Leitfaden: Algebra I

Vorbemerkung: Ist M eine Menge, so wird ihre Mächtigkeit (= Kardinalität) mit $|M|$ bezeichnet. Bei einer Gruppe G wird die Mächtigkeit der Grundmenge die *Ordnung* der Gruppe genannt.

I. Gruppen

0. Definitionen und Beispiele.

Gruppen. Eine *Gruppe* $G = (G, \mu)$ ist eine Menge (die "Grundmenge") mit einer Abbildung μ: $G \times G \to G$ (die "Gruppen-Operation" oder auch "Multiplikation"); verlangt wird, daß folgende Bedingungen erfüllt sind: (dabei schreibt man meist $g_1 g_2$ oder $g_1 \cdot g_2$ statt $\mu(g_1, g_2)$):

(G1) (Assoziativität): Für alle Elemente $g_1, g_2, g_3 \in G$ gilt $(g_1 g_2) g_3 = g_1(g_2 g_3)$.

(G2) (Existenz eines Einselements): Es gibt ein Element $e \in G$ mit $eg = g = ge$ für alle $g \in G$.

(G3) (Lösbarkeit von Gleichungen): Sind g_1, g_2 Elemente von G, so gibt es h, h' in G mit $g_1 h = g_2$, und $h' g_1 = g_2$.

Ist G eine Gruppe, und gilt $g_1 g_2 = g_2 g_1$ für alle $g_1, g_2 \in G$, so heißt G *kommutative* oder auch *abelsche* Gruppe.

Bemerkungen:

(1) Wegen (G1) kann man bei Produktbildungen $g_1 g_2 g_3$ auf das Klammersetzen verzichten (und damit auch bei längeren Produkten $g_1 g_2 \cdots g_n$).

(2) Für das in (G2) gegebene Element e gilt $e \cdot e = e$ (es ist "idempotent"), wegen (G3) ist e das einzige Element mit dieser Eigenschaft. Das Element e ist also eindeutig bestimmt, man schreibt meist 1 oder 1_G statt e und nennt es das *Einselement* der Gruppe.

(3) Insbesondere kann man in (G3) für g_2 das Einselement wählen: Wir sehen: zu $g \in G$ gibt es h, h' mit $gh = 1 = h'g$. Wegen $h = 1 \cdot h = h'gh = h' \cdot 1 = h'$ $(*)$ sieht man, daß $h = h'$ gilt. Man nennt h das zu g *inverse* Element und schreibt $h = g^{-1}$. (Die Rechnung $(*)$ zeigt, daß für jedes Element g das zu g inverse Element eindeutig bestimmt ist!)

(4) Die zu g_1, g_2 in (G3) gegebenen Elemente h, h' lassen sich mit Hilfe von g_1^{-1} folgendermaßen berechnen: es ist $h = g_1^{-1} g_2$, und $h' = g_2 g_1^{-1}$, insbesondere sind die Elemente h, h' eindeutig bestimmt.

(5) Statt (G, μ) schreibt man meist einfach G. Zur Bezeichnung der Gruppen-Operation μ werden manchmal statt des Multiplikationspunktes Symbole wie $\circ, *$ oder auch $+$ verwandt. Wenn es zur Klarstellung sinnvoll erscheint, schreibt man statt (G, μ) oder G auch $(G, \circ)$ usw. Insbesondere wird in abelschen Gruppen oft $+$ statt $\cdot$ geschrieben, und dann wird das Einselement mit 0 bezeichnet!

Homomorphismen. Sind $G = (G, \cdot)$ und $H = (H, \circ)$ Gruppen, so nennt man eine Abbildung

$$\phi\colon G \to H$$

einen *Gruppen-Homomorphismus*, oder einfach einen *Homomorphismus*, falls

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

für alle $g_1, g_2 \in G$ gilt. Für jeden Gruppen-Homomorphismus $\phi\colon G \to H$ gilt $\phi(1_G) = 1_H$ (denn $\phi(1_G)$ ist ein "idempotentes" Element von H und jede Gruppe besitzt nur ein derartiges Element).

