Algebra: Gruppen, Ringe, Körper

Skript zur Vorlesung im Sommersemester 2023

Prof. Meinolf Geck, Lehrstuhl für Algebra, Universität Stuttgart
https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf

Dieses Skript zur Vorlesung Algebra (V4Ü2, 14 Wochen) ist geeignet sowohl für die Bachelor- als auch die Lehramtsvariante; es handelt sich um eine etwas schlankere, leicht modifizierte und umorganisierte Version des Textes:

M. Geck, *Algebra: Gruppen, Ringe, Körper – Mit einer Einführung in die Darstellungstheorie endlicher Gruppen*. Edition Delkhofen, 2014. (Erhältlich z.B. bei Wittwer/Thalia.)

In diesem Skript ist insbesondere das erste Kapitel eine ausführlichere Einleitung, in der an Definitionen und Beispiele erinnert wird, die vermutlich schon zumindest ansatzweise in der Vorlesung Lineare Algebra I (oder Analysis I) eine Rolle spielten. Außerdem werden hier bereits einige grundlegende Begriffe und Konstruktionen eingeführt, bevor sie in den späteren drei Kapiteln zu Gruppen, Ringen und Körpern vertieft werden.

Die "Galois-Theorie" wird in obigem Text behandelt (und auch dort bereits in einer gegenüber vielen Lehrbüchern vereinfachten Form), kommt aber hier nicht mehr vor. Alternativ ist dieser Teil des Stoffes auch zum Beispiel gut geeignet für 4-5 Vorträge in einem Hauptseminar in einem der folgenden Semester. Auch ohne Galois-Theorie werden wir trotzdem das Ziel erreichen, den berühmten "Satz von Abel–Ruffini" von zeigen: Es gibt keine allgemeinen Lösungsformeln für Polynome vom Grad $\geqslant 5$.

Der obige Text enthält ansonsten einige Ergänzungskapitel, die weitere Algebra-Themen behandeln und auch zum Selbststudium geeignet sind (z.B. eine Einführung in die Charaktertheorie endlicher Gruppen). Umgekehrt findet sich bis auf wenige Ausnahmen alles, was in diesem Skript vorkommt, auch in obigem Text (manchmal mit alternativen Beweisen). Eine solche Ausnahme ist die Beschreibung des RSA-Verschlüsselungs-Verfahrens in §5; eine weitere der sogenannte Hauptsatz über symmetrische Polynome (siehe §**??**). Schließlich wird in einem Anhang die Existenz eines algebraischen Abschlusses eines Körpers diskutiert.

Im Durchschnitt werden pro Woche etwa 6 Seiten dieses Skriptes behandelt (am Anfang, bei den Wiederholungen aus der Linearen Algebra, etwas mehr). **Kommentare sehr willkommen!** (Insbesondere Druckfehler, sonstige Unklarheiten, Verbesserungsvorschläge etc.)

Stuttgart, März 2023

Literatur

[EAr] E. Artin, Galois Theory. Edited and with a supplemental chapter by Arthur N. Milgram. Reprint of the 1944 second edition. Dover Publications, Inc., Mineola, NY, 1998

[MAr] M. Artin, Algebra. Aus dem Englischen übersetzt von Annette A'Campo. Birkhäuser Verlag, 1993.

[Bo] N. Bourbaki, Éléments de Mathématiques. Algèbre. Chap. 1 à 3, Masson, Paris, 1970; Chap. 4 à 7, Masson, Paris, 1981.

[Eb] H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel und R. Remmert, Zahlen. Grundwissen Mathematik, vol. 1, Springer-Verlag, Berlin, 1983.

[Fi] G. Fischer, Lehrbuch der Algebra, Springer Spektrum, 2008.

[FS] G. Fischer und R. Sacher, Einführung in die Algebra (Teubner Studienbücher Mathematik). Vieweg + Teubner Verlag; 3. Auflage 1983.

[Fr] J. B. Fraleigh, A first course in abstract algebra. Pearson, 7th edition, 2002.

[GAP] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.11.0, 2020. Frei verfügbares Computer-Algebra-System, siehe http://www.gap-system.org.

[G14] M. Geck, Algebra: Gruppen, Ringe, Körper – Mit einer Einführung in die Darstellungstheorie endlicher Gruppen. Edition Delkhofen, 2014.

[Ha] P. R. Halmos, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.

[Ja] N. Jacobson, Basic Algebra I, II. 2nd Edition. H. Freeman and Company, New York, 1985 und 1989.

[KM] C. Karpfinger und K. Meyberg, Algebra: Gruppen - Ringe - Körper. Spektrum Akademischer Verlag, 2008.

[KS] H. Kurzweil und B. Stellmacher, The theory of finite groups. Springer–Verlag, 2004.

[LF] J. W. Lawrence and F. A. Zorzitto, Abstract Algebra, A Comprehensive Introduction. Cambridge University Press, 2021.

[Lo] F. Lorenz, Einführung in die Algebra (2 Bände). Spektrum Akademischer Verlag, 1996 und 1997.

[Pe] N. Perrin, Cours d'algèbre. Ellipses, Paris, 1996.

[Ro] M. I. Rosen, Niels Hendrik Abel and equations of the fifth degree, Amer. Math. Monthly **102** (1995), 495–505.

[So] R. Solomon, A brief history of the classification of the finite simple groups. Bull. Amer. Math. Soc. **38** (2001), 315–352; siehe auch http://en.wikipedia.org/wiki/List_of_finite_simple_groups.

[St] J. Stillwell, Elements of algebra. Geometry, numbers, equations. Undergraduate Texts in Mathematics, Springer–Verlag, New York, 1994.

Kapitel I: Grundlagen

In der Linearen Algebra haben Sie vermutlich bereits die Definitionen der grundlegenden algebraischen Strukturen gesehen: Gruppen, Ringe, Körper und natürlich Vektorräume. In diesem Einleitungskapitel beginnen wir mit einigen Erinnerungen, Beispielen und grundlegenden Konstruktionen. Alle Argumente werden hier etwas ausführlicher als später ausgeführt, weil sie tatsächlich wesentlich zum Verständnis des weiteren Stoffes sind.

1. *Algebraische Strukturen*

Eine nicht-leere Menge G zusammen mit einer Verknüpfung $\star\colon G \times G \to G$ heißt ***Gruppe***, wenn die Verknüpfung assoziativ ist (also $a \star (b \star c) = (a \star b) \star c$ für alle $a, b, c \in G$), es ein neutrales Element gibt (also ein $e \in G$ mit $a \star e = e \star a = a$ für alle $a \in G$) und jedes Element von G ein Inverses besitzt (es also zu jedem $a \in G$ ein $a' \in G$ gibt mit $a \star a' = a' \star a = e$). Wie bei Vektorräumen zeigt man dann leicht, dass das neutrale Element e eindeutig bestimmt ist, und dass das Inverse eines Elements ebenfalls eindeutig bestimmt ist. Beachte: Für das Inverse eines Produktes gilt die Regel $(a \star b)' = b' \star a'$ für alle $a, b \in G$. (Denn: Setze $c := b' \star a'$. Dann gilt $b \star c = b \star (b' \star a') = (b \star b') \star a' = e \star a' = a'$ und damit $(a \star b) \star c = a \star (b \star c) = a \star a' = e$; analog sieht man $c \star (a \star b) = e$.)

Beispiele von Gruppen:

• Sei $n \geqslant 1$. Die ***symmetrische Gruppe*** S_n ist die Menge aller bijektiven Abbildungen $\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}$ (auch Permutationen genannt), zusammen mit der Hintereinanderausführung "$\circ$" als Verknüpfung. Das neutrale Element ist die identische Abbildung $\mathrm{id} \in S_n$ (mit $\mathrm{id}(i) = i$ für $1 \leqslant i \leqslant n$) und das Inverse von $\sigma \in S_n$ die Umkehrabbildung σ^{-1}. Elemente von S_n schreiben wir in der Form $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \in S_n$.

Sei etwa $n = 3$ und $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right) \in S_3$, $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right) \in S_3$; dann ist $\sigma \circ \tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ (denn $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 2$, $(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(3) = 3$, $(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(2) = 1$).

• Etwas allgemeiner: Sei $X \neq \varnothing$ eine Menge und S_X die Menge aller bijektiven Abbildungen $\sigma\colon X \to X$. Dann ist S_X eine Gruppe mit der Hintereinanderausführung "$\circ$" von Abbildungen als Verknüpfung. Das neutrale Element ist die identische Abbildung id_X; das Inverse von $\sigma \in S_X$ ist wiederum die Umkehrabbildung von σ. Diese Gruppe heißt ***symmetrische Gruppe*** auf X. Dann gilt also $S_n = S_X$ mit $X = \{1, \dots, n\}$.

• Sei K ein Körper und $n \geqslant 1$. Mit $M_n(K)$ bezeichnen wir den Vektorraum aller $n \times n$-Matrizen mit Einträgen in K. Aus der Linearen Algebra ist bekannt: $A \in M_n(K)$ ist invertierbar genau dann, wenn $\det(A) \neq 0$ gilt; außerdem: Für $A, B \in M_n(K)$ gilt $\det(A \cdot B) =$

$\det(A)\det(B)$. Damit ist $GL_n(K) := \{A \in M_n(K) \mid \det(A) \neq 0\}$ eine Gruppe mit der üblichen Matrixmultiplikation als Verknüpfung; das neutrale Element ist die Einheitsmatrix I_n. Diese Gruppe heißt die ***allgemeine lineare Gruppe***.

Definition 1.1. Eine Gruppe G heißt ***abelsch*** (zu Ehren des Mathematikers H. N. Abel), wenn die Multiplikation kommutativ ist, also $a \star b = b \star a$ für alle $a, b \in G$. In diesem Fall wird die Verknüpfung auch oft als Addition $a + b$ geschrieben, das neutrale Element mit 0 bezeichnet und das Inverse von $a \in G$ mit $-a$.

Beispiele: Die Gruppe der ganzen Zahlen $\mathbb{Z}$, mit der üblichen Addition, ist abelsch. (Bezüglich der Multiplikation ist $\mathbb{Z}$ keine Gruppe, weil nicht jedes Element ein Inverses besitzt.) Die symmetrischen Gruppen S_1 und S_2 sind ebenfalls abelsch. Für $n = 3$ gilt:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \Rightarrow \quad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Also ist S_3 nicht abelsch; genauso sieht man, dass S_n für $n \geqslant 3$ niemals abelsch ist. Für $n = 1$ ist $GL_1(K) = \{(a) \mid 0 \neq a \in K\}$ abelsch; für $n \geqslant 2$ ist $GL_n(K)$ nicht abelsch. (Finden Sie selbst zwei invertierbare Matrizen, die nicht vertauschbar sind.)

Abelsche Gruppen sind bereits aus der Linearen Algebra vertraut: Ein Vektorraum V über einem Körper K ist *zunächst* eine abelsche Gruppe $(V, +)$, auf der zusätzlich eine "äußere" Verknüpfung $K \times V \to V$ (Multiplikation von Vektoren mit Skalaren aus einem Körper K) definiert ist, so dass die bekannten Bedingungen gelten.

Ein ***Ring*** R ist eine abelsche Gruppe $(R, +)$, auf der zusätzlich eine Multiplikation $\bullet\colon R \times R \to R$ definiert ist, die assoziativ ist und so dass die Distributivregeln gelten: $a \bullet (b + c) = a \bullet b + a \bullet c$ und $(a + b) \bullet c = a \bullet c + b \bullet c$ für alle $a, b, c \in R$.
Aus diesen Regeln folgt zum Beispiel sofort: $a \bullet 0 = 0 \bullet a = 0$ für alle $a \in R$.
Wir bezeichnen R als kommutativen Ring, wenn die Multiplikation kommutativ ist, also $a \bullet b = b \bullet a$ gilt für alle $a, b \in R$.

