1 Algebraische Grundlagen

Wir setzen hier voraus, dass die Leser und Leserinnen mit den Sprech- und Bezeichnungsweisen der Mengenlehre und dem Abbildungsbegriff hinreichend vertraut sind. Wir sind nicht der Meinung, dass die Vorlesung „Lineare Algebra“ dazu benutzt werden sollte, Allgemeinheiten über algebraische Strukturen wie z. B. allgemeine Struktursätze in aller Ausführlichkeit von Grund auf zu behandeln. Allerdings ist der Gruppen- und Körperbegriff für den Aufbau der linearen Algebra fundamental, und deswegen beginnen wir das Buch mit einigen Fragen zu den grundlegenden Eigenschaften des Gruppen- und Körperbegriffs.

1.1 Der Begriff der Gruppe

Gruppen spielen nicht nur in der Linearen Algebra eine zentrale Rolle (z. B. ist ein Vektorraum insbesondere auch eine abelsche Gruppe bezüglich der Addition), sondern besitzen auch zahlreiche Anwendungen in außermathematischen Bereichen wie der Chemie („kristallografische Gruppe“) oder in der Physik (etwa bei der Klassifikation der Elementarteilchen). Die Schlagkraft der axiomatischen Methode bei der Einführung dieser Begriffe wird sich an vielen Beispielen zeigen.

Frage 1 Was versteht man unter einer **Gruppe**? Wann heißt eine Gruppe **abelsch** bzw. **kommutativ**?

Antwort: Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung „$*$“, d. h. einer Abbildung $*\colon G \times G \to G$, für die die folgenden Axiome gelten

(G1) *(Assoziativität)* Für alle $a, b, c \in G$ gilt

$$(a * b) * c = a * (b * c).$$

(G2) *(Existenz neutraler Elemente)* Es gibt ein $e \in G$, so dass für alle $a \in G$ gilt

$$e * a = a.$$

e heißt *neutrales* Element von G.

(G3) *(Existenz inverser Elemente)* Zu jedem $a \in G$ gibt es ein $\widetilde{a} \in G$ mit

$$\widetilde{a} * a = e,$$

wobei e das neutrale Element bezeichnet. $\widetilde{a}$ heißt in diesem Fall das zu a **inverse Element**.

Eine Gruppe $(G, *)$ heißt **abelsch** bzw. **kommutativ**, wenn zusätzlich $a*b = b*a$ für jedes $a, b \in G$ gilt. ⧫

Frage 2 Warum gilt für jede Gruppe $(G, *)$ mit neutralem Element e

$$e * a = a \Longrightarrow a * e = a \qquad \text{für alle } a \in G$$

sowie

$$\widetilde{a} * a = e \Longrightarrow a * \widetilde{a} = e \qquad \text{für alle } a \in G?$$

Mit anderen Worten, warum ist ein *linksneutrales* Element in jeder Gruppe G stets auch *rechtsneutral* und ein *linksinverses* Element zu $a \in G$ stets auch *rechtsinvers*?

Antwort: Zu $\widetilde{a}$ gibt es nach G3 ein linksinverses Element $\widetilde{\widetilde{a}}$. Damit gilt

$$a\widetilde{a} = e\,(a\widetilde{a}) = \left(\widetilde{\widetilde{a}}\widetilde{a}\right)(a\widetilde{a}) = \widetilde{\widetilde{a}}\,(\widetilde{a}\,(a\widetilde{a})) = \widetilde{\widetilde{a}}\,((\widetilde{a}a)\,\widetilde{a}) = \widetilde{\widetilde{a}}\,(e\widetilde{a}) = \widetilde{\widetilde{a}}\widetilde{a} = e.$$

Das beantwortet den zweiten Teil der Frage. Der erste folgt damit aus

$$a * e = a * (\widetilde{a} * a) = (a * \widetilde{a}) * a = e * a = a. \qquad \blacklozenge$$

Frage 3 Warum ist das neutrale Element e und das zu $a \in G$ inverse Element $\widetilde{a}$ eindeutig bestimmt, so dass man also von *dem* neutralen und *dem* zu $a \in G$ inversen Element sprechen kann?

Antwort: Ist e' ein (eventuell von e unterschiedenes) neutrales Element, so folgt mit der Antwort zur vorigen Frage

$$e' * e = e \quad \text{sowie} \quad e' * e = e',$$

also $e' = e$.

Ist $\widetilde{a}'$ ein (eventuell von a verschiedenes) inverses Element zu a, so gilt

$$\widetilde{a}' = \widetilde{a}' * e = \widetilde{a}' * (a * \widetilde{a}) = (\widetilde{a}' * a) * \widetilde{a} = e * \widetilde{a} = \widetilde{a}. \qquad \blacklozenge$$

Frage 4 Warum ist eine nichtleere Menge G mit einer assoziativen Verknüpfung $*$ genau dann eine Gruppe, wenn es zu je zwei Elementen $a, b \in G$ ein $x \in G$ und ein $y \in G$ gibt mit

$$x * a = b \qquad \text{und} \qquad a * y = b?$$

Antwort: Aus der ersten Gleichung erhält man für beliebiges $a \in G$ ein $e \in G$ mit $e * a = a$. Für jedes andere $b \in G$ gilt dann

$$e * b = e * (a * y) = (e * a) * y = a * y = b,$$

also ist e ein neutrales Element in G. Durch Lösen der Gleichung $x * a = e$ erhält man das zu a inverse Element. Dieses existiert also für jedes $a \in G$, und folglich ist G eine Gruppe. $\blacklozenge$

Frage 5 Sei G eine Gruppe und seien $a, b \in G$. Können Sie die folgenden Rechenregeln beweisen:

$$(a^{-1})^{-1} = a \qquad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}?$$

(Wir lassen an dieser Stelle die bisher gebrauchten Notationen hinter uns und benutzen in Zukunft der Übersichtlichkeit wegen bei der Untersuchung allgemeiner Gruppen die für multiplikative Strukturen gängigen Bezeichnungen. D. h., a^{-1} bezeichnet das zu a inverse Element, und für das Verknüpfungssymbol verwenden wir das Multiplikationszeichen, das gegebenenfalls auch unterdrückt werden kann.)

Antwort: Es ist

$$(a^{-1})^{-1} = (a^{-1})^{-1} \cdot e = (a^{-1})^{-1} \cdot (a^{-1} \cdot a) = ((a^{-1})^{-1} \cdot a^{-1}) \cdot a = e \cdot a = a.$$

Das beweist die erste Gleichung, die zweite folgt aus

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e. \qquad \blacklozenge$$

Frage 6 Können Sie Beispiele für abelsche und nicht-abelsche Gruppen angeben?

Antwort: (a) Die **ganzen Zahlen** $\mathbb{Z}$ bilden bezüglich der Addition eine abelsche Gruppe mit unendlich vielen Elementen.

(b) Ist K ein beliebiger **Körper**, so ist $(K, +)$ eine additive abelsche Gruppe und $(K^*, \cdot)$ eine multiplikative abelsche Gruppe. Dabei ist $K^* := K \setminus \{0\}$, wobei 0 das neutrale Element bezüglich der Addition bezeichnet.

(c) Jeder **Vektorraum** ist bezüglich der Addition von Vektoren eine abelsche Gruppe.

(d) Für ein $n > 0$ und $r \in \mathbb{Z}$ betrachte man die Menge

$$r + n\mathbb{Z} := \{r + n \cdot a \,;\, a \in \mathbb{Z}\} \subset \mathbb{Z},$$

die sogenannte *Restklasse von r modulo n*. Es gilt $r + n\mathbb{Z} = q + n\mathbb{Z}$ genau dann, wenn $r - q$ durch n teilbar ist bzw. wenn für r und q bei der ganzzahligen Division durch n derselbe Rest übrig bleibt. Daher gibt es genau n verschiedene Restklassen modulo n, nämlich

$$n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}.$$

Mit $\mathbb{Z}/n\mathbb{Z}$ bzw. $\mathbb{Z}_n$ bezeichnet man die Menge dieser n Restklassen. Diese sind paarweise disjunkt, und ihre Vereinigung ist $\mathbb{Z}$. Somit liegt jede ganze Zahl a in genau einer der n Restklassen. Die Abbildung $\overline{}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ordne jedem $a \in \mathbb{Z}$ seine Restklasse modulo n zu. Dann ist durch

$$\overline{a} \oplus \overline{b} := \overline{a + b}$$

auf $\mathbb{Z}/n\mathbb{Z}$ eine Verknüpfung definiert. Diese ist assoziativ und kommutativ, da die übliche Addition auf $\mathbb{Z}$ dies ist, ferner ist $\overline{0}$ ein neutrales Element in $\mathbb{Z}/n\mathbb{Z}$, und das zu $\overline{a}$ inverse Element ist durch $\overline{-a}$ gegeben. $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ ist damit eine additive abelsche Gruppe, die **Restklassengruppe modulo** n.

(e) Für eine Menge X sei $\mathrm{Sym}(X)$ die Menge aller bijektiven Selbstabbildungen $X \to X$. $\mathrm{Sym}(X)$ bildet bezüglich der Verkettung von Abbildungen eine Gruppe, die allerdings nicht kommutativ ist, wenn X mehr als 2 Elemente hat. Die Assoziativität ist automatisch erfüllt, da die Hintereinanderausführung von Abbildungen assoziativ ist, mit der identischen Abbildung $x \mapsto x$ enthält $\mathrm{Sym}(X)$ ein neutrales Element, und aufgrund der Bijektivität ist mit F auch die Umkehrabbildung F^{-1}, also das zu F inverse Element, in $\mathrm{Sym}(X)$ enthalten. $(\mathrm{Sym}(X), \circ)$ ist damit eine Gruppe, die sogenannte **symmetrische Gruppe auf** X.

Ist speziell $X = \{1, 2, \ldots, n\}$, so schreibt man S_n für $\mathrm{Sym}(X)$. S_n besteht aus allen Permutationen der ersten n natürlichen Zahlen, und daher nennt man S_n auch **Permutationsgruppe**.

(f) Zu einem Körper K bezeichnet $\mathrm{GL}(n, K)$ (**General Linear Group**) die Menge aller $n \times n$-Matrizen in K mit nichtverschwindender Determinante. $\mathrm{GL}_n(K)$ bildet bezüglich der Matrizenmultiplikation eine nicht-abelsche Gruppe (s. Frage 191).

(g) Ist K ein Körper und V ein K-Vektorraum, dann lässt sich unabhängig von einer Basis die Menge $\mathrm{Aut}(V)$ aller bijektiven K-linearen Selbstabbildungen (*Automorphismen*) auf V definieren. $\mathrm{Aut}(V)$ ist dann bezüglich der Hintereinanderausführung von Abbildungen eine Gruppe, die **Automorphismengruppe** von V. Hat V die Dimension n, dann existiert bezüglich der Wahl einer Basis in V ein Isomorphismus $\mathrm{Aut}(V) \to \mathrm{GL}_n(K)$, der einem Automorphismus $V \to V$ seine Matrix bezüglich der Basis zuordnet.

(h) Zu zwei Gruppen $(G, *_G)$ und $(H, *_H)$ ist das **direkte Produkt**

$$G \times H := \{(g, h)\ ;\ g \in G, h \in H\}$$

zusammen mit der komponentenweise erklärten Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 *_G g_2, h_1 *_H h_2)$$

ebenfalls eine Gruppe. Das neutrale Element ist gegeben durch (e_G, e_H), das zu (g, h) inverse Element durch (g^{-1}, h^{-1}). ♦

Frage 7 Sei M eine beliebige nichtleere Menge. Warum ist die Menge $\mathrm{Abb}(M, M)$ der Abbildungen $M \longrightarrow M$ bezüglich der Hintereinanderausführung von Abbildungen keine Gruppe?

Antwort: Die Abbildungen aus $\mathrm{Abb}(M, M)$ sind in der Regel nicht bijektiv und besitzen in diesen Fällen keine Umkehrabbildung $M \to M$, also kein inverses Element in $\mathrm{Abb}(M, M)$. ♦

Frage 8 Was besagt die **Kürzungsregel** in einer Gruppe G?

Antwort: Für $a, b, c \in G$ gilt:

$$c \cdot a = c \cdot b \Longrightarrow a = b, \qquad a \cdot c = b \cdot c \Longrightarrow a = b.$$

Die beiden Regeln erhält man, wenn man beide Seiten der jeweiligen Gleichung links- bzw. rechtsseitig mit c^{-1} verknüpft. ♦

Frage 9 Ist $G = \{a_1 = e, a_2 \ldots, a_n\}$ eine Menge mit n Elementen, wie kann man dann auf übersichtliche Weise eine Verknüpfung auf G angeben?

Antwort: Die Gruppenstruktur lässt sich in einer sogenannten *Verknüpfungstafel* darstellen, in der alle n^2 Verknüpfungen $a_i \cdot a_j$ in einem quadratischen Schema eingetragen sind.