Sei $\phi\colon G \to H$ ein Gruppen-Homomorphismus. Ist ϕ bijektiv (also injektiv und surjektiv), so ist die Abbildung ϕ^{-1} definiert. Sie ist selbst wieder ein Gruppen-Homomorphismus, denn

$$\phi^{-1}(ab) = \phi^{-1}\big(\phi\phi^{-1}(a)\phi\phi^{-1}(b)\big) = \phi^{-1}\phi\big(\phi^{-1}(a)\phi^{-1}(b)\big) = \phi^{-1}(a)\phi^{-1}(b).$$

Bijektive Homomorphismen nennt man *Isomorphismen.* Gibt es einen Isomorphismus $G \to H$, so nennt man die Gruppen G und H *isomorph.*

Untergruppen. Sei U eine Teilmenge der Gruppe $G = (G, \cdot)$. Man nennt U eine *Untergruppe*, falls U zusammen mit $\cdot$ selbst eine Gruppe ist. Genau dann ist U eine Untergruppe, wenn gilt

(U1) (Abgeschlossenheit unter der Multiplikation) Für $u_1, u_2 \in U$ ist auch $u_1 \cdot u_2 \in U$.
(U2) (Eins) Es ist $1_G \in U$.
(U3) (Inverses) Ist $u \in U$, so ist auch u^{-1} in U.

Bemerkung: Ist G eine endliche Gruppe, so folgt die Bedingung (U3) aus der Bedingung (U1), denn ist $u \in G$, so gibt es eine natürliche Zahl $n \geq 1$ mit $u^n = 1$, also gilt $u^{n-1} = u^{-1}$ (wir sehen also, daß sich das zu u inverse Element u^{-1} als Potenz von u mit nicht-negativem Exponenten schreiben läßt).

Sind U_1, U_2 Untergruppen der Gruppe G, so ist auch $U_1 \cap U_2$ (also der mengentheoretische Durchschnitt) wieder eine Untergruppe von G; allgemeiner gilt: Ist U_i $(i \in I)$ eine Menge von Untergruppen von G, so ist $\bigcap_{i\in I} U_i$ eine Untergruppe von G. Ist X eine Teilmenge einer Gruppe G, so kann man den Durchschnitt aller Untergruppen U von G bilden, für die $X \subseteq U$ gilt; dies ist die kleinste Untergruppe von G, die X enthält, man nennt sie *die von X erzeugte* Untergruppe.

Warnung: Sind U_1, U_2 Untergruppen einer Gruppe G, so ist die mengentheoretische Vereinigung $U_1 \cup U_2$ im allgemeinen **keine** Untergruppe! Diese Menge $U_1 \cup U_2$ ist im allgemeinen nicht unter der Produkt-Bildung abgeschlossen. Natürlich gibt es (wie für jede Teilmenge) eine kleinste Untergruppe, die $U_1 \cup U_2$ enthält, die von $U_1 \cup U_2$ erzeugte Untergruppe. Zweite Warnung: Sind U_1, U_2 Untergruppen, so bildet man manchmal $U_1U_2 = \{u_1u_2 \mid u_1 \in U_1, u_2 \in U_2\}$; auch diese Untermenge wird im allgemeinen **keine** Untergruppe sein — warum sollte auch jedes Produkt u_2u_1 mit $u_2 \in U_2, u_1 \in U_1$ zu U_1U_2 gehören? Wir werden im Abschnitt 1 den Begriff des "Normalteilers" kennenlernen: Ist mindestens eine der beiden Untergruppen U_1, U_2 ein "Normalteiler", so ist U_1U_2 eine Untergruppe von G.

Sei $\phi\colon G \to H$ ein Gruppen-Homomorphismus. Das Bild $\operatorname{Im}\phi$ von ϕ (also die Menge der Elemente $\phi(g)$ mit $g \in G$) ist eine Untergruppe von G. (Umgekehrt gilt natürlich auch: Ist U eine Untergruppe von G, so ist die Inklusionsabbildung $\iota\colon U \to G$ mit $\iota(u) = u$ für $u \in U$ ein Gruppen-Homomorphismus, und sein Bild ist gerade die Untergruppe U.) Die Menge der Elemente $g \in G$ mit $\phi(g) = 1$ nennt man den *Kern* von ϕ und man schreibt $\operatorname{Ker}\phi$ für diese Menge. Der Kern von ϕ ist eine Untergruppe von G (sogar ein "Normalteiler", wie wir im Abschnitt 2 sehen werden).

