Algebra: Gruppen, Ringe, Körper

Skript zur Vorlesung im Wintersemester 2023/24

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

Dieses Skript zur Vorlesung Algebra (V4Ü2, 14-15 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. im Stuvus-Kopierlädle.)

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 §**??**; 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, September 2023

Inhaltsverzeichnis

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**.

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 §??).

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: $\quad a \equiv b \bmod m \quad$ 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: $\quad \overline{1}^{-1} = \overline{1}, \quad \overline{2}^{-1} = \overline{3}, \quad \overline{3}^{-1} = \overline{2}, \quad \overline{4}^{-1} = \overline{4}.$

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

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 $\mathbb{Z}/(m)$.

Ab hier Woche 2

INDEX