$\cdot$	e	a_2	$\cdots$	a_n
e	ee	ea_2	$\cdots$	ea_n
a_2	a_2e	a_2a_2	$\cdots$	a_2a_n
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	a_ne	a_na_2	$\cdots$	a_na_n

♦

Frage 10 Wie kann man aus einer Verknüpfungstafel ablesen, ob eine Menge $G = \{a_1, \ldots, a_n\}$ eine Gruppe ist?

Antwort: Es gilt:

- G enthält ein neutrales Element $e = a_k$ genau dann, wenn die k-te Zeile und die k-te Spalte einfach die Anordnung der Gruppenelemente wiederholen.
- G enthält inverse Elemente genau dann, wenn die Anordnung in jeder Zeile und Spalte aus einer Permutation der Gruppenelemente hervorgeht.
- Wegen $a^{-1}a = aa^{-1} = e$ muss für eine Gruppe zusätzlich gelten, dass die neutralen Elemente in der Gruppentafel symmetrisch zur Hauptdiagonalen $i = j$ liegen. Bei der Verknüpfungstafel einer *abelschen* Gruppe liegen alle Einträge symmetrisch zur Hauptdiagonalen.

Die Gültigkeit der Axiome $G2$ und $G3$ spiegelt sich damit unmittelbar in den offen zu Tage liegenden Eigenschaften der Verknüpfungstafel wider, und lässt sich dementsprechend leicht überprüfen. Das gilt allerdings nicht für das Assoziativgesetz. Um dieses zu verifizieren, müssen n^3 Gleichungen überprüft werden. ♦

Frage 11 Können Sie die Verknüpfungstafeln für $G := \mathbb{Z}_5 := \mathbb{Z}/5\mathbb{Z}$ und für S_3 angeben?

Antwort: Die Verknüpfungstafel der Restklassengruppe $\mathbb{Z}/5\mathbb{Z}$ lautet

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Hier handelt es sich um eine abelsche Gruppe.

Die Gruppe S_3 besteht aus den sechs Elementen (Permutationen)

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad \sigma_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
$$\sigma_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \sigma_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \quad \sigma_6 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

Dabei stehen in der unteren Zeile die Bilder der Zahlen $1, 2, 3$ unter der jeweiligen Permutation.

Man erhält damit folgende Verknüpfungstafel für die Gruppe S_3

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_5	σ_6	σ_4
σ_3	σ_3	σ_1	σ_2	σ_6	σ_4	σ_5
σ_4	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2
σ_5	σ_5	σ_4	σ_6	σ_2	σ_1	σ_3
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

Da die Verknüpfungstafel nicht symmetrisch zur Hauptdiagonalen ist, handelt es sich bei S_3 um keine abelsche Gruppe. ♦

Frage 12 Warum ist eine Gruppe G mit neutralem Element e abelsch, wenn $a^2 = e$ für jedes $a \in G$ gilt? Können Sie ein Beispiel für eine solche Gruppe angeben?

Antwort: Für beliebige Elemente $a, b \in G$ gilt unter diesen Voraussetzungen $a = a^{-1}$, $b = b^{-1}$ sowie $ab = (ab)^{-1}$, und daraus folgt insgesamt

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Das einfachste Beispiel einer Gruppe mit dieser Eigenschaft ist $\mathbb{Z}/2\mathbb{Z}$. Davon ausgehend lassen sich durch Bildung direkter Produkte

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$$

Gruppen mit Ordnung 2^n angeben, bei denen jedes Element zu sich selbst invers ist. ⧫

Frage 13 Warum ist jede Gruppe mit vier Elementen abelsch?

Antwort: Seien a und b mit $a \neq b$ zwei Elemente aus G. Da jedes Element mit seinem Inversen und das neutrale Element mit jedem anderen Element kommutiert, bleibt nur der Fall $ab = c$ mit $a \neq e$ und $b \neq e$ sowie $c \notin \{e, a, b\}$ zu untersuchen. In diesem Fall muss aber auch $ba = c$ gelten, denn aus $ba = a$ bzw. $ba = b$ bzw. $ba = e$ würde $b = e$ bzw. $a = e$ bzw. $b = a^{-1}$ folgen, und das hatten wir bereits ausgeschlossen. ⧫

Frage 14 Was versteht man unter der **Ordnung** einer endlichen Gruppe?

Antwort: Die Ordnung von G ist die Kardinalität der Menge G und wird mit $\operatorname{ord} G$ oder $|G|$ bezeichnet. Ist $|G|$ endlich, so ist die Ordnung von G also die Anzahl der Elemente in G. Im anderen Fall hat G unendliche Ordnung.

Frage 15 Welche Ordnung hat die Gruppe S_n?

Antwort: Eine Permutation einer n-elementigen Menge lässt sich auf $n!$ verschiedene Arten festlegen: Für das Bild des ersten Elements hat man n Möglichkeiten, für das zweite noch $n-1$ Möglichkeiten usw., bis schließlich für das Bild des letzten Elements nur noch eine Möglichkeit übrig bleibt. Die Gruppe S_n hat somit die Ordnung $n!$. ⧫

Frage 16 Wie ist die **Ordnung** eines Elements a einer Gruppe G definiert?

Antwort: Definiert man für $a \in G$ und $n \in \mathbb{Z}$

$$a^n := \begin{cases} \overbrace{aa\cdots a}^{n\text{-mal}} & \text{für } n > 0 \\ e & \text{für } n = 0 \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n\text{-mal}} & \text{für } n < 0 \,. \end{cases},$$

dann gelten die üblichen „Potenzregeln“

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn},$$

und aus diesen folgt

$$\{n \in \mathbb{Z} \,;\, a^n = e\} = k\mathbb{Z}$$

für eine nichtnegative ganze Zahl k. Für $k > 0$ hat a eine *endliche Ordnung* in G. Die Zahl k ist in diesem Fall die *Ordnung* von a in G. Im Fall $k = 0$ sagt man, a hat *unendliche Ordnung* in G.

Besitzt a eine endliche Ordnung in G, so ist die Ordnung von a also die kleinste natürliche Zahl n, für die $a^n = e$ gilt. Gibt es keine natürliche Zahl mit dieser Eigenschaft, dann hat a unendliche Ordnung in G. ♦

Frage 17 Können Sie für die Gruppe S_3 jeweils die Ordnungen der sechs Elemente angeben?

Antwort: Das neutrale Element σ_1 ist wie in jeder Gruppe das einzige Element mit der Ordnung 1. Die Elemente σ_2 und σ_3 besitzen beide die Ordnung 3, und σ_4, σ_5 und σ_6 besitzen jeweils die Ordnung 2. ♦

Frage 18 Wann heißt eine Gruppe **zyklisch**?

Antwort: Eine Gruppe G heißt *zyklisch*, wenn sie von einem einzigen Element $a \in G$ erzeugt ist. D. h., für jedes $g \in G$ gibt es eine ganze Zahl m mit $g = a^m$. Im Fall einer endlichen Gruppe der Ordnung n gilt dann $G = \{e, a, a^2, \ldots, a^{n-1}\}$. Ist $|G|$ unendlich, dann gilt $G = \{e, a, a^{-1}, a^2, a^{-2}, \ldots\}$. ♦

Frage 19 Warum ist jede zyklische Gruppe abelsch?

Antwort: Sei g das erzeugende Element von G. Für alle $a, b \in G$ gibt es dann $m, n \in \mathbb{Z}$ mit $a = g^m$ und $b = g^n$. Es folgt

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba.$$ ♦

Frage 20 Können Sie jeweils ein Beispiel einer endlichen und einer nichtendlichen zyklischen Gruppe angeben?

Antwort: Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung n, erzeugt von der Restklasse $\overline{1}$.

Die ganzen Zahlen sind eine zyklische Gruppe, deren Ordnung nichtendlich ist. Das erzeugende Element ist die 1.

Mit diesen beiden Beispielen sind bis auf Isomorphie schon alle zyklischen Gruppen mit endlicher bzw. nichtendlicher Ordnung aufgezählt. Eine zyklische Gruppe $G = \{e, a^1, a^2, \ldots, a^n\}$ der Ordnung n ist nämlich vermöge der Abbildung

$$\mathbb{Z}/n\mathbb{Z} \to G, \qquad \overline{m} \mapsto a^m$$

isomorph zu $\mathbb{Z}/n\mathbb{Z}$, und für eine nichtendliche Gruppe $H = \{e, h^1, h^{-1}, h^2, h^{-2}, \ldots\}$ ist die Abbildung

$$\mathbb{Z} \to h, \qquad m \mapsto h^m$$

ein Isomorphismus. ♦

1.2 Abbildungen zwischen Gruppen, Untergruppen

Für zwei Gruppen G und G' sind vor allem diejenigen Abbildungen $F\colon G \longrightarrow G'$ von Interesse, durch die nicht nur die Elemente, sondern auch die Gruppenstruktur von G in bestimmter Weise auf diejenige von G' abgebildet wird, sodass gruppentheoretische Relationen zwischen zwei Elementen $a, b \in G$ auch zwischen den Bildern von a und b in G' bestehen. Abbildungen mit dieser Eigenschaft nennt man *Homomorphismen*.

Frage 21 Was versteht man unter einem **Homomorphismus** zwischen zwei Gruppen $(G, *)$ und $(H, \diamond)$? Wann heißt ein Homomorphismus

(a) **Monomorphismus**,
(b) **Epimorphismus**,
(c) **Isomorphismus**,
(d) **Endomorphismus**,
(e) **Automorphismus**?

Antwort: Eine Abbildung $F : G \longrightarrow H$ heißt *Homorphismus*, wenn für alle $a, b \in G$ gilt:

$$F(a * b) = F(a) \diamond F(b).$$

Die anderen vier Begriffe beschreiben spezielle Homomorphismen. Ein Homomorphismus F heißt

(a) *Monomorphismus,* falls F injektiv ist,
(b) *Epimorphismus,* falls F surjektiv ist,
(c) *Isomorphismus,* falls F bijektiv ist,
(d) *Endomorphismus,* falls F ein Homomorphismus von G in sich selbst ist,
(e) *Automorphismus,* falls F ein Isomorphismus von G in sich selbst ist. ⧫

Frage 22 Wann heißen zwei Gruppen **isomorph**?

Antwort: Zwei Gruppen G und H heißen *isomorph*, geschrieben $G \simeq H$, wenn es einen Isomorphismus von G nach H gibt. ⧫

Frage 23 Können Sie einige Beispiele von Homomorphismen nennen?

Antwort: (a) Für zwei Gruppen G und H ist die Abbildung $G \longrightarrow H$, die jedes $g \in G$ auf das neutrale Element in H abbildet, stets ein Homomorphismus.

(b) Ist G eine Gruppe und $H \subset G$ eine Untergruppe, dann ist die identische Abbildung $H \longrightarrow G$, $g \longmapsto g$ ein Homomorphismus.

(c) Die Abbildung

$$\overline{}\colon (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, \oplus) \qquad n \mapsto \overline{n}$$

ist wegen $\overline{n+m} = \overline{n} \oplus \overline{m}$ ein Homomorphismus. Dies ist ein Beispiel eines allgemeineren Prinzips, das in Frage 39 genauer erläutert wird: Ist G eine Gruppe und N ein Normalteiler in G, dann ist die sogenannte *kanonische Projektion*

$$\pi\colon G \longrightarrow G/N, \qquad g \mapsto gN$$

von G in die Menge G/N der Linksnebenklassen von N in G ein Gruppenhomomorphismus.

(d) Die Exponentialfunktion $\exp\colon \mathbb{R} \longrightarrow \mathbb{R}_+$ ist wegen

$$\exp(x+y) = \exp(x)\exp(y)$$

ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{R}, +)$ in die multiplikative Gruppe $(\mathbb{R}_+, \cdot)$. Da die Exponentialfunktion die reellen Zahlen bijektiv auf $\mathbb{R}_+$ abbildet, handelt es sich dabei um einen Isomorphismus.

(e) Die komplexe Konjugation

$$\overline{\ }\colon \mathbb{C} \longrightarrow \mathbb{C}, \qquad a + \mathrm{i}b \mapsto a - \mathrm{i}b$$

ist offensichtlich ein Automorphismus der additiven Gruppe $, +)$. Wegen

$$\overline{(a+\mathrm{i}b)\cdot(c+\mathrm{i}d)} = (ac-bd) - \mathrm{i}(ad+bc) = \overline{(a+\mathrm{i}b)}\cdot\overline{(c+\mathrm{i}d)}$$

handelt es sich aber auch um einen Automorphismus der multiplikativen Gruppe $(\mathbb{C}^*, \cdot)$. Die komplexe Konjugation beschreibt also einen *Körperautomorphismus* von $\mathbb{C}$.

(f) Die komplexe Exponentialfunktion $\exp\colon \mathbb{C} \longrightarrow \mathbb{C}$ ist ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{C}, +)$ in die multiplikative Gruppe $(\mathbb{C}^*, \cdot)$. Dieser ist surjektiv, aber wegen $\exp(z) = \exp(z + 2k\pi\mathrm{i})$ für alle $k \in \mathbb{Z}$ nicht injektiv.