Beispiele:

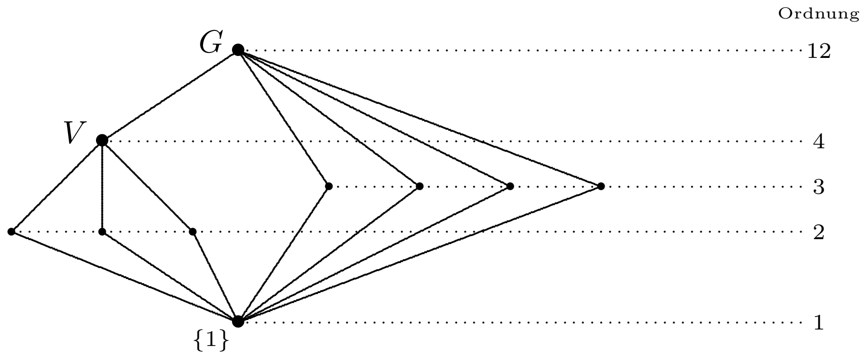
(1) Die symmetrischen und die alternierenden Gruppen. Sei M eine Menge. Eine *Permutation* von M ist eine bijektive Abbildung $M \to M$. Die Menge der Permutationen von M bildet bezüglich der Hintereinanderschaltung von Abbildungen eine Gruppe, die *volle Permutationsgruppe* S_M von M, man nennt sie auch die *symmetrische* Gruppe S_M.

Insbesondere setzt man $S_n = S_{\{1,2,\ldots,n\}}$, dies ist also die Menge der Permutationen der Menge $\{1,2,\ldots,n\}$. Ist M eine beliebige Menge mit genau n Elementen, so ist die Gruppe S_M zu S_n isomorph.

Bekannt sollte sein: (1) Die Gruppe S_n hat genau $n!$ Elemente. (2) Jedes Element von S_n läßt sich als Produkt von Transpositionen schreiben; dabei heißt eine Permutation $\tau \in S_n$ eine *Transposition*, wenn es Zahlen i, j mit $1 \le i < j \le n$ gibt mit $\tau(i) = j, \tau(j) = i$ und $\tau(x) = x$ für alle übrigen Elemente x in $\{1,2,\ldots,n\}$. (3) Ist $\sigma \in S_n$ ein Produkt von m Transpositionen, wobei m gerade ist, so ist in jeder Darstellung von σ als Produkt von Transpositionen die Anzahl der Faktoren geradzahlig. Man nennt solche Permutationen *gerade*. Die Menge der geraden Permutationen von $\{1,2,\ldots,n\}$ ist eine Untergruppe von S_n, man nennt diese Untergruppe die *alternierende Gruppe A_n vom Grad n.*

Wir werden uns später genauer mit den Gruppen S_n und A_n beschäftigen; wir werden für die Elemente der S_n eine recht praktische Schreibweise, die sogenannte "Zykel-Notation" einführen, siehe Abschnitt 1.

Hier ist der Untergruppen-Verband der Gruppe A_4



Dabei ist V die Untergruppe, die neben dem Einselement die drei Elemente (12)(34), (13)(24), (14)(23) enthält (wir verwenden hier schon die Zykel-Schreibweise, die im Abschnitt 1 vorgestellt wird). Man nennt V die *Klein'sche Vierergruppe.* Zwischen den Untergruppen $\{1\}$ und V liegen die drei Untergruppen der Ordnung 2; sie enthalten neben dem Einselement jeweils eines der Elemente $(12)(34), (13)(24), (14)(23)$. Die vier Untergruppen rechts haben Ordnung 3; sie enthalten jeweils zwei Elemente g, g^2 der Ordnung 3, dabei können wir für g die vier Elemente (123), (124), (134), (234) nehmen. Die Untergruppen $\{1\}, V, G$ sind durch fette Punkte hervorgehoben, es sind dies die "Normalteiler" der Gruppe A_4.

Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe (nämlich $G \to S_G$, mit $g \mapsto g\cdot$, dabei ist $g\cdot$ die Linksmultiplikation mit g, dies ist eine bijektive Abbildung $G \to G$, also ein Element in S_G.) Man nennt dies den **Satz von Cayley**.

