \in H$, also $y \equiv x \bmod H$.

(2)
- (a)$\Longrightarrow$(b) $x \equiv y \bmod H$ heißt $x^{-1}y \in H$. Da auch das Inverse in H ist, folgt $y^{-1}x = (x^{-1}y)^{-1} \in H$.
- (b)$\Longrightarrow$(c) Ist $y^{-1}x \in H$, schreiben wir $y^{-1}x = h$, so folgt $x = yh \in yH$.
- (c)$\Longrightarrow$(d) Aus $x \in yH$ folgt $\{x\} \subseteq yH$, und damit $xH \subseteq yHH = yH$. Es gibt $h \in H$ mit $x = yh$. Dann ist $y = xh^{-1} \in xH$, und wie eben folgt $yH \subseteq xH$. Insgesamt ergibt sich $xH = yH$.
- (d)$\Longrightarrow$(e) Dies ist trivial.
- (e)$\Longrightarrow$(a) Sei $z \in xH \cap yH$. Dann gibt es $h_1, h_2 \in H$ mit $z = xh_1 = yh_2$. Es folgt $y = xh_1h_2^{-1}$, und damit $x^{-1}y = x^{-1}xh_1h_2^{-1} = h_1h_2^{-1} \in H$, also $x \equiv y \bmod H$.

(3) Dies folgt aus der Definition:

$$\begin{aligned} y \in \{y \in G : y \equiv x \bmod H\} \quad &\Longleftrightarrow \quad y \equiv x \bmod H \equiv \Longleftrightarrow \quad x \equiv y \bmod H \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad x^{-1}y \in H \quad \Longleftrightarrow \quad y \in xH, \end{aligned}$$

also

$$\{y \in G : y \equiv x \bmod H\} = xH,$$

wie behauptet. ■

Definition. *Sei* G *eine Gruppe und* H *eine Untergruppe von* G*.*

(1) *Eine* **Linksnebenklasse** *von* H *in* G *ist eine Teilmenge von* G *der Form*

$$aH = \{ah : h \in H\}$$

mit $a \in G$*.*

(2) *Die Menge der Linksnebenklassen von* H *in* G *wird mit* G/H *bezeichnet, also*

$$G/H = \{aH : a \in G\}.$$

Die Mächtigkeit von G/H *bezeichnet man auch als* **Index** *von* H *und* G *und schreibt*

$$[G : H] = |G/H|$$

oder auch $(G : H)$*.*

(3) *Eine* **Rechtsnebenklasse** *von* H *in* G *ist eine Teilmenge von* G *der Form*

$$Ha = \{ha : h \in H\}$$

mit $a \in G$*.*

(4) *Die Menge der Rechtsnebenklassen von H in G wird mit $H\backslash G$ bezeichnet, also*

$$H\backslash G = \{Ha : a \in G\}.$$

(Achtung! $H\backslash G$ sollte man nicht mit der Mengendifferenz $H\backslash G = \{h \in H : h \notin G\}$ verwechseln, die hier natürlich die leere Menge ist.)

Bemerkungen und Bezeichnungen: Sei G eine Gruppe und H eine Untergruppe.

(1) Die Äquivalenzklasse von a bezüglich der Kongruenz modulo H bezeichnet man auch oft mit $\overline{a}$ und nennt sie auch die Restklasse von a modulo H. Dann gilt also

$$\overline{a} = aH.$$

Die Menge der Äquivalenzklassen ist dann G/H, also

$$G/H = \{\overline{a} : a \in H\}.$$

Es gilt dann:

$$a \equiv b \bmod H \quad \Longleftrightarrow \quad \overline{a} = \overline{b} \quad \Longleftrightarrow \quad aH = bH.$$

(Bei Verwendung der Schreibweise $\overline{a}$ muss natürlich klar sein, welche Untergruppe H hier zugrundeliegt.)

(2) Die Abbildung, die jedem $a \in G$ seine Äquivalenzklasse $\overline{a} = aH$ zuordnet, bezeichnet man auch als **kanonische Abbildung**

$$\pi : G \to G/H, \quad a \mapsto \overline{a} = aH.$$

(3) Unter einem **Repräsentantensystem** von G/H (G modulo H) verstehen wir eine Menge $a_i, i \in I$ von Elementen von G, sodass gilt:
- Für jedes $a \in G$ gibt es ein a_i mit $a \equiv a_i \bmod H$.
- Es gilt $a_i \not\equiv a_j \bmod H$ für alle $i \neq j$.

Alternativ kann man das auch so ausdrücken:
- $G = \bigcup_{i\in I} a_i H$.
- $a_i H \neq a_j H$ für $i \neq j$. (Dies ist äquivalent mit $a_i H \cap a_j H = \emptyset$.)

(4) Alle Äquivalenzklassen aH sind gleichmächtig. (Dies sieht man auch daran, dass $H \mapsto aH$, $h \mapsto ah$ offensichtlich bijektiv ist.) Ist also $a_i, i \in I$, ein Repräsentantensystem der Äquivalenzklassen, so ist G die disjunkte Vereinigung der Nebenklassen $a_i H$, also

$$G = \bigcup_{i\in I} a_i H \quad \text{mit} \quad a_i H \cap a_j H = \emptyset \text{ für } i \neq j.$$

Da die Indexmenge I gleichmächtig wie G/H ist, ergibt sich sofort folgender Satz:

Satz (Lagrange). *Ist G eine endliche Gruppe und H eine Untergruppe von G, so gilt*

$$|G| = |G/H| \cdot |H| = [G : H] \cdot |H|.$$

Insbesondere gilt

$$|H| \mid |G|.$$

(Die Untergruppenordnung teilt die Gruppenordnung.)

Bemerkung: Ist $H = \{e\}$, so erhält man

$$|G| = [G : \{e\}].$$

Der letzte Satz lässt sich leicht verallgemeinern:

Satz. *Sei G eine Gruppe und H, K Untergruppen mit $K \subseteq H \subseteq G$. Dann ist natürlich K auch eine Untergruppe von H. Sind zwei der Indizes $[G : H]$, $[G : K]$, $[H : K]$ endlich, so auch der dritte, und es gilt*

$$[G : K] = [G : H] \cdot [H : K].$$

Beweis: Sei $x_i, i \in I$ ein Repräsentantensystem von G/H, d.h.

$$G = \bigcup_{i\in I} x_i H, \quad x_i H \neq x_j H \text{ für } i \neq j, \quad |I| = [G : H]$$

und $y_j, j \in J$ ein Repräsentantensystem von H/K, d.h.

$$H = \bigcup_{j\in J} y_j K, \quad y_j K \neq y_k K \text{ für } j \neq k, \quad |J| = [H : K].$$

Wir wollen zeigen, dass $x_i y_j, (i, j) \in I \times J$ ein Repräsentantensystem von G/K ist.

- Aus
$$H = \bigcup_{j\in J} y_j K \quad \text{folgt} \quad x_i H = \bigcup_{j\in J} x_i y_j K,$$
und damit
$$G = \bigcup_{i\in I} x_i H = \bigcup_{i\in I} \bigcup_{j\in J} x_i y_j K.$$
Dies impliziert
$$G/K = \{x_i y_j K : (i, j) \in I \times J\}.$$
Wir müssen noch zeigen, dass $x_i y_j, (i, j) \in I \times J$ jede Nebenklasse nur einmal liefert.
- Es gelte also $x_i y_j K = x_k y_l K$. Aus $\{1\} \subseteq K \subseteq H$ sieht man $KH = H$. Multiplizieren wir also $x_i y_j K = x_k y_l K$ von rechts mit H, so folgt
$$x_i y_j H = x_k y_l H.$$
Nun gilt aber $y_j, y_l \in H$, und damit $y_j H = y_l H = H$, sodass weiter
$$x_i H = x_k H$$
gilt. Da die x_i die alle Nebenklassen von H in G repräsentieren, folgt $i = j$.
Unter Beachtung von $x_i = x_k$ folgt aus $x_i y_j K = x_k y_l K$ durch Linksmultiplikation mit x_i^{-1} sofort $y_j K = y_l K$. Da die y_j ein Repräsentantensystem von H/K sind, folgt $j = l$.

Damit haben wir gezeigt, dass $x_i y_j, (i, j) \in I \times J$ ein Repräsentantensystem von G/K ist. Damit erhalten wir

$$[G : K] = |G/K| = |I| \cdot |J| = |G/H| \cdot |H/K| = [G : H] \cdot [H : K],$$

was wir zeigen wollten. ■

Rechtsnebenklassen: Die bijektive Abbildung $G \to G$, $x \mapsto x^{-1}$ bildet Linksnebenklassen aH auf Rechtsnebenklassen Ha^{-1} ab und liefert daher eine Bijektion

$$G/H \to H\backslash G, \quad aH \mapsto Ha^{-1}.$$

Allerdings müssen Linksnebenklassen keine Rechtsnebenklassen sein, wie das folgende Beispiel zeigt.

