Elemente der Algebra

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Sommersemester 2015

Inhaltsverzeichnis

Vorwort 4
1. Vorlesung - Gruppen 5
1. Arbeitsblatt 10
2. Vorlesung - Ringe 14
2. Arbeitsblatt 21
3. Vorlesung - Körper 24
3. Arbeitsblatt 30
4. Vorlesung - Polynomringe 35
4. Arbeitsblatt 42
5. Vorlesung - Division mit Rest 46
5. Arbeitsblatt 50
6. Vorlesung - Teilbarkeit 53
6. Arbeitsblatt 56
7. Vorlesung - Ideale 59
7. Arbeitsblatt 63
8. Vorlesung - Hauptidealbereiche 66
8. Arbeitsblatt 69
9. Vorlesung - Faktorielle Bereiche 72
9. Arbeitsblatt 76
10. Vorlesung - Homomorphismen 80
10. Arbeitsblatt 85
11. Vorlesung - Nebenklassen 90
11. Arbeitsblatt 93
12. Vorlesung - Restklassenbildung 98
12. Arbeitsblatt 102
13. Vorlesung - Ringhomomorphismen 104
13. Arbeitsblatt 108
14. Vorlesung - Restklassenringe 111
14. Arbeitsblatt 116
15. Vorlesung - Chinesischer Restsatz 119
15. Arbeitsblatt 122

16. Vorlesung - Chinesischer Restsatz für $\mathbb{Z}$ 127
16. Arbeitsblatt 130
17. Vorlesung - Quotientenkörper 133
17. Arbeitsblatt 137
18. Vorlesung - Partialbruchzerlegung 141
18. Arbeitsblatt 146
19. Vorlesung - Vektorräume 150
19. Arbeitsblatt 154
20. Vorlesung - Basen 155
20. Arbeitsblatt 161
21. Vorlesung - Dimension 165
21. Arbeitsblatt 169
22. Vorlesung - Körpererweiterungen 172
22. Arbeitsblatt 177
23. Vorlesung - Algebraische Zahlen 179
23. Arbeitsblatt 183
24. Vorlesung - Die Gradformel 184
24. Arbeitsblatt 188
25. Vorlesung - Zirkel und Lineal 193
25. Arbeitsblatt 197
26. Vorlesung - Quadrate und konstruierbare Zahlen 200
26. Arbeitsblatt 204
27. Vorlesung - Quadratur des Kreises 206
27. Arbeitsblatt 212
28. Vorlesung - Einheitswurzeln 214
28. Arbeitsblatt 219
Anhang A: Bildlizenzen 221
Abbildungsverzeichnis 221

Vorwort

Dieses Skript gibt die Vorlesung Elemente der Algebra wieder, die ich im Sommersemester 2015 an der Universität Osnabrück im Studiengang Mathematik (Bildung Erziehung Unterricht) gehalten habe.

 Ich bedanke mich bei der Wikimedia-Gemeinschaft und insbesondere bei Benutzer Exxu für die wichtigen Beiträge im Projekt semantische Vorlagen, die eine weitgehend automatische Erstellung des Latexcodes ermöglichen.

Bei Sabrina Syed bedanke ich mich für die Durchführung des Übungsbetriebs. Bei Frau Marianne Gausmann bedanke ich mich für die Erstellung der Pdf-Files und bei den Studierenden für einzelne Korrekturen.

Holger Brenner

1. Vorlesung - Gruppen

Der Gruppenbegriff

Definition 1.1. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto \circ(x,y) = x \circ y.$$

Statt $\circ(x,y)$ schreibt man $x \circ y$ oder (je nach Kontext) $x + y$ oder $x * y$ oder einfach xy.

Definition 1.2. Ein *Monoid* ist eine Menge M zusammen mit einer Verknüpfung

$$\circ : M \times M \to M$$

und einem ausgezeichneten Element $e \in M$ derart, dass folgende beiden Bedingungen erfüllt sind.

(1) Die Verknüpfung ist *assoziativ*, d.h. es gilt

$$(x \circ y) \circ z = x \circ (y \circ z)$$

für alle $x, y, z \in M$.

(2) e ist *neutrales Element* der Verknüpfung, d.h. es gilt

$$x \circ e = x = e \circ x$$

für alle $x \in M$.

In einem Monoid ist das neutrale Element eindeutig bestimmt. Wenn es nämlich zwei Elemente e_1 und e_2 gibt mit der neutralen Eigenschaft, so folgt sofort

$$e_1 \ = \ e_1 e_2 \ = \ e_2.$$

Definition 1.3. Ein Monoid $(G, e, \circ)$ heißt *Gruppe*, wenn jedes Element ein *inverses Element* besitzt, d.h. wenn es zu jedem $x \in G$ ein $y \in G$ mit $x \circ y \ = \ e \ = \ y \circ x$ gibt.

Die Menge aller Abbildungen auf einer Menge X in sich selbst ist mit der Hintereinanderschaltung ein Monoid; die nicht bijektiven Abbildungen sind aber nicht umkehrbar, so dass sie kein Inverses besitzen und daher keine Gruppe vorliegt. Die Menge der bijektiven Selbstabbildungen einer Menge und die Menge der Bewegungen eines geometrischen Objektes sind hingegen eine Gruppe. In einer Gruppe ist das inverse Element zu einem Element $x \in G$ eindeutig bestimmt. Wenn nämlich y und z die Eigenschaft besitzen, zu x invers zu sein, so gilt

$$y \ = \ ye \ = \ y(xz) \ = \ (yx)z \ = \ ez \ = \ z.$$

Daher schreibt man das zu einem Gruppenelement $x \in G$ eindeutig bestimmte inverse Element als

$$x^{-1}\,.$$

Definition 1.4. Eine Gruppe $(G, e, \circ)$ heißt *kommutativ* (oder *abelsch*), wenn die Verknüpfung kommutativ ist, wenn also $x \circ y = y \circ x$ für alle $x, y \in G$ gilt.

Aus der Grundvorlesung sind schon viele kommutative Gruppen bekannt. Zunächst gibt es die additiven Zahlbereiche, also

$$(\mathbb{Z}, 0, +),\ (\mathbb{Q}, 0, +),\ (\mathbb{R}, 0, +),\ (\mathbb{C}, 0, +)\,,$$

wobei jeweils das Inverse durch das Negative einer Zahl gegeben ist. Diese Zahlbereiche haben allerdings über die additive Gruppenstruktur hinaus noch mehr Struktur, nämlich die Multiplikation, die mit der Addition durch die Distributivgesetze verbunden sind. Dies wird später mit dem Begriff des „Ringes“ bzw. des „Körpers“ präzisiert. Bei $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ gilt ferner, dass man durch jede von null verschiedene Zahl „dividieren darf“. Dies ist gleichbedeutend damit, dass multiplikative Gruppen

$$(\mathbb{Q} \setminus \{0\}, 1, \cdot),\ (\mathbb{R} \setminus \{0\}, 1, \cdot),\ (\mathbb{C} \setminus \{0\}, 1, \cdot)$$

vorliegen. Diese werden meistens mit $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ bezeichnet. Innerhalb der ganzen Zahlen darf man nur durch 1 und -1 dividieren, und in der Tat ist die Menge $\{1, -1\}$ mit der Multiplikation eine Gruppe. Und wenn wir schon bei kleinen Gruppen sind: Es gibt im wesentlichen genau eine Gruppe mit nur einem Element, die man die triviale Gruppe nennt.

Ferner ist der Begriff des Vektorraums bekannt, also beispielsweise der $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ mit komponentenweiser Addition. Das neutrale Element ist der Nullvektor $0 = (0, \ldots, 0)$, und das Inverse ist wieder das Negative eines Vektors, das wiederum komponentenweise gegeben ist. Diese Gruppen sind alle kommutativ.

Die Drehungen in der Ebene an einem regelmäßigen n-Eck bilden wiederum eine kommutative Gruppe, die aus n Elementen besteht (siehe unten). Die Menge aller ebenen Drehungen zu einem beliebigen Winkel α, $0 \leq \alpha < 2\pi$, ist ebenfalls eine Gruppe, die sogenannte *Kreisgruppe*. Sie ist die Symmetriegruppe des Kreises.

Lösbarkeit von Gleichungen

Häufig wird gesagt, dass es in der Algebra um die Lösbarkeit und die Lösungen von Gleichungen geht.

Satz 1.5. *Sei $(G, e, \circ)$ eine Gruppe. Dann besitzen zu je zwei Gruppenelementen $a, b \in G$ die beiden Gleichungen*

$$a \circ x = b \text{ und } y \circ a = b$$

eindeutige Lösungen $x, y \in G$.

Beweis. Wir betrachten die linke Gleichung. Aus beidseitiger Multiplikation mit a^{-1} (bzw. mit a) von links folgt, dass nur

$$x = a^{-1} \circ b$$

als Lösung in Frage kommt. Wenn man dies einsetzt, so sieht man, dass es sich in der Tat um eine Lösung handelt. □

Im Aufbau des Zahlsystems spielt das Bestreben eine wichtige Rolle, Gleichungen eines bestimmten Typs lösbar zu machen. So erklärt sich der Übergang von $\mathbb{N}$ nach $\mathbb{Z}$ dadurch, Gleichungen der Form

$$a + x = b \text{ mit } a, b \in \mathbb{N}\,,$$

lösen zu können, und der Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ dadurch, Gleichungen der Form

$$ax = b \text{ mit } a, b \in \mathbb{Z},\ a \neq 0\,,$$

lösen zu können.

Potenzgesetze

Sei G eine (multiplikativ geschriebene) Gruppe und $g \in G$ ein Element. Dann definieren wir zu jeder ganzen Zahl $k \in \mathbb{Z}$ die k-te *Potenz* von g, geschrieben g^k, durch

$$g^k = \begin{cases} e_G, \text{ falls } k = 0\,, \\ gg\cdots g \quad k - \text{mal, falls } k \text{ positiv ist}\,, \\ g^{-1}g^{-1}\cdots g^{-1} \quad (-k) - \text{mal, falls } k \text{ negativ ist}\,. \end{cases}$$

Bei additiver Schreibweise schreibt man kg und spricht vom k-ten *Vielfachen* von g.

Lemma 1.6. *Sei G eine Gruppe und $g \in G$ ein Element, und seien $m, n \in \mathbb{Z}$ ganze Zahlen. Dann gelten die folgenden Potenzgesetze.*

(1) *Es ist $g^0 = e_G$.*
(2) *Es ist $g^{m+n} = g^m g^n$.*

Beweis. Die erste Aussage folgt aus der Definition. Die zweite Aussage ist klar, wenn beide Zahlen ≥ 0 oder beide ≤ 0 sind. Sei also m positiv und n negativ. Bei $m \geq -n$ kann man in $g^m g^n$ „innen“ $-n$-mal g mit g^{-1} zu e_G kürzen, und übrig bleibt die $m - (-n) = (m + n)$-te Potenz von g, also g^{m+n}. Bei $m < -n$ kann man m-mal g mit g^{-1} kürzen und übrig bleibt die $-n - m = -(m + n)$- te Potenz von g^{-1}. Das ist wieder g^{m+n}. □

Die vorstehende Aussage werden wir später so formulieren, dass ein Gruppenhomomorphismus von $\mathbb{Z}$ nach G vorliegt, siehe hierzu auch Lemma 10.7.

Gruppenordnung und Elementordnung

Definition 1.7. Zu einer endlichen Gruppe G bezeichnet man die Anzahl ihrer Elemente als *Gruppenordnung* oder als die *Ordnung der Gruppe*, geschrieben

$$\operatorname{ord}(G) = \#(G).$$

Definition 1.8. Sei G eine Gruppe und $g \in G$ ein Element. Dann nennt man die kleinste positive Zahl n mit $g^n = e_G$ die *Ordnung* von g. Man schreibt hierfür $\operatorname{ord}(g)$. Wenn alle positiven Potenzen von g vom neutralen Element verschieden sind, so setzt man $\operatorname{ord}(g) = \infty$.

Lemma 1.9. *Sei G eine endliche Gruppe. Dann besitzt jedes Element $g \in G$ eine endliche Ordnung. Die Potenzen*

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

sind alle verschieden.

Beweis. Da G endlich ist, muss es unter den positiven Potenzen

$$g^1,\ g^2,\ g^3, \ldots$$

eine Wiederholung geben, sagen wir $g^m = g^n$ mit $m < n$. Wir multiplizieren diese Gleichung mit g^{-m} und erhalten

$$g^{n-m} = g^m g^{-m} = (g^1 g^{-1})^m = e_G^m = e_G.$$

Also ist die Ordnung von g maximal gleich $n - m$. Mit dem gleichen Argument kann man die Annahme, dass es unterhalb der Ordnung zu einer Wiederholung kommt, zum Widerspruch führen. □

Untergruppen

Definition 1.10. Sei $(G, e, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe* von G wenn folgendes gilt.

(1) $e \in H$.
(2) Mit $g, h \in H$ ist auch $g \circ h \in H$.
(3) Mit $g \in H$ ist auch $g^{-1} \in H$.

Man hat beispielsweise die beiden Ketten von sukzessiven additiven Untergruppen,

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

und multiplikativen Gruppen

$$\{1, -1\} \subseteq \mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times.$$

Die triviale Gruppe $\{e\}$ ist Untergruppe von jeder Gruppe. Untervektorräume eines Vektorraums sind ebenfalls Untergruppen.

Lemma 1.11. *Sei G eine Gruppe und $H_i \subseteq G$, $i \in I$, eine Familie von Untergruppen. Dann ist auch der Durchschnitt*

$$\bigcap_{i \in I} H_i$$

eine Untergruppe von G.

Beweis. Siehe Aufgabe 2.2. □

Definition 1.12. Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge. Dann nennt man

$$(M) = \bigcap_{M \subseteq H,\, H \text{Untergruppe}} H$$

die von M *erzeugte Untergruppe*.

Insbesondere spricht man zu einer endlichen Menge $g_1, \ldots, g_n \in G$ von der davon erzeugten Untergruppe

$$(g_1, \ldots, g_n)\,.$$

Sie besteht aus allen „Wörtern“ oder „Termen“ (Buchstabenkombinationen) in den g_i und g_i^{-1}. Zu einem einzigen Element g hat die davon erzeugte Gruppe eine besonders einfache Gestalt, sie besteht nämlich aus allen Potenzen

$$g^k,\ k \in \mathbb{Z}\,,$$

wobei diese Potenzen untereinander nicht verschieden sein müssen.

Zyklische Gruppen

Definition 1.13. Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

Die Gruppe $\mathbb{Z}$ der ganzen Zahlen ist zyklisch, und zwar ist 1 aber auch -1 ein Erzeuger. Alle anderen ganzen Zahlen sind kein Erzeuger von $\mathbb{Z}$, da die 1 nur ein ganzzahliges Vielfaches von 1 und von -1 ist (allerdings ist die von einer ganzen Zahl $n \neq 0$ erzeugte Untergruppe „isomorph“ zu $\mathbb{Z}$). Ebenso sind die „Restklassengruppen“

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$$

zyklisch, und 1 und -1 sind ebenfalls Erzeuger. Allerdings gibt es dort in aller Regel noch viele weitere Erzeuger; mit deren genauer Charakterisierung werden wir uns bald beschäftigen.

Wie gesagt, in einer zyklischen Gruppe gibt es ein Element g derart, dass man jedes andere Element als g^k mit einer ganzen Zahl $k \in \mathbb{Z}$ schreiben kann, die im Allgemeinen nicht eindeutig bestimmt ist. Daraus folgt sofort die folgende Beobachtung.

Lemma 1.14. *Eine zyklische Gruppe ist kommutativ.*

Beweis. Das ist trivial. □

Wir erwähnen zwei Modelle für die zyklische Gruppe der Ordnung n.

Eine zyklische Blüte der Ordnung fünf.

Beispiel 1.15. Sei $n \in \mathbb{N}$. Dann bilden die ebenen Drehungen um Vielfache des Winkels $360/n$ Grad eine zyklische Gruppe der Ordnung n.

Beispiel 1.16. Sei $n \in \mathbb{N}$. Bei Division durch n besitzt jede ganze Zahl k einen eindeutig bestimmten Rest aus

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\},$$

den man mit $k \mod n$ bezeichnet. Auf der Menge dieser Reste kann man addieren, und zwar setzt man

$$a + b := (a + b) \mod n.$$

D.h. man ersetzt die in $\mathbb{Z}$ durch die gewöhnliche Addition gewonnene Summe durch ihren Rest modulo n. Dies ist ebenfalls eine zyklische Gruppe, siehe Aufgabe 1.17, mit 1 als Erzeuger.

1. Arbeitsblatt

Übungsaufgaben

Aufgabe 1.1. Betrachte die ganzen Zahlen $\mathbb{Z}$ mit der Differenz als Verknüpfung, also die Abbildung

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},\ (a,b) \longmapsto a-b.$$

Besitzt diese Verknüpfung ein neutrales Element? Ist diese Verknüpfung assoziativ, kommutativ, gibt es zu jedem Element ein inverses Element?

Aufgabe 1.2. Zeige, dass die Verknüpfung auf einer Geraden, die zwei Punkten ihren Mittelpunkt zuordnet, kommutativ, aber nicht assoziativ ist. Gibt es ein neutrales Element?

Aufgabe 1.3. Man untersuche die Verknüpfung

$$\mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0},\ (x,y) \longmapsto \min(x,y),$$

auf Assoziativität, Kommutativität, die Existenz von einem neutralen Element und die Existenz von inversen Elementen.

Aufgabe 1.4. Es sei S eine Menge und

$$M = \text{Abb}\ (S,S)$$

sei versehen mit der Hintereinanderschaltung von Abbildungen als Verknüpfung. Ist die Verknüpfung assoziativ, kommutativ, gibt es ein (eindeutiges) neutrales Element, für welche $F \in M$ gibt es ein inverses Element?

Aufgabe 1.5. Es sei S eine Menge und

$$G = \{F : S \to S |\, F \text{ bijektiv}\}.$$

Zeige, dass G mit der Hintereinanderschaltung von Abbildungen eine Gruppe ist.

Aufgabe 1.6. Sei M eine Menge und sei $f : M \to M$ eine Abbildung. Zeige, dass f genau dann injektiv ist, wenn f ein Linksinverses besitzt, und dass f genau dann surjektiv ist, wenn f ein Rechtsinverses besitzt.

Aufgabe 1.7. Es sei $(M, \circ, e)$ ein Monoid.

a) Folgt aus $x = y$ die Beziehung $a \circ x = a \circ y$?

b) Folgt aus $a \circ x = a \circ y$ die Beziehung $x = y$?

Aufgabe 1.8.*

Sei G eine Gruppe. Zeige, dass

$$\left(x^{-1}\right)^{-1} = x$$

für alle $x \in G$ ist.

Aufgabe 1.9. Sei G eine Gruppe und $x, y \in G$. Drücke das Inverse von xy durch die Inversen von x und y aus.

Aufgabe 1.10. Man gebe ein Beispiel eines endlichen Monoids M und eines Elementes $m \in M$ derart, dass alle positiven Potenzen von m vom neutralen Element verschieden sind.

Aufgabe 1.11. Es sei M ein endliches Monoid. Es gelte die folgende „Kürzungsregel“: aus $ax = ay$ folgt $x = y$. Zeige, dass M eine Gruppe ist.

Aufgabe 1.12. Man konstruiere eine Gruppe mit drei Elementen.

Aufgabe 1.13. Sei G eine Gruppe und $x \in G$ ein Element. Beweise durch Induktion unter Verwendung der Lemma 1.6, dass für $m, n \in \mathbb{Z}$ gilt:

$$x^{mn} = (x^m)^n \,.$$

Aufgabe 1.14.*

Beweise das folgende *Untergruppenkriterium.*Eine nichtleere Teilmenge $H \subseteq G$ einer Gruppe G ist genau dann eine Untergruppe, wenn gilt:

$$\text{für alle } g, h \in H \text{ ist } gh^{-1} \in H \,.$$

Aufgabe 1.15. Es sei G eine Gruppe und $H_i \subseteq G$, $i \in I$, eine Familie von Untergruppen. Zeige, dass der Durchschnitt

$$\bigcap_{i \in I} H_i$$

eine Untergruppe von G ist.

Aufgabe 1.16. Wir betrachten rationale Zahlen als gemischte Brüche.

a) Zeige, dass bei der Addition von zwei positiven gemischten Brüchen der Bruchterm der Summe nur von den Bruchtermen der Summanden abhängt.

b) Wie sieht dies mit dem ganzen Teil aus?

c) Wie sieht dies für beliebige rationale Zahlen aus?

Aufgabe 1.17. Wir betrachten die Menge

$$M \;=\; \{q \in \mathbb{Q} |\, 0 \leq q < 1\}$$

Zeige, dass auf M durch

$$a \oplus b := \begin{cases} a+b, \text{ falls } a+b < 1\,, \\ a+b-1 \text{ sonst}\,. \end{cases}$$

eine wohldefinierte Verknüpfung gegeben ist.

Aufgabe 1.18. Wir betrachten die Menge

$$M \;=\; \{q \in \mathbb{Q} |\, 0 \leq q < 1\}$$

mit der in Aufgabe 1.17 definierten Verknüpfung.

a) Berechne

$$\left(\left(\left(\left(\frac{4}{5} \oplus \frac{3}{4}\right) \oplus \frac{2}{3}\right) \oplus \frac{5}{7}\right) \oplus \frac{1}{3}\right)\,.$$

b) Finde eine Lösung für die Gleichung

$$\frac{3}{5} \oplus x \;=\; \frac{1}{2}.$$

Aufgaben zum Abgeben

Aufgabe 1.19. (3 Punkte)

Sei $n \in \mathbb{N}_+$ und betrachte auf

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$$

die Verknüpfung

$$a + b := (a+b) \mod n = \begin{cases} a+b \text{ falls } a+b < n \\ a+b-n \text{ falls } a+b \geq n\,. \end{cases}$$

Zeige, dass dadurch eine assoziative Verknüpfung auf dieser Menge definiert ist, und dass damit sogar eine Gruppe vorliegt.

Aufgabe 1.20. (4 Punkte)

Zeige, dass die Menge

$$M = \{q \in \mathbb{Q} | \, 0 \leq q < 1\}$$

mit der in Aufgabe 1.17 definierten Verknüpfung eine kommutative Gruppe ist.

Aufgabe 1.21. (2 Punkte)

Man untersuche die Verknüpfung

$$\mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}, \, (x, y) \longmapsto \max(x, y),$$

auf Assoziativität, Kommutativität, die Existenz von einem neutralen Element und die Existenz von inversen Elementen.

Aufgabe 1.22. (3 Punkte)

Sei M eine Menge mit einer assoziativen Verknüpfung. Es gebe ein *linksneutrales Element* e (d.h. $ex = x$ für alle $x \in M$) und zu jedem $x \in M$ gebe es ein *Linksinverses*, d.h. ein Element y mit $yx = e$. Zeige, dass dann M schon eine Gruppe ist.

Aufgabe 1.23. (2 Punkte)

Betrachte die Gruppe der Drehungen am Kreis um Vielfache des Winkels $\alpha = 360/12 = 30$ Grad. Welche Drehungen sind Erzeuger dieser Gruppe?

2. Vorlesung - Ringe

Ringe

Die wichtigsten mathematischen Strukturen wie $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ besitzen nicht nur eine, sondern zwei Verknüpfungen.

Definition 2.1. Ein *Ring* R ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist eine abelsche Gruppe.
(2) $(R, \cdot, 1)$ ist ein Monoid.
(3) Es gelten die *Distributivgesetze*, also $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

Definition 2.2. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

In einem kommutativen Ring muss man nicht zwischen den beiden Formen des Distributivgesetzes unterscheiden. Das Basismodell für einen (kommutativen) Ring bildet die Menge der ganzen Zahlen $\mathbb{Z}$ mit der natürlichen Addition und Multiplikation. Die 0 ist das neutrale Element der Addition und die 1 ist das neutrale Element der Multiplikation. Der Nachweis, dass $\mathbb{Z}$ die Axiome eines Ringes, also die oben aufgelisteten Eigenschaften, erfüllt, beruht letztlich auf den Peano-Axiomen für die natürlichen Zahlen $\mathbb{N}$ und ist ziemlich formal. Darauf wollen wir verzichten und stattdessen diese seit langem vertrauten Gesetzmäßigkeiten akzeptieren.

Die natürlichen Zahlen bilden keinen Ring, da sie noch nicht einmal eine additive Gruppe bilden. Die Zahlbereiche $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind ebenfalls kommutative Ringe, wobei der Nachweis der Eigenschaften dadurch geschieht, dass man die Konstruktion dieser Zahlbereiche aus den „vorhergehenden“ betrachtet (etwa $\mathbb{R}$ aus $\mathbb{Q}$) und die Gültigkeit (in $\mathbb{R}$) auf die Gültigkeit im „Vorgänger“ ($\mathbb{Q}$) zurückführt.

Wir benutzen allgemein die *Klammerkonvention*, dass Punktrechnung stärker bindet als Strichrechnung, d.h. wir schreiben einfach $ab+cd$ statt $(ab)+(cd)$. Das Inverse zu $a \in R$ bezüglich der Addition, das es ja immer gibt, schreiben wir als $-a$ und nennen es das *Negative* von a. Statt $a + (-b)$ schreiben wir $a-b$. An weiteren Notationen verwenden wir für ein Ringelement $a \in R$ und eine natürliche Zahl $n \in \mathbb{N}$ die Schreibweisen $na = a+\cdots+a$ (n Summanden) und $a^n = a \cdots a$ (n Faktoren). Bei einem negativen $n \in \mathbb{Z}$ ist $na = (-n)(-a)$ zu interpretieren (dies beruht auf den „Potenzgesetzen“ in einer Gruppe aus der ersten Vorlesung, wobei hier die Gruppe additiv geschrieben wird und deshalb Vielfache genommmen werden) (dagegen macht a^n mit negativen Exponenten im Allgemeinen keinen Sinn). Statt $n1 = n1_R$ schreiben wir einfach n (bzw. manchmal n_R), d.h. jede ganze Zahl findet sich in jedem Ring wieder.

Beispiel 2.3. Die einelementige Menge $R = \{0\}$ kann man zu einem Ring machen, indem man sowohl die Addition als auch die Multiplikation auf die einzig mögliche Weise erklärt, nämlich durch $0 + 0 = 0$ und $0 \cdot 0 = 0$. In diesem Fall ist $1 = 0$, dies ist also ausdrücklich erlaubt. Diesen Ring nennt man den *Nullring*.

Nach dem Nullring ist der folgende Ring der zweitkleinste Ring.

Beispiel 2.4. Wir suchen nach einer Ringstruktur auf der Menge $\{0, 1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element der Multiplikation sein soll, so ist dadurch schon alles festgelegt, da $1 + 1 = 0$ sein muss. Die Operationstafeln sehen also wie folgt aus.

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Durch etwas aufwändiges Nachrechnen stellt man fest, dass es sich in der Tat um einen kommutativen Ring handelt (sogar um einen Körper).

Eine „natürliche“ Interpretation dieses Ringes gewinnt man, wenn man sich die geraden ganzen Zahlen durch 0 und die ungeraden ganzen Zahlen durch 1 repräsentiert denkt. Beispielsweise ist die Summe zweier ungerader Zahlen stets gerade, was der obigen Gleichung $1 + 1 = 0$ entspricht.

Zu jeder natürlichen Zahl $n \in \mathbb{N}$ kann man einen kommutativen Ring $\mathbb{Z}/(n)$ definieren, nämlich als die Menge $\{0, 1, 2, \ldots, n-2, n-1$, wobei die Addition und die Multiplikation zuerst in $\mathbb{N}$ ausgeführt wird und davon der Rest bei Division durch n genommen wird. Die exakte Durchführung dieser Konstruktion und der Nachweis der Ringeigenschaften verschieben wir auf später, es ist aber sinnvoll, diese (verglichen mit $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) untypischen Ringe schon jetzt zur Verfügung zu haben. Der obige Ring mit zwei Elementen ist beispielsweise gleich $\mathbb{Z}/(2)$.

Lemma 2.5. *Sei R ein Ring und seien $a, b, c, a_1, \ldots, a_r, b_1, \ldots, b_s$ Elemente aus R. Dann gelten folgende Aussagen*

(1) $0a = a0 = 0$ *(*Annullationsregel*),*
(2) $a(-b) = -(ab) = (-a)b$
(3) $(-a)(-b) = ab$ *(*Vorzeichenregel*),*
(4) $a(b-c) = ab - ac$ *und* $(b-c)a = ba - ca$*,*
(5) $(\sum_{i=1}^{r} a_i)\,(\sum_{k=1}^{s} b_k) = \sum_{1 \le i \le r,\, 1 \le k \le s} a_i b_k$ *(*allgemeines Distributivgesetz*).*

Beweis. Wir beweisen im nicht kommutativen Fall je nur eine Hälfte.

(1) Es ist $a0 = a(0+0) = a0 + a0$. Durch beidseitiges Abziehen von $a0$ ergibt sich die Behauptung.
(2)
$$(-a)b + ab = (-a+a)b = 0b = 0$$
nach Teil (1). Daher ist $(-a)b$ das (eindeutig bestimmte) Negative von ab.
(3) Nach (2) ist $(-a)(-b) = (-(-a))b$ und wegen $-(-a) = a$ (dies gilt in jeder Gruppe) folgt die Behauptung.
(4) Dies folgt auch aus dem bisher Bewiesenen.
(5) Dies folgt aus einer einfachen Doppelinduktion.

□

Die Binomialkoeffizienten

Die *erste binomische Formel* besagt bekanntlich

$$(a+b)^2 \;=\; a^2 + 2ab + b^2.$$

Für die dritte Potenz einer Summe gilt

$$(a+b)^3 \;=\; a^3 + 3a^2b + 3ab^2 + b^3$$

und für die vierte Potenz

$$(a+b)^4 \;=\; a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

In dieser Weise kann man jede Potenz einer Summe als Summe von Produkten ausdrücken, wobei die auftretenden Koeffizienten *Binomialkoeffizienten* heißen. Diese werden mit Hilfe der Fakultät definiert, wobei die Fakultät $n!$ einer natürlichen Zahl durch

$$n! \;=\; n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$

definiert ist.

Definition 2.6. Es seien k und n natürliche Zahlen mit $k \leq n$. Dann nennt man

$$\binom{n}{k} \;=\; \frac{n!}{k!(n-k)!}$$

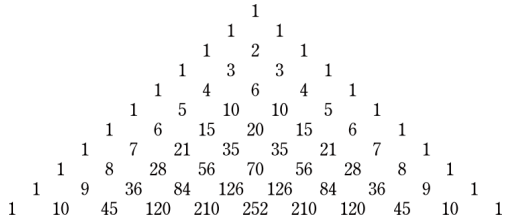
den *Binomialkoeffizienten* „n über k“.

Diesen Bruch kann man auch als

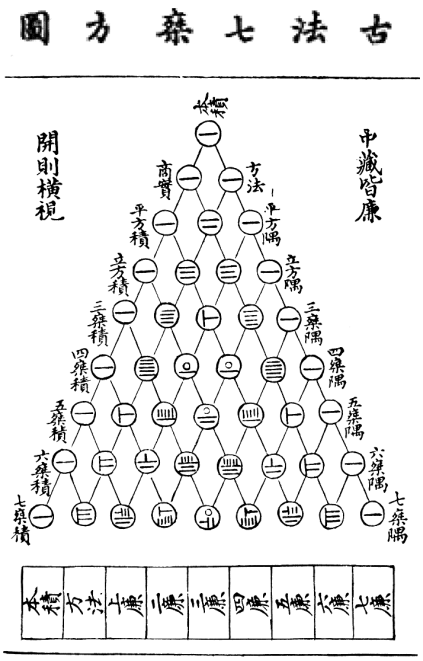
$$\frac{n(n-1)(n-2)\cdots(n-k+2)(n-k+1)}{k(k-1)(k-2)\cdots 2 \cdot 1}$$

schreiben, da die Faktoren aus $(n-k)!$ auch in $n!$ vorkommen und daher kürzbar sind. In dieser Darstellung stehen im Zähler und im Nenner gleich viele Faktoren. Gelegentlich ist es sinnvoll, auch negative k oder $k > n$ zuzulassen und in diesen Fällen die Binomialkoeffizienten gleich 0 zu setzen.

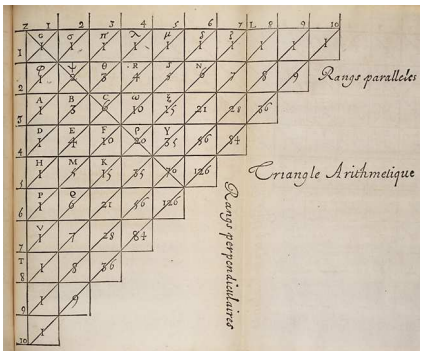
Von der Definition her ist es nicht sofort klar, dass es sich bei den Binomialkoeffizienten um natürliche Zahlen handelt. Dies folgt aus der folgenden Beziehung.



Das *Dreieck der Binomialkoeffizienten* war in Indien und in Persien schon um 1000 bekannt,



in China heißt es *Yanghui-Dreieck* (nach Yang Hui (um 1238-1298)),



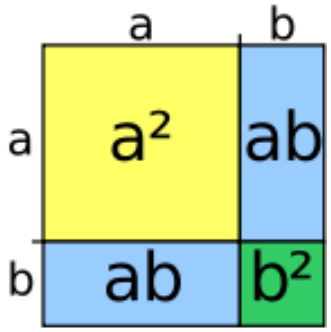
in Europa heißt es das *Pascalsche Dreieck* (nach Blaise Pascal (1623-1662)).

Lemma 2.7. *Die Binomialkoeffizienten erfüllen die rekursive Beziehung*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Beweis. Siehe Aufgabe 2.7. □

Der Binomialkoeffizient $\binom{n}{k}$ hat die folgende inhaltliche Bedeutung: Er gibt für eine n-elementige Menge M die Anzahl sämtlicher k-elementigen Teilmengen von M an, siehe Aufgabe 2.8. Wenn $k > n$ ist oder wenn k negativ ist so setzt man den Binomialkoeffizienten gleich null.



Die folgende *allgemeine binomische Formel* bringt die Addition und die Multiplikation in einem kommutativen Ring miteinander in Beziehung.

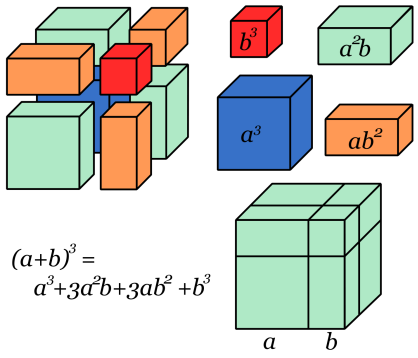
Satz 2.8. *Es sei R ein kommutativer Ring und $a, b \in R$. Ferner sei n eine natürliche Zahl. Dann gilt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} .$$

Beweis. Wir führen Induktion nach n. Für $n = 0$ steht einerseits $(a+b)^0 = 1$ und andererseits $a^0 b^0 = 1$. Sei die Aussage bereits für n bewiesen. Dann ist

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= a\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) + b\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=1}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\end{aligned}$$

□



Nichtnullteiler und Integritätsbereiche

Definition 2.9. Ein Element a in einem kommutativen Ring R heißt *Nullteiler*, wenn es ein von 0 verschiedenes Element b mit $ab = 0$ gibt. Andernfalls heißt es ein *Nichtnullteiler*.

Die Eins ist stets ein Nichtnullteiler, da aus $1b = 0$ sofort $b = 0$ folgt. Andererseits ist das Nullelement stets ein Nullteiler, es sei denn, der Nullring liegt vor. In $\mathbb{Z}/(6)$ gilt $2 \cdot 3 = 0$ und daher sind 2 und 3 Nullteiler in diesem Ring. Die folgende Aussage bedeutet, dass man in einer Gleichung Nichtnullteiler weg*kürzen* kann.

Lemma 2.10. *Es sei R ein kommutativer Ring und sei $f \in R$ ein Nichtnullteiler. Dann folgt aus einer Gleichung*

$$fx = fy\,,$$

dass $x = y$ sein muss.

Beweis. Man kann die Gleichung zu

$$0 = fx - fy = f(x - y).$$

umschreiben. Da f ein Nichtnullteiler ist, ist $x - y = 0$, also $x = y$. □

Ein Ring, bei dem es außer der Null keine Nullteiler gibt, heißt *nullteilerfrei*.

Definition 2.11. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Die Eigenschaft, dass jedes Element $\neq 0$ ein Nichtnullteiler ist, kann man auch so ausdrücken, dass aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt, bzw., dass mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ ist.

Unterringe

Wir haben die Kette von Unterringen

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

im Sinne der folgenden Definition.

Definition 2.12. Eine Teilmenge $S \subseteq R$ eines Ringes nennt man einen *Unterring*, wenn sowohl $(S, +, 0)$ eine Untergruppe von $(R, +, 0)$ als auch $(S, \cdot, 1)$ ein Untermonoid von $(R, \cdot, 1)$ ist.

Diese Bedingung besagt insbesondere, dass sich die Addition und die Multiplikation von R auf S einschränken lässt. Ein Unterring ist selbst ein Ring. Zum Nachweis, dass eine gegebene Teilmenge $S \subseteq R$ ein Unterring ist, hat man Folgendes zu zeigen.

(1) $0, 1 \in S$.
(2) S ist abgeschlossen unter der Addition und der Multiplikation.
(3) Mit $f \in S$ ist auch $-f \in S$.

Die natürlichen Zahlen $\mathbb{N}$ erfüllen in $\mathbb{Z}$ die ersten beiden Bedingungen, aber nicht die dritte. Die Menge aller geraden Zahlen erfüllen alle Bedingungen außer der, dass 1 dazugehört. Ebenso ist $\{0\}$ kein Unterring, da darin die 1 fehlt (obwohl im Nullring für sich betrachtet $0 = 1$ ist, das ist aber nicht die 1 von $\mathbb{Z}$). Die Menge $\{-1, 0, 1\}$ erfüllt die erste und die dritte Bedingung und ist abgeschlossen unter der Multiplikation, aber nicht unter der Addition. Die ganzen Zahlen $\mathbb{Z}$ haben überhaupt nur sich selbst als Unterring.

Zu einer Teilmenge $M \subseteq R$ eines Ringes definiert man den durch M *erzeugten Unterring* als den kleinsten Unterring von R, der M umfasst. Wir bezeichnen ihn mit $\mathbb{Z}[M]$, da ja jeder Unterring automatisch alle Vielfachen der 1 enthalten muss. Dieser kleinste Unterring ist der Durchschnitt über alle Unterringe, die M umfassen. Er besteht aus allen Termen, die man mit den Elementen aus M und ihren Negativen mit Addition und Multiplikation erhalten kann.

2. Arbeitsblatt

Übungsaufgaben

Aufgabe 2.1. Zeige, dass ein Ring mit $0 = 1$ der Nullring ist.

Aufgabe 2.2. Zeige, dass es keinen echten Zwischenring zwischen $\mathbb{R}$ und $\mathbb{C}$ gibt.

Aufgabe 2.3. Formuliere und beweise das allgemeine Distributivitätsgesetz für einen Ring.

Aufgabe 2.4. Sei R ein Ring und seien $\spadesuit, \heartsuit$ und $\clubsuit$ Elemente in R. Berechne das Produkt

$$(\spadesuit^2 - 3\heartsuit\clubsuit\heartsuit - 2\clubsuit\heartsuit^2 + 4\spadesuit\heartsuit^2)(2\spadesuit\heartsuit^3\spadesuit - \clubsuit^2\spadesuit\heartsuit\spadesuit)(1 - 3\clubsuit\heartsuit\spadesuit\clubsuit^2\heartsuit)\,.$$

Wie lautet das Ergebnis, wenn der Ring kommutativ ist?

Aufgabe 2.5. Es sei R ein kommutativer Ring und $f, a_i, b_j \in R$. Zeige die folgenden Gleichungen:

$$\sum_{i=0}^{n} a_i f^i + \sum_{j=0}^{m} b_j f^j = \sum_{k=0}^{\max(n,m)} (a_k + b_k) f^k$$

und

$$\sum_{i=0}^{n} a_i f^i \cdot \sum_{j=0}^{m} b_j f^j = \sum_{k=0}^{n+m} c_k f^k \text{ mit } c_k = \sum_{r=0}^{n} a_r b_{k-r}\,.$$

Aufgabe 2.6. Formuliere die *binomischen Formeln* für zwei reelle Zahlen und beweise die Formeln mit Hilfe des Distributivgesetzes.

Aufgabe 2.7.*

Zeige, dass die Binomialkoeffizienten die rekursive Bedingung

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

erfüllen.

Man mache sich dies auch für $k < 0$ und $k \geq n$ klar.

Aufgabe 2.8.*

Es sei M eine n-elementige Menge. Zeige, dass die Anzahl der k-elementigen Teilmengen von M gleich dem Binomialkoeffizienten

$$\binom{n}{k}$$

ist.

Aufgabe 2.9. Sei R ein Ring und M eine Menge. Definiere auf der Abbildungsmenge

$$A = \{f : M \to R | \, f \text{ Abbildung}\}$$

eine Ringstruktur.

Aufgabe 2.10. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 2.11. Sei R ein Ring und seien $S_i \subseteq R$, $i \in I$, Unterringe. Zeige, dass dann auch der Durchschnitt $\bigcap_{i \in I} S_i$ ein Unterring von R ist.

Aufgaben zum Abgeben

Aufgabe 2.12. (3 Punkte)

Sei M eine Menge. Zeige, dass die Potenzmenge $\mathfrak{P}(M)$ mit dem Durchschnitt $\cap$ als Multiplikation und der symmetrischen Differenz $A \triangle B = (A \setminus B) \cup (B \setminus A)$ als Addition ein kommutativer Ring ist.

Aufgabe 2.13. (4 Punkte)

Beweise die Formel

$$n2^{n-1} = \sum_{k=0}^{n} k \binom{n}{k}.$$

Aufgabe 2.14. (3 Punkte)

Bestimme die Nullteiler und die Nichtnullteiler in $\mathbb{Z}/(12)$.

Die nächste Aufgabe verwendet den Begriff des *nilpotenten* Elementes in einem Ring.

Ein Element a eines Ringes R heißt *nilpotent*, wenn $a^n = 0$ ist für eine natürliche Zahl n.

Aufgabe 2.15. (2 Punkte)

Es sei R ein kommutativer Ring und es seien $f, g \in R$ nilpotente Elemente. Zeige, dass dann die Summe $f + g$ ebenfalls nilpotent ist.

Aufgabe 2.16. (2 Punkte)

Es sei $n \in \mathbb{N}_+$ eine fixierte positive natürliche Zahl. Zeige, dass die Menge aller rationalen Zahlen, die man mit einer Potenz von n als Nenner schreiben kann, einen Unterring von $\mathbb{Q}$ bildet.

Aufgabe 2.17. (3 Punkte)

Es sei $R = \mathbb{Z}[\frac{2}{3}]$ der von $\mathbb{Z}$ und $2/3$ erzeugte Unterring von $\mathbb{Q}$. Zeige, dass R alle rationalen Zahlen enthält, die sich mit einer Potenz von 3 im Nenner schreiben lassen.

3. Vorlesung - Körper

In dieser Vorlesung besprechen wir Körper, das sind kommutative Ringe, in denen jedes von 0 verschiedene Element ein Inverses (bezüglich der Multiplikation) besitzt. Solche Elemente nennt man Einheiten. Als einen wichtigen Körper führen wir die komplexen Zahlen ein.

Einheiten

Definition 3.1. Ein Element u in einem Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit

$$uv = vu = 1$$

gibt.

Das Element v mit der Eigenschaft $uv = vu = 1$ ist dabei eindeutig bestimmt. Hat nämlich auch w die Eigenschaft $uw = wu = 1$, so ist

$$v = v1 = v(uw) = (vu)w = 1w = w.$$

Das im Falle der Existenz eindeutig bestimmte v mit $uv = vu = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit

$$u^{-1}$$

oder auch mit $\frac{1}{u}$. Im kommutativen Fall muss man natürlich nur die Eigenschaft $uv = 1$ überprüfen. Eine Einheit ist stets ein Nichtnullteiler. Aus $ux = 0$ folgt ja sofort (unter Verwendung von Lemma 2.5 (1)) $x = u^{-1}ux = 0$.

Definition 3.2. Die *Einheitengruppe* in einem Ring R ist die Teilmenge aller Einheiten in R. Sie wird mit $R^\times$ bezeichnet.

Die Menge aller Einheiten in einem Ring bilden in der Tat eine Gruppe (bezüglich der Multiplikation mit 1 als neutralem Element). Wenn nämlich v und w die Inversen v^{-1} und w^{-1} haben, so ist das Inverse von vw gleich $w^{-1}v^{-1}$ und somit ist das Produkt von zwei Einheiten wieder eine Einheit.

Zu einer Einheit $u \in R$ machen auch Potenzen mit einem negativen Exponenten Sinn, d.h. es ist dann u^n für alle $n \in \mathbb{Z}$ definiert. Die Zahl -1 (also das Negative zu 1) ist stets eine Einheit, da ja (nach Lemma 2.5 (3)) $(-1)(-1) = 1$ ist. Bei $\mathbb{Z}$ besteht die Einheitengruppe aus diesen beiden Elementen, also $\mathbb{Z}^\times = \{1, -1\}$. Die Null ist mit der Ausnahme des Nullrings nie eine Einheit.

Beispiel 3.3. Wir betrachten den Ring $\mathbb{Z}/(5)$. Die Elemente 1 und $4 = -1$ sind wie in jedem Ring Einheiten. Wegen

$$2 \cdot 3 \; = \; 6 \; = \; 1$$

sind 2 und 3 invers zueinander und insbesondere Einheiten. Die Einheitengruppe ist also $\{1, 2, 3, 4\} = \mathbb{Z}/(5) \setminus \{0\}$.

Bei $\mathbb{Z}/(12)$ sind wieder 1 und $11 = -1$ Einheiten. Ferner sind wegen

$$5 \cdot 5 \; = \; 25 \; = \; 1$$

und

$$7 \cdot 7 \; = \; 49 \; = \; 1$$

auch 5 und 7 Einheiten. Die anderen acht Zahlen sind keine Einheiten.

Für eine Einheit ist auch die *Bruchschreibweise* erlaubt und gebräuchlich. D.h. wenn u eine Einheit ist und $x \in R$ beliebig, so setzt man

$$\frac{x}{u} = xu^{-1} \, .$$

Wie gesagt, der Nenner muss eine Einheit sein!

Wenn außer der Null alle Elemente Einheiten sind, so verdient das einen eigenen Namen, wovon der folgende Abschnitt handelt.

Körper

Viele wichtige Zahlbereiche wie $\mathbb{Q}$ und $\mathbb{R}$ haben die Eigenschaft, dass man durch jede Zahl - mit der Ausnahme der Null! - auch dividieren darf. Dies wird durch den Begriff des Körpers präzisiert.

Definition 3.4. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Es wird also explizit gefordert, dass $1 \neq 0$ ist und dass jedes von 0 verschiedene Element eine Einheit ist. Die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ bilden einen Körper, die ganzen Zahlen dagegen nicht. Im obigen Beispiel haben wir gesehen, dass $\mathbb{Z}/(5)$ ein Körper ist, aber $\mathbb{Z}/(12)$ nicht. Wir werden im Laufe dieser Vorlesung noch viele weitere Körper kennenlernen. Einen Körper kann man auch charakterisieren als einen kommutativen Ring, bei der die von 0 verschiedenen Elemente eine Gruppe (mit der Multiplikation) bilden.

Definition 3.5. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

Beispielsweise ist $\mathbb{Q}$ ein Unterkörper von $\mathbb{R}$. Wenn ein Unterring $R \subseteq K$ in einem Körper vorliegt, so muss man nur noch schauen, ob R mit jedem von null verschiedenen Element x auch das Inverse x^{-1} (das in K existiert) enthält. Bei einem Unterring $R \subseteq S$, wobei R ein Körper ist, aber S nicht, so spricht man nicht von einem Unterkörper. Die Situation, wo ein Körper in einem anderen Körper liegt, wird als Körpererweiterung bezeichnet.

Definition 3.6. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Komplexe Zahlen

Die Produktmenge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ ist mit komponentenweiser Addition und komponentenweiser Multiplikation ein kommutativer Ring (wobei $(0,0)$ das Nullelement und $(1,1)$ das Einselement ist). Es handelt sich aber nicht um einen Körper, da beispielsweise $(1,0) \cdot (0,1) = (0,0)$ zeigt, dass es darin Nullteiler gibt. Allerdings kann man $\mathbb{R}^2$ mit einer anderen Multiplikation zu einem Körper machen.

Definition 3.7. Die Menge

$$\mathbb{R}^2$$

mit $0 := (0,0)$ und $1 := (1,0)$, mit der komponentenweisen Addition und der durch

$$(a,b) \cdot (c,d) := (ac - bd, ad + bc)$$

definierten Multiplikation nennt man *Körper der komplexen Zahlen*. Er wird mit

$$\mathbb{C}$$

bezeichnet.

Die Addition ist also einfach die vektorielle Addition im $\mathbb{R}^2$, während die Multiplikation eine neuartige Verknüpfung ist, die zwar numerisch einfach durchführbar ist, an die man sich aber dennoch gewöhnen muss.

Lemma 3.8. *Die komplexen Zahlen bilden einen Körper.*

Beweis. Siehe Aufgabe 3.11. □

Hierbei sind nur das Assoziativgesetz, das Distibutivgesetz und die Existenz der Inversen nicht unmittelbar klar.

Wir lösen uns von der Paarschreibweise und schreiben

$$a + bi := (a,b).$$

Insbesondere ist $i = (0, 1)$, diese Zahl heißt *imaginäre Einheit*. Diese Zahl hat die wichtige Eigenschaft

$$i^2 = -1.$$

Aus dieser Eigenschaft ergeben sich sämtliche algebraischen Eigenschaften der komplexen Zahlen durch die Körpergesetze. So kann man sich auch die obige Multiplikationsregel merken, es ist ja

$$(a+bi)(c+di) = ac+adi+bic+bidi = ac+bdi^2+(ad+bc)i = ac-bd+(ad+bc)i.$$

Wir fassen eine reelle Zahl a als die komplexe Zahl $a + 0i = (a, 0)$ auf. In diesem Sinne ist $\mathbb{R} \subset \mathbb{C}$ eine Körpererweiterung. Es ist gleichgültig, ob man zwei reelle Zahlen als reelle Zahlen oder als komplexe Zahlen addiert oder multipliziert.

Definition 3.9. Zu einer komplexen Zahl

$$z = a + bi$$

heißt

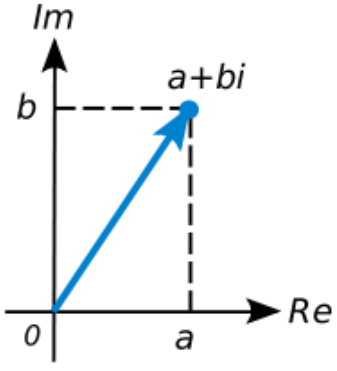
$$\mathrm{Re}\,(z) = a$$

der *Realteil* von z und

$$\mathrm{Im}\,(z) = b$$

heißt der *Imaginärteil* von z.

Man sollte sich allerdings die Menge der komplexen Zahlen nicht als etwas vorstellen, das weniger real als andere Zahlensysteme ist. Die Konstruktion der komplexen Zahlen aus den reellen Zahlen ist bei Weitem einfacher als die Konstruktion der reellen Zahlen aus den rationalen Zahlen. Allerdings war es historisch ein langer Prozess, bis die komplexen Zahlen als Zahlen anerkannt wurden; das Irreale daran ist, dass sie einen Körper bilden, der nicht angeordnet werden kann, und dass es sich daher scheinbar um keine Größen handelt, mit denen man sinnvollerweise etwas messen kann.



Man kann sich die komplexen Zahlen als die Punkte in einer Ebene vorstellen; für die additive Struktur gilt ja einfach $\mathbb{C} = \mathbb{R}^2$. In diesem Zusammenhang spricht man von der *Gaussschen Zahlenebene*. Die horizontale Achse nennt man dann die *reelle Achse* und die vertikale Achse die *imaginäre Achse*.

Lemma 3.10. *Real- und Imaginärteil von komplexen Zahlen erfüllen folgende Eigenschaften (für z und w aus $\mathbb{C}$).*

(1) $z = \mathrm{Re}\,(z) + \mathrm{Im}\,(z)\,i$.
(2) $\mathrm{Re}\,(z+w) = \mathrm{Re}\,(z) + \mathrm{Re}\,(w)$.
(3) $\mathrm{Im}\,(z+w) = \mathrm{Im}\,(z) + \mathrm{Im}\,(w)$.
(4) *Für $r \in \mathbb{R}$ ist*

$$\mathrm{Re}\,(rz) = r\,\mathrm{Re}\,(z) \;\; \textit{und} \;\; \mathrm{Im}\,(rz) = r\,\mathrm{Im}\,(z)\ .$$

(5) *Es ist $z = \mathrm{Re}\,(z)$ genau dann, wenn $z \in \mathbb{R}$ ist, und dies ist genau dann der Fall, wenn $\mathrm{Im}\,(z) = 0$ ist.*

Beweis. Siehe Aufgabe 3.16. □

Definition 3.11. Die Abbildung

$$\mathbb{C} \longrightarrow \mathbb{C},\ z = a + bi \longmapsto \overline{z} := a - bi,$$

heißt *komplexe Konjugation*.