(2) Die zyklischen Gruppen. Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

Die Menge $\mathbb{Z}$ der ganzen Zahlen ist bezüglich der Addition eine Gruppe $(\mathbb{Z}, +)$, man nennt sie die *unendliche zyklische Gruppe,* da sie vom Element 1 erzeugt wird. (Warnung: Das Element 1 ist nicht das Einselement der Gruppe! Da wir die Gruppe additiv schreiben, ist das Einselement bezüglich der Gruppen-Operation die Zahl 0). Neben 1 ist auch -1 ein erzeugendes Element der Gruppe.

Für $n \geq 2$ sei C_n die Drehgruppe des regelmäßigen n-Ecks (also die Menge der Drehungen in der Ebene mit festem Zentrum und mit Drehwinkel $\frac{2\pi t}{n}$, mit $0 \leq t < n$, mit der Hintereinanderschaltung der Drehungen als Gruppen-Operation). Die Gruppe hat die Ordnung n, es gibt ein Element g mit $C_n = \{g^t \mid 0 \leq t < n\}$, nämlich die Drehung $g = \rho_n$ mit dem Drehwinkel $\frac{2\pi}{n}$; die Gruppe C_n wird daher vom Element ρ_n erzeugt; für $n \geq 3$ gibt es weitere Elemente, die die Gruppe C_n erzeugen: jedes Element der Form ρ_n^t, wobei n, t teilerfremd sind, erzeugt die Gruppe C_n. Man nennt C_n die *zyklische Gruppe der Ordnung* n. (Das regelmäßige n-Eck sei dabei die Menge der komplexen Zahlen $e^{\frac{2\pi i t}{n}}$ mit $0 \leq t < n$; bezüglich der Multiplikation der komplexen Zahlen ist dies selbst eine zu C_n isomorphe Gruppe! Wir haben bisher nur den Fall $n \geq 2$ betrachten; es sei C_1 "die" Gruppe der Ordnung 1.)

Es gibt einen surjektiven Gruppen-Homomorphismus $(\mathbb{Z}, +) \to C_n$, mit $z \mapsto \rho_n^z$. Der Kern von diesem Homomorphismus ist die Menge $n\mathbb{Z}$ der durch n teilbaren Zahlen.

Im Abschnitt 2 werden wir Faktorgruppen einführen, der sogenannte "Erste Isomorphie-Satz" liefert dann:

$$(\mathbb{Z}, +)/n\mathbb{Z} \simeq C_n$$

Sei G eine beliebige Gruppe, die von einem Element g erzeugt wird. Hat g unendliche Ordnung, so ist der Gruppen-Homomorphismus $(\mathbb{Z},+) \to G$, mit $z \mapsto g^z$ ein Isomorphismus, also ist G zu $(\mathbb{Z},+)$ isomorph. Hat g endliche Ordnung, etwa m, so liefert der Gruppen-Homomorphismus $(\mathbb{Z},+) \to G$, mit $z \mapsto g^z$, einen Isomorphismus $(\mathbb{Z},+)/m\mathbb{Z} \simeq G$. Insgesamt sehen wir, daß es bis auf Isomorphie nur die folgenden zyklischen Gruppen gibt: $(\mathbb{Z},+)$ und die Gruppen C_n mit $n \in \mathbb{N}_0$.

Ist G eine Gruppe, und $g \in G$, so kann man die von g erzeugte Untergruppe $\langle g \rangle$ betrachten. Die *Ordnung* von g ist die Ordnung der von g erzeugten Untergruppe $\langle g \rangle$; es ist die kleinste natürliche Zahl $n \geq 1$ mit $g^n = 1$, falls es eine solche Zahl gibt, sonst sagt man, daß g unendliche Ordnung hat. Genau dann hat g die Ordnung $n < \infty$, wenn $\langle g \rangle \simeq C_n$ gilt. In einer endlichen Gruppe hat natürlich jedes Element endliche Ordnung; diese Ordnung ist ein Teiler der Gruppen-Ordnung, wie wir im Abschnitt 2 sehen werden.