(g) Jede lineare Abbildung $V \longrightarrow W$ zwischen zwei Vektorräumen V und W ist insbesondere ein Homomorphismus zwischen den Gruppen $(V, +)$ und $(W, *)$. ♦

Frage 24 Warum gilt für einen Gruppenhomomorphismus $F\colon (G, *) \longrightarrow (G', \diamond)$ stets

(a) $F(e) = e'$ für die neutralen Elemente $e \in G$ und $e' \in G'$ sowie

(b) $F(a^{-1}) = \big(F(a)\big)^{-1}$ für alle $a \in G$?

Antwort: Für beliebiges $a \in G$ ist

$$F(a) = F(a * e) = F(a) \diamond F(e),$$

also $F(e) = e'$. Das zeigt (a). Damit gilt dann

$$e' = F(e) = F(a * a^{-1}) = F(a) \diamond F(a^{-1}),$$

und daraus folgt (b). ♦

Frage 25 Was versteht man unter dem **Kern** eines Homomorphismus?

Antwort: Der Kern eines Homomorphismus $F\colon G \longrightarrow G'$, geschrieben $\ker F$, ist die Menge aller $a \in G$, die durch F auf das neutrale Element in G' abgebildet werden. Es ist also

$$\ker(F) := \{a \in G\ ;\ F(a) = e'\}.$$ ⧫

Frage 26 Warum ist ein Homomorphismus $F : (G, *) \longrightarrow (G', \diamond)$ genau dann injektiv, wenn $\ker F = \{e\}$ mit dem neutralen Element $e \in G$ gilt?

Antwort: Sei zunächst $\ker F = \{e\}$. Für $a, b \in G$ mit $F(a) = F(b)$ gilt dann

$$F(a * b^{-1}) = F(a) \diamond F(b^{-1}) = F(a) \diamond \big(F(b)\big)^{-1} = e',$$

also $a * b^{-1} \in \ker(F)$ und damit wegen der Voraussetzung $a = b$. Das heißt, F ist injektiv.

Die andere Richtung folgt aus $F(e) = e'$. Ist F injektiv, dann ist e das einzige Element, das auf e' abgebildet wird. ⧫

Frage 27 Warum ist die Zusammensetzung von Homomorphismen wieder ein Homomorphismus?

Antwort: Für Homomorphismen

$$F\colon (G, *) \longrightarrow (G', \diamond) \quad \text{und} \quad F'\colon (G', \diamond) \longrightarrow (G'', \bullet)$$

und Elemente $a, b \in G$ gilt

$$F' \circ F(a * b) = F'\big(F(a) \diamond F(b)\big) = F'\big(F(a)\big) \bullet F'\big(F(b)\big) = F' \circ F(a) \bullet F' \circ F(b).$$

Damit ist die Abbildung $F' \circ F\colon G \longrightarrow G''$ ein Homomorphismus. ⧫

Frage 28 Können Sie folgende Aussagen begründen?

(a) Die identische Abbildung $\mathrm{id}\colon G \longrightarrow G$ ist ein Isomorphismus.
(b) Ist $F\colon G \longrightarrow G'$ ein Isomorphismus, dann ist die (wohldefinierte) Umkehrabbildung $F^{-1}\colon G' \longrightarrow G$ ebenfalls ein Isomorphismus.
(c) Die Zusammensetzung von Isomorphismen ist wieder ein Isomorphismus.

Antwort: (a) Die identische Abbildung ist bijektiv und ferner wegen $\mathrm{id}(a + b) = a + b = \mathrm{id}(a) + \mathrm{id}(b)$ ein Homomorphismus.

(b) Als Umkehrabbildung einer bijektiven Abbildung ist F^{-1} ebenfalls bijektiv. Sind ferner a', b' beliebige Elemente aus G', dann gibt es $a, b \in G$ mit $F(a) = a'$ und $F(b) = b'$ und es gilt:

$$F^{-1}(a' \cdot b') = F^{-1}\big(F(a) \cdot F(b)\big) = F^{-1}\big(F(a \cdot b)\big) = a \cdot b = F^{-1}(a') \cdot F^{-1}(b'),$$

also ist F^{-1} ein Homomorphismus.

(c) Dies folgt aus dem Ergebnis zu Frage 27 zusammen mit der Tatsache, dass die Verkettung bijektiver Abbildungen wieder bijektiv ist. ⧫

Frage 29 Wann heißt eine Teilmenge $H \subset G$ einer Gruppe $(G, \cdot)$ **Untergruppe**?

Antwort: $H \subset G$ ist eine *Untergruppe von* G, wenn die Elemente aus H bezüglich der Verknüpfung „$\cdot$“ ebenfalls eine Gruppe bilden. ⧫

Frage 30 Was besagt das **Untergruppenkriterium**?

Antwort: Das Kriterium besagt:

Eine nichtleere Teilmenge $U \subset G$ einer Gruppe G ist eine Untergruppe von G genau dann, wenn gilt

(i) $a \in U \Longrightarrow a^{-1} \in U$
(ii) $a, b \in U \Longrightarrow ab \in U$.

Beweis: Dass jede Untergruppe U die beiden Bedingungen erfüllen muss, gilt definitionsgemäß. Umgekehrt folgt aus (i) und (ii) zusammen $e \in U$. Da das Assoziativgesetz in ganz G und somit insbesondere in U gilt, erfüllt U folglich alle drei Gruppenaxiome. ⧫

Frage 31 Ist $F : G \longrightarrow G'$ ein Gruppenhomomorphismus, warum tragen $\ker F$ und das Bild $\operatorname{im} F$ von F dann in natürlicher Weise eine Gruppenstruktur?

Antwort: Für $a, b \in \ker F$ gilt $F(ab) = F(a)F(b) = ee = e$, also $ab \in \ker F$. Ferner gilt wegen $F(a^{-1}) = \big(F(a)\big)^{-1}$, dass mit a auch a^{-1} in $\ker F$ enthalten ist. Der Kern von F ist also nach dem Kriterium aus Frage 30 eine Untergruppe von G.

Für $a', b' \in \operatorname{im} F$ gibt es $a, b \in G$ mit $F(a) = a'$ und $F(b) = b'$. Somit gilt $F(ab) = a'b'$, also $a'b' \in \operatorname{im} F$. Außerdem gilt $F(a^{-1}) = F(a)^{-1} = a'^{-1}$, also ist mit a' auch a'^{-1} in $\operatorname{im} F$ enthalten und $\operatorname{im} F$ daher eine Untergruppe von G'. ⧫

Frage 32 Was versteht man unter einer **Linksnebenklasse** von G bezüglich einer Untergruppe $H \subset G$? Was ist eine **Rechtsnebenklasse**?

Antwort: Für eine Unterguppe $H \subset G$ heißt die Menge

$$aH = \{ah \,;\, h \in H\}$$

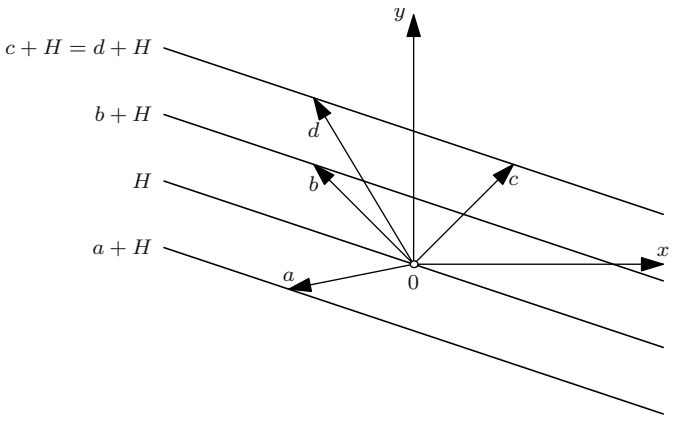
für $a \in G$ eine *Linksnebenklasse von H in G*. Entsprechend heißt

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

eine *Rechtsnebenklasse von H in G*.

Beispiel: Sei $G = (\mathbb{R}^2, +)$ und $H \subset G$ ein eindimensionaler Unterraum, d. h. eine Gerade durch den Ursprung. Dann ist H insbesondere eine Untergruppe von G. Für $v \in \mathbb{R}^2$ bezeichnet dann die Linksnebenklasse $v + H$ in geometrischer Hinsicht die zu H parallele Gerade im $\mathbb{R}^2$, die durch den Punkt $O + v$ verläuft.

Die Menge der Linksnebenklassen bezüglich H wird mit G/H bezeichnet. Die Rechtsnebenklassen bezeichnet man mit $G\backslash H$. Die Abbildung $g \longmapsto g^{-1}$ bildet jedes Element $ah \in aH$ auf $(ah)^{-1} = h^{-1}a^{-1} \in Ha^{-1}$ ab und vermittelt daher eine Bijektion zwischen G/H und $G\backslash H$, die aH auf Ha^{-1} abbildet.



Ist G abelsch, so sind Links- und Rechtsnebenklassen trivialerweise identisch. Das gilt im Allgemeinen allerdings nicht. Diejenigen Untergruppen H, für die $aH = Ha$ gilt, besitzen besonderes Interesse (vgl. Frage 39). ⧫

Frage 33 Wieso sind zwei Linksnebenklassen von H in G entweder disjunkt oder identisch?

Antwort: Es genügt, die folgende Implikation zu zeigen:

$$a \in bH \Longrightarrow aH = bH. \qquad (*)$$

Aus $a' \in aH \cap bH$ folgt dann nämlich sofort $a'H = aH = bH$.

Sei also $a \in bH$, dann gilt $a = bh_1$ und $b = ah_1^{-1}$ für ein $h_1 \in H$. Für ein beliebiges Element $c \in bH$ gibt es entsprechend ein $h_2 \in H$ mit $c = bh_2$, und daraus folgt $c = ah_1^{-1}h_2 \in aH$. Also gilt $bH \subset aH$. Gilt umgekehrt $c \in aH$, also $c = ah_3$ für ein $h_3 \in H$, dann folgt $c = bh_1h_3 \in bH$. Damit ist auch $aH \subset bH$ und insgesamt $(*)$ gezeigt. ⧫

Frage 34 Was versteht man unter dem **Index** einer Untergruppe H einer endlichen Gruppe G?

Antwort: Unter dem Index von H in G versteht man die Anzahl der Linksnebenklassen (und damit der Rechtsnebenklassen) von H in G. Man bezeichnet diese Zahl mit $(G : H)$. ⧫

Frage 35 Was besagt der **Satz von Lagrange**?

Antwort: Der Satz von Lagrange besagt:

Ist G eine endliche Untergruppe und $H \subset G$ eine Untergruppe, dann gilt

$$|G| = (G : H) \cdot |H|.$$

Der *Beweis* ergibt sich im Wesentlichen aus Antwort 33. Aus dieser folgt insbesondere, dass G die disjunkte Vereinigung der Linksnebenklassen von H in G ist. Da in jeder Linksnebenklasse aH genau $|H|$ Elemente liegen, folgt daraus schon der Satz von Lagrange. ⧫

Frage 36 Warum ist in einer endlichen Gruppe G die Ordnung einer Untergruppe H stets ein Teiler der Ordnung von G?

Antwort: Da $(G : H)$ eine natürliche Zahl ist, ergibt sich die Antwort als eine unmittelbare Konsequenz aus dem Satz von Lagrange. ⧫

Frage 37 Was besagt der **kleine Fermat'sche Satz**? Was besagt er im Spezialfall $G = (\mathbb{Z}/p\mathbb{Z})^*$, wo p eine Primzahl ist?

Antwort: Aus dem Satz von Lagrange erhält man als Spezialfall:

Die Ordnung eines Elements $a \in G$ ist ein Teiler der Gruppenordnung. Für jedes $a \in G$ gilt also

$$a^{|G|} = a^{m \cdot \operatorname{ord} a} = e^m = e.$$

Das ist der kleine Fermat'sche Satz in gruppentheoretischer Sprechweise.

Ist $G = (\mathbb{Z}/p\mathbb{Z})^*$, so gilt wegen $|G| = p - 1$ speziell $\overline{a}^{p-1} = \overline{1}$ für alle $\overline{a} \in G$ bzw.

$$a^{p-1} = 1 \pmod{p} \qquad \text{für alle } a \in \mathbb{Z},$$

So lautet der kleine Fermat'sche Satz in seiner klassischen zahlentheoretischen Formulierung. ⧫

Frage 38 Warum ist jede Gruppe von Primzahlordnung p zyklisch und damit abelsch?

Antwort: Nach dem Satz von Lagrange hat jedes Element aus G entweder die Ordnung 1 oder die Ordnung p. Jedes vom neutralen Element verschiedene Element aus G erzeugt daher die Gruppe G. ⧫

Frage 39 Was versteht man unter einem **Normalteiler** in G?