Zu z heißt $\overline{z}$ die *konjugiert-komplexe Zahl* von z. Geometrisch betrachtet ist die komplexe Konjugation zu $z \in \mathbb{C}$ einfach die Achsenspiegelung an der reellen Achse.

Lemma 3.12. *Für die komplexe Konjugation gelten die folgenden Rechenregeln (für beliebige $z, w \in \mathbb{C}$).*

(1) $\overline{z+w} = \overline{z} + \overline{w}$.
(2) $\overline{-z} = -\overline{z}$.
(3) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
(4) *Für $z \neq 0$ ist* $\overline{1/z} = 1/\overline{z}$.
(5) $\overline{\overline{z}} = z$.
(6) $\overline{z} = z$ *genau dann, wenn $z \in \mathbb{R}$ ist.*

Beweis. Siehe Aufgabe 3.24. □

Das Quadrat d^2 einer reellen Zahl ist stets nichtnegativ, und die Summe von zwei nichtnegativen reellen Zahlen ist wieder nichtnegativ. Zu einer nichtnegativen reellen Zahl c gibt es eine eindeutige nichtnegative *Quadratwurzel* $\sqrt{c}$. Daher liefert folgende Definition eine wohldefinierte nichtnegative reelle Zahl.

Definition 3.13. Zu einer komplexen Zahl

$$z = a + bi$$

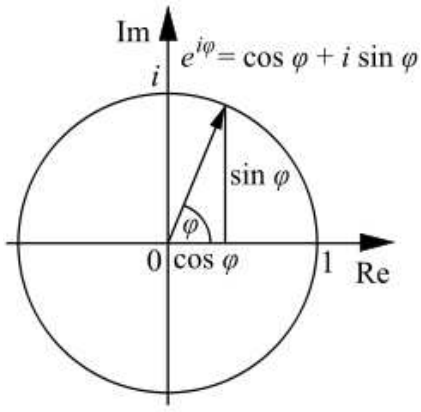
ist der *Betrag* durch

$$|z| = \sqrt{a^2 + b^2}$$

definiert.

Der Betrag einer komplexen Zahl z ist aufgrund des *Satzes des Pythagoras* der Abstand von z zum Nullpunkt $0 = (0, 0)$. Insgesamt ist der Betrag eine Abbildung

$$\mathbb{C} \longrightarrow \mathbb{R}_{\geq 0},\ z \longmapsto |z|\,.$$



Die Menge aller komplexen Zahlen mit einem bestimmten Betrag bilden einen Kreis mit dem Nullpunkt als Mittelpunkt und mit dem Betrag als Radius. Insbesondere bilden alle komplexen Zahlen mit dem Betrag 1 den *komplexen Einheitskreis*. Es sei hier erwähnt, dass das Produkt von zwei komplexen Zahlen auf dem Einheitskreis sich ergibt, indem man die zugehörigen Winkel, gemessen von der positiven reellen Achse aus gegen den Uhrzeigersinn, addiert.

Lemma 3.14. *Für eine komplexe Zahl z gelten die folgenden Beziehungen.*

(1) $|z| = \sqrt{z\ \overline{z}}$.
(2) $\text{Re}\ (z) = \frac{z+\overline{z}}{2}$.
(3) $\text{Im}\ (z) = \frac{z-\overline{z}}{2i}$.
(4) $\overline{z} = \text{Re}\ (z) - i\,\text{Im}\ (z)$.
(5) *Für $z \neq 0$ ist* $z^{-1} = \frac{\overline{z}}{|z|^2}$.

Beweis. Siehe Aufgabe 3.17. □

Lemma 3.15. *Für den Betrag von komplexen Zahlen gelten folgende Eigenschaften.*

(1) *Für reelles z stimmen reeller und komplexer Betrag überein.*
(2) *Es ist $|z| = 0$ genau dann, wenn $z = 0$ ist.*

(3) $|z| = |\overline{z}|$.
(4) $|zw| = |z|\,|w|$.
(5) $|\mathrm{Re}\,(z)|\,, |\mathrm{Im}\,(z)| \leq |z|$.
(6) $|z + w| \leq |z| + |w|$.
(7) *Für* $z \neq 0$ *ist* $|1/z| = 1/\,|z|$.

Beweis. Wir zeigen die Dreiecksungleichung, für die anderen Aussagen siehe Aufgabe 3.18. Zunächst gilt nach (5) für jede komplexe Zahl u die Abschätzung $\mathrm{Re}\,(u) \leq |u|$. Daher ist

$$\mathrm{Re}\,(z\overline{w}) \leq |z|\,|w|\,,$$

und somit ist

$$\begin{aligned} |z+w|^2 &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \\ &= |z|^2 + 2\,\mathrm{Re}\,(z\overline{w}) + |w|^2 \\ &\leq |z|^2 + 2\,|z|\,|w| + |w|^2 \\ &= (|z| + |w|)^2. \end{aligned}$$

Durch Wurzelziehen ergibt sich die gewünschte Abschätzung. □

3. Arbeitsblatt

Übungsaufgaben

Aufgabe 3.1. Es sei R ein kommutativer Ring mit Elementen $x, y, z, w \in R$, wobei z und w Einheiten seien. Beweise die folgenden Bruchrechenregeln.

(1)
$$\frac{x}{1} = x\,,$$

(2)
$$\frac{1}{x} = x^{-1}\,,$$

(3)
$$\frac{1}{-1} = -1\,,$$

(4)
$$\frac{0}{z} = 0\,,$$

(5)
$$\frac{z}{z} = 1\,,$$

(6)
$$\frac{x}{z} = \frac{xw}{zw}$$

(7)
$$\frac{x}{z} \cdot \frac{y}{w} = \frac{xy}{zw},$$

(8)
$$\frac{x}{z} \cdot \frac{y}{w} = \frac{xw + yz}{zw}.$$

Gilt die zu (8) analoge Formel, die entsteht, wenn man die Addition mit der Multiplikation vertauscht, also

$$(x - z) + (y - w) = (x + w)(y + z) - (z + w)\,?$$

Zeige, dass die „beliebte Formel“

$$\frac{x}{z} + \frac{y}{w} = \frac{x + y}{z + w}$$

nicht gilt, außer im Nullring.

Aufgabe 3.2.*

Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

$$\mu_f \colon R \longrightarrow R,\, g \longmapsto fg,$$

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 3.3. Zeige, dass ein Unterring eines Körpers ein Integritätsbereich ist.

Aufgabe 3.4. Zeige, dass in einem Körper das „umgekehrte Distributivgesetz“, also

$$a + (bc) \;=\; (a + b) \cdot (a + c),$$

nicht gilt.

Aufgabe 3.5. Es sei K ein Körper mit

$$2 \neq 0.$$

Zeige, dass für $f, g \in K$ die Beziehung

$$fg \;=\; \frac{1}{4}\left((f + g)^2 - (f - g)^2\right)$$

gilt.

Aufgabe 3.6. Zeige für einen Körper K die folgenden Eigenschaften.

(1) Für jedes $a \in K$ ist die Abbildung

$$\alpha_a \colon K \longrightarrow K,\, x \longmapsto x + a,$$

bijektiv.

(2) Für jedes $b \in K$, $b \neq 0$, ist die Abbildung

$$\mu_b \colon K \longrightarrow K,\, x \longmapsto bx,$$

bijektiv.

Aufgabe 3.7. Zeige, dass die einelementige Menge $\{0\}$ alle Körperaxiome erfüllt mit der einzigen Ausnahme, dass $0 = 1$ ist.

Bei den Rechenaufgaben zu den komplexen Zahlen muss das Ergebnis immer in der Form $a + bi$ mit reellen Zahlen a, b angegeben werden, wobei diese so einfach wie möglich sein sollen.

Aufgabe 3.8. Berechne die folgenden Ausdrücke innerhalb der komplexen Zahlen.

(1) $(5 + 4i)(3 - 2i)$.
(2) $(2 + 3i)(2 - 4i) + 3(1 - i)$.
(3) $(2i + 3)^2$.
(4) i^{1011}.
(5) $(-2 + 5i)^{-1}$.
(6) $\frac{4-3i}{2+i}$.

Aufgabe 3.9. Bestimme die inversen Elemente der folgenden komplexen Zahlen.

(1) 3.
(2) $5i$.
(3) $3 + 5i$.

Aufgabe 3.10. Zeige, dass für reelle Zahlen die Addition und die Multiplikation als reelle Zahlen und als komplexe Zahlen übereinstimmen.

Aufgabe 3.11. Zeige, dass die komplexen Zahlen einen Körper bilden.

Aufgabe 3.12. Zeige, dass $P = \mathbb{R}^2$ mit der komponentenweisen Addition und der komponentenweisen Multiplikation kein Körper ist.

Aufgabe 3.13. Skizziere die folgenden Teilmengen.

(1) $\{z \in \mathbb{C} |\ \mathrm{Re}\ (z) \geq -3\}$,
(2) $\{z \in \mathbb{C} |\ \mathrm{Im}\ (z) \leq 2\}$,
(3) $\{z \in \mathbb{C} |\ |z| \leq 5\}$.

Aufgabe 3.14.*

a) Berechne

$$(4 - 7i)(5 + 3i)\,.$$

b) Bestimme das inverse Element z^{-1} zu $z = 3 + 4i$.

c) Welchen Abstand hat z^{-1} aus Teil (b) zum Nullpunkt?

Aufgabe 3.15.*

Löse die lineare Gleichung

$$(2 + 5i)z \ = \ (3 - 7i)$$

über $\mathbb{C}$ und berechne den Betrag der Lösung.

Aufgabe 3.16. Beweise die folgenden Aussagen zu Real- und Imaginärteil von komplexen Zahlen.

(1) $z = \mathrm{Re}\ (z) + \mathrm{Im}\ (z)\, i$.
(2) $\mathrm{Re}\ (z + w) = \mathrm{Re}\ (z) + \mathrm{Re}\ (w)$.
(3) $\mathrm{Im}\ (z + w) = \mathrm{Im}\ (z) + \mathrm{Im}\ (w)$.
(4) Für $r \in \mathbb{R}$ ist

$$\mathrm{Re}\ (rz) = r\,\mathrm{Re}\ (z) \ \text{ und } \ \mathrm{Im}\ (rz) = r\,\mathrm{Im}\ (z)\ .$$

(5) $z = \mathrm{Re}\ (z)$ genau dann, wenn $z \in \mathbb{R}$ ist, und dies ist genau dann der Fall, wenn $\mathrm{Im}\ (z) = 0$ ist.

Aufgabe 3.17. Zeige, dass innerhalb der komplexen Zahlen folgende Rechenregeln gelten.

(1) $|z| = \sqrt{z\ \overline{z}}$.
(2) $\mathrm{Re}\ (z) = \frac{z+\overline{z}}{2}$.
(3) $\mathrm{Im}\ (z) = \frac{z-\overline{z}}{2i}$.
(4) $\overline{z} = \mathrm{Re}\ (z) - i\,\mathrm{Im}\ (z)$.
(5) Für $z \neq 0$ ist $z^{-1} = \frac{\overline{z}}{|z|^2}$.

Aufgabe 3.18. Zeige die folgenden Regeln für den Betrag von komplexen Zahlen.

(1) Für reelles z stimmen reeller und komplexer Betrag überein.
(2) Es ist $|z| = 0$ genau dann, wenn $z = 0$ ist.
(3) $|z| = |\overline{z}|$.
(4) $|zw| = |z|\,|w|$.
(5) $|\mathrm{Re}\,(z)|\,, |\mathrm{Im}\,(z)| \leq |z|$.
(6) Für $z \neq 0$ ist $|1/z| = 1/\,|z|$.

Aufgaben zum Abgeben

Aufgabe 3.19. (2 Punkte)

Bestimme die Einheiten von $\mathbb{Z}/(8)$.

Aufgabe 3.20. (3 Punkte)

Sei R ein kommutativer Ring mit endlich vielen Elementen. Zeige, dass R genau dann ein Integritätsbereich ist, wenn R ein Körper ist.

Aufgabe 3.21. (2 Punkte)

Es sei R ein kommutativer Ring und $f \in R$ ein nilpotentes Element. Zeige, dass $1 + f$ eine Einheit ist.

Aufgabe 3.22. (3 Punkte)

Berechne die komplexen Zahlen

$$(1+i)^n$$

für $n = 1, 2, 3, 4, 5$.

Aufgabe 3.23. (2 Punkte)

Löse die lineare Gleichung

$$(4-i)z \;=\; (6+5i)$$

über $\mathbb{C}$ und berechne den Betrag der Lösung.

Aufgabe 3.24. (3 Punkte)

Zeige, dass für die komplexe Konjugation die folgenden Rechenregeln gelten.

(1) $\overline{z+w} = \overline{z} + \overline{w}$.
(2) $\overline{-z} = -\overline{z}$.
(3) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
(4) Für $z \neq 0$ ist $\overline{1/z} = 1/\overline{z}$.
(5) $\overline{\overline{z}} = z$.
(6) $\overline{z} = z$ genau dann, wenn $z \in \mathbb{R}$ ist.

4. Vorlesung - Polynomringe

Terme und Gleichungen

Unter einem (arithmetischen) „Term“ versteht man einen „zahlähnlichen“ Ausdruck, der sich aus „Zahlen“ und „Variablen“ mit Hilfe der Verknüpfungssymbole $+$ und $\cdot$ (eventuell mit $-$ und $:$ oder daraus abgeleiteten Operationen wie Potenzen) und mit Klammern „korrekt“ bilden lässt. Das sind typischerweise auch die Ausdrücke, die auf einer Seite einer Gleichung (oder Ungleichung) stehen können. Beispielsweise sind

$$3 \cdot (4+5),\ x,\ 2x+7,\ 4x^3-y,\ (a+b)^2,\ a^2+2ab+b^2,\ 0 \cdot 1,$$

Terme. Dagegen sind

$$3 \cdot (4+5)),\ 2x+7=0,$$

keine Terme. Bei

$$n!,\ \binom{n}{k},\ \pi,\ e^u, x^y,\ 5^x,\ \sqrt{x},\ \heartsuit$$

kann man sich darüber streiten (in der mathematischren Logik wird der Termbegriff unter Bezug auf Funktionssymbole präzisiert), es sind jedenfalls keine rein algebraischen Terme. Wichtig ist, dass man Terme nur dann als gleich ansieht, wenn es sich um dieselbe Zeichenreihe handelt. Beispielsweise sind $(a+b)^2$ und $a^2+2ab+b^2$ verschiedene Terme. Gleichheit zwischen diesen Ausdrücken gilt nur bei einer bestimmten Interpretation, wenn man a und b als Elemente eines kommutativen Ringes interpretiert (erste binomische Formel).

Eine wichtige Funktion von Termen ist ihr Auftreten in Gleichungen. Gleichungen und Terme treten in der Mathematik in verschiedener Bedeutung auf.

1) Identitäten von Elementen

Das sind Gleichungen der Form $2+4 = 6$ oder

$$3 \cdot 7 = 21,$$

die besagen, das zwei irgendwie gegebene Elemente einer Menge gleich sind. $2+4$ und 6 sind unterschiedliche Terme, haben aber denselben Zahlwert. In solchen Gleichungen kommen keine Variablen vor. Häufig werden solche Gleichungen verwendet, um etwas auszurechnen, also einen komplizierten Ausdruck in eine Standardfrom zu bringen.

2) Termidentitäten (Formeln, Rechengesetze)

Beispiel dazu sind

$$a(b+c) = ab+ac$$

oder

$$(a+b)^2 = a^2+2ab+b^2$$

oder

$$a^2 + b^2 = c^2.$$

Sie drücken eine Gesetzmäßigkeit aus, die unter bestimmten Bedingungen gilt, beispielsweise wenn a, b Elemente eines kommutativen Ringes sind oder wenn a, b Kathetenlängen und c die Hypothenusenlänge eines rechtwinkligen Dreiecks ist. Charakteristisch für solche Gleichungen ist, dass in ihnen Variablen vorkommen und dass, wenn man für die Variablen simultan (also an jeder Stelle, wo die Variable steht) Elemente, die die Bedingung erfüllen, einsetzt, eine wahre Elementgleichung entsteht. Eine solche Identität repräsentiert also eine Vielzahl an einzelnen Elementgleichungen. Aus dem Distributivgesetz ensteht beispielsweise durch Einsetzen die spezielle Identität $3 \cdot (5 + 4) = 3 \cdot 5 + 3 \cdot 4$.

3) Gleichungen als Bedingung

Damit sind Gleichungen wie

$$4x = 9,\ 2x + 7 = 0,\ 5x^2 - 3x + 4 = 0,\ x = y$$

gemeint. In diesen kommen (in aller Regel) Variablen vor, es wird aber nicht eine allgemeingültige Formel zum Ausdruck gebracht, sondern es wird eine Bedingung an die auftretenden Variablen formuliert. D.h. es werden die Elemente gesucht, die die Gleichungen erfüllen, die man also für die Variablen einsetzen kann, damit eine wahre Elementidentität entsteht. Gleichungen in diesem Sinne definieren die Aufgabenstellung, nach Lösungen zu suchen. Statt einer einzigen Gleichung kann auch ein (beispielsweise lineares) Gleichungssystem vorliegen.

4) Definitionsgleichungen

Das sind Gleichungen, durch die eine abkürzende Schreibweise für einen komplexeren Ausdruck eingeführt wird. Beispiele sind

$$a^3 = a \cdot a \cdot a,\ n! = n(n-1) \cdot 3 \cdot 2 \cdot 1,\ |a + bi| = \sqrt{a^2 + b^2},\ P = 4x^2 + 7x - 5\,.$$

Hierbei schreibt man häufig := statt =.

Manche Gleichungen kann man in mehrfacher Weise auffassen. So kann man die Gleichung

$$a^2 + b^2 = c^2$$

als Gesetzmäßigkeit in einem rechtwinkligen Dreieck auffassen (bei richtiger Interpretation der einzelnen Variablen) oder als Aufgabenstellung, alle Tripel (a, b, c) zu bestimmen, die diese Gleichung erfüllen.

Polynomringe in einer Variablen

Zu einem kommutativen Ausgangsring wie $\mathbb{Z}$ oder $\mathbb{R}$ und einer fixierten Variablen X kann man sich fragen, welche Terme man mit dieser Variablen über

diesem Ring „basteln“ kann. Dazu gehören

$$5,\ 3X+3,\ 3(X+1),\ (2X-6)(4X+3),\ X\cdot(X\cdot X),\ 5+3X-6X^2+7X^3,\ X^2-4+5X^2+7X-13X,$$

wobei wir Potenzschreibweise verwendet und einige Klammern wegelassen haben. Als Terme sind $3X+3$ und $3(X+1)$ verschieden. Bei jeder Interpertation von X in einem Ring sind diese Ausdrücke aber gleich. Der Polynomring besteht aus genau diesen Termen, wobei allerdings Terme miteinander identifiziert werden, wenn dies in jedem kommutativen Ring gilt (die Menge aller Terme ist kein Ring)!

Definition 4.1. Der *Polynomring* über einem kommutativen Ring R besteht aus allen *Polynomen*

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

mit $a_i \in R$, $i = 0, \ldots, n$ $n \in \mathbb{N}$, und mit komponentenweiser Addition und einer Multiplikation, die durch distributive Fortsetzung der Regel

$$X^n \cdot X^m := X^{n+m}$$

definiert ist.

Ein Polynom

$$P = \sum_{i=0}^{n} a_iX^i = a_0 + a_1X + \cdots + a_nX^n$$

ist formal gesehen nichts anderes als das Tupel $(a_0, a_1, \ldots, a_n)$, die die *Koeffizienten* des Polynoms heißen. Der Ring R heißt in diesem Zusammenhang der *Grundring* des Polynomrings. Aufgrund der komponentenweisen Definition der Addition liegt unmittelbar eine Gruppe vor, mit dem *Nullpolynom* (bei dem alle Koeffizienten null sind) als neutralem Element. Zwei Polynome sind genau dann gleich, wenn sie in allen ihren Koeffizienten übereinstimmen. Die Polynome mit $a_i = 0$ für alle $i \geq 1$ heißen *konstante Polynome*, man schreibt sie einfach als a_0. Ein von 0 verschiedenes Polynom kann man als $\sum_{i=0}^{n} a_iX^i$ mit $a_n \neq 0$ schreiben. Der Koeffizient a_n heißt dann der *Leitkoeffizient* des Polynoms.

Die für ein einfaches Tupel zunächst ungewöhnliche Schreibweise deutet in suggestiver Weise an, wie die Multiplikation aussehen soll, das Produkt X^iX^j ist nämlich durch die Addition der Exponenten gegeben. Dabei nennt man X die *Variable* des Polynomrings. Für beliebige Polynome ergibt sich die Multiplikation aus dieser einfachen Multiplikationsbedingung durch distributive Fortsetzung gemäß der Vorschrift, „alles mit allem“ zu multiplizieren. Die Multiplikation ist also explizit durch folgende Regel gegeben:

$$\left(\sum_{i=0}^{n} a_iX^i\right) \cdot \left(\sum_{j=0}^{m} b_jX^j\right) = \sum_{k=0}^{n+m} c_kX^k \text{ mit } c_k = \sum_{r=0}^{k} a_rb_{k-r}\,.$$

Beispielsweise ist

$$\begin{aligned} & \left(iX^2+(3-i)X+5\right)\left(-X^2+4X+2i\right) \\ = \; & -iX^4+(4i-(3-i))X^3+(2ii+(3-i)4-5)X^2+((3-i)2i+20)X+10i \\ = \; & -iX^4+(-3+5i)X^3+(5-4i)X^2+(22+6i)X+10i \end{aligned}$$

Lemma 4.2. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Dann gelten folgende Aussagen.*

(1) *R ist ein Unterring von $R[X]$.*
(2) *R ist genau dann ein Integritätsbereich, wenn $R[X]$ ein Integritätsbereich ist.*

Beweis. (1) Ein Element $r \in R$ wird als konstantes Polynom aufgefasst, wobei es egal ist, ob man Addition und Multiplikation in R oder in $R[X]$ ausführt.

(2) Wenn $R[X]$ integer ist, so überträgt sich dies sofort auf den Unterring R. Sei also R ein Integritätsbereich und seien $P = \sum_{i=0}^{n} a_i X^i$ und $Q = \sum_{j=0}^{m} b_j X^j$ zwei von null verschiedene Polynome. Wir können annehmen, dass a_n und b_m von null verschieden sind. Dann ist $a_n b_m \neq 0$ und dies ist der Leitkoeffizient des Produktes PQ, das damit nicht null sein kann.

□

Korollar 4.3. *Sei R ein kommutativer Ring. und sei $S \subseteq R$ ein Unterring. Dann ist auch $S[X]$ ein Unterring von $R[X]$.*

Beweis. Siehe Aufgabe 4.7. □

Die vorstehende Aussage bedeutet einfach, dass man ein Polynom mit Koeffizienten aus S direkt auch als Polynom mit Koeffizienten aus R auffassen kann. So ist ein Polynom mit ganzzahligen Koeffizienten insbesondere auch ein Polynom mit rationalen Koeffizienten und mit reellen Koeffizienten. Die Addition und die Multiplikation von zwei Polynomen hängt nicht davon ab, ob man sie über einem kleineren oder einem größeren Grundring ausrechnet, so lange dieser nur alle beteiligten Koeffizienten enthält. Es gibt aber auch viele wichtige Eigenschaften, die vom Grundring abhängen, wie beispielsweise die Eigenschaft, irreduzibel zu sein, siehe Beispiel 6.8.

In ein Polynom $P \in R[X]$ kann man ein Element $r \in R$ einsetzen. Dabei ersetzt man überall die Variable X durch r und rechnet das Ergebnis in R aus. Dieses Ergebnis wird mit $P(r)$ bezeichnet. Ein fixiertes Element $r \in R$ definiert dann eine Abbildung (die *Auswertungsabbildung* zu r)

$$R[X] \longrightarrow R,\ P \longmapsto P(r).$$

Andererseits definiert ein fixiertes Polynom $P \in R[X]$ die zugehörige Polynomfunktion, die durch

$$R \longrightarrow R,\, x \longmapsto P(x).$$

Diese wird insbesondere bei einem Körper $R = K$ studiert, siehe weiter unten.

Der Grad eines Polynoms

Definition 4.4. Der *Grad* eines von 0 verschiedenen Polynoms

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

mit $a_n \neq 0$ ist n.

Wenn der Leitkoeffizient $a_n = 1$ ist, so nennt man das Polynom *normiert*. Dem Nullpolynom wird im Allgemeinen kein Grad zugewiesen; manchmal sind gewisse Gleichungen oder Bedingungen aber auch so zu verstehen, dass dem Nullpolynom jeder Grad zugewiesen wird. Polynome vom Grad 0 heißen *konstante Polynome*, Polynome vom Grad 1 heißen *lineare Polynome* und Polynome vom Grad 2 heißen *quadratische Polynome*.

Lemma 4.5. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Dann gelten für den Grad folgende Aussagen.*

(1) $\operatorname{grad}(P+Q) \leq \max\{\operatorname{grad}(P), \operatorname{grad}(Q)\}$
(2) $\operatorname{grad}(P \cdot Q) \leq \operatorname{grad}(P) + \operatorname{grad}(Q)$
(3) *Wenn R ein Integritätsbereich ist, so gilt in (2) die Gleichheit.*

Beweis. Siehe Aufgabe 4.8. □

Polynomringe in mehreren Variablen

Die Konstruktion von Polynomringen aus einem Grundring kann man iterieren. Aus R kann man $R[X]$ machen und daraus mit einer neuen Variablen den Ring $(R[X])[Y]$ bilden. Für diesen Ring schreibt man auch $R[X,Y]$. Ein Element darin hat die Gestalt

$$\sum_{i,j} a_{ij}X^iY^j\,,$$

wobei die Summe endlich ist. Ein Ausdruck der Form X^iY^j heißt Monom. Polynome kann man auf unterschiedliche Art sortieren. Man kann die Potenz einer Variablen (etwa Y) herausnehmen und schauen, welche Polynome in X sich darauf beziehen. Dann sieht ein Polynom folgendermaßen aus:

$$2+3X-X^2-5X^3+(1+3X-X^2+3X^5)Y+(4+X+7X^2-6X^4)Y^2+(2-X^3)Y^3\,.$$

Oder man kann entlang dem Summengrad sortieren, dies ergibt

$$2+3X+Y-X^2+3XY+4Y^2-5X^3-X^2Y+XY^2+2Y^3+7X^2Y^2+3X^5Y \\ +6X^4Y^2-X^3Y^3.$$

Polynomiale Identitäten haben viel mit allgemeingültigen Termidentitäten zu tun. In $\mathbb{Z}[X,Y]$ gilt beispielsweise

$$(X+Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^k Y^{n-k}$$

Diese Identität zwischen zwei Polynomen entspricht der allgemeinen binomischen Formel. Einerseits ist sie ein Spezialfall davon, da wir in dem kommutativen Ring $\mathbb{Z}[X,Y]$ sind und die speziellen Elemente X und Y anschauen. Andererseits kann man aus dieser polynomialen Identität die allgemeine binomische Formel zurückgewinnen, da man für X und Y beliebige Elemente a und b eines kommutativen Ringes einsetzen kann (und man weiß, wie man ganze Zahlen in jedem Ring interpretiert) und sich dabei die Identität erhält. Natürlich gibt es auch Polynomringe in beliebig vielen Variablen, dafür schreibt man $R[X_1, X_2, \ldots, X_n]$.

Polynomringe über einem Körper

Für uns sind zunächst die Polynomringe über einem Körper von besonderer Bedeutung.

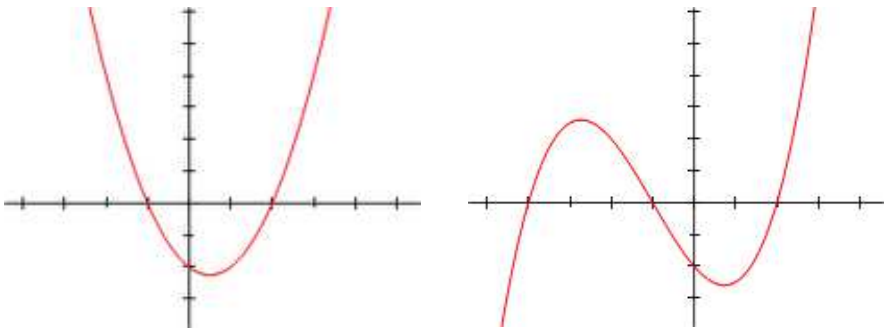
Definition 4.6. Es sei K ein Körper und seien $a_0, a_1, \ldots, a_n \in K$. Eine Funktion

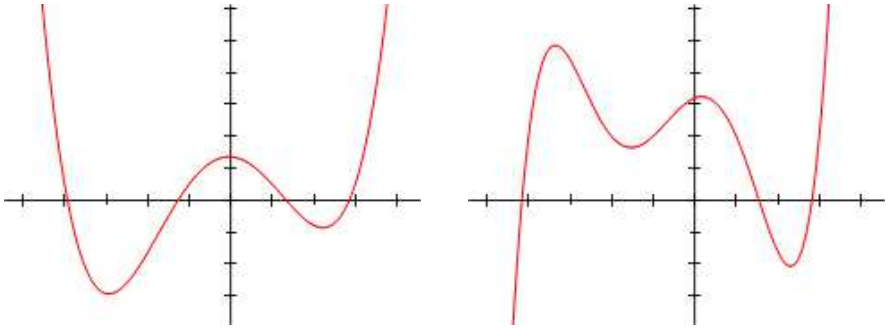
$$P\colon\ K \longrightarrow K,\ x \longmapsto P(x),$$

mit

$$P(x) \ = \ \sum_{i=0}^{n} a_i x^i \ = \ a_0 + a_1 x + \cdots + a_n x^n$$

heißt *Polynomfunktion.*





Man muss zwischen Polynomen und Polynomfunktionen unterscheiden, insbesondere für $K = \mathbb{Z}/(p)$. Das Polynom

$$X^p - X$$

hat beispielsweise nach dem kleinen Fermat für jedes $a \in K$ den Wert $a^p - a = 0$. D.h. die durch dieses Polynom definierte Polynomfunktion ist die Nullfunktion, obwohl das Polynom selbst nicht das Nullpolynom ist.

Bei $K = \mathbb{R}$ lassen sich die Polynomfunktionen graphisch veranschaulichen.

Eine wichtige Frage ist, für welche Elemente $x \in K$ die Polynomfunktion einen bestimmten Wert annimmt. Hierbei ist insbesondere der Wert 0 wichtig, da ja die Gleichung $P(x) = a$ äquivalent zu

$$P(x) - a = 0$$

ist und $P - a$ wieder ein Polynom ist. Für lineare Polynome $aX + b$ (mit $a \neq 0$) ist $x = \frac{-b}{a}$ die einzige Lösung. Für quadratische Polynome der reinen Form $X^2 + c$ sind die Quadratwurzeln von $-c$ aus K, falls sie denn existieren, die Lösungen. Für ein quadratisches Polynom $aX^2 + bX + c$ kann man das Bestimmen der Nullstellen durch quadratisches Ergänzen auf die reine Form zurückführen, siehe Aufgabe 4.13.

Der folgende Satz heißt *Interpolationssatz* und beschreibt die Interpolation von vorgegebenen Funktionswerten durch Polynome.

Satz 4.7. *Es sei K ein Körper und es seien n verschiedene Elemente $a_1, \ldots, a_n \in K$ und n Elemente $b_1, \ldots, b_n \in K$ gegeben. Dann gibt es ein eindeutiges Polynom $P \in K[X]$ vom Grad $\leq n-1$ derart, dass $P(a_i) = b_i$ für alle i ist.*

Beweis. Wir beweisen die Existenz und betrachten zuerst die Situation, wo $b_j = 0$ ist für alle $j \neq i$. Dann ist

$$(X - a_1) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)$$

ein Polynom vom Grad $n-1$, das an den Stellen $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ den Wert 0 hat. Das Polynom

$$\frac{b_i}{(a_i - a_1)\cdots(a_i - a_{i-1})(a_i - a_{i+1})\cdots(a_i - a_n)} \\ (X - a_1)\cdots(X - a_{i-1})(X - a_{i+1})\cdots(X - a_n)$$

hat an diesen Stellen ebenfalls eine Nullstelle, zusätzlich aber noch bei a_i den Wert b_i. Nennen wir dieses Polynom P_i. Dann ist

$$P \;=\; P_1 + P_2 + \cdots + P_n$$

das gesuchte Polynom. An der Stelle a_i gilt ja

$$P_j(a_i) \;=\; 0$$

für $j \neq i$ und $P_i(a_i) \;=\; b_i$.

Die Eindeutigkeit folgt aus Korollar 5.6. □

4. Arbeitsblatt

Übungsaufgaben

Aufgabe 4.1. Diskutiere, ob es sich bei

$$n!,\ \binom{n}{k},\ \pi,\ e^u, x^y,\ 5^x,\ \sqrt{x},\ \heartsuit$$

um Terme handelt.

Aufgabe 4.2. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass die Multipliktion auf $K[X]$ assoziativ, kommutativ und distributiv ist und dass das (konstante) Polynom 1 neutrales Element der Multiplikation ist.

Aufgabe 4.3. Berechne das Produkt

$$(2X^3 + 4X + 5) \cdot (X^4 + 5X^2 + 6)$$

im Polynomring $\mathbb{Z}/(7)[X]$.

Aufgabe 4.4. Berechne im Polynomring $\mathbb{C}[X]$ das Produkt

$$((4+i)X^2 - 3X + 9i) \cdot ((-3+7i)X^2 + (2+2i)X - 1 + 6i)\,.$$

Aufgabe 4.5. Beweise die Formel

$$X^n - 1 \;=\; (X-1)(X^{n-1} + X^{n-2} + X^{n-3} + \cdots + X^2 + X + 1).$$

Aufgabe 4.6.* Sei R ein Integritätsbereich und $R[X]$ der Polynomring über R. Zeige, dass die Einheiten von $R[X]$ genau die Einheiten von R sind.

Aufgabe 4.7. Sei R ein kommutativer Ring. und sei $S \subseteq R$ ein Unterring. Zeige, dass $S[X]$ ein Unterring von $R[X]$ ist.

Aufgabe 4.8. Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Zeige, dass der Grad folgende Eigenschaft erfüllt.

(1) $\operatorname{grad}(P+Q) \leq \max\{\operatorname{grad}(P), \operatorname{grad}(Q)\}$
(2) $\operatorname{grad}(P \cdot Q) \leq \operatorname{grad}(P) + \operatorname{grad}(Q)$
(3) Wenn R ein Integritätsbereich ist, so gilt in (2) die Gleichheit.

Aufgabe 4.9. Berechne das Ergebnis, wenn man im Polynom

$$2X^3 - 5X^2 - 4X + 7$$

die Variable X durch die komplexe Zahl $2 - 5i$ ersetzt.

Aufgabe 4.10. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $a \in K$. Zeige, dass die Einsetzungsabbildung, also die Zuordnung

$$\psi\colon\ K[X] \longrightarrow K,\ P \longmapsto P(a),$$

folgende Eigenschaften erfüllt (dabei seien $P, Q \in K[X]$).

(1) $(P+Q)(a) = P(a) + Q(a)$.
(2) $(P \cdot Q)(a) = P(a) \cdot Q(a)$.
(3) $1(a) = 1$.

Aufgabe 4.11. Schreibe das Polynom

$$X^3 + 2X^2 - 3X + 4$$

in der neuen Variablen $U = X + 2$.

Aufgabe 4.12. Schreibe das Polynom

$$Z^3 - (2i)Z^2 + 3iZ - (45i)$$

in der neuen Variablen $W = Z + 2 - i$.

Aufgabe 4.13.*

Formuliere und beweise die *Lösungsformel für eine quadratische Gleichung*

$$ax^2 + bx + c = 0$$

mit $a, b, c \in \mathbb{R}$, $a \neq 0$.

In welchen Körpern gilt diese Lösungsformel ebenso?

Aufgabe 4.14. Lucy Sonnenschein möchte sich ein quadratisches Grundstück kaufen. Drum rum möchte sie einen Heckenzaun pflanzen. Der Quadratmeterpreis beträgt 200 Euro, ein Meter Hecke kostet 30 Euro und die Eintragung ins Grundbuch kostet 1000 Euro. Lucy möchte eine Million Euro investieren. Welche Seitenlänge hat das Grundstück?

Aufgabe 4.15. Man finde ein Polynom

$$f = a + bX + cX^2$$

mit $a, b, c \in \mathbb{R}$ derart, dass die folgenden Bedingungen erfüllt werden.

$$f(-1) = 2,\ f(1) = 0,\ f(3) = 5\,.$$

Aufgabe 4.16. Man finde ein Polynom

$$f = a + bX + cX^2 + dX^3$$

mit $a, b, c, d \in \mathbb{R}$ derart, dass die folgenden Bedingungen erfüllt werden.

$$f(0) = 1,\ f(1) = 2,\ f(2) = 0,\ f(-1) = 1\,.$$

Aufgabe 4.17. Man finde ein Polynom

$$f = a + bX + cX^2$$

mit $a, b, c \in \mathbb{C}$ derart, dass die folgenden Bedingungen erfüllt werden.

$$f(i) = 1,\ f(1) = 1 + i,\ f(1 - 2i) = -i\,.$$

Aufgabe 4.18. Multipliziere in $\mathbb{Z}/(5)[x, y]$ die beiden Polynome

$$x^4 + 2x^2y^2 - xy^3 + 2y^3 \text{ und } x^4y + 4x^2y + 3xy^2 - x^2y^2 + 2y^2\,.$$

Aufgabe 4.19. Multipliziere in $\mathbb{Z}[x, y, z]$ die beiden Polynome

$$x^5 + 3x^2y^2 - xyz^3 \text{ und } 2x^3yz + z^2 + 5xy^2z - x^2y\,.$$

Aufgabe 4.20. Beweise die Identität

$$(X+Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^k Y^{n-k}$$

im Polynomring $\mathbb{Z}[X,Y]$.

Aufgaben zum Abgeben

Aufgabe 4.21. (3 Punkte)

Berechne im Polynomring $\mathbb{C}[X]$ das Produkt

$$((4+i)X^3 - iX^2 + 2X + 3 + 2i) \cdot ((2-i)X^3 + (3-5i)X^2 + (2+i)X + 1 + 5i)\,.$$

Aufgabe 4.22. (3 Punkte)

Beweise die Formel

$$X^u + 1 \;=\; (X+1)(X^{u-1} - X^{u-2} + X^{u-3} - \cdots + X^2 - X + 1)$$

für u ungerade.

Aufgabe 4.23. (4 Punkte)

Es sei R ein kommutativer Ring und $r \in R$ ein nilpotentes Element. Konstruiere dazu ein lineares Polynom in $R[X]$, das eine Einheit ist. Man gebe auch das Inverse dazu an.

Aufgabe 4.24. (4 Punkte)

Man finde ein Polynom f vom Grad ≤ 3, für welches

$$f(0) = -1,\; f(-1) = -3,\; f(1) = 7,\; f(2) = 21\,.$$

gilt

Aufgabe 4.25. (8 Punkte)

Zwei Personen A und B spielen Polynome-Erraten. Dabei denkt sich A ein Polynom $P(x)$ aus, wobei alle Koeffizienten aus $\mathbb{N}$ sein müssen. Person B darf fragen, was der Wert $P(n_1), P(n_2), \ldots, P(n_r)$ zu gewissen natürlichen Zahlen $n_1, n_2, \ldots, n_r$ ist. Dabei darf B diese Zahlen beliebig wählen und dabei auch vorhergehende Antworten berücksichtigen. Ziel ist es, das Polynom zu erschließen.

Entwickle eine Fragestrategie für B, die immer zur Lösung führt und bei der die Anzahl der Fragen (unabhängig vom Polynom) beschränkt ist.

5. Vorlesung - Division mit Rest

Es bestehen viele und weitreichende Parallelen zwischen dem Ring $\mathbb{Z}$ der ganzen Zahlen und einem Polynomring in einer Variablen über einem Körper. Grundlegend ist, dass man in beiden Situation eine *Division mit Rest* durchführen kann.

Division mit Rest in $\mathbb{Z}$

Zu einer ganzen Zahl d ist die Menge

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

aller Vielfachen von d eine Untergruppe von $\mathbb{Z}$. Wir wollen zeigen, dass jede Untergruppe der ganzen Zahlen $\mathbb{Z}$ diese Gestalt besitzt, also von einem Element erzeugt wird.

Satz 5.1. *Sei d eine fixierte positive natürliche Zahl. Dann gibt es zu jeder ganzen Zahl n eine eindeutig bestimmte ganze Zahl q und eine eindeutig bestimmte natürliche Zahl r, $0 \leq r \leq d-1$, mit*

$$n = qd + r \, .$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

In der Notation des vorstehenden Satzes soll q an *Quotient* und r an *Rest* erinnern. Die Division mit Rest kann man auch so verstehen, dass man jede rationale Zahl n/d als

$$\frac{n}{d} = \lfloor \frac{n}{d} \rfloor + \frac{r}{d}$$

schreiben kann, wobei $\lfloor s \rfloor$ die größte ganze Zahl $\leq s$ bedeutet und der rationale Rest r/d die Bedingungen $0 \leq r/d < 1$ erfüllt. In dieser Form kann man auch eine Division mit Rest für jede reelle Zahl aus den Axiomen der reellen Zahlen beweisen.

Satz 5.2. *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form*

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nicht-negativen Zahl d.

Beweis. Eine Teilmenge der Form $\mathbb{Z}d$ ist aufgrund der Distributivgesetze eine Untergruppe. Sei umgekehrt $H \subseteq \mathbb{Z}$ eine Untergruppe. Bei $H = 0$ kann man $d = 0$ nehmen, so dass wir voraussetzen dürfen, dass H neben 0 noch mindestens ein weiteres Element x enthält. Wenn x negativ ist, so muss die Untergruppe H auch das Negative davon, also $-x$ enthalten, welches positiv ist. D.h. H enthält auch positive Zahlen. Sei nun d die kleinste positive Zahl aus H. Wir behaupten $H = \mathbb{Z}d$. Dabei ist die Inklusion $\mathbb{Z}d \subseteq H$ klar, da mit

d alle (positiven und negativen) Vielfache von d dazugehören müssen. Für die umgekehrte Inklusion sei $h \in H$ beliebig. Nach Satz 5.1 gilt

$$h = qd + r \text{ mit } 0 \leq r < d\,.$$

Wegen $h \in H$ und $qd \in H$ ist auch $r = h - qd \in H$. Nach der Wahl von d muss wegen $r < d$ gelten: $r = 0$. Dies bedeutet $h = qd$ und damit $h \in \mathbb{Z}d$, also $H \subseteq \mathbb{Z}d$. □

Division mit Rest in $K[X]$

Satz 5.3. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $P, T \in K[X]$ zwei Polynome mit $T \neq 0$. Dann gibt es eindeutig bestimmte Polynome $Q, R \in K[X]$ mit*

$$P = TQ + R \text{ und mit } \operatorname{grad}(R) < \operatorname{grad}(T) \text{ oder } R = 0\,.$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Die Berechnung der Polynome Q und R heißt *Polynomdivision*. Wir geben dazu ein Beispiel über den komplexen Zahlen.

Beispiel 5.4. Wir führen die Polynomdivision

$$P = 6X^3 + X + 1 \text{ durch } T = 3X^2 + 2X - 4$$

durch. Es wird also ein Polynom vom Grad 3 durch ein Polynom vom Grad 2 dividiert, d.h. dass der Quotient und auch der Rest (maximal) vom Grad 1 sind. Im ersten Schritt überlegt man, mit welchem Term man T multiplizieren muss, damit das Produkt mit P im Leitterm übereinstimmt. Das ist offenbar $2X$. Das Produkt ist

$$2X\left(3X^2 + 2X - 4\right) = 6X^3 + 4X^2 - 8X.$$

Die Differenz von P zu diesem Produkt ist

$$6X^3 + X + 1 - \left(6X^3 + 4X^2 - 8X\right) = -4X^2 + 9X + 1.$$

Mit diesem Polynom, nennen wir es P', setzen wir die Division durch T fort. Um Übereinstimmung im Leitkoeffizienten zu erhalten, muss man T mit $\frac{-4}{3}$ multiplizieren. Dies ergibt

$$-\frac{4}{3}T = -\frac{4}{3}\left(3X^2 + 2X - 4\right) = -4X^2 - \frac{8}{3}X + \frac{16}{3}.$$

Die Differenz zu P' ist somit

$$-4X^2 + 9X + 1 - \left(-4X^2 - \frac{8}{3}X + \frac{16}{3}\right) = \frac{35}{3}X - \frac{13}{3}.$$

Dies ist das Restpolynom und somit ist insgesamt

$$6X^3 + X + 1 = \left(3X^2 + 2X - 4\right)\left(2X - \frac{4}{3}\right) + \frac{35}{3}X - \frac{13}{3}.$$

Lemma 5.5. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist, so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a - a)Q(a) = 0\,.$$

Im Allgemeinen gibt es aufgrund der Division mit Rest eine Darstellung

$$P = (X - a)Q + R\,,$$

wobei $R = 0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R\,.$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X - a)Q$ ist. □

Korollar 5.6. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom ($\neq 0$) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X - a)$ nach Lemma 5.5 und Q hat den Grad $d - 1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d - 1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b - a)$. Dies kann nur dann 0 sein, wenn einer der Faktoren 0 ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

Korollar 5.7. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann besitzt jedes $P \in K[X]$, $P \neq 0$, eine Produktzerlegung*

$$P = (X - \lambda_1)^{\mu_1} \cdots (X - \lambda_k)^{\mu_k} \cdot Q$$

mit $\mu_j \geq 1$ und einem nullstellenfreien Polynom Q. Dabei sind die auftretenden verschiedenen Zahlen $\lambda_1, \ldots, \lambda_k$ und die zugehörigen Exponenten $\mu_1, \ldots, \mu_k$ (bis auf die Reihenfolge) eindeutig bestimmt.

Beweis. Siehe Aufgabe 5.8. □

Es gilt allgemeiner, dass die Zerlegung eines Polynoms in irreduzible Faktoren im Wesentlichen eindeutig ist. Das werden wir später behandeln.

Der Fundamentalsatz der Algebra

Es gilt der folgende *Fundamentalsatz der Algebra*, den wir hier ohne Beweis erwähnen.

Satz 5.8. *Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.*

Aus dem Fundamentalsatz der Algebra folgt, dass jedes von 0 verschiedene Polynom $P \in \mathbb{C}[X]$ in Linearfaktoren zerfällt, d.h. man kann schreiben

$$P = c(X - z_1)(X - z_2) \cdot (X - z_n)$$

mit eindeutig bestimmten komplexen Zahlen $z_1, \ldots, z_n$ (wobei Wiederholungen erlaubt sind).

Euklidische Bereiche

Ringe, in denen man eine Division mit Rest sinnvoll durchführen kann, bekommen einen eigenen Namen.

Definition 5.9. Ein *euklidischer Bereich* (oder *euklidischer Ring*) ist ein Integritätsbereich R, für den eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ existiert, die die folgende Eigenschaft erfüllt:

Für Elemente a, b mit $b \neq 0$ gibt es $q, r \in R$ mit

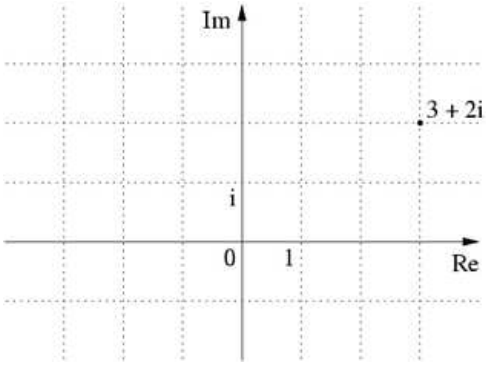
$$a = qb + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(b)\,.$$

Die in der Definition auftauchende Abbildung δ nennt man auch *euklidische Funktion*. Die ganzen Zahlen $\mathbb{Z}$ bilden also einen euklidischen Ring mit dem Betrag als euklidischer Funktion.

Beispiel 5.10. Für einen Körper K ist der Polynomring $K[X]$ in einer Variablen ein euklidischer Bereich, wobei die euklidische Funktion δ durch die Gradfunktion gegeben ist. Viele Parallelen zwischen dem Polynomring $K[X]$ und $\mathbb{Z}$ beruhen auf dieser Eigenschaft. Die Gradfunktion hat die Eigenschaft

$$\delta(fg) = \delta(f) + \delta(g)\,.$$

Beispiel 5.11. Eine Gaußsche Zahl z ist durch $z = a + b\mathrm{i}$ gegeben, wobei a und b ganze Zahlen sind. Die Menge dieser Zahlen wird mit $\mathbb{Z}[\mathrm{i}]$ bezeichnet. Die Gaußschen Zahlen sind die Gitterpunkte, d.h. die Punkte mit ganzzahligen Koordinaten, in der komplexen Ebene. Sie bilden mit komponentenweiser Addition und mit der induzierten komplexen Multiplikation einen kommutativen Ring.



Gaußsche Zahlen als Gitterpunkte in der komplexen Zahlenebene

Eine euklidische Funktion ist durch die Norm N gegeben, die durch $N(a + b\mathrm{i}) := a^2 + b^2$ definiert ist. Man kann auch schreiben $N(z) = z \cdot \bar{z}$, wobei $\bar{z}$ die komplexe Konjugation bezeichnet. Die Norm ist das Quadrat des komplexen Absolutbetrages und wie dieser multiplikativ, also $N(zw) = N(z)N(w)$.

Mit der Norm lassen sich auch leicht die Einheiten von $\mathbb{Z}[\mathrm{i}]$ bestimmen: ist $wz = 1$, so ist auch $N(zw) = N(z)N(w) = 1$, also $N(z) = 1$. Damit sind genau die Elemente $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ diejenigen Gaußschen Zahlen, die Einheiten sind.

Lemma 5.12. *Der Ring der Gaußschen Zahlen ist mit der Normfunktion ein euklidischer Bereich.*

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

5. Arbeitsblatt

Übungsaufgaben

Aufgabe 5.1. Es seien $q, d, s \in \mathbb{N}$ mit $d \geq 1$ und $n = qd + s$. Zeige, dass der Rest von n bei Division durch d gleich dem Rest von s bei Division durch d ist.

Aufgabe 5.2. Sei d eine positive natürliche Zahl. Es seien a, b natürliche Zahlen und es seien r bzw. s die Reste von a bzw. b bei Division durch d. Zeige, dass der Rest von $a + b$ bei Division durch d gleich dem Rest von $r + s$ bei Division durch d ist. Formuliere und beweise die entsprechende Aussage für die Multiplikation.

Aufgabe 5.3. Es seien $a, d \in \mathbb{N}$, $d \geq 1$. Zeige, dass bei Division mit Rest durch d aller Potenzen von a (also $a^0, a^1, a^2, \ldots$) schließlich eine Periodizität eintreten muss. Es gibt also $i < j$ derart, dass sich die Reste von $a^i, a^{i+1}, a^{i+2}, \ldots, a^{j-2}, a^{j-1}$ bei den folgenden Potenzen periodisch (oder „zyklisch“) wiederholen (insbesondere besitzen also a^i und a^j den gleichen Rest). Zeige ebenfalls, dass diese Periodizität nicht bei $a^0 = 1$ anfangen muss.

Aufgabe 5.4.*

Führe in $\mathbb{Z}/(5)[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = X^3 + 4X^2 + 3X - 1$ und $T = 3X^2 + 2X + 1$ durch.

Aufgabe 5.5. Führe in $\mathbb{Q}[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = 3X^4 + 7X^2 - 2X + 5$ und $T = 2X^2 + 3X - 1$ durch.

Aufgabe 5.6. Führe in $\mathbb{C}[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = (2 - i)X^5 + (3 + i)X^3 + (3 - i)X - 2i$ und $T = iX^2 + 5X + 6 - 2i$ durch.

Aufgabe 5.7. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Wie lautet das Ergebnis der Division mit Rest, wenn man ein Polynom P durch X^m teilt?

Aufgabe 5.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass jedes Polynom $P \in K[X]$, $P \neq 0$, eine Produktzerlegung

$$P = (X - \lambda_1)^{\mu_1} \cdots (X - \lambda_k)^{\mu_k} \cdot Q$$

mit $\mu_j \geq 1$ und einem nullstellenfreien Polynom Q besitzt, wobei die auftretenden verschiedenen Zahlen $\lambda_1, \ldots, \lambda_k$ und die zugehörigen Exponenten $\mu_1, \ldots, \mu_k$ bis auf die Reihenfolge eindeutig bestimmt sind.

Aufgabe 5.9. Es sei $K \subseteq L$ eine Körpererweiterung und seien $P, T \in K[X]$ Polynome. Zeige, dass es für die Division mit Rest „P durch T“ unerheblich ist, ob man sie in $K[X]$ oder in $L[X]$ durchführt.

Aufgabe 5.10. Zeige, dass ein reelles Polynom von ungeradem Grad mindestens eine reelle Nullstelle besitzt.

Aufgabe 5.11.*

Bestimme sämtliche komplexen Nullstellen des Polynoms

$$X^3 - 1$$

und gebe die Primfaktorzerlegung von diesem Polynom in $\mathbb{R}[X]$ und in $\mathbb{C}[X]$ an.