Standard-Beispiele: $R = \mathbb{Z}$ ist ein kommutativer Ring, mit der üblichen Addition und Multiplikation von ganzen Zahlen. Außerdem ist $R = M_n(K)$ ein Ring mit der üblichen Addition und Multiplikation von Matrizen. Dieser Ring ist kommutativ genau dann, wenn $n = 1$.

Definition 1.2. Sei R ein Ring, der ein neutrales Element 1_R bezüglich der Multiplikation besitzt (kurz: R ist ein Ring mit 1). Ein Element $a \in R$ heißt ***Einheit***, wenn a bezüglich der Multiplikation ein Inverses besitzt, es also ein $b \in R$ gibt mit $a \bullet b = b \bullet a = 1_R$. Dann heißt

$$R^\times := \{a \in R \mid a \text{ Einheit}\}$$

die ***Einheitengruppe*** von R. Zum Beispiel ist $1_R \in R^\times$. Man sieht sofort, dass $R^\times$ tatsächlich eine Gruppe bezüglich der Multiplikation in R ist; das neutrale Element ist 1_R.

Beachte: Der Extremfall $1_R = 0$ ist in der Definition nicht ausgeschlossen. Aber aus $1_R = 0$ folgt $a = a \bullet 1_R = a \bullet 0 = 0$ für alle $a \in R$; also $R = R^\times = \{0\}$.

Ein ***Körper*** K ist damit ein kommutativer Ring mit $1 \neq 0$, so dass $K^\times = K \setminus \{0\}$ gilt. Dann heißt $K^\times$ auch die multiplikative Gruppe von K. Standard-Beispiele sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$; für jede Primzahl p gibt es auch einen Körper $\mathbb{F}_p$ mit p Elementen (den Sie vielleicht schon in der Linearen Algebra gesehen haben; ansonsten siehe §4).

Beispiele zu Einheitengruppen: Für $R = \mathbb{Z}$ ist $\mathbb{Z}^\times = \{1, -1\}$. Für $R = M_n(K)$ (mit K Körper) ist $M_n(K)^\times = \{A \in M_n(K) \mid A \text{ invertierbar}\} = GL_n(K)$.

Eine Methode, um neue algebraische Strukturen zu erhalten, besteht darin, Unterstrukturen zu betrachten (analog zu Unterräumen von Vektorräumen).

Definition 1.3. (a) Sei $(G, \star)$ eine Gruppe und $U \subseteq G$ eine Teilmenge. Dann heißt U eine ***Untergruppe*** von G (in Zeichen: $U \leqslant G$), wenn gilt:

$$1_G \in U, \qquad a \star b \in U \qquad \text{und} \quad a' \in U \qquad \text{für alle } a, b \in U.$$

(Hier ist a' das Inverse von a.) Dann ist U zusammen mit der Einschränkung der Verknüpfung auf G auch selbst eine Gruppe. Zum Beispiel sind $\{1_G\}$ und G immer Untergruppen.

(b) Sei $(R, +, \bullet)$ ein Ring und $S \subseteq R$ eine Teilmenge. Dann heißt S ein ***Teilring*** von R, wenn S eine Untergruppe von R bezüglich der Addition $+$ ist und außerdem $a \bullet b \in S$ für alle $a, b \in S$ gilt. Wiederum ist S selbst zusammen mit den Einschränkungen der Verknüpfung auf R auch selbst ein Ring. Zum Beispiel sind $\{0\}$ und R immer Teilringe.

Bemerkung 1.4. Sei $\{U_i\}_{i \in I}$ eine Familie von Untergruppen von G (mit beliebiger Indexmenge I). Dann ist auch $\bigcap_{i \in I} U_i$ eine Untergruppe (wie Sie sofort nachprüfen), aber $\bigcup_{i \in I} U_i$ ist im Allgemeinen keine Untergruppe (siehe Übungen). Analoge Aussagen gelten für Durchschnitte von Teilringen.

Beispiel 1.5. Sei $G = GL_n(K)$ die allgemeine lineare Gruppe. Sei $B_n(K) \subseteq G$ die Teilmenge, die aus allen oberen Dreiecksmatrizen mit Einträgen ungleich Null auf der Diagonalen besteht. Dann ist $B_n(K)$ eine Untergruppe. Denn erstens gilt $I_n \in B_n(K)$. Sind außerdem $A, B \in B_n(K)$, so folgt leicht aus der Definition des Matrixprodukts, dass auch $A \cdot B$ eine obere Dreiecksmatrix ist; sind außerdem $a_1, \ldots, a_n$ die Diagonaleinträge von A und $b_1, \ldots, b_n$ die Diagonaleinträge von B, so sind $a_1 b_1, \ldots, a_n b_n$ die Diagonaleinträge von $A \cdot B$. Also sind auch diese alle ungleich Null und damit $A \cdot B \in B_n(K)$. Schließlich gilt $\det(A) = a_1 \cdots a_n \neq 0$, also ist A invertierbar. Dann muss man sich noch überzeugen, dass A^{-1} ebenfalls eine obere Dreiecksmatrix ist, mit Diagonaleinträgen $a_1^{-1}, \ldots, a_n^{-1}$. Also ist auch $A^{-1} \in B_n(K)$.

Beispiel 1.6. Die ***Gauß'schen Zahlen*** $\mathbb{Z}[i] := \{n + mi \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$ bilden einen Teilring des Körpers $\mathbb{C}$ (wobei wie üblich $i = \sqrt{-1} \in \mathbb{C}$). Denn sind $n + mi \in \mathbb{Z}[i]$ und $n' + m'i \in \mathbb{Z}[i]$, so gilt

$$(n + mi) + (n' + m'i) = (n + n') + (m + m')i \in \mathbb{Z}[i],$$
$$(n + mi) \cdot (n' + m'i) = (nn' - mm') + (nm' + n'm)i \in \mathbb{Z}[i].$$

Daran sieht man sofort, dass die Teilring-Bedingungen gelten. Da $\mathbb{C}$ ein Körper ist, ist $\mathbb{Z}[i]$ ein kommutativer Ring. Die Zahl 1 ist das neutrale Element bezüglich der Multiplikation.

Behauptung: $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Dazu: Es ist klar, dass ± 1 und $\pm i$ Einheiten sind. Sei umgekehrt $0 \neq n + mi \in \mathbb{Z}[i]^\times$. Dann gibt es also $n', m' \in \mathbb{Z}$ mit $1 = (n + mi)(n' + m'i)$. Anwenden von komplexer Konjugation ergibt $1 = (n - mi)(n' - m'i)$, also ist auch $n - mi \in \mathbb{Z}[i]^\times$ und damit $n^2+m^2 = (n+mi)(n-mi) \in \mathbb{Z}[i]^\times$. Also gibt es $n'', m'' \in \mathbb{Z}$ mit $1 = (n^2+m^2)(n''+m''i) = (n^2+m^2)n''+(n^2+m^2)m''i$; dann muss aber $1 = (n^2+m^2)n''$ gelten, also $n^2+m^2 = \pm 1$. Dies ist nur möglich für $n = 0$, $m = \pm 1$ oder für $n = \pm 1$, $m = 0$. — Wie man an diesem Beispiel erahnt, kann es für beliebige Ringe durchaus schwierig sein, die Einheiten zu bestimmen.

Bemerkung 1.7. Sei R ein Ring und $S \subseteq R$ ein Teilring. Besitzt R ein Eins-Element, so muss S nicht unbedingt ein Eins-Element besitzen. Und selbst wenn dies der Fall ist, so können R und S verschiedene Eins-Elemente besitzen. Beispiele:

• Sei $S := 2\mathbb{Z} = \{\text{alle geraden ganzen Zahlen}\} \subseteq R = \mathbb{Z}$. Dann ist S ein Teilring; dieser besitzt aber kein Eins-Element.

• Sei $S := \{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right) \mid a \in \mathbb{Q}\} \subseteq R = M_2(\mathbb{Q})$. Dann ist S ein Teilring mit Eins-Element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq I_2$.

Schließlich: Ist $0 \neq s \in S$ eine Einheit in R, so gibt es also ein Inverses $s^{-1} \in R$, aber es muss nicht unbedingt $s^{-1} \in S$ gelten. Beispiel: $S = \mathbb{Z} \subseteq R = \mathbb{Q}$, $2^{-1} = \frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z}$.

Ein weiteres allgemeines Konstruktionsprinzip sind direkte Produkte.

Definition 1.8. Seien $(G_1, \star_1)$ und $(G_2, \star_2)$ Gruppen. Wir betrachten das kartesische Produkt $G := G_1 \times G_2 = \{(a_1, a_2) \mid a_1 \in G_1, a_2 \in G_2\}$ und definieren eine Verknüpfung auf G durch $(a_1, a_2) \star (b_1, b_2) := (a_1 \star_1 b_1, a_2 \star_2 b_2)$ für alle $a_1, b_1 \in G_1$ und $a_2, b_2 \in G_2$. Dann sieht man leicht, dass $(G, \star)$ auch eine Gruppe ist, die als ***direktes Produkt*** bezeichnet wird. Das neutrale Element ist $e := (e_1, e_2) \in G$ wobei e_1 das neutrale Element in G_1 und $e_2 \in G_2$ das neutrale Element in G_2 ist. Das Inverse von $(a_1, a_2) \in G$ ist gegeben durch $(a_1, a_2)' = (a_1', a_2')$, wobei jeweils $a_i' \in G_i$ das Inverse zu a_i in G_i ist. Sind G_1 und G_2 abelsch, so ist auch G abelsch.

Analog definiert man auch das direkte Produkt von zwei Ringen $(R_1, +_1, \bullet_1)$ und $(R_2, +_2, \bullet_2)$. Man bildet das kartesische Produkt $R := R_1 \times R_2$ und definiert Verknüpfungen

$$(a_1, a_2) + (b_1, b_2) := (a_1 +_1 b_1, a_2 +_2 b_2) \quad \text{und} \quad (a_1, a_2) \bullet (b_1, b_2) := (a_1 \bullet_1 b_1, a_2 \bullet_2 b_2)$$

für alle $a_1, b_1 \in R_1$ und $a_2, b_2 \in R_2$. Dann sieht man leicht, dass $(R, +, \bullet)$ wieder ein Ring ist. Sind R_1 und R_2 kommutativ, so ist auch R kommutativ. Besitzen R_1 und R_2 Eins-Elemente 1_{R_1} und 1_{R_2}, so ist $1_R = (1_{R_1}, 1_{R_2})$ ein Eins-Element von R. In diesem Fall folgt dann auch sofort, dass $R^\times = R_1^\times \times R_2^\times$ gilt.

Schließlich erwähnen wir, dass direkte Produkte nicht nur mit zwei Faktoren, sondern auch mit endlich vielen Faktoren gebildet werden können.

2. *Faktorstrukturen*

Sei M eine nicht-leere Menge und $\sim$ eine Äquivalenzrelation auf M (also eine reflexive, symmetrische, transitive Relation). Für $m \in M$ bezeichne $[m] := \{m' \in M \mid m' \sim m\}$ die Äquivalenzklasse von m. Sei $M/\sim$ die Menge der Äquivalenzklassen. Ist M nicht nur eine Menge, sondern eine algebraische Struktur, und ist $\sim$ mit dieser Struktur verträglich, so besteht eine gute Chance, dass auch $M/\sim$ wieder eine (neue) algebraische Struktur ist. Dies ist ein sehr vielseitiges und schlagkräftiges Konstruktionsprinzip.