Beispiel: In der symmetrischen Gruppe S_3 betrachten wir die Untergruppe $H = \langle(12)\rangle = \{(1), (12)\}$. Es ist

$$H = \{(1), (12)\}, \quad (13)H = \{(13), (123)\}, \quad (23)H = \{(23), (132)\}$$

und

$$H = \{(1), (12)\}, \quad H(13) = \{(13), (132)\}, \quad H(23) = \{(23), (123)\}.$$

Die Linksnebenklassen stimmen hier also nicht mit den Rechtsnebenklassen überein.

Frage: Sei G eine Gruppe und H eine Untergruppe. Können wir dann eine Verknüpfung auf G/H einführen, die mit der Verknüpfung auf G verträglich ist? Gilt also

$$x_1 \equiv x_2 \bmod H \text{ und } y_1 \equiv y_2 \bmod H \quad \Longrightarrow \quad x_1 y_1 \equiv x_2 y_2 \bmod H\,?$$

Das folgende Beispiel zeigt, dass dies nicht der Fall sein muss.

Beispiel: Wir betrachten wieder $G = S_3$ mit $H = \langle(12)\rangle$. Die Linksnebenklassen, also Restklassen modulo H, sind

$$H = \{(1), (12)\}, \quad (13)H = \{(13), (123)\}, \quad (23)H = \{(23), (132)\}.$$

Nun gilt:

$$(13) \equiv (123) \bmod H \quad \text{und} \quad (23) \equiv (132) \bmod H.$$

Es ist

$$(13)(23) = (132) \quad \text{und} \quad (123)(132) = (1),$$

also

$$(13)(23) \not\equiv (123)(132) \bmod H.$$

Die Multiplikation lässt sich nicht einfach auf G/H fortsetzen.

Überlegung: Sei G eine Gruppe und H eine Untergruppe. Wann gilt:

$$x_1 \equiv x_2 \bmod H \text{ und } y_1 \equiv y_2 \bmod H \implies x_1y_1 \equiv x_2y_2 \bmod H\,?$$

Wir schreiben $x_1 = x_2h$ und $y_1 = y_2k$ mit $h, k \in H$. Dann gilt

$$(x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_1^{-1}x_2y_2 = k^{-1}y_2^{-1}h^{-1}x_2^{-1}x_2y_2 = k^{-1}y_2^{-1}h^{-1}y_2.$$

Also:

$$x_1y_1 \equiv x_2y_2 \bmod H \iff k^{-1}y_2^{-1}h^{-1}y_2 \in H \iff y_2^{-1}h^{-1}y_2 \in H.$$

Wollen wir, dass dies für alle $y_2 \in G$ und alle $h \in H$ gilt, so kommen wir auf die Bedingung $xHx^{-1} \subseteq H$ für alle $x \in G$. Wie vor vorhin gesehen haben, erfüllt nicht jede Untergruppe diese Bedingung. Untergruppen, die diese Bedingung aber erfüllen, spielen eine wichtige Rolle und werden im nächsten Abschnitt behandelt.

3. Normalteiler

Definition. *Eine Untergruppe H einer Gruppe G heißt* **Normalteiler** *von G (oder* **normale Untergruppe** *von G), wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

1. *$aHa^{-1} \subseteq H$ für alle $a \in G$, d.h. für alle $a \in G$ und alle $h \in H$ gilt $aha^{-1} \in H$.*
2. *$aH = Ha$ für alle $a \in G$, d.h. jede Linksnebenklasse ist auch Rechtsnebenklasse.*
3. *$aHa^{-1} = H$.*

Man nennt dann die zu a gehörige Nebenklasse aH auch die **Restklasse von** *a* **modulo** *H. Man schreibt dafür auch $\overline{a}$, wenn klar ist, welche Untergruppe H zugrundeliegt.*

Beweis der Äquivalenz der Bedingungen: Es gelte Bedingung (1). Für a liefert die Bedingung durch Multiplikation mit a von rechts:

$$aHa^{-1} \subseteq H \implies aH \subseteq Ha.$$

Für a^{-1} liefert die Bedingung durch Multiplikation mit a von links, und dann mit a^{-1} von rechts:

$$a^{-1}H(a^{-1})^{-1} \subseteq H \implies a^{-1}Ha \subseteq H \implies Ha \subseteq aH \implies H \subseteq aHa^{-1}.$$

Daraus kann man sofort

$$aH = Ha \quad \text{und} \quad aHa^{-1} = H$$

ablesen, also die Bedingungen (2) und (3). Da natürlich (1) aus (3) folgt, haben wir die Äquivalenz der Bedingungen bewiesen. ■

Beispiele:

1. Ist e das neutrale Element von G, so sind $\{e\}$ und G Normalteiler von G, die „trivialen“ Normalteiler von G.
2. Ist G eine abelsche Gruppe, so ist jede Untergruppe ein Normalteiler.

Das folgende Lemma enthält wichtige Beispiele von Normalteilern.

Lemma. *Sei G eine Gruppe.*

1. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus und ist $N \subseteq H$ ein Normalteiler in H, so ist $\phi^{-1}(N)$ ein Normalteiler in G.*
2. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, so ist* $\mathrm{Kern}(\phi)$ *ein Normalteiler von G.*
3. *Ist $\phi : G \to H$ ein surjektiver Gruppenhomomorphismus und N ein Normalteiler in G, so ist $\phi(N)$ ein Normalteiler in H.*

(4) *Ist N_i, $i \in I$, eine Familie von Normalteilern in G, so ist auch der Durchschnitt $\bigcap_{i\in I} N_i$ ein Normalteiler in G.*
(5) *Das Zentrum $Z(G)$ ist ein Normalteiler von G.*
(6) *Ist $H \subseteq G$ eine Untergruppe vom Index 2, so ist H ein Normalteiler von G.*

Beweis:

(1) Sei $g \in G$ und $n \in \phi^{-1}(N)$, d.h. $\phi(n) \in N$. Dann ist
$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} \in N,$$
da N ein Normalteiler ist, also
$$gng^{-1} \in \phi^{-1}(N).$$
Dies zeigt, dass $\phi^{-1}(N)$ ein Normalteiler in G ist.
(2) Dies ist eine Konsequenz aus (1), da $\mathrm{Kern}(\phi) = \phi^{-1}(\{e_H\})$ ist und $\{e_H\}$ Normalteiler in H ist. Wir geben aber nochmals einen direkten Beweis: Sei $a \in G$ und $h \in \mathrm{Kern}(\phi)$, d.h. $\phi(h) = e_H$. Dann gilt
$$\phi(aha^{-1}) = \phi(a)\phi(h)\phi(a^{-1}) = \phi(a)\phi(a)^{-1} = e_H, \text{ also } aha^{-1} \in \mathrm{Kern}(\phi).$$
Daher ist $\mathrm{Kern}(\varphi)$ ein Normalteiler.
(3) Seien $\widetilde{g} \in H$ und $\widetilde{n} \in \phi(N)$. Wegen der Surjektivität gibt es ein $g \in G$ mit $\widetilde{g} = \phi(g)$ und natürlich ein $n \in N$ mit $\widetilde{n} = \phi(n)$. Dann ist
$$\widetilde{g}\widetilde{n}\widetilde{g}^{-1} = \phi(g)\phi(n)\phi(g)^{-1} = \phi(gng^{-1}) \in \phi(N),$$
da $gng^{-1} \in N$ wegen der Normalteilereigenschaft von N gilt. Dies beweist, dass $\phi(N)$ ein Normalteiler in H ist.
(4) Sei $g \in G$ und $n \in \cap_{i\in I} N_i$. Da N_i Normalteiler ist, gilt $gng^{-1} \in N_i$. Daraus folgt direkt $gng^{-1} \in \cap_{i\in I} N_i$. Dies zeigt, dass $\cap_{i\in I} N_i$ ein Normalteiler in G ist.
(5) Sei $z \in Z(G)$ und $g \in G$. Dann gilt
$$gzg^{-1} = gg^{-1}z = z \in Z(G),$$
da z mit allen Elementen aus G kommutiert. Also ist $Z(G)$ ein Normalteiler von G.
(6) Ist $a \in G \setminus H$, so haben wir die disjunkten Zerlegungen in Links- und Rechtsnebenklassen.
$$G = H \cup aH \quad \text{und} \quad G = H \cup Ha.$$
Daraus folgt sofort $aH = Ha$, also ist H ein Normalteiler. ■

Beispiele: Wir betrachten Untergruppen der symmetrischen Gruppe S_4.