Primfaktorzerlegung haben wir noch nicht begrifflich eingeführt. Gemeint ist eine faktorielle Zerlegung, die man nicht weiter aufspalten kann.

Aufgabe 5.12. Es sei $P \in \mathbb{R}[X]$ ein Polynom mit reellen Koeffizienten und $z \in \mathbb{C}$ sei eine Nullstelle von P. Zeige, dass dann auch die konjugiert-komplexe Zahl $\overline{z}$ eine Nullstelle von P ist.

Aufgabe 5.13. Sei R ein ein euklidischer Bereich mit euklidischer Funktion δ. Zeige, dass ein Element $f \in R$ ($f \neq 0$) mit $\delta(f) = 0$ eine Einheit ist.

Aufgaben zum Abgeben

Aufgabe 5.14. (3 Punkte)

Führe in $\mathbb{Z}/(7)[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = 5X^4 + 3X^3 + 5X^2 + 3X - 1$ und $T = 3X^2 + 6X + 4$ durch.

Aufgabe 5.15. (3 Punkte)

Führe in $\mathbb{C}[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = (5 + i)X^4 + iX^2 + (3 - 2i)X - 1$ und $T = X^2 + iX + 3 - i$ durch.

Aufgabe 5.16. (3 Punkte)

Bestimme sämtliche komplexen Nullstellen des Polynoms

$$X^4 - 1$$

und gebe die Primfaktorzerlegung von diesem Polynom in $\mathbb{R}[X]$ und in $\mathbb{C}[X]$ an.

Aufgabe 5.17. (5 Punkte)

Es sei $P \in \mathbb{R}[X]$ ein nichtkonstantes Polynom mit reellen Koeffizienten. Zeige, dass man P als ein Produkt von reellen Polynomen vom Grad 1 oder 2 schreiben kann.

Tipp: Man führe Induktion über den Grad und verwende den Fundamentalsatz der Algebra, Aufgabe 5.12 und Aufgabe 5.9

6. Vorlesung - Teilbarkeit

Wir wollen für den Polynomring in einer Variablen über einem Körper zeigen, dass dort viele wichtige Sätze, die für den Ring der ganzen Zahlen gelten, ebenfalls Gültigkeit haben. Dass ein euklidischer Bereich vorliegt, haben wir schon gesehen. Es gilt aber auch die eindeutige Primfaktorzerlegung. Um diese adäquat formulieren zu können, brauchen wir einige Vorbereitungen zur allgemeinen Teilbarkeitslehre.

Teilbarkeitsbegriffe

Definition 6.1. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Beispielsweise ist 2 ein Teiler von 6 in $\mathbb{Z}$, aber kein Teiler von 5. In $\mathbb{C}[X]$ ist $X - i$ ein Teiler von $X^2 + 1$, aber nicht von $X + 2$.

Lemma 6.2. *In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jedes Element a gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jedes Element a gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jedes $c \in R$.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid rb + sc$ für beliebige Elemente $r, s \in R$.*

Beweis. Siehe Aufgabe 6.7. □

Definition 6.3. Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ gibt derart, dass $a = ub$ ist.

Die Assoziiertheit ist eine Äquivalenzrelation, siehe Aufgabe 6.3.

In $R = \mathbb{Z}$ sind zwei Zahlen genau dann zueinander assoziiert, wenn ihr Betrag übereinstimmt, wenn sie also gleich oder negativ zueinander sind. Bei $R = K[X]$ sind zwei Polynome zueinander assoziiert, wenn sie durch Multiplikation mit einem Skalar $\lambda \in K$, $\lambda \neq 0$, ineinander übergehen. Durch diese Operation kann man erreichen, dass der Leitkoeffizient eins wird. Jedes Polynom ist also assoziiert zu einen normierten Polynom.

Das folgende Lemma besagt, dass es für die Teilbarkeitsrelation nicht auf Einheiten und Assoziiertheit ankommt.

Lemma 6.4. *In einem kommutativen Ring R gelten folgende Teilbarkeitsbeziehungen.*

(1) *Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.*
(2) *Ist R ein Integritätsbereich, so gilt hiervon auch die Umkehrung.*

Beweis. Siehe Aufgabe 6.4. □

Irreduzibel und prim

Für Teilbarkeitsuntersuchungen sind die beiden folgenden Begriffe fundamental. Unter bestimmten Voraussetzungen, etwa wenn ein Hauptidealbereich (siehe nächste Vorlesung) vorliegt, sind sie äquivalent.

Definition 6.5. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Begriffsbildung orientiert sich offenbar an den Primzahlen. Dagegen taucht das Wort „prim“ in der folgenden Definition auf.

Definition 6.6. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Für die ganzen Zahlen und für viele weitere Ringe fallen die beiden Begriffe zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

Lemma 6.7. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

In vielen wichtigen Ringen gilt hiervon auch die Umkehrung, worauf wir noch ausführlich zu sprechen kommen.

Irreduzible Polynome

Die irreduziblen Elemente im Polynomring $K[X]$ über einem Körper K sind nicht einfach zu charakterisieren. Die Antwort hängt auch wesentlich vom Körper ab, und nicht für jeden Körper lassen sich die irreduziblen Polynome übersichtlich beschreiben. Bei Irreduzibilitätsfragen kann man stets mit Einheiten multiplizieren, daher muss man nur normierte Polynome untersuchen.

Beispiel 6.8. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2+1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2+1 = (X+i)(X-i)\,.$$

Ebenso ist das Polynom $X^2-5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2-5 = (X-\sqrt{5})(X+\sqrt{5})\,.$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.

Als echte Faktoren für ein Polynom kommen nur Polynome von kleinerem Grad in Frage. Insbesondere sind daher *lineare Polynome*, also Polynome von Typ $aX+b$, $a \neq 0$, stets irreduzibel. Eine notwendige Bedingung an die Irreduzibilität eines Polynoms $P \in K[X]$ ist wegen Lemma 5.5, dass es keine Nullstelle in K besitzt. Deshalb und aufgrund des Fundamentalsatzes der Algebra sind daher in $\mathbb{C}[X]$ die linearen Polynome die einzigen irreduziblen Polynome.

Lemma 6.9. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann ist ein Polynom vom Grad zwei oder drei genau dann irreduzibel, wenn es keine Nullstelle in K besitzt.*

Beweis. In einer echten Primfaktorzerlegung von P, $\operatorname{grad}(P) \leq 3$, muss ein Polynom vom Grad eins vorkommen, also ein lineares Polynom. Ein lineares Polynom $X-a$ teilt aber nach Lemma 5.5 das Polynom P genau dann, wenn $P(a)=0$ ist. □

Beispiel 6.10. Das Polynom X^4+1 ist im Reellen stets positiv und hat daher keine reelle Nullstelle. Daher besitzt es in $\mathbb{R}[X]$ nach Lemma 5.5 auch keinen linearen Faktor. Wegen der Zerlegung

$$X^4+1 \;=\; \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$$

ist das Polynom aber nicht irreduzibel.

Größter gemeinsamer Teiler

Definition 6.11. Sei R ein kommutativer Ring und $a_1,\ldots,a_k \in R$. Dann heißt ein Element $t \in R$ *gemeinsamer Teiler* der $a_1,\ldots,a_k$, wenn t jedes a_i teilt ($i=1,\ldots,k$). Ein Element $g \in R$ heißt *größter gemeinsamer Teiler* der $a_1,\ldots,a_k$, wenn g ein gemeinsamer Teiler ist und wenn jeder gemeinsame Teiler t dieses g teilt.

Die Elemente $a_1,\ldots,a_k$ heißen *teilerfremd*, wenn 1 ihr größter gemeinsamer Teiler ist.

„Größer“ ist hier bezüglich der Teilbarkeitsrelation zu verstehen, wenn b von a geteilt wird, so gilt es gemäß diesem Sprachgebrauch als größer. Dies rührt natürlich von der Situation in $\mathbb{N}$ her, wo Vielfache in der Tat größer im Sinne der natürlichen Ordnung als die Teiler sind.

Bemerkung 6.12. Eine Einheit ist immer ein gemeinsamer Teiler für jede Auswahl von Elementen. Ein größter gemeinsamer Teiler muss nicht existieren im Allgemeinen. Ist t ein gemeinsamer Teiler der $a_1, \ldots, a_k$ und u eine Einheit, so ist auch ut ein gemeinsamer Teiler der $a_1, \ldots, a_k$. Die Elemente $a_1, \ldots, a_k$ sind *teilerfremd* genau dann, wenn jeder gemeinsame Teiler davon eine Einheit ist (es gibt noch andere Definitionen von teilerfremd, die nicht immer inhaltlich mit dieser übereinstimmen).

Definition 6.13. Es sei R ein kommutativer Ring und

$$a_1, \ldots, a_n \in R\,.$$

Ein Element $b \in R$ heißt ein *gemeinsames Vielfaches* der $a_1, \ldots, a_n$, wenn b ein Vielfaches von jedem a_i ist, also von jedem a_i geteilt wird. b heißt ein *kleinstes gemeinsames Vielfaches* der $a_1, \ldots, a_n$, wenn b ein gemeinsames Vielfaches ist und wenn jedes andere gemeinsame Vielfache ein Vielfaches von b ist.

6. Arbeitsblatt

Übungsaufgaben

Aufgabe 6.1. Skizziere ein Teilerdiagramm für die Zahlen $25, 30, 36$ sowie all ihrer positiven Teiler.

Aufgabe 6.2. Zeige, dass für je zwei ganze Zahlen $a, b \in \mathbb{Z}$ aus

$$a|b \text{ und } b|a$$

die Beziehung $a = \pm b$ folgt.

Aufgabe 6.3.*

Zeige, dass für jede ungerade Zahl n die Zahl $25n^2 - 17$ ein Vielfaches von 8 ist.

Aufgabe 6.4. Zeige, dass eine natürliche Zahl n genau dann gerade ist, wenn ihre letzte Ziffer im Dezimalsystem gleich $0, 2, 4, 6$ oder 8 ist.

Aufgabe 6.5. Formuliere und beweise (bekannte) Teilbarkeitskriterien für Zahlen im Dezimalsystem für die Teiler $k = 2, 3, 5, 9, 11$.

Aufgabe 6.6. Betrachte im 15er System mit den Ziffern $0, 1, \ldots, 8, 9, A, B, C, D, E$ die Zahl

$$EA09B4CA\,.$$

Ist diese Zahl durch 7 teilbar?

Aufgabe 6.7.*

Seien $a, b \geq 2$ und sei $n = ab$.

a) Zeige, dass die beiden Polynome $X^a - 1$ und $X^b - 1$ Teiler des Polynoms $X^n - 1$ sind.

b) Sei $a \neq b$. Ist $(X^a - 1)(X^b - 1)$ stets ein Teiler von $X^n - 1$?

c) Man gebe drei Primfaktoren von $2^{30} - 1$ an.

Aufgabe 6.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K und seien $F, G \in K[X]$ zwei Polynome. Es sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass F ein Teiler von G in $K[X]$ genau dann ist, wenn F ein Teiler von G in $L[X]$ ist.

Aufgabe 6.9. Zeige, dass die Assoziiertheit in einem kommutativen Ring eine Äquivalenzrelation ist.

Aufgabe 6.10. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(2) Ist R ein Integritätsbereich, so gilt hiervon auch die Umkehrung.

Aufgabe 6.11. Zeige, dass die Primzahlen $2, 3, 5$ Primelemente in $\mathbb{Z}$ sind.

Aufgabe 6.12. Zeige, dass im Polynomring $K[X]$ über einem Körper K die Variable X irreduzibel und prim ist.

Aufgabe 6.13. Zeige, dass im Polynomring $K[X]$ über einem Körper K die linearen Polynome $aX + b$ ($a \neq 0$) irreduzibel und prim ist.

Aufgabe 6.14. Bestimme im Polynomring $\mathbb{Z}/(2)[X]$ alle irreduziblen Polynome vom Grad $2, 3, 4$.

Aufgabe 6.15. Es sei R ein Integritätsbereich mit $2 \neq 0$ und $r \in R$ ein Element, das keine Quadratwurzel in R besitze. Zeige, dass das Polynom $X^2 - r \in R[X]$ irreduzibel ist.

Aufgabe 6.16. Zeige, dass ein reelles Polynom von ungeradem Grad nicht irreduzibel ist.

Hinweis: Der Zwischenwertsatz hilft.

Aufgabe 6.17. Zeige, dass das Polynom $X^3 + 2X^2 - 5$ in $\mathbb{Q}[X]$ irreduzibel ist.

Aufgabe 6.18. Bestimme den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von 105 und 150.

Aufgabe 6.19. Sei $a_1, \ldots, a_n$ eine Menge von ganzen Zahlen. Zeige, dass der nichtnegative größte gemeinsame Teiler der a_i mit demjenigen gemeinsamen Teiler übereinstimmt, der bezüglich der Ordnungsrelation $\geq$ der größte gemeinsame Teiler ist.

Aufgaben zum Abgeben

Aufgabe 6.20. (3 Punkte)

Beweise die folgenden Eigenschaften zur Teilbarkeit in einem kommutativen Ring R

(1) Für jedes Element a gilt $1|a$ und $a|a$.
(2) Für jedes Element a gilt $a|0$.
(3) Gilt $a|b$ und $b|c$, so gilt auch $a|c$.
(4) Gilt $a|b$ und $c|d$, so gilt auch $ac|bd$.
(5) Gilt $a|b$, so gilt auch $ac|bc$ für jedes $c \in R$.
(6) Gilt $a|b$ und $a|c$, so gilt auch $a|rb+sc$ für beliebige Elemente $r, s \in R$.

Aufgabe 6.21. (4 Punkte)

Sei R ein Integritätsbereich und sei $R[X]$ der Polynomring darüber. Zeige, dass ein Polynom der Form $X + c$ ein Primelement ist.

Man gebe auch ein Beispiel, dass dies für Polynome der Form $aX + c$ nicht gelten muss.

Aufgabe 6.22. (4 Punkte)

Betrachte den Unterring

$$R = K[X^2, X^3, X^4, X^5, \ldots] \subset K[X] .$$

Zeige, dass die Elemente X^2 und X^3 in R irreduzibel, aber nicht prim sind.

Aufgabe 6.23. (5 Punkte)

Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle irreduziblen Polynome vom Grad 4.

In der folgenden Aufgabe sind die Eigenschaften prim und irreduzibel in einem Monoid zu verstehen, ohne dass ein Ring vorliegt.

Aufgabe 6.24. (4 Punkte)

Betrachte die Menge M, die aus allen positiven natürlichen Zahlen besteht, in deren Primfaktorzerlegung (in $\mathbb{N}$) eine gerade Anzahl (mit Vielfachheiten gezählt) von Primfaktoren vorkommt. Zeige, dass M ein multiplikatives Untermonoid ist. Man charakterisiere die irreduziblen Elemente und die Primelemente in M.

7. Vorlesung - Ideale

Ideale

Definition 7.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Die Eigenschaft, nichtleer zu sein, kann man durch die Bedingung $0 \in \mathfrak{a}$ ersetzen. Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich unter Skalarmultiplikation abgeschlossen ist.

Definition 7.2. Zu einer Familie von Elementen $a_1, a_2, \ldots, a_n \in R$ in einem kommutativen Ring R bezeichnet $(a_1, a_2, \ldots, a_n)$ das von diesen Elementen *erzeugte Ideal*. Es besteht aus allen *Linearkombinationen*

$$r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \,,$$

wobei $r_1, r_2, \ldots, r_n \in R$ sind.

Definition 7.3. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

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

heißt *Hauptideal*.

Das Nullelement bildet in jedem Ring das sogenannte *Nullideal*, was wir einfach als $0 = (0) = \{0\}$ schreiben. Die 1 und überhaupt jede Einheit erzeugt als Ideal schon den ganzen Ring.

Definition 7.4. Das *Einheitsideal* in einem kommutativen Ring R ist der Ring selbst.

In einem Körper gibt es nur diese beiden Ideale.

Lemma 7.5. *Es sei R ein kommutativer Ring. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Körper.*
(2) *Es gibt in R genau zwei Ideale.*

Beweis. Wenn R ein Körper ist, so gibt es das Nullideal und das Einheitsideal, die voneinander verschieden sind. Sei I ein von null verschiedenes Ideal in R. Dann enthält I ein Element $x \neq 0$, das eine Einheit ist. Damit ist $1 = xx^{-1} \in I$ und damit $I = R$.

Sei umgekehrt R ein kommutativer Ring mit genau zwei Idealen. Dann kann R nicht der Nullring sein. Sei nun x ein von null verschiedenes Element in R. Das von x erzeugte Hauptideal Rx ist $\neq 0$ und muss daher mit dem anderen Ideal, also mit dem Einheitsideal übereinstimmen. Das heißt insbesondere, dass $1 \in Rx$ ist. Das bedeutet also $1 = xr$ für ein $r \in R$, so dass x eine Einheit ist. □

Operationen für Ideale

Der Durchschnitt von Idealen ist wieder ein Ideal (der Durchschnitt von Hauptidealen ist im Allgemeinen kein Hauptideal). Daneben gibt es noch zwei weitere Operationen für Ideale, die zu neuen Idealen führen.

Definition 7.6. Zu Idealen $\mathfrak{a}, \mathfrak{b} \subseteq R$ in einem kommutativen Ring R nennt man das Ideal

$$\mathfrak{a} + \mathfrak{b} = \{a + b | \, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$$

die *Summe der Ideale*.

Die Summe ist wieder ein Ideal. Ein endlich erzeugtes Ideal ist die Summe von Hauptidealen, nämlich

$$(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n).$$

Definition 7.7. Zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ in einem kommutativen Ring wird das *Produkt* durch

$$\mathfrak{ab} = \{a_1b_1 + a_2b_2 + \cdots + a_kb_k\}$$

mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ definiert. Das ist das Ideal, das von allen Produkten ab (mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) erzeugt wird.

Die Menge aller Produkte $ab, a \in \mathfrak{a}, b \in \mathfrak{b}$ ist im Allgemeinen kein Ideal. Für Hauptideale ist $(a) \cdot (b) = (a \cdot b)$ (aber *nicht* $(a) + (b) = (a + b)$).

Wenn das Produkt eines Ideals mit sich selbst genommen wird, verwendet man die Potenzschreibweise, d.h. $\mathfrak{a}^n$ bedeutet das n-fache Produkt des Ideals mit sich selbst. In $K[X, Y]$ ist beispielsweise

$$(X, Y)^2 = (X^2, XY, Y^2).$$

Ideale und Teilbarkeitsbeziehungen

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

Lemma 7.8. *Sei R ein kommutativer Ring und $a, b \in R$. Dann gelten folgende Aussagen.*

(1) *Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.*
(2) *a ist eine Einheit genau dann, wenn $(a) = R = (1)$.*
(3) *Jede Einheit teilt jedes Element.*
(4) *Teilt a eine Einheit, so ist a selbst eine Einheit.*

Beweis. Siehe Aufgabe 7.6. □

Lemma 7.9. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{a} = (a_1, \ldots, a_k)$ das davon erzeugte Ideal. Ein Element $t \in R$ ist ein gemeinsamer Teiler von $a_1, \ldots, a_k \in R$ genau dann, wenn $\mathfrak{a} \subseteq (t)$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn für jedes $s \in R$ mit $\mathfrak{a} \subseteq (s)$ folgt, dass $(t) \subseteq (s)$ ist. Ein größter gemeinsamer Teiler erzeugt also ein minimales Hauptoberideal von $\mathfrak{a}$.*

Beweis. Aus $\mathfrak{a} = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $(a_i) \subseteq (t)$ für $i = 1, \ldots, k$, was gerade bedeutet, dass t diese Elemente teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in (t)$ und da $\mathfrak{a} = (a_1, \ldots, a_k)$ das kleinste Ideal ist, das alle a_i enthält, muss $\mathfrak{a} \subseteq (t)$ gelten. Der zweite Teil folgt sofort aus dem ersten. □

Lemma 7.10. *Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und $\mathfrak{b} = (a_1) \cap \ldots \cap (a_k)$ der Durchschnitt der zugehörigen Hauptideale. Ein Element $r \in R$ ist ein gemeinsames Vielfaches von $a_1, \ldots, a_k \in R$ genau dann, wenn $(r) \subseteq \mathfrak{b}$ ist, und r ist ein kleinstes gemeinsames Vielfaches genau dann, wenn für jedes $s \in R$ mit $(s) \subseteq \mathfrak{b}$ folgt, dass $(s) \subseteq (r)$ ist. Ein kleinstes gemeinsames Vielfaches erzeugt also ein maximales Hauptdeal innerhalb von $\mathfrak{b}$.*

Beweis. Siehe Aufgabe 8.1. □

Das Radikal

Definition 7.11. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R heißt *Radikal* (oder *Radikalideal*), wenn folgendes gilt: Falls $f^n \in \mathfrak{a}$ ist für ein $n \in \mathbb{N}$, so ist bereits $f \in \mathfrak{a}$.

Definition 7.12. Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann nennt man die Menge

$$\{f \in R | \text{ es gibt ein } r \text{ mit } f^r \in \mathfrak{a}\}$$

das *Radikal* zu $\mathfrak{a}$. Es wird mit $\operatorname{rad}(\mathfrak{a})$ bezeichnet.

Das Radikal zu einem Ideal ist selbst ein Radikal und insbesondere ein Ideal.

Lemma 7.13. *Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist das Radikal zu $\mathfrak{a}$ ein Radikalideal.*

Beweis. Wir zeigen zunächst, dass ein Ideal vorliegt. 0 gehört offenbar zum Radikal und mit $f \in \operatorname{rad}(\mathfrak{a})$, sagen wir $f^r \in \mathfrak{a}$, ist auch $(af)^r = a^r f^r \in \mathfrak{a}$, also gehört af zum Radikal. Zur Summeneigenschaft seien $f, g \in \operatorname{rad} \mathfrak{a}$ mit $f^r \in \mathfrak{a}$ und $g^s \in \mathfrak{a}$. Dann ist

$$(f+g)^{r+s} = \sum_{i+j=r+s} \binom{r+s}{i} f^i g^j = \sum_{i+j=r+s,\, i<r} \binom{r+s}{i} f^i g^j + \sum_{i+j=r+s,\, i\geq r} \binom{r+s}{i} f^i g^j \in \mathfrak{a}\,.$$

Sei nun $f^k \in \operatorname{rad}(\mathfrak{a})$. Dann ist $(f^k)^r = f^{kr} \in \mathfrak{a}$, also $f \in \operatorname{rad}(\mathfrak{a})$. □

Definition 7.14. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Lemma 7.15. *Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist.*

Beweis. Siehe Aufgabe 7.14. □

Definition 7.16. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

Lemma 7.17. *Sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Siehe Aufgabe 7.20. □

7. Arbeitsblatt

Übungsaufgaben

Aufgabe 7.1. a) Zeige, dass ein Ideal in einem kommutativen Ring R eine Untergruppe von R ist.

b) Zeige, dass für $R = \mathbb{Z}$ die Begriffe Untergruppe und Ideal zusammenfallen.

c) Man gebe eine Beispiel für einen kommutativen Ring R und eine Untergruppe $U \subseteq R$, die kein Ideal ist.

Aufgabe 7.2. Es sei K ein Körper und $d \in \mathbb{N}$. Zeige, dass die Menge

$$\left\{ P = \sum_{i=0}^{n} a_i X^i \in K[X] |\, a_0 = a_1 = \ldots = a_d = 0 \right\}$$

ein Ideal in $K[X]$ ist. Ist es ein Hauptideal?

Aufgabe 7.3.*

Zeige, dass im Polynomring $K[X, Y]$ über einem Körper K das Ideal (X, Y) kein Hauptideal ist.

Aufgabe 7.4. Es sei R ein kommutativer Ring und seien $\mathfrak{a}_j$, $j \in J$, eine Familie von Idealen. Zeige, dass der Durchschnitt $\bigcap_{j \in J} \mathfrak{a}_j$ wieder ein Ideal ist.

Aufgabe 7.5. Sei R ein kommutativer Ring und sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige ebenso durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 7.6. Sei R ein kommutativer Ring und $a, b \in R$. Zeige folgende Aussagen.

(1) Das Element a ist ein Teiler von b (also $a|b$), genau dann, wenn $(b) \subseteq (a)$.
(2) a ist eine Einheit genau dann, wenn $(a) = R = (1)$.
(3) Jede Einheit teilt jedes Element.
(4) Teilt a eine Einheit, so ist a selbst eine Einheit.

Aufgabe 7.7. Sei R ein kommutativer Ring, $a_1, \ldots, a_k \in R$ und

$$\mathfrak{b} = (a_1) \cap (a_2) \cap \ldots \cap (a_k)$$

der Durchschnitt der zugehörigen Hauptideale und $r \in R$. Zeige, dass r ein gemeinsames Vielfaches von $a_1, \ldots, a_k \in R$ genau dann ist, wenn $(r) \subseteq \mathfrak{b}$ ist.

Aufgabe 7.8. Zeige, dass das Produkt von Hauptidealen wieder ein Hauptideal ist.

Aufgabe 7.9. Es sei R ein kommutativer Ring und sei M die Menge aller Ideale in R, die wir mit den beiden Verknüpfungen Summe von Idealen und Produkt von Idealen versehen. Welche Ringaxiome gelten dafür?

Aufgabe 7.10.*

Es seien I und J Ideale in einem kommutativen Ring R und sei $n \in \mathbb{N}$. Zeige die Gleichheit

$$(I+J)^n = I^n + I^{n-1}J + I^{n-2}J^2 + \cdots + I^2J^{n-2} + IJ^{n-1} + J^n.$$

Ein homogenes Polynom $P \in K[X_1, \ldots, X_n]$ ist ein Polynom, bei dem alle beteiligten Monome den gleichen Summengrad besitzen.

Aufgabe 7.11. Sei R ein kommutativer Ring und $P = R[X_1, \ldots, X_m]$ der Polynomring darüber in m Variablen. Es sei $\mathfrak{m} = (X_1, \ldots, X_m)$ das von den Variablen erzeugte Ideal. Zeige, dass $\mathfrak{m}^n = P_{\geq n}$ ist, wobei $P_{\geq n}$ das Ideal in P bezeichnet, das von allen homogenen Polynomen vom Grad $\geq n$ erzeugt wird.

Aufgabe 7.12. Bestimme für $\mathbb{Z}$ die Radikale, die Primideale und die maximalen Ideale.

Aufgabe 7.13. Bestimme in $\mathbb{Z}$ das Radikal zum Ideal $\mathbb{Z}27$.

Aufgabe 7.14. Zeige, dass ein Primideal ein Radikal ist.

Aufgabe 7.15. Sei R ein Integritätsbereich und sei $0 \neq p \in R$ keine Einheit. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Ideal $(p) \subset R$ ein Primideal ist.

Aufgabe 7.16. Es sei K ein Körper, $K[X]$ der Polynomring über K und $P = aX+b$ ein lineares Polynom ($a \neq 0$). Zeige, dass das Hauptideal maximal ist.

Aufgabe 7.17. Es sei K ein Körper, $K[X,Y]$ der Polynomring über K und $a, b \in K$ zwei Elemente. Zeige, dass die Menge

$$\mathfrak{m} = \{P \in K[X,Y] | \, P(a,b) = 0\}$$

ein maximales Ideal in $K[X,Y]$ ist.

Aufgaben zum Abgeben

Aufgabe 7.18. (4 Punkte)

Zeige, dass im Polynomring $\mathbb{Z}[X]$ das Ideal $(X, 5)$ kein Hauptideal ist.

Aufgabe 7.19. (4 Punkte)

Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem kommutativen Ring R. Zeige, dass die Potenzen $\mathfrak{a}^n$, $n \in \mathbb{N}_+$, alle dasselbe Radikal besitzen.

Aufgabe 7.20. (4 Punkte)

Sei R ein kommutativer Ring und sei $\mathfrak{a} \neq R$ ein Ideal in R. Zeige: $\mathfrak{a}$ ist genau dann ein maximales Ideal, wenn es zu jedem $g \in R$, $g \notin \mathfrak{a}$, ein $f \in \mathfrak{a}$ und ein $r \in R$ gibt mit $rg + f = 1$.

Aufgabe 7.21. (4 Punkte)

Zeige, dass ein maximales Ideal $\mathfrak{m}$ in einem kommutativen Ring R ein Primideal ist.

8. Vorlesung - Hauptidealbereiche

Hauptidealbereiche

Die Summe von Hauptidealen und der Durchschnitt von Hauptidealen ist wieder ein Ideal, aber im Allgemeinen kein Hauptideal. Damit hängt zusammen, dass weder ein größter gemeinsamer Teiler noch ein kleinstes gemeinsames Vielfaches von Elementen $a, b \in \mathbb{R}$ existieren muss. Eine besondere Situation liegt daher vor, wenn überhaupt jedes Ideal ein Hauptideal ist. Dies trifft auf $\mathbb{Z}$ und auf $K[X]$ (K ein Körper) zu.

Definition 8.1. Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*. Ein integrer Hauptidealring heißt *Hauptidealbereich*.

Euklidische Bereiche sind Hauptidealbereiche

Satz 8.2. *Ein euklidischer Bereich ist ein Hauptidealbereich.*

Beweis. Sei I ein von null verschiedenes Ideal. Betrachte die nicht-leere Menge

$$\{\delta(a) : a \in I, a \neq 0\}.$$

Diese Menge hat ein Minimum m, das von einem Element $b \in I$, $b \neq 0$ herrührt, sagen wir $m = \delta(b)$. Wir behaupten, dass $I = (b)$ ist. Dabei ist die Inklusion „ $\supseteq$“ klar. Zum Beweis der Inklusion „$\subseteq$“ sei $a \in I$ gegeben. Aufgrund der Definition eines euklidischen Bereiches gilt $a = qb+r$ mit $r = 0$ oder $\delta(r) < \delta(b)$. Wegen $r \in I$ und der Minimalität von $\delta(b)$ kann der zweite Fall nicht eintreten. Also ist $r = 0$ und a ist ein Vielfaches von b. □

Die beiden folgenden Sätze folgen direkt aus Satz 8.2, da sowohl $\mathbb{Z}$ als auch $K[X]$ euklidische Bereiche sind. Wir geben zusätzlich noch jeweils einen spezifischen Beweis an.

Satz 8.3. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

Beweis. Sei I ein von null verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) |\, P \in I,\, P \neq 0\}.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Sei hierzu $P \in I$ gegeben. Aufgrund von Satz 5.3 gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

Satz 8.4. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealbereich.*

Beweis. Zunächst ist $\mathbb{Z}$ ein Integritätsbereich. Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Damit ist I insbesondere eine (additive) Untergruppe von $\mathbb{Z}$ und hat nach Satz 5.2 die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal. □

Teilbarkeitslehre in Hauptidealbereichen

Die folgende Aussage heißt *Lemma von Bezout.*

Satz 8.5. *Sei R ein Hauptidealring. Dann gilt:*

Elemente $a_1, \ldots, a_n$ besitzen stets einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt Elemente $r_1, \ldots, r_n \in R$ mit $r_1a_1 + r_2a_2 + \cdots + r_na_n = d$.

Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der 1.

Beweis. Sei $I = (a_1, \ldots, a_n)$ das von den Elementen erzeugte Ideal. Da wir in einem Hauptidealring sind, handelt es sich um ein Hauptideal; es gibt also ein Element d mit $I = (d)$. Wir behaupten, dass d ein größter gemeinsamer Teiler der $a_1, \ldots, a_n$ ist. Die Inklusionen $(a_i) \subseteq I = (d)$ zeigen, dass es sich um einen gemeinsamen Teiler handelt. Sei e ein weiterer gemeinsamer Teiler der $a_1, \ldots, a_n$. Dann ist wieder $(d) = I \subseteq (e)$, was wiederum $e|d$ bedeutet. Die Darstellungsaussage folgt unmittelbar aus $d \in I = (a_1, \ldots, a_n)$.

Im teilerfremden Fall ist $I = (a_1, \ldots, a_n) = R$. □

Die folgende Kurzform wird auch oft als *Lemma von Bezout* bezeichnet.

Korollar 8.6. *Sei R ein Hauptidealbereich und seien $a, b \in R$ zwei teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Dies folgt direkt aus Satz 8.5. □

Die folgende Aussage heißt *Lemma von Euklid.*

Satz 8.7. *Sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

Satz 8.8. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 6.7 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach dem Lemma von Euklid den anderen Faktor b. □

Lemma 8.9. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von irreduziblen Elementen.*

Beweis. Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei a_{n+1} ein nicht-trivialer Teiler von a_n ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots .$$

Die Vereinigung dieser Ideale ist aber ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. □

Euklidischer Algorithmus

Definition 8.10. Seien zwei Elemente a, b (mit $b \neq 0$) eines euklidischen Bereichs R mit euklidischer Funktion δ gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels der Division mit Rest

$$r_i \ = \ q_i r_{i+1} + r_{i+2}$$

rekursiv bestimmte Folge r_i die *Folge der euklidischen Reste*.

Satz 8.11. *Seien zwei Elemente $r_0 = a, r_1 = b \neq 0$ eines euklidischen Bereiches R mit euklidischer Funktion δ gegeben. Dann besitzt die Folge r_i, $i = 0, 1, 2, \ldots$, der euklidischen Reste folgende Eigenschaften.*

(1) *Es ist $r_{i+2} = 0$ oder $\delta(r_{i+2}) < \delta(r_{i+1})$.*
(2) *Es gibt ein (minimales) $k \geq 2$ mit $r_k = 0$.*
(3) *Es ist*
$$\mathrm{ggT}(r_{i+1}, r_i) \ = \ \mathrm{ggT}(r_i, r_{i-1}).$$
(4) *Sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist*
$$\mathrm{ggT}(a, b) \ = \ r_{k-1}.$$

Beweis. (1) Dies folgt unmittelbar aus der Definition der Division mit Rest.
(2) Solange $r_i \neq 0$ ist, wird die Folge der natürlichen Zahlen $\delta(r_i)$ immer kleiner, so dass irgendwann der Fall $r_i = 0$ eintreten muss.

(3) Wenn t ein gemeinsamer Teiler von r_{i+1} und von r_{i+2} ist, so zeigt die Beziehung
$$r_i = q_i r_{i+1} + r_{i+2},$$
dass t auch ein Teiler von r_i und damit ein gemeinsamer Teiler von r_{i+1} und von r_i ist. Die Umkehrung folgt genauso.

(4) Dies folgt aus (3) mit der Gleichungskette

$$\begin{aligned} \mathrm{ggT}(a,b) &= \mathrm{ggT}(b,r_2) \\ &= \mathrm{ggT}(r_2,r_3) \\ &= \dots \\ &= \mathrm{ggT}(r_{k-2},r_{k-1}) = \mathrm{ggT}(r_{k-1},r_k) = \mathrm{ggT}(r_{k-1},0) = r_{k-1}. \end{aligned}$$

□

Mit dem euklidischen Algorithmus berechnet man also einen größten gemeinsamen Teiler. Indem man die im Algorithmus auftretenden Gleichungen von hinten nach vorne verwendet, erhält man auch eine Darstellung eines größten gemeinsamen Teilers als Linearkombination von a und b.

8. Arbeitsblatt

Übungsaufgaben

Aufgabe 8.1. Finde eine Darstellung der 1 (im Sinne des Lemmas von Bezout) für die folgenden Zahlenpaare: 5 und 7; 20 und 27; 23 und 157.

Aufgabe 8.2.*

Die Wasserspedition „Alles im Eimer“ verfügt über einen 7- und einen 10-Liter-Eimer, die allerdings keine Markierungen haben. Sie erhält den Auftrag, insgesamt genau einen Liter Wasser von der Nordsee in die Ostsee zu transportieren. Kann sie diesen Auftrag erfüllen?

Aufgabe 8.3. Alle Flöhe leben auf einem unendlichen Zentimeter-Band. Ein Flohmännchen springt bei jedem Sprung 78 cm und die deutlich kräftigeren Flohweibchen springen mit jedem Sprung 126 cm. Die Flohmännchen Florian, Flöhchen und Carlo sitzen in den Positionen $-123,55$ und -49. Die Flohweibchen Flora und Florentina sitzen in Position 17 bzw. 109. Welche Flöhe können sich treffen?

Aufgabe 8.4. Es seien a und b natürliche Zahlen, deren Produkt ab von einer natürlichen Zahl n geteilt werde. Die Zahlen n und a seien teilerfremd. Zeige, dass b von n geteilt wird.

Aufgabe 8.5. Seien r und s teilerfremde Zahlen. Zeige, dass jede Lösung (x, y) der Gleichung

$$rx + sy = 0$$

die Gestalt $(x, y) = v(s, -r)$ hat, mit einer eindeutig bestimmten Zahl v.

Aufgabe 8.6. Es seien a und d teilerfremde ganze Zahlen. Zeige, dass es eine Potenz a^i mit $i \geq 1$ gibt, deren Rest bei Division durch d gleich 1 ist.

Aufgabe 8.7. Es sei $p \neq 2, 5$ eine Primzahl. Zeige, dass es eine natürliche Zahl der Form (im Dezimalsystem)

$$111 \ldots 111$$

gibt, die ein Vielfaches von p ist.

Aufgabe 8.8. Zeige, dass in einem Hauptidealbereich R zu beliebigen Elementen $a_1, \ldots, a_n \in R$ sowohl ein größter gemeinsame Teiler als auch ein kleinstes gemeinsames Vielfaches existieren.

Aufgabe 8.9. Es seien $a, b \in R$ zwei irreduzible, nicht assoziierte Elemente in einem Integritätsbereich. Zeige, dass a und b teilerfremd sind.

Aufgabe 8.10. Betrachte den Unterring

$$R = K[X^2, X^3, X^4, X^5, \ldots] \subset K[X].$$

Zeige, dass für die Elemente X^2 und X^3 kein kleinstes gemeinsames Vielfaches existiert.

Aufgabe 8.11. Betrachte den Unterring

$$R = K[X^2, X^3, X^4, X^5, \ldots] \subset K[X].$$

Zeige, dass für die Elemente X^2 und X^3 ein größter gemeinsamer Teiler existiert, dieser aber nicht als Linearkombination daraus darstellbar ist.

Aufgabe 8.12.*

Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 1071 und 1029.

Aufgabe 8.13. Bestimmen Sie den größten gemeinsamen Teiler von 12733 und 3983. Geben Sie eine Darstellung des ggT von 12733 und 3983 an.

Aufgabe 8.14. Bestimme in $\mathbb{Q}[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^3+2X^2+5X+2$ und $Q = X^2 + 4X - 3$.

Statt $\mathbb{Z}/(p)$ für eine Primzahl p schreiben wir gelegentlich auch $\mathbb{F}_p$.

Aufgabe 8.15. Bestimme in $\mathbb{F}_3[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^3+2X^2+X+2$ und $Q = 2X^2 + 1$.

Man gebe auch eine Darstellung des ggT an.

Aufgabe 8.16. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X, Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 8.17.*

Zeige durch Induktion, dass jede natürliche Zahl $n \geq 2$ eine Zerlegung in Primzahlen besitzt.

Aufgaben zum Abgeben

Aufgabe 8.18. (5 Punkte)

Wir betrachten eine digitale Uhr, die 24 Stunden, 60 Minuten und 60 Sekunden anzeigt. Zur Karnevalszeit läuft sie aber nicht in Sekundenschritten, sondern addiert, ausgehend von der Nullstellung, in jedem Zählschritt immer 11 Stunden, 11 Minuten und 11 Sekunden dazu. Wird bei dieser Zählweise jede mögliche digitale Anzeige erreicht? Nach wie vielen Schritten kehrt zum ersten Mal die Nullstellung zurück?

Aufgabe 8.19. (3 Punkte)

Die Wasserspedition „Alles im Eimer“ verfügt über 77-, 91- und 143-Liter Eimer, die allerdings keine Markierungen haben. Sie erhält den Auftrag, genau einen Liter Wasser von der Nordsee in die Ostsee zu transportieren. Wie kann sie den Auftrag erfüllen?

Aufgabe 8.20. (4 Punkte)

Es sei R ein Integritätsbereich und $a \in R$ ein Element. Zeige, dass a genau dann irreduzibel ist, wenn das Hauptideal (a) unter allen vom Einheitsideal verschiedenen Hauptidealen maximal ist.

Aufgabe 8.21. (3 Punkte)

Bestimme in $\mathbb{C}[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^3 + (2-i)X^2 + 4$ und $Q = (3-i)X^2 + 5X - 3$.

Man gebe auch eine Darstellung des ggT an.

Aufgabe 8.22. (4 Punkte)

Bestimme in $\mathbb{F}_5[X]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Polynome $P = X^4 + 3X^3 + X^2 + 4X + 2$ und $Q = 2X^3 + 4X^2 + X + 3$.

Man gebe auch eine Darstellung des ggT an.

Aufgabe 8.23. (4 Punkte)

Es sei R ein kommutativer Ring und $S \subseteq R$ ein Unterring. Bestätige oder widerlege die folgenden Aussagen.

(1) Zu einem Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Ideal (in S).
(2) Zu einem Radikal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Radikal.
(3) Zu einem Primideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein Primideal.
(4) Zu einem maximalen Ideal $\mathfrak{a} \subseteq R$ ist auch $\mathfrak{a} \cap S$ ein maximales Ideal.

9. Vorlesung - Faktorielle Bereiche

Faktorielle Ringe

In der letzten Vorlesung haben wir gesehen, dass in einem Hauptidealbereich einerseits jedes irreduzible Element prim ist und andererseits jedes Element ein Produkt von irreduziblen Elementen und damit auch von Primelementen ist. Wir werden gleich zeigen, dass unter diesen Voraussetzung die Zerlegung in Primelemente sogar im Wesentlichen eindeutig ist. Um dies prägnant fassen zu können, dient der Begriff des faktoriellen Bereiches.

Definition 9.1. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Satz 9.2. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*

(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein zu q_2 assoziiertes Element ergibt. Das gekürzte Element $p_2 \cdots p_s$ hat eine Faktorzerlegung mit $s-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. □

Satz 9.3. *Ein Hauptidelabereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Satz 8.8, Lemma 8.9 und Satz 9.2. □

Zerlegung in irreduzible Polynome

Wir möchten nun, abhängig von einem gewählten Grundkörper K, Aussagen über die irreduziblen Elemente in $K[X]$ und über die Primfaktorzerlegung von Polynomen treffen.

Korollar 9.4. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann besitzt jedes Polynom $F \in K[X]$, $F \neq 0$, eine eindeutige Faktorzerlegung*

$$F = \lambda P_1^{r_1} \cdots P_k^{r_k},$$

wobei $\lambda \in K$ ist und die P_i verschiedene, normierte, irreduzible Polynome sind.

Beweis. Dies folgt aus Satz 8.3, aus Satz 9.2 und daraus, dass jedes Polynom $\neq 0$ zu einem normierten Polynom assoziiert ist. □

Die irreduziblen Elemente stimmen mit den Primelementen überein, man spricht meist von *irreduziblen Polynomen*.

Beispiel 9.5. Das Polynom $X^6 - 1$ besitzt in $\mathbb{Q}[X]$ die Primfaktorzerlegung

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1),$$

die quadratischen Polynome sind nicht weiter zerlegbar, da sie in $\mathbb{Q}$ (ebenson in $\mathbb{R}$) keine Nullstelle besitzen.

Im Allgemeinen ist es schwierig, zu einem gegebenen Polynom die Primfaktorzerlegung zu finden.

Der Hauptsatz der elementaren Zahlentheorie

Wir beweisen nun, dass sich jede natürliche Zahl in eindeutiger Weise als Produkt von Primzahlen darstellen lässt.

Satz 9.6. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine eindeutige Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1 \cdots p_r$$

mit Primzahlen p_i, und dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Dies folgt aus Satz 8.4 und aus Satz 9.2. □

Exponententest

Definition 9.7. Es sei R ein faktorieller Bereich und $p \in R$ ein Primelement. Dann heißt zu jedem $f \in R$, $f \neq 0$, die natürliche Zahl $n \in \mathbb{N}$ mit $p^n | f$ aber $p^{n+1} \not| f$, der *Exponent* (oder die *Ordnung*) von f zu p. Er wird mit $\exp_p(f)$ bezeichnet.

Wenn von f die kanonische Primfaktorzerlegung

$$f = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

und p zu p_i assoziiert ist, so ist

$$\exp_p(f) = r_i.$$

Denn offenbar wird f von $p_i^{r_i}$ geteilt, aber nicht von $p_i^{r_i+1}$, da nach kürzen mit $p_i^{r_i}$ folgen würde, dass p_i einen der übrigen Faktoren $p_2, \ldots, p_k$ teilt. Insbeondere ist also der Exponent wohldefiniert.

Lemma 9.8. *Es sei R ein faktorieller Integritätsbereich und $p \in R$ ein Primelement. Dann besitzt der Exponent die Eigenschaft*

$$\exp_p(fg) = \exp_p(f) + \exp_p(g).$$

Beweis. Dies folgt aus Satz 9.2. □

Der Exponent übersetzt also die Multiplikation in die Addition.

Mit diesen Bezeichnungen kann man die Primfaktorzerlegung in einem faktoriellen Bereich als

$$f = u \prod_p p^{\nu_p(n)}$$

mit einer Einheit u schreiben, wobei das Produkt rechts endlich in dem Sinne ist, dass nur endlich viele Exponenten von 0 verschieden sind, und wobei für zueinander assoziierte Primelemente jeweils ein Vertreter genommen wird (das Produkt erstreckt sich also beispielsweise über alle positiven Primzahlen oder über alle irreduziblen normierten Polynome). Die Teilbarkeit und einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches kann man aus den Exponenten ablesen.

Lemma 9.9. *Es sei R ein faktorieller Integritätsbereich und $a, b \in R$. Dann ist a ein Teiler von b genau dann, wenn für die Exponenten zu jedem Primelement die Abschätzung*

$$\exp_p(a) \leq \exp_p(b)$$

gelten.

Beweis. (1) $\Rightarrow$ (2). Aus der Beziehung $b = ac$ folgt mit Lemma 9.8 direkt

$$\exp_p(b) = \exp_p(ac) = \exp_p(a) + \exp_p(c) \geq \exp_p(a).$$

(2) $\Rightarrow$ (1). Wir schreiben

$$a = u \prod_p p^{\exp_p(a)}$$

und

$$b = v \prod_p p^{\exp_p(b)}$$

mit Einheiten u, v. Wenn die Exponentenbedingung erfüllt ist, so ist $t = u^{-1}v\prod_p p^{\nu_p(b)-\nu_p(a)}$ ein Ringelement, das mit a multipliziert gerade b ergibt. □

Korollar 9.10. *Es sei R ein faktorieller Bereich und $a_1, \ldots, a_n \in R$ Elemente mit Primfaktorzerlegungen*

$$a_i = u_i \prod_p p^{\exp_p(a_i)}.$$

Dann ist

$$\mathrm{kgV}\,(a_1, \ldots, a_n) = \prod_p p^{\max\left(\exp_p(a_1),\ldots,\exp_p(a_n)\right)}$$

und

$$\mathrm{ggT}\,(a_1, \ldots, a_n) = \prod_p p^{\min\left(\exp_p(a_1),\ldots,\exp_p(a_n)\right)}.$$

Beweis. Dies folgt direkt aus Lemma 9.9. □

Insbesondere kann man den größten gemeinsamen Teiler primelementweise bestimmen, indem man schaut, mit welcher Potenz p in a_1, a_2 etc. aufgeht.

In einem faktoriellen Bereich muss ein größter gemeinsamer Teiler nicht als Linearkombination der Elemente darstellbar sein. Beispielsweise ist $K[X, Y]$ faktoriell, aber kein Hauptidealbereich, die beiden Variablen X und Y sind prim und teilerfremd, erzeugen aber nicht das Einheitsideal.

9. Arbeitsblatt

Übungsaufgaben

Aufgabe 9.1. Finde einen Primfaktor der Zahl $2^{25} - 1$.

Aufgabe 9.2. Finde einen Primfaktor der Zahl $2^{25} + 1$.

Aufgabe 9.3. Finde einen Primfaktor der folgenden drei Zahlen

$$2^{33} - 1,\ 2^{91} - 1,\ 2^{13} + 1\,.$$

Aufgabe 9.4.* Finde die Primfaktorzerlegung von 1728.

Aufgabe 9.5.* Man gebe zwei Primfaktoren von $2^{35} - 1$ an.

Aufgabe 9.6.*

Finde zwei natürliche Zahlen, deren Summe 65 und deren Produkt 1000 ist.

Aufgabe 9.7.*

Beweise den Satz, dass es unendlich viele Primzahlen gibt.

Aufgabe 9.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass es unendlich viele normierte irreduzible Polynome in $K[X]$ gibt.

Aufgabe 9.9. Zeige, dass in einem faktoriellen Bereich R der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache von zwei Elementen $f, g \in R$ existieren.

Aufgabe 9.10. Zeige, dass die Verknüpfung

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},\ (a,b) \longmapsto \text{kgV}\,(a,b),$$

(wobei man das kgV ≥ 0 wählt), ein Monoid definiert.

Aufgabe 9.11. Sei R ein faktorieller Bereich. Zeige, dass jedes von null verschiedene Primideal ein Primelement enthält.

Aufgabe 9.12. Charakterisiere in $\mathbb{Z}$ die Radikale mit Hilfe der Primfaktorzerlegung.

Aufgabe 9.13. Seien a, b und r positive natürliche Zahlen. Zeige, dass die Teilbarkeit $a^r | b^r$ die Teilbarkeit $a|b$ impliziert.

Aufgabe 9.14.*

a) Berechne den größten gemeinsamen Teiler der ganzen Zahlen $2 \cdot 3^2 \cdot 7^4$ und $2^4 \cdot 3^3 \cdot 5^{11} \cdot 7$.

b) Berechne den größten gemeinsamen Teiler der ganzen Zahlen $2 \cdot 3^2 \cdot 6 \cdot 7$ und $2^2 \cdot 3^3 \cdot 5^4$.

Aufgabe 9.15. Begründe, ob der größte gemeinsame Teiler zu zwei Zahlen $a, b \in \mathbb{Z}$ im Allgemeinen einfacher über die Primfaktorzerlegung der beiden Zahlen oder über den euklidischen Algorithmus zu finden ist.

Die folgenden Aufgaben zeigen, dass die eindeutige Primfaktorzerlegung keineswegs selbstverständlich ist.

Aufgabe 9.16. Es sei $M \subseteq \mathbb{N}_+$ diejenige Teilmenge, die aus allen natürlichen Zahlen besteht, die bei Division durch 4 den Rest 1 besitzen, also $M = \{1, 5, 9, 13, 17, \ldots\}$. Zeige, dass man 441 innerhalb von M auf zwei verschiedene Arten in Faktoren zerlegen kann, die in M nicht weiter zerlegbar sind.

Aufgabe 9.17. Betrachte den Unterring

$$R = K[X^2, X^3, X^4, X^5, \ldots] \subset K[X].$$

Zeige, dass X^6 zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente besitzt.

Die folgenden Aufgaben beschäftigen sich mit dem kommutativen Ring $R = K[\mathbb{Q}_{\geq 0}]$, wobei K ein fixierter Körper ist. Er besteht aus allen Ausdrücken der Form

$$a_1 X^{q_1} + a_2 X^{q_2} + \cdots + a_n X^{q_n}$$

mit $a_i \in K$ und $q_i \in \mathbb{Q}_{\geq 0}$ besteht, und wobei die Addition komponentenweise und die Multiplikation durch distributive Fortsetzung der Regel

$$X^q \cdot X^p := X^{p+q}$$

gegeben ist. Beispielsweise ist

$$\begin{aligned} \left(2X^{1/2} + 5X^{2/3}\right)\left(3X^{1/2} - 4X^{1/3}\right) &= 6X - 8X^{5/6} + 15X^{7/6} - 20X \\ &= -14X - 8X^{5/6} + 15X^{7/6}. \end{aligned}$$

Man kann sich bei $K = \mathbb{R}$ die Elemente $X^{a/b}$ als die Funktionen

$$\mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0},\ x \longmapsto x^{a/b} = \sqrt[b]{x^a}$$

vorstellen.

Aufgabe 9.18. Berechne in $R = \mathbb{R}[\mathbb{Q}_{\geq 0}]$ das Produkt

$$\left(X^2 + 4X^{3/2} - 5X + X^{1/2}\right)\left(2X^{3/2} + 4X - 7X^{1/2}\right).$$

Aufgabe 9.19. Zeige, dass man jedes Element $F \in R = K[\mathbb{Q}_{\geq 0}]$ (K ein Körper) als ein Polynom in $X^{1/b}$ mit einem $b \in \mathbb{N}_+$ schreiben kann, dass es also ein $P \in K[Y]$ derart gibt, dass $F = P(X^{1/b})$ gilt. Welches Polynom kann man bei

$$F = X^{1/2} + X^{1/3} + X^{1/5}$$

nehmen?

Aufgabe 9.20. Zeige, dass in $R = K[\mathbb{Q}_{\geq 0}]$ das Element X keine Zerlegung in irreduzible Elemente besitzt.

Aufgabe 9.21. Zeige, dass in $R = \mathbb{R}[\mathbb{Q}_{\geq 0}]$ das Element $X^2 + 1$ nicht irreduzibel ist.

Die folgende Aufgabe verwendet Logarithmen und benötigt Grundkenntnisse in linearer Algebra.

Aufgabe 9.22. Betrachte die reellen Zahlen $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum. Zeige, dass die Menge der reellen Zahlen $\ln p$, wobei p durch die Menge der Primzahlen läuft, linear unabhängig ist.