Als erstes und bekanntes Beispiel behandeln wir die rationalen Zahlen, also Brüche $\frac{n}{m} \in \mathbb{Q}$ mit $n, m \in \mathbb{Z}$ wobei $m \neq 0$. Ein Bruch wie $\frac{2}{3} \in \mathbb{Q}$ kann auf verschiedene Weise dargestellt werden, etwa $\frac{2}{3} = \frac{4}{6} = \frac{-10}{-15}$. Der formal korrekte Hintergrund dieser verschiedenen Darstellungsweisen ist letztlich eine Äquivalenzrelation.

Beispiel 2.1. (Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$). Sei $M := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, also die Menge aller Paare (a, b) mit $a, b \in \mathbb{Z}$ und $b \neq 0$. Wir definieren eine Relation $\sim$ auf M wie folgt: Für $(a, b) \in M$ und $(c, d) \in M$ sei $(a, b) \sim (c, d)$, wenn $ad = bc$. Diese Relation ist reflexiv, denn es gilt $(a, b) \sim (a, b)$ wegen $ab = ba$. Sie ist symmetrisch, denn aus $(a, b) \sim (c, d)$ folgt $ad = bc$ und damit auch $cb = da$, also $(c, d) \sim (a, b)$. Schließlich ist $\sim$ auch transitiv, denn seien $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$; dann gilt $ad = bc$, $cf = de$ und damit $daf = (ad)f = (bc)f = b(cf) = b(de) = dbe$. Nun ist $d \neq 0$, also kann man d auf beiden Seiten kürzen. Also gilt auch $af = be$ und $(a, b) \sim (e, f)$.

Damit ist $\sim$ eine Äquivalenzrelation. Die Äquivalenzklasse von $(a, b) \in M$ bezeichnen wir mit a/b; die Menge aller Äquivalenzklassen definieren wir als $\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$.

Wir wollen nun Verknüpfungen auf $\mathbb{Q}$ definieren. Für $(a, b) \in M$ und $(c, d) \in M$ setzen wir:

$$a/b + c/d := (ad + bc)/bd \qquad \text{und} \qquad a/b \cdot c/d := (ac)/(bd).$$

(Beachte: Wegen $b \neq 0$ und $d \neq 0$ ist auch $bd \neq 0$.) Damit diese Operationen überhaupt sinnvoll sind, muss zuerst gezeigt werden, dass sie ***wohl-definiert*** sind, d.h., nicht von der Wahl der Repräsentanten (a, b) und (c, d) abhängen. Konkret heißt das in diesem Fall: Seien $(a', b') \in M$ und $(c', d') \in M$ mit $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$; dann muss man zeigen, dass auch $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ und $(ac, bd) \sim (a'c', b'd')$ gilt, also bei der Berechnung der Addition oder Multiplikation jeweils das gleiche Ergebnis herauskommt. Diese einfache Rechnung sei als Übung überlassen. Man rechnet dann insgesamt nach, dass $\mathbb{Q}$ mit diesen Operationen ein kommutativer Ring mit 1 ist. Das neutrale Element bezüglich der Addition ist die Äquivalenzklasse $0/1 \in \mathbb{Q}$; das neutrale Element bezüglich der Multiplikation ist $1/1 = \{a/a \mid 0 \neq a \in \mathbb{Z}\}$.

Weiterhin erhält man: Ist $a/b \in \mathbb{Q}$ und $a/b \neq 0/1$, so folgt $a \neq 0$ und $b \neq 0$; also ist auch $b/a \in \mathbb{Q}$ und $a/b \cdot b/a = 1/1$. Folglich ist $\mathbb{Q}$ ein Körper, denn alle Elemente ungleich $0/1$ in $\mathbb{Q}$ sind Einheiten. Schließlich können wir $\mathbb{Z}$ als eine Teilmenge von $\mathbb{Q}$ auffassen, indem wir $n \in \mathbb{Z}$ mit dem Bruch $n/1 \in \mathbb{Q}$ identifizieren. Die Abbildung $n \mapsto n/1$ ist injektiv, denn $n/1 = m/1$ (für $n, m \in \mathbb{Z}$) impliziert $n = m$ nach Definition von $\sim$. Mit dieser Identifikation entsprechen dann auch die übliche Addition $n + m$ und Multiplikation nm in $\mathbb{Z}$ den Operationen $n/1 + m/1$ und $n/1 \cdot m/1$.

Man sieht, dass im Detail viele Regeln verifiziert werden müssen, aber dies meistens Routine-Aufgaben sind, nachdem einmal gezeigt ist, dass die Operationen "wohl-definiert" sind.

Beispiel 2.2. In einer Vorlesung (oder einem Lehrbuch) zur Analysis werden Sie vielleicht die Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$ mit Hilfe von Cauchy-Folgen gesehen haben. Auch dies ist ein Beispiel für obiges allgemeines Konstruktionsprinzip: Man erhält $\mathbb{R}$ als Menge der Äquivalenzklassen von Cauchy-Folgen $(a_n)_{n\in\mathbb{N}}$ (mit $a_n \in \mathbb{Q}$ für alle $n \in \mathbb{N}$), wobei $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ in Relation stehen, wenn $(a_n - b_n)_{n\in\mathbb{N}}$ eine Nullfolge ist. Genauso wie in obigem Beispiel muss man dann zahlreiche Regeln im Detail nachweisen, um zu sehen, dass die Menge der Äquivalenzklassen ein Körper ist (also $\mathbb{R}$), in dem jede Cauchy-Folge konvergiert. Schließlich fassen wir $\mathbb{Q}$ als Teilmenge von $\mathbb{R}$ auf, indem wir $x \in \mathbb{Q}$ mit der Äquivalenzklasse der Folge $(x, x, x, \ldots)$ identifizieren.

Für das folgende Beispiel wiederholen wir einige Grundtatsachen zu ganzen Zahlen. Zunächst sei an die Bezeichnungen $\mathbb{N} = \{1, 2, 3, \ldots\}$ und $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ erinnert. (In manchen Büchern ist $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.) Seien $m, n \in \mathbb{Z}$. Wie üblich schreiben wir $m \mid n$, wenn m ein Teiler von n ist, es also ein $k \in \mathbb{Z}$ mit $n = km$ gibt. Wir setzen außerdem die ***Division mit Rest*** als bekannt voraus. Sind also $m \in \mathbb{N}$ und $n \in \mathbb{Z}$ gegeben, so gibt es $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 \leqslant r < m$; hierbei sind q, r eindeutig bestimmt. Zum Beispiel für $m = 5$ und $n = 17$:

Es gilt $1\cdot 5,\ 2\cdot 5,\ 3\cdot 5 \leqslant 17$ aber $4\cdot 5 > 17$; dies ergibt $17 = 3\cdot 5+2$, also $q = 3$, $r = 2$; dann ist $-17 = (-3)\cdot 5 - 2 = (-3)\cdot 5 + (3-5) = (-4)\cdot 5 + 3$, also $q = -4$, $r = 3$.

Beispiel 2.3. (Die Ringe $\mathbb{Z}/m\mathbb{Z}$). Sei $m \in \mathbb{N}$ fest. Wir definieren eine Relation $\sim$ auf $\mathbb{Z}$ durch $a \sim b$, wenn $m \mid b-a$ (für $a, b \in \mathbb{Z}$). Man sieht leicht, dass dies eine Äquivalenzrelation ist. Die Äquivalenzklasse von $a \in \mathbb{Z}$ bezeichnen wir mit $\overline{a}$ und die Menge aller Äquivalenzklassen mit $\mathbb{Z}/m\mathbb{Z}$. Weitere Schreibweise: $a \equiv b \bmod m$ falls $m \mid b-a$.

Durch Division mit Rest erhalten wir $a = qm + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < m$. Also ist $a \equiv r \bmod m$ und damit $\overline{a} = \overline{r}$. Es folgt $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ und $|\mathbb{Z}/m\mathbb{Z}| = m$. Wir wollen nun eine Addition und eine Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ definieren. Für $a, b \in \mathbb{Z}$ setze

$$\overline{a} + \overline{b} := \overline{a+b} \qquad \text{und} \qquad \overline{a}\cdot\overline{b} := \overline{ab}.$$

Wie üblich müssen wir zuerst zeigen, dass dies ***wohl-definiert*** ist. Seien also $a, b, a', b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, d.h., $m \mid a'-a$ und $m \mid b'-b$. Dann ist auch $(a'+b')-(a+b) = (a'-a)+(b'-b)$ ein Vielfaches von m; und ebenso $a'b'-ab = a'b'-ab'+ab'-ab = (a'-a)b' + a(b'-b)$. Also gilt $\overline{a+b} = \overline{a'+b'}$ und $\overline{ab} = \overline{a'b'}$, wie gewünscht. Aufgrund der obigen Definition ist klar, dass $\overline{0}$ neutrales Element bezüglich "+" und $\overline{1}$ neutrales Element bezüglich "$\cdot$" ist. Jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ hat ein Inverses bezüglich "+", nämlich $\overline{-a}$. Die weiteren Ring-Axiome folgen sofort aus den entsprechenden Regeln in $\mathbb{Z}$, zum Beispiel:

$$\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{(b+c)} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac} = \overline{a}\cdot\overline{b} + \overline{a}\cdot\overline{c}.$$

Man rechnet insgesamt nach, dass $\mathbb{Z}/m\mathbb{Z}$ ein kommutativer Ring mit 1 ist.

Für $m = 1$ ist $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. Für $m = 2$ ist $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ mit $\overline{1}+\overline{1} = \overline{0}$. Für $m = 3, 4$ sind die Verknüpfungstabellen wie folgt gegeben:

$m = 3$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(also $\overline{2}^{-1} = \overline{2}$)

$m = 4$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(kein Körper)

In $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ gilt: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

In §4 werden wir sehen, dass $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper ist, wenn m eine Primzahl ist.

Ab hier Woche 2

Zum Abschluss dieses Abschnittes wollen wir die obige Konstruktion von $\mathbb{Z}/m\mathbb{Z}$ in einen etwas allgemeineren Kontext versetzen.