Antwort: Eine Untergruppe $N \subset G$ heißt *Normalteiler in* G, wenn gilt:

$$aN = Na \qquad \text{für alle } a \in G,$$

d. h., wenn die Links- und Rechtsnebenklassen von N in G übereinstimmen.

Frage 40 Aus welchem Grund spielen die Normalteiler in einer Gruppe eine ausgezeichnete Rolle?

Antwort: Ist N ein Normalteiler in G, dann lässt sich auf der Menge der Linksnebenklassen G/N von N in G eine Gruppenstruktur definieren, indem man für zwei Linksnebenklassen aN und bN deren Produkt durch

$$aN \cdot bN := abN \tag{$*$}$$

erklärt. Allerdings muss begründet werden, dass auf diese Weise tatsächlich eine Verknüpfung in der Menge der Linksnebenklassen von N in G gegeben ist. In der Definition $(*)$ werden nämlich Repräsentanten der vorkommenden Linksnebenklassen benutzt und es ist *a priori* nicht selbstverständlich, dass man bei der Wahl von anderen Repräsentanten derselben Klassen das gleiche Ergebnis bekommt. Es muss daher gezeigt werden, dass die Verknüpfung *wohldefiniert*, d. h. unabhängig von der Auswahl der Repräsentanten ist. Genau muss Folgendes gezeigt werden

$$\text{Aus } a'N = aN \text{ und } b'N = bN \text{ folgt stets } abN = a'b'N.$$

Seien also die beiden Voraussetzungen erfüllt. Dann gibt es Elemente $n_1, n_2 \in N$ mit $a = a'n_1$ und $b = b'n_2$, und daraus folgt

$$abN = ab'n_2N = ab'N = aNb' = a'n_2Nb' = a'Nb' = a'b'N.$$

Das zeigt die Wohldefiniertheit der Verknüpfung. Man beachte, dass hier zweimal von der Normalteilereigenschaft von N Gebrauch gemacht wurde. Diese Argumentation lässt sich daher nicht auf Links- oder Rechtsnebenklassen übertragen.

Die Gruppenstruktur von G/N ergibt sich nun leicht aus derjenigen von G. So überträgt sich die Assoziativität der Verknüpfung $(*)$ unmittelbar von G auf G/N. Die Verknüpfungsdefinition garantiert unmittelbar, dass mit aN und bN auch $aN \cdot bN$ eine Linknsnebenklasse von N in G ist. Ferner ist mit $eN = N$ ein neutrales Element in G/N gegeben und zu jeder Linksnebenklasse $aN \in G/N$ existiert mit $a^{-1}N$ ein inverses Element in G/N. Damit ist G/N eine Gruppe und die *kanonische Projektion*

$$\pi\colon G \longrightarrow G/N, \qquad a \mapsto aN$$

ein Gruppenhomomorphismus. ⧫

Frage 41 Ist der Kern eines Gruppenhomomorphismus $F: G \longrightarrow G'$ stets ein Normalteiler in G?

Antwort: Sei $b \in \ker F$. Dann gilt für jedes $a \in G$

$$F(aba^{-1}) = F(a)F(b)F(a^{-1}) = F(a)F(a^{-1}) = 1,$$

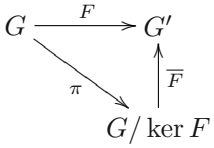
also $aba^{-1} \in \ker F$. Daraus folgt zunächst $a \cdot \ker F \cdot a^{-1} \subset \ker F$ und durch einen Mächtigkeitsvergleich der beiden Mengen dieser Inklusion anschließend $a \cdot \ker F \cdot a^{-1} = \ker F$, also $a \cdot \ker F = \ker F \cdot a$. Demnach ist $\ker F$ ein Normalteiler in G.

Die Aussage des folgenden Homomorphiesatzes impliziert, dass jeder Normalteiler in G sich als Kern eines Gruppenhomomorphismus realisieren lässt. ♦

Frage 42 Was besagt der **Homomorphiesatz** für Gruppen?

Antwort: Der Homomorphiesatz besagt:

Zu jedem Gruppenhomomorphismus $F: G \longrightarrow G'$ gibt es einen eindeutig bestimmten Homomorphismus $\overline{F}: G/\ker F \longrightarrow G'$, so dass das folgende Diagramm kommutiert.



Es gilt $\operatorname{im} F = \operatorname{im} \overline{F}$ *und* $\ker \overline{F} = \overline{0}$*, insbesondere ist* $\overline{F}$ *injektiv. Für surjektives* F *gilt also*

$$G' \simeq G/\ker F.$$

Beweis: Falls überhaupt eine Abbildung $\overline{F}$ mit diesen Eigenschaften existiert, dann gilt für alle $a \in G$:

$$\overline{F}(a \ker F) = F(a). \qquad (*)$$

Umgekehrt folgt die Existenz von $\overline{F}$, wenn man zeigen kann, dass die durch $(*)$ gegebene Abbildung wohldefiniert, also unabhängig von der Auswahl der Repräsentanten ist. Dazu muss gezeigt werden, dass aus $a \ker F = b \ker F$ stets $\overline{F}(a \ker F) = \overline{F}(b \ker F)$ folgt.

Sei also $a \ker F = b \ker F$, dann gilt $ab^{-1} \in \ker F$, also $F(ab^{-1}) = F(a)F^{-1}(b) = 1$, also $F(a) = F(b)$, und mit Definition $(*)$ folgt wie gewünscht $\overline{F}(a \ker F) = \overline{F}(b \ker F)$. Das zeigt, dass $\overline{F}$ durch $(*)$ wohldefiniert ist. Also existiert ein Homomorphismus mit den gesuchten Eigenschaften. Dieser ist eindeutig, weil er $(*)$ erfüllen muss.

Beispiel: Sei $\mathrm{GL}(n, K)$ die Gruppe der invertierbaren $n \times n$-Matrizen über einem Körper K. Die Determinantenabbildung

$$\det: \mathrm{GL}(n, K) \longrightarrow K^*$$

ist ein surjektiver Gruppenhomomorphismus (vgl. Frage 265) mit dem Kern $\mathrm{SL}(n,K)$ („Special Linear Group“: die Menge aller $n \times n$-Matrizen über K mit Determinante 1). Mit dem Homomorphiesatz schließt man

$$\mathrm{GL}(n,K)/\mathrm{SL}(n,K) \simeq K^*.$$

Weitere Anwendungsbeispiele des Homomorphiesatzes finden sich in den Antworten zu Frage 51 und Frage 64. ⧫

Frage 43 Was besagt der **Satz von Cayley**?

Antwort: Der Satz von Cayley besagt:

Für jede Gruppe existiert ein kanonischer injektiver Homomorphismus

$$G \longrightarrow \mathrm{Sym}\, G$$

in die Gruppe $\mathrm{Sym}\, G$ *aller Selbstabbildungen von* G*. Mit anderen Worten, jede Gruppe der Ordnung* n *ist isomorph zu einer Untergruppe von* S_n*.*

Zum *Beweis* betrachte man für $a \in G$ die Abbildung

$$\tau_a \colon G \longrightarrow G, \qquad g \mapsto ag.$$

Man verifiziert leicht die folgenden drei Eigenschaften

(i) τ_a ist bijektiv für jedes $a \in G$
(ii) $\tau_a \circ \tau_b = \tau_{ab}$ für alle $a, b \in G$
(iii) $\tau_a \circ \tau_{a^{-1}} = \mathrm{id}$ für alle $a \in G$.

Aus (i), (ii) und (iii) folgt, dass die Menge $\Theta := \{\tau_a \,;\, a \in G\}$ eine Untergruppe der symmetrischen Gruppe $\mathrm{Sym}(G)$ ist. Wegen (ii) ist

$$G \longrightarrow \Theta, \qquad a \mapsto \tau_a$$

ein Homomorphismus. Dieser ist injektiv, denn aus $\tau_a = \tau_b$ folgt $ag = bg$ für alle $g \in G$, also $a = b$. ⧫

Frage 44 Können Sie alle Untergruppen der symmetrischen Gruppe S_3 beschreiben?

Antwort: Die einzigen Untergruppen der Ordnung 2 in S_3 sind die von den Transpositionen σ_4, σ_5 und σ_6 (zur Bezeichnung siehe Frage 11) erzeugten Untergruppen.

Eine Untergruppe der Ordnung 3 ist mit $\langle \sigma_2 \rangle := \{1, \sigma_2, \sigma_3\}$ gegeben.

Mehr Untergruppen der Ordnung 3 kann es nicht geben, denn eine von $\langle \sigma_2 \rangle$ verschiedene Untergruppe der Ordnung 3 müsste mindestens eine der Permutationen σ_4, σ_5 oder σ_6 der Ordnung 2 enthalten, was aufgrund des Satzes von Lagrange nicht sein kann.

Da nach dem Satz von Lagrange jede echte Untergruppe von S_3 höchstens die Ordnung 3 hat, sind damit alle Untergruppen aufgezählt. ⧫

Frage 45 Warum ist jede Gruppe der Ordnung ≤ 5 eine abelsche Gruppe?

Antwort: Die Gruppen der Ordnung $2, 3$ und 5 sind Gruppen von Primzahlordnung. Für eine Gruppe G, deren Ordnung eine Primzahl p ist, folgt aber aus dem Satz von Lagrange, dass jedes vom neutralen Element verschiedene Element aus G die Ordnung p hat und damit ein Erzeuger von G ist. Gruppen mit Primzahlordnung sind also zyklisch und damit nach Antwort 38 abelsch.

Für Gruppen der Ordnung 4 wurde die Behauptung schon in der Antwort zu Frage 13 gezeigt, und für Gruppen der Ordnung 1 ist sie trivial. ♦

1.3 Der Signum-Homomorphismus

Jeder Permutation $\sigma\colon \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ lässt sich ein Vorzeichen so zuordnen, dass die Abbildung

$$\varepsilon\colon S_n \longrightarrow \{-1, 1\}$$

ein Gruppenhomomorphismus ist. Die Homomorphieeigenschaft von ε spielt in vielen Zusammenhängen eine große Rolle, insbesondere bei der Definition der Determinante nach Leibniz (vgl. Frage 271).

Frage 46 Was versteht man unter dem **Fehlstand** einer Permutation $\sigma \in S_n$?

Antwort: Ein Paar $(j, k) \in \{1, \ldots, n\}^2$ nennt man einen *Fehlstand* von $\sigma \in S_n$, wenn

$$j < k \quad \text{aber} \quad \sigma(j) > \sigma(k)$$

gilt. Zum Beispiel hat die Permutation $\left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]$ genau zwei Fehlstände, nämlich das Paar $(1, 3)$ und das Paar $(2, 3)$. ♦

Frage 47 Wie ist das **Vorzeichen** einer Permutation $\sigma \in S_n$ definiert?

Antwort: Für $\sigma \in S_n$ ist das **Vorzeichen** $\operatorname{sign} \sigma$ definiert durch

$$\operatorname{sign} \sigma = \begin{cases} +1, & \text{falls } \sigma \text{ eine gerade Anzahl an Fehlständen hat} \\ -1, & \text{falls } \sigma \text{ eine ungerade Anzahl an Fehlständen hat.} \end{cases}$$ ♦

Frage 48 Wann heißt ein Element $\tau \in S_n$ eine **Transposition**?

Antwort: Eine Permutation $\tau \in S_n$ heißt *Transposition*, wenn sie zwei Elemente aus $\{1, \ldots, n\}$ vertauscht und alle anderen fest lässt, wenn es also zwei Elemente k, j aus $\{1, \ldots, n\}$ mit $k \neq j$ gibt, so dass gilt:

$$\tau(k) = j, \qquad \tau(j) = k, \qquad \tau(m) = m \quad \text{für alle } m \in \{1, \ldots, n\} \setminus \{j, k\}.$$

Zur Bezeichnung der Transposition benutzt man die Schreibweise (j, k). ♦

Frage 49 Warum ist jede Permutation $\sigma \in S_n$ für $n \geq 2$ ein endliches Produkt von Transpositionen?

Antwort: Ist σ die identische Abbildung, dann gilt $\sigma = \tau \cdot \tau^{-1}$ für jede beliebige Transposition $\tau \in S_n$.

Im anderen Fall gibt es eine kleinste Zahl $j \in \{1, \ldots, n\}$, für die $\sigma(j) \neq j$ gilt, spezieller $\sigma(j) > j$ wegen der Bijektivität von σ. Ist τ_1 die Abbildung, welche j mit $\sigma(j)$ vertauscht, dann ist $\tau_1 \cdot \sigma$ eine Permutation, die mindestens die ersten j Elemente aus $\{1, \ldots, n\}$ fest lässt, d. h., $\tau_1 \cdot \sigma$ bildet mindestens ein Element mehr als σ auf sich selbst ab. Daraus folgt induktiv die Existenz von Transpositionen $\tau_1, \tau_2, \ldots, t_k$ mit $k < n - j + 1$, für die gilt $\tau_k \cdots \tau_2 \cdot \tau_1 \cdot \sigma = \mathrm{id}$, also $\sigma = \tau_1^{-1} \cdot \tau_2^{-1} \cdots \tau_k^{-1}$.