(3) Diedergruppen. Für $n \geq 3$ sei D_n die volle Symmetriegruppe des regelmäßigen n-Ecks, sie enthält C_n als Untergruppe, zusätzlich gibt es noch n Spiegelungen. Die Gruppe D_n hat also die Ordnung $2n$.

(4) Die Symmetriegruppen und die Drehgruppen geometrischer Objekte. Zum Beispiel: des Tetraeders, des Würfels, des Ikosaeders.

(5) Das Produkt zweier Gruppen. Für zwei Mengen M_1, M_2 ist das (mengentheoretische) Produkt $M_1 \times M_2$ die Menge der Paare (m_1, m_2) mit $m_1 \in M_1, m_2 \in M_2$. Sind G, H Gruppen, so ist das Produkt $G \times H$ mit der komponentenweise Multiplikation wieder eine Gruppe (für $g, g' \in G$ und $h, h' \in H$ ist also $(g, h)(g', h') = (gg', hh')$ gesetzt). Die Teilmenge $\{(g, 1) \mid g \in G\}$ ist eine Untergruppe von $G \times H$, die zu G isomorph ist; die Teilmenge $\{(1, h) \mid h \in H\}$ ist eine Untergruppe von $G \times H$, die zu H isomorph ist.

1. Die Gruppen S_n und A_n.

Konjugation. Sei G eine Gruppe. Zwei Elemente $x, y \in G$ heißen *konjugiert*, falls es ein $g \in G$ mit $y = gxg^{-1}$ gibt. (Erinnerung: Sei k ein Körper. Zwei Matrizen $A, B \in M(n \times n, k)$ heißen ähnlich, wenn es eine invertierbare Matrix $P \in M(n \times n, k)$ gibt mit $B = PAP^{-1}$. In der Gruppe $\mathrm{GL}(n, k)$ sind also zwei Matrizen genau dann konjugiert, wenn sie ähnlich sind.)

Konjugiertheit ist eine Äquivalenzrelation. Die entsprechenden Äquivalenzklassen heißen *Konjugationsklassen.*

Normalteiler. Sei G eine Gruppe.Eine Untergruppe U von G heißt *Normalteiler,* wenn $gUg^{-1} = U$ für alle g gilt. (Dabei genügt es zu verlangen, daß $gUg^{-1} \subseteq U$ für alle $g \in G$ gilt. Dann dann gilt dies auch für g^{-1}, also $g^{-1}Ug \subseteq U$; multiplizieren wir von links mit g und von rechts mit g^{-1}, so erhalten wir die Inklusion $U \subseteq gUg^{-1}$.) Umformulierung: Eine Untergruppe U ist genau dann ein Normalteiler, wenn gilt: Ist $u \in U$, so sind alle zu u konjugierten Elemente in U.

Beispiele.
(1) Trivial: Ist G eine Gruppe, so sind natürlich G selbst und die Einsuntergruppe $\{1\}$ Normalteiler von G.
(2) Trivial: In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.
(3) Jede Diedergruppen D_n $(n \geq 3)$ besitzt genau n Untergruppen der Ordnung 2 und keine dieser Untergruppen ist ein Normalteiler.
(4) Die Untergruppe V von A_4 ist ein Normalteiler.
(5) Die Untergruppe C_n von D_n ist ein Normalteiler.

Einfachheit. Eine Gruppe G der Ordnung $|G| \geq 2$ heißt *einfach,* wenn es außer $\{1\}$ und G keine Normalteiler in G gibt. Ist G eine Gruppe von Primzahlordnung, so gibt es außer G und $\{1\}$ überhaupt keine weiteren Untergruppen: *Gruppen von Primzahlordnung sind einfach.* Wir werden sehen, daß jede endliche Gruppe $G \neq \{1\}$, deren Ordnung keine Primzahl ist, neben G und $\{1\}$ weitere Untergruppen besitzt (ist p eine Primzahl, die $|G|$ teilt, so hat G eine Untergruppe der Ordnung p). Wir werden Gruppen kennenlernen, die zwar viele Untergruppen, aber außer G und $\{1\}$ überhaupt keine weiteren Normalteiler besitzen, also einfach sind. Die Bezeichnung "einfache Gruppe" ist in mancher Hinsicht irreführend: die sogenannten "einfachen Gruppen" sind eher als sehr schwierig zu analysierende Gruppen anzusehen: da sie keine Normalteiler haben, gibt es wenig Möglichkeiten, Eigenschaften dieser Gruppen induktiv zu bestimmen. Die Bezeichnung "einfach" soll andeuten, daß man diese Gruppen als Bausteine zur Konstruktion von beliebigen Gruppen verwendet.