Definition 2.4. Sei $(R,+,\cdot)$ ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein ***Ideal*** in R (in Zeichen $I \trianglelefteq R$), wenn I eine Untergruppe von $(R,+)$ ist und für alle $a \in I$, $b \in R$ auch $a \cdot b \in I$ und $b \cdot a \in I$ gilt. Wir definieren eine Relation $\sim$ auf R wie folgt. Seien $a, b \in R$; dann ist $a \sim b$ falls $b - a \in I$. Dies ist eine Äquivalenzrelation. Dazu: Die Relation ist reflexiv, denn $a - a = 0 \in I$; sie ist symmetrisch, weil mit $b - a \in I$ auch $a - b = -(b - a) \in I$ gilt; sie ist transitiv, weil mit $b - a \in I$ und $c - b \in I$ auch $c - a = (c - b) + (b - a) \in I$ gilt. (Jedesmal benutzen wir, dass I eine Untergruppe bezüglich der Addition ist.) Die Äquivalenzklasse von $a \in R$ bezeichnen wir mit $\overline{a}$ und die Menge aller Äquivalenzklassen mit R/I. Es gilt:

$$\bar{a} = \{b \in R \mid b - a \in I\} = \{b \in R \mid b - a = c \text{ für ein } c \in I\} = \{a + c \mid c \in I\};$$

wir schreiben dies auch kurz als $a + I$. Wir wollen nun eine Addition und eine Multiplikation auf R/I definieren. Für $a, b \in R$ setze

$$\overline{a} + \overline{b} := \overline{a + b} \qquad \text{und} \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}.$$

Wie zuvor müssen wir zuerst zeigen, dass dies ***wohl-definiert*** ist. Seien also $a, b, a', b' \in R$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, d.h., $a' - a \in I$ und $b' - b \in I$. Dann ist auch $(a' + b') - (a + b) = (a' - a) + (b' - b) \in I$, weil I eine Untergruppe von R bezüglich der Addition ist; und ebenso $a' \cdot b' - a \cdot b = a' \cdot b' - a \cdot b' + a \cdot b' - a \cdot b = (a' - a) \cdot b' + a \cdot (b' - b) \in I$ aufgrund der weiteren Bedingung an I. Also gilt $\overline{a+b} = \overline{a'+b'}$ und $\overline{a \cdot b} = \overline{a' \cdot b'}$, d.h., die Verknüpfungen sind wohl-definiert. Sobald dies gezeigt ist, folgt wiederum sofort aus den Ring-Axiomen für R, dass die Axiome auch für R/I gelten. Der Ring R/I heißt ***Faktorring*** von R nach I. Ist R kommutativ, so auch R/I; besitzt R ein Eins-Element 1_R, so ist $\overline{1}_R$ ein Eins-Element in R/I.

Beispiel 2.5. Sei $(R,+,\cdot)$ ein kommutativer Ring. Wir setzen $(a) := \{a \cdot b \mid b \in R\} \subseteq R$ für ein festes $a \in R$. Dann sieht man sofort, dass (a) ein Ideal ist. Ideale dieser Form heißen ***Hauptideale***. Wir können also den Faktorring $R/(a)$ für jedes $a \in R$ bilden.
Ist $R = \mathbb{Z}$ und $m \in \mathbb{N}$, so ist $(m) = m\mathbb{Z}$ die Menge aller $n \in \mathbb{Z}$ mit $m \mid n$. Damit gilt $b - a \in (m) \Leftrightarrow m \mid b - a \Leftrightarrow a \equiv b \bmod m$ für alle $a, b \in \mathbb{Z}$. Also ist $\mathbb{Z}/m\mathbb{Z}$ (wie in Beispiel 2.3) das Gleiche wie $\mathbb{Z}/(m)$.

3. *Der Satz von Lagrange*

In Analogie zu obiger Definition eines Faktorringes werden wir in §?? auch Faktorgruppen nach bestimmten Untergruppen bilden. Hier zeigen wir nun zunächst den Satz von Lagrange, der grundlegend für viele Aussagen über endliche Gruppen ist.

Sei G eine Gruppe. Meistens schreiben wir nun die Verknüpfung in G als $a \cdot b$ oder einfach als ab. Üblicherweise wird dann auch das neutrale Element mit 1_G (oder einfach 1) bezeichnet,

sowie das inverse Element mit a^{-1}. Die Mächtigkeit $|G|$ wird auch als ***Ordnung*** von G bezeichnet. Wir werden sowohl endliche als auch unendliche Gruppen betrachten. Für beliebige Teilmengen $A, B \subseteq G$ schreiben wir

$$A \cdot B := \{a \cdot b \mid a \in A, b \in B\} \qquad \text{und} \qquad A^{-1} := \{a^{-1} \mid a \in A\}.$$

Ist $g \in G$, so sei $g \cdot A := \{g \cdot a \mid a \in A\}$ und $A \cdot g := \{a \cdot g \mid a \in A\}$. Damit gilt für eine Teilmenge $U \subseteq G$: $\quad U$ ist eine Untergruppe $\iff 1_G \in U, \quad U \cdot U \subseteq U, \quad U^{-1} \subseteq U.$

Satz 3.1. *Sei $U \leqslant G$ eine Untergruppe. Wir definieren wie folgt eine Relation $\sim_U$ auf G. Für $a, b \in G$ schreibe $a \sim_U b$, falls $a^{-1} \cdot b \in U$. Dann gilt:*

(a) *Die Relation $\sim_U$ ist eine Äquivalenzrelation. Sei G/U die Menge der Äquivalenzklassen. Diese sind von der Form $a \cdot U$ mit $a \in G$ und heißen **Linksnebenklassen**. Ist also T ein Vertretersystem der Äquivalenzklassen, so gilt*

$$G = \bigcup_{t \in T} t \cdot U \qquad \textit{(disjunkte Vereinigung).}$$

(b) *Für jedes feste $a \in G$ ist $U \to a \cdot U$, $u \mapsto a \cdot u$, eine Bijektion. Also gilt $|a \cdot U| = |U|$.*

Beweis. (a) Die Relation $\sim_U$ ist reflexiv: Für $a \in G$ ist $1_G = a^{-1} \cdot a \in U$ also $a \sim_U a$.
Die Relation $\sim_U$ ist symmetrisch: Für $a, b \in G$ mit $a \sim_U b$ ist $a^{-1} \cdot b \in U$ also auch $b^{-1} \cdot a = (a^{-1} \cdot b)^{-1} \in U$ und damit $b \sim_U a$.
Die Relation $\sim_U$ ist transitiv: Seien $a, b, c \in G$ mit $a \sim_U b$ und $b \sim_U c$. Dann ist $a^{-1} \cdot b \in U$ und $b^{-1} \cdot c \in U$, also auch $a^{-1} \cdot c = (a^{-1} \cdot b) \cdot (b^{-1} \cdot c) \in U$ und damit $a \sim_U c$.
Damit ist $\sim_U$ eine Äquivalenzrelation. Sei $a \in G$ fest. Dann gilt $a \sim_U b \Leftrightarrow a^{-1} \cdot b \in U \Leftrightarrow a^{-1} \cdot b = u$ für ein $u \in U \Leftrightarrow b = a \cdot u$ für ein $u \in U \Leftrightarrow b \in a \cdot U$. Also sind alle Äquivalenzklassen von der Form $a \cdot U$ mit einem $a \in G$.

(b) Die Abbildung ist offenbar surjektiv; sie ist injektiv da $a \in G$ ein Inverses besitzt. Aus $a \cdot u = a \cdot u'$ folgt also $u = 1_G \cdot u = (a^{-1} \cdot a) \cdot u = a^{-1} \cdot (a \cdot u) = a^{-1} \cdot (a \cdot u') = \ldots = u'$. $\square$

Bemerkung 3.2. Wir können auch eine Relation $\sim'_U$ wie folgt definieren: $a \sim'_U b \overset{\text{def.}}{\iff} a \cdot b^{-1} \in U$ für alle $a, b \in G$. (Beachte: Ist G abelsch, so sind $\sim_U$ und $\sim'_U$ gleich; aber im Allgemeinen ist dies nicht der Fall.) Dann gelten die analogen Aussagen wie oben, also:

(a) $\sim'_U$ ist eine Äquivalenzrelation. Sei $U\backslash G$ die Menge der Äquivalenzklassen. Diese sind von der Form $U \cdot a$ mit $a \in G$ und heißen ***Rechtsnebenklassen***. Ist also T' ein Vertretersystem der Äquivalenzklassen, so gilt $G = \bigcup_{t \in T'} U \cdot t$, wobei die Vereinigung disjunkt ist.

(b) Für jedes feste $a \in G$ ist $U \to U \cdot a$, $u \mapsto u \cdot a$, eine Bijektion. Also gilt $|U| = |U \cdot a|$.

Die Beziehung zwischen $\sim_U$ und $\sim'_U$ ist wie folgt gegeben:

(c) Ist T ein Vertretersystem der Äquivalenzklassen von $\sim_U$, so ist $T' := T^{-1}$ ein Vertretersystem der Äquivalenzklassen von $\sim'_U$. Es gilt also $|G/U| = |U\backslash G|$.

Denn: Sei $a \in G$. Dann gibt es ein $t \in T$ mit $a^{-1} \in t \cdot U$, also $a^{-1} = t \cdot u$ mit $u \in U$, und damit $a = (t \cdot u)^{-1} = u^{-1} \cdot t^{-1} \in U \cdot t^{-1}$. Also folgt bereits $G = \bigcup_{t \in T} U \cdot t^{-1}$. Diese Vereinigung ist disjunkt, denn seien $t_1, t_2 \in T$ mit $U \cdot t_1^{-1} \cap U \cdot t_2^{-1} \neq \varnothing$. Dann gibt es $u, v \in U$ mit $u \cdot t_1^{-1} = v \cdot t_2^{-1}$, also $t_1^{-1} \cdot t_2 = u^{-1} \cdot v \in U$, d.h., $t_1 \sim_U t_2$ und damit $t_1 = t_2$.

Satz 3.3 (Lagrange). *Sei $|G| < \infty$. Ist $U \leqslant G$ eine Untergruppe, so gilt $|G| = |U| \cdot |G/U|$; insbesondere ist $|U|$ ein Teiler von $|G|$. Dann heißt $[G : U] := |G/U|$ der **Index** von U in G. (Beachte: Wegen Bemerkung 3.2(c) gilt auch $[G : U] = |U\backslash G|$.)*

Beweis. Sei $T = \{t_1, \ldots, t_r\}$ ein Vertretersystem wie in Satz 3.1. Dann gilt $|G/U| = r$ und $|G| = \sum_{i=1}^{r} |U \cdot t_i|$. Wegen $|U| = |U \cdot t_i|$ für alle i folgt also $|G| = r|U|$. □

Sei G beliebig und $g \in G$ fest. Für jedes $m \in \mathbb{Z}$ können wir die Potenz $g^m \in G$ bilden (mit den Konventionen: $g^3 = g \cdot g \cdot g$, $g^0 = 1_G$, $g^{-5} = (g^{-1})^5$, usw.). Es gilt dann $g^{n+m} = g^n \cdot g^m$ und $g^{nm} = (g^n)^m$ für alle $m, n \in \mathbb{Z}$, und man sieht sofort, dass $\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}$ eine Untergruppe von G ist; diese heißt die von g erzeugte ***zyklische Untergruppe*** von G.
Gilt $G = \langle g \rangle$ für ein $g \in G$, so bezeichnen wir G als ***zyklische Gruppe*** und sagen, dass G von g erzeugt wird. Dies sind gewissermaßen die Gruppen mit der einfachst möglichen Struktur; offensichtlich sind zyklische Gruppen abelsch.
Standardbeispiele von zyklischen Gruppen: $(\mathbb{Z}, +)$ und $(\mathbb{Z}/m\mathbb{Z}, +)$ (mit $m \in \mathbb{N}$); diese werden von 1 bzw. $\bar{1}$ erzeugt (beachte, dass die Verknüpfungen hier additiv geschrieben werden).

Definition 3.4. Sei $g \in G$. Gibt es ein $m \in \mathbb{N}$ mit $g^m = 1_G$, so definieren wir

$$o(g) := \min\{m \in \mathbb{N} \mid g^m = 1_G\};$$

gibt es kein solches m, so setzen wir $o(g) = \infty$. Dann heißt $o(g)$ die ***Ordnung von*** g. Diese kann sowohl endlich oder unendlich sein.