(1) Es gibt genau drei Permutationen vom Typ $(2,2)$, nämlich
$$a = (12)(34), \quad b = (13)(24), \quad c = (14)(23).$$
Man rechnet nach, dass gilt
$$a^2 = b^2 = c^2 = (1), \quad ab = ba, \quad ac = ca, \quad bc = cb, \quad abc = (1).$$
Daher ist
$$V = \{(1), (12)(34), (13)(24), (14)(23)\} = \{(1), a, b, c\}$$
eine Untergruppe von S_4. Man überprüft auch leicht, dass
$$\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to V \quad \text{mit} \quad \phi((0,0)) = (1), \quad \phi((0,1)) = a, \quad \phi((1,0)) = b, \quad \phi((1,1)) = c$$
ein Gruppenisomorphismus ist. Also ist
$$V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,$$
d.h. V ist isomorph zur Kleinschen Vierergruppe.
Da bei Konjugation der Typ einer Permutation festbleibt, gilt $\sigma V \sigma^{-1} \subseteq V$ für alle $\sigma \in S_4$. Also ist V ein Normalteiler von S_4.

(2) Wir betrachten die Untergruppe

$$H = \langle (123) \rangle = \{(1), (123), (132)\}.$$

Für $\sigma = (14)$ gilt

$$\sigma(123)\sigma^{-1} = (423) \notin H.$$

Also ist H kein Normalteiler von S_4.

4. Faktorgruppen

LEMMA. *Ist G eine Gruppe und H ein Normalteiler in G, so gilt*

$$x_1 \equiv x_2 \bmod H \text{ und } y_1 \equiv y_2 \bmod H \quad \Longrightarrow \quad x_1 y_1 \equiv x_2 y_2 \bmod H.$$

Daher wird durch

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

eine Verknüpfung auf G/H definiert, die G/H zu einer Gruppe und die kanonische Abbildung $\pi : G \to G/H$ zu einem surjektiven Gruppenhomomorphismus mit Kern H gemacht. Man nennt G/H dann die **Faktorgruppe** *von G nach H oder von G modulo H.*

Beweis:

(1) Es gelte $x_1 \equiv x_2 \bmod H$ und $y_1 \equiv y_2 \bmod H$. Dann gibt es $h, k \in H$ mit $x_1 = x_2 h$ und $y_1 = y_2 k$. Es folgt

$$x_1 y_1 = (x_2 h)(y_2 k) = x_2 y_2 \cdot y_2^{-1} h y_2 \cdot k.$$

Da H ein Normalteiler ist, gilt $y_2^{-1} h y_2 \in H$, also auch $y_2^{-1} h y_2 k \in H$, und damit

$$x_1 y_1 \equiv x_2 y_2 \bmod H,$$

wie behauptet.

(2) Definieren wir eine Verknüpfung auf G/H durch

$$\overline{x} \cdot \overline{y} = \overline{xy},$$

so hängt dies Verknüpfung nicht von den ausgewählten Repräsentanten ab, ist also wohldefiniert. Mit der kanonischen Abbildung $\pi : G \to G/H$ ausgedrückt haben wir also

$$\pi(xy) = \pi(x)\pi(y).$$

(3) Man zeigt leicht, dass G/H mit der angegebenen Verknüpfung eine Gruppe ist und π dann ein Gruppenhomomorphismus.

(4) Natürlich ist π surjektiv. Es gilt:

$$\begin{aligned} x \in \mathrm{Kern}(\pi) \quad &\Longleftrightarrow \quad \pi(x) = \overline{e} \quad \Longleftrightarrow \quad \overline{x} = \overline{e} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad x \equiv e \bmod H \Longleftrightarrow \quad xH = eH = H \quad \Longleftrightarrow \quad x \in H, \end{aligned}$$

also $\mathrm{Kern}(\pi) = H$, wie behauptet. ■

Bemerkung: Ist G eine Gruppe und H ein Normalteiler in G, so gilt für das Mengenprodukt zweier Nebenklassen xH und yH wegen $Hy = yH$ und $HH = H$

$$(xH)(yH) = x(Hy)H = x(yH)H = xyHH = xyH.$$

Das Produkt zweier Nebenklassen ist also wieder eine Nebenklasse. Wir hätten daher auch direkt die Verknüpfung auf G/H so einführen können.

Beispiel: Wir betrachten die Diedergruppe G der Ordnung 8, erzeugt von δ und σ mit

$$\mathrm{ord}\,(\delta) = 4, \quad \mathrm{ord}\,(\sigma) = 2 \quad \text{und } \sigma\delta\sigma^{-1} = \delta^{-1},$$

wobei wir 1 für das neutrale Element δ^0 schreiben. Es ist

$$G = \{1, \delta, \delta^2, \delta^3, \sigma, \delta\sigma, \delta^2\sigma, \delta^3\sigma\}.$$

Das Zentrum ist $Z(G) = \{1, \delta^2\}$. Wir betrachten die Restklassen modulo $Z(G)$:

$$\begin{aligned} \overline{1} = \overline{\delta^2} &= \{1, \delta^2\}, \\ \overline{\delta} = \overline{\delta^3} &= \{\delta, \delta^3\}, \\ \overline{\sigma} = \overline{\delta^2\sigma} &= \{\sigma, \delta^2\sigma\}, \\ \overline{\delta\sigma} = \overline{\delta^3\sigma} &= \{\delta\sigma, \delta^3\sigma\}. \end{aligned}$$

Die Faktorgruppe ist

$$G/H = \{\overline{1}, \overline{\delta}, \overline{\sigma}, \overline{\delta\sigma}\}.$$

Es ist

$$\overline{\delta}^2 = \overline{\delta^2} = \overline{1}, \quad \overline{\sigma}^2 = \overline{\sigma^2} = \overline{1}, \quad \overline{\delta\sigma}^2 = \overline{\delta\sigma\delta\sigma} = \overline{\delta\sigma\delta\sigma^{-1}} = \overline{\delta\delta^{-1}} = \overline{1}.$$

Alle von $\overline{1}$ verschiedenen Elemente von G/H haben also Ordnung 2. Weiter gilt

$$\overline{\delta} \cdot \overline{\sigma} \cdot \overline{\delta\sigma} = \overline{\delta\sigma\delta\sigma} = \overline{\delta\sigma\delta\sigma^{-1}} = \overline{\delta\delta^{-1}} = \overline{1}.$$

Daraus sieht man schnell, dass G/H isomorph zur Kleinschen Vierergruppe ist:

$$G/H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Nun betrachten wir ein Beispiel mit Gruppen in additiver Schreibweise.

Beispiel: Sei $G = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ und $H = \langle 4 \rangle = \{0, 4\}$. Die Restklassen sind

$$\begin{aligned} \overline{0} = \overline{4} &= \{0, 4\}, \\ \overline{1} = \overline{5} &= \{1, 5\}, \\ \overline{2} = \overline{6} &= \{2, 6\}, \\ \overline{3} = \overline{7} &= \{3, 7\}. \end{aligned}$$

Es ist

$$\begin{aligned} 2 \cdot \overline{1} &= \overline{1} + \overline{1} = \overline{1+1} = \overline{2}, \\ 3 \cdot \overline{1} &= \overline{1} + \overline{1} + \overline{1} = \overline{1+1+1} = \overline{3}, \\ 4 \cdot \overline{1} &= \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{1+1+1+1} = \overline{4} = \overline{0}. \end{aligned}$$

Also gilt

$$\operatorname{ord}(\overline{1}) = 4, \quad G/H = \langle \overline{1} \rangle.$$

Beispiel: In S_4 betrachten wir den Normalteiler

$$V = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

Die Linksnebenklassen von V in G sind

$$\begin{aligned} \overline{(1)} &= \{(1), (12)(34), (13)(24), (14)(23)\}, \\ \overline{(12)} &= \{(12), (34), (1324), (1423)\}, \\ \overline{(13)} &= \{(13), (24), (1234), (1432)\}, \\ \overline{(14)} &= \{(14), (23), (1243), (1342)\}, \\ \overline{(123)} &= \{(123), (134), (142), (243)\}, \\ \overline{(124)} &= \{(124), (132), (143), (234)\}. \end{aligned}$$

Wir rechnen nun in der Faktorgruppe S_4/V:

$$\overline{(12)} \cdot \overline{(13)} = \overline{(12)(13)} = \overline{(132)} = \overline{(124)} \quad \text{und} \quad \overline{(13)} \cdot \overline{(12)} = \overline{(13)(12)} = \overline{(123)}.$$

Daraus sieht man, dass S_4/V nicht kommutativ ist.

Der Beweis des folgenden Satzes zeigt eine erste Anwendung von Faktorgruppen.

SATZ. *Ist G eine endliche abelsche Gruppe und p eine Primzahl, die die Gruppenordnung teilt, so gibt es ein Element $g \in G$ mit Ordnung p.*

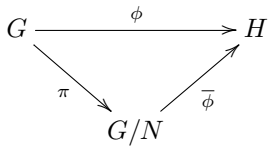
Beweis: Wir schreiben $|G| = pm$ und machen Induktion nach m.