Satz 1 (Einfachheit der alternierenden Gruppen). *Für $n \geq 5$ ist A_n einfach.*

Bemerkung: Die Gruppe A_4 hat die Ordnung 12 und besitzt einen Normalteiler der Ordnung 4, ist also sicher nicht einfach. Die Gruppe A_3 hat die Ordnung 3, ist also einfach.

Zykel-Schreibweise. Da wir mit den Elementen der symmetrischen Gruppe S_n intensiv arbeiten müssen, werden wir eine recht praktische Notation einführen, die sogenannte Zykelschreibweise: Unter einem *t-Zykel* verstehen wir eine Permutation α der Menge M, zu der es t paarweise verschiedene Elemente $x_i \in M$ mit $1 \leq i \leq t$ gibt, so daß gilt: es ist einerseits $\alpha(x_i) = x_{i+1}$ für $1 \leq i < t$ und $\alpha(x_t) = x_1$, andererseits ist $\alpha(x) = x$ für $x \in M \setminus \{x_1, \ldots, x_t\}$; ist $t \geq 2$, so nennt man die Menge $\{x_1, \ldots, x_t\}$ den Träger von α und man schreibt[1] $\alpha = (x_1, x_2, \ldots, x_t)$ (oder auch $\alpha = (x_2, \ldots, x_t, x_1)$ und so weiter). (Erinnerung: Einen 2-Zykel nennt man eine Transposition.) *Jede Permutation σ kann als Produkt von Zyklen der Länge $t \geq 2$ mit paarweise disjunkten Trägern geschrieben werden;* man nennt dies die Zykel-Beschreibung von σ (im Fall der identischen Permutation σ handelt es sich um das leere Produkt, man schreibt dann als Zyklenschreibweise (1)).

Beispiel. Betrachte die folgende Permutation $\sigma \in S_8$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 5 & 3 & 7 & 1 & 4 & 6 \end{pmatrix}$$

Zykel-Beschreibungen von σ sind

$$\sigma = (186)(3574) = (4357)(861) = (3574)(861) = \ldots$$

Wie erhält man die Zykelschreibweise zu einer gegebenen Permutation σ? Man wählt ein beliebiges Element $x \in \{1, \ldots, n\}$, das unter σ bewegt wird, und bildet die sogenannte *Bahn* von x unter σ, also die Menge $\{x, \sigma(x), \sigma^2(x), \ldots\}$. Es seien die Elemente $x, \sigma(x), \ldots, \sigma^{t-1}(x)$ paarweise verschieden, aber $\sigma^t(x)$ gehöre zur Menge $\{x, \sigma(x), \ldots, \sigma^{t-1}(x)\}$. Dann muß notwendigerweise gelten $\sigma^t(x) = x$ (denn sonst wäre σ nicht injektiv). Die Menge $\{x, \sigma(x), \ldots, \sigma^{t-1}(x)\}$ ist also die Bahn von x unter σ. Die geklammerte Folge $(x, \sigma(x), \ldots, \sigma^{t-1}(x))$ ist einer der Zyklen, die wir suchen. Wieder wegen der Injektivität gilt: Sind x, y beliebige Elemente, so sind deren Bahnen entweder gleich oder disjunkt. Wir schreiben nun einfach die Zyklen zu allen Bahnen der Länge mindestens 2 nebeneinander. Wichtig: *Die Zykel-Beschreibung ist nicht eindeutig!* Und zwar gilt erstens: *Innerhalb einer Klammer kann man die Elemente zyklisch vertauschen.* Und zweitens: *Je zwei Zyklen in einer Zykel-Beschreibung von σ können vertauscht werden* (denn die jeweiligen Bahnen sind diskunkt). Noch eine Konvention: Zykel der Länge 1 kann man zusätzlich hinzufügen, tut dies aber üblicherweise nicht, außer eben beim Einselement, dort notiert man wenigstens einen 1-Zykel. Noch einmal: Bei diesen Zykel-Beschreibung von σ ist wichtig, daß die jeweiligen Zykel paarweise disjunkte Träger haben, daß also kein Element in zwei