Aufgaben zum Abgeben

Aufgabe 9.23. (2 Punkte)

Man bestimme das kleinste gemeinsame Vielfache der Zahlen

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10\,.$$

Aufgabe 9.24. (4 Punkte)

Es sei S ein Integritätsbereich und $R \subseteq S$ ein Unterring mit

$$S^\times \cap R \,=\, R^\times.$$

In S besitze jede Nichteinheit eine Zerlegung in irreduzible Elemente. Zeige, dass diese Eigenschaft auch in R gilt.

Aufgabe 9.25. (4 (2+2) Punkte)

Es sei R ein kommutativer Ring und $a_1, a_2, \ldots, a_n, b, f \in R$ Elemente. Zeige die folgenden Aussagen.

1) Wenn b ein größter gemeinsamer Teiler der $a_1, a_2, \ldots, a_n$ ist, so ist auch fb ein größter gemeinsamer Teiler der $fa_1, fa_2, \ldots, fa_n$.

2) Wenn f ein Nichtnullteiler ist, so gilt hiervon auch die Umkehrung.

Aufgabe 9.26. (3 Punkte)

Es sei R ein faktorieller Bereich und $a, b \in R$. Zeige, dass ab und das Produkt aus kgV (a, b) und ggT (ab) zueinander assoziiert sind.

Aufgabe 9.27. (2 (1+1) Punkte)

Es seien $a_1, a_2, \ldots, a_n \in R$ Elemente in einem faktoriellen Bereich R und $k \in \mathbb{N}$.

a) Zeige, dass

$$\text{kgV}\left(a_1^k, a_2^k, \ldots, a_n^k\right) \text{ und } \left(\text{kgV}\left(a_1, a_2, \ldots, a_n\right)\right)^k$$

zueinander assoziiert sind.

b) Zeige, dass

$$\text{ggT}\left(a_1^k, a_2^k, \ldots, a_n^k\right) \text{ und } \left(\text{ggT}\left(a_1, a_2, \ldots, a_n\right)\right)^k$$

zueinander assoziiert sind.

Aufgabe 9.28. (5 Punkte)

Zeige, dass es in $R = \mathbb{C}[\mathbb{Q}_{\geq 0}]$ keine irreduziblen Elemente gibt.

10. Vorlesung - Homomorphismen

Gruppenhomomorphismen

Definition 10.1. Seien $(G, \circ, e_G)$ und $(H, \circ, e_H)$ Gruppen. Eine Abbildung

$$\psi : G \longrightarrow H$$

heißt *Gruppenhomomorphismus*, wenn die Gleichheit

$$\psi(g \circ g') = \psi(g) \circ \psi(g')$$

für alle $g, g' \in G$ gilt.

Beispiel 10.2. Sei $d \in \mathbb{N}$. Die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto dn,$$

ist ein Gruppenhomomorphismus. Dies folgt unmittelbar aus dem Distributivgesetz. Für $d \geq 1$ ist die Abbildung injektiv und das Bild ist die Untergruppe $\mathbb{Z}d \subseteq \mathbb{Z}$. Bei $d = 0$ liegt die Nullabbildung vor. Bei $d = 1$ ist die Abbildung die Identität, bei $d \geq 2$ ist die Abbildung nicht surjektiv.

Beispiel 10.3. Sei $d \in \mathbb{N}_+$. Wir betrachten

$$\mathbb{Z}/(d) = \{0, 1, \ldots, d-1\}$$

mit der in Aufgabe 1.19 beschriebenen Addition. Die Abbildung

$$\varphi\colon\ \mathbb{Z} \longrightarrow \mathbb{Z}/(d),$$

die eine ganze Zahl n auf ihren Rest bei Division durch d abbildet, ist ein Gruppenhomomorphismus. Sind nämlich $m = ad + r$ und $n = bd + s$ mit $0 \leq r, s < d$ gegeben, so ist

$$m + n = (a + b) + r + s,$$

wobei allerdings $r+s \geq d$ sein kann. In diesem Fall ist

$$\varphi(m+n) \;=\; r+s-d$$

und das stimmt mit der Addition von r und s in $\mathbb{Z}/(d)$ überein. Diese Abbildungen sind surjektiv, aber nicht injektiv.

Beispiel 10.4. Wir fassen den komplexen Betrag als Abbildung

$$|-| : \mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot, 1) \longrightarrow (\mathbb{R}_+, \cdot, 1),\, z \longmapsto |z|\,,$$

auf. Dabei liegen links und rechts Gruppen vor, und nach Lemma 3.15 (4) liegt ein Gruppenhomomorphismus vor. Die Abbildung ist surjektiv (da wir eben die positiven reellen Zahlen als Zielbereich gewählt haben), aber nicht injektiv, da beispielsweise der gesamte Einheitskreis auf 1 abgebildet wird.

Die folgenden beiden Lemmata folgen direkt aus der Definition.

Lemma 10.5. *Es seien G und H Gruppen und $\varphi\colon G \to H$ sei ein Gruppenhomomorphismus. Dann ist $\varphi(e_G) = e_H$ und $(\varphi(g))^{-1} = \varphi(g^{-1})$ für jedes $g \in G$.*

Beweis. Zum Beweis der ersten Aussage betrachten wir

$$\varphi(e_G) \;=\; \varphi(e_G e_G) \;=\; \varphi(e_G)\varphi(e_G).$$

Durch Multiplikation mit $\varphi(e_G)^{-1}$ folgt $e_H = \varphi(e_G)$. Zum Beweis der zweiten Behauptung ist

$$\varphi\left(g^{-1}\right)\varphi(g) \;=\; \varphi\left(g^{-1}g\right) \;=\; \varphi(e_G) \;=\; e_H.$$

Das heißt, dass $\varphi\left(g^{-1}\right)$ die Eigenschaft besitzt, die für das Inverse von $\varphi(g)$ charakteristisch ist. Da das Inverse in einer Gruppe eindeutig bestimmt ist, muss $\varphi\left(g^{-1}\right) \;=\; (\varphi(g))^{-1}$ gelten. □

Lemma 10.6. *Es seien F, G, H Gruppen. Dann gelten folgende Eigenschaften.*

(1) *Die Identität* $\mathrm{id} : G \to G$ *ist ein Gruppenhomomorphismus.*
(2) *Sind $\varphi : F \to G$ und $\psi : G \to H$ Gruppenhomomorphismen, so ist auch die Hintereinanderschaltung $\psi \circ \varphi : F \to H$ ein Gruppenhomomorphismus.*
(3) *Ist $F \subseteq G$ eine Untergruppe, so ist die Inklusion $F \hookrightarrow G$ ein Gruppenhomomorphismus.*
(4) *Sei $\{e\}$ die triviale Gruppe. Dann ist die Abbildung $\{e\} \to G$, die e auf e_G schickt, ein Gruppenhomomorphismus. Ebenso ist die (konstante) Abbildung $G \to \{e\}$ ein Gruppenhomomorphismus.*

Beweis. Siehe Aufgabe 10.1. □

Wir charakterisieren nun die Gruppenhomomorphismen von $\mathbb{Z}$ nach G.

Lemma 10.7. *Sei G eine Gruppe. Dann entsprechen sich eindeutig Gruppenelemente $g \in G$ und Gruppenhomomorphismen φ von $\mathbb{Z}$ nach G über die Korrespondenz*

$$g \longmapsto (n \mapsto g^n) \text{ und } \varphi \longmapsto \varphi(1)\,.$$

Beweis. Sei $g \in G$ fixiert. Dass die Abbildung

$$\varphi_g \colon \mathbb{Z} \longrightarrow G,\, n \longmapsto g^n,$$

ein Gruppenhomomorphismus ist, ist eine Umformulierung der Potenzgesetze. Wegen $\varphi_g(1) = g^1 = g$ erhält man aus der Potenzabbildung das Gruppenelement zurück. Umgekehrt ist ein Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$ durch $\varphi(1)$ eindeutig festgelegt, da $\varphi(n) = (\varphi(1))^n$ für n positiv und $\varphi(n) = ((\varphi(1))^{-1})^{-n}$ für n negativ gelten muss. □

Die Gruppenhomomorphismen von einer Gruppe G nach $\mathbb{Z}$ sind schwieriger zu charakterisieren. Die Gruppenhomomorphismen von $\mathbb{Z}$ nach $\mathbb{Z}$ sind die Multiplikationen mit einer festen ganzen Zahl a, also

$$\mathbb{Z} \longrightarrow \mathbb{Z},\, x \longmapsto ax.$$

Gruppenisomorphismen

Definition 10.8. Seien G und H Gruppen. Einen bijektiven Gruppenhomomorphismus

$$\varphi \colon G \longrightarrow H$$

nennt man einen *Isomorphismus* (oder eine *Isomorphie*). Die beiden Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

Beispiel 10.9. Betrachte die additive Gruppe der reellen Zahlen, also $(\mathbb{R}, 0, +)$, und die multiplikative Gruppe der positiven reellen Zahlen, also $(\mathbb{R}_+, 1, \cdot)$. Dann ist die Exponentialabbildung

$$\exp \colon \mathbb{R} \longrightarrow \mathbb{R}_+,\, x \longmapsto \exp(x),$$

ein Gruppenisomorphismus. Dies beruht auf grundlegenden analytischen Eigenschaften der Exponentialfunktion. Die Homomorphieeigenschaft ist lediglich eine Umformulierung des Exponentialgesetzes

$$\exp(x+y) \;=\; e^{x+y} \;=\; e^x e^y \;=\; \exp(x)\exp(y).$$

Die Injektivität der Abbildung folgt aus der strengen Monotonie, die Surjektivität folgt aus dem Zwischenwertsatz. Die Umkehrabbildung ist der natürliche Logarithmus, der somit ebenfalls ein Gruppenisomorphismus ist.

Lemma 10.10. *Seien G und H Gruppen und sei*

$$\varphi \colon G \longrightarrow H$$

ein Gruppenisomorphismus. Dann ist auch die Umkehrabbildung

$$\varphi^{-1} \colon H \longrightarrow G,\, h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus.

Beweis. Dies folgt aus $\varphi^{-1}(e_H) = e_G$ und aus

$$\begin{aligned} \varphi^{-1}(h_1h_2) &= \varphi^{-1}\left(\varphi(\varphi^{-1}(h_1))\varphi(\varphi^{-1}(h_2))\right) \\ &= \varphi^{-1}\left(\varphi(\varphi^{-1}(h_1)\varphi^{-1}(h_2))\right) \\ &= \varphi^{-1}(h_1)\varphi^{-1}(h_2). \end{aligned}$$

□

Isomorphe Gruppen sind bezüglich ihrer gruppentheoretischen Eigenschaften als gleich anzusehen. Isomorphismen einer Gruppe auf sich selbst nennt man auch *Automorphismen.*

Der Kern eines Gruppenhomomorphismus

Definition 10.11. Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann nennt man das Urbild des neutralen Elementes den *Kern* von φ, geschrieben

$$\operatorname{kern}\varphi = \varphi^{-1}(e_H) = \{g \in G |\, \varphi(g) = e_H\}\ .$$

Lemma 10.12. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern von φ eine Untergruppe von G.

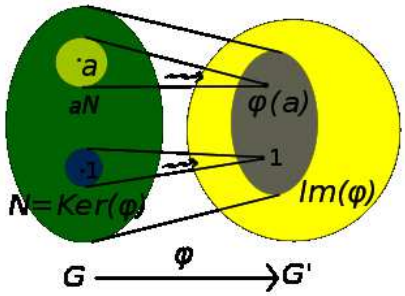
Beweis. Wegen $\varphi(e_G) = e_H$ ist $e_G \in \ker\varphi$. Seien $g, g' \in \ker\varphi$. Dann ist

$$\varphi(gg') = \varphi(g)\varphi(g') = e_He_H = e_H$$

und daher ist auch $gg' \in \ker\varphi$. Der Kern ist also ein Untermonoid. Sei nun $g \in \ker\varphi$ und betrachte das inverse Element g^{-1}. Es ist

$$\varphi(g^{-1}) = (\varphi(g))^{-1} = e_H^{-1} = e_H\,,$$

also auch $g^{-1} \in \ker\varphi$. □



Lemma 10.13. *Seien G und H Gruppen. Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn der Kern von φ trivial ist.*

Beweis. Wenn φ injektiv ist, so darf auf jedes Element $h \in H$ höchstens ein Element aus G gehen. Da e_G auf e_H geschickt wird, darf kein weiteres Element auf e_H gehen, d.h. $\ker \varphi = \{e_G\}$. Sei umgekehrt dies der Fall und sei angenommen, dass $g, \tilde{g} \in G$ beide auf $h \in H$ geschickt werden. Dann ist

$$\varphi\left(g\tilde{g}^{-1}\right) = \varphi(g)\varphi(\tilde{g})^{-1} = hh^{-1} = e_H$$

und damit ist $g\tilde{g}^{-1} \in \ker \varphi$, also $g\tilde{g}^{-1} = e_G$ nach Voraussetzung und damit $g = \tilde{g}$. □

Das Bild eines Gruppenhomomorphismus

Lemma 10.14. *Seien G und H Gruppen und sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild von φ eine Untergruppe von H.*

Beweis. Sei $B := \text{bild } \varphi$. Dann ist $e_H = \varphi(e_G) \in B$. Seien $h_1, h_2 \in B$. Dann gibt es $g_1, g_2 \in G$ mit $\varphi(g_1) = h_1$ und $\varphi(g_2) = h_2$. Damit ist $h_1 + h_2 = \varphi(g_1) + \varphi(g_2) = \varphi(g_1 + g_2) \in B$. Ebenso gibt es für $h \in B$ ein $g \in G$ mit $\varphi(g) = h$. Somit ist $h^{-1} = (\varphi(g))^{-1} = \varphi(g^{-1}) \in B$. □

Beispiel 10.15. Betrachte die analytische Abbildung

$$\mathbb{R} \longrightarrow \mathbb{C},\ t \longmapsto e^{it} = \cos t + i \sin t.$$

Aufgrund des Exponentialgesetzes ist $e^{i(t+s)} = e^{it}e^{is}$ und $e^{i0} = e^0 = 1$. Daher liegt ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{R}, +, 0)$ in die multiplikative Gruppe $(\mathbb{C}^\times, \cdot, 1)$ vor. Wir bestimmen den Kern und das Bild dieser Abbildung. Für den Kern muss man diejenigen reellen Zahlen t bestimmen, für die

$$\cos t = 1 \text{ und } \sin t = 0$$

ist. Aufgrund der Periodizität der trigonometrischen Funktionen ist dies genau dann der Fall, wenn t ein Vielfaches von 2π ist. Der Kern ist also die Untergruppe $2\pi\mathbb{Z}$. Für einen Bildpunkt gilt $|e^{it}| = \sin^2 t + \cos^2 t = 1$, so dass der Bildpunkt auf dem komplexen Einheitskreis liegt. Andererseits durchlaufen die trigonometrischen Funktionen den gesamten Einheitskreis, so dass die Bildgruppe der Einheitskreis mit der komplexen Multiplikation ist.

10. Arbeitsblatt

Übungsaufgaben

Aufgabe 10.1. Beweise Lemma 10.6.

Aufgabe 10.2. Sei G eine (multiplikativ geschriebene) kommutative Gruppe und sei $n \in \mathbb{N}$. Zeige, dass das Potenzieren

$$G \longrightarrow G,\, x \longmapsto x^n,$$

ein Gruppenhomomorphismus ist.

Aufgabe 10.3. Es sei G eine additiv geschriebene kommutative Gruppe. Zeige, dass die Negation, also die Abbildung

$$G \longrightarrow G,\, x \longmapsto -x,$$

ein Gruppenisomorphismus ist.

Aufgabe 10.4.*

Es sei G eine kommutative Gruppe und

$$\varphi\colon\, G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Zeige, dass H ebenfalls kommutativ ist.

Aufgabe 10.5.*

Bestimme, ob die durch die Gaußklammer gegebene Abbildung

$$\mathbb{Q} \longrightarrow \mathbb{Z},\, q \longmapsto \lfloor q \rfloor,$$

ein Gruppenhomomorphismus ist oder nicht.

Aufgabe 10.6.*

Es sei R ein kommutativer Ring und $h \in R$. Zeige, dass die Abbildung

$$R \longrightarrow R,\, f \longmapsto hf,$$

ein Gruppenhomomorphismus ist. Beschreibe das Bild und den Kern dieser Abbildung.

Aufgabe 10.7. a) Für welche reellen Polynome $P \in \mathbb{R}[X]$ ist die zugehörige polynomiale Abbildung

$$(\mathbb{R}, 0, +) \longrightarrow (\mathbb{R}, 0, +),\ x \longmapsto P(x),$$

ein Gruppenhomomorphismus?

b) Für welche reellen Polynome $Q \in \mathbb{R}[X]$ ist allenfalls 0 eine Nullstelle und die zugehörige polynomiale Abbildung

$$(\mathbb{R}^\times, 1, \cdot) \longrightarrow (\mathbb{R}^\times, 1, \cdot),\ x \longmapsto Q(x),$$

ein Gruppenhomomorphismus?

Aufgabe 10.8. Sei $d \in \mathbb{N}_{\geq 2}$. Wir betrachten

$$\mathbb{Z}/(d) = \{0, 1, \ldots, d-1\}$$

mit der in Aufgabe 1.19 beschriebenen Addition. Zeige, dass die Abbildung

$$\psi\colon\ \mathbb{Z}/(d) \longrightarrow \mathbb{Z},\ r \longmapsto r,$$

kein Gruppenhomomorphismus ist.

Wir erinnern an den Begriff einer Matrix.

Sei R ein kommutativer Ring. Unter einer $m \times n$-*Matrix* (über R) versteht man einen Ausdruck der Form

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix},$$

wobei die Einträge a_{ij} aus R sind.

Aufgabe 10.9. Es sei R ein kommutativer Ring und

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

eine Matrix über R. Zeige, dass die Matrix einen Gruppenhomomorphismus

$$R^n \longrightarrow R^m$$

definiert, indem man

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

anwendet, wobei

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} a_{1i}x_i \\ \sum_{i=1}^{n} a_{2i}x_i \\ \vdots \\ \sum_{i=1}^{n} a_{mi}x_i \end{pmatrix}$$

ist.

Aufgabe 10.10. In einer Kekspackung befinden sich Schokokekse, Waffelröllchen, Mandelsterne und Nougatringe. Die Kalorien, der Vitamin C-Gehalt und der Anteil an linksdrehenden Fettsäuren werden durch folgende Tabelle (in geeigneten Maßeinheiten) wiedergegeben:

Sorte	Kalorien	Vitamin C	Fett
Schokokeks	10	5	3
Waffelröllchen	8	7	6
Mandelstern	7	3	1
Nougatring	12	0	5

a) Beschreibe mit einer Matrix die Abbildung, die zu einem Verzehrtupel (x, y, z, w) das Aufnahmetupel (K, V, F) berechnet.

b) Heinz isst 100 Schokokekse. Berechne seine Vitaminaufnahme.

c) Ludmilla isst 10 Nougatringe und 11 Waffelröllchen. Berechne ihre Gesamtaufnahme an Nährstoffen.

d) Peter isst 5 Mandelsterne mehr und 7 Schokokekse weniger als Fritz. Bestimme die Differenz ihrer Kalorienaufnahme.

Matrizen werden miteinander multipliziert, indem jede Zeile der linken Matrix mit jeder Spalte der rechten Matrix gemäß der Merkregel

$$(ZEILE)\begin{pmatrix} S \\ P \\ A \\ L \\ T \end{pmatrix} = ZS + EP + IA + LL + ET$$

multipliziert wird (insbesondere muss die Spaltenanzahl der linken Matrix mit der Zeilenanzahl der rechten Matrix übereinstimmen) und das Ergebnis an die entsprechende Stelle gesetzt wird.

Aufgabe 10.11. Berechne das Matrizenprodukt

$$\begin{pmatrix} Z & E & I & L & E \\ R & E & I & H & E \\ H & O & R & I & Z \\ O & N & T & A & L \end{pmatrix} \cdot \begin{pmatrix} S & E & I \\ P & V & K \\ A & E & A \\ L & R & A \\ T & T & L \end{pmatrix}.$$

Aufgabe 10.12. Es sei K ein Körper und sei

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K,\ ad - bc \neq 0 \right\}$$

die Menge aller invertierbaren 2×2-Matrizen.

a) Zeige, dass M mit der Matrizenmultiplikation eine Gruppe bildet.

b) Zeige, dass die Abbildung

$$M \longrightarrow K^\times,\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto ad - bc,$$

ein Gruppenhomomorphismus ist.

Aufgabe 10.13. Es sei M eine endliche Menge und $T \subseteq M$ eine Teilmenge, und es seien Aut T und Aut M die zugehörigen Automorphismengruppen(also die Menge aller bijektiven Abbildungen auf M, siehe Aufgabe 1.5). Zeige, dass durch

$$\Psi\colon\ \text{Aut } T \longrightarrow \text{Aut } M,\ \varphi \longmapsto \tilde{\varphi},$$

mit

$$\tilde{\varphi}(x) = \begin{cases} \varphi(x), \text{ falls } x \in T, \\ x \text{ sonst}, \end{cases}$$

ein injektiver Gruppenhomomorphismus gegeben ist.

Aufgabe 10.14. Es sei G eine Gruppe und $h \in G$. Zeige, dass die Abbildung

$$G \longrightarrow G,\, g \longmapsto hgh^{-1},$$

eine Gruppenautomorphismus ist.

Die Automorphismen der vorstehenden Aufgabe nennt man auch *innere Automorphismen*.

Aufgabe 10.15. Sei G eine Gruppe und sei $g \in G$ ein Element und sei

$$\varphi\colon\, G \longrightarrow G,\, h \longmapsto hg,$$

die Multiplikation mit g. Zeige, dass φ bijektiv ist, und dass φ genau dann ein Gruppenhomomorphismus ist, wenn $g = e_G$ ist.

Aufgaben zum Abgeben

Aufgabe 10.16. (3 (1+2) Punkte)

Es seien $G_1, \ldots, G_n$ Gruppen.

a) Definiere eine Gruppenstruktur auf dem Produkt

$$G_1 \times \cdots \times G_n\,.$$

b) Es sei H eine weitere Gruppe. Zeige, dass eine Abbildung

$$\varphi\colon\, H \longrightarrow G_1 \times \cdots \times G_n,\, x \longmapsto \varphi(x) = (\varphi_1(x), \ldots, \varphi_n(x)),$$

genau dann ein Gruppenhomomorphismus ist, wenn alle Komponenten φ_i Gruppenhomomorphismen sind.

Aufgabe 10.17. (4 Punkte)

Bestimme die Gruppenhomomorphismen von $(\mathbb{Q}, +, 0)$ nach $(\mathbb{Z}, +, 0)$.

Die folgende Aufgabe knüpft an Aufgabe 1.20 an. Zu einer reellen Zahl x bezeichnet $\lfloor x \rfloor$ die größte ganze Zahl, die kleiner oder gleich x ist.

Aufgabe 10.18. (3 Punkte)

Wir betrachten

$$M \,=\, \{q \in \mathbb{Q} |\, 0 \leq q < 1\}$$

mit der in Aufgabe 1.17 definierten Verknüpfung, die nach Aufgabe 1.20 eine Gruppe ist. Zeige, dass die Abbildung

$$\mathbb{Q} \longrightarrow M,\, q \longmapsto q - \lfloor q \rfloor,$$

ein Gruppenhomomorphismus ist.

Aufgabe 10.19. (2 Punkte)

Bestimme für jedes $n \in \mathbb{N}$ den Kern des Potenzierens

$$\mathbb{R}^\times \longrightarrow \mathbb{R}^\times,\, z \longmapsto z^n.$$

Aufgabe 10.20. (1 Punkt)

Zeige, dass es keinen Gruppenhomomorphismus

$$\varphi\colon\, (\mathbb{R}, 0, +) \longrightarrow G$$

in eine Gruppe G mit der Eigenschaft gibt, dass $r \in \mathbb{R}$ genau dann irrational ist, wenn $\varphi(r) = 0$ ist.

11. Vorlesung - Nebenklassen

Nebenklassen

Definition 11.1. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wir setzen $x \sim_H y$ (und sagen, dass x und y äquivalent sind) wenn $x^{-1}y \in H$.

Dies ist in der Tat eine Äquivalenzrelation: Aus $x^{-1}x = e_G \in H$ folgt, dass diese Relation reflexiv ist. Aus $x^{-1}y \in H$ folgt sofort $y^{-1}x = (x^{-1}y)^{-1} \in H$ und aus $x^{-1}y \in H$ und $y^{-1}z \in H$ folgt $x^{-1}z \in H$.

Definition 11.2. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann heißt zu jedem $x \in G$ die Teilmenge

$$xH \,=\, \{xh|\, h \in H\}$$

die *Linksnebenklasse von* x in G bezüglich H. Jede Teilmenge von dieser Form heißt *Linksnebenklasse*. Entsprechend heißt eine Menge der Form

$$Hy \,=\, \{hy|\, h \in H\}$$

Rechtsnebenklasse (zu y).

Die Äquivalenzklassen zu der oben definierten Äquivalenzrelation sind wegen

$$\begin{array}{rcl} [x] & = & \{y \in G|\, x \sim y\} \\ & = & \left\{y \in G|\, x^{-1}y \in H\right\} \\ & = & \left\{y \in G|\, \text{es gibt } h \in H \text{ mit } x^{-1}y = h\right\} \\ & = & \{y \in G|\, \text{es gibt } h \in H \text{ mit } y = xh\} \\ & = & xH \end{array}$$

genau die Linksnebenklassen. Die Linksnebenklassen bilden somit eine disjunkte Zerlegung (eine *Partition*) von G. Dies gilt ebenso für die Rechtsnebenklassen. Im kommutativen Fall muss man nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

Lemma 11.3. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Es seien $x, y \in G$ zwei Elemente. Dann sind folgende Aussagen äquivalent.*

(1) $x \in yH$
(2) $y \in xH$
(3) $y^{-1}x \in H$
(4) $x^{-1}y \in H$
(5) $xH \cap yH \neq \emptyset$
(6) $x \sim_H y$.
(7) $xH = yH$.

Beweis. Die Äquivalenz von (1) und (3) (und die von (2) und (4)) folgt aus Multiplikation mit y^{-1} bzw. mit y. Die Äquivalenz von (3) und (4) folgt durch Übergang zum Inversen. Aus (1) folgt (5) wegen $1 \in H$. Wenn (5) erfüllt ist, so bedeutet das $xh_1 = yh_2$ mit $h_1, h_2 \in H$. Damit ist $x = yh_2h_1^{-1}$ und (1) ist erfüllt. (4) und (6) sind nach Definition 11.1 äquivalent. Da die Nebenklassen Äquivalenzklassen sind, ergibt sich die Äquivalenz von (5) und (7). □

Beispiel 11.4. Zu $d \in \mathbb{N}$ bzw. zur Untergruppe $\mathbb{Z}d \subseteq \mathbb{Z}$ gibt es die d Nebenklassen

$$\mathbb{Z}d, 1 + \mathbb{Z}d, 2 + \mathbb{Z}d, \ldots, d - 1 + \mathbb{Z}d\,.$$

Die Nebenklasse $i + \mathbb{Z}d$ besteht aus allen ganzen Zahlen, die bei Division durch d den Rest i ergeben.

Beispiel 11.5. Wir betrachten die Einheitengruppe von $\mathbb{C}$, also $(\mathbb{C}^\times, 1, \cdot)$.

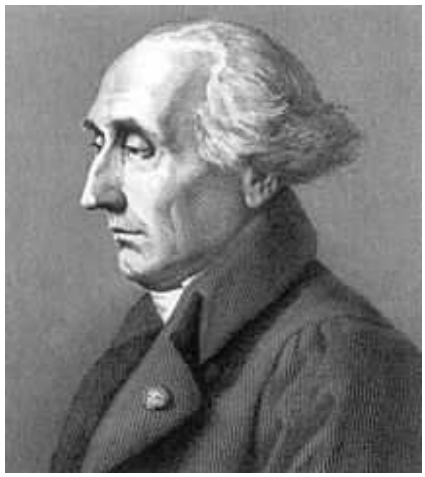
Zur Untergruppe $\mathbb{R}_+ \subseteq \mathbb{C}^\times$ sind zwei komplexe Zahlen äquivalent, wenn sie durch Multiplikation mit einer positiven reellen Zahl auseinander hervorgehen. Die Nebenklassen sind also die Halbstrahlen, die vom Nullpunkt ausgehen.

Zur Untergruppe $S^1 = \{z \in \mathbb{C} |\ |z| = 1\} \subseteq \mathbb{C}^\times$ sind zwei komplexe Zahlen äquivalent, wenn sie den gleichen Betrag besitzen, also durch eine Drehung ineinander überführbar sind. Die Nebenklassen sind also die Kreise mit dem Nullpunkt als Mittelpunkt.

Der Satz von Lagrange

Satz 11.6. *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann ist ihre Kardinalität $\#(H)$ ein Teiler von $\#(G)$.*

Beweis. Betrachte die Linksnebenklassen $gH := \{gh |\ h \in H\}$ für sämtliche $g \in G$. Es ist $h \mapsto gh$ eine Bijektion zwischen H und gH, so dass alle Nebenklassen gleich groß sind (und zwar $\#(H)$ Elemente haben). Die Nebenklassen bilden (als Äquivalenzklassen) zusammen eine Zerlegung von G, so dass $\#(G)$ ein Vielfaches von $\#(H)$ sein muss. □



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Korollar 11.7. *Sei G eine endliche Gruppe und sei $g \in G$ ein Element. Dann teilt die Ordnung von g die Gruppenordnung.*

Beweis. Sei H die von g erzeugte Untergruppe. Nach Lemma 1.9 ist $\operatorname{ord}(g) = \operatorname{ord}(H)$. Daher teilt diese Zahl nach Satz 11.6 die Gruppenordnung von G. □

Definition 11.8. Zu einer Untergruppe $H \subseteq G$ heißt die Anzahl der (Links- oder Rechts)Nebenklassen der *Index* von H in G, geschrieben

$$\operatorname{ind}_G H\,.$$

In der vorstehenden Definition ist Anzahl im allgemeinen als die *Mächtigkeit* einer Menge zu verstehen. Der Index wird aber hauptsächlich dann verwendet, wenn er endlich ist, wenn es also nur endlich viele Nebenklassen gibt. Das ist bei endlichem G automatisch der Fall, kann aber auch bei unendlichem G der Fall sein, wie schon die Beispiele $\mathbb{Z}n \subseteq \mathbb{Z}$, , zeigen. Wenn G eine endliche Gruppe ist und $H \subseteq G$ eine Untergruppe, so gilt aufgrund des Satzes von Lagrange die einfache *Indexformel*

$$\#(G) \;=\; \#(H) \cdot \operatorname{ind}_G H.$$

Normalteiler

Definition 11.9. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Man nennt H einen *Normalteiler*, wenn

$$xH \;=\; Hx$$

für alle $x \in G$ ist, wenn also die Linksnebenklasse zu x mit der Rechtsnebenklasse zu x übereinstimmt.

Bei einem Normalteiler braucht man nicht zwischen Links- und Rechtsnebenklassen zu unterscheiden und spricht einfach von *Nebenklassen*. Statt xH oder Hx schreiben wir meistens $[x]$. Die Gleichheit $xH = Hx$ bedeutet *nicht*, dass $xh = hx$ für alle $h \in H$ ist, sondern lediglich, dass es zu jedem $h \in H$ ein $\tilde{h} \in H$ gibt mit $xh = \tilde{h}x$.

Lemma 11.10. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Aussagen äquivalent.*

(1) *H ist ein Normalteiler*
(2) *Es ist $xhx^{-1} \in H$ für alle $x \in G$ und $h \in H$.*
(3) *H ist invariant unter jedem inneren Automorphismus von G.*

Beweis. (1) bedeutet bei gegebenem $h \in H$, dass man $xh = \tilde{h}x$ mit einem $\tilde{h} \in H$ schreiben kann. Durch Multiplikation mit x^{-1} von rechts ergibt sich $xhx^{-1} = \tilde{h} \in H$, also (2). Dieses Argument rückwärts ergibt die Implikation (2) $\Rightarrow$ (1). Ferner ist (2) eine explizite Umformulierung von (3). □

Beispiel 11.11. Wir betrachten die Permutationsgruppe $G = S_3$ zu einer dreielementigen Menge, d.h. S_3 besteht aus den bijektiven Abbildungen der Menge $\{1, 2, 3\}$ in sich. Die triviale Gruppe $\{\mathrm{id}\}$ und die ganze Gruppe sind Normalteiler. Die Teilmenge $H = \{\mathrm{id}, \varphi\}$, wobei φ die Elemente 1 und 2 vertauscht und 3 unverändert lässt, ist eine Untergruppe. Sie ist aber kein Normalteiler. Um dies zu zeigen, sei ψ die Bijektion, die 1 fest lässt und 2 und 3 vertauscht. Dieses ψ ist zu sich selbst invers. Die Konjugation $\psi\varphi\psi^{-1} = \psi\varphi\psi$ ist dann die Abbildung, die 1 auf 3, 2 auf 2 und 3 auf 1 schickt, und diese Bijektion gehört nicht zu H.

Lemma 11.12. *Seien G und H Gruppen und sei*

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern $\ker\varphi$ *ein Normalteiler in G.*

Beweis. Wir verwenden Lemma 11.10. Sei also $x \in G$ beliebig und $h \in \ker\varphi$. Dann ist

$$\varphi\left(xhx^{-1}\right) = \varphi(x)\varphi(h)\varphi\left(x^{-1}\right) = \varphi(x)e_H\varphi\left(x^{-1}\right) = \varphi(x)\varphi(x)^{-1} = e_H,$$

also gehört xhx^{-1} ebenfalls zum Kern. □

11. Arbeitsblatt

Übungsaufgaben

Aufgabe 11.1. Bestimme die Nebenklassen zu den folgenden Untergruppen von kommutativen Gruppen.

(1) $(\mathbb{Z}, 0, +) \subseteq (\mathbb{R}, 0, +)$.
(2) $(\mathbb{Q}, 0, +) \subseteq (\mathbb{R}, 0, +)$.
(3) $(\mathbb{R}, 0, +) \subseteq (\mathbb{C}, 0, +)$.
(4) $(\mathbb{Z}n, 0, +) \subseteq (\mathbb{Z}, 0, +)$ $(n \in \mathbb{N})$.
(5) $(\{z \in \mathbb{C} |\ |z| = 1\}, 1, \cdot) \subseteq (\mathbb{C} \setminus \{0\}, 1, \cdot)$.
(6) $(\{z \in \mathbb{C} |\ z^n = 1\}, 1, \cdot) \subseteq (\{z \in \mathbb{C} |\ |z| = 1\}, 1, \cdot)$ $(n \in \mathbb{N})$.

Wann bestehen die Nebenklassen aus endlich vielen Elementen, wann ist der Index endlich?

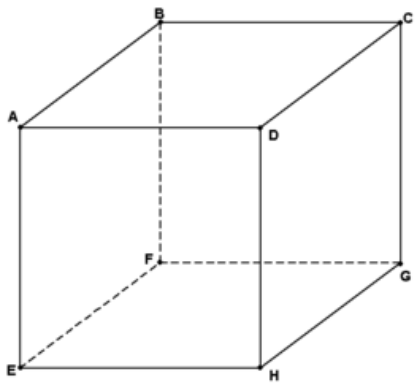
Aufgabe 11.2. Sei p eine Primzahl und sei G eine Gruppe der Ordnung p. Zeige, dass G eine zyklische Gruppe ist.

Aufgabe 11.3.*

Es sei R ein kommutativer Ring mit p Elementen, wobei p eine Primzahl sei. Zeige, dass R ein Körper ist.

Aufgabe 11.4. Bestimme die Untergruppen von $\mathbb{Z}/(15)$.

Aufgabe 11.5. Es sei $G = S_3$ die Permutationsgruppe zu einer dreielementigen Menge. Welche Zahlen treten als Ordnungen von Untergruppen und welche als Ordnungen von Elementen auf?



Eine *eigentliche Würfelsymmetrie* ist eine Bewegung an einem Würfel, die ihn in sich selbst überführt.

Aufgabe 11.6. Welche Zahlen treten als Ordnungen von eigentlichen Würfelsymmetrien auf? Beschreibe die Wirkungsweise der Symmetrie auf den Eckpunkten, den Kanten und den Seiten des Würfels sowie auf den Raumdiagonalachsen, den Seitenmittelpunktsachsen und den Kantenmittelpunktsachsen.

Aufgabe 11.7.*

Seien G und H Gruppen und sei

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Zeige, dass das Urbild $\varphi^{-1}(N)$ eines Normalteilers $N \subseteq H$ ein Normalteiler in G ist.

Aufgabe 11.8. Zeige, dass der Durchschnitt von Normalteilern N_i, $i \in I$, in einer Gruppe G ist ein Normalteiler.

Aufgabe 11.9. Seien G und H Gruppen und sei

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Ist das Bild von φ ein Normalteiler in H?

In den folgenden Aufgaben werden Äquivalenzrelationen wiederholt.

Aufgabe 11.10. Auf den ganzen Zahlen $\mathbb{Z}$ lebe eine Kolonie von Flöhen, und jeder Flohsprung geht fünf Einheiten weit (in beide Richtungen). Wie viele Flohpopulationen gibt es? Wie kann man einfach charakterisieren, ob zwei Flöhe zur gleichen Population gehören oder nicht?

Aufgabe 11.11. Betrachte die Schachfiguren Turm, Läufer, Pferd und Esel zusammen mit ihren erlaubten Zügen auf einem 8×8-Schachbrett. Ein Esel darf dabei pro Zug einen Doppelschritt nach vorne, nach hinten, nach rechts oder nach links machen. Jede dieser Figuren definiert eine Äquivalenzrelation auf den 64 Feldern, indem zwei Felder als äquivalent angesehen werden, wenn das eine Feld von dem anderen Feld aus mit dieser Figur in endlich vielen Zügen erreichbar ist. Beschreibe für jede dieser Schachfiguren die zugehörige Äquivalenzrelation und ihre Äquivalenzklassen. Wie sieht es auf einem 3×3-Schachbrett aus?

Aufgabe 11.12. Sei B ein Blatt Papier (oder ein Taschentuch). Man versuche, sich die folgenden Äquivalenzrelationen auf B und die zugehörige Identifizierungsabbildungen vorzustellen (möglichst geometrisch).

(1) Die vier Eckpunkte sind untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(2) Alle Randpunkte sind untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(3) Jeder Punkt des linken Randes ist äquivalent zu seinem horizontal gegenüber liegenden Punkt am rechten Rand, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(4) Jeder Punkt des linken Randes ist äquivalent zu seinem horizontal gegenüber liegenden Punkt am rechten Rand und jeder Punkt des oberen Randes ist äquivalent zu seinem vertikal gegenüber liegenden Punkt, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(5) Jeder Punkt des Randes ist äquivalent zu seinem punktsymmetrisch (bezüglich des Mittelpunktes des Blattes) gegenüber liegenden Punkt, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(6) Sei K ein Kreis (d.h. eine Kreislinie) auf dem Blatt. Alle Kreispunkte seien untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(7) Es gebe zwei Punkte $P \neq Q$, die untereinander äquivalent seien, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(8) Sei H die horizontale Halbierungsgerade des Blattes. Zwei Punkte sind genau dann äquivalent, wenn sie achsensymmetrisch zu H sind.

Aufgabe 11.13. Es sei K ein Körper und V ein K-Vektorraum. Zeige, dass die Relation auf V, die durch

$$v \sim w, \text{ falls es ein } \lambda \in K, \lambda \neq 0, \text{ mit } v = \lambda w \text{ gibt}$$

eine Äquivalenzrelation ist. Was sind die Äquivalenzklassen?

Aufgaben zum Abgeben

Aufgabe 11.14. (2 Punkte)

Bestimme die Untergruppen von $\mathbb{Z}/(20)$.

Aufgabe 11.15. (3 Punkte)

Sei M eine endliche Menge und sei σ eine Permutation auf M und $x \in M$. Zeige, dass $\{n \in \mathbb{Z} | \, \sigma^n(x) = x\}$ eine Untergruppe von $\mathbb{Z}$ ist. Den eindeutig bestimmten nichtnegativen Erzeuger dieser Untergruppe bezeichnen wir mit $\operatorname{ord}_x \sigma$. Zeige die Beziehung

$$\operatorname{ord}(\sigma) = \operatorname{kgV}\{\operatorname{ord}_x \sigma | \, x \in M\} \ .$$

Aufgabe 11.16. (2 Punkte)

Seien G und H Gruppen und sei

$$\varphi \colon G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Zeige, dass das Bild $\varphi(N)$ eines Normalteilers $N \subseteq G$ ein Normalteiler in H ist.

Aufgabe 11.17. (2 Punkte)

Zeige, dass jede Untergruppe vom Index zwei in einer Gruppe G ein Normalteiler in G ist.

Aufgabe 11.18. (2 Punkte)

Sei G eine Gruppe und sei M eine Menge mit einer Verknüpfung. Es sei

$$\varphi \colon G \longrightarrow M$$

eine surjektive Abbildung mit $\varphi(gh) = \varphi(g)\varphi(h)$ für alle $g, h \in G$. Zeige, dass M eine Gruppe und φ ein Gruppenhomomorphismus ist.

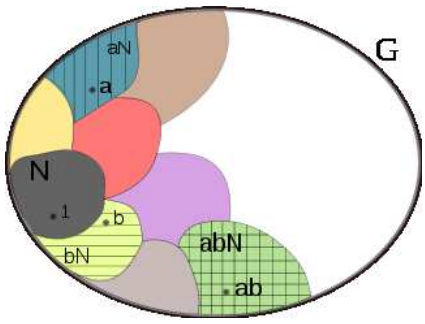
Aufgabe 11.19. (5 Punkte)

Man gebe ein Beispiel von drei Untergruppen $F \subseteq G \subseteq H$ an derart, dass F ein Normalteiler in G und G ein Normalteiler in H, aber F kein Normalteiler in H ist.

12. Vorlesung - Restklassenbildung

Restklassenbildung

In der letzten Vorlesung haben wir in Lemma 11.12 gesehen, dass der Kern eines Gruppenhomomorphismus ein Normalteiler ist. Wir zeigen nun umgekehrt, dass sich jeder Normalteiler als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt.



Die Multiplikation der Nebenklassen zu einem Normalteiler $N \subseteq G$.

Satz 12.1. *Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Es sei G/H die Menge der Nebenklassen (die Quotientenmenge) und*

$$q\colon\ G \longrightarrow G/H,\ g \longmapsto [g],$$

die kanonische Projektion. Dann gibt es eine eindeutig bestimmte Gruppenstruktur auf G/H derart, dass q ein Gruppenhomomorphismus ist.

Beweis. Da die kanonische Projektion zu einem Gruppenhomomorphismus werden soll, muss die Verknüpfung durch

$$[x][y] = [xy]$$

gegeben sein. Wir müssen also zeigen, dass durch diese Vorschrift eine wohldefinierte Verknüpfung auf G/H definiert ist, die unabhängig von der Wahl der Repräsentanten ist. D.h. wir haben für $[x] = [x']$ und $[y] = [y']$ zu zeigen, dass $[xy] = [x'y']$ ist. Nach Voraussetzung können wir $x' = xh$ und $hy' = \tilde{h}y = yh'$ mit $h, \tilde{h}, h' \in H$ schreiben. Damit ist

$$x'y' = (xh)y' = x(hy') = x(yh') = xyh'.$$

Somit ist $[xy] = [x'y']$. Aus der Wohldefiniertheit der Verknüpfung auf G/H folgen die Gruppeneigenschaften, die Homomorphieeigenschaft der Projektion und die Eindeutigkeit. □

Definition 12.2. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 12.1 eindeutig bestimmten Gruppenstruktur heißt *Restklassengruppe von G modulo H*. Die Elemente $[g] \in G/H$ heißen *Restklassen*. Für eine Restklasse $[g]$ heißt jedes Element $g' \in G$ mit $[g'] = [g]$ ein *Repräsentant* von $[g]$.

Beispiel 12.3. Die Untergruppen der ganzen Zahlen sind nach Satz 5.2 von der Form $\mathbb{Z}n$ mit $n \geq 0$. Die Restklassengruppen werden mit

$$\mathbb{Z}/(n)$$

bezeichnet (sprich „$\mathbb{Z}$ modulo n“). Bei $n = 0$ ist das einfach $\mathbb{Z}$ selbst, bei $n = 1$ ist das die triviale Gruppe. Im Allgemeinen ist die durch die Untergruppe $\mathbb{Z}n$ definierte Äquivalenzrelation auf $\mathbb{Z}$ dadurch gegeben, dass zwei ganze Zahlen a und b genau dann äquivalent sind, wenn ihre Differenz $a - b$ zu $\mathbb{Z}n$ gehört, also ein Vielfaches von n ist. Daher ist (bei $n \geq 1$) jede ganze Zahl zu genau einer der n Zahlen

$$0, 1, 2, \ldots, n-1$$

äquivalent (oder, wie man auch sagt, *kongruent modulo* n), nämlich zum Rest, der sich bei Division durch n ergibt. Diese Reste bilden also ein Repräsentantensystem für die Restklassengruppe, und diese besitzt n Elemente. Die Tatsache, dass die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\ a \longmapsto [a] = a \mod n,$$

ein Homomorphismus ist, kann man auch so ausdrücken, dass der Rest einer Summe von zwei ganzen Zahlen nur von den beiden Resten, nicht aber von den Zahlen selbst, abhängt. Als Bild der zyklischen Gruppe $\mathbb{Z}$ ist auch $\mathbb{Z}/(n)$ zyklisch, und zwar ist 1 (aber auch -1) stets ein Erzeuger.

Wie bei jeder Äquivalenzrelation $\sim$ auf G nennt man eine Teilmenge $R \subseteq G$ ein Repräsentantensystem für die Äquivalenzrelation, wenn jede Äquivalenzklasse genau ein Element aus R enthält. Dies bedeutet, dass die Abbildung $R \to G/\sim$ bijektiv ist. Solche Repräsentantensysteme gibt es immer. In unserem gruppentheoretischen Kontext gibt es manchmal eine Untergruppe $F \subseteq G$ mit der Eigenschaft, dass die Gesamtabbildung

$$F \longrightarrow G/H,\ f \longmapsto [f],$$

bijektiv und damit ein Isomorphismus ist. Dies liefert dann eine einfache Beschreibung der Restklassengruppe, wie im folgenden Beispiel.

Beispiel 12.4. Wir betrachten die Einheitengruppe von $\mathbb{C}$, also $(\mathbb{C}^\times, 1, \cdot)$.

Zur Untergruppe $\mathbb{R}_+ \subseteq \mathbb{C}^\times$ ist die Abbildung

$$S^1 = \{z \in \mathbb{C} |\ |z| = 1\} \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}/\mathbb{R}_+$$

ein Isomorphismus, die Restklassengruppe ist also isomorph zur Kreisgruppe. Der Kern der Gesamtabbildung besteht aus dem Durchschnitt

$$S^1 \cap \mathbb{R}_+ = \{1\},$$

daher ist die Abbildung nach Lemma 10.13 injektiv. Zum Beweis der Surjektivität müssen wir zeigen, dass die Äquivalenzklasse zu jedem $x \in \mathbb{C}^\times$ durch ein Element des Einheitskreises repräsentiert werden kann. Hierzu kann man $\frac{x}{|x|}$ nehmen.

Zur Untergruppe $S^1 \subseteq \mathbb{C}^\times$ ist die Abbildung

$$\mathbb{R}_+ \longrightarrow \mathbb{C}^\times \longrightarrow \mathbb{C}/S^1$$

bijektiv, die Restklassengruppe ist also isomorph zur Gruppe der positiven reellen Zahlen. Die Injektivität ergibt sich wie eben. Die Surjektivität ergibt sich daraus, dass $x \in \mathbb{C}^\times$ zu $|x|$ (bezüglich der Untergruppe S^1) äquivalent ist.

Homomorphie- und Isomorphiesatz

Satz 12.5. *Seien G, Q und H Gruppen, es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $\psi\colon G \to Q$ ein surjektiver Gruppenhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$$

ist. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi} : Q \longrightarrow H$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} G & \longrightarrow & Q \\ & \searrow & \downarrow \\ & & H \end{array}$$

ist kommutativ.

Beweis. Wir zeigen zuerst die Eindeutigkeit. Für jedes Element $u \in Q$ gibt es mindestens ein $g \in G$ mit $\psi(g) = u$. Wegen der Kommutativität des Diagramms muss

$$\tilde{\varphi}(u) = \varphi(g)$$

gelten. Das bedeutet, dass es maximal ein $\tilde{\varphi}$ geben kann. Wir haben zu zeigen, dass durch diese Bedingung eine wohldefinierte Abbildung gegeben ist. Seien also $g, g' \in G$ zwei Urbilder von u. Dann ist

$$g'g^{-1} \in \operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$$

und daher ist $\varphi(g) = \varphi(g')$. Die Abbildung ist also wohldefiniert. Seien $u, v \in Q$ und seien $g, h \in G$ Urbilder davon. Dann ist gh ein Urbild von uv und daher ist

$$\tilde{\varphi}(uv) \;=\; \varphi(gh) \;=\; \varphi(g)\varphi(h) \;=\; \tilde{\varphi}(u)\tilde{\varphi}(v).$$

D.h. $\tilde{\varphi}$ ist ein Gruppenhomomorphismus. □

Die im vorstehenden Satz konstruierte Abbildung heißt *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus*.

Korollar 12.6. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Dann gibt es eine kanonische Isomorphie

$$\tilde{\varphi}\colon\ G/\operatorname{kern}\varphi \longrightarrow H.$$

Beweis. Wir wenden Satz 12.5 auf $Q = G/\operatorname{kern}\varphi$ und die kanonische Projektion $q\colon\ G \to G/\operatorname{kern}\varphi$ an. Dies induziert einen Gruppenhomomorphismus

$$\tilde{\varphi}\colon\ G/\operatorname{kern}\varphi \longrightarrow H$$

mit $\varphi = \tilde{\varphi} \circ q$, der surjektiv ist. Sei $[x] \in G/\operatorname{kern}\varphi$ und $[x] \in \operatorname{kern}\tilde{\varphi}$. Dann ist

$$\tilde{\varphi}([x]) \ = \ \varphi(x) \ = \ e_H,$$

also $x \in \operatorname{kern}\varphi$. Damit ist $[x] = e_Q$, d.h. der Kern von $\tilde{\varphi}$ ist trivial und nach Lemma 10.13 ist $\tilde{\varphi}$ auch injektiv. □

Satz 12.7. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$G \xrightarrow{\ q\ } G/\operatorname{kern}\varphi \xrightarrow{\ \theta\ } \operatorname{bild}\varphi \xhookrightarrow{\ \iota\ } H\,,$$

wobei q die kanonische Projektion, θ ein Gruppenisomorphismus und ι die kanonische Inklusion der Bildgruppe ist.

Beweis. Dies folgt aus Korollar 12.6 angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 12.8. *Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler mit der Restklassengruppe $Q = G/N$. Es sei $H \subseteq G$ eine weiterer Normalteiler in G, der N umfasst. Dann ist das Bild $\overline{H}$ von H in Q ein Normalteiler und es gilt die kanonische Isomorphie*

$$G/H \cong Q/\overline{H}\,.$$

Beweis. Für die erste Aussage siehe Aufgabe 11.6. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

$$p \circ q : G \longrightarrow Q \longrightarrow Q/\overline{H}\,.$$

Wegen

$$\begin{aligned}\operatorname{kern} p \circ q &= \{x \in G |\, p \circ q(x) = e\} \\ &= \{x \in G |\, q(x) \in \operatorname{kern} p\} \\ &= \left\{x \in G |\, q(x) \in \overline{H}\right\} \\ &= H\end{aligned}$$

ist $\operatorname{kern} p \circ q = H$. Daher ergibt Korollar 12.6 die kanonische Isomorphie

$$G/H \longrightarrow Q/\overline{H}.$$

□

Kurz gesagt ist also

$$G/H \;=\; (G/N)/(H/N).$$

12. Arbeitsblatt

Übungsaufgaben

Aufgabe 12.1. Bringe die Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ mit der in Aufgabe 1.17 direkt eingeführten Gruppe in Verbindung.

Aufgabe 12.2.*

Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich n ist.

Aufgabe 12.3. Zeige, dass es keine Untergruppe $F \subseteq (\mathbb{Q}, 0, +)$ derart gibt, dass

$$F \longrightarrow \mathbb{Q}/\mathbb{Z}$$

ein Isomorphismus ist.

Aufgabe 12.4. Bestimme die Restklassengruppe zu $\{1, -1\} \subset \mathbb{R}^\times$.

Aufgabe 12.5. Finde in der Permutationsgruppe S_3 einen Normalteiler $N \neq 0, S_3$ und bestimme die zugehörige Restklassengruppe.

Aufgabe 12.6. Sei G eine Gruppe und $g \in G$ ein Element mit dem (nach Lemma 10.7) zugehörigen Gruppenhomomorphismus

$$\varphi\colon\, \mathbb{Z} \longrightarrow G,\, n \longmapsto g^n.$$

Beschreibe die kanonische Faktorisierung von φ gemäß Satz 12.7.