- Im Fall $m = 1$ ist $|G| = p$. Ist $g \in G \setminus \{e_G\}$, so folgt aus $\operatorname{ord}(g) > 1$ und $\operatorname{ord}(g) \mid |G|$ sofort $\operatorname{ord}(g) = p$.
- Sei nun $m \geq 2$ und die Aussage bereits für alle kleineren m bewiesen. Wir wählen ein Element $h \in G \setminus \{e_G\}$ und unterscheiden zwei Fälle:
  - Gilt $p \mid \operatorname{ord}(h)$, so hat
  $$g = h^{\frac{\operatorname{ord}(h)}{p}}$$
  Ordnung p und wir sind fertig.
  - Gilt $p \nmid \operatorname{ord}(h)$, so betrachten wir $H = \langle h \rangle$ und die Faktorgruppe G/H. Wegen $p \nmid |H|$ ist $|G/H| = [G : H] = \frac{|G|}{|H|} = p\,m'$ mit $m' < m$. Nach Induktionsvoraussetzung gibt es ein $\overline{g} \in G/H$ mit $\operatorname{ord}(\overline{g}) = p$. Sei g irgendein Urbild von $\overline{g}$ in G. Dann gilt $\operatorname{ord}(\overline{g}) \mid \operatorname{ord}(g)$, also $p \mid g$. Dann hat
  $$g^{\frac{\operatorname{ord}(g)}{p}}$$
  Ordnung p.

Damit ist die Behauptung durch Induktion bewiesen. ■

Der folgende Satz wird bei Bosch „Homomorphiesatz“ und bei Fischer „Faktorisierungssatz“ genannt.

SATZ. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus und $N \subseteq G$ ein Normalteiler mit $N \subseteq \operatorname{Kern}(\phi)$. Dann gibt es genau einen Gruppenhomomorphismus*
$$\overline{\phi} : G/N \to H,$$
sodass gilt
$$\phi = \overline{\phi} \circ \pi.$$
ϕ „faktorisiert“ also über G/N. Dies drückt sich auch in folgendem sogenannten kommutativen Diagramm aus:



Weiter gilt:
$$\operatorname{Bild}(\overline{\phi}) = \operatorname{Bild}(\phi), \quad \operatorname{Kern}(\overline{\phi}) = \pi(\operatorname{Kern}(\phi)), \quad \operatorname{Kern}(\phi) = \pi^{-1}(\operatorname{Kern}(\overline{\phi})).$$
Insbesondere:

- *Ist $N = \operatorname{Kern}(\phi)$, so ist $\overline{\phi}$ injektiv, also eine Einbettung: $G/\operatorname{Kern}(\phi) \hookrightarrow H$.*
- *Ist $N = \operatorname{Kern}(\phi)$ und ϕ surjektiv, so ist $\overline{\phi}$ ein Isomorphismus: $G/\operatorname{Kern}(\phi) \simeq H$.*

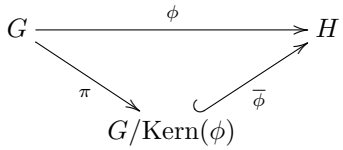
Beweis:

- Wir zeigen zunächst die Eindeutigkeit einer solchen Abbildung $\overline{\phi}$: Ist $x \in G$, so folgt mit $\phi = \overline{\phi} \circ \pi$
  $$\phi(x) = (\overline{\phi} \circ \pi)(x) = \overline{\phi}(\overline{x}).$$
  Also ist $\overline{\phi}$ eindeutig bestimmt.
- Seien $x, y \in G$ mit $\overline{x} = \overline{y}$. Es gibt also ein $n \in N$ mit $x = yn$. Die Voraussetzung $N \subseteq \operatorname{Kern}(\phi)$ liefert $\phi(n) = e_H$, und damit
  $$\phi(x) = \phi(yn) = \phi(y)\phi(n) = \phi(y).$$
  Definieren wir daher $\overline{\phi} : G/N \to H$ durch
  $$\overline{\phi}(\overline{x}) = \phi(x),$$
  so ist $\overline{\phi}$ wohldefiniert.
- Warum ist $\overline{\phi}$ ein Gruppenhomomorphismus?
  $$\overline{\phi}(\overline{x} \cdot \overline{y}) = \overline{\phi}(\overline{xy}) = \phi(xy) = \phi(x)\phi(y) = \overline{\phi}(\overline{x}) \cdot \overline{\phi}(\overline{y}).$$
- $\operatorname{Bild}(\overline{\phi}) = \operatorname{Bild}(\phi)$ ist klar.

- Die restlichen Aussagen folgen ähnlich. ■

Wir erwähnen folgenden wichtigen Spezialfall:

Satz (Noetherscher Homomorphiesatz). *Jeder Gruppenhomomorphismus $\phi : G \to H$ faktorisiert über $G/\mathrm{Kern}(\phi)$:*



Dabei ist $\overline{\phi} : G/\mathrm{Kern}(\phi) \to H$ eine Einbettung. Ist ϕ surjektiv, so ist $\overline{\phi}$ ein Isomorphismus.

Beispiele:

(1) Sei $n \in \mathbb{N}$ und $\phi : \mathbb{Z} \to \mathbb{Z}_n$ der durch $\phi(1) = 1$ definierte Gruppenhomomorphismus, für den $\phi(a) = a \bmod n$ für alle $a \in \mathbb{Z}$ gilt. ϕ ist surjektiv mit Kern $\mathbb{Z}\,n$, sodass wir einen Isomorphismus
$$\mathbb{Z}/\mathbb{Z}\,n \simeq \mathbb{Z}_n$$
erhalten.

(2) Seien $m, n \in \mathbb{Z}$ mit $n \mid m$. Dann haben wir den surjektiven Homomorphismus
$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$
von eben. Es ist $\mathbb{Z}\,m \subseteq \mathrm{Kern}(\phi) = \mathbb{Z}\,n$, also erhalten wir eine induzierte Abbildung
$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_n, \quad \text{also} \quad \mathbb{Z}_m \to \mathbb{Z}_n.$$

(3) Eine Folge $(a_n)_{n\geq 1}$ rationaler Zahlen nennen wir eine Cauchy-Folge, wenn für alle $\varepsilon \in \mathbb{Q}_{>0}$ ein $n_\varepsilon \in \mathbb{N}$ existiert mit der Eigenschaft:
$$m, n \geq n_\varepsilon \quad \Longrightarrow \quad |a_m - a_n| < \varepsilon.$$
Mit der komponentenweisen Addition bildet die Menge dieser Cauchy-Folgen eine abelsche Gruppe:
$$C = \{(a_n)_{n\geq 1} : a_n \in \mathbb{Q}, (a_n) \text{ ist Cauchy-Folge}\}.$$
Cauchy-Folgen konvergieren in $\mathbb{R}$, wir erhalten also einen Gruppenhomomorphismus
$$\phi : C \to \mathbb{R}, \quad (c_n)_{n\geq 1} \mapsto \lim_{n\to\infty} c_n.$$
Man kann zeigen, dass ϕ surjektiv ist. Der Kern von ϕ sind die Nullfolgen:
$$N = \{(a_n)_{n\geq 1} : a_n \in \mathbb{Q}, (a_n) \text{ ist Nullfolge}\}.$$
Daher erhalten wir einen Gruppenisomorphismus
$$C/N \simeq \mathbb{R}.$$
Die Größen links kann man nur mit Hilfe von $\mathbb{Q}$ definieren. Auf diese Weise kann man dann die reellen Zahlen durch den Quotienten C/N definieren.

5. Isomorphiesätze

Oft findet im Zusammenhang mit Faktorgruppen auch sogenannte „Isomorphiesätze“Ẇir erwähnen zwei, die auf Emmy Noether zurückgehen. (Die Zählung ist nicht einheitlich, wir verwenden die Nummerierung des Meusburger-Algebra-Skripts.)

Satz (2. Noetherscher Isomorphiesatz). *Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe und $N \subseteq G$ ein Normalteiler. Dann gilt:*

(1) *HN ist eine Untergruppe von G.*
(2) *$HN = NH$.*
(3) *N ist ein Normalteiler in HN.*
(4) *$H \cap N$ ist ein Normalteiler in H.*

(5) *Die Komposition der kanonischen Abbildungen $H \to HN \to HN/N$ induziert einen Isomorphismus*

$$H/H \cap N \simeq HN/N.$$

Beweis:

(1) Wir überprüfen die Untergruppeneigenschaften:
- Sind $h_1n_1, h_2n_2 \in HN$ (mit $h_1, h_2 \in H$ und $n_1, n_2 \in N$, so gilt
$$h_1n_1h_2n_2 = h_1h_2(h_2^{-1}n_1h_2)n_2.$$
Da N ein Normalteiler ist, ist
$$\widetilde{n} = h_2^{-1}n_1h_2 \in N,$$
und damit
$$h_1n_1 \cdot h_2n_2 = h_1h_2 \cdot \widetilde{n}n_2 \in HN.$$
HN ist also abgeschlossen unter der Verknüpfung.
- Natürlich ist das neutrale Element in HN, da H und N das neutrale Element enthalten.
- Ist $hn \in HN$ mit $h \in H$ und $n \in \mathbb{N}$, so gilt
$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$
Da N Normalteiler ist, gilt
$$\widetilde{n} = hn^{-1}h^{-1} \in N,$$
und damit
$$(hn)^{-1} = h^{-1}\widetilde{n} \in HN.$$
Also ist HN auch abgeschlossen unter Inversenbildung.