Beispiel. Für die Permutation $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{smallmatrix}\right]$ erhält man nacheinander

$$\begin{aligned} (1,4) \cdot \sigma &= \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{smallmatrix}\right], \\ (2,5) \cdot (1,4) \cdot \sigma &= \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{smallmatrix}\right], \\ (3,4) \cdot (2,5) \cdot (1,4) \cdot \sigma &= \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{smallmatrix}\right], \\ (4,5) \cdot (3,4) \cdot (2,5) \cdot (1,4) \cdot \sigma &= \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{smallmatrix}\right] = \mathrm{id}. \end{aligned}$$

Es folgt $\sigma = \big((4,5) \cdot (3,4) \cdot (2,5) \cdot (1,4)\big)^{-1} = (1,4) \cdot (2,5) \cdot (3,4) \cdot (4,5)$. ♦

Frage 50 Warum ist die Abbildung

$$\varepsilon \colon S_n \longrightarrow \{-1, 1\}, \qquad \sigma \mapsto \varepsilon(\sigma) := \text{Vorzeichen von } \sigma$$

ein Gruppenhomomorphismus?

Antwort: Es muss gezeigt werden, dass für $\tau, \sigma \in S_n$ gilt:

$$\operatorname{sign}(\tau \cdot \sigma) = \operatorname{sign} \tau \cdot \operatorname{sign} \sigma. \tag{$*$}$$

Dieser Zusammenhang ergibt sich im Wesentlichen aus der folgenden Darstellung des Signums:

$$\operatorname{sign} \sigma = \prod_{\pi(j) < \pi(k)} \frac{\sigma(k) - \sigma(j)}{k - j}, \tag{$**$}$$

wobei $\pi \in S_n$ beliebig gewählt werden kann. Um Formel $(**)$ einzusehen, mache man sich klar, dass im Zähler des rechts vom Gleichheitszeichen stehenden Produktes bis auf die Reihenfolge und das Vorzeichen genau dieselben Differenzen als Faktoren vorkommen wie im Nenner. Somit beträgt der Wert des Produkts ± 1. Weiter trägt ein Quotient $\frac{\sigma(k)-\sigma(j)}{k-j}$ genau dann ein negatives Vorzeichen, wenn das Paar (k, j) ein Fehlstand von σ ist. Daraus folgt insgesamt $((**))$.

Den Zusammenhang $(*)$ erhält man damit nun aus

$$\begin{aligned}\operatorname{sign}(\tau\cdot\sigma) &= \prod_{j<k}\frac{\tau(\sigma(k))-\tau(\sigma(j))}{k-j} = \prod_{j<k}\frac{\tau(\sigma(k))-\tau(\sigma(j))}{\sigma(k)-\sigma(j)}\cdot\prod_{j<k}\frac{\sigma(k)-\sigma(j)}{k-j}\\ &= \prod_{j<k}\frac{\tau(\sigma(k))-\tau(\sigma(j))}{\sigma(k)-\sigma(j)}\cdot\operatorname{sign}\sigma = \prod_{\sigma(j)<\sigma(k)}\frac{\tau(\sigma(k))-\tau(\sigma(j))}{\sigma(k)-\sigma(j)}\cdot\operatorname{sign}\sigma\\ &= \prod_{j<k}\frac{\tau(k)-\tau(j)}{k-j}\cdot\operatorname{sign}\sigma = \operatorname{sign}\tau\cdot\operatorname{sign}\sigma. \qquad \blacklozenge\end{aligned}$$

Frage 51 Wie viele Elemente hat $A_n = \ker\varepsilon$?

Antwort: A_n ist als Kern des Gruppenhomomorphismus ε ein Normalteiler in S_n (vgl. Frage 41). Da ε surjektiv ist, folgt mit dem Homomorphiesatz (vgl. Frage 42)

$$S_n/A_n \simeq \{-1,1\},$$

also insbesondere $|S_n/A_n| = (S_n : A_n) = 2$. Mit dem Satz von Lagrange folgt hieraus $|A_n| = |S_n|/2$, also $|A_n| = \frac{1}{2}n!$. $\blacklozenge$

Frage 52 Wann heißt eine Permutation $\sigma \in S_n$ **gerade**, wann **ungerade**? Wie lassen sich demnach die Elemente aus A_n charakterisieren?

Antwort: Die Darstellung einer Permutation als Produkt von Transpositionen, deren generelle Möglichkeit in Frage 49 gezeigt wurde, ist in der Regel nicht eindeutig. Für jede Permutation σ ist jedoch eindeutig bestimmt, ob sie sich als Produkt einer geraden oder ungeraden Anzahl von Transpositionen schreiben lässt.

Für den Nachweis zeigen wir, dass für eine beliebige Permutation $\sigma \in S_n$ und eine beliebige Transposition $\tau \in S_n$ stets gilt:

$$\operatorname{sign}(\tau\cdot\sigma) = -\operatorname{sign}\sigma.$$

Daraus folgt, dass sich jede Permutation mit ungeradem Vorzeichen nur als Produkt einer ungeraden Anzahl an Transpositionen darstellen lässt und entsprechend jede Permutation mit geradem Vorzeichen nur als Produkt einer geraden Anzahl an Transpositionen. Sei

$$\sigma = \begin{bmatrix}\cdots & j & \cdots & i & \cdots & k & \cdots\\ \cdots & \sigma(j) & \cdots & \sigma(i) & \cdots & \sigma(k) & \cdots\end{bmatrix} \qquad (*)$$

und τ die Transpostion, die $\sigma(j)$ und $\sigma(k)$ miteinander vertauscht. Beim Übergang von σ zu $\tau\cdot\sigma$ ändert sich die Anzahl der Fehlstände, und diese Anzahl hängt ab von

- der Änderung der Reihenfolge von $\sigma(j)$ und $\sigma(k)$. Dies bewirkt genau einen zusätzlichen Fehlstand oder genau einen Fehlstand weniger
- der Änderung der Reihenfolge von $\sigma(j)$ und $\sigma(i)$ sowie $\sigma(i)$ und $\sigma(k)$ für alle i mit $j < i < k$. Hier muss unterschieden werden:
  - Ist $\sigma(i) < \min\{\sigma(j), \sigma(k)\}$ oder $\sigma(i) > \max\{\sigma(j), \sigma(k)\}$, so ändert sich die Anzahl der Fehlstände nicht.
  - Für $\min\{\sigma(j), \sigma(k)\} < \sigma(i) < \max\{\sigma(j), \sigma(k)\}$ ändert sich die Anzahl der Fehlstände um $+2$ oder -2.

Das Aufsummieren der hinzugekommenen bzw. weggefallenen Fehlstände ergibt also in jedem Fall eine ungerade Zahl. Daraus folgt $(*)$ und insgesamt die Behauptung.

Bezüglich A_n gilt damit

$$A_n = \{\sigma \in S_n \,;\, \sigma \text{ ist ein Produkt einer geraden Anzahl von Transpositionen}\}.$$

⧫

Frage 53 Warum ist A_n für $n \geq 4$ keine abelsche Gruppe?

Antwort: Für paarweise verschiedene $x_1, x_2, x_3 \in \{1, \ldots, n\}$ gilt

$$(x_1, x_2, x_3) = (x_1, x_2) \circ (x_2, x_3).$$

Das heißt, dass jeder Drei-Zyklus (also eine Permutation, die genau drei Elemente nicht fest lässt) sich als Produkt zweier Transpositionen schreiben lässt und folglich zu A_n gehört. Ist $n \geq 4$, so enthält A_n die beiden Drei-Zyklen $\sigma_1 = (1, 2, 3)$ und $\sigma_2 = (2, 3, 4)$. Für diese gilt

$$\sigma_1 \circ \sigma_2 = (1, 2) \circ (3, 4) \neq (1, 3) \circ (2, 4) = \sigma_2 \circ \sigma_1.$$ ⧫

1.4 Ringe und Körper

Neben dem Gruppenbegriff sind für die Lineare Algebra auch die Strukturen „Ring“ und „Körper“ von großer Bedeutung. Wir bringen an dieser Stelle aus systematischen Gründen auch schon tiefer liegende Sachverhalte insbesondere über Ringe zur Sprache, die erst an späterer Stelle ab Kapitel 5.3 gebraucht werden.

Frage 54 Was versteht man unter

(a) einem **Ring**,
(b) einem **Schiefkörper**,
(c) einem **Körper**?

Benutzen Sie bei Ihren Antworten nach Möglichkeit die Sprache der Gruppentheorie.

Antwort: (a) Ein *Ring* ist eine Menge R mit zwei inneren Verknüpfungen „+“ und „·“ mit den Eigenschaften

(R1) $(R, +)$ ist eine abelsche Gruppe.
(R2) Die Verknüpfung „·“ ist assoziativ.
(R2) Es gelten die *Distributivgesetze*

$$(a + b) \cdot c = a \cdot c + b \cdot c, \qquad c \cdot (a + b) = c \cdot a + c \cdot b \qquad \text{für } a, b, c \in R.$$

Besitzt R außerdem ein Einselement bezüglich der Multiplikation, so nennt man R einen *Ring mit Eins*. Wo nicht ausdrücklich anders gesagt, verstehen wir unter einem Ring stets einen Ring mit Eins.

(b) Ein *Schiefkörper* S ist ein Ring mit der zusätzlichen Eigenschaft, dass $(S^*, \cdot) = (S \setminus \{0\}, \cdot)$ eine multiplikative Gruppe bildet, Zusätzlich zu den Eigenschaften R1, R2 und R3 gilt für S also noch, dass zu jedem $a \in S^*$ ein inverses Element a^{-1} existiert, so dass gilt

$$a^{-1} \cdot a = 1.$$

(c) Ein *Körper* K ist ein Schiefkörper mit der zusätzlichen Eigenschaft, dass die multiplikative Gruppe $(K^*, \cdot)$ kommutativ ist. ♦

Frage 55 Können Sie Beispiele nennen für

(a) Ringe (nichtkommutative und kommutative),
(b) einen Schiefkörper,
(c) einige Körper?

Antwort: (a) Die Menge der ganzen Zahlen ist ein kommutativer Ring mit 1. Die Mengen $n\mathbb{Z}$ für $n \in \mathbb{N}$ sind ebenfalls kommutative Ringe, besitzen jedoch kein Einselement bezüglich der Multiplikation. Ferner sind alle Körper und Schiefkörper insbesondere auch Ringe.

Aus einem gegebenen Ring R lassen sich durch verschiedene Konstruktionsprozesse weitere Ringe gewinnen:

Für einen Körper K sei $R = K^{n \times n}$ die Menge der $(n \times n)$-Matrizen mit Koeffizienten in K. Dann ist R bezüglich der üblichen Addition und Multiplikation von Matrizen ein Ring mit der Einheitsmatrix als neutralem multiplikativem Element. R ist für $n \geq 2$ nicht kommutativ. Etwas allgemeiner gilt, dass für einen Vektorraum V die Menge der linearen Abbildungen $V \longrightarrow V$ die Struktur eines Rings besitzt, wobei die additive Struktur durch die übliche Addition von Abbildungen und die Multiplikation durch die Verknüpfung von Abbildungen gegeben ist. Man beachte, dass die Gültigkeit des Distributivgesetzes hier von der *Linearität* der Abbildungen abhängt.

Für eine Menge M und einen Ring R sei R^M die Menge aller Abbildungen $M \longrightarrow R$. Definiert man für $f, g \in R^M$ die Verknüpfungen

$$f + g\colon X \longrightarrow R, \qquad x \mapsto f(x) + g(x)$$
$$f \cdot g\colon X \longrightarrow R, \qquad x \mapsto f(x) \cdot g(x),$$

dann ist R^M auf natürliche Weise ein Ring.

Im Fall $I = \mathbb{N}$ erhält man aus dem vorhergehenden Punkt einen wichtigen Spezialfall. Der *Polynomring* $R[X]$ ist definiert als

$$R[X] := \{(a_i)_{i\in\mathbb{N}}\ ;\ a_i \in R \text{ und } a_i = 0 \text{ für alle bis auf endlich viele } i\}.$$

$R[X]$ ist damit isomorph zu einem Unterring von $R^{\mathbb{N}}$. Genauer gilt:

$$R[X] \simeq R^{(\mathbb{N})} := \{f \in R^{\mathbb{N}}\ ;\ f(n) = 0 \text{ für alle bis auf endlich viele } n \in \mathbb{N}\}$$

(b) Das bekannteste Beispiel eines Schiefkörpers ist der Schiefkörper $\mathbb{H}$ der *Hamilton'schen Quaternionen*. Zur Konstruktion von $\mathbb{H}$ gehe man aus von einem vierdimensionalen Vektorraum V mit Basis e, i, j, k und definiere

$$e^2 = e, \quad ei = ie = i, \quad ej = je = j, \quad ek = ke = k,$$
$$i^2 = j^2 = k^2 = -e,$$
$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Das Produkt beliebiger Elemente aus V erklärt man hiervon ausgehend durch $\mathbb{R}$-lineare Ausdehnung. Mit dieser Multiplikation und der gewöhnlichen Vektoraddition ist $(V, +, \cdot) =: \mathbb{H}$ ein Schiefkörper.