[1] Warnung: Zykel lesen wir von links nach rechts, dagegen wird die Hintereinanderschaltung von Permutation (wie von allen Abbildungen) von rechts nach links gelesen. Wenn man sich dessen bewußt ist, sollte dies nicht zu Schwierigkeiten führen. Es ist also $(123) \circ (12) = (13)$, denn es handelt sich ja um die Anwendung zuerst der Abbildung $f = (12) = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ und dann der Abbildung $g = (123) = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ und $gf(1) = g(2) = 3$, usw.)

dieser Klammern vorkommt; kommt ein Element nicht vor, so ist dies wegen unserer Konvention ein "Fixpunkt" (also ein Element x mit $\sigma(x) = x$). (Will man eine eindeutig bestimmte Beschreibung $\sigma = (x_1, \ldots, x_t)(x_{t+1} \ldots) \ldots (\ldots)$ so wähle man $x_1 = 1$, dann für x_{t+1} die kleinste Zahl, die bisher nicht auftrat, und so weiter.) Die Längen λ_i der verschiedenen Zykel einer Permutation (einschließlich derer der Länge 1) faßt man als Folge $(\lambda_1, \ldots, \lambda_t)$ mit $\lambda_1 \geq \lambda_2 \geq \ldots$ zusammen, *wir erhalten auf diese Weise eine Partition* (die Partition der Zykellängen). In unserem Beispiel haben wir einen 4-Zykel, einen 3-Zykel und einen 1-Zykel, wir erhalten also die Partition $(4, 3, 1)$. (Beispiel: Die Transpositionen sind gerade die Permutationen mit zugehöriger Partition $(2, 1, \ldots, 1)$.)

Wichtig ist folgendes: Wir werden häufig Elemente der S_n konjugieren. Seien also $\sigma, \tau \in S_n$, und betrachte $\sigma' = \tau\sigma\tau^{-1}$. Ist $\sigma(x) = y$, so ist

$$\sigma'(\tau(x)) = (\tau\sigma\tau^{-1})\tau(x) = \tau(y).$$

Wir sehen also, daß wir aus der Zykelbeschreibung von σ sehr einfach diejenige von $\tau\sigma\tau^{-1}$ erhalten: wir ersetzen jedes x durch $\tau(x)$.

Beispiel: Sei $\sigma = (186)(3574)$, sei $\tau = (123)$. Dann ist

$$\tau\sigma\tau^{-1} = \big(\tau(1)\tau(8)\tau(6)\big)\big(\tau(3)\tau(5)\tau(7)\tau(4)\big) = (286)(1574).$$

Es folgt: *Genau dann sind zwei Elemente von S_n konjugiert, wenn die Zykellängen die gleiche Partition liefern.*

Zwei Hilfssätze, die auch sonst von Interesse sind, werden gebraucht:

(1) *Für $n \geq 3$ gilt: Jedes Element von A_n läßt sich als Produkt von 3-Zykeln schreiben.* Und daraus folgt: *Für $n \geq 3$ gilt: Die 3-Zykeln erzeugen A_n.* Denn wir wissen zusätzlich, daß jeder 3-Zykel gerade ist, also liegen alle 3-Zykeln in A_n.

Beweis: Seien i, j, k paarweise verschieden:

$$(i, j)(i, k) = (i, k, j),$$

Seien i, j, k, l paarweise verschieden:

$$(i, j)(k, l) = (i, j, k)(j, k, l).$$

Wir wissen, daß sich jede gerade Permutation σ als Produkt $\sigma = \tau_1 \circ \cdots \circ \tau_{2m}$ einer geraden Anzahl von Transpositionen τ_i schreiben läßt. Wie wir gesehen haben, können wir jeweils $\tau_{2i-1} \circ \tau_{2i}$ zusammenfassen und als Produkt von höchstens zwei 3-Zykeln schreiben.

(2) *Für $n \geq 5$ sind alle 3-Zykeln in A_n konjugiert.* (In A_4 gilt dagegen: Die 3-Zykeln $(1, 2, 3)$ und $(1, 3, 2)$ sind in A_4 **nicht** konjugiert.)