Damit ist HN eine Untergruppe von G.

(2) Für $n \in N$, $h \in H$ gilt wegen $h^{-1}nh \in N$:
$$nh = hh^{-1}nh = h(h^{-1}nh) \in HN.$$
Daraus folgt $NH \subseteq HN$. Ist $h \in H$, $n \in N$, so gilt
$$hn = hnh^{-1}h = (hnh^{-1})h \in NH.$$
Es folgt $HN \subseteq NH$, sodass wir insgesamt
$$HN = NH$$
erhalten.

(3) Da N ein Normalteiler in G ist, da $N \subseteq HN$ gilt, ist natürlich N auch ein Normalteiler in HN.

(4) Sei $n \in H \cap N$ und $h \in H$. Da N Normalteiler in G ist, gilt $hnh^{-1} \in N$. Wegen $n \in H \cap N$ gilt auch $hnh^{-1} \in H$, also insgesamt $hnh^{-1} \in H \cap N$. Also ist $H \cap N$ Normalteiler in H.

(5) Wir schreiben
$$\alpha : H \to HN, \quad x \mapsto x \quad \text{und} \quad \pi : HN \to HN/N, \quad y \mapsto \overline{y} = yN.$$
Ist $hn \in HN$ (mit $h \in H$ und $n \in \mathbb{N}$), so gilt
$$\pi(hn) = \pi(h) = \pi(\alpha(h)) = (\pi \circ \alpha)(h).$$
Dies zeigt, dass $\pi \circ \alpha$ surjektiv ist. Was ist der Kern von $\pi \circ \alpha$? Für $h \in H$ gilt:
$$\begin{aligned} h \in \mathrm{Kern}(\pi \circ \alpha) \quad &\iff \quad (\pi \circ \alpha)(h) = \overline{e} \quad \iff \quad \pi(h) = \overline{e} \quad \iff \\ &\iff \quad \overline{h} = \overline{e} \quad \iff \quad h \in N \quad \iff \quad h \in H \cap N. \end{aligned}$$
Damit gilt $\mathrm{Kern}(\pi \circ \alpha) = H \cap N$. Aus
$$\mathrm{Bild}(\pi \circ \alpha) \simeq H/\mathrm{Kern}(\pi \circ \alpha)$$
folgt dann
$$HN/N \simeq H/H \cap N.$$
Dies war zu zeigen. ■

Bemerkung: Sind H_1 und H_2 Untergruppen einer Gruppe G, so muss H_1H_2 keine Untergruppe sein, wie folgendes Beispiel zeigt: Wir betrachten in S_3 die Untergruppen

$$H_1 = \{(1), (12)\} \quad \text{und} \quad H_2 = \{(1), (13)\}.$$

Dann gilt

$$H_1H_2 = \{(1), (13), (12), (132)\} \quad \text{und} \quad H_2H_1 = \{(1), (12), (13), (123)\}.$$

Offensichtlich sind H_1H_2 und H_2H_1 keine Untergruppen, außerdem sind sie verschieden.

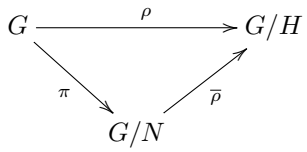
Satz (1. Noetherscher Isomorphiesatz). *G sei eine Gruppe und H, N Normalteiler in G mit $N \subseteq H$. Dann ist N auch Normalteiler von H und es gilt*

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

Beweis: Wir betrachten die natürliche (surjektive) Abbildung

$$\rho : G \to G/H$$

mit Kern H. Wegen $N \subseteq H = \text{Kern}(\rho)$ erhalten wir eine induzierte (surjektive) Abbildung $\overline{\rho}$:



Was ist $\text{Kern}(\overline{\rho})$? Für $x \in G$ gilt:

$$\begin{aligned} \pi(x) \in \text{Kern}(\overline{\rho}) \quad &\iff \quad \overline{\rho}(\pi(x)) = \overline{e} \quad \iff \quad \rho(x) = \overline{e} \quad \iff \\ &\iff \quad x \in \text{Kern}(\rho) \quad \iff \quad x \in H. \end{aligned}$$

Also ist

$$\text{Kern}(\overline{\rho}) = \pi(H),$$

was man auch als H/N schreibt. Es folgt

$$G/H \simeq (G/N)/\pi(H) = (G/N)/(H/N),$$

wie behauptet. ■

6. Normalreihen, einfache und auflösbare Gruppen

Wir führen hier ein paar Begriffe ein, entwickeln aber die Theorie nicht ausführlich.

Definition. *Sei G eine Gruppe. Eine Folge von Untergruppen*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{e\}$$

heißt eine **Normalreihe** *für G, wenn G_{i+1} ein Normalteiler in G_i ist. Die Faktorgruppen G_i/G_{i+1} heißen die* **Faktoren** *der Normalreihe.*

Beispiele:

(1) Da in jeder Gruppe G die Untergruppe $\{e\}$ ein Normalteiler ist, hat man immer die „triviale“ Normalreihe

$$G \supseteq \{e\}.$$

(2) In S_3 betrachten wir die Untergruppe $\langle(123)\rangle$, die ein Normalteiler ist, da sie Index 2 in S_3 hat. Wir erhalten die Normalreihe

$$S_3 \supseteq \langle(123)\rangle \supseteq \{(1)\}$$

mit den Faktoren

$$S_3/\langle(123)\rangle \simeq \mathbb{Z}_2 \quad \text{und} \quad \langle(123)\rangle/\{(1)\} \simeq \mathbb{Z}_3.$$

(3) In S_4 kennen wir die Normalteiler

$$A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (134), (143), (234), (243)\}$$

und

$$V = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

Da V Ordnung 4 hat, ist $\langle(12)(34)\rangle$ ein Normalteiler vom Index 2 (und der Ordnung 2). Wir erhalten also die Normalreihe

$$S_4 \supseteq A_4 \supseteq V \supseteq \langle(12)(34)\rangle \supseteq \{(1)\}$$

mit den Faktoren

$$S_4/A_4 \simeq \mathbb{Z}_2, \quad A_4/V \simeq \mathbb{Z}_3, \quad V/\langle(12)(34)\rangle \simeq \mathbb{Z}_2, \quad \langle(12)(34)\rangle/\{(1)\} \simeq \mathbb{Z}_2.$$

Das folgende Lemma zeigt, wie man aus einer Normalreihe für eine Gruppe G Normalreihen für Untergruppen und Faktorgruppen bzw. für Bilder von surjektiven Gruppenhomomorphismen erhält.

LEMMA. *Sei G eine Gruppe und*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots \supseteq G_m = \{e_G\}$$

eine Normalreihe für G.

(1) *Ist H eine Untergruppe von G, definiert man $H_i = G_i \cap H$, so ist*

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{e_G\}$$

eine Normalreihe für H. Für die Faktoren gilt

$$H_i/H_{i+1} \hookrightarrow G_i/G_{i+1}.$$

(2) *Ist $\phi : G \to H$ ein surjektiver Gruppenhomomorphismus, definiert man $H_i = \phi(G_i)$, so ist*

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{e_H\}$$

eine Normalreihe für H. Für die Faktoren gibt es einen surjektiven Gruppenhomomorphismus

$$G_i/G_{i+1} \to H_i/H_{i+1} \text{ surjektiv.}$$

Beweis:

(1) Natürlich gilt $H = H_0$ und $H_m = \{e_G\}$. Wir zeigen, dass H_{i+1} ein Normalteiler in H_i ist. Ist $h_i \in H_i$ und $h_{i+1} \in H_{i+1}$, so gilt auch $h_i \in G_i$ und $h_{i+1} \in G_{i+1}$. Da G_{i+1} ein Normalteiler in G_i ist, ist $h_i h_{i+1} h_i^{-1} \in G_{i+1}$. Wegen $h_i, h_{i+1} \in H$ gilt auch $h_i h_{i+1} h_i^{-1} \in G_{i+1} \cap H = H_{i+1}$. Dies zeigt, dass H_{i+1} ein Normalteiler in H_i ist. Wir betrachten die natürliche Abbildung

$$\phi : H_i \to G_i \to G_i/G_{i+1}.$$

Offensichtlich ist $\text{Kern}(\phi) = H \cap G_{i+1} = H_{i+1}$, so dass wir eine Einbettung

$$H_i/H_{i+1} \hookrightarrow G_i/G_{i+1}$$

erhalten.