(c) Beispiele für Körper sind $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$. Zwischen $\mathbb{Q}$ und $\mathbb{C}$ liegen unendlich viele *Zwischenkörper*, etwa $\mathbb{Q}(\sqrt{2}) := \{a+b\sqrt{2},\ ;\ a, b \in \mathbb{Q}\}$ oder $\mathbb{Q}(i) := \{a+bi,\ ;\ a, b \in \mathbb{Q}\}$. Diese Körper enthalten alle unendlich viele Elemente.

Beispiele *endlicher Körper* sind für jede Primzahl p die Mengen $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Ist allgemeiner $q = p^n$ eine Primzahlpotenz, so existiert ein Körper $\mathbb{F}_q$ mit q Elementen. Diesen erhält man als Erweiterungskörper von $\mathbb{F}_p$. (vgl. [5]).

Für einen Körper K ist die Menge $K(X)$ der *rationalen* Funktionen ebenfalls ein Körper. Diesen erhält man rein algebraisch als *Quotientenkörper* des Polynomrings $K[X]$ (analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$). ⧫

Frage 56 Was versteht man unter einem **Integritätsring**?

Antwort: Ein Ring R heißt *Integritätsring*, wenn für zwei Elemente $a, b \in R$ mit $a \neq 0$ und $b \neq 0$ stets auch $ab \neq 0$ gilt. Ein Integritätsring ist somit ein *nullteilerfreier* Ring. ⧫

Frage 57 Worin besteht der Unterschied zwischen einem kommutativen Ring mit Einselement ($\neq 0$) und einem Körper?

Antwort: Ein Ring, der kein Körper ist, besitzt nicht zu jedem Element ein multiplikativ Inverses, ist also bezüglich der Multiplikation keine Gruppe. ⧫

Frage 58 Warum besitzt der Körper $\mathbb{Q}$ der rationalen Zahlen keinen echten Unterkörper?

Antwort: Sei $U \subset \mathbb{Q}$ ein Unterkörper von $\mathbb{Q}$. Wegen $1 \in U$ folgt zunächst $\mathbb{Z} \in U$ und damit auch $\frac{1}{m} \in U$ für alle $m \in \mathbb{Z}^*$. Beide Zwischenergebnisse zusammen implizieren aber, dass die Brüche $\frac{n}{m}$ für alle $n \in \mathbb{Z}$ und alle $m \in \mathbb{Z}^*$ in U enthalten sind, dass also $U = \mathbb{Q}$ gilt. ♦

Frage 59 Was versteht man unter der **Charakteristik** eines Körpers K?

Antwort: Für $n \in \mathbb{N}$ betrachte man die endlichen Summen

$$\underbrace{1_K + 1_K + \cdots + 1_K}_{n \text{ Summanden}} =: n \cdot 1_K.$$

Sind diese alle von null verschieden, so setzt man $\mathrm{char}(K) = 0$. Andernfalls gibt es eine kleinste Zahl n, für die $n \cdot 1_K = 0$ gilt. In diesem Fall ist $\mathrm{char}(K) = n$. ♦

Frage 60 Welche Charakteristik haben die Körper $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) := \{a+b\sqrt{2}\,;\ a, b \in \mathbb{Q}\}$ und $\mathbb{C}$?

Antwort: Alle drei Körper besitzen die Charakteristik 0. ♦

Frage 61 Gibt es Körper der Charakteristik 2 mit unendlich vielen Elementen?

Antwort: Ja, beispielsweise ist der Körper $K = \mathbb{F}_2(X)$ der rationalen Funktionen über dem Körper $\mathbb{F}_2$ ein Körper mit unendlich vielen Elementen, für den $1_K + 1_K = 0$ gilt.

Ein weiteres Beispiel ist der *algebraische Abschluss* $\overline{\mathbb{F}}_2$ von $\mathbb{F}_2$. Zur Definition des algebraischen Abschlusses vergleiche [5]. ♦

Frage 62 Warum ist die Charakteristik eines endlichen Körpers stets eine Primzahl?

Antwort: Sei $\mathrm{char}(K) = n = pq$ eine zusammengesetzte Zahl mit $1 < p, q < n$. Definitionsgemäß ist dann n die kleinste natürliche Zahl mit $n1_K = 0$. Aufgrund des Distributivgesetzes gilt

$$(p1_K) \cdot (q1_K) = \underbrace{(1_K + \cdots + 1_K)}_{p\text{-mal}} \cdot \underbrace{(1_K + \cdots + 1_K)}_{q\text{-mal}} = (pq)1_K = n1_K = 0$$

Nach Voraussetzung ist $q1_K \neq 0$, also existiert ein Inverses $(q1_K)^{-1}$, und es folgt

$$p1_K = (p1_K) \cdot (q1_K) \cdot (q1_K)^{-1} = 0 \cdot (q1_K)^{-1} = 0,$$

im Widerspruch zur Voraussetzung. ♦

Frage 63 Was versteht man unter dem **Primkörper** eines Körpers K?

Antwort: Der Primkörper von K ist der kleinste Unterkörper von K. ⧫

Frage 64 Ist K ein Körper und P sein Primkörper. Warum gilt dann

(a) $\operatorname{char}(K) = p \iff P \simeq \mathbb{Z}/p\mathbb{Z}$,
(b) $\operatorname{char}(K) = 0 \iff P \simeq \mathbb{Q}$?

Mit anderen Worten: Warum sind $\mathbb{Q}$ und die Restklassenkörper $\mathbb{Z}/p\mathbb{Z}$ bis auf Isomorphie die einzigen Primkörper?

Antwort: (a) Ist $P = \mathbb{Z}/p\mathbb{Z}$, dann gilt $\operatorname{char}(K) = p$, andernfalls würde $q1_K = 0$ für ein $q < p$ gelten, und damit wäre $\mathbb{Z}/p\mathbb{Z}$ kein Unterkörper von K.

Zum Beweis der anderen Richtung betrachte man die Abbildung

$$F\colon \mathbb{Z} \longrightarrow K, \qquad n \longrightarrow n1_K.$$

Man überprüft leicht, dass es sich dabei um einen Homomorphismus von Ringen handelt, insbesondere also um einen Gruppenhomomorphismus der additiven Gruppe $(\mathbb{Z}, +)$ in die additive Gruppe $(K, +)$. Ist $\operatorname{char}(K) = p$, so gilt $\ker F = p\mathbb{Z}$, und aus dem Homomorphiesatz (Frage 42) folgt $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{im} F \subset K$.

(b) Ist $\operatorname{char}(K) = 0$, so sind alle endlichen Summen $n1_K$ für $n \in \mathbb{Z} \setminus \{0\}$ von null verschieden und besitzen daher ein inverses Element. Man betrachte

$$F^*\colon \mathbb{Q} \longrightarrow K, \qquad \frac{n}{m} \mapsto n1_K \cdot (m1_K)^{-1}.$$

Die Abbildung F^* ist wegen

$$F^*\left(\frac{kn}{km}\right) = kn1_K\cdot(km1_K)^{-1} = k1_K\cdot n1_K\cdot(k1_K\cdot m1_K)^{-1} = n1_K\cdot(m1_K)^{-1} = F^*\left(\frac{n}{m}\right)$$

wohldefiniert. Ferner ist F^*, wie man leicht überprüft, ein injektiver Körperhomomorphismus. Daraus folgt $\mathbb{Q} \subset K$ und folglich $\mathbb{Q} = P$, da $\mathbb{Q}$ keine weiteren Unterkörper enthält.

Die Umkehrung der Aussage ist trivial. ⧫

Frage 65 Was ist ein **Ideal** in einem Ring R?

Antwort: Eine Teilmenge $\mathfrak{a} \subset R$ heißt *Ideal*, wenn gilt:

(i) $\mathfrak{a}$ ist eine additive Untergruppe.
(ii) Für alle $a \in \mathfrak{a}$ und alle $r \in R$ gilt $ra \in \mathfrak{a}$ und $ar \in \mathfrak{a}$.

Zum Beispiel bilden für jedes $a \in R$ die Mengen

$$Ra := (a) := \{ra\ ;\ r \in R\}$$

ein Ideal in R. ⧫

Frage 66 Welches sind die Ideale in $\mathbb{Z}$?

Antwort: Die Ideale in $\mathbb{Z}$ sind genau die Mengen $a\mathbb{Z} := \{am \ ; \ m \in \mathbb{Z}\}$ mit $a \in \mathbb{Z}$. ♦

Frage 67 Ist ein Ideal $\mathfrak{a} \subset R$ stets auch ein Unterring von R?

Antwort: Nein, denn im Allgemeinen ist $1 \neq \mathfrak{a}$. Genauer folgt aus $1 \in \mathfrak{a}$ bereits $\mathfrak{a} = R$, da für jedes $r \in R$ gilt $r = 1 \cdot r \in \mathfrak{a}$. ♦

Frage 68 Was versteht man unter einem **Hauptidealring**? Kennen Sie ein Beispiel?

Antwort: Ein Ring R heißt *Hauptidealring*, wenn jedes Ideal $\mathfrak{a} \subset R$ von einem einzigen Element erzeugt wird, wenn also ein $a \in R$ existiert mit

$$\mathfrak{a} = Ra := (a) := \{ra \ ; \ r \in R\}.$$

Ein einfaches Beispiel eines Hauptidealrings ist $\mathbb{Z}$. ♦

Frage 69 Können Sie zeigen, dass für einen Homomorphismus $FR \longrightarrow R'$ zwischen Ringen R und R' der Kern von F ein Ideal in $\mathbb{Z}$ ist?

Antwort: Für $a, b \in \ker F$ gilt $F(a+b) = F(a) + F(b) = 0 + 0 = 0$, also $a + b \in \ker F$. Ferner folgt für beliebiges $r \in R$ $F(ra) = r \cdot F(a) = r \cdot 0 = 0$, also $ra \in \ker F$. Das zeigt die Behauptung. ♦

Frage 70 Wie ist für einen Ring R und ein Ideal $\mathfrak{a} \subset R$ der **Quotienten- bzw. Restklassenring** $R/\mathfrak{a}R$ definiert? Können Sie zeigen, dass $R/\mathfrak{a}R$ von R tatsächlich die Struktur eines Rings erbt?

Antwort: Ähnlich wie für Untergruppen definiert man für ein Ideal $\mathfrak{a} \subset R$ eine Relation „$\sim_\mathfrak{a}$“ auf R durch

$$a \sim_\mathfrak{a} b \Longleftrightarrow a - b \in \mathfrak{a}.$$

Die Relation „$\sim_\mathfrak{a}$“ ist dann eine Äquivalenzrelation. Denn wegen $a - a = 0 \in \mathfrak{a}$ für jedes $a \in R$ gilt $a \sim_\mathfrak{a} a$, die Relation ist also reflexiv. Sie ist symmetrisch, da aus $a - b \in \mathfrak{a}$, also $a \sim_\mathfrak{a} b$ auch $b - a = -(a - b) \in \mathfrak{a}$, also $b \sim_\mathfrak{a} a$ folgt. Um die Transitivität zu zeigen, nehme man $a \sim_\mathfrak{a} b$ und $b \sim_\mathfrak{a} c$ mit $a, b, c \in R$ an. Dann gilt $a - b \in \mathfrak{a}$ und $b - c \in \mathfrak{a}$ und daraus folgt

$$(a - b) + (b - c) = a - c \in \mathfrak{a},$$

also $a \sim_\mathfrak{a} c$. Das zeigt die Transitivität.

Man kann daher zu jedem $a \in R$ die Nebenklasse

$$[a] := \{b \in R \ ; \ b \sim_\mathfrak{a} a\} = a + \mathfrak{a}$$

bilden. Nach Frage 33 sind zwei Nebenklassen entweder disjunkt oder identisch, insbesondere ist R die disjunkte Vereinigung der Nebenklassen modulo $\mathfrak{a}$.

Eine Ringstruktur auf $R/\mathfrak{a}$ erklärt man mittels der Verknüpfungsregeln

$$[a]+[b] := [a+b], \qquad [a]\cdot[b] := [a\cdot b].$$

Hier ist wie in Antwort 40 zu zeigen, dass diese Regeln unabhängig von der Auswahl der Repräsentanten sind. Gilt etwa $[a]=[a']$ und $[b]=[b']$, dann hat man $a-a' \in \mathfrak{a}$ und $b-b' \in \mathfrak{a}$, und es folgt

$$(a+b)-(a'+b') = (a-a')+(b-b') \in \mathfrak{a}, \qquad (a\cdot b)-(a'\cdot b') = b(a-a')+a'(b-b') \in \mathfrak{a},$$

also

$$[a+b]=[a'+b'], \qquad [a\cdot b]=[a'\cdot b'].$$

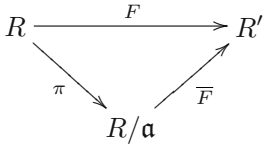
Die Multiplikation und Division in $R/\mathfrak{a}$ ist also wirklich unabhängig von der Auswahl der Repräsentanten.