Aufgabe 12.7.*

Es sei G eine Gruppe und $g \in G$ ein Element mit endlicher Ordnung. Zeige, dass die Ordnung von g mit dem minimalen $d \in \mathbb{N}_+$ übereinstimmt, zu dem es einen Gruppenhomomorphismus

$$\mathbb{Z}/(d) \longrightarrow G$$

gibt, in dessen Bild das Element g liegt.

Aufgabe 12.8. Zeige mit Hilfe der Homomorphiesätze, dass zyklische Gruppen mit der gleichen Ordnung isomorph sind.

Aufgabe 12.9. Seien G, H und F Gruppen und seien $\varphi\colon G \to H$ und $\psi\colon G \to F$ Gruppenhomomorphismen mit ψ surjektiv und mit $\operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$. Bestimme den Kern des induzierten Homomorphismus

$$\tilde{\varphi}\colon F \longrightarrow H.$$

Aufgabe 12.10. Zeige, dass für jede reelle Zahl $a \neq 0$ die Restklassengruppen $\mathbb{R}/\mathbb{Z}a$ untereinander isomorph sind.

Aufgabe 12.11. Sei p eine Primzahl. Definiere einen Gruppenhomomorphismus

$$(\mathbb{Q} \setminus \{0\}, \cdot, 1) \longrightarrow (\mathbb{Z}, +, 0),$$

der $p \mapsto 1$ und alle anderen Primzahlen auf null schickt.

Bestimme auch den Kern dieses Gruppenhomomorphismus.

Aufgabe 12.12. Es seien G_1 und G_2 Gruppen und seien $N_1 \subseteq G_1$ und $N_2 \subseteq G_2$ Normalteiler. Zeige, dass $N_1 \times N_2$ ein Normalteiler in $G_1 \times G_2$ ist und dass eine Isomorphie

$$(G_1 \times G_2/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$$

vorliegt.

Aufgabe 12.13. Sei H eine (additive) Untergruppe der reellen Zahlen $\mathbb{R}$. Zeige, dass entweder $H = \mathbb{Z}a$ mit einer eindeutig bestimmten nicht-negativen reellen Zahl a ist, oder aber H dicht in $\mathbb{R}$ ist.

Aufgaben zum Abgeben

Aufgabe 12.14. (3 Punkte)

Es seien G und H Gruppen mit der Produktgruppe $G \times H$. Zeige, dass die Gruppe $G \times \{e_H\}$ ein Normalteiler in $G \times H$ ist, und dass die Restklassengruppe $(G \times H)/G \times \{e_H\}$ kanonisch isomorph zu H ist.

Aufgabe 12.15. (4 Punkte)

Bestimme die Gruppenhomomorphismen zwischen zwei zyklischen Gruppen. Welche sind injektiv und welche sind surjektiv?

Aufgabe 12.16. (2 Punkte)

Zeige, dass es eine Gruppe G und einen Gruppenhomomorphismus

$$\varphi\colon\ (\mathbb{R}, 0, +) \longrightarrow G$$

mit der Eigenschaft gibt, dass $r \in \mathbb{R}$ genau dann rational ist, wenn $\varphi(r) = 0$ ist.

Aufgabe 12.17. (3 Punkte)

Bestimme sämtliche Gruppen mit vier Elementen.

13. Vorlesung - Ringhomomorphismen

Ringhomomorphismen

Definition 13.1. Seien R und S Ringe. Eine Abbildung

$$\varphi\colon\ R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$
(2) $\varphi(1) = 1$
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Ein Ringhomomorphismus ist also zugleich ein Gruppenhomomorphismus für die additive Struktur und ein Monoidhomomorphismus für die multiplikative Struktur. Einen bijektiven Ringhomomorphismus nennt man einen *Ringisomorphismus*, und zwei Ringe heißen *isomorph*, wenn es einen Ringisomorphismus zwischen ihnen gibt. Ein Ringisomorphismus eines Ringes auf sich selbst heißt *Ringautomorphismus*. Wenn R und S Körper sind, so spricht man manchmal auch von einem Körperhomomorphismus statt von einem Ringhomomorphismus. Dieser hat aber keine zusätzlichen Eigenschaften.

Die konstante Abbildung $R \to 0$ in den Nullring ist stets ein Ringhomomorphismus, dagegen ist die umgekehrte Abbildung, also $0 \to R$, nur bei $R = 0$ ein Ringhomomorphismus.

Lemma 13.2. *Es seien R, S, T Ringe. Dann gelten folgende Eigenschaften.*

(1) *Die Identität* $\mathrm{id} : R \to R$ *ist ein Ringhomomorphismus.*
(2) *Sind $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen, so ist auch die Hintereinanderschaltung $\psi \circ \varphi : R \to T$ ein Ringhomomorphismus.*
(3) *Ist $R \subseteq S$ ein Unterring, so ist die Inklusion $R \hookrightarrow S$ ein Ringhomomorphismus.*

Beweis. Siehe Aufgabe 13.4. □

Satz 13.3. *Sei R ein Ring. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\mathbb{Z} \longrightarrow R.$$

Beweis. Ein Ringhomomorphismus muss die 1 auf die 1_R abbilden. Deshalb gibt es nach Lemma 10.7 genau einen Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow (R, +, 0),\ n \longmapsto n1_R.$$

Wir müssen zeigen, dass diese Abbildung auch die Multiplikation respektiert, d.h. dass $(mn)1_R = (m1_R) * (n1_R)$ ist, wobei $*$ hier die Multiplikation in R bezeichnet. Dies folgt aber aus Lemma 2.5. □

Den in dieser Aussage konstruierten und eindeutig bestimmten Ringhomomorphismus nennt man auch den *kanonischen Ringhomomorphismus* (oder den *charakteristischen Ringhomomorphismus*) von $\mathbb{Z}$ nach R.

Definition 13.4. Die *Charakteristik* eines kommutativen Ringes R ist die kleinste positive natürliche Zahl n mit der Eigenschaft $n \cdot 1_R = 0$. Die Charakteristik ist 0, falls keine solche Zahl existiert.

Die Charakteristik beschreibt genau den Kern des obigen kanonischen (charakteristischen) Ringhomomorphismus.

Lemma 13.5. *Sei R ein Integritätsbereich. Dann ist die Charakteristik von R null oder eine Primzahl.*

Beweis. Die Charakteristik sei $n > 0$ und es sei angenommen, dass n keine Primzahl ist, also eine Zerlegung $n = ab$ mit kleineren Zahlen $0 < a, b < n$ besitzt. Nach Definition der Charakteristik ist $n_R = 0$ in R und n ist die kleinste positive Zahl mit dieser Eigenschaft. Aufgrund von Satz 13.3 ist $a_R b_R = n_R = 0$, so dass, weil R ein Integritätsbereich ist, einer der Faktoren null sein muss, im Widerspruch zur Minimalität von n. □

Lemma 13.6. *Seien R und S Ringe und sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus. Es sei $u \in R^\times$ eine Einheit. Dann ist auch $\varphi(u)$ eine Einheit. Mit anderen Worten: Ein Ringhomomorphismus induziert einen Gruppenhomomorphismus

$$R^\times \longrightarrow S^\times.$$

Beweis. Das ist trivial. □

Der Einsetzungshomomorphismus

Satz 13.7. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei A ein weiterer kommutativer Ring und es sei $\varphi\colon\ R \to A$ ein Ringhomomorphismus und $a \in A$ ein Element. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\psi\colon\ R[X] \longrightarrow A$$

mit $\psi(X) = a$ und mit $\psi \circ i = \varphi$, wobei $i\colon\ R \to R[X]$ die kanonische Einbettung ist. Dabei geht das Polynom $P = \sum_{j=0}^n c_j X^j$ auf $\sum_{j=0}^n \varphi(c_j)a^j$.

Beweis. Bei einem Ringhomomorphismus

$$\psi\colon\ R[X] \longrightarrow A$$

mit $\psi \circ i = \varphi$ müssen die Konstanten $c \in R$ auf $\varphi(c)$ und X auf a gehen. Daher muss X^j auf a^j gehen. Da Summen respektiert werden, kann es nur einen Ringhomorphismus geben, der die im Zusatz angegebene Gestalt haben muss. Es ist also zu zeigen, dass durch diese Vorschrift wirklich ein Ringhomomorphismus definiert ist. Dies folgt aber direkt aus dem Distributivgesetz. □

Den in diesem Satz konstruierten Ringhomomorphismus nennt man den *Einsetzungshomomorphismus*.

Korollar 13.8. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei $r \in R$ ein Element. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\psi\colon\ R[X] \longrightarrow R$$

mit $\psi(X) = r$ und mit $\psi \circ i = \varphi$, wobei $i\colon\ R \to R[X]$ die kanonische Einbettung ist. Dabei geht das Polynom $P = \sum_{j=0}^n c_j X^j$ auf $\sum_{j=0}^n \varphi(c_j)r^j$.

Beweis. Dies folgt unmittelbar aus Satz 13.7. □

Korollar 13.9. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei $Y = aX + b$, wobei a eine Einheit in R sei. Dann gibt es einen Ringisomorphismus*

$$R[X] \longrightarrow R[X],\ X \longmapsto aX + b.$$

Beweis. Die Einsetzungshomomorphismen zu $X \mapsto aX + b$ und $X \mapsto a^{-1}X - a^{-1}b$ definieren aufgrund von Satz 13.7 jeweils einen Ringhomomorphismus ψ und φ von $R[X]$ nach $R[X]$, die wir hintereinander schalten:

$$R[X] \xrightarrow{\psi} R[X] \xrightarrow{\varphi} R[X]\,.$$

Bei diesem Ringhomomorphismus bleiben die Elemente aus R unverändert, und die Variable X wird insgesamt auf

$$a(a^{-1}X - a^{-1}b) + b \;=\; aa^{-1}X - aa^{-1}b + b \;=\; X$$

geschickt. Daher muss die Verknüpfung aufgrund der Eindeutigkeit in Satz 13.7 die Identität sein. Dies gilt auch für die Hintereinanderschaltung in umgekehrter Reihenfolge, so dass ein Isomorphismus vorliegt. □

Ideale unter einem Ringhomomorphismus

Der Zusammenhang zwischen Ringhomomorphismen und Idealen wird durch folgenden Satz hergestellt.

Satz 13.10. *Seien R und S kommutative Ringe und sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Dann ist der Kern

$$\operatorname{kern}\varphi = \{f \in R |\, \varphi(f) = 0\}$$

ein Ideal in R.

Beweis. Sei $I := \varphi^{-1}(0)$. Wegen $\varphi(0) = 0$ ist $0 \in I$. Seien $a, b \in I$. Das bedeutet $\varphi(a) = 0$ und $\varphi(b) = 0$. Dann ist

$$\varphi(a + b) \;=\; \varphi(a) + \varphi(b) \;=\; 0 + 0 \;=\; 0$$

und daher $a + b \in I$.

Sei nun $a \in I$ und $r \in R$ beliebig. Dann ist

$$\varphi(ra) \;=\; \varphi(r)\varphi(a) \;=\; \varphi(r) \cdot 0 \;=\; 0,$$

also ist $ra \in I$. □

Da ein Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der zugrunde liegenden additiven Gruppe ist, gilt wieder das Kernkriterium für die Injektivität. Eine Anwendung davon ist das folgende Korollar.

Korollar 13.11. *Es sei K ein Körper und S ein vom Nullring verschiedener Ring. Es sei*

$$\varphi\colon K \longrightarrow S$$

ein Ringhomomorphismus. Dann ist φ injektiv.

Beweis. Es genügt nach Lemma 10.13 zu zeigen, dass der Kern der Abbildung gleich null ist. Nach Satz 13.10 ist der Kern ein Ideal. Da die 1 auf $1 \neq 0$ geht, ist der Kern nicht ganz K. Da es nach Lemma 7.5 in einem Körper überhaupt nur zwei Ideale gibt, muss der Kern das Nullideal sein. □

13. Arbeitsblatt

Übungsaufgaben

Aufgabe 13.1. Zeige, dass das Bild unter einem Ringhomomorphismus ein Unterring ist.

Aufgabe 13.2. Zeige, dass die Umkehrabbildung eines Ringisomorphismus wieder ein Ringhomomorphismus ist.

Aufgabe 13.3. Es seien R, S, T Ringe. Zeige die folgenden Eigenschaften.

(1) Die Identität $\mathrm{id} : R \to R$ ist ein Ringhomomorphismus.
(2) Sind $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen, so ist auch die Hintereinanderschaltung $\psi \circ \varphi : R \to T$ ein Ringhomomorphismus.
(3) Ist $R \subseteq S$ ein Unterring, so ist die Inklusion $R \hookrightarrow S$ ein Ringhomomorphismus.

Aufgabe 13.4. Sei R ein kommutativer Ring und sei $\varphi\colon \mathbb{Z} \to R$ der kanonische Homomorphismus. Zeige, dass die Charakteristik von R der eindeutig bestimmte nichtnegative Erzeuger des Kernideals $\ker \varphi \subseteq \mathbb{Z}$ ist.

Aufgabe 13.5. Es sei R ein Integritätsbereich der Charakteristik $n \in \mathbb{N}$. Zeige, dass die Ordnung von jedem Element $x \in R$, $x \neq 0$, ebenfalls n ist.

Aufgabe 13.6. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Berechne das Bild des Polynoms X^3+4X-3 unter dem durch $X \mapsto X^2+X-1$ definierten Einsetzungshomomorphismus $K[X] \to K[X]$.

Aufgabe 13.7. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $a \in K$ ein fixiertes Element. Bestimme den Kern des Einsetzungshomomorphismus

$$K[X] \longrightarrow K,\, X \longmapsto a.$$

Aufgabe 13.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P \in K[X]$ ein nicht-konstantes Polynom. Zeige, dass der durch $X \mapsto P$ definierte Einsetzungshomomorphismus von $K[X]$ nach $K[X]$ injektiv ist und dass der durch P erzeugte Unterring $K[P] \subseteq K[X]$ isomorph zum Polynomring in einer Variablen ist.

Aufgabe 13.9. Es sei R ein kommutativer Ring und 0 der Nullring. Bestimme die Ringhomomorphismen von R nach 0 und die Ringhomomorphismen von 0 nach R.

Aufgabe 13.10. Zeige, dass die komplexe Konjugation ein Körperautomorphismus ist.

Aufgabe 13.11. Zeige, dass es keinen Ringhomomorphismus von $\mathbb{Q}$ nach $\mathbb{Z}$ gibt.

Aufgabe 13.12.*

Zeige, dass es keinen Ringhomomorphismus von $\mathbb{C}$ nach $\mathbb{R}$ gibt.

Aufgabe 13.13. Bestimme die Körperautomorphismen von $\mathbb{R}$.

Aufgabe 13.14. Sei R ein Ring und seien L und M zwei Mengen mit den in Aufgabe 2.9 konstruierten Ringen $A = \mathrm{Abb}\,(L, R)$ und $B = \mathrm{Abb}\,(M, R)$. Zeige, dass eine Abbildung $L \to M$ einen Ringhomomorphismus

$$B \longrightarrow A$$

induziert.

Aufgabe 13.15.*

Es sei K ein Körper, R ein Ring mit $0 \neq 1$ und

$$\varphi\colon\, K \longrightarrow R$$

ein Ringhomomorphismus. Zeige direkt, dass φ injektiv ist.

Aufgabe 13.16. Es sei K ein Körper und sei

$$\varphi\colon\ K \longrightarrow K$$

ein Körperautomorphismus. Zeige, dass die Abbildung

$$K[X] \longrightarrow K[X],\ \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \varphi(a_i) X^i,$$

ein Ringautomorphismus des Polynomrings $K[X]$ ist.

Aufgaben zum Abgeben

Aufgabe 13.17. (2 Punkte)

Es sei R ein kommutativer Ring der Charakteristik $n \in \mathbb{N}$. Zeige, dass die Ordnung von jedem Element $x \in R$, $x \neq 0$, ein Teiler von n ist.

Aufgabe 13.18. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Berechne das Bild des Polynoms $X^4 - 2X^2 + 5X - 2$ unter dem durch $X \mapsto 2X^3 + X - 1$ definierten Einsetzungshomomorphismus $K[X] \to K[X]$.

Aufgabe 13.19. (2 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass ein Polynom $P \in K[X]$ genau dann irreduzibel ist, wenn das um $a \in K$ „verschobene“ Polynom (das entsteht, wenn man in P die Variable X durch $X-a$ ersetzt) irreduzibel ist.

Aufgabe 13.20. (3 Punkte)

Zeige, dass es keinen Ringhomomorphismus von $\mathbb{R}$ nach $\mathbb{Q}$ gibt.

Aufgabe 13.21. (3 Punkte)

Sei p eine Primzahl. Zeige, dass

$$\binom{p}{k} \equiv 0 \mod p$$

ist für alle $k = 1, \ldots, p-1$.

Aufgabe 13.22. (3 Punkte)

Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobenius-Homomorphismus* nennt.

14. Vorlesung - Restklassenringe

Restklassenringe

Nach Satz 13.10 ist der Kern eines Ringhomomorphismus ein Ideal. Man kann umgekehrt zu jedem Ideal $I \subseteq R$ in einem (kommutativen) Ring einen Ring R/I konstruieren, und zwar zusammen mit einem surjektiven Ringhomomorphismus

$$R \longrightarrow R/I,$$

dessen Kern gerade das vorgegebene Ideal I ist. Ideale und Kerne von Ringhomomorphismen sind also im Wesentlichen äquivalente Objekte, so wie das bei Gruppen für Kerne von Gruppenhomomorphismen und Normalteilern gilt. In der Tat gelten die entsprechenden Homomorphiesätze hier wieder, und können weitgehend auf die Gruppensituation zurückgeführt werden. Wir werden uns bei den Beweisen also kurz fassen können.

Definition 14.1. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zu $a \in R$ heißt die Teilmenge

$$a + I = \{a + f | \, f \in I\}$$

die *Nebenklasse von* a zum Ideal I. Jede Teilmenge von dieser Form heißt *Nebenklasse* zu I.

Diese Nebenklassen sind gerade die Nebenklassen zur Untergruppe $I \subseteq R$, die wegen der Kommutativität ein Normalteiler ist. Zwei Elemente $a, b \in R$ definieren genau dann die gleiche Nebenklasse, also $a + I = b + I$, wenn ihre Differenz $a - b$ zum Ideal gehört. Man sagt dann auch, dass a und b dieselbe Nebenklasse *repräsentieren*.

Definition 14.2. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Dann ist der *Restklassenring* R/I (sprich „R modulo I“) ein kommutativer Ring, der durch folgende Daten festgelegt ist.

(1) Als Menge ist R/I die Menge der Nebenklassen zu I.
(2) Durch
$$(a + I) + (b + I) := (a + b + I)$$
wird eine Addition von Nebenklassen definiert.

(3) Durch
$$(a+I)\cdot(b+I) := (a\cdot b+I)$$
wird eine Multiplikation von Nebenklassen definiert.
(4) $\bar{0} = 0+I = I$ definiert das neutrale Element für die Addition (die Nullklasse).
(5) $\bar{1} = 1+I$ definiert das neutrale Element für die Multiplikation (die Einsklasse).

Man muss dabei zeigen, dass diese Abbildungen (also Addition und Multiplikation) wohldefiniert sind, d.h. unabhängig vom Repräsentanten, und dass die Ringaxiome erfüllt sind. Da I insbesondere eine Untergruppe der kommutativen Gruppe $(R,+,0)$ ist, liegt ein Normalteiler vor, so dass R/I eine Gruppe ist und die Restklassenabbildung

$$R \longrightarrow R/I,\ a \longmapsto a+I =: \bar{a},$$

ein Gruppenhomomorphismus ist. Das einzig Neue gegenüber der Gruppensituation ist also die Anwesenheit einer Multiplikation. Die Wohldefiniertheit der Multiplikation ergibt sich so: Seien zwei Restklassen gegeben mit unterschiedlichen Repräsentanten, also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Dann ist $a-a' \in I$ und $b-b' \in I$ bzw. $a' = a+x$ und $b' = b+y$ mit $x,y \in I$. Daraus ergibt sich

$$a'b' = (a+x)(b+y) = ab+ay+xb+xy.$$

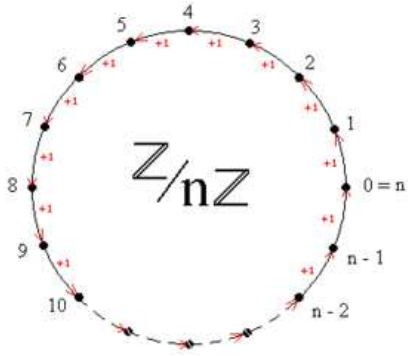
Die drei hinteren Summanden gehören zum Ideal, so dass die Differenz $a'b'-ab \in I$ ist.

Aus der Wohldefiniertheit folgen die anderen Eigenschaften und insbesondere, dass ein Ringhomomorphismus in den Restklassenring vorliegt. Diesen nennt man wieder die *Restklassenabbildung* oder den *Restklassenhomomorphismus*. Das Bild von $a \in R$ in R/I wird häufig mit $[a]$, $\bar{a}$ oder einfach mit a selbst bezeichnet und heißt die *Restklasse* von a. Bei dieser Abbildung gehen genau die Elemente aus dem Ideal auf 0, d.h. der Kern dieser Restklassenabbildung ist das vorgegebene Ideal.

Das einfachste Beispiel für diesen Prozess ist die Abbildung, die einer ganzen Zahl a den Rest bei Division durch eine fixierte Zahl d zuordnet. Jeder Rest wird dann repräsentiert durch eine der Zahlen $0,1,2,\ldots,d-1$. Im Allgemeinen gibt es nicht immer ein solch übersichtliches Repräsentantensystem.

Die Restklassenringe von $\mathbb{Z}$

Die Restklassengruppen $\mathbb{Z}/(d)$ haben wir bereits kennengelernt, es handelt sich um zyklische Gruppen der Ordnung d. Diese Gruppen bekommen jetzt aber noch zusätzlich eine Ringstruktur.



Korollar 14.3. *Sei $d \geq 0$ eine natürliche Zahl. Dann gibt es eine eindeutig bestimmte Ringstruktur auf $\mathbb{Z}/(d)$ derart, dass die Restklassenabbildung*

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(d),\, a \longmapsto \overline{a}\,,$$

ein Ringhomomorphismus ist. $\mathbb{Z}/(d)$ ist ein kommutativer Ring mit d Elementen (bei $d \geq 1$).

Beweis. Dies ist ein Spezialfall der obigen Überlegungen. □

Die Restklassenringe $S = K[X]/(P)$ sind ebenfalls gut überschaubar. Wenn P den Grad d besitzt, so wird jede Restklasse in S durch ein eindeutiges Polynom von einem Grad $< d$ repräsentiert. Dieses ist der Rest, den man erhält, wenn man durch P durchdividiert.

Die Homomorphiesätze für Ringe

Für Ringe, ihre Ideale und Ringhomomorphismen gelten die analogen Homomorphiesätze wie für Gruppen, ihre Normalteiler und Gruppenhomomorphismen, siehe die zwölfte Vorlesung. Wir beschränken uns auf kommutative Ringe.

Satz 14.4. *Seien R, S und T kommutative Ringe, es sei $\varphi\colon R \to S$ ein Ringhomomorphismus und $\psi\colon R \to T$ ein surjektiver Ringhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$$

ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon T \longrightarrow S$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} R & \longrightarrow & T \\ & \searrow & \downarrow \\ & & S \end{array}$$

ist kommutativ.

Beweis. Aufgrund von Satz 12.5 gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon\ T \longrightarrow S,$$

der die Eigenschaften erfüllt. Es ist also lediglich noch zu zeigen, dass $\tilde{\varphi}$ auch die Multiplikation respektiert. Seien dazu $t, t' \in T$, und diese seien repräsentiert durch r bzw. r' aus R. Dann wird tt' durch rr' repräsentiert und daher ist

$$\tilde{\varphi}(tt') = \varphi(rr') = \varphi(r)\varphi(r') = \tilde{\varphi}(t)\tilde{\varphi}(t').$$

□

Die im vorstehenden Satz konstruierte Abbildung heißt wieder *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus.*

Korollar 14.5. *Es seien R und S kommutative Ringe und es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein surjektiver Ringhomomorphismus. Dann gibt es eine kanonische Isomorphie von Ringen

$$\tilde{\varphi}\colon\ R/\operatorname{kern}\varphi \longrightarrow S.$$

Beweis. Aufgrund von Korollar 12.6 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 14.4 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

Satz 14.6. *Es seien R und S kommutative Ringe und es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$R \xrightarrow{q} R/\operatorname{kern}\varphi \xrightarrow{\theta} \operatorname{bild}\varphi \overset{\iota}{\hookrightarrow} S\,,$$

wobei q die kanonische Projektion, θ ein Ringisomorphismus und ι die kanonische Inklusion des Bildes ist.

Beweis. Dies beruht auf Satz 12.7 und Satz 14.4. □

Es gilt also wieder:

Bild = Urbild modulo Kern.

Satz 14.7. *Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R mit dem Restklassenring $S = R/I$. Es sei J ein weiteres Ideal in R, das I umfasst. Dann ist das Bild $\overline{J}$ von J in S ein Ideal und es gilt die kanonische Isomorphie*

$$R/J \cong S/\overline{J}\,.$$

Beweis. Auch dies ergibt sich aus der Gruppensituation und Satz 14.4. □

Anwendung auf $\mathbb{Z}/(d)$

Die Charakteristik von $\mathbb{Z}/(d)$ ist d. Dies zeigt insbesondere, dass es zu jeder Zahl n Ringe gibt mit dieser Charakteristik. Zu einem beliebigen Ring R der Charakteristik d faktorisiert der charakteristische Ringhomomorphismus $\mathbb{Z} \to R$ nach Satz 14.6 durch Ringhomomorphismen

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(d) \longrightarrow R\,,$$

wobei die hintere Abbildung injektiv ist. Der Ring $\mathbb{Z}/(d)$, $d = \operatorname{char}(R)$, ist der kleinste Unterring von R, und wird der *Primring* von R genannt.

Korollar 14.8. *Seien n und k positive natürliche Zahlen, und k teile n. Dann gibt es einen kanonischen Ringhomomorphismus*

$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k),\ (a \mod n) \longmapsto (a \mod k).$$

Beweis. Wir betrachten die Ringhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \stackrel{\varphi}{\longrightarrow} & \mathbb{Z}/(k) \\ \phi\downarrow & & \\ \mathbb{Z}/(n) & & \end{array}$$

Aufgrund der Teilerbeziehung haben wir die Beziehung

$$\ker\phi \;=\; (n) \;\subseteq\; (k) \;=\; \ker\varphi.$$

Aufgrund des Homomorphiesatzes hat man daher einen kanonischen Ringhomomorphismus von links unten nach rechts oben. □

Einheiten im Restklassenring

Lemma 14.9. *Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Dann ist ein Element $a \in R$ genau dann eine Einheit modulo I, wenn a und I zusammen das Einheitsideal in R erzeugen.*

Beweis. Es sei $\overline{a}$ eine Einheit im Restklassenring R/I. Dies ist genau dann der Fall, wenn es ein $r \in R$ gibt mit

$$\overline{a}\,\overline{r} \;= \overline{1}\;.$$

Dies bedeutet zurückübersetzt nach R, dass

$$ar - 1 \in I$$

ist, was wiederum äquivalent dazu ist, dass I und (a) zusammen das Einheitsideal erzeugen. □

14. Arbeitsblatt

Übungsaufgaben

Aufgabe 14.1. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $a \in K$ ein fixiertes Element. Zeige, dass der Restklassenring $K[X]/(X-a)$ zu K isomorph ist.

Aufgabe 14.2. Es sei K ein Körper und $P \in K[X]$ ein Polynom vom Grad d. Zeige, dass jedes Element im Restklassenring $R = K[X]/(P)$ durch ein Polynom vom Grad $< d$ repräsentiert werden kann.

Aufgabe 14.3. Berechne in $\mathbb{Q}[X]/(X^5)$ das Produkt

$$\left(7X^4 - \frac{2}{3}X^3 + 2X + \frac{1}{5}\right)\left(-\frac{4}{7}X^3 + 4X^2 - 3\right).$$

Aufgabe 14.4.*

Berechne in

$$\mathbb{Z}/(7)[X]/(X^3 + 4X^2 + X + 5)$$

das Produkt

$$(2x^2 + 5x + 3) \cdot (3x^2 + x + 6)$$

(x bezeichne die Restklasse von X).

Aufgabe 14.5. Zeige, dass der Restklassenring $\mathbb{R}[X]/(X^2+1)$ isomorph zu $\mathbb{C}$ ist.

Aufgabe 14.6. Vereinfache den Restklassenring $\mathbb{Z}[X]/(3, 11X^2 - 4)$.

Aufgabe 14.7. Berechne im Restklassenring $\mathbb{Z}[X]/(6X)$ das Produkt

$$(4X^3 - 2X + 3)(3X^3 - 3X^2 + 4).$$

Aufgabe 14.8. Lucy Sonnenschein kennt von einer natürlichen Zahl n nur den Rest bei Division durch 12. Welche der Reste von n bei Division durch die folgenden Zahlen e kann sie daraus erschließen?

(1) $e = 1$,
(2) $e = 2$,
(3) $e = 3$,

(4) $e = 4$,
(5) $e = 5$,
(6) $e = 6$,
(7) $e = 7$,
(8) $e = 8$,
(9) $e = 0$.

Aufgabe 14.9. Man konstruiere zu jedem $n \in \mathbb{N}_+$ einen kommutativen Ring R der Charakteristik 0 derart, dass es in R ein Element der Ordnung (bezüglich der additiven Struktur) n gibt.

Aufgabe 14.10. Man konstruiere einen kommutativen Ring R, in dem die 4 mindestens drei Quadratwurzeln besitzt.

Aufgabe 14.11.*

Man gebe zu jedem $n \geq 2$ einen kommutativen Ring R und ein Element $x \in R$, $x \neq 0$, an, für das $nx = 0$ und $x^n = 0$ gilt.

Aufgabe 14.12. Bestimme den Kern und das Bild des Einsetzungshomomorphismus

$$\varphi\colon \mathbb{Q}[X] \longrightarrow \mathbb{R},\ X \longmapsto \sqrt{5}.$$

Aufgabe 14.13. Sei R ein Integritätsbereich und sei $f \in R$, $f \neq 0$, ein Element. Zeige, dass f genau dann ein Primelement ist, wenn der Restklassenring $R/(f)$ ein Integritätsbereich ist.

Aufgabe 14.14. Zeige, dass jeder Restklassenring eines Hauptidealringes wieder ein Hauptidealring ist. Man gebe ein Beispiel, dass ein Restklassenring eines Hauptidealbereiches kein Hauptidealbereich sein muss.

Aufgabe 14.15. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal. Zeige, dass $\mathfrak{p}$ genau dann ein Primideal ist, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.

Aufgabe 14.16. Seien R und S kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus. Sei $\mathfrak{p}$ ein Primideal in S. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{p})$ ein Primideal in R ist.

Zeige durch ein Beispiel, dass das Urbild eines maximalen Ideales kein maximales Ideal sein muss.

Aufgabe 14.17. Seien R und S kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus. Sei $\mathfrak{a}$ ein Radikal in S. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{a})$ ein Radikal in R ist.

Aufgabe 14.18.

(1) Zu einem Körper K sei $R = \mathrm{Folg}(K)$ die Menge der *Folgen* mit Werten in K. Zeige, dass R ein kommutativer Ring ist. Besitzt ein solcher Ring nicht-triviale idempotente Elemente?
(2) Sei von nun an $K = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$, so dass man eine Metrik zur Verfügung hat. Zeige, dass die Menge der *konvergenten Folgen* $\mathrm{Folg}_{\mathrm{konv}}(K)$ einen Unterring von R bildet.
(3) Zeige im Fall $K = \mathbb{Q}$, dass die Menge $\mathrm{Folg}_{\mathrm{Cauchy}}(\mathbb{Q})$ der Cauchy-Folgen ebenfalls ein Unterring ist.
(4) Betrachte nun die Menge N der *Nullfolgen* und begründe, dass diese ein Ideal in den verschiedenen Ringen ist. Zeige, dass N die Eigenschaft besitzt, dass wenn $x \cdot y \in N$ ist, dass dann einer der Faktoren dazu gehören muss.
(5) Definiere einen natürlichen Ringhomomorphismus

$$\mathrm{Folg}_{\mathrm{Cauchy}}(\mathbb{Q}) \longrightarrow \mathbb{R}$$

derart, dass eine Ringisomorphie

$$\mathrm{Folg}_{\mathrm{Cauchy}}(\mathbb{Q})/N \longrightarrow \mathbb{R}$$

entsteht.

Aufgaben zum Abgeben

Aufgabe 14.19. (3 Punkte)

Es seien a und n natürliche Zahlen mit $n \geq 2$. Es sei

$$a = \sum_{i=0}^{\ell} a_i n^i$$

die Darstellung von a zur Basis n (also mit $0 \leq a_i < n$). Es sei k ein Teiler von $n-1$. Dann wird a von k genau dann geteilt, wenn die *Quersumme* $\sum_{i=0}^{\ell} a_i$ von k geteilt wird.

Aufgabe 14.20. (3 Punkte)

Sei a eine positive reelle Zahl. Zeige, dass der Restklassenring $\mathbb{R}[X]/(X^2+a)$ isomorph zu $\mathbb{C}$ ist.

Aufgabe 14.21. (3 Punkte)

Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zeige, dass I genau dann ein maximales Ideal ist, wenn der Restklassenring R/I ein Körper ist.

Aufgabe 14.22. (4 Punkte)

Zeige, dass der Restklassenring

$$\mathbb{Z}/(2)[X]/(X^2+X+1)$$

ein Körper mit vier Elementen ist.

Die nächste Aufgabe verwendet folgende Definition.

Ein kommutativer Ring R heißt *reduziert*, wenn 0 das einzige nilpotente Element von R ist.

Aufgabe 14.23. (3 Punkte)

Zeige, dass ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R genau dann ein Radikal ist, wenn der Restklassenring $R/\mathfrak{a}$ reduziert ist.

15. Vorlesung - Chinesischer Restsatz

In dieser Vorlesung wollen wir die Restklassenringe von Hauptidealbereichen verstehen.

Restklassenringe von Hauptidealbereichen

Satz 15.1. *Sei R ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *p ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von 0 verschieden. Wir bezeichnen einen Repräsentanten davon in R ebenfalls mit a. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a,p)$. Ferner können wir $(a,p) = (b)$ schreiben , da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da c keine Einheit ist und p prim (also irreduzibel) ist, muss b eine Einheit sein. Es ist also $(a,p) = (1)$, und das bedeutet modulo p, also in $R/(p)$, dass a eine Einheit ist. Also ist $R/(p)$ ein Körper. $\square$

Satz 15.2. *Es sei $n \geq 1$ eine natürliche Zahl und $\mathbb{Z}/(n)$ der zugehörige Restklassenring. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathbb{Z}/(n)$ ist ein Körper.*
(2) *$\mathbb{Z}/(n)$ ist ein Integritätsbereich.*
(3) *n ist eine Primzahl.*

Beweis. Dies ist ein Spezialfall von Satz 15.1. □

Wenn also p eine Primzahl ist, so ist der Restklassenring $\mathbb{Z}/(p)$ ein Körper mit p Elementen, den man auch den *Restklassenkörper* nennt. Die Einheitengruppe

$$\mathbb{Z}/(p)^\times = \{1, \ldots, p-1\}$$

ist eine Gruppe mit $p-1$ Elementen (bezüglich der Multiplikation). Bei $p = 5$ hat man beispielsweise

$$\overline{2}^{\,0} = \overline{1}\,,\ \overline{2}^{\,1} = \overline{2}\,,\ \overline{2}^{\,2} = \overline{4} = \overline{-1}\,,\ \overline{2}^{\,3} = \overline{8} = \overline{3}\ ,$$

d.h. die Potenzen von $\overline{2}$ durchlaufen sämtliche vier Elemente dieser Gruppe, die sich damit als zyklisch erweist. Es gilt generell, ws wir aber nicht beweisen werden, dass für jede Primzahl p die Einheitengruppe des Restklassenkörpers $\mathbb{Z}/(p)$ zyklisch ist! Diese Gruppen nennt man auch die *primen Restklassengruppen*.

Pierre de Fermat (1607/08-1665)

Die folgende Aussage heißt *kleiner Fermat*.

Satz 15.3. *Für eine Primzahl p und eine beliebige ganze Zahl a gilt*

$$a^p \equiv a \mod p\,.$$

Anders ausgedrückt: $a^p - a$ ist durch p teilbar.

Beweis. Ist a nicht durch p teilbar, so definiert a ein Element $\bar{a}$ in der Einheitengruppe $(\mathbb{Z}/p)^\times$; diese Gruppe hat die Ordnung $p-1$, und nach dem Satz von Lagrange gilt $\bar{a}^{p-1} = 1$. Durch Multiplikation mit a ergibt sich die Behauptung. Für Vielfache von p gilt die Aussage ebenso, da dann beidseitig null steht. □

Für $p = 5$ gilt beispielsweise in $\mathbb{Z}/(5)$

$$1^p = 1,\ 2^5 = 32 = 2,\ 3^5 = 243 = 3,\ 4^5 = 1024 = 4\,,$$

Für Zahlen, die keine Primzahlen sind, gilt die entsprechende Aussage nicht. So ist etwa in $\mathbb{Z}/(5)$

$$3^4 \;=\; 81 \;=\; 1 \;\neq\; 3.$$

Produktringe

Um die Restklassenringe von $\mathbb{Z}$ besser verstehen zu können, insbesondere dann, wenn man n als Produkt von kleineren Zahlen schreiben kann - z.B., wenn die Primfaktorzerlegung bekannt ist - braucht man den Begriff des Produktringes.

Definition 15.4. Seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n\,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

Eng verwandt mit dem Begriff des Produktringes ist das Konzept der idempotenten Elemente.

Definition 15.5. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Die Elemente 0 und 1 sind trivialerweise idempotent, man nennt sie die trivialen idempotenten Elemente. In einem Produktring sind auch diejenigen Elemente, die in allen Komponenten nur den Wert 0 oder 1 besitzen, idempotent, also beispielsweise $(1, 0)$. In einem Integritätsbereich gibt es nur die beiden trivialen idempotenten Elemente: Ein idempotentes Element e besitzt die Eigenschaft

$$e(1-e) \;=\; e - e^2 \;=\; e - e \;=\; 0.$$

Im nullteilerfreien Fall folgt daraus $e = 1$ oder $e = 0$.

Lemma 15.6. *Es sei $R = R_1 \times \cdots \times R_n$ ein Produkt aus kommutativen Ringen. Dann gilt für die Einheitengruppe von R die Beziehung*

$$R^\times = R_1^\times \times \cdots \times R_n^\times$$

Beweis. Dies ist klar, da ein Element genau dann eine Einheit ist, wenn es in jeder Komponente eine Einheit ist. □

Der chinesische Restsatz

Für die Restklassenringe von Hauptidealbereichen gilt der sogenannte *chinesische Restsatz* (für beliebige faktorielle Bereiche gilt er nicht, da das Lemma von Bezout dafür im Allgemeinen nicht gilt).

Satz 15.7. *Es sei R ein Hauptidealbereich und $f \in R$, $f \neq 0$, ein Element mit kanonischer Primfaktorzerlegung*

$$f = p_1^{r_1} \cdots p_k^{r_k} .$$

Dann gilt für den Restklassenring $R/(f)$ die kanonische Isomorphie

$$R/(f) \cong R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k})$$

Beweis. Wegen $p_i^{r_i} | f$ gelten die Idealinklusionen $(f) \subseteq (p_i^{r_i})$ und daher gibt es kanonische Ringhomomorphismen

$$R/(f) \longrightarrow R/(p_i^{r_i}).$$

Diese setzen sich zu einem Ringhomomorphismus in den Produktring zusammen, nämlich

$$R/(f) \longrightarrow R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k}),\ a \longmapsto (a \mod p_1^{r_1}, \ldots, a \mod p_k^{r_k}).$$

Wir müssen zeigen, dass dieser bijektiv ist. Zur Injektivität sei $a \in R$ derart, dass es in jeder Komponente auf 0 abgebildet wird. Das bedeutet $a \in (p_i^{r_i})$ für alle i. D.h. a ist ein Vielfaches dieser $p_i^{r_i}$ und aufgrund der Primfaktorzerlegung folgt, dass a ein Vielfaches von f sein muss. Also ist $\overline{a} = 0$ in $R/(f)$. Zur Surjektivität genügt es zu zeigen, dass alle Elemente, die in einer Komponente den Wert 1 und in allen anderen Komponenten den Wert 0 haben, im Bild liegen. Sei also $(1, 0, \ldots, 0)$ vorgegeben. Wegen der Eindeutigkeit der Primfaktorzerlegung sind $p_1^{r_1}$ und $p_2^{r_2} \cdots p_k^{r_k}$ teilerfremd. Daher gibt es nach dem Lemma von Bezout eine Darstellung der Eins, sagen wir

$$s p_1^{r_1} + t p_2^{r_2} + \cdots + p_k^{r_k} = 1.$$

Betrachten wir $t p_2^{r_2} \cdots p_k^{r_k} = 1 - s p_1^{r_1} \in R$. Das wird unter der Restklassenabbildung in der ersten Komponente auf 1 und in den übrigen Komponenten auf 0 abgebildet, wie gewünscht. □

15. Arbeitsblatt

Übungsaufgaben

Aufgabe 15.1. Bestätige den kleinen Fermat direkt für die Primzahlen $p = 2, 3, 5, 7, 11$.

Aufgabe 15.2. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

Aufgabe 15.3.*

Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 15.4. Finde einen Restklassenring $\mathbb{Z}/(n)$ derart, dass die Einheitengruppe davon nicht zyklisch ist.

Aufgabe 15.5. Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32$ und 49 Elementen.

Aufgabe 15.6.*

Sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ derart gibt, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) \, = \, g(a)$$

gilt.

Aufgabe 15.7. Sei $f(x) = x^7+2x^3+3x+4 \in (\mathbb{Z}/(5))[x]$. Finde ein Polynom $g(x) \in (\mathbb{Z}/(5))[x]$ vom Grad < 5, das für alle Elemente aus $\mathbb{Z}/(5)$ mit $f(x)$ übereinstimmt.

Aufgabe 15.8.*

a) Zeige, dass durch

$$K = \mathbb{Z}/(7)[T]/(T^3 - 2)$$

ein Körper mit 343 Elementen gegeben ist.

b) Berechne in K das Produkt $(T^2 + 2T + 4)(2T^2 + 5)$.

c) Berechne das (multiplikativ) Inverse zu $T + 1$.

Aufgabe 15.9. Zeige, dass $\mathbb{Q}[X]/(X^3 - 2)$ ein Körper ist und bestimme das Inverse von $4x^2 - 2x + 5$, wobei x die Restklasse von X bezeichne.

Aufgabe 15.10. Man gebe einen Restklassenring $\mathbb{Z}/(d)$ an, in dem es nichttriviale idempotente Elemente gibt.

Aufgabe 15.11. Finde in $\mathbb{Q}[X](X^2-1)$ nichttriviale idempotente Elemente.

Aufgabe 15.12. Sei R ein kommutativer Ring und sei $f \in R$. Es sei f sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

Aufgabe 15.13. Seien R und S kommutative Ringe und sei $R \times S$ der Produktring $R \times S$. Zeige, dass die Teilmenge $R \times 0$ ein Hauptideal ist.

Aufgabe 15.14. Sei R ein faktorieller Bereich und $p \in R$ ein Primelement. Zeige, dass der Restklassenring $R/(p^n)$ nur die beiden trivialen idempotenten Elemente 0 und 1 besitzt.

Aufgabe 15.15. Seien R ein kommutativer Ring und I, J Ideale in R. Sei weiter

$$\varphi\colon\ R \longrightarrow R/I \times R/J,\ r \longmapsto (r+I, r+J).$$

Zeige, dass φ genau dann surjektiv ist, wenn $I + J = R$ gilt. Wie sieht $\ker \varphi$ aus? Benutze jetzt den Homomorphiesatz um einzusehen, was das im Falle $R = \mathbb{Z}$ mit dem chinesischen Restsatz zu tun hat.

Aufgabe 15.16. Sei R ein kommutativer Ring und seien $I, J \subseteq R$ Ideale. Wir betrachten die Gruppenhomomorphismen

$$\varphi\colon\ R/I \cap J \longrightarrow R/I \times R/J,\ r \longmapsto (r, r),$$

und

$$\psi\colon\ R/I \times R/J \longrightarrow R/I + J,\ (s,t) \longmapsto s - t.$$

Zeige, dass φ injektiv ist, dass ψ surjektiv ist und dass

$$\operatorname{bild} \varphi \ = \ \operatorname{kern} \psi$$

ist. Sind φ und ψ Ringhomomorphismen?

Aufgabe 15.17. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $a_1, \ldots, a_n \in K$ verschiedene Elemente und

$$F \ = \ (X - a_1) \cdots (X - a_n)$$

das Produkt der zugehörigen linearen Polynome. Zeige, dass der Restklassenring $K[X]/(F)$ isomorph zum Produktring K^n ist.

Aufgabe 15.18.*

Das Polynom $X^3 - 7X^2 + 3X - 21$ besitzt in $\mathbb{R}[X]$ die Zerlegung

$$X^3 - 7X^2 + 3X - 21 = (X - 7)(X^2 + 3)$$

in irreduzible Faktoren und daher gilt die Isomorphie

$$\mathbb{R}[X]/(X^3 - 7X^2 + 3X - 21) \cong \mathbb{R}[X]/(X - 7) \times \mathbb{R}[X]/(X^2 + 3).$$

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(1, 0)$ entspricht.

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(0, 1)$ entspricht.

Aufgabe 15.19.*

Schreibe den Restklassenring $\mathbb{Q}[X]/(X^4 - 1)$ als ein Produkt von Körpern, wobei lediglich die Körper $\mathbb{Q}$ und $\mathbb{Q}[i]$ vorkommen. Schreibe die Restklasse von $X^3 + X$ als ein Tupel in dieser Produktzerlegung.

Aufgabe 15.20. Zeige, dass jeder echte Restklassenring von $\mathbb{C}[X]$ isomorph zu einem Produktring der Form

$$\begin{aligned}\mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{C}[X]/(X^2) \times \cdots \times \mathbb{C}[X]/(X^2) \times \mathbb{C}[X]/(X^3) \times \cdots \\ \times \mathbb{C}[X]/(X^3) \times \cdots \times \mathbb{C}[X]/(X^m) \times \cdots \times \mathbb{C}[X]/(X^m)\end{aligned}$$

ist.

Aufgabe 15.21. Realisiere den Produktring

$$\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$$

als Restklassenring von $\mathbb{R}[X]$.

Aufgabe 15.22.*

Es seien $R_1, R_2, \ldots, R_n$ kommutative Ringe und sei

$$R = R_1 \times R_2 \times \cdots \times R_n$$

der Produktring.

(1) Es seien

$$I_1 \subseteq R_1, I_2 \subseteq R_2, \ldots, I_n \subseteq R_n$$

Ideale. Zeige, dass die Produktmenge

$$I_1 \times I_2 \times \cdots \times I_n$$

ein Ideal in R ist.

(2) Zeige, dass jedes Ideal $I \subseteq R$ die Form
$$I = I_1 \times I_2 \times \cdots \times I_n$$
mit Idealen $I_j \subseteq R_j$ besitzt.

(3) Sei
$$I = I_1 \times I_2 \times \cdots \times I_n$$
ein Ideal in R. Zeige, dass I genau dann ein Hauptideal ist, wenn sämtliche I_j Hauptideale sind.

(4) Zeige, dass R genau dann ein Hauptidealring ist, wenn alle R_j Hauptidealringe sind.

Aufgaben zum Abgeben

Aufgabe 15.23. (3 Punkte)

Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 15.24. (3 Punkte)

Sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p für jede ganze Zahl a ist.

Aufgabe 15.25. (4 Punkte)

Zeige, dass $\mathbb{Q}[X]/(X^3 - 5)$ ein Körper ist und bestimme das Inverse von $5x^2 - x + 7$, wobei x die Restklasse von X bezeichne.

Aufgabe 15.26. (4 Punkte)

Sei R ein kommutativer Ring und sei $e \in R$ ein idempotentes Element. Zeige, dass auch $1 - e$ idempotent ist und dass die „zusammengesetzte“ Restklassenabbildung
$$R \longrightarrow R/(e) \times R/(1-e)$$
eine Bijektion ist.

Der folgende Satz heißt *Satz von Wilson*.

Sei p eine Primzahl. Dann ist
$$(p-1)! = -1 \mod p\,.$$

Aufgabe 15.27. (4 Punkte)

Bestimme die Zerlegung von $X^{p-1} - 1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.

16. Vorlesung - Chinesischer Restsatz für $\mathbb{Z}$

Der Chinesische Restsatz für $\mathbb{Z}$

Satz 16.1. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n) \to \mathbb{Z}/(p_i^{r_i})$ einen Isomorphismus*

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k}) .$$

Zu einer gegebenen ganzen Zahl $(a_1, a_2, \ldots, a_k)$ gibt es also genau eine natürliche Zahl $a < n$, die die simultanen Kongruenzen

$$a = a_1 \mod p_1^{r_1},\ a = a_2 \mod p_2^{r_2},\ \ldots,\ a = a_k \mod p_k^{r_k}$$

löst.

Beweis. Dies folgt unmittelbar aus Satz 15.7. □

Beweisvariante

Da die Ringe links und rechts beide endlich sind und die gleiche Anzahl von Elementen haben, nämlich n, genügt es, die Injektivität zu zeigen. Sei x eine natürliche Zahl, die im Produktring (rechts) zu 0 wird, also modulo $p_i^{r_i}$ den Rest 0 hat für alle $i = 1, 2, \ldots, k$. Dann ist x ein Vielfaches von $p_i^{r_i}$ für alle $i = 1, 2, \ldots, k$, d.h. in der Primfaktorzerlegung von x muss p_i zumindest mit Exponent r_i vorkommen. Also muss x nach Lemma 9.9 ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv.

Unter den Basislösungen zu einer simultanen Kongruenz versteht man die kleinsten natürlichen Zahlen, die modulo den vorgegebenen Zahlen ein Restetupel ergeben, das an genau einer Stelle den Wert 1 und sonst überall den Wert 0 besizt. Aus diesen Basislösungen kann man die Lösungen zu sämtlichen simultanen Kongruenzen berechnen.

Beispiel 16.2. Aufgabe:

(a) Bestimme für die Zahlen 3, 5 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

die Restetupel $(1, 0, 0)$, $(0, 1, 0)$ und $(0, 0, 1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 2 \mod 3, x = 4 \mod 5 \text{ und } x = 3 \mod 7$$

Lösung:

(a) $(1,0,0)$

alle Vielfachen von $5\cdot 7 = 35$ haben modulo 5 und modulo 7 den Rest 0. Unter diesen Vielfachen muss also die Lösung liegen. 35 hat modulo 3 den Rest 2, somit hat 70 modulo 3 den Rest 1. Also repräsentiert 70 das Restetupel $(1,0,0)$.

$(0,1,0)$: hier betrachtet man die Vielfachen von 21, und 21 hat modulo 5 den Rest 1. Also repräsentiert 21 das Restetupel $(0,1,0)$.

$(0,0,1)$: hier betrachtet man die Vielfachen von 15, und 15 hat modulo 7 den Rest 1. Also repräsentiert 15 das Restetupel $(0,0,1)$.

(b) Man schreibt (in $\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$)

$$(2,4,3) \;=\; 2(1,0,0) + 4(0,1,0) + 3(0,0,1).$$

Die Lösung ist dann

$$2 \cdot 70 + 4 \cdot 21 + 3 \cdot 15 \;=\; 140 + 84 + 45 \;=\; 269.$$

Die minimale Lösung ist dann $269 - 2 \cdot 105 \;=\; 59$.

Korollar 16.3. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann gibt es einen kanonischen Gruppenisomorphismus*

$$(\mathbb{Z}/(n))^\times \;\cong\; (\mathbb{Z}/(p_1^{r_1}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times .$$

Insbesondere ist eine Zahl a genau dann eine Einheit modulo n, wenn sie eine Einheit modulo $p_i^{r_i}$ ist für $i = 1, \ldots, k$.

Beweis. Dies folgt aus dem chinesischen Restsatz und Lemma 15.6. □

Die Eulersche φ-Funktion

Satz 16.4. *Genau dann ist $a \in \mathbb{Z}$ eine Einheit modulo n (d.h. a repräsentiert eine Einheit in $\mathbb{Z}/(n)$) wenn a und n teilerfremd sind.*

Beweis. Dies folgt aus Lemma 14.9. □

Beweisvariante

Sind a und n teilerfremd, so gibt es nach Satz 8.5 eine Darstellung der 1, es gibt also natürliche Zahlen r, s mit $ra + sn = 1$. Betrachtet man diese Gleichung modulo n, so ergibt sich $ra = 1$ in $\mathbb{Z}/(n)$. Damit ist a eine Einheit mit Inversem $a^{-1} = r$.

Ist umgekehrt a eine Einheit in $\mathbb{Z}/(n)$, so gibt es ein $r \in \mathbb{Z}/(n)$ mit $ar = 1$ in $\mathbb{Z}/(n)$. Das bedeutet aber, dass $ar - 1$ ein Vielfaches von n ist, so dass also $ar - 1 = sn$ gilt. Dann ist aber wieder $ar - sn = 1$ und a und n sind teilerfremd.

Leonhard Euler (1707-1783)

Definition 16.5. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion*.