(2) Da ϕ surjektiv ist, gilt $H = \phi(G) = \phi(G_0) = H_0$. Trivialerweise gilt $H_m = \phi(\{e_G\}) = \{e_H\}$. Wir zeigen, dass H_{i+1} ein Normalteiler in H_i ist. Seien also $h_i \in H_i$ und $h_{i+1} \in H_{i+1}$. Wegen der Surjektivität von ϕ gibt es $g_i \in G_i$ und $g_{i+1} \in G_{i+1}$ mit $h_i = \phi(g_i)$ und $h_{i+1} = \phi(g_{i+1})$. Da G_{i+1} normal in G_i ist, gilt $g_i g_{i+1} g_i^{-1} \in G_{i+1}$. Es folgt

$$h_i h_{i+1} h_i^{-1} = \phi(g_i)\phi(g_{i+1})\phi(g_i)^{-1} = \phi(g_i g_{i+1} g_i^{-1}) \in \phi(G_{i+1}) = H_{i+1}.$$

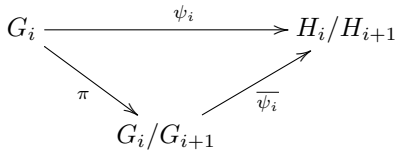
Also ist H_{i+1} normal in H_i. Wir betrachten die Abbildung

$$\psi_i : G_i \to H_i \to H_i/H_{i+1} \text{ mit } \psi_i(g_i) = \overline{\phi(g_i)} = \phi(g_i)H_{i+1}.$$

Wegen $H_i = \phi(G_i)$ ist ψ_i surjektiv. Wegen $H_{i+1} = \phi(G_{i+1})$ gilt

$$G_{i+1} \subseteq \text{Kern}(\psi_i).$$

Also faktorisiert ψ_i über G_i/G_{i+1}:



Da ψ_i surjektiv ist, erhält man für die Faktoren einen surjektiven Gruppenhomomorphismus

$$G_i/G_{i+1} \to H_i/H_{i+1} \text{ surjektiv.}$$

Dies sollte gezeigt werden. ■

Beispiel: Wir betrachten die zuvor beschriebene Normalreihe für die symmetrische Gruppe S_4:

$$S_4 \supseteq A_4 \supseteq V \supseteq \langle(12)(34)\rangle \supseteq \{(1)\}.$$

Also Untergruppe betrachten wir die Gruppe S_3:

$$H = \langle(12),(123)\rangle = \{(1),(12),(13),(23),(123),(132)\}.$$

Dann ist

$$\begin{aligned} S_4 \cap H &= \{(1),(12),(13),(23),(123),(132)\}, \\ A_4 \cap H &= \{(1),(123),(132)\}, \\ V \cap H &= \{(1)\}, \\ \langle(12)(34)\rangle \cap H &= \{(1)\}, \\ \{(1) \cap H &= \{(1)\}. \end{aligned}$$

Das folgende Lemma zeigt, wie man aus der Normalreihe eines Normalteilers N und einer Normalreihe der Faktorgruppe G/N eine Normalreihe der Gruppe G erhält:

LEMMA. *Sei G eine Gruppe mit einem Normalteiler N und $\pi : G \to G/N$ die zugehörige kanonische Abbildung. Seien*

$$G/N = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \overline{M}_2 \supseteq \cdots \supseteq \overline{M}_m = \{\overline{e}\}$$

und

$$N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n = \{e\}$$

Normalreihen für G/N und N. Definiert man $M_i = \pi^{-1}(\overline{M}_i)$, so gilt:

(1) *$M_0 = G$ und $M_m = N$.*
(2) *M_{i+1} ist normal in M_i.*
(3) *Es gilt $M_i/M_{i+1} \simeq \overline{M}_i/\overline{M}_{i+1}$.*
(4) *Eine Normalreihe für G ist*

$$G = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_m = N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n = \{e\}$$

mit den Faktoren

$$M_i/M_{i+1} \simeq \overline{M}_i/\overline{M}_{i+1} \text{ für } i = 0,\ldots,m-1 \quad \text{und} \quad N_i/N_{i+1} \text{ für } i = 0,\ldots,n-1.$$

Beweis:

(1) Dies folgt aus $M_0\pi^{-1}(\overline{M}_0) = \pi^{-1}(G/N) = G$ und $M_m = \pi^{-1}(\overline{M}_m) = \pi^{-1}(\{\overline{e}\}) = N$.
(2) Seien $m_i \in M_i$ und $m_{i+1} \in M_{i+1}$. Da $\overline{M}_{i+1}$ normal in $\overline{M}_i$ ist, gilt $\pi(m_i)\pi(m_{i+1})\pi(m_i)^{-1} \in \overline{M}_{i+1}$, und damit

$$\pi(m_i m_{i+1} m_i^{-1}) = \pi(m_i)\pi(m_{i+1})\pi(m_i)^{-1} \in \overline{M}_{i+1}, \quad \text{also} \quad m_i m_{i+1} m_i^{-1} \in \pi^{-1}(\overline{M}_{i+1}) = M_{i+1}.$$

Dies beweist, dass M_{i+1} normal in M_i ist.

(3) Wir betrachten die Komposition der natürlichen, surjektiven Abbildungen

$$M_i \xrightarrow{\pi} \overline{M}_i \to \overline{M}_i/\overline{M}_{i+1}, \quad x \mapsto \overline{\pi(x)} = \pi(x)\overline{M}_{i+1}.$$

Der Kern ist offensichtlich $\pi^{-1}(\overline{M}_{i+1}) = M_{i+1}$, sodass wir M_{i+1} herausfaktorisieren können und einen Isomorphismus

$$M_i/M_{i+1} \simeq \overline{M}_i/\overline{M}_{i+1}$$

erhalten.

(4) Dies erhält man durch Zusammensetzen der vorangegangenen Punkte. ■

Gruppen, die nur die triviale Normalreihe zulassen, haben einen eigenen Namen:

DEFINITION. *Eine Gruppe $G \neq \{e\}$ heißt* **einfach***, wenn die einzigen Normalteiler die trivialen Normalteiler G und $\{e\}$ sind.*

Bei abelschen Gruppen lässt sich genau sagen, welche einfach sind:

SATZ. *Eine abelsche Gruppe $(A, +)$ ist genau dann einfach, wenn A endlich und von Primzahlordnung ist, d.h. $|A| = p$ mit einer Primzahl p. In diesem Fall ist $A \simeq \mathbb{Z}_p$.*

Beweis: Wir unterscheiden ein paar Fälle:

- **Fall $|A| = \infty$:** Wir wählen ein $a \in A \setminus \{0\}$ und unterscheiden zwei Fälle:
  - Hat a unendliche Ordnung, so auch $2a$ und es gilt
    $$\{0\} \subsetneq \langle 2a\rangle \subsetneq \langle a\rangle \subseteq A.$$
    Also ist $\langle 2a\rangle$ eine nichttriviale Untergruppe von A. Daher ist A nicht einfach.
  - Hat a endliche Ordnung, so gilt
    $$\{0\} \subsetneq \langle a\rangle \subsetneq A,$$
    also ist $\langle a\rangle$ eine nichttriviale Untergruppe von A. Auch in diesem Fall ist A nicht einfach.
- **Fall $1 < |A| < \infty$:** Sei p ein Primteiler von $|A|$. Nach einem früheren Satz existiert ein $a \in A$ mit $\operatorname{ord}(a) = p$.
  - Ist $\langle a\rangle \neq A$, so ist $\langle a\rangle$ eine nichttriviale Untergruppe von A, A ist also nicht einfach.
  - Ist $A = \langle a\rangle$, so ist A zyklisch von Primzahlordnung. Die Untergruppen von A entsprechen genau den Teilern von p, sodass A nur die trivialen Untergruppen besitzt. A ist also einfach. ■

Die symmetrischen Gruppen S_n sind für $n \geq 3$ nie einfach, da sie die alternierende Gruppe A_n als Normalteiler haben. (Es ist $A_n = \operatorname{Kern}(\operatorname{sgn})$.) Dagegen gilt:

SATZ. *Für $n \geq 5$ ist die alternierende Gruppe einfach.*

Den Beweis werden wir später nachholen.

Bemerkung: Zur Klassifikation der endlichen einfachen Gruppen kann man sich den folgenden Artikel aus dem Jahr 2004 anschauen: M. Aschbacher. The Status of the Classification of the Finite Simple Groups.