Es genügt zu zeigen, daß (i, j, k) zu $(1, 2, 3)$ konjugiert ist. Sei

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}$$

in S_n. Ist diese Permutation nicht in A_n, so gehört die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & m & l & \cdots \end{pmatrix}$$

zu A_n (wobei nur m, l vertauscht sind). Das Konjugieren mit jedem der beiden Elemente führt $(1, 2, 3)$ in (i, j, k) über.

Beweis des Satzes. Sei $N \neq \{1\}$ ein Normalteiler von A_n. Zu zeigen ist, daß N einen 3-Zykel enthält.

Sei $a \neq 1$ ein Element von N. Wir werden mehrfach verwenden, daß für jedes Element $c \in A_n$ das Element $aca^{-1}c^{-1}$ zu N gehört (mit a gehört auch a^{-1} zu N, also liegt $ca^{-1}c^{-1}$ in $cNc^{-1} = N$, und es ist $aca^{-1}c^{-1} = a \cdot ca^{-1}c^{-1}$).

Wir betrachten die Zykel-Zerlegung von a und unterscheiden mehrere Fälle; dabei konstruieren wir jeweils einen Dreier-Zykel c und bilden $g = aca^{-1}c^{-1}$. Da Dreier-Zykeln zur A_n gehören, wissen wir, daß g zu N gehört.

Fall 1. In der Zykel-Zerlegung von a gibt es einen Zykel der Länge r mit $r \geq 4$, etwa $(i, j, k, l, \ldots)$. Sei $c = (i, j, k)$. Es ist

$$g = (aca^{-1})c^{-1} = (j, k, l)(i, k, j) = (i, l, j)$$

ein Dreier-Zykel: wir haben also in N einen Dreier-Zykel gefunden.

Wir können nun voraussetzen, daß alle Zykel in der Zykel-Zerlegung von a Länge höchstens 3 haben.

Fall 2: In der Zykel-Zerlegung von a gibt es mindestens zwei Dreier-Zykel, $a = (i, j, k)(l, m, p) \cdots$. Sei $c = (i, j, l)$, es ist

$$g = (aca^{-1})c^{-1} = (j, k, m)(i, l, j) = (i, l, k, m, j),$$

und wir können Fall 1 anwenden.

Fall 3. In der Zykel-Zerlegung von a gibt es genau einen Dreier-Zykel. Dann ist a^2 ein Dreier-Zykel.

Fall 4: Es gibt keinen Dreier-Zykel, aber mindestens drei Zweier-Zykeln. Also $a = (i, j)(k, l)(m, r) \cdots$. Sei nun $c = (i, k, m)$. Wir bilden

$$g = (aca^{-1})c^{-1} = (j, l, r)(i, m, k),$$

der rechte Ausdruck ist die Zykel-Beschreibung von g, also haben wir ein Element gefunden, das wie im Fall 2 behandelt werden kann.

Fall 5: Es gibt keinen Dreier-Zykel, und höchstens zwei Zweier-Zykeln. Da a eine gerade Permutation ist und $a \neq 1$ gilt, gibt es genau zwei Zwei-Zykeln, also $a = (i, j)(k, l)$. Wegen $n \geq 5$ gibt es m, so daß i, j, k, l, m paarweise verschieden sind. Es ist $a(m) = m$. Sei nun $c = (i, k, m)$. Wir bilden

$$g = (aca^{-1})c^{-1} = (j, l, m)(i, m, k) = (i, l, m, k),$$

Auf dieses Element g können wir wieder Fall 1 anwenden.

Wir haben gesehen, daß N einen Dreier-Zykel g enthält. Die übrigen Dreier-Zykel der A_n sind nach (2) von der Form hgh^{-1} mit $h \in A_n$, denn alle Dreier-Zykeln sind in der Gruppe A_n konjugiert. Da g zu N gehört, gehört hgh^{-1} zu $hNh^{-1} = N$, denn N ist ein Normalteiler. Also sehen wir: alle Dreier-Zykeln gehören zu N. Nach (1) erzeugen diese aber die Gruppe A_n. Dies zeigt: $N = A_n$.