Ist zum Beispiel $G = \mathrm{GL}_2(\mathbb{Q})$ und $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$, so gilt $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ für alle $n \in \mathbb{Z}$, also ist $o(g) = \infty$. Ist dagegen $g = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, so erhalten wir $o(g) = 6$, denn

$$g^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad g^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g^4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad g^5 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad g^6 = I_2.$$

Lemma 3.5. *Sei $g \in G$ fest.*
(a) *Sei $m \in \mathbb{N}$ mit $g^m = 1_G$; dann gilt $o(g) \mid m$.*
(b) *Ist $o(g) < \infty$, so gilt $o(g) = |\langle g \rangle|$ und $\langle g \rangle = \{1_G, g, g^2, \ldots, g^{o(g)-1}\}$.*
(c) *Ist $o(g) = \infty$, so gilt $g^i \neq g^j$ für alle $i, j \in \mathbb{Z}$, $i \neq j$; folglich ist $|\langle g \rangle| = \infty$.*

Beweis. (a) Sei $d := o(g) < \infty$. Division mit Rest ergibt $m = qd + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < d$. Damit ist $g^m = g^{qd+r} = (g^d)^q \cdot g^r = 1_G^q \cdot g^r = g^r$. Da $g^m = 1_G$ gilt, ist also auch $g^r = 1_G$ und damit $r = 0$ wegen der Minimalität von d. Also gilt $o(g) = d \mid m$.

(b) Sei wieder $d := o(g)$. Sei $i \in \mathbb{Z}$ beliebig. Division mit Rest ergibt $i = dq + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < d$. Wie oben folgt $g^i = g^{dq+r} = g^r$. Damit ist $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{d-1}\}$. Für $0 \leqslant i < j \leqslant d - 1$ ist $g^i \neq g^j$, denn sonst wäre $g^{j-i} = 1_G$ mit $1 \leqslant j - i < d$, Widerspruch zur Minimalität von d. Also ist $|\langle g \rangle| = d = o(g)$.

(c) Gibt es $i > j$ in $\mathbb{Z}$ mit $g^i = g^j$, so folgt $g^{i-j} = 1_G$ und damit $o(g) < \infty$. □

Folgerung 3.6. *Sei G eine endliche Gruppe, also $|G| < \infty$. Für alle $g \in G$ ist dann $o(g) < \infty$ ein Teiler von $|G|$ und es gilt $g^{|G|} = 1$.*

Beweis. Wäre $o(g) = \infty$, so auch $|\langle g \rangle| = \infty$ nach Lemma 3.5(c), und damit $|G| = \infty$, Widerspruch. Nach Lemma 3.5(b) hat die Untergruppe $\langle g \rangle \leqslant G$ genau $o(g)$ Elemente, also ist $o(g)$ ein Teiler von $|G|$ nach dem Satz von Lagrange. Schreiben wir $|G| = o(g)m$ mit $m \in \mathbb{N}$, so folgt also $g^{|G|} = (g^{o(g)})^m = 1_G^m = 1_G$. □

Bemerkung 3.7. Sei $g \in G$ mit $o(g) < \infty$. Behauptung: Für $d \in \mathbb{N}$ mit $d \mid o(g)$ gilt $o(g^d) = o(g)/d$. Dazu: Sei $m := o(g^d)$ und $n := o(g)/d$. Dann ist $(g^d)^n = g^{dn} = g^{o(g)} = 1_G$, also $m = o(g^d) \mid n$ nach Lemma 3.5. Umgekehrt ist $1_G = (g^d)^m = g^{dm}$, also $o(g) \mid dm$ (wiederum nach Lemma 3.5) und damit $n = o(g)/d \mid m$. Also folgt $n = m$.

Allein mit dem Satz von Lagrange und den obigen Folgerungen können wir bereits eine Reihe von Beispielen untersuchen.

Beispiel 3.8. (a) Sei $|G| = p$ eine Primzahl. Dann ist G zyklisch, und G besitzt überhaupt nur die Untergruppen $\{1_G\}$ und G. Denn ist $U \leqslant G$, so ist $|U|$ ein Teiler von $p = |G|$, also $|U| = 1$ oder $|U| = p$, also $U = \{1_G\}$ oder $U = G$. Ist $g \neq 1_G$, so folgt damit $\{1_G\} \neq \langle g \rangle = G$.

(b) Sei $|G| = 4$. Dann ist $o(g) \in \{1, 2, 4\}$ für alle $g \in G$. Gibt es ein $g \in G$ mit $o(g) = 4$, so ist $G = \langle g \rangle$ zyklisch. Sonst gilt $g^2 = 1_G$ für alle $g \in G$.

Dann ist $G = \{1_G, x, y, z\}$ mit folgender Multiplikationstabelle:

	1_G	x	y	z
1_G	1_G	x	y	z
x	x	1_G	z	y
y	y	z	1_G	x
z	z	y	x	1_G

Dazu: Betrachte $xy \in G$. Dies muss also gleich 1_G, x, y oder z sein. Ist $xy = 1_G$, so $x = y^{-1} = y$ (wegen $y^2 = 1_G$), Widerspruch; ist $xy = x$, so $y = 1_G$, Widerspruch; ist $xy = y$, so $x = 1_G$, Widerspruch. Also muss $xy = z$ gelten. Analog findet man alle anderen Produkte. Insbesondere sieht man, dass G abelsch ist. Ein solches G heißt ***Klein'sche Vierergruppe***.

Beispiel 3.9. Sei $G = S_3$. Dann besteht G genau aus den 6 Permutationen:

$$\mathrm{id} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \sigma_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \pi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \pi' = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Wir berechnen $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \mathrm{id}$, $\pi^2 = \pi'$ und $\pi^3 = \pi'^3 = \mathrm{id}$. Also gilt $o(\sigma_1) = o(\sigma_2) = o(\sigma_3) = 2$ und $o(\pi) = o(\pi') = 3$. Damit erhalten wir folgende zyklische Untergruppen:

$$U_i = \langle\sigma_i\rangle = \{\mathrm{id}, \sigma_i\} \quad \text{für } i = 1,2,3, \qquad V = \langle\pi\rangle = \langle\pi'\rangle = \{\mathrm{id}, \pi, \pi'\}.$$

Wir behaupten, dass dies alle echten Untergruppen von G sind. Sei also $U' \leqslant G$ eine beliebige Untergruppe mit $\{\mathrm{id}\} \neq U' \neq G$. Nach Lagrange ist $|U'|$ ein Teiler von 6, also $|U'| = 2$ oder 3. Nach Beispiel 3.8(a) ist U' zyklisch und muss daher eine der obigen Untergruppen sein.

Beispiel 3.10. Wir betrachten die folgenden Elemente in $G = \mathrm{GL}_2(\mathbb{C})$:

$$E = \begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad I = \begin{pmatrix}0&1\\-1&0\end{pmatrix}, \quad J = \begin{pmatrix}0&i\\i&0\end{pmatrix}, \quad K = \begin{pmatrix}i&0\\0&-i\end{pmatrix},$$

(wobei wie üblich $i = \sqrt{-1}$). Man rechnet sofort nach, dass $I^2 = J^2 = K^2 = I\cdot J\cdot K = -E$ gilt; daraus erhält man $I^{-1} = -I$, $J^{-1} = -J$, $K^{-1} = -K$ sowie $I\cdot J = -K^{-1} = K$, $J\cdot K = -I^{-1} = I$, $I\cdot K = -J$. Damit sieht man auch leicht, dass $Q_8 := \{\pm E, \pm I, \pm J, \pm K\}$ eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ ist. Diese Gruppe wird als ***Quaternionengruppe*** bezeichnet; sie hat genau 8 Elemente und ist nicht abelsch (zum Beispiel ist $I\cdot J = K$ und $J\cdot I = -K$). Die obigen Rechnungen zeigen, dass $o(-E) = 2$ und $o(\pm I) = o(\pm J) = o(\pm K) = 4$ gilt. Wir erhalten also die folgenden zyklischen Untergruppen:

$$U_1 = \langle I\rangle = \{\pm E, \pm I\}, \quad U_2 = \langle J\rangle = \{\pm E, \pm J\}, \quad U_3 = \langle K\rangle = \{\pm E, \pm K\}, \quad Z = \langle -E\rangle = \{\pm E\}.$$

Wir behaupten wiederum, dass dies alle echten Untergruppen von G sind. Sei also $U' \leqslant Q_8$ eine beliebige Untergruppe mit $\{\mathrm{id}\} \neq U' \neq Q_8$. Nach Lagrange ist $|U'|$ ein Teiler von 8, also $|U'| = 2$ oder 4. Ist $|U'| = 2$, so ist U' zyklisch, also muss $U' = Z$ gelten, denn es gibt nur ein Element der Ordnung 2 (nämlich $-E$). Sei nun $|U'| = 4$. Ist U' zyklisch, so muss $U' = U_i$ für $i \in \{1,2,3\}$ gelten, denn jedes Element der Ordnung 4 liegt in einer dieser Untergruppen. Bleibt also noch die Möglichkeit, dass U' nicht zyklisch ist. Nach Beispiel 3.8(b) enthält dann U' aber 3 Elemente der Ordnung 2, Widerspruch.

Beispiel 3.11. Sei G eine zyklische Gruppe, also $G = \langle g\rangle$ mit einem $g \in G$. Dann gilt: Ist $U \leqslant G$ beliebige Untergruppe, so ist U zyklisch; es gibt ein $m \in \mathbb{N}_0$ mit $U = \langle g^m\rangle$.

Dazu: Ist $U = \{1_G\}$, so gilt die Behauptung mit $m = 0$. Sei nun $U \neq \{1_G\}$; es gibt also ein $i \in \mathbb{Z}$, $i \neq 0$, mit $g^i \in U$. Ist $i < 0$, so gilt auch $g^{-i} = (g^{-1})^i \in U$. In jedem Fall existiert also ein $m \in \mathbb{N}$ mit $g^m \in U$; sei m minimal mit dieser Eigenschaft. Wegen $g^m \in U$ ist auch $\langle g^m\rangle \subseteq U$. Umgekehrt sei $u \in U$ beliebig. Schreibe $u = g^j$ mit $j \in \mathbb{Z}$. Division mit Rest

ergibt $j = qm + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < m$. Dann ist $g^r = g^{j-qm} = g^j \cdot (g^m)^{-q} \in U$. Ist $r > 0$, so erhalten wir einen Widerspruch zur Minimalität von m. Also muss $r = 0$ gelten und damit $u = g^j = (g^m)^q \in \langle g^m \rangle$. Also gilt auch $U \subseteq \langle g^m \rangle$, und damit Gleichheit.

4. *Die Eulersche Phi-Funktion*

In diesem Abschnitt erinnern wir zunächst an einige Begriffe und Definitionen aus der elementaren Zahlentheorie. Seien $d, n \in \mathbb{Z}$ mit $d \neq 0$ und $n \neq 0$. Gilt $d \mid n$ (d.h., d teilt n), so folgt natürlich auch $(-d) \mid n$ und $|d| \leqslant n$. Also gibt es nur endlich viele positive Teiler von n. Sind $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$ gegeben, so definieren wir

$$\mathrm{ggT}(n, m) := \max\{\, a \in \mathbb{N} \mid \text{es gilt } a \mid n \text{ und } a \mid m \,\}$$

als den ***größten gemeinsamen Teiler*** von n und m. Gilt $\mathrm{ggT}(n, m) = 1$, so bezeichnen wir m und n als ***teilerfremd***.