Bemerkung 16.6. Die Eulersche Funktion $\varphi(n)$ gibt also nach Satz 16.4 an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

Für eine Primzahl p ist $\varphi(p) = p - 1$. Eine Verallgemeinerung des *kleinen Fermat* ist der folgende Satz von Euler.

Satz 16.7. *Sei n eine natürliche Zahl. Dann gilt für jede zu n teilerfremde Zahl a die Beziehung*

$$a^{\varphi(n)} = 1 \mod n\,.$$

Beweis. Das Element a gehört zur Einheitengruppe $(\mathbb{Z}/(n))^\times$, die $\varphi(n)$ Elemente besitzt. Nach Satz 11.6 ist aber die Gruppenordnung ein Vielfaches der Ordnung des Elementes. □

Wir geben abschließend Formeln an, wie man die Eulersche φ-Funktion berechnet, wenn die Primfaktorzerlegung bekannt ist.

Lemma 16.8. *Es sei p eine Primzahl und p^r eine Potenz davon. Dann ist*

$$\varphi(p^r) = p^{r-1}(p-1).$$

Beweis. Eine Zahl a ist genau dann teilerfremd zu einer Primzahlpotenz p^r, wenn sie teilerfremd zu p selbst ist, und dies ist genau dann der Fall, wenn sie kein Vielfaches von p ist. Unter den natürlichen Zahlen $< p^r$ sind genau die Zahlen

$$0, p, 2p, 3p, \ldots, (p^{r-1} - 1)p$$

Vielfache von p. Das sind p^{r-1} Stück, und daher gibt es

$$p^r - p^{r-1} = p^{r-1}(p-1)$$

Einheiten in $\mathbb{Z}/(p^r)$. Also ist $\varphi(p^r) = p^{r-1}(p-1)$. □

Korollar 16.9. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann ist*

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = (p_1 - 1)p^{r_1 - 1} \cdots (p_k - 1)p^{r_k - 1}.$$

Beweis. Die erste Gleichung folgt aus Korollar 16.3 und die zweite aus Lemma 16.8. □

16. Arbeitsblatt

Aufgabe 16.1.*

(a) Bestimme für die Zahlen 3, 5 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 2 \mod 3,\ x = 4 \mod 5 \text{ und } x = 3 \mod 7\,.$$

Aufgabe 16.2.*

(a) Bestimme für die Zahlen 2, 9 und 25 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(9) \times \mathbb{Z}/(25)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 0 \mod 2,\ x = 3 \mod 9 \text{ und } x = 5 \mod 25\,.$$

Aufgabe 16.3. a) Bestimme für die Zahlen 2, 3 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung a der Kongruenzen

$$a = 1 \mod 2,\ a = 2 \mod 3 \text{ und } a = 2 \mod 7\,.$$

Aufgabe 16.4. Gibt es eine natürliche Zahl n, die modulo 4 den Rest 3 und modulo 6 den Rest 2 besitzt?

Aufgabe 16.5.*

Man berechne in $\mathbb{Z}/(80)$ die Elemente

(1) $3^{1234567}$,
(2) $2^{1234567}$,
(3) $5^{1234567}$.

Aufgabe 16.6. Sei $n \geq 2$ eine natürliche Zahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) In der Primfaktorzerlegung von n kommt jeder Primfaktor mit Exponent 1 vor.
(2) Der Restklassenring $\mathbb{Z}/(n)$ ist reduziert.
(3) Der Restklassenring $\mathbb{Z}/(n)$ ist das Produkt von Körpern.

Aufgabe 16.7. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten in $\mathbb{Z}/(72)$.

Aufgabe 16.8. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(100)$.

Aufgabe 16.9. In dieser Aufgabe geht es um den Restklassenring $\mathbb{Z}/(360)$.

(1) Schreibe $\mathbb{Z}/(360)$ als Produktring.
(2) Wie viele Einheiten besitzt $\mathbb{Z}/(360)$?
(3) Schreibe das Element 239 in komponentenweiser Darstellung. Begründe, warum es sich um eine Einheit handelt und finde das Inverse in komponentenweiser Darstellung.
(4) Berechne die Ordnung von 239 in $\mathbb{Z}/(360)$.

Die nächste Aufgabe verwendet die folgende Definition.

Sei R ein kommutativer Ring und n_R das Nilideal von R, das aus allen nilpotenten Elementen von R besteht. Dann nennt man den Restklassenring R/n_R die *Reduktion* von R.

Aufgabe 16.10. Beschreibe die nilpotenten Elemente von $\mathbb{Z}/(n)$ und die Reduktion von $\mathbb{Z}/(n)$.

Aufgabe 16.11. Berechne die Werte der Eulerschen Funktion $\varphi(n)$ für $n \leq 20$.

Aufgabe 16.12. Zeige, dass die Eulersche Funktion φ für natürliche Zahlen n, m die Eigenschaft

$$\varphi(\mathrm{ggT}(m,n))\varphi(\mathrm{kgV}(m,n)) = \varphi(n)\varphi(m)$$

erfüllt.

Aufgaben zum Abgeben

Aufgabe 16.13. (4 Punkte)

(a) Bestimme für die Zahlen 4, 5 und 11 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{11}$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung a der *simultanen Kongruenzen*

$$a = 3 \mod 4,\ a = 2 \mod 5 \text{ und } a = 10 \mod 11\,.$$

Aufgabe 16.14. (3 Punkte)

Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(60)$.

Aufgabe 16.15. (3 Punkte)

Bestimme den Rest von 11! modulo 91.

Aufgabe 16.16. (4 Punkte)

Beweise die *Eulersche Formel* für die Eulersche Funktion φ, das ist die Aussage, dass

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ prim}} \left(1 - \frac{1}{p}\right)$$

gilt.

17. Vorlesung - Quotientenkörper

Quotientenkörper

Bei der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ betrachtet man die formalen Brüche

$$\frac{a}{b},\ a,b \in \mathbb{Z},\ b \neq 0$$

und identifiziert zwei Brüche $\frac{a}{b}$ und $\frac{c}{d}$, wenn $ad = bc$ ist. Das gleiche Verfahren kann man für jeden Integritätsbereich R anwenden und erhält dadurch einen Körper, in dem R als Unterring enthalten ist.

Definition 17.1. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

$$Q(R) = \left\{ \frac{r}{s} : r,s \in R,\ s \neq 0 \right\}$$

mit natürlichen Identifizierungen und Operationen.

Diese Definition ist etwas vage, gemein ist das folgende: Auf der Menge der Paare aus $R \times (R \setminus \{0\})$ führt man eine Äquivalenzrelation ein, indem man

$$(a,b) \sim (a',b') \text{ setzt, wenn } ab' = a'b \text{ ist}.$$

Die zugehörige Quotientenmenge ist dann der Quotientenkörper, also

$$Q(R) = R \times (R \setminus \{0\}) / \sim$$

Die Äquivalenzklasse zu (a,b) schreibt man als $\frac{a}{b}$. Man definiert dann durch $0 = \frac{0}{1}$, $1 = \frac{1}{1}$, spezielle Elemente in $Q(R)$ und durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

und

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

(wohldefinierte) Verknüpfungen, die $Q(R)$ zu einem kommutativen Ring machen. Bei $a,b \neq 0$ gilt

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1$$

und somit liegt ein Körper vor. Die Abbildung

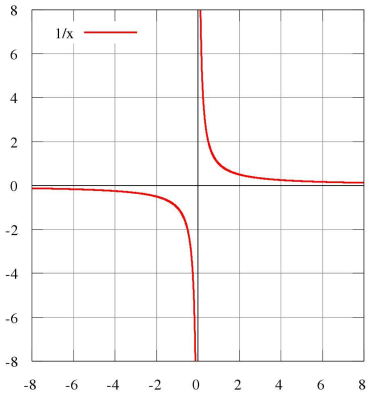
$$R \longrightarrow Q(R),\ r \longmapsto \frac{r}{1},$$

ist ein injektiver Ringhomomorphismus.

Die wichtigsten Beispiele für einen Quotientenkörper sind die rationalen Zahlen $Q(\mathbb{Z}) = \mathbb{Q}$

und der Quotientenkörper des Polynomrings in einer Variablen über einem (Grund-)körper K. Man bezeichnet ihn mit

$K(X) = Q(K[X])$ und nennt ihn den *Körper der rationalen Funktionen* (über K).



Man kann auch Brüche P/Q von Polynomen als Funktionen auffassen, die außerhalb der Nullstellen des Nenners definiert sind. Das Beispiel zeigt den Graph der rationalen Funktion $1/X$.

In der Tat definiert ein Bruch P/Q aus zwei Polynomen $P, Q \in K[X]$, $Q \neq 0$, eine Funktion

$$U \longrightarrow K,\, x \longmapsto \frac{P(x)}{Q(x)},$$

wobei $U \subseteq K$ das Komplement der Nullstellenmenge von Q bezeichnet. Wie schon im Fall von Polynomen und den dadurch definierten polynomialen Funktionen muss man auch hier bei einem endlichen Grundkörper vorsichtig sein und darf nicht die formalen Brüche mit den dadurch definierten Funktionen gleichsetzen.Bei $K = \mathbb{R}$ ist dies aber eine richtige und hilfreiche Vorstellung.

Die folgende Aussage kann man so verstehen, dass der Quotientenkörper der minimale Körper ist, in dem man einen Integritätsbereich als Unterring realisieren kann.

Satz 17.2. *Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Es sei*

$$\varphi\colon\, R \longrightarrow K$$

ein injektiver Ringhomomorphismus in einen Körper K Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon\, Q(R) \longrightarrow K$$

mit

$$\varphi = \tilde{\varphi}\tilde{i},$$

wobei i die kanonische Einbettung

$$i\colon\, R \longrightarrow Q(R)$$

bezeichnet.

Beweis. Damit die Ringhomomorphismen kommutieren muss

$$\tilde{\varphi}\,(1/b) \;=\; (\varphi(b))^{-1}$$

und damit $\tilde{\varphi}\,(a/b) \;=\; \varphi(a)(\varphi(b))^{-1}$ sein. Es kann also maximal einen solchen Ringhomomorphismus geben, der durch die letzte Gleichung definiert sein muss. Da für $b \neq 0$ auch $\varphi(b) \neq 0$ ist und K ein Körper ist, gibt es $\varphi(b)^{-1} \in K$. Es ist zu zeigen, dass dadurch ein wohldefinierter Ringhomomorphismus gegeben ist. Zur Wohldefiniertheit sei $\frac{a}{b} = \frac{c}{d}$, also $ad = bc$. Dann ist auch $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$ und durch Multiplizieren mit der Einheit $\varphi(b)^{-1}\varphi(d)^{-1}$ folgt

$$\varphi(a)(\varphi(b))^{-1} \;=\; \varphi(c)(\varphi(d))^{-1}.$$

Wir zeigen exemplarisch für die Addition, dass ein Ringhomomorphismus vorliegt. Es ist

$$\begin{aligned}
\tilde{\varphi}\left(\frac{a}{b}+\frac{c}{d}\right) &= \tilde{\varphi}\left(\frac{ad+cb}{bd}\right) \\
&= \varphi(ad+bc)\varphi(bd)^{-1} \\
&= (\varphi(a)\varphi(d)+\varphi(b)\varphi(c))\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1}+\varphi(c)\varphi(d)^{-1} \\
&= \tilde{\varphi}\left(\frac{a}{b}\right)+\tilde{\varphi}\left(\frac{c}{d}\right).
\end{aligned}$$

□

Für die vorstehende Aussage ist die Injektivität der Abbildung $R \to K$ wichtig. Beispielsweise gibt es für den Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/(p)$ keine Faktorisierung über $\mathbb{Q}$, da es überhaupt keinen Ringhomomorphismus von $\mathbb{Q}$ in einen endlichen Restklassenring von $\mathbb{Z}$ gibt.

Quotientenkörper zu faktoriellen Ringen

Lemma 17.3. *Zu einem Primelement $p \in R$ in einem faktoriellen Bereich R mit Quotientenkörper $Q(R)$ ist die Zuordnung*

$$Q(R)^\times \longrightarrow \mathbb{Z},\, \frac{f}{g} \longmapsto \exp_p(f) - \exp_p(g),$$

ein (wohldefinierter) Gruppenhomomorphismus.

Beweis. Zum Nachweis der Wohldefiniertheit sei

$$\frac{f}{g} \;=\; \frac{h}{q}$$

eine weitere Darstellung, also

$$fq \;=\; hg.$$

Dann ist nach Lemma 9.8

$$\exp_p(f)+\exp_p(q) \;=\; \exp_p(fq) \;=\; \exp_p(hg) \;=\; \exp_p(h)+\exp_p(g),$$

woraus sich

$$\exp_p(f) - \exp_p(g) \;=\; \exp_p(h) - \exp_p(q)$$

ergibt. Die Gruppenhomomorphie ergibt sich ebenfalls aus Lemma 9.8. $\square$

Satz 17.4. *Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Dann besitzt jedes Element $f \in K$, $f \neq 0$, eine im Wesentlichen eindeutige Produktzerlegung*

$$f \;=\; up_1^{r_1} \cdots p_n^{r_n}$$

mit einer Einheit $u \in R$ und ganzzahligen Exponenten r_i.

Beweis. Wir schreiben

$$f \;=\; \frac{a}{b}$$

mit von 0 verschiedenen Elementen $a, b \in R$. Die Primfaktorzerlegungen dieser Elemente seien $a = u_1 p_1^{m_1} \cdots p_n^{m_n}$ und $b = u_2 p_1^{k_1} \cdots p_n^{k_n}$, wobei die p_i nicht untereinander assoziiert seien, $m_i, k_i \in \mathbb{N}_{\geq 0}$ und u_1, u_2 Einheiten sind. Dann ist

$$\frac{a}{b} \;=\; \frac{u_1 p_1^{m_1} \cdots p_n^{m_n}}{u_2 p_1^{k_1} \cdots p_n^{k_n}} \;=\; u_1 u_2^{-1} p_1^{m_1 - k_1} \cdots p_n^{m_n - k_n}$$

eine Darstellung der gewünschten Art. Wenn zwei Dastellungen

$$up_1^{r_1} \cdots p_n^{r_n} \;=\; f \;=\; vp_1^{s_1} \cdots p_n^{s_n}$$

gegeben sind, so erhält man durch Multiplikation mit $(p_1 \cdots p_n)^t$ für hinreichend großes t, dass links und rechts alle Exponenten positiv werden. Aus der Faktorialität folgt daraus $r_i = s_i$ für alle i und damit auch $u = v$. $\square$

Man kann also beispielsweise jede rationale Zahl $q = a/b$ eindeutig schreiben als

$$q \;=\; \pm p_1^{r_1} \cdots p_n^{r_n}$$

mit Primzahlen $p_1, \ldots, p_n$ und Exponenten $r_1, \ldots, r_n \in \mathbb{Z}$. Der multiplikative Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ enspricht also auf der Ebene der Exponenten dem additiven Übergang von $\mathbb{N}$ nach $\mathbb{Z}$.

Die eben angeführte eindeutige Darstellung ist mit der Multiplikation verträglich. In der nächsten Aussage bedeutet die Schreibweise $\mathbb{Z}^{(I)}$ die Menge aller I-Tupel mit Werten in $\mathbb{Z}$, wobei aber jeweils nur endlich viele Einträge von 0 verschieden sein dürfen.

Satz 17.5. *Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Es sei p_i, $i \in I$, ein System von paarweise nicht assoziierten Primelementen von R und sei U die Einheitengruppe von R Dann ist (wobei $u(q)$ die nach Satz 17.4 eindeutige Einheit bezeichnet)*

$$Q(R)^\times \longrightarrow U \times \mathbb{Z}^{(I)},\; q \longmapsto (u(q), \exp_{p_i}(q)),$$

ein Gruppenisomorphismus mit der Umkehrabbildung

$$U \times \mathbb{Z}^{(I)} \longrightarrow Q(R)^\times,\; (u, e_{p_i}) \longmapsto u \prod_{i \in I} p^{e_{p_i}}.$$

Beweis. Dies folgt aus Lemma 17.3 und Satz 17.4. □

17. Arbeitsblatt

Übungsaufgaben

Aufgabe 17.1. Sei R ein Integritätsbereich und K ein Körper mit $R \subseteq K$. Zeige, dass dann auch $Q(R) \subseteq K$ gilt.

Aufgabe 17.2. Sei $\mathfrak{a}$ ein Ideal in einem kommutativen Ring R. Zeige, dass $\mathfrak{a}$ genau dann ein Primideal ist, wenn $\mathfrak{a}$ der Kern eines Ringhomomorphismus $\varphi\colon R \to K$ in einen Körper K ist.

Aufgabe 17.3. Berechne in $\mathbb{Q}(X)$ die folgenden Ausdrücke.

(1) Das Produkt
$$\frac{2X^3-5X^2+X-1}{X^2-2X+6} \cdot \frac{X^2+3}{5X^3-4X^2-7},$$
(2) Die Summe
$$\frac{4X^3-X^2+6X-2}{X^2-4X-3} + \frac{X^2-3}{3X^2+5},$$
(3) Das Inverse von
$$\frac{6X^3-9X^2+5X-1}{X^4-4X^3+3X^2-8X-3}.$$

Aufgabe 17.4. Zeige die Gleichheit
$$\frac{3X^4+2X^3+4X^2+1}{X^3+X+1} = X^2+3X+1$$
als Funktion von $\mathbb{Z}/(5)$ nach $\mathbb{Z}/(5)$.

Aufgabe 17.5. Skizziere die Graphen der folgenden rationalen Funktionen
$$\frac{1}{x}\ \frac{1}{x-1}, \frac{1}{x^2}, \frac{1}{x(x-1)}, \frac{x-1}{x^2}.$$

Aufgabe 17.6. Erstelle eine Wertetabelle für die rationale Funktion
$$\frac{X^2+4X+3}{X^3+X+2} \in \mathbb{Z}/(7)(X).$$

Aufgabe 17.7. Es sei

$$G = \langle \frac{2}{3}, \frac{4}{5} \rangle \subseteq (\mathbb{Q}, 0, +)$$

die von $\frac{2}{3}$ und $\frac{4}{5}$ erzeugte Untergruppe. Zeige, dass G auch von einem Element erzeugt wird. Von welchem?

Aufgabe 17.8. Es seien $a, b \in \mathbb{N}_+$ und sei

$$G = \langle \frac{1}{a}, \frac{1}{b} \rangle \subseteq (\mathbb{Q}, 0, +)$$

die von $\frac{1}{a}$ und $\frac{1}{b}$ erzeugte Untergruppe. Zeige, dass G von $\frac{1}{\mathrm{KgV}(a,b)}$ erzeugt wird.

Aufgabe 17.9. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Zeige, dass sie nicht endlich erzeugt ist.

Aufgabe 17.10. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Es sei $G \subseteq \mathbb{Q}$ eine endlich erzeugte Untergruppe. Zeige, dass G zyklisch ist.

Aufgabe 17.11. Es sei $T \subseteq \mathbb{P}$ eine Teilmenge der Primzahlen. Zeige, dass die Menge

$$R_T = \{q \in Q |\ q \text{ lässt sich mit einem Nenner schreiben, in dem nur Primzahlen aus } T \text{ vorkommen } \}$$

ein Unterring von $\mathbb{Q}$ ist. Was ergibt sich bei $T = \emptyset$, $T = \mathbb{P}$, $T = \{3\}$, $T = \{2, 5\}$?

Aufgabe 17.12. Es sei $\mathbb{P}$ die Menge der Primzahlen und

$$\alpha \colon \mathbb{P} \longrightarrow \mathbb{Z}$$

eine Abbildung. Zeige, dass die Menge

$$G_\alpha = \left\{ q \in \mathbb{Q}^\times |\ \exp_p(q) \geq \alpha(p) \text{ für alle } p \right\} \cup \{0\}$$

eine Untergruppe von $(\mathbb{Q}, 0, +)$ ist.

Aufgabe 17.13.*

Sei p eine Primzahl. Man gebe einen Körper der Charakteristik p an, der unendlich viele Elemente besitzt.

Die folgende Definition wird in den nächsten Aufgaben verwendet.

Ein kommutativer Ring heißt *angeordnet*, wenn es eine totale Ordnung „$\geq$“ auf R gibt, die die beiden Eigenschaften

(1) Aus $a \geq b$ folgt $a + c \geq b + c$ für beliebige $a, b, c \in R$,
(2) Aus $a \geq b$ folgt $ac \geq bc$ für beliebige $a, b, c \in R$ mit $c \geq 0$,

erfüllt.

Die ganzen Zahlen bilden einen angeordneten Ring. Die Anordnung überträgt sich auf den Quotientenkörper, die rationalen Zahlen bilden also einen angeordneten Körper.

Aufgabe 17.14. Zeige, dass $\mathbb{Q}$ mit der durch $\frac{a}{b} \geq \frac{c}{d}$ (bei $b, d \in \mathbb{N}_+$), falls $ad \geq cb$ in $\mathbb{Z}$ gilt, definierten Beziehung ein angeordneter Körper ist (dabei dürfen nur Eigenschaften der Ordnung auf $\mathbb{Z}$ verwendet werden).

Aufgabe 17.15. Man gebe fünf rationale Zahlen an, die (echt) zwischen $\frac{3}{8}$ und $\frac{7}{8}$ liegen.

Aufgabe 17.16. Person A wird 80 Jahre alt und Person B wird 70 Jahre alt. Vergleiche die Gesamtlebenswachzeit und die Gesamtlebensschlafzeit der beiden Personen bei folgendem Schlafverhalten.

(1) A schläft jede Nacht 7 Stunden und B schläft jede Nacht 8 Stunden.
(2) A schläft jede Nacht 8 Stunden und B schläft jede Nacht 7 Stunden.

Aufgabe 17.17.*

Eine Bahncard 25, mit der man ein Jahr lang 25 Prozent des Normalpreises einspart, kostet 62 Euro und eine Bahncard 50, mit der man ein Jahr lang 50 Prozent des Normalpreises einspart, kostet 255 Euro. Für welchen Jahresgesamtnormalpreis ist keine Bahncard, die Bahncard 25 oder die Bahncard 50 die günstigste Option?

Aufgabe 17.18.*

Zwei Fahrradfahrer, A und B, fahren auf ihren Fahrrädern eine Straße entlang. Fahrer A macht pro Minute 40 Pedalumdrehungen, hat eine Übersetzung von Pedal zu Hinterrad von 1 zu 6 und Reifen mit einem Radius von 39 Zentimetern. Fahrer B braucht für eine Pedaldrehung 2 Sekunden, hat eine Übersetzung von 1 zu 7 und Reifen mit einem Radius von 45 Zentimetern.

Wer fährt schneller?

Aufgabe 17.19. Man gebe die Antworten als Bruch (bezogen auf das angegebene Vergleichsmaß): Um wie viel ist eine drei Viertel Stunde länger als eine halbe Stunde, und um wie viel ist eine halbe Stunde kürzer als eine drei Viertel Stunde?

Aufgaben zum Abgeben

Aufgabe 17.20. (3 Punkte)

Bestimme einen Erzeuger für die Untergruppe $H \subseteq (\mathbb{Q}, +, 0)$, die durch die rationalen Zahlen

$$\frac{8}{7}, \frac{5}{11}, \frac{7}{10}$$

erzeugt wird.

Aufgabe 17.21. (4 Punkte)

Es seien $a, b, c, d \in \mathbb{N}_+$ und sei

$$G = \langle \frac{a}{b}, \frac{c}{d} \rangle \subseteq (\mathbb{Q}, 0, +)$$

die von $\frac{a}{b}$ und $\frac{c}{d}$ erzeugte Untergruppe. Zeige, dass G von $\frac{\mathrm{GgT}(a,c)}{\mathrm{KgV}(b,d)}$ erzeugt wird.

Aufgabe 17.22. (3 Punkte)

Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Zeige, dass jedes Element $f \in K$, $f \neq 0$, eine im Wesentlichen eindeutige Produktzerlegung

$$f = u p_1^{r_1} \cdots p_n^{r_n}$$

mit einer Einheit $u \in R$ und ganzzahligen Exponenten r_i besitzt.

Aufgabe 17.23. (3 Punkte)

Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Es sei $a \in K$ ein Element mit $a^n \in R$ für eine natürliche Zahl $n \geq 1$. Zeige, dass dann schon a zu R gehört.

Was bedeutet dies für $R = \mathbb{Z}$?

Aufgabe 17.24. (3 Punkte)

Zeige, dass die beiden kommutativen Gruppen $(\mathbb{Q}, 0, +)$ und $(\mathbb{Q}_+, 1, \cdot)$ nicht isomorph sind.

18. Vorlesung - Partialbruchzerlegung

Partialbruchzerlegung

Betrachten wir den Bruch $\frac{1}{6}$. Diesen kann man als

$$\frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3}$$

schreiben, man kann also die Primfaktoren des Nenners multiplikativ trennen. Es gilt aber auch, und das ist überraschender, die Darstellung

$$\frac{1}{6} = \frac{1}{2} - \frac{1}{3},$$

man kann also in diesem Fall den Bruch als eine Summe von Brüchen schreiben, bei denen jeweils nur ein Primfaktor des Nenners vorkommt. In ähnlicher Weise gilt

$$\frac{1}{35} = -\frac{2}{5} + \frac{3}{7},$$

auch hier lässt sich ein Bruch mit einem „komplizierten“ Nenner als Summe von Brüchen mit einem einfachen Nenner schreiben. Dagegen ist es nicht möglich, $\frac{1}{4}$ als Summe von $\frac{1}{2}$ zu schreiben. Wir werden gleich sehen, dass man jede rationale Zahl als eine Summe von Stammbrüchen zu Primzahlpotenzen erhalten kann. Dies beruht auf einer Gesetzmäßigkeit, die allgemeiner für Hauptidealbereiche gilt.

Satz 18.1. *Es sei R ein Hauptidealbereich und $f, g \in R$, $g \neq 0$, mit der Primfaktorzerlegung*

$$g = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Dann gibt es im Quotientenkörper $Q(R)$ eine Darstellung

$$\frac{f}{g} = \frac{a_1}{p_1^{r_1}} + \frac{a_2}{p_2^{r_2}} + \cdots + \frac{a_k}{p_k^{r_k}}$$

mit $a_1, \ldots, a_k \in R$.

Beweis. Wir führen Induktion über die Anzahl k der verschiedenen Primfaktoren von g. Wenn g eine Einheit ist oder nur ein Primfaktor (mit einem beliebigen Exponenten) vorkommt, ist nichts zu zeigen. Sei also $k \geq 2$ und die Aussage für kleinere k schon bewiesen. Sei

$$h = p_2^{r_2} \cdots p_k^{r_k}.$$

Da $p_1^{r_1}$ und h teilerfremd sind, gibt es nach Satz 8.5 eine Darstellung der Form

$$up_1^{r_1} + vh = 1$$

mit $u, v \in R$. Division durch

$$g = p_1^{r_1} h$$

ergibt

$$\frac{1}{g} = \frac{v}{p_1^{r_1}} + \frac{u}{h}.$$

Multiplikation mit f liefert eine Darstellung der Form

$$\frac{f}{g} = \frac{a_1}{p_1^{r_1}} + \frac{c}{h}$$

und die Induktionsvoraussetzung angewendet auf $\frac{c}{h}$ liefert das Resultat. $\square$

Für $R = \mathbb{Z}$ und $R = K[X]$ und überhaupt für euklidische Bereiche lässt sich diese Aussage noch präzisieren.

Satz 18.2. *Es sei R ein euklidischer Bereich und $f, g \in R$, $g \neq 0$, mit der Primfaktorzerlegung*

$$g = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Dann gibt es im Quotientenkörper $Q(R)$ eine Darstellung

$$\frac{f}{g} = b + \frac{a_1}{p_1^{r_1}} + \frac{a_2}{p_2^{r_2}} + \cdots + \frac{a_k}{p_k^{r_k}}$$

mit $b, a_1, \ldots, a_k \in R$ mit $a_j = 0$ oder

$$\delta(a_j) < \delta(p_j^{r_j}).$$

Die Summanden $\frac{a_j}{p_j^{r_j}}$ kann man als

$$\frac{c_j}{p_j^{r_j}} = b_j + \frac{c_{j,1}}{p_j} + \frac{c_{j,2}}{p_j^2} + \cdots + \frac{c_{j,r_j}}{p_j^{r_j}}$$

mit

$$\delta(c_{j,i}) \leq \delta(p_j)$$

schreiben.

Beweis. Nach Satz 18.1 gibt es eine Darstellung

$$\frac{f}{g} = \frac{a_1}{p_1^{r_1}} + \frac{a_2}{p_2^{r_2}} + \cdots + \frac{a_k}{p_k^{r_k}}.$$

Auf die einzelnen Summanden wenden wir die Division mit Rest durch $p_j^{r_j}$ an und erhalten

$$\frac{a_j}{p_j^{r_j}} = b_j + \frac{a_j'}{p_j^{r_j}}$$

mit

$$\delta\left(a_j'\right) < \delta\left(p_j^{r_j}\right).$$

Ferner kann man auf a_j auch die Division mit Rest durch p_j anwenden und erhält

$$\frac{a_j}{p_j^{r_j}} = \frac{c_j p + t}{p_j^{r_j}} = \frac{c_j}{p_j^{r_j - 1}} + \frac{t}{p_j^{r_j}}$$

mit

$$\delta(t) < \delta(p).$$

Den vorderen Summanden kann man in dieser Weise weiter abarbeiten. □

Korollar 18.3. *Es seien $f, g \in \mathbb{Z}$, $g > 0$, mit der Primfaktorzerlegung*

$$g = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Dann gibt es im Quotientenkörper $Q(R)$ eine Darstellung

$$\frac{f}{g} = n + \frac{a_1}{p_1^{r_1}} + \frac{a_2}{p_2^{r_2}} + \cdots + \frac{a_k}{p_k^{r_k}}$$

mit $n, a_1, \ldots, a_k \in \mathbb{Z}$ und mit $|a_j| < p_j^{r_j}$. Für die Summanden gibt es ferner eine Darstellung

$$\frac{a_j}{p_j^{r_j}} = n_j + \frac{c_{j,1}}{p_j} + \frac{c_{j,2}}{p_j^2} + \cdots + \frac{c_{j,r_j}}{p_j^{r_j}}$$

mit $|c_{j,i}| < p_j$. Dabei kann man die $c_{j,i} \geq 0$ wählen.

Beweis. Dies folgt unmittelbar aus Satz 18.2. □

Beispiel 18.4. Wir berechnen die Partialbruchzerlegung von $\frac{1}{100}$. Es ist

$$100 = 4 \cdot 25 = 2^2 \cdot 5^2.$$

Wegen

$$25 - 6 \cdot 4 = 1$$

ergibt sich

$$\frac{1}{100} = \frac{1}{4} - 6\frac{1}{25} = \frac{1}{4} - \frac{1}{5} - \frac{1}{25}.$$

Wenn man nichtnegative Zähler haben möchte, so schreibt man

$$\begin{aligned} \frac{1}{4} - 6\frac{1}{25} &= -1 + \frac{1}{4} + 1 - 6\frac{1}{25} \\ &= -1 + \frac{1}{4} + \frac{25-6}{25} \\ &= -1 + \frac{1}{4} + \frac{19}{25} \\ &= -1 + \frac{1}{4} + \frac{3}{5} + \frac{4}{25}. \end{aligned}$$

Korollar 18.5. *Es sei K ein Körper und $f, g \in K[X]$, $g \neq 0$, mit der Zerlegung in irreduzible Polynome*

$$g = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Dann gibt es im Quotientenkörper $K(X)$ eine Darstellung

$$\frac{f}{g} = h + \frac{q_1}{p_1^{r_1}} + \frac{q_2}{p_2^{r_2}} + \cdots + \frac{q_k}{p_k^{r_k}}$$

mit $h, q_1, \ldots, q_k \in K[X]$ mit $q_j = 0$ oder

$$\operatorname{grad}(q_j) < \operatorname{grad}(p_j^{r_j}).$$

Die Summanden $\frac{q_j}{p_j^{r_j}}$ *kann man als*

$$\frac{q_j}{p_j^{r_j}} = h_j + \frac{c_{j,1}}{p_j} + \frac{c_{j,2}}{p_j^2} + \cdots + \frac{c_{j,r_j}}{p_j^{r_j}}$$

mit

$$\operatorname{grad}(c_{j,i}) < \operatorname{grad}(p_j).$$

schreiben.

Beweis. Dies folgt unmittelbar aus Satz 18.2. □

Korollar 18.6. *Es seien* $P, Q \in \mathbb{C}[X]$, $Q \neq 0$, *Polynome und es sei*

$$Q = (X - a_1)^{r_1} \cdots (X - a_s)^{r_s}$$

mit verschiedenen $a_i \in \mathbb{C}$. *Dann gibt es ein eindeutig bestimmtes Polynom* $H \in \mathbb{C}[X]$ *und eindeutig bestimmte Koeffizienten* $c_{ij} \in \mathbb{C}$, $1 \leq i \leq s$, $1 \leq j \leq r_i$, *mit*

$$\frac{P}{Q} = H + \frac{c_{11}}{X - a_1} + \frac{c_{12}}{(X - a_1)^2} + \cdots + \frac{c_{1r_1}}{(X - a_1)^{r_1}} + \cdots + \frac{c_{s1}}{X - a_s} + \frac{c_{s2}}{(X - a_s)^2} + \cdots + \frac{c_{sr_s}}{(X - a_s)^{r_s}}.$$

Beweis. Dies ergibt sich, abgesehen von der Eindeutigkeit, die wir nicht beweisen, aus Korollar 18.5 und dem Fundamentalsatz der Algebra. □

Korollar 18.7. *Es seien* $P, Q \in \mathbb{R}[X]$, $Q \neq 0$, *Polynome und es sei*

$$Q = (X - a_1)^{r_1} \cdots (X - a_s)^{r_s} Q_1^{t_1} \cdots Q_u^{t_u}$$

mit verschiedenen $a_i \in \mathbb{R}$ *und verschiedenen quadratischen Polynomen* Q_k *ohne reelle Nullstellen. Dann gibt es ein eindeutig bestimmtes Polynom* $H \in \mathbb{R}[X]$ *und eindeutig bestimmte Koeffizienten* $c_{ij} \in \mathbb{R}$, $1 \leq i \leq s$, $1 \leq j \leq r_i$, *und eindeutig bestimmte lineare Polynome* $L_{k\ell} = d_{k\ell}X + e_{k\ell}$, $1 \leq k \leq u$, $1 \leq \ell \leq t_k$, *mit*

$$\begin{aligned}\frac{P}{Q} = {} & H + \frac{c_{11}}{X - a_1} + \frac{c_{12}}{(X - a_1)^2} + \cdots + \frac{c_{1r_1}}{(X - a_1)^{r_1}} \\ & + \cdots + \frac{c_{s1}}{X - a_s} + \frac{c_{s2}}{(X - a_s)^2} + \cdots + \frac{c_{sr_s}}{(X - a_s)^{r_s}} \\ & + \frac{L_{11}}{Q_1} + \frac{L_{12}}{Q_1^2} + \cdots + \frac{L_{1t_1}}{Q_1^{t_1}} \\ & + \cdots + \frac{L_{u1}}{Q_u} + \frac{L_{u2}}{Q_u^2} + \cdots + \frac{L_{ut_u}}{Q_u^{t_u}}.\end{aligned}$$

Beweis. Dies ergibt sich, abgesehen von der Eindeutigkeit, die wir nicht beweisen, aus Korollar 18.5 und der Tatsache, dass es in $\mathbb{R}[X]$ nur lineare und quadratische Primpolynome gibt. □

Beispiel 18.8. Wir betrachten die rationale Funktion

$$\frac{1}{X^3-1} = \frac{1}{(X-1)\,(X^2+X+1)}.$$

wobei der Faktor rechts reell nicht weiter zerlegbar ist. Daher muss es eine eindeutige Darstellung

$$\frac{1}{X^3-1} = \frac{a}{X-1} + \frac{bX+c}{X^2+X+1}$$

geben. Multiplikation mit dem Nennerpolynom führt auf

$$\begin{aligned} 1 &= a\left(X^2+X+1\right) + (bX+c)(X-1) \\ &= (a+b)X^2 + (a+c-b)X + a - c. \end{aligned}$$

Koeffizientenvergleich führt auf das inhomogene lineare Gleichungssystem

$$a+b=0 \text{ und } a+c-b=0 \text{ und } a-c=1$$

mit den eindeutigen Lösungen

$$a=\frac{1}{3},\ b=-\frac{1}{3},\ c=-\frac{2}{3}\,.$$

Die Partialbruchzerlegung ist also

$$\frac{1}{X^3-1} = \frac{\frac{1}{3}}{X-1} + \frac{-\frac{1}{3}X-\frac{2}{3}}{X^2+X+1} = \frac{1}{3}\cdot\frac{1}{X-1} - \frac{1}{3}\cdot\frac{X+2}{X^2+X+1}.$$

Beispiel 18.9. Wir betrachten die rationale Funktion

$$\frac{X^3-X+5}{X^4+X^2} = \frac{X^3-X+5}{X^2\,(X^2+1)},$$

wo die Faktorzerlegung des Nennerpolynoms sofort ersichtlich ist. Der Ansatz

$$\frac{X^3-X+5}{X^2\,(X^2+1)} = \frac{a}{X} + \frac{b}{X^2} + \frac{cX+d}{X^2+1}$$

führt durch Multiplikation mit dem Nennerpolynom auf

$$\begin{aligned} X^3-X+5 &= aX\left(X^2+1\right) + b\left(X^2+1\right) + (cX+d)X^2 \\ &= aX^3+aX+bX^2+b+cX^3+dX^2 \\ &= (a+c)X^3+(b+d)X^2+aX+b. \end{aligned}$$

Koeffizientenvergleich führt auf das inhomogene lineare Gleichungssystem

$$a+c=1 \text{ und } b+d=0 \text{ und } a=-1 \text{ und } b=5$$

mit der Lösung

$$b=5,\ a=-1,\ d=-5,\ c=2\,.$$

Insgesamt ist die Partialbruchzerlegung also gleich

$$\frac{X^3-X+5}{X^2(X^2+1)} = -\frac{1}{X} + \frac{5}{X^2} + \frac{2X-5}{X^2+1}\,.$$

Bemerkung 18.10. Eine wichtige Anwendung der reellen Partialbruchzerlegung ist es, zu rationalen Funktionen P/Q, $P, Q \in \mathbb{R}[X]$, $Q \neq 0$, eine Stammfunktion zu finden, also zu integrieren. Man berechnet hierzu die Partialbruchzerlegung von P/Q und muss dann zu dem Polynom H und den Summanden der Form $\frac{b}{(X-a)^r}$ bzw. $\frac{c+dX}{Q_i^r}$ mit einem quadratischen nullstellenfreien Polynom Q_i Stammfunktionen bestimmen. Dafür gibt es dann Standardverfahren. Eine Stammfunktion zu $\frac{b}{(X-a)}$ ist $b \ln |X-a|$ und eine Stammfunktion zu $\frac{b}{(X-a)}$, $r \geq 2$, ist $\frac{b}{(1-r)(X-a)^{r-1}}$. Wenn ein quadratischer Nenner vorliegt, wird es schwieriger; eine Stammfunktion zu $\frac{1}{1+x^2}$ ist beispielsweise $\arctan X$.

18. Arbeitsblatt

Übungsaufgaben

Aufgabe 18.1. Man gebe die Partialbruchzerlegung der Stammbrüche

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{25}$$

an.

Aufgabe 18.2. Man gebe die Partialbruchzerlegung der Stammbrüche

$$\frac{1}{10}, \frac{1}{100}, \frac{1}{1000}, \frac{1}{10000}, \ldots$$

an.

Aufgabe 18.3. Finde eine Darstellung der rationalen Zahl $1/60$ als Summe von rationalen Zahlen, deren Nenner Primzahlpotenzen sind.

Aufgabe 18.4. Zeige, dass für Zahlen $n, r \in \mathbb{N}_+$ die Gleichheit

$$\frac{n^r - 1}{n^r} = \frac{n-1}{n} + \frac{n-1}{n^2} + \cdots + \frac{n-1}{n^{r-1}} + \frac{n-1}{n^r}$$

gilt.

Was bedeutet die vorstehende Aufgabe bei $n = 10$?

Aufgabe 18.5. Bestimme die Partialbruchzerlegung von

$$\frac{100}{77}.$$

Aufgabe 18.6. Bestimme die Partialbruchzerlegung von

$$\frac{999}{75}.$$

Aufgabe 18.7. Bestimme die Partialbruchzerlegung von

$$\frac{1}{X(X-1)}$$

über einem Körper K.

Aufgabe 18.8. Bestimme die Partialbruchzerlegung von

$$\frac{3X^5+4X^4-2X^2+5X-6}{X^3}.$$

Aufgabe 18.9. Bestimme die Koeffizienten in der Partialbruchzerlegung in Beispiel 18.9 durch Einsetzen von einigen Zahlen für X.

Aufgabe 18.10.*

Bestimme die reelle Partialbruchzerlegung von

$$\frac{1}{x^4+1}$$

unter Verwendung der Zerlegung

$$x^4+1 = \left(x^2+\sqrt{2}x+1\right)\left(x^2-\sqrt{2}x+1\right).$$

Aufgabe 18.11. Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{1}{X^2(X^2+1)}.$$

Aufgabe 18.12. Bestimme die komplexe Partialbruchzerlegung von

$$\frac{1}{X^3-1}.$$

Aufgabe 18.13. Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{1}{X^3(X-1)^3}.$$

Aufgabe 18.14. Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{X^3+4X^2+7}{X^2-X-2}\,.$$

Aufgabe 18.15. Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{1}{X(X-1)(X-2)(X-3)}\,.$$

Aufgabe 18.16.*

Es sei

$$f(x)=\frac{x^3+7x^2-5x+4}{x^2-3}\,.$$

a) Bestimme die reelle Partialbruchzerlegung von $f(x)$.

b) Bestimme eine Stammfunktion von $f(x)$.

Aufgabe 18.17.*

a) Zeige, dass X^3+X^2+2 irreduzibel in $\mathbb{Z}/(3)[X]$ ist.

b) Bestimme die Partialbruchzerlegung von

$$\frac{X^4}{\left(X^3+X^2+2\right)^2}$$

in $\mathbb{Z}/(3)(X)$.

Aufgabe 18.18.*

a) Zeige, dass X^2+2 irreduzibel in $\mathbb{Z}/(5)[X]$ ist.

b) Zeige, dass X^3+X+1 irreduzibel in $\mathbb{Z}/(5)[X]$ ist.

c) Bestimme die Partialbruchzerlegung von

$$\frac{1}{\left(X^2+2\right)\left(X^3+X+1\right)}$$

in $\mathbb{Z}/(5)(X)$.

Aufgabe 18.19.*

a) Zeige, dass X^2+1 irreduzibel in $\mathbb{Q}[X]$ ist.

b) Zeige, dass X^4+1 irreduzibel in $\mathbb{Q}[X]$ ist. (Tipp: In $\mathbb{R}[X]$ gilt die Zerlegung $X^4+1 = \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$)

c) Bestimme die Partialbruchzerlegung von

$$\frac{1}{(X^2+1)(X^4+1)}$$

in $\mathbb{Q}(X)$.

Aufgaben zum Abgeben

Aufgabe 18.20. (4 Punkte)

Finde eine Darstellung der rationalen Zahl 1/210 als Summe von rationalen Zahlen, deren Nenner Primzahlpotenzen sind.

Aufgabe 18.21. (3 Punkte)

Bestimme die Partialbruchzerlegung von

$$\frac{1536}{245}.$$

Aufgabe 18.22. (2 Punkte)

Es sei K ein Körper. Zeige, dass im Funktionenkörper $K(X)$ die Gleichheit

$$\frac{X^r-1}{X^r} = \frac{X-1}{X} + \frac{X-1}{X^2} + \cdots + \frac{X-1}{X^{r-1}} + \frac{X-1}{X^r}$$

gilt.

Aufgabe 18.23. (4 Punkte)

Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{1}{X^4-1}.$$

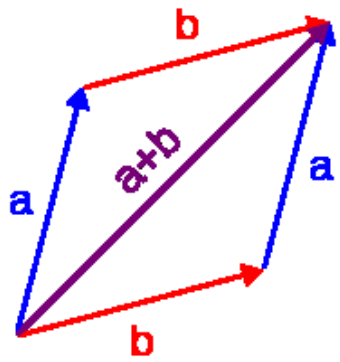
Aufgabe 18.24. (5 Punkte)

Bestimme die komplexe und die reelle Partialbruchzerlegung von

$$\frac{X^7+X^4-5X+3}{X^8+X^6-X^4-X^2}.$$

19. Vorlesung - Vektorräume

Vektorräume



Die Addition von zwei Pfeilen a und b, ein typisches Beispiel für Vektoren.

Der zentrale Begriff der linearen Algebra ist der Vektorraum.

Definition 19.1. Es sei K ein Körper und V eine Menge mit einem ausgezeichneten Element $0 \in V$ und mit zwei Abbildungen

$$+\colon V \times V \longrightarrow V,\ (u,v) \longmapsto u+v,$$

und

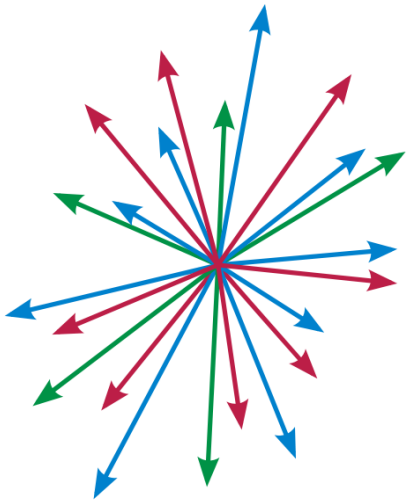
$$K \times V \longrightarrow V,\ (s,v) \longmapsto sv = s \cdot v.$$

Dann nennt man V einen *K-Vektorraum* (oder einen Vektorraum über K), wenn die folgenden Axiome erfüllt sind (dabei seien $r,s \in K$ und $u,v,w \in V$ beliebig)

(1) $u+v = v+u$,
(2) $(u+v)+w = u+(v+w)$,
(3) $v+0 = v$,
(4) Zu jedem v gibt es ein z mit $v+z = 0$,
(5) $r(su) = (rs)u$,
(6) $r(u+v) = ru+rv$,
(7) $(r+s)u = ru+su$,
(8) $1 \cdot u = u$.

Die Verknüpfung in V nennt man (Vektor)-Addition und die Operation $K \times V \to V$ nennt man *Skalarmultiplikation*. Die Elemente in einem Vektorraum nennt man *Vektoren*, und die Elemente $r \in K$ heißen *Skalare*. Das Nullelement $0 \in V$ wird auch als *Nullvektor* bezeichnet, und zu $v \in V$ heißt das inverse Element das *Negative* zu v und wird mit $-v$ bezeichnet. Den Körper, der im Vektorraumbegriff vorausgesetzt ist, nennt man auch

den *Grundkörper*. Alle Begriffe der linearen Algebra beziehen sich auf einen solchen Grundkörper, er darf also nie vergessen werden, auch wenn er manchmal nicht explizit aufgeführt wird. Bei $K = \mathbb{R}$ spricht man von *reellen Vektorräumen* und bei $K = \mathbb{C}$ von *komplexen Vektorräumen*. Bei reellen und komplexen Vektorräumen gibt es zusätzliche Strukturen wie Längen, Winkel, Skalarprodukt. Zunächst entwickeln wir aber die algebraische Theorie der Vektorräume über einem beliebigen Körper.



Beispiel 19.2. Es sei K ein Körper und $n \in \mathbb{N}_+$. Dann ist die Produktmenge

$$K^n = \underbrace{K \times \cdots \times K}_{n-\text{mal}} = \{(x_1, \ldots, x_n) | \, x_i \in K\}$$

mit der komponentenweisen Addition und der durch

$$s(x_1, \ldots, x_n) \ = \ (sx_1, \ldots, sx_n)$$

definierten Skalarmultiplikation ein Vektorraum. Man nennt ihn den n-dimensionalen *Standardraum*. Insbesondere ist $K^1 = K$ selbst ein Vektorraum.

Der Nullraum 0, der aus dem einzigen Element 0 besteht, ist ebenfalls ein Vektorraum. Man kann ihn auch als $K^0 = 0$ auffassen.

Die Vektoren im Standardraum K^n kann man als Zeilenvektoren

$$(a_1, \, a_2, \, \ldots, \, a_n)$$

oder als Spaltenvektor

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

schreiben. Der Vektor

$$e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

wobei die 1 an der i-ten Stelle steht, heißt i-ter *Standardvektor*.

Beispiel 19.3. Die komplexen Zahlen $\mathbb{C}$ bilden einen Körper und daher bilden sie einen Vektorraum über sich selbst. Andererseits sind die komplexen Zahlen als additive Struktur gleich $\mathbb{R}^2$. Die Multiplikation einer komplexen Zahl $a + bi$ mit einer reellen Zahl $s = (s, 0)$ geschieht komponentenweise, d.h. diese Multiplikation stimmt mit der skalaren Multiplikation auf $\mathbb{R}^2$ überein. Daher sind die komplexen Zahlen auch ein reeller Vektorraum. Unter Verwendung einer späteren Terminologie kann man sagen, dass $\mathbb{C}$ ein eindimensionaler komplexer Vektorraum ist und dass $\mathbb{C}$ ein zweidimensionaler reeller Vektorraum ist mit der reellen Basis 1 und i.

Beispiel 19.4. Zu einem Körper K und gegebenen natürlichen Zahlen m, n bildet die Menge

$$\mathrm{Mat}_{m\times n}(K)$$

der $m \times n$-Matrizen mit komponentenweiser Addition und komponentenweiser Skalarmultiplikation einen K-Vektorraum. Das Nullelement in diesem Vektorraum ist die *Nullmatrix*

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}.$$

Beispiel 19.5. Sei $R = K[X]$ der Polynomring in einer Variablen über dem Körper K. Mit der (komponentenweisen) Addition und der ebenfalls komponentenweisen Multiplikation mit einem Skalar $s \in K$ (was man auch als die Multiplikation mit dem konstanten Polynom s auffassen kann) ist der Polynomring ein K-Vektorraum.

Lemma 19.6. *Es sei K ein Körper und V ein K-Vektorraum. Dann gelten die folgenden Eigenschaften (dabei sei $v \in V$ und $s \in K$).*

(1) *Es ist $0v = 0$.* [1]
(2) *Es ist $s0 = 0$.*
(3) *Es ist $(-1)v = -v$.*
(4) *Aus $s \neq 0$ und $v \neq 0$ folgt $sv \neq 0$.*

[1] Man mache sich hier und im Folgenden klar, wann die 0 in K und wann sie in V zu verstehen ist.

Beweis. Siehe Aufgabe 19.6. □

Untervektorräume

Definition 19.7. Es sei K ein Körper und V ein K-Vektorraum. Eine Teilmenge $U \subseteq V$ heißt *Untervektorraum*, wenn die folgenden Eigenschaften gelten.

(1) $0 \in U$.
(2) Mit $u, v \in U$ ist auch $u + v \in U$.
(3) Mit $u \in U$ und $s \in K$ ist auch $su \in U$.

Auf einem solchen Untervektorraum kann man die Addition und die skalare Multiplikation einschränken. Daher ist ein Untervektorraum selbst ein Vektorraum, siehe Aufgabe 19.4. Die einfachsten Untervektorräume in einem Vektorraum V sind der Nullraum 0 und der gesamte Vektorraum V.

Lemma 19.8. *Es sei K ein Körper und*

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & 0 \end{array}$$

ein homogenes lineares Gleichungssystem über K. Dann ist die Menge aller Lösungen des Gleichungssystems ein Untervektorraum des K^n (mit komponentenweiser Addition und Skalarmultiplikation).

Beweis. Siehe Aufgabe 19.3. □

Man spricht daher auch vom *Lösungsraum* des Gleichungssystems. Insbesondere ist die Summe von zwei Lösungen eines linearen Gleichungssystems wieder eine Lösung. Die Lösungsmenge eines inhomogenen Gleichungssystems ist kein Vektorraum. Man kann aber zu einer Lösung eines inhomogenen Gleichungssystems eine Lösung des zugehörigen homogenen Gleichungssystems hinzuaddieren und erhält wieder eine Lösung des inhomogenen Gleichungssystems.

19. Arbeitsblatt

Übungsaufgaben

Aufgabe 19.1. Es sei K ein Körper und es seien V und W Vektorräume über K. Zeige, dass auch das Produkt

$$V \times W$$

ein K-Vektorraum ist.

Aufgabe 19.2. Es sei K ein Körper und I eine Indexmenge. Zeige, dass

$$K^I = \text{Abb } (I, K)$$

mit stellenweiser Addition und skalarer Multiplikation ein K-Vektorraum ist.

Aufgabe 19.3. Es sei K ein Körper und

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & 0 \end{array}$$

ein lineares Gleichungssystem über K. Zeige, dass die Menge aller Lösungen des Gleichungssystems ein Untervektorraum des K^n ist. Wie verhält sich dieser Lösungsraum zu den Lösungsräumen der einzelnen Gleichungen?

Aufgabe 19.4. Man mache sich klar, dass sich die Addition und die skalare Multiplikation auf einen Untervektorraum einschränken lässt und dass dieser mit den von V geerbten Strukturen selbst ein Vektorraum ist.

Aufgabe 19.5. Es sei K ein Körper und V ein K-Vektorraum. Es seien $U, W \subseteq V$ Untervektorräume. Zeige, dass die Vereinigung $U \cup W$ nur dann ein Untervektorraum ist, wenn $U \subseteq W$ oder $W \subseteq U$ gilt.