Der folgende Begriff spielt bei der Behandlung algebraischer Gleichungen eine Rolle. Wir erläutern nur die Grundlagen.

DEFINITION. *Eine Gruppe G heißt* **auflösbar***, wenn G eine Normalreihe mit abelschen Faktoren besitzt, also Untergruppen G_i, $i = 0, \ldots, m$ mit folgenden Eigenschaften:*

- $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{e_G\}$.
- *G_{i+1} ist Normalteiler in G_i.*

- *G_i/G_{i+1} ist eine abelsche Gruppe.*

Beispiele:

(1) $A_2 = \{(1)\}$ und $A_3 = \langle(123)\rangle$ sind als zyklische Gruppe natürlich auflösbar:

$$A_2 = \{(1)\}, \quad A_3 = \langle(123)\rangle \supseteq \{(1)\} \text{ mit } A_3/\{(1)\} \simeq \mathbb{Z}_3.$$

(2) Wir haben gesehen, dass in S_4 die Gruppe

$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$

ein Normalteiler ist. (Es ist $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.) Offensichtlich gilt $V \subseteq A_4$. Daher ist

$$A_4 \supseteq V \supseteq \{(1)\}$$

eine Normalreihe für A_4. Es ist $[A_4 : V] = 3$, also ist $A_4/V \simeq \mathbb{Z}_3$. Daher ist die angegebene Normalreihe abelsch mit den Faktoren

$$A_4/V \simeq \mathbb{Z}_3, \quad V/\{(1)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Die alternierende Gruppe A_4 ist also auflösbar.

Mit den zuvor hergeleiteten Aussagen über Normalreihen kann man leicht die folgenden Aussagen beweisen:

SATZ. *Sei G eine Gruppe.*

(1) *Ist G auflösbar, so auch jede Untergruppe von G.*
(2) *Ist G auflösbar und $\phi : G \to H$ ein surjektiver Gruppenhomomorphismus, so ist auch H auflösbar.*
(3) *Ist N ein Normalteiler in G, so gilt:*

$$G \text{ ist auflösbar} \quad \Longleftrightarrow \quad N \text{ und } G/N \text{ sind auflösbar.}$$

Wir haben gesehen, dass jede endliche abelsche Gruppe, der Gruppenordnung durch eine Primzahl p teilbar ist, ein Element der Ordnung p enthält. Damit kann man leicht folgendes Lemma beweisen:

LEMMA. *Ist G eine Gruppe, sind G_i und G_{i+1} Untergruppen, sodass G_{i+1} normal in G_i und G_i/G_{i+1} eine endliche abelsche Gruppe ist, wobei die Gruppenordnung $|G_i/G_{i+1}|$ durch eine Primzahl p teilbar ist. Dann gibt es eine Untergruppe U in G mit $G_{i+1} \subseteq U \subseteq G_i$, sodass G_{i+1} normal in U und U normal in G_i ist, sodass $U/G_{i+1} \simeq \mathbb{Z}_p$ ist und G_i/U abelsch mit Ordnung $\frac{[G_i:G_{i+1}]}{p}$.*

Mit diesem Lemma erhält man dann sofort folgenden Satz:

SATZ. *Ist G eine endliche auflösbare Gruppe, so gibt es eine Normalreihe*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{e\},$$

deren Faktoren G_i/G_{i+1} alle von Primzahlordnung sind.

Beispiel: Für S_4 haben wir bereits die Normalreihe

$$S_4 \supseteq A_4 \supseteq V \supseteq \langle(12)(34)\rangle \supseteq \{(1)\}$$

gesehen, deren Faktoren $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$ sind.

7. Für $n \geq 5$ ist die alternierende Gruppe A_n einfach

Erinnerung:

- In der symmetrischen Gruppe S_n lässt sich jedes Element als (eventuell leeres) Produkt elementfremder Zykel schreiben.
- Für $k \geq 2$ lässt sich jeder k-Zykel als Produkt von Transpositionen schreiben:

$$(i_1 i_2 i_3 \dots i_{k-1} i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-2} i_{k-1})(i_{k-1} i_k).$$

Beispiele:

$$(12) = (12), \quad (123) = (12)(23), \quad (1234) = (12)(23)(34), \quad (12345) = (12)(23)(34)(45), \quad \dots$$

LEMMA (A). *Sei $n \geq 3$. Wir betrachten die alternierende Gruppe A_n.*

(1) *Sind i, j, k, l vier verschiedene Zahlen aus $\{1, \dots, n\}$, so gilt*

$$(ij)(kl) = (ijk)(jkl) \quad \textit{und} \quad (ij)(ik) = (ikj) \quad \textit{und} \quad (ij)(ij) = (1).$$

(2) *Jedes Element von A_n lässt sich als (eventuell leeres) Produkt von 3-Zykeln schreiben.*

Beweis:

(1) Dies überprüft man sofort.

(2) Sei $\sigma \in A_n$ ein beliebiges Element. Nach den Vorbemerkungen können wir σ als Produkt von Transpositionen τ_i schreiben:

$$\sigma = \tau_1 \tau_2 \dots \tau_{n-1} \tau_n.$$

Da σ gerade, τ aber ungerade ist, muss n gerade sein, wir können also schreiben $n = 2m$ und erhalten

$$\sigma = (\tau_1 \tau_2)(\tau_3 \tau_4) \dots (\tau_{2m-1} \tau_{2m}).$$

Jedes Paar $\tau_{2i-1}\tau_{2i}$ schreiben wir mit den Regeln aus (1) aus Produkt von 3-Zykeln. Dadurch wird σ zu einem Produkt von 3-Zykeln, was wir zeigen wollten. ■

LEMMA (B). *In A_n wird die Konjugiertheit von 3-Zykeln betrachtet.*

(1) *A_3 zerfällt in 3 Konjugationsklassen:*

$$\{(1)\}, \quad \{(123)\}, \quad \{(132)\}.$$

(2) *In A_4 zerfallen die 3-Zykel in 2 Konjugationsklassen:*

$$\{(123), (134), (142), (243)\} \quad \textit{und} \quad \{(132), (143), (124), (234)\}.$$

(3) *Im Fall $n \geq 5$ sind alle 3-Zykel konjugiert.*

Beweis:

(1) Dies ist klar, da A_3 abelsch ist.

(2) Dies rechnet man einfach nach.

(3) Seien i, j, k drei verschiedene Zahlen aus $\{1, \dots, n\}$ und l, m zwei verschiedene Zahlen aus $\{1, \dots, n\} \setminus \{i, j, k\}$. Wir wählen $\sigma_1 \in S_n$ mit

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ i & j & k & l & m & \dots \end{pmatrix}.$$

Mit der Transposition (lm) gilt

$$\sigma_2 = (lm) \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ i & j & k & m & l & \dots \end{pmatrix}.$$

Nun ist $\operatorname{sgn}(\sigma_2) = -\operatorname{sgn}(\sigma_1)$. Wählen wir

$$\sigma = \begin{cases} \sigma_1, & \text{falls } \operatorname{sgn}(\sigma_1) = 1, \\ \sigma_2, & \text{falls } \operatorname{sgn}(\sigma_1) = -1, \end{cases}$$

so gilt

$$\sigma \in A_n \quad \text{und} \quad \sigma(123)\sigma^{-1} = (ijk).$$

Also liegt (ijk) in der Konjugationsklasse von (123). Daher sind alle 3-Zykel konjugiert, wie behauptet. ■

LEMMA (C). *Sei $n \geq 5$ und N ein Normalteiler alternierenden Gruppe A_n. Enthält N ein Element $\sigma \neq (1)$, so auch einen 3-Zykel.*

Beweis:

- Im Folgenden schreiben wir Permutation meist konkret, beispielsweise $\sigma = (123)(456)\sigma_3 \dots \sigma_r$. Man kann dies auch in als $\sigma = (i_1 i_2 i_3)(i_4 i_5 i_6)\sigma_3 \dots \sigma_r$ lesen, was aber das Schreiben und Lesen umständlicher macht.
- Beim Beweis wird von der Zykelzerlegung von Permutationen Gebrauch gemacht, auch von der Tatsache, dass elementfremde Zykel vertauschbar sind.
- Beim Beweis werden verschiedene Fälle betrachtet:
  - **Fall 1: σ enthält einen Zykel der Länge $m \geq 4$:** Wir schreiben die Zykelzerlegung o.E. in der Form
  $$\sigma = (1234 \dots m)\sigma_2 \dots \sigma_r.$$
  - **Fall 2: σ enthält zwei Zykel der Länge 3:** Wir schreiben die Zykelzerlegung o.E. in der Form
  $$\sigma = (123)(456)\sigma_3 \dots \sigma_r.$$
  - **Fall 3: σ enthält einen Zykel der Länge 3 und sonst höchstens Zykel der Länge 2:** Wir schreiben die Zykelzerlegung o.E. in der Form
  $$\sigma = (123)\sigma_2 \dots \sigma_r \quad \text{mit Transpositionen } \sigma_2, \dots, \sigma_r.$$
  - **Fall 4: σ enthält nur Transpositionen, hat aber Fixpunkte:** Wir können dann o.E. schreiben
  $$\sigma = (12)(34)(5)\sigma_3 \dots \sigma_r \text{ mit Transpositionen } \sigma_3, \dots, \sigma_r.$$
  - **Fall 5: σ enthält nur Transpositionen, habe aber keine Fixpunkte:** Wir können dann schreiben
  $$\sigma = (12)(34)(56)\sigma_4 \dots \sigma_r \text{ mit Transpositionen } \sigma_4, \dots, \sigma_r.$$
- **Fall 1: σ enthält einen Zykel der Länge $m \geq 4$:** Wir schreiben o.E.
$$\sigma = (1234 \dots m)\sigma_2 \dots \sigma_r \in N.$$
Dann ist
$$(123)\sigma(123)^{-1} = (2314 \dots m)\sigma_2 \dots \sigma_r \in N$$
und
$$\begin{aligned}(123)\sigma(123)^{-1} \cdot \sigma^{-1} &= (2314 \dots m)\sigma_2 \dots \sigma_r \cdot \sigma_r^{-1} \dots \sigma_2^{-1}(m \dots 4321) = \\ &= (2314 \dots m)(m \dots 4321) = (124) \in N.\end{aligned}$$
Also enthält N einen 3-Zykel.
- **Fall 2: σ enthält zwei 3-Zykel:** Wir schreiben o.E.
$$\sigma = (123)(456)\sigma_3 \dots \sigma_r \in N.$$
Dann ist
$$(124)\sigma(124)^{-1} = (243)(156)\sigma_3 \dots \sigma_r \in N$$
und
$$\begin{aligned}(124)\sigma(124)^{-1} \cdot \sigma^{-1} &= (243)(156)\sigma_3 \dots \sigma_r \cdot \sigma_r^{-1} \dots \sigma_3^{-1}(654)(321) = \\ &= (243)(156) \cdot (654)(321) = (12534) \in N.\end{aligned}$$
Damit gilt auch
$$(125)(12534)(125)^{-1} = (25134) \in N$$

und

$$(25134) \cdot (12534)^{-1} = (25134) \cdot (43521) = (123) \in N.$$

Der 3-Zykel (123) liegt also in N.

- **Fall 3: σ enthält einen 3-Zykel und sonst höchstens 2-Zykel:** Wir schreiben o.E.

$$\sigma = (123)\sigma_2 \dots \sigma_r \text{ mit Transpositionen } \sigma_2 \dots \sigma_r \in N.$$

Da Transpositionen Ordnung 2 haben, folgt

$$\sigma^2 = (132) \in N.$$

Damit liegt der 3-Zykel (132) in N.

- **Fall 4: σ enthält nur 2-Zykel, σ hat Fixpunkte:** Wir können annehmen, dass σ die Transposition (12) enthält. Da σ eine gerade Permutation ist, muss es mindestens eine weitere Transposition geben. Wir können o.E. schreiben

$$\sigma = (12)(34)(5)\sigma_3 \dots \sigma_r \in N.$$

Dann ist

$$(125)\sigma(125)^{-1} = (25)(34)(1)\sigma_3 \dots \sigma_r \in N$$

und

$$\begin{aligned}(125)\sigma(125)^{-1} \cdot \sigma^{-1} &= (25)(34)(1)\sigma_3 \dots \sigma_r \cdot \sigma_r^{-1} \dots \sigma_3^{-1}(5)(43)(21) = \\ &= (25)(34)(34)(12) = (152) \in N.\end{aligned}$$

Der 3-Zykel (152) liegt also in N.

- **Fall 5: σ enthält nur 2-Zykel und keine Fixpunkte:** Wegen $n \geq 5$ können wir o.E. schreiben

$$\sigma = (12)(34)(56)\sigma_4 \dots \sigma_r \text{ mit Transpositionen } \sigma_4, \dots, \sigma_r \in N.$$

Dann ist

$$(135)\sigma(135)^{-1} = (32)(54)(16)\sigma_4 \dots \sigma_r \in N$$

und

$$\begin{aligned}(135)\sigma(135)^{-1} \cdot \sigma^{-1} &= (23)(45)(16)\sigma_4 \dots \sigma_r \cdot \sigma_r^{-1} \dots \sigma_4^{-1}(56)(34)(12) = \\ &= (23)(45)(16) \cdot (56)(34)(12) = (135)(264) \in N.\end{aligned}$$

Nun ist man im Fall 2 und kann auf die dort angegebene Weise einen 3-Zykel in N finden.

- In jedem der fünf Fälle haben wir gezeigt, wie man aus einem Element $\sigma \in N \setminus \{(1)\}$ einen 3-Zykel in N finden kann. Damit folgt die Behauptung. ■

SATZ. *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis: Sei $N \subseteq A_n$ ein Normalteiler $\neq \{(1)\}$. Wähle ein Element $\sigma \in N \setminus \{(1)\}$. Mit Lemma (C) findet man einen 3-Zykel $(ijk) \in N$. Nach Lemma (B) sind alle 3-Zykel konjugiert. Da N als Normalteiler unter Konjugation abgeschlossen ist, enthält N alle 3-Zykel. Da sich nach Lemma (A) jedes Element von A_n als Produkt von 3-Zykel schreiben lässt, folgt sofort $N = A_n$. Die alternierende Gruppe A_n hat also nur die trivialen Normalteiler $\{(1)\}$ und N, und ist daher einfach. ■

SATZ. *Für $n \geq 5$ sind die Normalteiler von S_n*

$$\{(1)\}, \quad A_n, \quad S_n.$$

Beweis: Sei $N \subseteq S_n$ ein Normalteiler. Da A_n ein Normalteiler von S_n ist, ist auch $N \cap A_n$ ein Normalteiler. Da dann $N \cap A_n$ auch ein Normalteiler in A_n ist, gibt es nach dem vorangegangenen Satz nur zwei Möglichkeiten:

$$N \cap A_n = \{(1)\} \quad \text{oder} \quad N \cap A_n = A_n.$$

- **Fall $N \cap A_n = \{(1)\}$:** Angenommen, es wäre $N \neq \{(1)\}$. Dann gäbe es ein $\sigma \in N \setminus A_n$, insbesondere also $\operatorname{sgn}(\sigma) = -1$.

– *Behauptung:* $N = \{(1), \sigma\}$.
Beweis: Sei $\sigma' \in N \setminus \{(1)\}$. Dann ist $\sigma' \notin A_n$, also $\operatorname{sgn}(\sigma') = -1$. Aus
$$\operatorname{sgn}(\sigma'\sigma^{-1}) = 1$$
folgt $\sigma'\sigma^{-1} \in N \cap A_n = \{(1)\}$, also $\sigma' = \sigma$, was die Behauptung beweist.
– *Behauptung:* Für alle $\tau \in S_n$ gilt $\tau\sigma\tau^{-1} = \sigma$.
Beweis: Da N Normalteiler sein soll, gilt $\tau\sigma\tau^{-1} \in N$. Aus $\operatorname{sgn}(\tau\sigma\tau^{-1}) = \operatorname{sgn}(\sigma) = -1$ folgt dann $\tau\sigma\tau^{-1} = \sigma$.
– Wegen $\sigma \neq (1)$ gibt es i, j mit $\sigma(i) = j$ und $i \neq j$. Wähle ein $k \in \{1, \ldots, n\} \setminus \{i, j\}$. Dann gilt mit der Transposition $\tau = (jk)$
$$\tau\sigma(i) = \tau(j) = k \quad \text{und} \quad \sigma\tau(i) = \sigma(i) = j,$$
also $\tau\sigma \neq \sigma\tau$, und damit $\tau\sigma\tau^{-1} \neq \sigma$, im Widerspruch zur vorangegangenen Behauptung. Die Annahme $N \neq \{(1)\}$ ist also falsch.

Es gilt also in diesem Fall
$$N = \{(1)\}.$$

- **Fall** $N \cap A_n = A_n$**:** Dann ist $A_n \subseteq N$. Aus
$$2 = [S_n : A_n] = [S_n : N]\dot{[}N : A_n] \quad \text{folgt} \quad [S_n : N] = 1 \text{ oder } [N : A_n] = 1,$$
also
$$N = S_n \quad \text{oder} \quad N = A_n.$$

Damit ist alles bewiesen. ■

Bemerkung: Die Normalteiler von S_3 sind
$$\{(1)\}, \quad A_3, \quad S_3.$$
Die Normalteiler von S_4 sind
$$\{(1)\}, \quad V_4, \quad A_4, \quad S_4$$
mit
$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}.$$