Lemma 4.1 (Lemma von Bézout)**.** *Gegeben seien $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$. Dann gibt es $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$. Insbesondere: Ist auch $d' \in \mathbb{N}$ ein gemeinsamer Teiler von n und m, so gilt nicht nur $d' \leqslant d$, sondern $d' \mid \mathrm{ggT}(n, m)$.*

Beweis. Zunächst beachte $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, m)$. Außerdem sieht man sofort $\mathrm{ggT}(m, n) = \mathrm{ggT}(\pm m, \pm n)$; gilt weiterhin $\mathrm{ggT}(m, n) = am + bn$ mit $a, b \in \mathbb{Z}$, so erhält man analoge Darstellungen von $\mathrm{ggT}(\pm m, \pm n)$ (z.B. $\mathrm{ggT}(-m, n) = (-a)(-m) + bn$). Also genügt es, den Fall $n, m \geqslant 0$ zu betrachten. Wir verwenden vollständige Induktion nach m.
Ist $m = 0$, so ist $n > 0$ und $n = \mathrm{ggT}(0, n) = 0 \cdot m + 1 \cdot n$, also gilt die Aussage.
Sei nun $m > 0$ und $n \geqslant 0$ beliebig. Teilen mit Rest ergibt $n = qm + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < m$. Nach Induktion gibt es $a_1, b_1 \in \mathbb{Z}$ mit $d := \mathrm{ggT}(r, m) = a_1 r + b_1 m$. Nun beachte: Ein gemeinsamer Teiler von r, m ist wegen $n = qm + r$ auch ein gemeinsamer Teiler von m, n; und umgekehrt ist ein gemeinsamer Teiler von m, n wegen $r = n - qm$ auch ein gemeinsamer Teiler von r, m. Also folgt $\mathrm{ggT}(m, n) = \mathrm{ggT}(r, m) = d$; außerdem ist $d = a_1 r + b_1 m = a_1(n - qm) + b_1 m = (b_1 - qa_1)m + a_1 n$. □

Aus dem obigen Beweis erhält man sogar ein Verfahren, genannt (erweiterter) ***Euklidischer Algorithmus***, zur Bestimmung von $\mathrm{ggT}(m, n)$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = am + bn$. Sei zum Beispiel $m = 462$ und $n = 1071$. Teilen mit Rest ergibt $1071 = 2 \cdot 462 + 147$, also gilt $\mathrm{ggT}(462, 1071) = \mathrm{ggT}(147, 462)$ (siehe obiger Beweis). Erneutes Teilen mit Rest ergibt $462 = 3 \cdot 147 + 21$, also nun $\mathrm{ggT}(147, 462) = \mathrm{ggT}(21, 147)$. Und nochmaliges Teilen mit Rest ergibt $147 = 7 \cdot 21 + 0$, also schließlich $\mathrm{ggT}(21, 147) = \mathrm{ggT}(0, 21) = 21$. Nun gehe obige Gleichungen vom Ende her durch, um $a, b \in \mathbb{Z}$ zu bestimmen mit $\mathrm{ggT}(m, n) = am + bn$. Hier erhalten

wir aus der vorletzten Gleichung $21 = 462 - 3 \cdot 147$; aus der vorherigen Gleichung erhalten wir $147 = 1071 - 2 \cdot 462$; Einsetzen ergibt $21 = 462 - 3 \cdot (1071 - 2 \cdot 462) = 7 \cdot 462 + (-3) \cdot 1071$.

Zum Beispiel in Python kann man den ganzen Algorithmus in nur 5 (!) Zeilen programmieren. "Input" sind $m, n \geqslant 0$; "Output" ist $\big(\mathrm{ggT}(m,n), a, b\big)$ wobei $\mathrm{ggT}(m,n) = am + bn$:

```
>>> def EuclAlg(m,n):
...   if m==0: return n,0,1
...   q,r=divmod(n,m)          # Teilen mit Rest
...   d,a1,b1=EuclAlg(r,m)
...   return d,b1-q*a1,a1
>>> EuclAlg(462,1071)
(21, 7, -3)
```

Bemerkung 4.2. Seien $m_1, m_2, n \in \mathbb{Z}$, $m_1 \neq 0$ und $m_2 \neq 0$. Dann gilt:

(a) $\mathrm{ggT}(m_i, n) = 1$ für $i = 1, 2$ $\Rightarrow$ $\mathrm{ggT}(m_1 m_2, n) = 1$,

(b) $\mathrm{ggT}(m_1, m_2) = 1$ und $m_i \mid n$ für $i = 1, 2$ $\Rightarrow$ $m_1 m_2 \mid n$.

Diese Aussagen folgen sofort aus der eindeutigen Zerlegung von ganzen Zahlen in Primfaktoren, aber man kann sie auch sehr leicht direkt mit Bézouts Lemma zeigen.

Zu (a): Es gibt $a_i, b_i \in \mathbb{Z}$ mit $a_i m_i + b_i n = 1$ für $i = 1, 2$. Dann erhalten wir auch eine Gleichung $1 = (a_1 m_1 + b_1 n)(a_2 m_2 + b_2 n) = a_1 a_2 m_1 m_2 + (a_1 m_1 b_2 + b_1 a_2 m + b_1 b_2 n)n$. Ist $d \in \mathbb{N}$ ein Teiler von $m_1 m_2$ und n, so teilt d die rechte Seite der Gleichung und damit $d = 1$.

Zu (b): Es gibt $a, b \in \mathbb{Z}$ mit $1 = am_1 + bm_2$; außerdem ist $n = c_i m_i$ mit $c_i \in \mathbb{Z}$ für $i = 1, 2$. Dann erhalten wir $n = am_1 n + bm_2 n = am_1 c_2 m_2 + bm_2 c_1 m_1$, also $m_1 m_2 \mid n$.

Satz 4.3. *Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann ist $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ genau dann, wenn $\mathrm{ggT}(a, m) = 1$ gilt. Insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn m eine Primzahl ist.*

Ist p eine Primzahl, so schreiben wir auch $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Beweis. Für $a \in \mathbb{Z}$ gelten die folgenden Äquivalenzen:

$$\begin{aligned} \bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \quad &\Leftrightarrow \quad \bar{1} = \bar{a} \cdot \bar{b} = \overline{ab} \text{ für ein } b \in \mathbb{Z} \quad \Leftrightarrow \quad m \mid ab - 1 \text{ für ein } b \in \mathbb{Z} \\ &\Leftrightarrow \quad 1 = ab + cm \text{ für ein } b \in \mathbb{Z} \text{ und ein } c \in \mathbb{Z}. \end{aligned}$$

Nach Bézouts Lemma ist aber die letzte Bedingung dazu äquivalent, dass $\mathrm{ggT}(a, m) = 1$ ist. Sei nun m eine Primzahl. Ist $\bar{a} \neq \bar{0}$, so gilt $m \nmid a$ und damit $\mathrm{ggT}(a, m) = 1$, also $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. D.h., jedes Element ungleich $\bar{0}$ in $\mathbb{Z}/m\mathbb{Z}$ ist eine Einheit. Also ist $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper. Umgekehrt: Ist m keine Primzahl, d.h., $m = m_1 m_2$ mit $0 < m_1, m_2 < m$, so gilt $\bar{m}_1 \cdot \bar{m}_2 = \bar{m} = \bar{0}$, aber $\bar{m}_1 \neq \bar{0}$ und $\bar{m}_2 \neq \bar{0}$. Wäre $\mathbb{Z}/m\mathbb{Z}$ ein Körper, so existiert $\bar{m}_1^{-1} \in \mathbb{Z}/m\mathbb{Z}$. Aber dann folgt $\bar{0} = \bar{m}_1^{-1} \cdot \bar{0} = \bar{m}_1^{-1} \cdot (\bar{m}_1 \cdot \bar{m}_2) = \bar{m}_2$, Widerspruch. □

Definition 4.4. Für $m \in \mathbb{N}$ setze $\phi(m) := |(\mathbb{Z}/m\mathbb{Z})^\times|$. Wegen $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ ist $\phi(m)$ also nach Satz 4.3 die Anzahl der $i \in \{0, 1, \ldots, m-1\}$ mit $\mathrm{ggT}(i, m) = 1$. Diese

Funktion heißt ***Eulersche Phi-Funktion***. Hier sind einige Werte:

m	1	2	3	4	5	6	7	8	9	10	11	12	...
$\phi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	...

Es gilt stets $\phi(m) > 0$ (denn $\bar{1} \in (\mathbb{Z}/m\mathbb{Z})^\times$, und dies gilt auch für $m = 1$). Ist p eine Primzahl, so gilt offenbar $\phi(p) = p - 1$.

Ab hier Woche 3

Folgerung 4.5 (Satz von Euler). *Sei* $m \in \mathbb{N}$. *Dann gilt* $a^{\phi(m)} \equiv 1 \bmod m$ *für alle* $a \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, m) = 1$.

Beweis. Sei $a \in \mathbb{Z}$ und $\mathrm{ggT}(a, m) = 1$. Nach Satz 4.3 ist also $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Wegen $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$ erhalten wir $\bar{a}^{\phi(m)} = \bar{1}$ mit Folgerung 3.6, also die Behauptung. □

Folgerung 4.6 (Kleiner Satz von Fermat). *Ist* p *eine Primzahl, so gilt* $a^p \equiv a \bmod p$ *für alle* $a \in \mathbb{Z}$.

Beweis. Sei zuerst $p \nmid a$, also $\mathrm{ggT}(a, p) = 1$. Wegen $\phi(p) = p - 1$ folgt $a^{p-1} \equiv 1 \bmod p$ aus dem Satz von Euler, also auch $a^p \equiv a \bmod p$. Ist $p \mid a$, so gilt auch $p \mid a^p$ und damit ebenfalls $a^p \equiv 0 \equiv a \bmod p$. □

Beispiel 4.7. Eine ***Mersenne-Zahl*** ist eine Zahl der Form $2^n - 1$ mit $n \in \mathbb{N}$. Diese Zahlen sind besonders geeignet, um große Primzahlen zu finden. Ist nämlich p eine Primzahl, so gilt $q > p$ für alle Primzahlen q mit $q \mid 2^p - 1$.
Beweis: Ist $q \mid 2^p - 1$, so gilt also $\bar{2}^p = \bar{1}$ in $\mathbb{Z}/q\mathbb{Z}$. Damit ist $\bar{2}$ eine Einheit in $\mathbb{Z}/q\mathbb{Z}$. Wegen $\bar{2}^p = \bar{1}$ folgt $o(\bar{2}) \mid p$; siehe Lemma 3.5. Wegen $\bar{2} \neq \bar{1}$ und weil p eine Primzahl ist, gilt $o(\bar{2}) = p$. Nach Satz 4.3 ist $\mathbb{Z}/q\mathbb{Z}$ ein Körper, also $|(\mathbb{Z}/q\mathbb{Z})^\times| = q - 1$. Mit Folgerung 3.6 folgt dann $p = o(\bar{2}) \mid q - 1$ und damit $p < q$.

Hier ist eine weitere Charakterisierung von $\phi(n)$, mittels Erzeugern für zyklische Gruppen.

Satz 4.8. *Sei* $G = \langle g \rangle$ *eine zyklische Gruppe mit* $n := o(g) < \infty$. *Für* $i \in \mathbb{Z}$ *gilt dann* $G = \langle g^i \rangle \Leftrightarrow \mathrm{ggT}(i, n) = 1$. *Folglich ist* $\phi(n)$ *gleich der Anzahl der* $x \in G$ *mit* $G = \langle x \rangle$.