Aufgaben zum Abgeben

Aufgabe 19.6. (3 Punkte)

Es sei K ein Körper und V ein K-Vektorraum. Zeige, dass die folgenden Eigenschaften gelten (dabei sei $\lambda \in K$ und $v \in V$).

(1) Es ist $0v = 0$.

(2) Es ist $\lambda 0 = 0$.
(3) Es ist $(-1)v = -v$.
(4) Aus $\lambda \neq 0$ und $v \neq 0$ folgt $\lambda v \neq 0$.

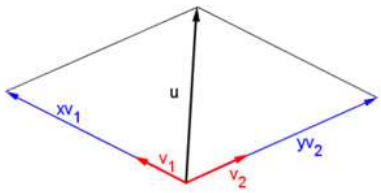
Aufgabe 19.7. (3 Punkte)

Man gebe ein Beispiel für einen Vektorraum V und von drei Teilmengen in V an, die jeweils zwei der Unterraumaxiome erfüllen, aber nicht das dritte.

20. Vorlesung - Basen

Die Lösungsmenge eines homogenen linearen Gleichungssystems in n Variablen über einem Körper K ist ein Untervektorraum des K^n. Häufig wird dieser Lösungsraum durch die Menge aller „Linearkombinationen“ von endlich vielen (besonders einfachen) Lösungen beschrieben. In dieser und der nächsten Vorlesung entwickeln wir die dazu notwendigen Begriffe.

Erzeugendensysteme



Die von zwei Vektoren v_1 und v_2 erzeugte Ebene besteht aus allen Linearkombinationen $u = xv_1 + yv_2$.

Definition 20.1. Es sei K ein Körper und V ein K-Vektorraum. Es sei $v_1, \ldots, v_n$ eine Familie von Vektoren in V. Dann heißt der Vektor

$$s_1v_1 + s_2v_2 + \cdots + s_nv_n \text{ mit } s_i \in K$$

eine *Linearkombination* dieser Vektoren (zum *Koeffiziententupel* $(s_1, \ldots, s_n)$).

Zwei unterschiedliche Koeffiziententupel können denselben Vektor definieren.

Definition 20.2. Es sei K ein Körper und V ein K-Vektorraum. Dann heißt eine Familie $v_i \in V$, $i \in I$, ein *Erzeugendensystem* von V, wenn man jeden

Vektor $v \in V$ darstellen kann als[2]

$$v = \sum_{j \in J} s_j v_j$$

mit einer endlichen Teilfamilie $J \subseteq I$ und mit $s_j \in K$.

Im K^n bilden die Standardvektoren e_i, $1 \leq i \leq n$, ein Erzeugendensystem. Im Polynomring $K[X]$ bilden die Potenzen X^n, $n \in \mathbb{N}$, ein (unendliches) Erzeugendensystem.

Definition 20.3. Es sei K ein Körper und V ein K-Vektorraum. Zu einer Familie v_i, $i \in I$, setzt man

$$\langle v_i,\, i \in I \rangle = \left\{ \sum_{i \in J} s_i v_i |\, s_i \in K,\, J \subseteq I \text{ endliche Teilmenge} \right\}$$

und nennt dies den von der Familie *erzeugten* oder *aufgespannten Untervektorraum.*

Der von der leeren Menge erzeugte Unterraum ist der Nullraum.[3] Dieser wird ebenso von der 0 erzeugt. Zu einem einzigen Vektor v besteht der aufgespannte Raum aus $Kv = \{sv |\, s \in K\}$. Bei $v \neq 0$ ist dies eine *Gerade*, was wir im Rahmen der Dimensionstheorie noch präzisieren werden. Bei zwei Vektoren v und w hängt die „Gestalt“ des aufgespannten Raumes davon ab, wie die beiden Vektoren sich zueinander verhalten. Wenn sie beide auf einer Geraden liegen, d.h. wenn gilt $w = sv$, so ist w überflüssig und der von den beiden Vektoren erzeugte Unterraum stimmt mit dem von v erzeugten Unterraum überein. Wenn dies nicht der Fall ist (und v und w nicht 0 sind), so erzeugen die beiden Vektoren eine „Ebene“.

Wir fassen einige einfache Eigenschaften für Erzeugendensysteme und Unterräume zusammen.

Lemma 20.4. *Es sei K ein Körper und V ein K-Vektorraum. Dann gelten folgende Aussagen.*

(1) *Sei U_j, $j \in J$, eine Familie von Untervektorräumen. Dann ist auch der Durchschnitt*[4]

$$U = \bigcap_{j \in J} U_j$$

ein Untervektorraum.

[2]Es bedeutet keinen Verständnisverlust, wenn man hier nur endliche Familien betrachtet. Das Summenzeichen über eine endliche Indexmenge bedeutet einfach, dass alle Elemente der Familie aufzusummieren sind.

[3]Dies kann man als Definition nehmen oder aber aus der Definition ableiten, wenn man die Konvention berücksichtigt, dass die leere Summe gleich 0 ist.

[4]Der Durchschnitt $\bigcap_{j \in J} T_j$ zu einer beliebigen Indexmenge J und einer durch J indizierten Familie T_j, $j \in J$, von Teilmengen einer festen Obermenge M besteht aus allem Elementen aus M, die in allen Mengen T_j enthalten sind.

(2) *Zu einer Familie v_i, $i \in I$, von Elementen in V ist der erzeugte Unterraum ein Unterraum*[5] *von V.*
(3) *Die Familie v_i, $i \in I$, ist genau dann ein Erzeugendensystem von V, wenn*

$$\langle v_i,\, i \in I \rangle = V$$

ist.

Beweis. Siehe Aufgabe 20.4. □

Lineare Unabhängigkeit

Definition 20.5. Es sei K ein Körper und V ein K-Vektorraum. Dann heißt eine Familie von Vektoren v_i, $i \in I$, (mit einer beliebigen endlichen Indexmenge I) *linear unabhängig*, wenn eine Gleichung

$$\sum_{i \in I} s_i v_i = 0 \text{ mit } s_i \in K$$

nur bei $s_i = 0$ für alle i möglich ist.

Wenn eine Familie nicht linear unabhängig ist, so nennt man sie *linear abhängig*. Man nennt übrigens eine Linearkombination $\sum_{i \in I} a_i v_i = 0$ eine *Darstellung des Nullvektors*. Sie heißt die *triviale Darstellung*, wenn alle Koeffizienten a_i null sind, andernfalls, wenn also mindestens ein Koeffizient nicht null ist, spricht man von einer *nichttrivialen Darstellung der Null*. Eine Familie von Vektoren ist genau dann linear unabhängig, wenn man mit ihnen nur auf die triviale Art den Nullvektor darstellen kann. Dies ist auch äquivalent dazu, dass man keinen Vektor aus der Familie als Linearkombination der anderen ausdrücken kann.

Lemma 20.6. *Sei K ein Körper, V ein K-Vektorraum und v_i, $i \in I$, eine Familie von Vektoren in V. Dann gelten folgende Aussagen.*

(1) *Wenn die Familie linear unabhängig ist, so ist auch zu jeder Teilmenge $J \subseteq I$ die Familie v_i , $i \in J$, linear unabhängig.*
(2) *Die leere Familie ist linear unabhängig.*
(3) *Wenn die Familie den Nullvektor enthält, so ist sie nicht linear unabhängig.*
(4) *Wenn in der Familie ein Vektor mehrfach vorkommt, so ist sie nicht linear unabhängig.*
(5) *Ein Vektor v ist genau dann linear unabhängig, wenn $v \neq 0$ ist.*
(6) *Zwei Vektoren v und u sind genau dann linear unabhängig, wenn weder u ein skalares Vielfaches von v ist noch umgekehrt.*

Beweis. Siehe Aufgabe 20.7. □

[5] In der Bezeichnung „erzeugter Unterraum“ wurde diese Eigenschaft schon vorweg genommen.

Beispiel 20.7. Die Standardvektoren im K^n sind linear unabhängig. Eine Darstellung

$$\sum_{i=1}^{n} s_i e_i \;=\; 0$$

bedeutet ja einfach

$$s_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + s_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + s_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} ,$$

woraus sich aus der i-ten Zeile direkt $s_i = 0$ ergibt.

Beispiel 20.8. Die drei Vektoren

$$\begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix} , \begin{pmatrix} 0 \\ 4 \\ 5 \end{pmatrix} \text{ und } \begin{pmatrix} 4 \\ 8 \\ 9 \end{pmatrix}$$

sind linear abhängig. Es ist nämlich

$$4 \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix} + 3 \begin{pmatrix} 0 \\ 4 \\ 5 \end{pmatrix} - 3 \begin{pmatrix} 4 \\ 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

eine nichttriviale Darstellung des Nullvektors.

Bemerkung 20.9. Die Vektoren $v_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} , \ldots , v_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \in K^m$ sind genau dann linear abhängig, wenn das homogene lineare Gleichungssystem

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & 0 \end{array}$$

eine nichttriviale (d.h. von 0 verschiedene) Lösung besitzt.

Basen

Definition 20.10. Es sei K ein Körper und V ein K-Vektorraum. Dann heißt ein linear unabhängiges Erzeugendensystem $v_i \in V$, $i \in I$, von V eine *Basis* von V.

Beispiel 20.11. Die Standardvektoren im K^n bilden eine Basis. Die lineare Unabhängigkeit wurde in Beispiel 20.7 gezeigt. Um zu zeigen, dass auch ein

Erzeugendensystem vorliegt, sei $v = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in K^n$ ein beliebiger Vektor. Dann ist aber direkt

$$v = \sum_{i=1}^{n} b_i e_i.$$

Also liegt eine Basis vor, die man die *Standardbasis* des K^n nennt.

Satz 20.12. *Es sei K ein Körper und V ein K-Vektorraum. Es sei $v_1, \ldots, v_n \in V$ eine Familie von Vektoren. Dann sind folgende Aussagen äquivalent.*

(1) *Die Familie ist eine Basis von V.*
(2) *Die Familie ist ein minimales Erzeugendensystem, d.h. sobald man einen Vektor v_i weglässt, liegt kein Erzeugendensystem mehr vor.*
(3) *Für jeden Vektor $u \in V$ gibt es genau eine Darstellung*

$$u = s_1 v_1 + \cdots + s_n v_n \, .$$

(4) *Die Familie ist maximal linear unabhängig, d.h. sobald man irgendeinen Vektor dazunimmt, ist die Familie nicht mehr linear unabhängig.*

Beweis. Wir führen einen Ringschluss durch. (1) $\Rightarrow$ (2). Die Familie ist ein Erzeugendensystem. Nehmen wir einen Vektor, sagen wir v_1, aus der Familie heraus. Wir müssen zeigen, dass dann die verbleibende Familie, also $v_2, \ldots, v_n$ kein Erzeugendensystem mehr ist. Wenn sie ein Erzeugendensystem wäre, so wäre insbesondere v_1 als Linearkombination der Vektoren darstellbar, d.h. man hätte

$$v_1 = \sum_{i=2}^{n} s_i v_i \, .$$

Dann ist aber

$$v_1 - \sum_{i=2}^{n} s_i v_i = 0$$

eine nichttriviale Darstellung der 0, im Widerspruch zur linearen Unabhängigkeit der Familie. (2) $\Rightarrow$ (3). Nach Voraussetzung ist die Familie ein Erzeugendensystem, so dass sich jeder Vektor als Linearkombination darstellen lässt. Angenommen, es gibt für ein $u \in V$ eine mehrfache Darstellung, d.h.

$$u = \sum_{i=1}^{n} s_i v_i = \sum_{i=1}^{n} t_i v_i,$$

wobei mindestens ein Koeffizient verschieden sei. Ohne Einschränkung sei $s_1 \neq t_1$. Dann erhält man die Beziehung

$$(s_1 - t_1) v_1 = \sum_{i=2}^{n} (t_i - s_i) v_i \, .$$

Wegen $s_1 - t_1 \neq 0$ kann man durch diese Zahl dividieren und erhält eine Darstellung von v_1 durch die anderen Vektoren. Nach Aufgabe 20.3 ist auch die Familie ohne v_1 ein Erzeugendensystem von V, im Widerspruch zur Minimalität. (3) $\Rightarrow$ (4). Wegen der eindeutigen Darstellbarkeit besitzt insbesondere der Nullvektor nur die triviale Darstellung, d.h. die Vektoren sind linear unabhängig. Nimmt man einen Vektor u hinzu, so besitzt dieser eine Darstellung

$$u = \sum_{i=1}^{n} s_i v_i$$

und daher ist

$$0 = u - \sum_{i=1}^{n} s_i v_i$$

eine nichttriviale Darstellung der 0, so dass die verlängerte Familie $u, v_1, \ldots, v_n$ nicht linear unabhängig ist. (4) $\Rightarrow$ (1). Die Familie ist linear unabhängig, wir müssen zeigen, dass sie auch ein Erzeugendensystem bildet. Sei dazu $u \in V$. Nach Voraussetzung ist die Familie $u, v_1, \ldots, v_n$ nicht linear unabhängig, d.h. es gibt eine nichttriviale Darstellung

$$0 = su + \sum_{i=1}^{n} s_i v_i \, .$$

Dabei ist $s \neq 0$, da andernfalls dies eine nichttriviale Darstellung der 0 allein mit den linear unabhängigen Vektoren $v_1, \ldots, v_n$ wäre. Daher können wir

$$u = -\sum_{i=1}^{n} \frac{s_i}{s} v_i$$

schreiben, so dass eine Darstellung von u möglich ist. □

Bemerkung 20.13. Es sei eine Basis $v_1, \ldots, v_n$ eines K-Vektorraums V gegeben. Aufgrund von Satz 20.12 bedeutet dies, dass es für jeden Vektor $u \in V$ eine eindeutig bestimmte Darstellung (eine Linearkombination)

$$u = s_1 v_1 + s_2 v_2 + \cdots + s_n v_n$$

gibt. Die dabei eindeutig bestimmten Elemente $s_i \in K$ (Skalare) heißen die *Koordinaten* von u bezüglich der gegebenen Basis. Bei einer gegebenen Basis entsprechen sich also die Vektoren und die Koordinatentupel $(s_1, s_2, \ldots, s_n) \in K^n$. Man sagt, dass eine Basis ein *lineares Koordinatensystem* festlegt.[6]

[6]Lineare Koordinaten vermitteln also eine bijektive Beziehung zwischen Punkten und Zahlentupeln. Aufgrund der Linearität ist eine solche Bijektion mit der Addition und der Skalarmultiplikation verträglich. In vielen anderen Kontexten spielen auch nichtlineare (oder krummlinige) Koordinaten eine wichtige Rolle. Auch diese setzen Raumpunkte mit Zahlentupel in eine bijektive Verbindung. Wichtige nichtlineare Koordinaten sind u.A. Polarkoordinaten, Zylinderkoordinaten und Kugelkoordinaten. Mathematische Probleme können häufig durch eine geeignete Wahl von Koordinaten vereinfacht werden, beispielsweise bei Volumenberechnungen.

Satz 20.14. *Es sei K ein Körper und V ein K-Vektorraum mit einem endlichen Erzeugendensystem. Dann besitzt V eine endliche Basis.*

Beweis. Es sei v_i, $i \in I$, ein Erzeugendensystem von V mit einer endlichen Indexmenge I. Wir wollen mit der Charakterisierung aus Satz 20.12 (2) argumentieren. Falls die Familie schon minimal ist, so liegt eine Basis vor. Andernfalls gibt es ein $k \in I$ derart, dass die um v_k reduzierte Familie, also v_i, $i \in I \setminus \{k\}$, ebenfalls ein Erzeugendensystem ist. In diesem Fall kann man mit der kleineren Indexmenge weiterargumentieren. Mit diesem Verfahren gelangt man letztlich zu einer Teilmenge $J \subseteq I$ derart, dass v_i, $i \in J$, ein minimales Erzeugendensystem, also eine Basis ist. □

20. Arbeitsblatt

Übungsaufgaben

Aufgabe 20.1. Drücke in $\mathbb{Q}^2$ den Vektor

$$(2, -7)$$

als Linearkombination der Vektoren

$$(5, -3) \text{ und } (-11, 4)$$

aus.

Aufgabe 20.2. Drücke in $\mathbb{C}^2$ den Vektor

$$(1, 0)$$

als Linearkombination der Vektoren

$$(3 + 5i, -3 + 2i) \text{ und } (1 - 6i, 4 - i)$$

aus.

Aufgabe 20.3. Es sei K ein Körper und V ein K-Vektorraum. Es sei v_i, $i \in I$, eine Familie von Vektoren in V und $w \in V$ ein weiterer Vektor. Es sei vorausgesetzt, dass die Familie

$$w, v_i, i \in I\,,$$

ein Erzeugendensystem von V ist und dass sich w als Linearkombination der v_i, $i \in I$, darstellen lässt. Zeige, dass dann schon v_i, $i \in I$, ein Erzeugendensystem von V ist.

Aufgabe 20.4. Es sei K ein Körper und V ein K-Vektorraum. Beweise folgende Aussagen.

(1) Sei U_j, $j \in J$, eine Familie von Untervektorräumen von V. Dann ist auch der Durchschnitt
$$U = \bigcap_{j \in J} U_j$$
ein Untervektorraum.
(2) Zu einer Familie v_i, $i \in I$, von Elementen in V ist der erzeugte Unterraum ein Unterraum.
(3) Die Familie v_i, $i \in I$, ist genau dann ein Erzeugendensystem von V, wenn
$$\langle v_i,\, i \in I \rangle = V$$
ist.

Aufgabe 20.5. Zeige, dass die drei Vektoren
$$\begin{pmatrix} 0 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 7 \\ 0 \\ -1 \end{pmatrix}$$
im $\mathbb{R}^4$ linear unabhängig sind.

Aufgabe 20.6. Man gebe im $\mathbb{R}^3$ drei Vektoren an, so dass je zwei von ihnen linear unabhängig sind, aber alle drei zusammen linear abhängig.

Aufgabe 20.7. Sei K ein Körper, V ein K-Vektorraum und v_i, $i \in I$, eine Familie von Vektoren in V. Beweise die folgenden Aussagen.

(1) Wenn die Familie linear unabhängig ist, so ist auch zu jeder Teilmenge $J \subseteq I$ die Familie v_i , $i \in J$, linear unabhängig.
(2) Die leere Familie ist linear unabhängig.
(3) Wenn die Familie den Nullvektor enthält, so ist sie nicht linear unabhängig.
(4) Wenn in der Familie ein Vektor mehrfach vorkommt, so ist sie nicht linear unabhängig.
(5) Ein Vektor v ist genau dann linear unabhängig, wenn $v \neq 0$ ist.
(6) Zwei Vektoren v und u sind genau dann linear unabhängig, wenn weder u ein skalares Vielfaches von v ist noch umgekehrt.

Aufgabe 20.8. Es sei K ein Körper, V ein K-Vektorraum und sei v_i, $i \in I$, eine Familie von Vektoren in V. Es sei λ_i, $i \in I$, eine Familie von Elementen $\neq 0$ aus K. Zeige, dass die Familie v_i, $i \in I$, genau dann linear unabhängig (ein Erzeugendensystem von V, eine Basis von V) ist, wenn dies für die Familie $\lambda_i v_i$, $i \in I$, gilt.

Aufgabe 20.9. Bestimme eine Basis für den Lösungsraum der linearen Gleichung

$$3x + 4y - 2z + 5w = 0\,.$$

Aufgabe 20.10. Bestimme eine Basis für den Lösungsraum des linearen Gleichungssystems

$$-2x + 3y - z + 4w = 0 \text{ und } 3z - 2w = 0\,.$$

Aufgabe 20.11. Zeige, dass im $\mathbb{R}^3$ die drei Vektoren

$$\begin{pmatrix} 2 \\ 1 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 7 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$$

eine Basis bilden.

Aufgabe 20.12. Bestimme, ob im $\mathbb{C}^2$ die zwei Vektoren

$$\begin{pmatrix} 2+7i \\ 3-i \end{pmatrix} \text{ und } \begin{pmatrix} 15+26i \\ 13-7i \end{pmatrix}$$

eine Basis bilden.

Aufgabe 20.13. Es sei K ein Körper. Man finde ein lineares Gleichungssystem in drei Variablen, dessen Lösungsraum genau

$$\left\{ \lambda \begin{pmatrix} 3 \\ 2 \\ -5 \end{pmatrix} \mid \lambda \in K \right\}$$

ist.

Aufgaben zum Abgeben

Aufgabe 20.14. (3 Punkte)

Drücke in $\mathbb{Q}^3$ den Vektor

$$(2, 5, -3)$$

als Linearkombination der Vektoren

$$(1, 2, 3), (0, 1, 1) \text{ und } (-1, 2, 4)$$

aus. Zeige, dass man ihn nicht als Linearkombination von zweien der drei Vektoren ausdrücken kann.

Aufgabe 20.15. (2 Punkte)

Bestimme, ob im $\mathbb{R}^3$ die drei Vektoren

$$\begin{pmatrix} 2 \\ 3 \\ -5 \end{pmatrix}, \begin{pmatrix} 9 \\ 2 \\ 6 \end{pmatrix}, \begin{pmatrix} -1 \\ 4 \\ -1 \end{pmatrix}$$

eine Basis bilden.

Aufgabe 20.16. (2 Punkte)

Bestimme, ob im $\mathbb{C}^2$ die zwei Vektoren

$$\begin{pmatrix} 2-7i \\ -3+2i \end{pmatrix} \text{ und } \begin{pmatrix} 5+6i \\ 3-17i \end{pmatrix}$$

eine Basis bilden.

Aufgabe 20.17. (4 Punkte)

Es sei $\mathbb{Q}^n$ der n-dimensionale Standardraum über $\mathbb{Q}$ und sei $v_1, \ldots, v_n \in \mathbb{Q}^n$ eine Familie von Vektoren. Zeige, dass diese Familie genau dann eine $\mathbb{Q}$-Basis des $\mathbb{Q}^n$ ist, wenn diese Familie aufgefasst im $\mathbb{R}^n$ eine $\mathbb{R}$-Basis des $\mathbb{R}^n$ bildet.

Aufgabe 20.18. (3 Punkte)

Es sei K ein Körper und sei

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

ein von 0 verschiedener Vektor. Man finde ein lineares Gleichungssystem in n Variablen mit $n-1$ Gleichungen, dessen Lösungsraum genau

$$\left\{ \lambda \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid \lambda \in K \right\}$$

ist.

21. Vorlesung - Dimension

Dimensionstheorie

Ein endlich erzeugter Vektorraum hat im Allgemeinen ganz unterschiedliche Basen. Allerdings ist die Anzahl der Elemente in einer Basis stets konstant und hängt nur vom Vektorraum ab. Diese wichtige Eigenschaft werden wir jetzt beweisen und als Ausgangspunkt für die Definition der Dimension eines Vektorraums nehmen.

Lemma 21.1. *Es sei K ein Körper und V ein K-Vektorraum mit einer Basis $v_1, \ldots, v_n$. Es sei $w \in V$ ein Vektor mit einer Darstellung*

$$w = \sum_{i=1}^{n} s_i v_i \, ,$$

wobei $s_k \neq 0$ sei für ein bestimmtes k. Dann ist auch die Familie

$$v_1, \ldots, v_{k-1}, w, v_{k+1}, \ldots, v_n$$

eine Basis von V.

Beweis. Wir zeigen zuerst, dass die neue Familie ein Erzeugendensystem ist. Zunächst kann man wegen

$$w = \sum_{i=1}^{n} s_i v_i$$

und $s_k \neq 0$ den Vektor v_k als

$$v_k = \frac{1}{s_k} w - \sum_{i=1}^{k-1} \frac{s_i}{s_k} v_i - \sum_{i=k+1}^{n} \frac{s_i}{s_k} v_i$$

schreiben. Sei nun $u \in V$ beliebig vorgegeben. Dann kann man schreiben

$$\begin{aligned} u &= \sum_{i=1}^{n} t_i v_i \\ &= \sum_{i=1}^{k-1} t_i v_i + t_k v_k + \sum_{i=k+1}^{n} t_i v_i \\ &= \sum_{i=1}^{k-1} t_i v_i + t_k \left(\frac{1}{s_k} w - \sum_{i=1}^{k-1} \frac{s_i}{s_k} v_i - \sum_{i=k+1}^{n} \frac{s_i}{s_k} v_i \right) + \sum_{i=k+1}^{n} t_i v_i \\ &= \sum_{i=1}^{k-1} \left(t_i - t_k \frac{s_i}{s_k} \right) v_i + \frac{t_k}{s_k} w + \sum_{i=k+1}^{n} \left(t_i - t_k \frac{s_i}{s_k} \right) v_i . \end{aligned}$$

Zum Nachweis der linearen Unabhängigkeit nehmen wir zwecks Notationsvereinfachung $k = 1$ an. Es sei

$$t_1 w + \sum_{i=2}^{n} t_i v_i = 0$$

eine Darstellung der Null. Dann ist

$$\begin{aligned} 0 &= t_1 w + \sum_{i=2}^{n} t_i v_i \\ &= t_1 \left(\sum_{i=1}^{n} s_i v_i \right) + \sum_{i=2}^{n} t_i v_i \\ &= t_1 s_1 v_1 + \sum_{i=2}^{n} (t_1 s_i + t_i) v_i. \end{aligned}$$

Aus der linearen Unabhängigkeit der Ausgangsfamilie folgt insbesondere $t_1 s_1 = 0$, und wegen $s_1 \neq 0$ ergibt sich $t_1 = 0$. Deshalb ist $\sum_{i=2}^{n} t_i v_i = 0$ und daher gilt $t_i = 0$ für alle i. □

Die vorstehende Aussage heißt *Austauschlemma*, die nachfolgende *Austauschsatz*.

Satz 21.2. *Es sei K ein Körper und V ein K-Vektorraum mit einer Basis*

$$b_1, \ldots, b_n \,.$$

Ferner sei

$$u_1, \ldots, u_k$$

eine Familie von linear unabhängigen Vektoren in V. Dann gibt es eine Teilmenge $J = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, \ldots, n\} = I$ derart, dass die Familie

$$u_1, \ldots, u_k, b_i, i \in I \setminus J \,,$$

eine Basis von V ist. Insbesondere ist $k \leq n$.

Beweis. Wir führen Induktion über k, also über die Anzahl der Vektoren in der Familie. Bei $k = 0$ ist nichts zu zeigen. Sei die Aussage für k schon bewiesen und seien $k + 1$ linear unabhängige Vektoren

$$u_1, \ldots, u_k, u_{k+1}$$

gegeben. Nach Induktionsvoraussetzung, angewandt auf die (ebenfalls linear unabhängigen) Vektoren

$$u_1, \ldots, u_k$$

gibt es eine Teilmenge $J = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ derart, dass die Familie

$$u_1, \ldots, u_k, b_i, i \in I \setminus J \,,$$

eine Basis von V ist. Wir wollen auf diese Basis Lemma 21.1 anwenden. Da eine Basis vorliegt, kann man

$$u_{k+1} = \sum_{j=1}^{k} c_j u_j + \sum_{i \in I \setminus J} d_i b_i$$

schreiben. Wären hierbei alle Koeffizienten $d_i = 0$, so ergäbe sich sofort ein Widerspruch zur linearen Unabhängigkeit der u_j, $j = 1, \ldots, k+1$. Es gibt also ein $i \in I \setminus J$ mit $d_i \neq 0$. Wir setzen $i_{k+1} := i$. Damit ist $J' = \{i_1, i_2, \ldots, i_k, i_{k+1}\}$ eine $(k+1)$-elementige Teilmenge von $\{1, \ldots, n\}$. Nach dem Austauschlemma kann man den Basisvektor $b_{i_{k+1}}$ durch u_{k+1} ersetzen und erhält die neue Basis

$$u_1, \ldots, u_k, u_{k+1}, b_i, i \in I \setminus J' .$$

Der Zusatz folgt sofort, da eine k-elementige Teilmenge einer n-elementigen Menge vorliegt. □

Satz 21.3. *Es sei K ein Körper und V ein K-Vektorraum mit einem endlichen Erzeugendensystem. Dann besitzen je zwei Basen von V die gleiche Anzahl von Basisvektoren.*

Beweis. Es seien $\mathfrak{b} = b_1, \ldots, b_n$ und $\mathfrak{u} = u_1, \ldots, u_k$ zwei Basen von V. Aufgrund des Basisaustauschsatzes, angewandt auf die Basis $\mathfrak{b}$ und die linear unabhängige Familie $\mathfrak{u}$ ergibt sich $k \leq n$. Wendet man den Austauschsatz umgekehrt an, so folgt $n \leq k$, also insgesamt $n = k$. □

Dieser Satz erlaubt die folgende Definition.

Definition 21.4. Es sei K ein Körper und V ein K-Vektorraum mit einem endlichen Erzeugendensystem. Dann nennt man die Anzahl der Vektoren in einer Basis von V die *Dimension* von V, geschrieben

$$\dim(V) .$$

Wenn ein Vektorraum nicht endlich erzeugt ist, so setzt man $\dim(V) = \infty$. Der Nullraum 0 hat die Dimension 0. Einen eindimensionalen Vektorraum nennt man auch eine *Gerade*, einen zweidimensionalen Vektorraum eine *Ebene*, einen dreidimensionalen Vektorraum einen *Raum* (im engeren Sinn), wobei man andererseits auch jeden Vektorraum einen Raum nennt.

Korollar 21.5. *Es sei K ein Körper und $n \in \mathbb{N}$. Dann besitzt der Standardraum K^n die Dimension n.*

Beweis. Die Standardbasis e_i, $i = 1, \ldots, n$, besteht aus n Vektoren, also ist die Dimension n. □

Beispiel 21.6. Die komplexen Zahlen bilden einen zweidimensionalen reellen Vektorraum, eine Basis ist z.B. 1 und i.

Beispiel 21.7. Der Polynomring $R = K[X]$ über einem Körper K ist kein endlichdimensionaler Vektorraum. Seien n Polynome $P_1, \ldots, P_n$ fixiert. Es sei d das Maximum der Grade dieser Polynome. Dann hat auch jede K-Linearkombination $\sum_{i=1}^{n} a_i P_i$ maximal den Grad d. Insbesondere können Polynome von einem größeren Grad nicht durch $P_1, \ldots, P_n$ dargestellt werden. Es gibt also kein endliches Erzeugendensystem.

Korollar 21.8. *Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Es sei $U \subseteq V$ ein Unterraum. Dann ist U ebenfalls endlichdimensional und es gilt*

$$\dim(U) \leq \dim(V) \ .$$

Beweis. Jede linear unabhängige Familie in U ist auch linear unabhängig in V. Daher kann es aufgrund des Basisaustauschsatzes in U nur linear unabhängige Familien der Länge $\leq n$ geben. Es sei $k \leq n$ derart, dass es in U eine linear unabhängige Familie mit k Vektoren gibt, aber nicht mit $k+1$ Vektoren. Sei $\mathfrak{u} = u_1, \ldots, u_k$ eine solche Familie. Diese ist dann insbesondere eine maximal linear unabhängige Familie in U und daher wegen Satz 20.12 eine Basis von U. □

Korollar 21.9. *Es sei K ein Körper und V ein K-Vektorraum mit endlicher Dimension $n = \dim(V)$. Es seien n Vektoren $v_1, \ldots, v_n$ in V gegeben. Dann sind folgende Eigenschaften äquivalent.*

(1) *$v_1, \ldots, v_n$ bilden eine Basis von V.*
(2) *$v_1, \ldots, v_n$ bilden ein Erzeugendensystem von V.*
(3) *$v_1, \ldots, v_n$ sind linear unabhängig.*

Beweis. Siehe Aufgabe 21.1. □

Beispiel 21.10. Es sei K ein Körper. Man kann sich einfach einen Überblick über die Unterräume des K^n verschaffen, als Dimension von Unterräumen kommt nur k mit $0 \leq k \leq n$ in Frage. Bei $n = 0$ gibt es nur den Nullraum selbst, bei $n = 1$ gibt es den Nullraum und K selbst. Bei $n = 2$ gibt es den Nullraum, die gesamte Ebene K^2, und die eindimensionalen Geraden durch den Nullpunkt. Jede solche Gerade G hat die Gestalt

$$G = Kv = \{sv | \, s \in K\}$$

mit einem von 0 verschiedenen Vektor v. Zwei von null verschiedene Vektoren definieren genau dann die gleiche Gerade, wenn sie linear abhängig sind.

Bei $n = 3$ gibt es den Nullraum, den Gesamtraum K^3, die eindimensionalen Geraden durch den Nullpunkt und die zweidimensionalen Ebenen durch den Nullpunkt.

Der folgende Satz heißt *Basisergänzungssatz*.

Satz 21.11. *Es sei K ein Körper und V ein endlichdimensionaler K-Vektorraum der Dimension $n = \dim(V)$. Es seien*

$$u_1, \ldots, u_k$$

linear unabhängige Vektoren in V Dann gibt es Vektoren

$$u_{k+1}, \ldots, u_n$$

derart, dass

$$u_1, \ldots, u_k, u_{k+1}, \ldots, u_n$$

eine Basis von V bilden.

Beweis. Es sei $b_1, \ldots, b_n$ eine Basis von V. Aufgrund des Austauschsatzes findet man $n-k$ Vektoren aus der Basis $\mathfrak{b}$, die zusammen mit den vorgegebenen $u_1, \ldots, u_k$ eine Basis von V bilden. □

21. Arbeitsblatt

Übungsaufgaben

Aufgabe 21.1. Es sei K ein Körper und V ein K-Vektorraum mit endlicher Dimension $n = \dim(V)$. Es seien n Vektoren $v_1, \ldots, v_n$ in V gegeben. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) $v_1, \ldots, v_n$ bilden eine Basis von V.
(2) $v_1, \ldots, v_n$ bilden ein Erzeugendensystem von V.
(3) $v_1, \ldots, v_n$ sind linear unabhängig.

Aufgabe 21.2. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $d \in \mathbb{N}$. Zeige, dass die Menge aller Polynome vom Grad $\leq d$ ein endlichdimensionaler Untervektorraum von $K[X]$ ist. Was ist seine Dimension?

Aufgabe 21.3. Zeige, dass die Menge aller reellen Polynome vom Grad ≤ 4, für die -2 und 3 Nullstellen sind, ein endlichdimensionaler Untervektorraum in $\mathbb{R}[X]$ ist. Bestimme die Dimension von diesem Vektorraum.

Aufgabe 21.4.*

Es sei K ein Körper und es seien V und W endlichdimensionale K-Vektorräume mit $\dim(V) = n$ und $\dim(W) = m$. Welche Dimension besitzt der Produktraum $V \times W$?

Aufgabe 21.5. Es sei V ein endlichdimensionaler Vektorraum über den komplexen Zahlen, und sei $v_1, \ldots, v_n$ eine Basis von V. Zeige, dass die Vektorenfamilie

$$v_1, \ldots, v_n \text{ und } iv_1, \ldots, iv_n$$

eine Basis von V, aufgefasst als reeller Vektorraum, ist.

Aufgabe 21.6. Es sei die Standardbasis e_1, e_2, e_3, e_4 im $\mathbb{R}^4$ gegeben und die drei Vektoren

$$\begin{pmatrix} 1 \\ 3 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 5 \\ 7 \end{pmatrix} \text{ und } \begin{pmatrix} -4 \\ 9 \\ -5 \\ 1 \end{pmatrix}.$$

Zeige, dass diese Vektoren linear unabhängig sind und ergänze sie mit einem geeigneten Standardvektor gemäß Lemma 21.1 zu einer Basis. Kann man jeden Standardvektor nehmen?

Aufgabe 21.7. Bestimme die Übergangsmatrizen $M_{\mathfrak{v}}^{\mathfrak{u}}$ und $M_{\mathfrak{u}}^{\mathfrak{v}}$ für die Standardbasis $\mathfrak{u}$ und die durch die Vektoren

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ und } v_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

gegebene Basis $\mathfrak{v}$ im $\mathbb{R}^4$.

Aufgabe 21.8. Bestimme die Übergangsmatrizen $M_{\mathfrak{v}}^{\mathfrak{u}}$ und $M_{\mathfrak{u}}^{\mathfrak{v}}$ für die Standardbasis $\mathfrak{u}$ und die durch die Vektoren

$$v_1 = \begin{pmatrix} 3+5i \\ 1-i \end{pmatrix} \text{ und } v_2 = \begin{pmatrix} 2+3i \\ 4+i \end{pmatrix},$$

gegebene Basis $\mathfrak{v}$ im $\mathbb{C}^2$.

Aufgabe 21.9. Wir betrachten die Vektorenfamilien

$$\mathfrak{v} = \begin{pmatrix} 7 \\ -4 \end{pmatrix}, \begin{pmatrix} 8 \\ 1 \end{pmatrix} \text{ und } \mathfrak{u} = \begin{pmatrix} 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 3 \end{pmatrix}$$

im $\mathbb{R}^2$.

a) Zeige, dass sowohl $\mathfrak{v}$ als auch $\mathfrak{u}$ eine Basis des $\mathbb{R}^2$ ist.

b) Es sei $P \in \mathbb{R}^2$ derjenige Punkt, der bezüglich der Basis $\mathfrak{v}$ die Koordinaten $(-2, 5)$ besitze. Welche Koordinaten besitzt der Punkt bezüglich der Basis $\mathfrak{u}$?

c) Bestimme die Übergangsmatrix, die den Basiswechsel von $\mathfrak{v}$ nach $\mathfrak{u}$ beschreibt.

Aufgaben zum Abgeben

Aufgabe 21.10. (4 Punkte)

Zeige, dass die Menge aller reellen Polynome vom Grad ≤ 6, für die -1, 0 und 1 Nullstellen sind, ein endlichdimensionaler Untervektorraum in $\mathbb{R}[X]$ ist. Bestimme die Dimension von diesem Vektorraum.

Aufgabe 21.11. (3 Punkte)

Es sei K ein Körper und V ein K-Vektorraum. Es sei $v_1, \ldots, v_m$ eine Familie von Vektoren in V und sei

$$U = \langle v_i,\, i = 1, \ldots, m \rangle$$

der davon aufgespannte Untervektorraum. Zeige, dass die Familie genau dann linear unabhängig ist, wenn die Dimension von U gleich m ist.

Aufgabe 21.12. (4 Punkte)

Bestimme die Übergangsmatrizen $M_{\mathfrak{v}}^{\mathfrak{u}}$ und $M_{\mathfrak{u}}^{\mathfrak{v}}$ für die Standardbasis $\mathfrak{u}$ und die durch die Vektoren

$$v_1 = \begin{pmatrix} 4 \\ 5 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 3 \\ -8 \end{pmatrix} \text{ und } v_3 = \begin{pmatrix} 5 \\ 7 \\ -3 \end{pmatrix}$$

gegebene Basis $\mathfrak{v}$ im $\mathbb{R}^3$.

Aufgabe 21.13. (6 Punkte)

Wir betrachten die Vektorenfamilien

$$\mathfrak{v} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 5 \end{pmatrix} \text{ und } \mathfrak{u} = \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 6 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \\ -2 \end{pmatrix}$$

im $\mathbb{R}^3$.

a) Zeige, dass sowohl $\mathfrak{v}$ als auch $\mathfrak{u}$ eine Basis des $\mathbb{R}^3$ ist.

b) Es sei $P \in \mathbb{R}^3$ derjenige Punkt, der bezüglich der Basis $\mathfrak{v}$ die Koordinaten $(2, 5, 4)$ besitze. Welche Koordinaten besitzt der Punkt bezüglich der Basis $\mathfrak{u}$?

c) Bestimme die Übergangsmatrix, die den Basiswechsel von $\mathfrak{v}$ nach $\mathfrak{u}$ beschreibt.

22. Vorlesung - Körpererweiterungen

In den verbleibenden Vorlesungen werden wir uns mit Körpererweiterungen $K \subseteq L$ beschäftigen. Wir betrachten beispielsweise in $\mathbb{R}$ den von $\mathbb{Q}$ und $\sqrt{7}$ erzeugten Unterring

$$L = \mathbb{Q}[\sqrt{7}].$$

Er besteht aus allen reellen Zahlen der Form

$$a + b\sqrt{7}$$

mit $a, b \in \mathbb{Q}$. Dabei kann man direkt nachprüfen, dass die Summe und das Produkt von zwei solchen Ausdrücken wieder von dieser Form ist, und somit liegt ein Unterring vor. Es handelt sich aber sogar um einen Körper. Es ist nämlich

$$\left(a + b\sqrt{7}\right)\left(a - b\sqrt{7}\right) = a^2 - 7b^2$$

und somit ist für $a + b\sqrt{7} \neq 0$

$$\left(a + b\sqrt{7}\right)\left(\frac{a}{a^2 - 7b^2} - \frac{b\sqrt{7}}{a^2 - 7b^2}\right) = 1,$$

also ist jedes von 0 verschiedene Element eine Einheit. Da $\sqrt{7}$ irrational ist, ist $a^2 - 7b^2 \neq 0$. Es liegt also eine Körpererweiterung

$$\mathbb{Q} = \mathbb{Q}[\sqrt{7}]$$

vor. Den Körper $\mathbb{Q}[\sqrt{7}]$ kann man auch einfach als Restklassenkörper von $\mathbb{Q}[X]$ beschreiben. Der Einsetzungshomomorphismus

$$\mathbb{Q}[X] \longrightarrow \mathbb{R},\ X \longmapsto \sqrt{7},$$

liefert eine surjektiven Ringhomomorphismus auf das Bild, also

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt{7}],\ X \longmapsto \sqrt{7}.$$

Unter dieser Abbildung geht $X^2 - 7$ auf 0, und in der Tat ist der Kern gleich dem Hauptideal $(X^2 - 7)$. Nach dem Isomorphiesatz gilt daher

$$\mathbb{Q}[X]/(X^2 - 7) \cong \mathbb{Q}[\sqrt{7}].$$

Rechnen in $K[X]/(P)$

Körper werden häufig ausgehend von einem schon bekannten Körper als Restklassenkörper des Polynomrings konstruiert. Die Arithmetik in einem solchen Erweiterungskörper wird in der folgenden Aussage beschrieben.

Proposition 22.1. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad n und $R = K[X]/(P)$ der zugehörige Restklassenring. Dann gelten folgende Rechenregeln (wir bezeichnen die Restklasse von X in R mit x).*

(1) *Man kann stets P als normiert annehmen (also $a_n = 1$; das werden wir im Folgenden tun).*
(2) *In R ist*
$$x^n = -\sum_{i=0}^{n-1} a_i x^i .$$
(3) *Höhere Potenzen x^k, $k \geq n$, kann man mit den Potenzen x^i, $i \leq n-1$, ausdrücken, indem man mittels Vielfachen von (2) sukzessive den Grad um eins reduziert.*
(4) *Die Potenzen $x^0 = 1$, $x^1, \ldots, x^{n-1}$ bilden eine K-Basis von R.*
(5) *R ist ein K-Vektorraum der Dimension n.*
(6) *In R werden zwei Elemente $P = \sum_{i=0}^{n-1} b_i x^i$ und $Q = \sum_{i=0}^{n-1} c_i x^i$ komponentenweise addiert, und multipliziert, indem sie als Polynome multipliziert werden und dann die Restklasse berechnet wird.*

Beweis. (1) Es ist $(P) = \left(\frac{P}{a_n}\right)$, da es bei einem Hauptideal nicht auf eine Einheit ankommt.
(2) Dies folgt direkt durch Umstellung der definierenden Gleichung.
(3) Dies folgt durch Multiplikation der Gleichung in (2) mit Potenzen von x.
(4) Dass die Potenzen x^i, $i = 0, \ldots, n-1$, ein Erzeugendensystem bildet, folgt aus Teil (2) und (3). Zum Beweis der linearen Unabhängigkeit sei angenommen, es gebe eine lineare Abhängigkeit, sagen wir $\sum_{i=0}^{n-1} c_i x^i = 0$. D.h., dass das Polynom $Q = \sum_{i=0}^{n-1} c_i X^i$ unter der Restklassenabbildung auf 0 geht, also zum Kern gehört. Dann muss es aber ein Vielfaches von P sein, was aber aus Gradgründen erzwingt, dass Q das Nullpolynom sein muss. Also sind alle $c_i = 0$.
(5) Dies folgt direkt aus (4).
(6) Dies ist klar.

□

Beispiel 22.2. Wir betrachten den Restklassenring
$$L = \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$
und bezeichnen die Restklasse von X mit x. Aufgrund von Proposition 22.1 besitzt jedes Element f aus L eine eindeutige Darstellung $f = ax^2 + bx + c$ mit $a, b, c \in \mathbb{Q}$, so dass also ein dreidimensionaler $\mathbb{Q}$-Vektorraum vorliegt. Da $X^3 + 2X^2 - 5$ in L zu 0 gemacht wird, gilt
$$x^3 = -2x^2 + 5.$$
Daraus ergeben sich die Gleichungen
$$x^4 = -2x^3 + 5x = -2(-2x^2 + 5) + 5x = 4x^2 + 5x - 10,$$

$$x^5 = -2x^4 + 5x^2 = -2(4x^2 + 5x - 10) + 5x^2 = -3x^2 - 10x + 20,$$

etc. Man kann hierbei auf verschiedene Arten zu dem eindeutig bestimmten kanonischen Repräsentanten reduzieren.

Berechnen wir nun das Produkt

$$(3x^2 - 2x + 4)(2x^2 + x - 1)\,.$$

Dabei wird distributiv ausmultipliziert und anschließend werden die Potenzen reduziert. Es ist

$$\begin{aligned} & (3x^2 - 2x + 4)(2x^2 + x - 1) \\ = \;& 6x^4 + 3x^3 - 3x^2 - 4x^3 - 2x^2 + 2x + 8x^2 + 4x - 4 \\ = \;& 6x^4 - x^3 + 3x^2 + 6x - 4 \\ = \;& 6(4x^2 + 5x - 10) + 2x^2 - 5 + 3x^2 + 6x - 4 = 29x^2 + 36x - 69. \end{aligned}$$

Endliche Körpererweiterungen

Wenn P in der vorstehenden Proposition irreduzibel ist, so ist $K[X]/(P)$ nach Satz 15.1 ein Körper und damit liegt eine Körpererweiterung

$$K \subseteq K[X]/P = L$$

vor. Bei einer K-Algebra (siehe unten) und insbesondere einer Körpererweiterung hat man durch den Vektorraumbegriff sofort die folgenden Begriffe zur Verfügung.

Definition 22.3. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.

Definition 22.4. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Bei $L = K[X]/(P)$ mit einem irreduziblen Polynom P ist nach Proposition 22.1 (5) der Grad der Körpererweiterung gleich dem Grad von P.

Algebren

Definition 22.5. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Häufig ist der Ringhomomorphismus, der zum Begriff der Algebra gehört, vom Kontext her klar und wird nicht explizit aufgeführt. Z.B. ist der Polynomring $R[X]$ eine R-Algebra, indem man die Elemente aus R als konstante Polynome auffasst, oder jeder Ring ist auf eine eindeutige Weise eine $\mathbb{Z}$-Algebra über den kanonischen Ringhomomorphismus $\mathbb{Z} \to R$, $n \mapsto n_R$.

Wir werden den Begriff der Algebra vor allem in dem Fall verwenden, wo der Grundring R ein Körper K ist. Eine K-Algebra A kann man stets in

natürlicher Weise als Vektorraum über dem Körper K auffassen. Die Skalarmultiplikation wird dabei einfach über den Strukturhomomorphismus erklärt. Eine typische Situation ist dabei, dass $\mathbb{Q}$ der Grundkörper ist und ein Zwischenring L, $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$, gegeben ist. Dann ist L über die Inklusion direkt eine $\mathbb{Q}$-Algebra.

Wenn man zwei Algebren über einem gemeinsamen Grundring hat, so sind vor allem diejenigen Ringhomomorphismen interessant, die den Grundring mitberücksichtigen. Dies führt zu folgendem Begriff.

Definition 22.6. Seien R und S zwei kommutative K-Algebren über einem kommutativen Grundring K. Dann nennt man einen Ringhomomorphismus

$$\varphi\colon\ R \longrightarrow S$$

einen *K-Algebra-Homomorphismus*, wenn er zusätzlich mit den beiden fixierten Ringhomomorphismen $K \to R$ und $K \to S$ verträglich ist.

Zum Beispiel ist jeder Ringhomomorphismus ein $\mathbb{Z}$-Algebra-Homomorphismus, da es zu jedem Ring A überhaupt nur den kanonischen Ringhomomorphismus $\mathbb{Z} \to A$ gibt. Mit dieser Terminologie kann man den Einsetzungshomomorphismus jetzt so verstehen, dass der Polynomring $R[X]$ mit seiner natürlichen Algebrastruktur und eine weitere R-Algebra A mit einem fixierten Element $a \in A$ vorliegt und dass dann durch $X \mapsto a$ ein R-Algebra-Homomorphismus $R[X] \to A$ definiert wird.

Definition 22.7. Sei A eine R-Algebra und sei $f_i \in A$, $i \in I$, eine Familie von Elementen aus A. Dann heißt die kleinste R-Unteralgebra von A, die alle f_i enthält, die von diesen Elementen *erzeugte R-Algebra*. Sie wird mit $R[f_i,\, i \in I]$ bezeichnet.

Man kann diese R-Algebra auch als den kleinsten Unterring von A charakterisieren, der sowohl R als auch die f_i enthält. Wir werden hauptsächlich von erzeugten K-Algebren in einer Körpererweiterung $K \subseteq L$ sprechen, wobei nur ein einziger Erzeuger vorgegeben ist. Man schreibt dafür dann einfach $K[f]$, und diese K-Algebra besteht aus allen K-Linearkombinationen von Potenzen von f. Dies ist das Bild unter dem durch $X \mapsto f$ gegebenen Einsetzungshomomorphismus.

Gelegentlich werden wir auch den kleinsten Unterkörper von L betrachten, der sowohl K als auch eine Elementfamilie f_i, $i \in I$, enthält. Dieser wird mit $K(f_i, i \in I)$ bezeichnet, und man sagt, dass die f_i ein *Körper-Erzeugendensystem* von diesem Körper bilden. Es ist $K[f_i, i \in I] \subseteq K(f_i, i \in I)$ und insbesondere $K[f] \subseteq K(f)$.

Minimalpolynom

Definition 22.8. Sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Wenn ein Polynom $P \neq 0$ das algebraische Element $f \in A$ annulliert (also $P(f) = 0$ ist), so kann man durch den Leitkoeffizienten dividieren und erhält dann auch ein normiertes annullierendes Polynom.

Definition 22.9. Sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von f.

Wenn f nicht algebraisch ist, so wird das Nullpolynom als Minimalpolynom betrachtet.

Beispiel 22.10. Bei einer Körpererweiterung $K \subseteq L$ sind die Elemente $a \in K$ trivialerweise algebraisch, und zwar ist jeweils $X - a \in K[X]$ das Minimalpolynom. Weitere Beispiele liefern über $K = \mathbb{Q}$ die komplexen Zahlen $\sqrt{2}, i, 3^{1/5}$, etc. Annullierende Polynome aus $\mathbb{Q}[X]$ sind dafür $X^2 - 2$, $X^2 + 1$, $X^5 - 3$ (es handelt sich dabei übrigens um die Minimalpolynome, was in den ersten zwei Fällen einfach und im dritten Fall etwas schwieriger zu zeigen ist). Man beachte, dass beispielsweise $X - \sqrt{2}$ zwar ein annullierendes Polynom für $\sqrt{2}$ ist, dessen Koeffizienten aber nicht zu $\mathbb{Q}$ gehören.

Lemma 22.11. *Sei K ein Körper, A eine K-Algebra und $f \in A$ ein Element. Es sei P das Minimalpolynom von f über K. Dann ist der Kern des kanonischen K-Algebra-Homomorphismus*

$$K[X] \longrightarrow A,\ X \longmapsto f,$$

das von P erzeugte Hauptideal.

Beweis. Wir betrachten den kanonischen Einsetzungshomorphismus

$$K[X] \longrightarrow A,\ X \longmapsto f.$$

Dessen Kern ist nach Satz 13.10 und nach Satz 8.3 ein Hauptideal, sagen wir $\mathfrak{a} = (F)$, wobei wir F als normiert annehmen dürfen (im nicht-algebraischen Fall liegt das Nullideal vor und die Aussage ist trivialerweise richtig). Das Minimalpolynom P gehört zu $\mathfrak{a}$. Andererseits ist der Grad von F größer oder gleich dem Grad von P, da ja dessen Grad minimal gewählt ist. Daher muss der Grad gleich sein und somit ist $P = F$, da beide normiert sind. $\square$

22. Arbeitsblatt

Übungsaufgaben

Aufgabe 22.1. Berechne im Körper $\mathbb{Q}[\sqrt{7}]$ das Produkt

$$(-2+\sqrt{7})\cdot(4-\sqrt{7})\,.$$

Aufgabe 22.2. Bestimme in $\mathbb{Q}[\sqrt{7}]$ das Inverse von $2+5\sqrt{7}$.

Aufgabe 22.3.*

Bestimme in $\mathbb{Q}[X]/(X^3+4X^2-7)$ das Inverse von $\frac{1}{3}x+5$ (x bezeichnet die Restklasse von X).

Aufgabe 22.4. Bestimme das Inverse von

$$1+\sqrt{2}+3\sqrt{10}$$

im Körper $\mathbb{Q}[\sqrt{2},\sqrt{5}]$.