Die Eigenschaften $R1$ bis $R3$ übertragen sich von R damit unmittelbar auf $R/\mathfrak{a}$, woraus insgesamt folgt, dass $R/\mathfrak{a}$ ein Ring ist. ⧫

Frage 71 Wie lautet der **Homomorphiesatz für Ringe**? Wie lässt er sich beweisen?

Antwort: Der Satz lautet:

Sei $F\colon R \longrightarrow R'$ ein Ringhomomorphismus, $\mathfrak{a}$ ein Ideal in R mit $\mathfrak{a} \subset \ker F$ und $\pi\colon R \longrightarrow R/\mathfrak{a}$ die natürliche Projektion. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\overline{F}\colon R/\mathfrak{a} \longrightarrow R'$, so dass das unten stehende Diagramm kommutiert.



Insbesondere gilt für surjektives F

$$R/(\ker F) \simeq R'.$$

Antwort: Der Beweis funktioniert nach demselben Muster wie der für Gruppen (vgl. Frage 42). Falls ein $\overline{F}$ mit den genannten Eigenschaften existiert, dann gilt für $\overline{a} \in R/\mathfrak{a}$ jedenfalls

$$\overline{F}(\overline{a}) = F(a). \qquad (*)$$

Nun zeigt man, dass durch die Festlegung $(*)$ tatsächlich ein wohldefinierter Homomorphismus $R/\mathfrak{a} \longrightarrow R'$ gegeben ist. Dazu ist wiederum nur die Unabhängigkeit der Definition von der Auswahl der Repräsentanten nachzuweisen. Sind a und b zwei Repräsentanten derselben Restklasse, dann gilt $a-b \in \mathfrak{a}$, also $a-b \in \ker F$, und daher liefert die Definition $(*)$

$$\overline{F}(\overline{a}) - \overline{F}(\overline{b}) = F(a) - F(b) = F(a-b) = 0,$$

also $\overline{F}(\overline{a}) = \overline{F}(\overline{b})$. Die Abbildung $\overline{F}$ ist folglich wohldefiniert und es gilt $\overline{F} \circ \pi = F$. Ferner ist $\overline{F}$ durch $(*)$ eindeutig festgelegt.

Ist F surjektiv, dann auch $\overline{F}$, und es gilt $F(a) = 0 \Longleftrightarrow a \in \ker F$, also $\overline{a} = 0 \in R/\ker F$. Daraus folgt der Zusatz. ⧫

1.5 Polynomringe

Das Studium der Polynome führt streng genommen über die Lineare Algebra hinaus und ist dem mathematischen Teilgebiet zuzurechnen, das man heutzutage allgemein als „Algebra“ bezeichnet. Polynome spielen trotzdem auch in der Linearen Algebra eine wesentliche Rolle, da in zahlreichen Fällen lineare Problemstellungen auf natürliche Weise die Untersuchung von Gleichungen „höheren“, eben polynomialen, Typs erfordern, etwa bei der Bestimmung der Eigenwerte eines Endomorphismus. Den Polynomring $R[X]$ über einem Ring R führen wir hier gleich im algebraischen Sinne ein, verstehen Polynome also nicht als spezielle Abbildungen $R \longrightarrow R$, sondern als Ring $R^{(\mathbb{N})}$. Auch einige allgemeine ringtheoretische Begriffe und Zusammenhänge werden behandelt.

Frage 72 Wie kann man für einen kommutativen Ring R den **Polynomring** $R[X]$ definieren?

Antwort: Man kann den Polynomring $R[X]$ als die Menge aller formal gebildeten Summen des Typs $\sum_{i=1}^{m} a_i X^i$ mit $a_i \in R$ einführen, wobei die obere Grenze m variabel aber stets endlich ist. Indem man auf diese Ausdrücke die Rechenregeln für gewöhnliche Summen anwendet, erkennt man $R[X]$ als kommutativen Ring. Eins- bzw. Nullelement entsprechen dabei dem Eins- bzw. Nullelement in R.

Etwas präziser lässt sich $R[X]$ definieren als die Menge aller Folgen $(a_i)_{i\in\mathbb{N}}$ mit Elementen $a_i \in R$, für die $a_i = 0$ für fast alle i gilt. Erklärt man die Addition und Multiplikation durch

$$\begin{aligned} (a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} &:= (a_i + b_i)_{i\in\mathbb{N}} \\ (a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} &:= (c_i)_{i\in\mathbb{N}} \qquad \text{mit } c_i = \sum_{\substack{k,\ell\in\mathbb{N} \\ k+\ell=i}} a_k b_\ell, \end{aligned}$$

so wird $R[X]$ unter dieser Definition zu einem kommutativen Ring mit 1. Die „Variable“ X kann man unter dieser Perspektive einführen als das Element

$$X := (0, 1, 0, \ldots) \in R^{(\mathbb{N})}.$$

Anwenden der Definition der Multiplikation auf X liefert dann

$$X^n = (\delta_{in})_{i\in\mathbb{N}} = (\underbrace{0, \ldots, 0}_{n \text{ - 1-mal}}, 1, 0, \ldots) \in R[X].$$

Identifiziert man die Elemente $a \in R$ mit $(a, 0, \ldots) \in R^{(\mathbb{N})}$, so ist diese Identifikation verträglich mit der Ringstruktur auf R, und jede Folge $f = (a_i)_{i\in\mathbb{N}} \in \mathbb{R}^{(\mathbb{N})}$ lässt sich als Summe der Gestalt $\sum_{i\in\mathbb{N}} a_i X^i$ darstellen. Die Definition der Addition und Multiplikation in $R[X]$ entspricht dann der Bildung von Summen und Produkten gewöhnlicher endlicher Summen. ♦

Frage 73 Wie ist der **Grad** eines Polynoms $f \in R[X]$ definiert?

Antwort: Ist f nicht das Nullpolynom, dann gibt es in der Darstellung $f = \sum_{i\in\mathbb{N}_0} a_i X^i \neq 0$ einen Koeffizienten $a_n \neq 0$, so dass $a_i = 0$ für alle $i > n$ gilt. Man nennt in diesem Fall a_n den *höchsten Koeffizienten* von f und bezeichnet n als den *Grad von* f, $n = \deg f$.

Für das Nullpolynom $f = 0$ gilt die Konvention $\deg f = -\infty$. ♦

Frage 74 Können Sie zeigen, dass für $f, g \in R[X]$ gilt

$$\deg(f + g) \leq \max\{\deg f, \deg g\}$$
$$\deg(f \cdot g) \leq \deg f + \deg g$$

sowie, falls R ein Integritätsring ist,

$$\deg(f \cdot g) = \deg f + \deg g?$$

Antwort: Sei

$$f = \sum_{i\in\mathbb{N}} a_i X^i \qquad g = \sum_{i\in\mathbb{N}} b_i X^i$$

mit $\deg f = n$ und $\deg g = m$. Dann gilt $a_i = 0$ und $b_j = 0$ und folglich $a_i + b_j = 0$ für alle $i > n$ und alle $j > m$, also $a_k + b_k = 0$ für alle $k > \max\{n, m\}$. Das zeigt die erste Behauptung.

Weiter gilt $a_i b_j = 0$, falls $i + j > n + m$ ist. Daraus folgt für

$$f \cdot g = \sum_{\ell\in\mathbb{N}} c_\ell \qquad \text{mit} \qquad c_\ell = \sum_{i+j=\ell} a_i b_j,$$

dass c_ℓ für alle $\ell > m + n$ verschwindet. Also gilt $\deg(f \cdot g) \leq \deg f + \deg g$.

Ist R zudem ein Integritätsring, dann folgt aus $a_n \neq 0$ und $b_m \neq 0$ auch $c_{n+m} = a_n b_m \neq 0$. Zusammen mit $\deg(f \cdot g) \leq m + n$ ergibt sich $\deg(f \cdot g) = \deg f + \deg g$. ♦

Frage 75 Wenn R ein Integritätsring ist, wieso dann auch $R[X]$?

Antwort: Für nichttriviale Polynome $f, g \in R[X]$ gilt $\deg f \geq 0$ und $\deg g \geq 0$. Dann ist nach Frage 74 aber auch $\deg(f \cdot g) = \deg f + \deg g \geq 0$, also $f \cdot g \neq 0$. Das zeigt, dass $R[X]$ ein Integritätsring ist. ♦

Frage 76 Wie ist für einen kommutativen Ring R und für ein Element $r \in R$ der **Einsetzungshomomorphismus** $F_r\colon\ R[X] \longrightarrow R$ definiert?

Antwort: Für $r \in R$ definiert man

$$F_r\colon\ R[X] \longrightarrow R, \qquad \sum_{i\in\mathbb{N}} c_i X^i \longmapsto \sum_{i\in\mathbb{N}} c_i r^i.$$

Dass dies ein Homomorphismus von Ringen ist, prüft man unmittelbar nach. ♦

Frage 77 Was versteht man unter einem **euklidischen Ring**?

Antwort: Ein Integritätsring R heißt *euklidischer Ring*, wenn es eine Abbildung $\delta\colon\ R \setminus \{0\} \longrightarrow \mathbb{N}$ gibt, die die folgende Eigenschaft besitzt: Zu je zwei Elementen $a, b \in R$ mit $b \neq 0$ existieren (nicht notwendig eindeutig bestimmte) Elemente $p, q \in R$, so dass

$$a = bq + r, \qquad r = 0 \text{ oder } \delta(r) < \delta(b)$$

gilt. Zum Beispiel ist $\mathbb{Z}$ aufgrund des Satzes über den euklidischen Algorithmus ein euklidischer Ring, wenn man δ als Betragsfunktion wählt. ♦

Frage 78 Können Sie zeigen, dass der Polynomring $K[X]$ zusammen mit der Gradabbildung ein euklidischer Ring ist?

Antwort: Seien f, g zwei Polynome aus $K[X]$ mit $g \neq 0$. Es muss gezeigt werden, dass Polynome $q, r \in K[X]$ existieren, für die gilt

$$f = qg + r, \qquad \deg r < \deg g. \tag{$*$}$$

Ist $\deg g > \deg f$, dann folgt dies bereits mit $q = 0$ und $r = f$. Man kann daher im Folgenden von

$$m = \deg f \geq \deg g = n$$

ausgehen. Für $f = aX^m + \cdots$ und $g = bX^n + \cdots$ setze man

$$q_1 := \frac{a}{b} \cdot X^{m-n}, \qquad f_1 = f - q_1 g.$$

Dann gilt $q_1 g = aX^m + \cdots$ und damit

$$f = q_1 g + f_1, \qquad \deg f_1 < \deg f.$$

Gilt nun bereits $\deg f_1 < \deg g$, so hat man eine Zerlegung des Typs $(*)$ gefunden. Andernfalls kann man dasselbeVerfahren für f_1 wiederholen und eine Zerlegung

$$f_1 = q_2 g + f_2, \qquad \deg f_2 < \deg f$$

finden. Derart fortfahrend lässt sich eine Serie $f_1, f_2, \ldots$ von Polynomen mit $\deg f_1 > \deg f_2 > \cdots$ konstruieren. Nach endlich vielen (genauer höchstens $m-n$) Schritten k gilt dann notwendigerweise $\deg f_k < \deg g$, und man erhält

$$f = q_1 g + q_2 g + \cdots + q_k g + f_k = (q_1 + \cdots + q_k) g + f_k, \qquad \deg f_k < \deg g.$$

Mit $q = q_1 + \cdots + q_k$ und $r = f_k$ folgt $(*)$.

Um die Eindeutigkeit zu zeigen, betrachte man eine weitere Darstellung $f = q'g + r'$ mit $\deg r' < \deg g$. Es gilt dann $(q - q')g + (r - r') = 0$ bzw.

$$(q - q')g = r' - r. \qquad (**)$$

Ist $(q - q') \neq 0$, dann folgt $\deg\big((q - q')g\big) \geq \deg g$. Andererseits ist nach Voraussetzung $\deg(r' - r) < \deg g$, im Widerspruch zu $(**)$. Also gilt $q = q'$ und damit auch $r = r'$. ♦

Frage 79 Können Sie das Verfahren aus Frage 78 an den beiden Polynomen

$$f = 4X^4 + 3X^3 + 2X^2 + X + 1, \qquad g = X^3 + X^2 + X + 1$$

veranschaulichen?