Beweis. Sei zuerst $G = \langle g \rangle = \langle g^i \rangle$. Dann ist $g = (g^i)^m = g^{im}$ für ein $m \in \mathbb{Z}$. Daraus folgt $g^{im-1} = 1_G$, also $n = o(g) \mid im - 1$ und damit $im - 1 = an$ mit $a \in \mathbb{Z}$. Dann ist $1 = im - an$, also $\mathrm{ggT}(i, n) = 1$. Sei umgekehrt $\mathrm{ggT}(i, n) = 1$. Nach Bézout gibt es $a, b \in \mathbb{Z}$ mit $1 = ai + bn$. Dann folgt $g = g^1 = g^{ai+bn} = (g^i)^a \cdot (g^n)^b = (g^i)^a \cdot 1_G = (g^i)^a \in \langle g^i \rangle$, also auch $G = \langle g \rangle \subseteq \langle g^i \rangle$. Die umgekehrte Inklusion ist klar, also gilt Gleichheit.

Nun ist $G = \{g^i \mid 0 \leqslant i \leqslant n - 1\}$. Sei $x \in G$, also $x = g^i$ mit $0 \leqslant i \leqslant n - 1$. Dann gilt $G = \langle x \rangle = \langle g^i \rangle \Leftrightarrow \mathrm{ggT}(i, n) = 1$. Also ist die Anzahl der $x \in G$ mit $G = \langle x \rangle$ genau gleich der Anzahl der $i \in \{0, 1, \ldots, n - 1\}$ mit $\mathrm{ggT}(i, n) = 1$, also gleich $\phi(n)$. □

5. *Eine Anwendung: Das RSA-Verfahren*

Als eine Anwendung von Bézouts Lemma und dem Satz von Euler beschreiben wir nun das ***RSA-Verschlüsselungsverfahren***, das 1977 von R. Rivest, A. Shamir und L. Adleman entwickelt wurde; siehe auch https://en.wikipedia.org/wiki/RSA_(cryptosystem).

Alice erwartet von Bob (übliche Namen in Texten zur Verschlüsselung) eine Nachricht, aber sie möchte vermeiden, dass andere auch diese Nachricht verstehen können (selbst wenn sie die Nachricht sehen können). Eine Nachricht ist hier einfach eine Zahl $m \in \mathbb{N}$, die man nach einem bestimmten Verfahren aus Buchstaben oder sonstigen Daten bildet.

Konkretes Beispiel: Alice erwartet von Bob einen Tipp, ob der VfB Stuttgart am nächsten Bundesliga-Spieltag gewinnt, verliert oder unentschieden spielt. Um dies zu vereinfachen, soll Bob einfach nur ein G, V oder U senden, also als Zahl 7, 22 oder 21 (Nummer im Alphabet).

Idee der Verschlüsselung. Alice wählt zwei Primzahlen $p \neq q$ und bildet $N := p \cdot q$. Hierbei muss $m < N$ gelten, für alle m die man als Nachricht senden möchte. (Und generell wird die Verschlüsselung umso sicherer, je größer p, q und damit N sind; siehe die Diskussion weiter unten.) Dann berechnet Alice den Wert von Eulers Funktion $\phi(N)$, wie folgt:

Lemma 5.1. *Sei $N = pq$ mit Primzahlen $p \neq q$ wie oben. Dann gilt $\phi(N) = (p-1)(q-1)$.*

Beweis. Ist $1 \leqslant d < N$, so gilt $\mathrm{ggT}(d, N) \in \{1, p, q\}$. Hier ist $\mathrm{ggT}(d, N) = p$ für $d = p, 2p, \ldots, (q-1)p$ (und keine dieser Zahlen ist durch q teilbar); analog ist $\mathrm{ggT}(d, N) = q$ für $d = q, 2q, \ldots, (p-1)q$ (und keine dieser Zahlen ist durch p teilbar). Also bleiben für $\mathrm{ggT}(d, N) = 1$ genau $(N-1) - (p-1) - (q-1) = (p-1)(q-1)$ Möglichkeiten übrig. □

Schließlich wählt Alice eine weitere Zahl $e \in \mathbb{N}$ mit

$$1 < e < \phi(N) \qquad \text{und} \qquad \mathrm{ggT}(e, \phi(N)) = 1,$$

also zum Beispiel eine weitere Primzahl, die $\phi(N)$ nicht teilt. Nun veröffentlicht Alice das Paar (e, N); dieses heißt daher auch "***public key***". (Aber Alice hält die Primzahlen p, q geheim.) Alle, die Alice eine Nachricht verschlüsselt schicken wollen, können nun wie folgt vorgehen: Ist $m \in \mathbb{N}$ die Nachricht ($1 \leqslant m < N$), so berechne m^e und dividiere dies mit Rest durch N; dies liefert ein eindeutiges $c \in \mathbb{Z}$ mit

$$m^e \equiv c \bmod N \qquad \text{und} \qquad 0 \leqslant c < N.$$

Dann verschicke c als verschlüsselte Nachricht. Wie kann Alice aus c, e, N die Zahl m (also die tatsächlich interessierende Nachricht) zurückberechnen? Nun, es gilt $\bar{m}^e = \bar{c}$ in $\mathbb{Z}/N\mathbb{Z}$; also müsste sie (oder auch jemand sonst) die e-te Wurzel von $\bar{c}$ in $\mathbb{Z}/N\mathbb{Z}$ berechnen. Sie

könnte also zum Beispiel einfach alle $0 \leqslant a < N$ darauf testen, ob $a^e \equiv c \bmod N$ gilt, aber für große N ist dies nicht praktikabel (zu viele Multiplikationen und Divisionen mit Rest).

Idee der Entschlüsselung. Hier kommt nun die Wahl von e ins Spiel. Alice hatte diese Zahl so gewählt, dass $\operatorname{ggT}(e, \phi(N)) = 1$ gilt, d.h., $\bar{e}$ ist eine Einheit in $\mathbb{Z}/\phi(N)\mathbb{Z}$. Also gibt es ein eindeutiges $d \in \mathbb{Z}$ mit $1 \leqslant d < \phi(N)$ und $\bar{d} \cdot \bar{e} = \bar{1}$ in $\mathbb{Z}/\phi(N)\mathbb{Z}$. Dieses d wird als "***private key***" bezeichnet, und wird von Alice geheim gehalten. Sie kann d leicht wie folgt berechnen. Nach Bézouts Lemma gibt es $a, b \in \mathbb{Z}$ mit $1 = \operatorname{ggT}(e, \phi(N)) = ae + b\phi(N)$; dann folgt $\bar{a} \cdot \bar{e} = \bar{1}$ in $\mathbb{Z}/\phi(N)\mathbb{Z}$. Division mit Rest liefert ein $d \in \mathbb{Z}$ mit $a \equiv d \bmod \phi(N)$ und $0 \leqslant d < \phi(N)$; dann ist $\bar{a} = \bar{d}$ und $d \neq 0$, also ist d der gewünschte "private key". Die folgende Aussage zeigt nun, dass wir damit eine effiziente Methode erhalten, um die e-te Wurzel einer Zahl modulo N zu bestimmen.

Lemma 5.2. *Mit obigen Bezeichnungen gilt* $(m^e)^d \equiv m \bmod N$.

Beweis. Wir zeigen zuerst $(m^e)^d \equiv m \bmod p$, d.h., $p \mid (m^e)^d - m$. Ist $p \mid m$, so auch $p \mid (m^e)^d$ und damit $(m^e)^d \equiv 0 \equiv m \bmod p$, wie gewünscht. Sei nun $p \nmid m$, also $\operatorname{ggT}(p, m) = 1$. Nun ist $\phi(p) = p - 1$. Aus dem Satz von Euler folgt also $m^{p-1} \equiv 1 \bmod p$. Die Zahl d war so definiert, dass $\bar{e} \cdot \bar{d} = \bar{1}$ in $\mathbb{Z}/\phi(N)\mathbb{Z}$ gilt, also $\phi(N) \mid ed - 1$. Nach Lemma 5.1 ist $\phi(N) = (p-1)(q-1)$. Also ist auch $p - 1 \mid ed - 1$ und wir schreiben $ed - 1 = a(p-1)$ mit $a \in \mathbb{N}$. Damit erhalten wir

$$(m^e)^d \equiv m^{ed} \equiv m^{ed-1+1} \equiv m^{a(p-1)+1} \equiv (m^{p-1})^a m \equiv 1^a m \equiv m \bmod p,$$

wie gewünscht. Auf völlig analoge Weise zeigt man dann auch $(m^e)^d \equiv m \bmod q$, d.h., $q \mid (m^e)^d - m$. Da p, q verschiedene Primzahlen sind, gilt $\operatorname{ggT}(p, q) = 1$ und mit Bemerkung 4.2(b) folgt schließlich auch $pq \mid (m^e)^d - m$, also die Behauptung. □

Alice kann nun leicht die empfangene Nachricht c entschlüsseln: Sie bildet c^d (mit dem "private key" d) und dividiert mit Rest durch N; wegen $c \equiv m^e$ ist der Rest genau die Nachricht m; siehe Lemma 5.2. — Noch eine Bemerkung dazu: Zum Berechnen von c^d (vor allem für große d) benutzt man am besten folgende Rekursion:

$$c^d \equiv \begin{cases} (c^2)^{d/2} \bmod N & \text{falls } d \text{ gerade,} \\ c(c^2)^{(d-1)/2} \bmod N & \text{falls } d \text{ ungerade.} \end{cases}$$

Wo liegt die Sicherheit dieses Verfahrens? Alice hält den private key d geheim, sowie die Primzahlen p und q, mit denen N gebildet wurde; sie kann d leicht mit dem Euklidischen Algorithmus und Bézouts Lemma ausrechnen, weil sie $\phi(N) = (p-1)(q-1)$ kennt. Aber für jemanden, der nur N und e kennt, ist es praktisch extrem schwierig (jedenfalls bei großen N) den Wert $\phi(N)$ (und damit dann auch den private key d) zu berechnen. Entweder testet

man direkt alle $i \in \{1, \dots, N-1\}$ darauf, ob $\mathrm{ggT}(i, N) = 1$ gilt, oder man versucht die Faktorisierung $N = p \cdot q$ zu finden. — In Anwendungen werden tatsächlich Primzahlen p und q mit Hunderten von Ziffern verwendet, und selbst die schnellsten Computer der Welt würden zu lange brauchen, um $\phi(N)$ direkt zu berechnen oder die Faktorisierung $N = pq$ zu finden. (Es gibt allerdings keinen formalen Beweis, dass dieses Problem nicht doch eines Tages eine effiziente Lösung findet.) Für weitere Details siehe auch

C. Karpfinger und H. Kiechle, Kryptologie, Algebraische Methoden und Algorithmen, Vieweg+Teubner Verlag, 2010.

Zurück zum konkreten Beispiel mit dem VfB–Tipp. Alice wählt $p = 101$ und $q = 103$. Damit erhält man $N = pq = 10403$ und $\phi(N) = (p-1)(q-1) = 10200$. Außerdem wählt sie $e = 1001$ und berechnet $d = 2201$. (Dann gilt in der Tat $ed \equiv 1 \bmod 10200$.) Also:

$$\text{“Public key”:} \quad (e, N) = (1001, 10403), \qquad \text{“private key”:} \quad d = 2201.$$

Alice erhält von Bob die Nachricht: $c = 2532$.
Welchen Tipp (also welche ursprüngliche Nachricht m) hat Bob ihr geschickt?

[Nun, es gilt $c^d = 2532^{2201} \equiv 7 \bmod 10403$, also war der Tipp natürlich $m = 7$, d.h., “Gewinn”.]

Was für uns hier bemerkenswert ist:

Am Beispiel des RSA-Verfahrens zeigt sich, dass Betrachtungen zu Primzahlen und Arithmetik in $\mathbb{Z}$, also Jahrhunderte alten Themen der reinen Mathematik, schließlich doch zu konkreten Anwendungen führen können.[1]

[1] Und die Geschichte hinsichtlich Verschlüsselungsverfahren ist hiermit noch keineswegs beendet, Stichwort “Elliptic Curve Cryptography”; siehe zum Beispiel die Diskussion in §6.3.4 im Buch von Karpfinger–Meyberg, oder Kapitel 13 im oben genannten Buch von Karpfinger–Kiechle.

Kapitel II: Gruppen

Wir haben bereits einige Aussagen zu Gruppen gezeigt, aber meistens zu abelschen oder zyklischen Gruppen. Hier geht es nun um den Fall allgemeiner (nicht unbedingt abelscher) Gruppen. Wie zuvor schreiben wir die Verknüpfung in einer Gruppe G als $a \cdot b$ oder einfach als ab; das neutrale Element wird mit 1_G bezeichnet, das zu $a \in G$ inverse Element mit a^{-1}.

6. *Erzeugendensysteme*

Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Wir definieren das ***Erzeugnis von*** S als

$$\langle S \rangle := \bigcap_{U \leqslant G \text{ mit } S \subseteq U} U.$$

Der Schnitt wird über eine nicht-leere Menge gebildet, denn $U = G$ kommt immer in dieser Menge vor. Wir haben bereits in §1 bemerkt, dass beliebige Durchschnitte von Untergruppen wieder Untergruppen sind. Also ist $\langle S \rangle$ eine Untergruppe von G. Für $S = \varnothing$ ist $\langle \varnothing \rangle = \{1_G\}$. Ist $S = \{s_1, \ldots, s_n\}$ eine endliche Menge, so schreiben wir auch einfach $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$. Die obige Konstruktion liefert einerseits ein praktisches Verfahren, um Untergruppen einer gegebenen Gruppe G zu definieren. Andererseits kann man sich für G selbst die Frage stellen, eine möglichst einfache oder kleine Teilmenge $S \subseteq G$ mit $G = \langle S \rangle$ zu finden.

Lemma 6.1. *Sei $\varnothing \neq S \subseteq G$. Dann ist $\langle S \rangle = \{1_G\} \cup \{s_1 \cdots s_r \mid r \geqslant 1, s_i \in S$ oder $s_i^{-1} \in S\}$. Für $S = \{g\}$ ist $\langle \{g\} \rangle = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ (wie bereits in §3 definiert).*

Beweis. Sei H die rechte Seite obiger Gleichung. Es gilt $1_G \in H$ und man sieht sofort, dass Produkte und Inverse von Elementen in H wieder in H sind. Also ist $H \leqslant G$. Nun ist $S \subseteq H$, also kommt H im Durchschnitt in der Definition von $\langle S \rangle$ vor. Damit gilt $\langle S \rangle \subseteq H$. Umgekehrt sei $U \leqslant G$ beliebig mit $S \subseteq U$. Dann ist auch $H \subseteq U$, also ist H auch im Durchschnitt in der Definition von $\langle S \rangle$ enthalten. Also gilt $H = \langle S \rangle$. Die Aussage über $\langle \{g\} \rangle$ ist dann klar. □

Beispiel 6.2. (a) Sei $G = S_3$. Dann gilt $G = \langle \sigma_1, \sigma_2 \rangle$, wobei $\sigma_1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ und $\sigma_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$. Beweis: Sei $U := \langle \sigma_1, \sigma_2 \rangle \leqslant G$. Wie in Beispiel 3.9 gilt $o(\sigma_1) = o(\sigma_2) = 2$. Wir berechnen $\sigma_1 \circ \sigma_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right) = \pi$ und $o(\pi) = 3$. Wegen $\sigma_1 \in U$ und $\pi \in U$ ist $|U|$ durch 2 und durch 3 teilbar, also durch 6. Also muss $U = G$ gelten.

(b) Sei $G = Q_8$ die Quaternionengruppe in Beispiel 3.10. Dann gilt $G = \langle I, J \rangle$. Denn sei $U := \langle I, J \rangle$. Es gilt nun $-E = I^2 \in U$, $K = I \cdot J \in U$, also schließlich $\pm I, \pm J, \pm K \in U$.

(c) Sei $S = \{g_1, \ldots, g_n\} \subseteq G$ und es gelte $g_i g_j = g_j g_i$ für alle i, j. Dann kann man Faktoren in Produkten der g_i beliebig vertauschen. Also folgt sofort dass $\langle S \rangle$ abelsch ist und es gilt $\langle S \rangle = \{g_1^{m_1} \cdots g_n^{m_n} \mid m_i \in \mathbb{Z}$ für $1 \leqslant i \leqslant n\}$.

Beispiel 6.3. Die Gruppe G heißt eine ***Diedergruppe***, wenn G von 2 Elementen der Ordnung 2 erzeugt wird. Es ist also $G = \langle s, t\rangle$ mit $s \neq t$, $s \neq 1$, $t \neq 1$ und $s^2 = t^2 = 1$. In den Übungen werden Sie zeigen: Ist $3 \leqslant m := o(st) < \infty$, so gilt $|G| = 2m$ und G ist nicht abelsch. Zum Beispiel ist $G = S_3$ eine Diedergruppe mit $m = 3$, denn die beiden Erzeuger σ_1, σ_2 im obigen Beispiel haben Ordnung 2. Die Quaternionengruppe ist keine Diedergruppe, denn es gibt in Q_8 überhaupt nur ein Element der Ordnung 2. In den Übungen haben Sie gesehen, dass die folgende Menge von Matrizen eine Diedergruppe der Ordnung 8 ist:

$$D_8 := \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Q}).$$

Beispiel 6.4. Sei $n \in \mathbb{N}$ und $G = S_n$ die symmetrische Gruppe. Wir führen einige nützliche Bezeichnungen ein. Seien $r \geqslant 1$ und $i_1, \ldots, i_r$ paarweise verschiedene Ziffern in $\{1, \ldots, n\}$. Dann definiere eine Permutation $\sigma \in S_n$ durch $\sigma(j) := j$ für $j \notin \{i_1, \ldots, i_r\}$, und

$$\sigma(i_1) := i_2, \qquad \sigma(i_2) := i_3, \qquad \ldots, \qquad \sigma(i_{r-1}) := i_r, \qquad \sigma(i_r) := i_1.$$

Eine solche Permutation heißt r-***Zykel*** (oder einfach Zykel); wir schreiben dann einfach $\sigma = (i_1\ i_2\ \ldots\ i_r) \in S_n$. Beachte: Die Reihenfolge der Ziffern $i_1, \ldots, i_r$ ist wichtig, aber es ist egal, wo man den Zykel beginnt; es gilt zum Beispiel auch $\sigma = (i_2\ \ldots\ i_r\ i_1)$, und so fort. Für $r = 1$ ist $\sigma = \mathrm{id}$. Für $r = 2$ ist $\sigma = (i_1\ i_2)$ die Permutation, die i_1 und i_2 vertauscht und alle anderen Ziffern festlässt; ein solcher 2-Zykel heißt auch ***Transposition***. Es gilt nun:

(a) Ist $r \geqslant 1$ und $\sigma \in S_n$ ein r-Zykel, so ist $o(\sigma) = r$.

Denn: Es gilt $\sigma^2(i_1) = \sigma(\sigma(i_1)) = \sigma(i_2) = i_3$ und dann analog $\sigma^d(i_1) = i_{d+1} \neq i_1$ für $1 \leqslant d < r$; also ist $o(\sigma) \geqslant r$. Wegen $\sigma^{r-1}(i_1) = i_r$ ist $\sigma^r(i_1) = i_1$. Analog findet man $\sigma^r(i_j) = i_j$ für $1 \leqslant j \leqslant r$, also $\sigma^r = \mathrm{id}$. Damit ist (a) gezeigt.

Sei nun auch $\tau = (j_1\ j_2\ \ldots\ j_s) \in S_n$ ein s-Zykel, wobei $s \geqslant 1$ und $j_1, \ldots, j_s$ paarweise verschieden sind. Dann heißen σ und τ disjunkte Zykeln, wenn $\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \varnothing$ gilt. Man sieht leicht, dass disjunkte Zykeln vertauschbar sind. Außerdem gilt:

(b) Jede Permutation $\pi \in S_n$ lässt sich als Produkt von disjunkten Zykeln schreiben[2].

Anstatt einen formalen Beweis zu geben, illustrieren wir dies mit einem Beispiel. Sei

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 5 & 1 & 2 & 7 & 6 \end{pmatrix} \in S_8 \qquad \rightsquigarrow \qquad \pi = (1\ 3\ 4\ 5) \circ (2\ 8\ 6) \circ (7).$$

Dazu beginnt man mit der Ziffer 1 und wendet wiederholt π darauf an, bis man wieder 1 erhält, also $1 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$. (Beachte: Wegen $o(\pi) < \infty$ muss es ein $d \geqslant 1$ mit $\pi^d(1) = 1$ geben.) Dies definiert den ersten Zykel $(1\ 3\ 4\ 5)$. Dann verfährt man genauso mit

[2] Für einen formalen Beweis der Zykel-Zerlegung siehe zum Beispiel §9.1 im Buch von Karpfinger–Meyberg. Auf diese Weise werden Permutationen auch in einem Computer-Algebra-System, z.B. GAP, dargestellt.

der kleinsten Ziffer, die nicht in diesem Zykel vorkommt, in diesem Fall also 2. Man erhält $2 \mapsto 8 \mapsto 6 \mapsto 2$; dies definiert den zweiten Zykel (2 8 6). Die kleinste Ziffer, die noch nicht in diesen beiden Zykeln vorkommt, ist 7. Nun erhält man $7 \mapsto 7$, also einen 1-Zykel, d.h., die Identität, die man dann auch in der Produktdarstellung weglassen kann. Weiterhin gilt:

(c) Ist $r \geqslant 1$ und $\sigma \in S_n$ ein r-Zykel, so ist σ ein Produkt von $r-1$ Transpositionen.

Denn es ist $\sigma = (i_1\ i_2) \circ (i_2\ i_3) \circ \cdots \circ (i_{r-1}\ i_r)$, wie man sofort verifiziert (indem man beide Seiten auf eine beliebige Ziffer $j \in \{1, \ldots, n\}$ anwendet). Zum Beispiel ist (1 3 4 5) = (1 3) ∘ (3 4) ∘ (4 5) und (2 8 6) = (2 8) ∘ (8 6), wobei (8 6) = (6 8). Für obiges Element $\pi \in S_8$ erhalten wir also $\pi = (1\ 3) \circ (3\ 4) \circ (4\ 5) \circ (2\ 8) \circ (6\ 8)$. Oder allgemein:

Satz 6.5. *Es gilt* $S_n = \langle (i\ j) \mid 1 \leqslant i < j \leqslant n \rangle$*, d.h.,* S_n *wird von Transpositionen erzeugt.*

Beweis. Sei $\pi \in S_n$ beliebig. Wie oben beschrieben ist $\pi = \pi_1 \circ \cdots \circ \pi_k$ mit disjunkten Zykeln $\pi_1, \ldots, \pi_k$. Weiterhin ist jedes π_j ein Produkt von Transpositionen, also insgesamt π ein Produkt von Transpositionen und damit $\pi \in \langle (i\ j) \mid 1 \leqslant i < j \leqslant n \rangle$. □

Ab hier Woche 4

Index