Antwort: Man erhält $q_1 g = 4X \cdot g = 4X^4 + 4X^3 + 4X^2 + 4X + 4$ und damit

$$f_1 = -X^3 - 2X^2 - 3X - 3.$$

Weiter ist $q_2 g = -1 \cdot g$, also

$$f_2 = f_1 + g = -X^2 - 2X - 2.$$

Damit erhält man wegen $\deg f_2 < \deg g$ mit

$$f = (4X - 1) \cdot g + (-X^2 - 2X - 2)$$

die gesuchte Zerlegung. ♦

Frage 80 Wieso ist jeder euklidische Ring ein Hauptidealring?

Antwort: Sei R ein euklidischer Ring und $\mathfrak{a}$ ein Ideal in R. Man kann $\mathfrak{a} \neq 0$ annehmen, da andernfalls bereits $\mathfrak{a} = (0)$ gilt. Sei

$$a = \min\{\delta(r)\ ;\ r \in \mathfrak{a}\}. \qquad (*)$$

Wir zeigen, dass $\mathfrak{a} = (a)$ gilt. Dazu wähle man ein beliebiges $b \in \mathfrak{a}$. Wegen $(*)$ gilt $\delta(b) \geq \delta(a)$, und da R ein euklidischer Ring ist, gibt es geeignete Elemente $q, r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $\delta(r) < \delta(a)$ gilt. Ist nun $\delta \neq 0$, dann kann r wegen $(*)$ nicht in $\mathfrak{a}$ enthalten sein, woraus $b - qa \notin \mathfrak{a}$ folgt. Das ist ein Widerspruch, da mit b und a auch $b - qa$ ein Element des Ideals $\mathfrak{a}$ ist. Es muss also $r = 0$ und damit $b = qa$, also $b \in (a)$ gelten. Daraus folgt $\mathfrak{a} = (a)$, also ist R ein Hauptidealring. ♦

Frage 81 Wann heißen zwei Elemente a, b eines Integritätsrings R **assoziiert**?

Antwort: Die beiden Elemente a und b heißen *assoziiert*, wenn es eine Einheit $e \in R^*$ mit $ae = b$ gibt. ♦

Frage 82 Wieso sind zwei Elemente a, b eines Integritätsrings R genau dann assoziiert, wenn $(a) = (b)$ gilt?

Antwort: Sind a und b assoziiert, dann gilt $ae = b$ und $be' = a$ mit Einheiten $e, e' \in R^*$. Daraus folgt $b \in (a)$ und $(a) \in b$, also $(b) \supset (a)$ und $(a) \supset (b)$. Das beweist die eine Richtung der Äquivalenz. Gelte nun umgekehrt $(a) = (b)$. Dann gibt es Elemente $p, q \in R$ mit $a = pb$ und $b = qa$, woraus $a = pqa$ bzw. $a \cdot (1 - pq) = 0$ folgt. Ist $a \neq 0$, dann erhält man $pq = 1$, die Elemente p und q sind also Einheiten und a und b folglich assoziiert. Dies gilt auch im Fall $a = 0$, denn wegen $b = qa$ folgt dann $a = b = 0$. ♦

Frage 83 Wann nennt man ein Element p eines Integritätsrings R **irreduzibel**, wann **Primelement**?

Antwort: (i) p heißt *irreduzibel*, wenn aus einer Gleichung $p = ab$ mit $a, b \in R$ stets folgt, dass a oder b eine Einheit in R ist. Im anderen Fall heißt p *reduzibel*.

(ii) p heißt *Primelement*, wenn aus $p|ab$ mit $a, b \in R$ stets $p|a$ oder $p|b$ folgt. Dabei bedeutet die Schreibweise $p|q$, dass p ein Teiler von q ist, also ein Element $r \in R$ mit $q = pr$ existiert.

Im Ring $\mathbb{Z}$ sind die irreduziblen Elemente genauso wie die Primelemente gerade die Primzahlen einschließlich der 1. ♦

Frage 84 Wieso ist in jedem Integritätsring R jedes Primelement auch irreduzibel?

Antwort: Sei $p \in R$ ein Primelement. Aus $p = ab$ folgt dann $p|a$ oder $p|b$. Ohne Beschränkung der Allgemeinheit können wir $p|b$, also $b = cp$ für ein $c \in R$ annehmen. Es folgt $p = acp$ oder $p \cdot (1 - ac) = 0$. Damit ist a eine Einheit in R und p folglich irreduzibel. ♦

Frage 85 Wieso gilt für einen Hauptidealring R auch, dass jedes irreduzible Element ein Primelement ist?

Antwort: Sei $p \in R$ irreduzibel und gelte $p|ab$ sowie $p \not| a$. Es muss $p|b$ gezeigt werden. Dazu betrachte man das Ideal

$$(a) + (p) = \{ra + sp \,;\; s, r \in R\}.$$

Da R nach Voraussetzung ein Hauptideal ist, wird $(a)+(p)$ von einem Element $c \in R$ erzeugt, also gilt $(a)+(p)=(c)$ und insbesondere $a \in (c)$ und $p \in (c)$, also $a = rc$ und $p = sc$ für geeignete Elemente $r, s \in R$. Da p irreduzibel ist, ist entweder s oder c eine Einheit in R. Im ersten Fall folgt $c = s^{-1}p$ und damit $a = rs^{-1}p$, im Widerspruch zur Voraussetzung, dass p kein Teiler von a ist. Also bleibt nur die Möglichkeit, dass c eine Einheit in R ist. Dies impliziert $(c) = (a)+(p) = R$, insbesondere gibt es $e, f \in R$ mit $ea+fp=1$. Multiplikation dieser Gleichung mit b liefert $eab + fpb = b$. Wegen $p|ab$ folgt aus dieser Gleichung wie gewünscht $p|b$. ⧫

Frage 86 Können Sie zeigen, dass sich in einem Hauptidealring R jedes Element $a \neq 0$, welches keine Einheit ist, als endliches Produkt von Primelementen schreiben lässt?

Antwort: Ist a irreduzibel, dann ist a nach Frage 84 prim und somit insbesondere ein endliches Produkt von Primelementen. Wir können folglich im Weiteren davon ausgehen, dass a reduzibel ist und führen den Beweis indirekt, nehmen also an, dass sich a nicht als endliches Produkt von Primelementen schreiben lässt. Da a reduzibel ist, gilt $a = a_1 b_1$ für zwei Nichteinheiten a_1 und b_1, von denen nach der Voraussetzung sich mindestens einer ebenfalls nicht als endliches Produkt von Primelementen schreiben lässt. Sei dies etwa a_1. Dann gilt aus denselben Gründen wie oben $a_1 = a_2 b_2$ für zwei Nichteinheiten $a_2, b_2 \in R$, wobei man ohne Beschränkung der Allgemeinheit annehmen kann, dass sich a_2 nicht als endliches Produkt von Primelementen schreiben lässt. Fährt man auf diese Weise fort, erhält man eine Folge

$$a = a_0, a_1, a_2, \ldots \in R, \qquad a_{i+1} | a_i.$$

Da ferner a_{i+1} und a_i nicht miteinander assoziiert sind, führt das auf eine echt aufsteigende Kette von Idealen

$$(a) = (a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots .$$

Nun ist leicht einzusehen, dass in diesem Fall auch $\mathfrak{b} = \bigcup_{i \in \mathbb{N}} (a_i)$ ein Ideal in R ist, und da R ein Hauptideal ist, gilt $\mathfrak{b} = (b)$ für ein $b \in R$. Nach Definition von $\mathfrak{b}$ gibt es dann einen Index i_0 mit $b \in (a_{i_0})$. Es folgt

$$\mathfrak{b} = (b) \subset (a_{i_0}) \subset (a_i) \subset \mathfrak{b}$$

für alle $i \geq i_0$. Also ist $(a_{i_0}) = (a_i)$ für $i \geq i_0$, im Widerspruch dazu, dass die Kette der Ideale echt aufsteigend ist. ⧫

Frage 87 Können Sie zeigen, dass die Primfaktorzerlegung in einem Integritätsring bis auf Assoziiertheit eindeutig ist, d. h. dass aus einer Gleichung der Form

$$p_1 \cdots p_r = q_1 \cdots q_s \qquad (*)$$

für Primelemente $p_i, q_i \in R$ stets folgt, dass nach geeigneter Umnummerierung p_i und q_i assoziiert sind und insbesondere $r = s$ gilt?

Antwort: Aus $(*)$ folgt $p_1|q_1 \cdots q_s$, und da $q_1, \ldots, q_s$ Primelemente sind, gibt es ein q_i mit $p_1|q_i$, also $p_1 = \epsilon_1 q_i$. Durch Umnummerierung kann man $i = 1$ erreichen und erhält damit die Gleichung

$$p_2 \cdots p_r = \epsilon_1 q_2 \cdots q_s.$$

Auf dieselbe Weise schließt man nun, dass p_2 zu einem der Elemente $q_2, \ldots, q_s$ assoziiert sein muss. Induktiv folgt daraus, dass p_i zu q_i für $i = 1, \ldots, r$ assoziiert ist, wenn man die Elemente $q_1, \ldots, q_s$ entsprechend umnummeriert. Insbesondere gilt $s > r$, und das Herauskürzen aller p_i liefert die Gleichung

$$1 = q_{r+1} \cdots q_s,$$

welche zeigt, dass die Elemente $q_{r+1}, \ldots, q_s$ sämtlich Einheiten sind, im Widerspruch zu ihrer Eigenschaft als Primelemente. ♦

Frage 88 Wie ist der **größte gemeinsame Teiler** von Ringelementen $r_1, \ldots, r_n \in R$ definiert?

Antwort: Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von $r_1, \ldots, r_n$, wenn gilt:

(i) $d|r_i$ für $i = 1, \ldots, n$, d. h. d ist ein gemeinsamer Teiler der r_i.
(ii) Ist a ein gemeinsamer Teiler der r_i, so gilt $d|a$.

Man schreibt in diesem Fall $d = \mathrm{ggT}\,(r_1, \ldots, r_n)$. ♦

Frage 89 Seien a, b Elemente eines Integritätsrings R und $d = \mathrm{ggT}\,(a, b)$. Dann gilt $aR + bR = dR$, insbesondere existieren $r, s \in R$ mit $ar + bs = d$, wobei $\mathrm{ggT}\,(r, s) = 1$ gilt. Können Sie das beweisen?

Antwort: Da R ein Hauptidealring ist, gilt $aR + bR = d'R$ für ein $d' \in R$, und es ist d' ein gemeinsamer Teiler von a und b und damit auch von d. Es gilt also $d'|d$. Andererseits impliziert die Gleichung $aR + bR = d'R$, dass $as + br = d'$ für bestimmte Zahlen $r, s \in R$ gilt, und hieraus folgt, dass jeder gemeinsame Teiler von a und b auch ein Teiler von d' ist. Also gilt $d|d'$ und folglich $d = d'$. Das beantwortet den ersten Teil der Frage. Ist d^* ein gemeinsamer Teiler von r und s, dann folgt aus der Gleichung $ar + bs = d$, dass d^*d ein Teiler von d ist. Folglich ist d^* eine Einheit, und es gilt $\mathrm{ggT}\,(r, s) = 1$. ♦

Frage 90 Können Sie zeigen, dass ein Element $p \neq 0$ eines Hauptidealrings R genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Körper ist?

Antwort: Sei p ein Primelement. Für jedes $a \in R \setminus (p)$ gilt dann $\mathrm{ggT}\,(a,p) = 1$, und nach Frage 89 gibt es $r, s \in R$ mit $ra + sp = 1$. Für die Restklasse $[ar + sp] = [a][r] \in R/(p)$ gilt daher $[r][a] = [1]$, d. h., $[a]$ ist eine Einheit in $R/(p)$. Damit ist $R/(p)$ ein Körper.

Ist umgekehrt p kein Primelement, dann gilt $p = ab$ für zwei Nichteinheiten $a, b \in R$. In $R/(p)$ gilt dann $[a] \neq [0]$ und $[b] \neq [0]$ aber $[a][b] = [ab] = [p] = [0]$. Der Ring $R/(p)$ besitzt in diesem Fall Nullteiler und kann daher kein Körper sein. ⧫

Frage 91 Was ist eine **Nullstelle** eines Polynoms $f \in R[X]$?

Antwort: Ein Element $a \in R$ heißt *Nullstelle* von f, wenn $f(a) = 0$ gilt, d. h. wenn f im Kern des Einsetzungshomomorphismus $F_a \colon R[X] \longrightarrow R$, $p \longmapsto p(a)$ liegt.

Frage 92 Sei $\alpha \in K$ eine Nullstelle des Polynoms $f \in K[X]$. Können Sie zeigen, dass dann ein Polynom $g \in K[X]$ existiert, so dass

$$f = (X - \alpha) \cdot g$$

gilt?

Antwort: Division mit Rest führt auf eine Gleichung

$$f = (X - \alpha) \cdot g + r \qquad (*)$$

mit $\deg r < \deg(X - \alpha) = 1$, also $r \in K$. Setzt man hier α für X ein, so folgt wegen $f(\alpha) = 0$ unmittelbar $r = 0$. ⧫