Aufgabe 22.5. Bestimme den Grad der Körpererweiterung $\mathbb{R}\subseteq\mathbb{C}$.

Aufgabe 22.6. Sei $K\subseteq L$ eine Körpererweiterung. Zeige, dass L ein K-Vektorraum ist.

Aufgabe 22.7. Sei $K\subseteq L$ eine Körpererweiterung und sei $f\in L$ ein Element. Zeige, dass dann $K(f)$ der Quotientenkörper von $K[f]$ ist.

Aufgabe 22.8. Seien K und L Körper, sei $K\subseteq L$ eine endliche Körpererweiterung und sei A, $K\subseteq A\subseteq L$, ein Zwischenring. Zeige, dass dann A ebenfalls ein Körper ist.

Aufgabe 22.9. Sei $K\subseteq L$ eine Körpererweiterung und $f\in L$ ein nicht algebraisches Element. Zeige, dass dann eine Isomorphie

$$K(X)\longrightarrow K(f)$$

von Körpern vorliegt.

Aufgabe 22.10. Es seien p und q zwei verschiedene Primzahlen. Zeige, dass $\mathbb{Q}[\sqrt{p},\sqrt{q}]$ ein Unterkörper von $\mathbb{R}$ ist, der über $\mathbb{Q}$ den Grad vier besitzt.

Aufgabe 22.11.*

Sei K ein endlicher Körper. Zeige, dass die Anzahl der Elemente von K die Potenz einer Primzahl ist.

Aufgabe 22.12.*

Zeige, dass es zu jeder natürlichen Zahl n eine Körpererweiterung $\mathbb{Q} \subseteq L$ vom Grad n gibt.

Aufgaben zum Abgeben

Aufgabe 22.13. (2 Punkte)

Bestimme in $\mathbb{Q}[\sqrt{11}]$ das Inverse von $3+5\sqrt{11}$.

Aufgabe 22.14. (5 (1+1+2+1) Punkte)

Betrachte den Körper $\mathbb{Z}/(13) = \{0,1,2,...,12\}$ mit 13 Elementen.

(1) Zeige, dass 5 kein Quadrat in $\mathbb{Z}/(13)$ ist und folgere, dass
$$\mathbb{Z}/(13)[X]/(X^2-5) =: \mathbb{Z}/(13)[\sqrt{5}]$$
ein Körper ist.
(2) Betrachte die quadratische Körpererweiterung
$$\mathbb{Z}/(13) \subset \mathbb{Z}/(13)[\sqrt{5}]$$
und berechne
$$(2+3\sqrt{5})(1+11\sqrt{5})(10+7\sqrt{5})$$
(3) Finde das Inverse zu $7+3\sqrt{5}$ in $\mathbb{Z}/(13)[\sqrt{5}]$.
(4) Zeige, dass -5 kein Quadrat in $\mathbb{Z}/(13)$ ist, dafür aber in $\mathbb{Z}/(13)[\sqrt{5}]$.

Aufgabe 22.15. (4 Punkte)

Bestimme das Inverse von
$$2+3\sqrt{5}+\sqrt{7}+3\sqrt{35}$$
im Körper $\mathbb{Q}[\sqrt{5},\sqrt{7}]$.

Aufgabe 22.16. (4 Punkte)

Führe in $(\mathbb{Q}[\sqrt{3}])[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = 3X^3-(2+\sqrt{3})X^2+5\sqrt{3}X+1+2\sqrt{3}$ und $T = \sqrt{3}X^2-X+2+7\sqrt{3}$ durch.

Aufgabe 22.17. (4 Punkte)

Bestimme das Minimalpolynom von

$$\sqrt{3}+\sqrt{5}$$

über $\mathbb{Q}$.

23. Vorlesung - Algebraische Zahlen

Weiteres zum Minimalpolynom

Satz 23.1. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Es sei P das Minimalpolynom von f. Dann gibt es eine kanonische K-Algebra-Isomorphie*

$$K[X]/(P) \longrightarrow K[f],\ X \longmapsto f.$$

Beweis. Die Einsetzung $X \mapsto f$ ergibt nach Satz 13.7 den kanonischen K-Algebra-Homomorphismus

$$K[X] \longrightarrow L,\ X \longmapsto f.$$

Das Bild davon ist genau $K[f]$, so dass ein surjektiver K-Algebra-Homomorphismus

$$K[X] \longrightarrow K[f]$$

vorliegt. Daher gibt es nach Korollar 14.5 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 22.11 das vom Minimalpolynom erzeugte Hauptideal. □

Lemma 23.2. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann gelten folgende Aussagen.*

(1) *Das Minimalpolynom P von f über K ist irreduzibel.*
(2) *Wenn $Q \in K[X]$ ein normiertes, irreduzibles Polynom mit $Q(f) = 0$ ist, so handelt es sich um das Minimalpolynom.*

Beweis. (1) Es sei $P = P_1P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(f) = P_1(f)P_2(f).$$

Da L ein Körper ist, muss ein Faktor 0 sein, sagen wir $P_1(f) = 0$. Da aber P unter allen Polynomen $\neq 0$, die f annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant ($\neq 0$), also eine Einheit sein.

(2) Wegen $Q(f) = 0$ ist Q aufgrund von Lemma 22.11 ein Vielfaches des Minimalpolynoms P, sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad 1 besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$.

□

Algebraische Körpererweiterung

Satz 23.3. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein Element. Dann sind folgende Aussagen äquivalent.*

(1) *f ist algebraisch über K.*
(2) *Es gibt ein normiertes Polynom $P \in K[X]$ mit $P(f) = 0$.*
(3) *Es besteht eine lineare Abhängigkeit zwischen den Potenzen*
$$f^0 = 1, f^1 = f, f^2, f^3, \ldots .$$
(4) *Die von f über K erzeugte K-Algebra $K[f]$ hat endliche K-Dimension.*
(5) *f liegt in einer endlichdimensionalen K-Algebra $M \subseteq L$.*

Beweis. (1) $\Rightarrow$ (2). Das ist trivial, da man ein von 0 verschiedenes Polynom stets normieren kann, indem man durch den Leitkoeffizienten dividiert. (2) $\Rightarrow$ (3). Nach (2) gibt es ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(f) = 0$. Sei
$$P = \sum_{i=0}^{n} c_i X^i .$$
Dann ist
$$P(f) = \sum_{i=0}^{n} c_i f^i = 0$$
eine lineare Abhängigkeit zwischen den Potenzen. (3) $\Rightarrow$ (1). Umgekehrt bedeutet die lineare Abhängigkeit, dass es Elemente c_i gibt, die nicht alle 0 sind mit $\sum_{i=0}^{n} c_i f^i = 0$. Dies ist aber die Einsetzung $P(f)$ für das Polynom $P = \sum_{i=0}^{n} c_i X^i$, und dieses ist nicht das Nullpolynom. (2) $\Rightarrow$ (4). Sei $P = \sum_{i=0}^{n} c_i X^i$ ein normiertes Polynom mit $P(f) = 0$, also mit $c_n = 1$. Dann kann man umstellen
$$f^n = -\sum_{i=0}^{n-1} c_i f^i$$
D.h. f^n kann man durch kleinere Potenzen ausdrücken. Durch Multiplikation dieser Gleichung mit weiteren Potenzen von f ergibt sich, dass man auch

die höheren Potenzen durch die Potenzen f^i, $i \leq n-1$, ausdrücken kann. (4) $\Rightarrow$ (5). Das ist trivial. (5) $\Rightarrow$ (3). Wenn f in einer endlichdimensionalen Algebra $M \subseteq L$ liegt, so liegen darin auch alle Potenzen von f. Da es in einem endlichdimensionalen Vektorraum keine unendliche Folge von linear unabhängigen Elementen geben kann, müssen diese Potenzen linear abhängig sein. □

Satz 23.4. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann ist die von f erzeugte K-Algebra $K[f] \subseteq L$ ein Körper.*

Beweis. Nach Satz 23.1 liegt eine K-Algebra-Isomorphie $K[X]/(P) \cong K[f]$ vor, wobei P das Minimalpolynom zu f ist. Nach Lemma 23.2 (2) ist P irreduzibel, so dass wegen Satz 15.1 der Restklassenring $K[f]$ ein Körper ist. □

Korollar 23.5. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann stimmen die von f über K erzeugte Unteralgebra und der von f über K erzeugte Unterkörper überein. Es gilt also $K[f] = K(f)$.*

Beweis. Die Inklusion $K[f] \subseteq K(f)$ gilt immer, und nach Vorraussetzung ist aufgrund von Satz 23.4 der Unterring $K[f]$ schon ein Körper. □

Bemerkung 23.6. Sei K ein Körper, $P \in K[X]$ ein irreduzibles Polynom und $K \subseteq L = K[X]/(P)$ die zugehörige Körpererweiterung. Dann kann man zu $z = F(x)$, $z \neq 0$, (mit $F \in K[X]$, $x = \overline{X}$) auf folgende Art das Inverse z^{-1} bestimmen. Es sind P und F teilerfremde Polynome in $K[X]$ und daher gibt es nach Satz 8.3 und Korollar 8.6 eine Darstellung der 1, die man mit Hilfe des euklidischen Algorithmus finden kann. Wenn $RF + SP = 1$ ist, so ist die Restklasse von R, also $\overline{R} = R(x)$, das Inverse zu $\overline{F} = z$.

Algebraischer Abschluss

Definition 23.7. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Menge

$$M = \{x \in L | \, x \text{ ist algebraisch über } K\}$$

den *algebraischen Abschluss* von K in L.

Satz 23.8. *Sei $K \subseteq L$ eine Körpererweiterung und sei M der algebraische Abschluss von K in L. Dann ist M ein Unterkörper von L.*

Beweis. Wir müssen zeigen, dass M bezüglich der Addition, der Multiplikation, des Negativen und des Inversen abgeschlossen ist. Seien $x, y \in M$. Wir betrachten die von x und y erzeugte K-Unteralgebra $U = K[x, y]$, die aus allen K-Linearkombinationen der $x^i y^j$, $i, j \in \mathbb{N}$, besteht. Da sowohl x als auch y algebraisch sind, kann man nach Satz 23.3 gewisse Potenzen x^n und y^m

durch kleinere Potenzen ersetzen. Daher kann man alle Linearkombinationen mit den Monomen $x^i y^j$, $i < n$, $j < m$, ausdrücken. D.h. alle Operationen spielen sich in dieser endlichdimensionalen Unteralgebra ab. Daher sind Summe, Produkt und das Negative nach Satz 23.3 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 23.4 ein Körper von endlicher Dimension. Daher ist $z^{-1} \in K[z]$ selbst algebraisch. □

Algebraische Zahlen

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 23.9. Eine komplexe Zahl z heißt *algebraisch* oder *algebraische Zahl*, wenn sie algebraisch über den rationalen Zahlen $\mathbb{Q}$ ist. Andernfalls heißt sie *transzendent*.

Die Menge der algebraischen Zahlen wird mit $\mathbb{A}$ bezeichnet.

Ferdinand von Lindemann (1852-1939)

Bemerkung 23.10. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von 0 verschiedenes Polynom P mit rationalen Koeffizienten und mit $P(z) = 0$ gibt. Durch Multiplikation mit einem Hauptnenner kann man für eine algebraische Zahl auch ein annullierendes Polynom mit ganzzahligen Koeffizienten finden (das allerdings nicht mehr normiert ist). Eine rationale Zahl q ist trivialerweise algebraisch, da sie Nullstelle des linearen rationalen Polynoms $X - q$ ist. Weiterhin sind die reellen Zahlen $\sqrt{q}$ und $q^{1/n}$ für $q \in \mathbb{Q}$ algebraisch. Dagegen sind die Zahlen e und π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Lindemann 1882 gezeigt.

23. Arbeitsblatt

Übungsaufgaben

Aufgabe 23.1.*

Bestimme das Minimalpolynom der komplexen Zahl $2+5i$ über $\mathbb{Q}$.

Aufgabe 23.2. Bestimme das Minimalpolynom der komplexen Zahl $\sqrt{2}-\sqrt{5}$ über $\mathbb{Q}$.

Aufgabe 23.3. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad 1. Zeige, dass $L = K$ ist.

Aufgabe 23.4. Es sei $\mathbb{C} \subseteq L$ eine endliche Körpererweiterung. Zeige

$$\mathbb{C} = L.$$

Aufgabe 23.5. Sei $K \subseteq L$ eine Körpererweiterung und sei $P \in K[X]$ ein Polynom. Zeige: P besitzt genau dann eine Nullstelle in L, wenn es einen K-Algebra-Homomorphismus $K[X]/(P) \to L$ gibt.

Aufgabe 23.6. Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein Element. Zeige: f ist genau dann algebraisch über K, wenn $K[f] = K(f)$ ist.

Aufgabe 23.7. Sei $K \subseteq L$ eine Körpererweiterung und $K \subseteq K' \subseteq L$ ein Zwischenkörper. Es sei $f \in L$ algebraisch über K. Zeige, dass dann f auch algebraisch über K' ist.

Aufgabe 23.8.*

Es sei $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, eine algebraische Zahl. Zeige, dass auch die konjugiert-komplexe Zahl $\overline{z} = a - bi$ sowie der Real- und der Imaginärteil von z algebraisch sind. Man bestimme den Grad der Körpererweiterung

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}\,.$$

Aufgabe 23.9. Zeige, dass die Menge der algebraischen Zahlen $\mathbb{A}$ keine endliche Körpererweiterung von $\mathbb{Q}$ ist.

Aufgabe 23.10. a) Man gebe eine Gerade G in der Ebene $\mathbb{R}^2 = \mathbb{C}$ an, die keine algebraische Zahl enthält.

b) Man gebe einen Kreis K in der Ebene $\mathbb{R}^2 = \mathbb{C}$ an, der keine algebraische Zahl enthält.

Aufgaben zum Abgeben

Aufgabe 23.11. (3 Punkte)

Bestimme das Inverse von $2x^2+3x-1$ im Körper $\mathbb{Q}[X]/(X^3-5)$ (x bezeichnet die Restklasse von X).

Aufgabe 23.12. (5 Punkte)

Sei K ein Körper und sei $L = K(X)$ der rationale Funktionenkörper über K. Zeige, dass es zu jedem $n \in \mathbb{N}_+$ einen Ringhomomorphismus $\varphi\colon L \to L$ gibt derart, dass $L \cong \varphi(L) \subseteq L$ eine endliche Körpererweiterung vom Grad n ist.

Aufgabe 23.13. (4 Punkte)

Bestimme das Minimalpolynom der komplexen Zahl $2i - 3\sqrt{3}$ über $\mathbb{Q}$.

Aufgabe 23.14. (2 Punkte)

Sei p eine Primzahl und $q = p^n$, $n \geq 2$. Zeige, dass $\mathbb{Z}/(p^n)$ kein Vektorraum über $\mathbb{Z}/(p)$ sein kann.

24. Vorlesung - Die Gradformel

Quadratische Körpererweiterungen

Die aller einfachste Körpererweiterung ist die *identische Körpererweiterung* $K = K$, die den Grad 1 besitzt. Die nächst einfachsten sind die vom Grad zwei.

Definition 24.1. Eine endliche Körpererweiterung $K \subseteq L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Beispiele sind $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}]$, wobei p eine Primzahl ist (oder sonst eine rationale Zahl ohne rationale Quadratwurzel) oder $K = K[X]/(P)$ zu einem irreduziblen quadratischen Polynom $P = X^2 + aX + b$.

Lemma 24.2. *Es sei K ein Körper mit einer Charakteristik $\neq 2$ und es sei $K \subset L$ eine quadratische Körpererweiterung. Dann gibt es ein $x \in L$, $x \notin K$ und $x^2 \in K$.*

Beweis. Nach Voraussetzung ist L ein zweidimensionaler Vektorraum über K, und darin ist $K = K1$ ein eindimensionaler Untervektorraum. Nach dem Basisergänzungssatz gibt es ein Element $y \in L$ derart, dass 1 und y eine K-Basis von L bilden. Wir können

$$y^2 = a + by$$

schreiben, bzw. (da 2 eine Einheit ist),

$$0 = y^2 - by - a = \left(y - \frac{b}{2}\right)^2 - \frac{b^2}{4} - a.$$

Mit $x = y - \frac{b}{2}$ gilt also $x^2 = \frac{b^2}{4} + a \in K$ und 1 und x bilden ebenfalls eine K-Basis von L. □

Satz 24.3. *Sei*

$$\mathbb{R} \subseteq K$$

eine endliche Körpererweiterung der reellen Zahlen. Dann ist K isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$.

Beweis. Das reelle normierte Polynom $P \in \mathbb{R}[X]$ zerfällt über den komplexen Zahlen $\mathbb{C}$ nach dem Fundamentalsatz der Algebra in Linearfaktoren, d.h. es ist

$$P = \prod_j (X - \lambda_j)$$

mit $\lambda_j = a_j + b_j i \in \mathbb{C}$. Da P reelle Koeffizienten hat, stimmt es mit seinem komplex-konjugierten überein, d.h. es ist insgesamt

$$\prod_j (X - \lambda_j) = P = \overline{P} = \prod_j (X - \overline{\lambda_j}).$$

Wegen der Eindeutigkeit der Primfaktorzerlegung gibt es zu jedem j ein k mit $\overline{\lambda_j} = \lambda_k$. D.h. entweder, dass $\lambda_j \in \mathbb{R}$ ist, und dann liegt ein reeller Linearfaktor vor, oder aber $j \neq k$ und dann ist

$$(X - \lambda_j)(X - \overline{\lambda_j}) = (X - a_j - b_j i))(X - a_j + b_j i) = X^2 - 2a_j X + a_j^2 + b_j^2$$

ein reelles Polynom. In der reellen Primfaktorzerlegung von P kommen also nur lineare und quadratische Faktoren vor, und insbesondere haben im Reellen alle irreduziblen Polynome den Grad eins oder zwei.

Sei nun $\mathbb{R} \subseteq L$ eine endliche Körpererweiterung. Sei $\mathbb{R} \subset L$ und $x \in L$, $x \notin \mathbb{R}$. Dann ist x algebraisch über $\mathbb{R}$ und nach Satz 23.1 ist $\mathbb{R}[x] \cong \mathbb{R}[X]/(P)$ mit einem irreduziblen Polynom P (dem Minimalpolynom zu x). Das Polynom P besitzt in $\mathbb{C}$ Nullstellen, so dass es einen $\mathbb{R}$-Algebra-Homomorphismus $\mathbb{R}[X]/(P) \to \mathbb{C}$ gibt. Da beides reell-zweidimensionale Körper sind, muss eine Isomorphie vorliegen. Wir erhalten also eine endliche Körpererweiterung

$\mathbb{C} \subseteq L$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, muss nach Aufgabe 24.16 $\mathbb{C} = L$ sein. □

Die Gradformel

Satz 24.4. *Seien $K \subseteq L$ und $L \subseteq M$ endliche Körpererweiterungen. Dann ist auch $K \subseteq M$ eine endliche Körpererweiterung und es gilt*

$$\operatorname{grad}_K M = \operatorname{grad}_K L \cdot \operatorname{grad}_L M\,.$$

Beweis. Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j, 1 \leq i \leq n, 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K erzeugen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \cdots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j}x_1 + \cdots + a_{nj}x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \cdots + b_m y_m \\ &= (a_{11}x_1 + \cdots + a_{n1}x_n)y_1 + \cdots + (a_{1m}x_1 + \cdots + a_{nm}x_n)y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} (\,)\, y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören, folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist, folgt, dass $c_{ij} = 0$ ist für alle i, j. □

Zerfällungskörper

Lemma 24.5. *Sei K ein Körper und F ein Polynom aus $K[X]$. Dann gibt es einen Erweiterungskörper $K \subseteq L$ derart, dass F über L in Linearfaktoren zerfällt.*

Beweis. Sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1(Y)) =: K'$$

eine Körpererweiterung von K nach Satz 15.1. Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt in $K'[X]$ die Faktorisierung

$$P_1 = (X - y)\tilde{P}\,,$$

wobei $\tilde{P}$ einen kleineren Grad als P_1 hat. Das Polynom F hat also über K' mindestens einen Linearfaktor mehr als über K. Induktive Anwendung von dieser Konstruktion liefert eine Kette von Erweiterungen $K \subset K' \subset K'' \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Definition 24.6. Es sei K ein Körper, $F \in K[X]$ ein Polynom und $K \subseteq L$ eine Körpererweiterung, über der F in Linearfaktoren zerfällt. Es seien $a_1, \ldots, a_n \in L$ die Nullstellen von F. Dann nennt man

$$K[a_1, \ldots, a_n] \subseteq L$$

einen *Zerfällungskörper* von F.

Es handelt sich hierbei wirklich um einen Körper, wie wir gleich sehen werden. Ferner ist er eindeutig bestimmt, es gibt also bis auf Isomorphie nur einen Zerfällungskörper zu einem Polynom. Er wird mit $Z(F)$ bezeichnet. Häufig beschränkt man sich auf Polynome vom Grad ≥ 1, bei konstanten Polynomen sehen wir einfach K selbst als Zerfällungskörper an. Über dem Zerfällungskörper zerfällt das gegebene Polynom in Linearfaktoren, da er ja nach Definition alle Nullstellen enthält, mit denen alle beteiligten Linearfaktoren formuliert werden können.

Lemma 24.7. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Es sei $K \subseteq K' \subseteq L$ ein Zwischenkörper. Dann ist L auch ein Zerfällungskörper des Polynoms $F \in K'[X]$.*

Beweis. Das ist trivial. □

Lemma 24.8. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Dann ist $K \subseteq L$ eine endliche Körpererweiterung.*

Beweis. Es sei $L = K[a_1, \ldots, a_n]$, wobei $a_i \in L$ die Nullstellen von F seien und F über L in Linearfaktoren zerfällt. Es liegt die Kette von K-Algebren

$$K \subseteq K[a_1] \subseteq K[a_1, a_2] \subseteq \cdots \subseteq K[a_1, \ldots, a_n] = L$$

vor. Dabei ist sukzessive a_i algebraisch über $K[a_1, \ldots, a_{i-1}]$, da ja a_i eine Nullstelle von $F \in K[X]$ ist. Daher sind die Inklusionen nach Satz 23.4 endliche Körpererweiterungen und nach Satz 24.4 ist dann die Gesamtkörpererweiterung ebenfalls endlich. □

Satz 24.9. *Es sei K ein Körper und sei $F \in K[X]$ ein Polynom. Es seien $K \subseteq L_1$ und $K \subseteq L_2$ zwei Zerfällungskörper von F. Dann gibt es einen K-Algebra-Isomorphismus*

$$\varphi\colon\ L_1 \longrightarrow L_2.$$

Insbesondere gibt es bis auf Isomorphie nur einen Zerfällungskörper zu einem Polynom.

Beweis. Wir beweisen die Aussage durch Induktion über den Grad $\operatorname{grad}_K L_1$. Wenn der Grad eins ist, so ist $K = L_1$ und das Polynom F zerfällt bereits über K in Linearfaktoren. Dann gehören alle Nullstellen von F in einem beliebigen Erweiterungskörper $K \subseteq M$ zu K selbst. Also ist auch $L_2 = K$. Es sei nun $\operatorname{grad}_K L_1 \geq 2$ und die Aussage sei für kleinere Grade bewiesen. Dann zerfällt F über K nicht in Linearfaktoren. Daher gibt es einen irreduziblen Faktor P von F mit $\operatorname{grad}(P) \geq 2$ und $K' = K[X]/(P)$ ist nach Satz 15.1 und nach Proposition 22.1 eine Körpererweiterung von K vom Grad ≥ 2. Da P als Faktor von F ebenfalls über L_1 und über L_2 in Linearfaktoren zerfällt, gibt es Ringhomomorphismen $K' \to L_1$ und $K' \to L_2$. Diese sind injektiv, so dass K' sowohl von L_1 als auch von L_2 ein Unterkörper ist. Nach Lemma 24.4 sind dann L_1 und L_2 Zerfällungskörper von $F \in K'[X]$. Nach Satz 24.4 ist $\operatorname{grad}_{K'} L_1 < \operatorname{grad}_K L_1$, so dass wir auf K', L_1, L_2 die Induktionsvoraussetzung anwenden können. Es gibt also einen K'-Algebra-Isomorphismus

$$\varphi\colon\ L_1 \longrightarrow L_2.$$

Dieser ist erst recht ein K-Algebra-Isomorphismus. □

24. Arbeitsblatt

Übungsaufgaben

Aufgabe 24.1.*

Bestimme eine ganze Zahl n derart, dass die Lösungen der quadratischen Gleichung

$$x^2 + 3x + \frac{7}{3} = 0$$

in $\mathbb{Q}[\sqrt{n}]$ liegen.

Aufgabe 24.2.*

Bestimme in $\mathbb{Q}[i]$ das multiplikative Inverse von

$$\frac{3}{7} + \frac{2}{5}i\,.$$

Die Antwort muss in der Form $p + qi$ mit $p, q \in \mathbb{Q}$ in gekürzter Form sein.

Aufgabe 24.3. Es sei $K \subseteq \mathbb{R}$ ein Unterkörper. Zeige, dass dann auch $K[i]$ ein Unterkörper von $\mathbb{C}$ ist.

Aufgabe 24.4. Es sei K ein Körper der Charakteristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Zeige, dass es neben der Identität einen weiteren K-Algebra-Automorphismus $L \to L$ gibt.

Aufgabe 24.5. Es sei $K \subset K' (\subseteq \mathbb{R})$ eine reell-quadratische Körpererweiterung. Zeige, dass dann auch $K[i] \subset K'[i]$ eine quadratische Körpererweiterung ist.

Aufgabe 24.6. Es sei K ein Körper. Zeige, dass

$$\left\{x \in K^\times \mid x \text{ besitzt eine Quadratwurzel in } K\right\}$$

eine Untergruppe der Einheitengruppe $K^\times$ ist.

Aufgabe 24.7. Beschreibe die Gruppe

$$\left\{x \in K^\times \mid x \text{ besitzt eine Quadratwurzel in } K\right\}$$

für die Körper

$$K = \mathbb{Q},\, \mathbb{R},\, \mathbb{C},\, \mathbb{Z}/(2),\, \mathbb{Z}/(3),\, \mathbb{Z}/(5),\, \mathbb{Z}/(7),\, \mathbb{Z}/(11)\,.$$

Aufgabe 24.8. Es sei p eine Primzahl und

$$K \,=\, \mathbb{Q}[\sqrt{p}]$$

die zugehörige Körpererweiterung von $\mathbb{Q}$. Zeige, dass die Elemente $x \in K$, die (in K) eine Quadratwurzel besitzen, von der Form

$$x \,=\, y^2$$

mit $y \in \mathbb{Q}$ oder von der Form

$$x \,=\, pz^2$$

mit $z \in \mathbb{Q}$ sind.

Aufgabe 24.9. Es sei p eine Primzahl. Wir betrachten die Unterkörper der komplexen Zahlen, $K = \mathbb{Q}[\sqrt{p}, i]$ und $L = \mathbb{Q}[\sqrt{p}, \sqrt{-p}]$. Zeige $K \,=\, L$.

Aufgabe 24.10.*

Es seien $p, q \in \mathbb{Q}_{\geq 0}$ und sei

$$f = \sqrt{p} + \sqrt{q}.$$

a) Zeige, dass es ein Polynom $G \in \mathbb{Q}[X]$ der Form

$$G = X^4 + cX^2 + d$$

mit $G(f) = 0$ gibt.

b) Es seien nun zusätzlich p und q verschiedene Primzahlen. Zeige, dass das Polynom G aus Teil a) das Minimalpolynom zu f ist.

Aufgabe 24.11. Betrachte die Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}, \sqrt{7}] = L.$$

Zeige, dass einerseits $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ und andererseits $(\sqrt{5} + \sqrt{7})^i$, $i = 0, 1, 2, 3$, eine $\mathbb{Q}$-Basis von L bildet. Berechne die Übergangsmatrizen für diese Basen.

Aufgabe 24.12. Sei $K \subseteq L$ eine Körpererweiterung vom Grad p, wobei p eine Primzahl sei. Es sei $x \in L$, $x \notin K$. Zeige, dass $K[x] = L$ ist.

Aufgabe 24.13. Es sei

$$L \subseteq \mathbb{C}$$

ein Unterkörper derart, dass $\mathbb{Q} \subseteq L$ eine Körpererweiterung von Grad 23 ist. Es sei

$$K = L \cap \mathbb{R}$$

Zeige, dass entweder $K = \mathbb{Q}$ oder $K = L$ ist.

Aufgabe 24.14. Bestimme den Grad von

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{3}, \sqrt[3]{7}].$$

Aufgabe 24.15.*

Es sei p eine Primzahl.

a) Bestimme den Grad der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{p}].$$

Man gebe auch eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\sqrt[3]{p}]$ an.

b) Zeige, dass in $\mathbb{Q}[\sqrt[3]{p}]$ alle Elemente der Form m^3p und n^3p^2 mit $m, n \in \mathbb{Q}$ eine dritte Wurzel besitzen.

c) Die rationale Zahl $x \in \mathbb{Q}$ besitze in $\mathbb{Q}[\sqrt[3]{p}]$ eine dritte Wurzel. Zeige, dass x die Form

$$x = k^3 \text{ oder } x = m^3 p \text{ oder } x = n^3 p^2$$

mit $k, m, n \in \mathbb{Q}$ besitzt.

d) Es sei nun q eine weitere, von p verschiedene Primzahl. Bestimme den Grad der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{p}, \sqrt[3]{q}].$$

Aufgabe 24.16. Zeige, dass die Körpererweiterung $\mathbb{R} \subseteq \mathbb{R}(X)$, wobei $\mathbb{R}(X)$ den Körper der rationalen Funktionen bezeichnet, nicht endlich ist.

Aufgabe 24.17. Zeige, dass der Körper der komplexen Zahlen $\mathbb{C}$ der Zerfällungskörper des Polynoms $X^2 + 1 \in \mathbb{R}[X]$ ist.

Aufgabe 24.18. Es sei $P = X^2 + aX + b \in K[X]$ ein quadratisches Polynom über einem Körper K. Welche Möglichkeiten gibt es für den Zerfällungskörper von P?

Aufgabe 24.19. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Zeige, dass es einen (injektiven) Ringhomomorphismus $L \to \mathbb{C}$ gibt.

Aufgabe 24.20. Es sei K ein Körper, $F \in K[X]$ ein Polynom vom Grad n und $K \subseteq L$ der Zerfällungskörper von F. Zeige, dass die Abschätzung

$$\operatorname{grad}_K L \leq n!$$

gilt.

Aufgabe 24.21. Es sei K ein Körper und seien $F_1, \ldots, F_r \in K[X]$ Polynome. Zeige, dass es eine endliche Körpererweiterung $K \subseteq L$ derart gibt, dass diese Polynome in $L[X]$ in Linearfaktoren zerfallen.

Aufgabe 24.22. Es sei $q \in \mathbb{Q}$ eine rationale Zahl und es sei L der Zerfällungskörper von $X^3 - q$. Welchen Grad besitzt L (über $\mathbb{Q}$)? Man gebe für jeden möglichen Grad Beispiele an.

Aufgaben zum Abgeben

Aufgabe 24.23. (3 Punkte)

Bestimme den Grad von

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{5}, \sqrt[3]{2}].$$

Aufgabe 24.24. (3 Punkte)

Es seien $\mathbb{Q} \subseteq K \subset \mathbb{C}$ und $\mathbb{Q} \subseteq L \subset \mathbb{C}$ zwei endliche Körpererweiterungen von $\mathbb{Q}$ vom Grad d bzw. e. Es seien d und e teilerfremd. Zeige, dass dann

$$K \cap L = \mathbb{Q}$$

ist.

Aufgabe 24.25. (6 (4+1+1) Punkte)

Sei p eine Primzahl.

a) Zeige, dass das Polynom $X^4 - p$ irreduzibel über $\mathbb{Q}$ ist.

b) Schließe daraus, dass

$$\mathbb{Q}[\sqrt[4]{p}] \subseteq \mathbb{R}$$

über $\mathbb{Q}$ den Grad vier besitzt.

c) Finde einen echten Zwischenkörper

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[\sqrt[4]{p}].$$

Aufgabe 24.26. (4 (3+1) Punkte)

Es sei K ein endlicher Körper der Charakteristik $p \neq 2$.

a) Zeige, dass es in K Elemente gibt, die keine Quadratwurzel besitzen.

b) Zeige, dass es eine endliche nichttriviale Körpererweiterung

$$K \subseteq L$$

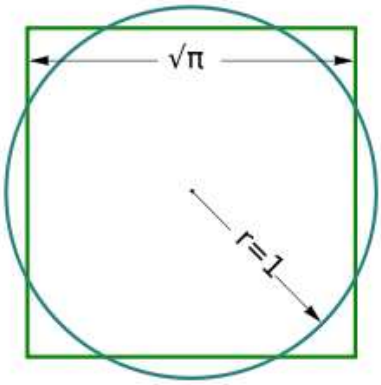
vom Grad zwei gibt.

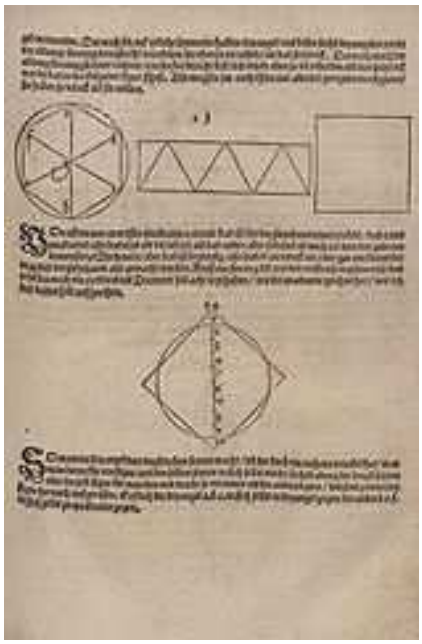
25. Vorlesung - Zirkel und Lineal

Unter den drei klassischen Problemen der antiken Mathematik versteht man

(1) die Quadratur des Kreises,
(2) die Dreiteilung des Winkels,
(3) die Würfelverdoppelung.

Dabei sollen diese Konstruktionen ausschließlich mit Zirkel und Lineal durchgeführt werden, wobei dies natürlich präzisiert werden muss. Nach langen vergeblichen Versuchen, solche Konstruktionen zu finden, ergab sich im Laufe des neunzehnten Jahrhunderts die Erkennntnis, dass es keine solche Konstruktionen geben kann. Dies erfordert natürlich, dass man eine Übersicht über alle möglichen Konstruktionen erhalten kann.





Auch Albrecht Dürer hatte Spaß an der Quadratur des Kreises

Konstruktionen mit Zirkel und Lineal

Unter der Ebene E verstehen wir im Folgenden die Anschauungsebene, die wir später mit $\mathbb{R}^2 \cong \mathbb{C}$ identifizieren. Zunächst sind die Konstruktionen „koordinatenfrei“. An elementargeometrischen Objekten verwenden wir Punkte, Geraden und Kreise. An elementargeometrischen Gesetzmäßigkeiten verwenden wir, dass zwei verschiedene Punkte eine eindeutige Gerade definieren, dass zwei Geraden entweder identisch sind oder parallel und schnittpunktfrei oder genau einen Schnittpunkt haben, u.s.w.

Definition 25.1. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Eine Gerade $G \subset E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $P, Q \in M$, $P \neq Q$, derart gibt, dass die Verbindungsgerade von P und Q gleich G ist. Ein Kreis $C \subseteq E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $Z, S \in M$, $Z \neq S$, derart gibt, dass der Kreis mit dem Mittelpunkt Z und durch den Punkt S gleich C ist.

Man kann also an zwei Punkte aus der vorgegebenen Menge M das *Lineal anlegen* und die dadurch definierte Gerade zeichnen, und man darf die *Nadelspitze des Zirkels* in einen Punkt der Menge stechen und die *Stiftspitze des Zirkels* an einen weiteren Punkt der Menge anlegen und den Kreis ziehen.

Wenn ein Koordinatensystem vorliegt, und zwei Punkte $P = (p_1, p_2)$ und $Q = (q_1, q_2)$ gegeben sind, so ist die Gleichung der Verbindungsgeraden der beiden Punkte bekanntlich

$$(p_1 - q_1)y + (q_2 - p_2)x + q_1p_2 - q_2p_1 = 0\,.$$

Wenn zwei Punkte $Z = (z_1, z_2)$ und $S = (s_1, s_2)$ gegeben sind, so besitzt der Kreis mit dem Mittelpunkt Z durch den Punkt S die Kreisgleichung

$$(x - z_1)^2 + (y - z_2)^2 - (s_1 - z_1)^2 - (s_2 - z_2)^2 = 0\,.$$

Definition 25.2. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Dann heißt ein Punkt $P \in E$ aus M *in einem Schritt konstruierbar*, wenn eine der folgenden Möglichkeiten zutrifft.

(1) Es gibt zwei aus M elementar konstruierbare Geraden G_1 und G_2 mit $G_1 \cap G_2 = \{P\}$.
(2) Es gibt eine aus M elementar konstruierbare Gerade G und einen aus M elementar konstruierbaren Kreis C derart, dass P ein Schnittpunkt von G und C ist.
(3) Es gibt zwei aus M elementar konstruierbare Kreise C_1 und C_2 derart, dass P ein Schnittpunkt der beiden Kreise ist.

Definition 25.3. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Dann heißt ein Punkt $P \in E$ aus M *konstruierbar* (oder *mit Zirkel und Lineal konstruierbar*), wenn es eine Folge von Punkten

$$P_1, \ldots, P_n = P$$

gibt derart, dass P_i jeweils aus $M \cup \{P_1, \ldots, P_{i-1}\}$ in einem Schritt konstruierbar ist.

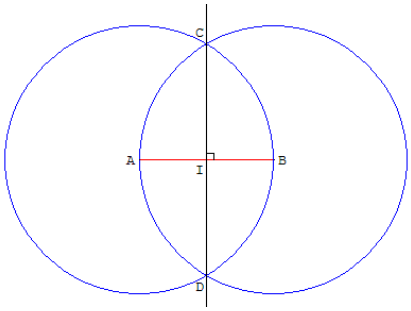
Definition 25.4. Eine Zahl $z \in \mathbb{C} \cong E$ heißt *konstruierbar* oder *konstruierbare Zahl*, wenn sie aus der Startmenge

$$\{0, 1\} \subset \mathbb{R} \subset \mathbb{C}$$

mit Zirkel und Lineal konstruierbar ist.

Bemerkung 25.5. Man startet also mit zwei beliebig vorgegebenen Punkten, die man 0 und 1 nennt und die dann die arithmetische Funktion übernehmen, die mit diesen Symbolen verbunden wird. Als erstes kann man die Gerade durch 0 und 1 ziehen, und diese Gerade wird mit den reellen Zahlen $\mathbb{R}$ identifiziert. Wir werden gleich sehen, dass man eine zu $\mathbb{R}$ senkrechte Gerade durch 0 konstruieren kann, mit deren Hilfe ein *kartesisches Koordinatensystem* entsteht und mit dem wir die Ebene mit den komplexen Zahlen $\mathbb{C}$ identifizieren können.

In den folgenden Konstruktionen verwenden wir einige Begrifflichkeiten aus der euklidischen Geometrie, wie Winkel, senkrecht, parallel, Strecke und elementare Grundtatsachen wie die Strahlensätze, Symmetriesätze und den Satz des Pythagoras.



Lemma 25.6. *In der Ebene lassen sich folgende Konstruktionen mit Zirkel und Lineal durchführen.*

(1) *Zu einer Geraden G und zwei Punkten $Q_1, Q_2 \in G$ kann man die zu G senkrechte Gerade zeichnen, die die Strecke zwischen Q_1 und Q_2 halbiert.*
(2) *Zu einer Geraden G und einem Punkt $P \in G$ kann man die zu G senkrechte Gerade durch P zeichnen.*
(3) *Zu einer Geraden G und einem Punkt P kann man die zu G senkrechte Gerade durch P zeichnen.*
(4) *Zu einer gegebenen Geraden G und einem gegebenen Punkt P kann man die Gerade G' durch P zeichnen, die zu G parallel ist.*

Beweis. Wir verwenden im Beweis einige elementargeometrische Grundtatsachen.

(1) Wir zeichnen die beiden Kreise C_1 und C_2 mit dem Mittelpunkt Q_1 durch Q_2 und umgekehrt. Die beiden Schnittpunkte von C_1 und C_2 seien S_1 und S_2. Deren Verbindungsgerade steht senkrecht auf G und halbiert die Strecke zwischen Q_1 und Q_2.

(2) Man zeichnet einen Kreis C mit P als Mittelpunkt und einem beliebigen Radius (dazu braucht man neben P noch einem weiteren Punkt). Es seien Q_1 und Q_2 die beiden Schnittpunkte der Gerade G mit C. Für diese beiden Punkte führen wir die in (1) beschriebene Konstruktion durch. Diese Halbierungsgerade läuft dann durch P und steht senkrecht auf G.
(3) Wenn P auf der Geraden liegt, sind wir schon fertig mit der Konstruktion in (2). Andernfalls zeichnen wir einen Kreis mit P als Mittelpunkt mit einem hinreichend großen Radius derart, dass sich zwei Schnittpunkte Q_1 und Q_2 mit der Geraden ergeben (dafür braucht man, dass mindestens ein weiterer Punkt zur Verfügung steht). Dann führt wieder die erste Konstruktion zum Ziel.
(4) Dafür führt man zuerst die Konstruktion der Senkrechten S durch P wie in (3) beschrieben durch. Mit P und S führt man dann die Konstruktion (2) durch.

□

Arithmetische Eigenschaften von konstruierbaren Zahlen

Lemma 25.7. *Sei $P = (x, y) \in \mathbb{C} \cong \mathbb{R}^2$ ein Punkt in der Ebene. Dann ist P genau dann konstruierbar, wenn die beiden Koordinaten x und y konstruierbar sind.*

Beweis. Zunächst einmal kann man aufgrund der vorgegebenen Punkte die x-Achse und dann wegen Lemma 25.6 die dazu senkrechte Achse durch 0, also die y-Achse, konstruieren. Es steht also das Achsenkreuz zur Verfügung. Wenn nun P gegeben ist, so kann man aufgrund von Lemma 25.6 (4) die zu den Achsen parallelen Geraden zeichnen und erhält somit die Koordinatenwerte. Den y-Wert kann man dann noch mit einem Kreis mit dem Nullpunkt als Mittelpunkt auf die x-Achse transportieren. Wenn umgekehrt die beiden Koordinaten gegeben sind, so kann man durch diese die senkrechten Geraden zeichnen. Deren Schnittpunkt ist der gesuchte Punkt. □

Lemma 25.8. *Es sei G eine mit 0 und 1 markierte Gerade, die wir mit den reellen Zahlen identifizieren. Es seien zwei Punkte $a, b \in G$ gegeben. Dann gelten folgende Aussagen*

(1) *Die Summe $a + b$ ist (mit Zirkel und Lineal) konstruierbar.*
(2) *Das Produkt ab ist konstruierbar.*
(3) *Bei $b \neq 0$ ist der Quotient a/b konstruierbar.*

Beweis. (1) Wir verwenden eine zu G senkrechte Gerade H durch 0 und darauf einen Punkt $x \neq 0$. Dazu nehmen wir die zu H senkrechte Gerade G' durch x, die also parallel zu G ist. Wir zeichen die Gerade H', die parallel zu H ist und durch $a \in G$ verläuft. Der Schnittpunkt von H' und G' markieren

wir als a', so dass der Abstand von a' zu x gleich a ist. Jetzt zeichnen wir die Gerade L durch b und x und dazu die parallele Gerade L' durch a'. Der Schnittpunkt von L' mit G ist $y = a + b$, da x, b, a', y ein Parallelogramm bilden. Zum Beweis von (2) und (3) verwenden wir wieder die zu G senkrechte Gerade H. Wir schlagen Kreise mit dem Nullpunkt als Mittelpunkt durch 1, a und b und markieren die entsprechenden Punkte auf H als $1'$, a' und b'. Dabei wählt man $1'$ als einen der beiden Schnittpunkte und a' und b' müssen dann auf den entsprechenden Halbgeraden sein. Um das Produkt zu erhalten, zeichnet man die Gerade L durch a und $1'$ und dazu die parallele Gerade L' durch b'. Diese Gerade schneidet G in genau einem Punkt x. Für diesen Punkt gilt nach dem Strahlensatz das Steckenverhältnis

$$\frac{x}{a} = \frac{b'}{1'} = \frac{b}{1}.$$

Also ist $x = ab$. Um den Quotienten $\frac{a}{b}$ bei $b \neq 0$ zu erhalten, zeichnet man die Gerade T durch 1 und b' und dazu parallel die Gerade T' durch a'. Der Schnittpunkt von T' mit G sei z. Aufgrund des Strahlensatzes gilt die Beziehung

$$\frac{a}{b} = \frac{a'}{b'} = z.$$

□

Satz 25.9. *Die Menge der konstruierbaren Zahlen ist ein Unterkörper von* $\mathbb{C}$.

Beweis. Die 0 und die 1 sind als Ausgangsmenge automatisch darin enthalten. Zu einem Punkt P gehört auch der „gegenüberliegende“ Punkt $-P$ dazu, da man ihn konstruieren kann, indem man die Gerade durch P und 0 und den Kreis mit Mittelpunkt 0 und Radius P zeichnet; der zweite Schnittpunkt von diesem Kreis und dieser Geraden ist $-P$. Die Menge der konstruierbaren Zahlen ist also unter der Bildung des Negativen abgeschlossen.

Aufgrund von Lemma 25.7 kann man sich beim Nachweis der Körpereigenschaften darauf beschränken, dass die reellen konstruierbaren Zahlen einen Körper bilden. Dies folgt aber aus Lemma 25.8. □

.

25. Arbeitsblatt

Übungsaufgaben

Aufgabe 25.1. Erstelle eine Geradengleichung für die Gerade im $\mathbb{R}^2$, die durch die beiden Punkte $(2, 3)$ und $(5, -7)$ läuft.

Aufgabe 25.2.*

Erstelle eine Kreisgleichung für den Kreis im $\mathbb{R}^2$ mit Mittelpunkt $(2,7)$, der durch den Punkt $(4,-3)$ läuft.

Aufgabe 25.3. Erstelle eine Kreisgleichung für den Kreis im $\mathbb{R}^2$ mit Mittelpunkt $(4,-1)$, der durch den Punkt $(-2,5)$ läuft.

Aufgabe 25.4. Bestimme die Koordinaten der beiden Schnittpunkte der Geraden G und des Kreises K, wobei G durch die Gleichung $2y-3x+1=0$ und K durch den Mittelpunkt $(2,2)$ und den Radius 5 gegeben ist.

Aufgabe 25.5.*

Berechne die Schnittpunkte der beiden Kreise K_1 und K_2, wobei K_1 den Mittelpunkt $(3,4)$ und den Radius 6 und K_2 den Mittelpunkt $(-8,1)$ und den Radius 7 besitzt.

Aufgabe 25.6. Es sei D ein Dreieck in der Ebene mit den drei Eckpunkten A,B,C. Zeige, dass man die Höhen, die Mittelsenkrechten und die Seitenhalbierenden mit Zirkel und Lineal konstruieren kann.

Aufgabe 25.7. Es sei ein Kreis K und ein Punkt $P \in K$ gegeben. Konstruiere die Tangente an den Kreis durch P.

Aufgabe 25.8. Es sei eine Gerade G und ein Punkt $P \notin G$ gegeben. Konstruiere einen Kreis mit Mittelpunkt P derart, dass die Gerade eine Tangente an den Kreis wird.

Aufgabe 25.9. Es sei $P \in \mathbb{C}$ ein nichtkonstruierbarer Punkt.

a) Zeige, dass es unendlich viele Geraden durch P gibt, auf denen mindestens ein konstruierbarer Punkt liegt.

b) Zeige, dass es maximal eine Gerade durch P gibt, auf der es mindestens zwei konstruierbare Punkte gibt.

Aufgabe 25.10. Rekapituliere die Strahlensätze.

Aufgabe 25.11. Erläutere geometrisch, warum die 0 das neutrale Element der geometrischen Addition von reellen Zahlen ist.

Aufgabe 25.12. Erläutere geometrisch, warum die 1 das neutrale Element der geometrischen Multiplikation von reellen Zahlen ist.

Aufgabe 25.13. Erläutere geometrisch, woran die geometrische Division von reellen Zahlen durch 0 scheitert.

Aufgabe 25.14. Es seien P, Q zwei Punkte auf einer Geraden L und M sei eine weitere Gerade durch P. Konstruiere mit Zirkel und Lineal eine *Raute*, so dass P und Q Eckpunkte sind und eine Seite auf M liegt.

Aufgabe 25.15. Es sei ein Dreieck D durch die Eckpunkte A, B, C in der Ebene E mit den Seiten S, T, R gegeben. Es sei ferner eine Strecke S' durch zwei Punkte $P, Q \in E$ gegeben. Konstruiere mit Zirkel und Lineal ein zu D ähnliches (also winkelgleiches) Dreieck D' derart, dass S' eine Seite von D' ist und dass S' der Seite S entspricht.

Tipp: Konstruiere zuerst ein zu D kongruentes Dreieck D'' derart, dass S'' zu S' parallel ist.

Aufgaben zum Abgeben

Aufgabe 25.16. (3 Punkte)

Berechne die Koordinaten der beiden Schnittpunkte der beiden Kreise K und L, wobei K den Mittelpunkt $(2, 3)$ und den Radius 4 und L den Mittelpunkt $(5, -1)$ und den Radius 7 besitzt.

Aufgabe 25.17. (6 Punkte)

Es sei eine zweielementige Menge $M = \{0, 1\}$ in der Ebene gegeben. Wie viele Punkte lassen sich aus M in einem Schritt, in zwei Schritten und in drei Schritten konstruieren?

Aufgabe 25.18. (3 Punkte)

Beschreibe die Konstruktion einer reellen Zahl x mit Hilfe von Zirkel und Lineal, deren Abweichung von $\sqrt{\pi}$ kleiner als $0,00001$ ist.

Aufgabe 25.19. (3 Punkte)

Bestimme alle Lösungen der Kreisgleichung

$$x^2 + y^2 = 1$$

für die Körper $K = \mathbb{Z}/(2)$, $\mathbb{Z}/(5)$ und $\mathbb{Z}/(11)$.

26. Vorlesung - Quadrate und konstruierbare Zahlen

Konstruktion von Quadratwurzeln

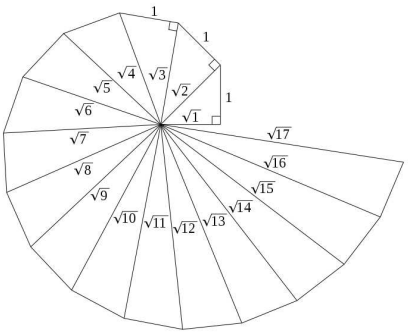
Wenn man sich zwei Punkte 0 und 1 vorgibt und man die dadurch definierte Gerade mit $\mathbb{R}$ identifiziert, so wird diese Gerade durch 0 in zwei Hälften (Halbgeraden) unterteilt, wobei man dann diejenige Hälfte, die 1 enthält, als positive Hälfte bezeichnet. Aus solchen positiven reellen Zahlen kann man mit Zirkel und Lineal die Quadratwurzel ziehen.

Lemma 26.1. *Es sei G eine mit zwei Punkten 0 und 1 markierte Gerade, die wir mit den reellen Zahlen identifizieren. Es sei $a \in G_+$ eine positive reelle Zahl. Dann ist die Quadratwurzel $\sqrt{a}$ aus $0, 1, a$ mittels Zirkel und Lineal konstruierbar.*

Beweis. Wir zeichnen den Kreis mit Mittelpunkt 0 durch 1 und markieren den zweiten Schnittpunkt dieses Kreises mit G als -1. Wir halbieren die Strecke zwischen -1 und a gemäß Lemma 25.6 und erhalten den konstruierbaren Punkt $M = \frac{a-1}{2} \in G$. Der Abstand von M zu a als auch zu -1 ist dann $\frac{a+1}{2}$. Wir zeichnen den Kreis mit Mittelpunkt M und Radius $\frac{a+1}{2}$ und markieren einen der Schnittpunkte des Kreises mit der zu G senkrechten Geraden H durch 0 als x. Wir wenden den *Satz des Pythagoras* auf das Dreieck mit den Ecken $0, x, M$ an. Daraus ergibt sich

$$x^2 = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 = \frac{a^2+2a+1-(a^2-2a+1)}{4} = \frac{4a}{4} = a.$$

Also repräsentiert (der Abstand von 0 zu) x die Quadratwurzel aus a. □



Die Spirale des Theodorus. In dieser Weise kann man alle Quadratwurzeln von natürlichen Zahlen konstruieren.

Die nächste Aussage bedeutet, dass man zu einem gegebenen Rechteck ein flächengleiches Quadrat konstruieren kann.

Korollar 26.2. *Es sei ein Rechteck in der Ebene gegeben. Dann lässt sich mit Zirkel und Lineal ein flächengleiches Quadrat konstruieren.*

Beweis. Die Längen der Rechteckseiten seien a und b. Wir wählen einen Eckpunkt des Rechtecks als Nullpunkt und verwenden die Geraden durch die anliegenden Rechteckseiten als Koordinatenachsen. Wir wählen willkürlich einen Punkt 1 ($\neq 0$) auf einer der Achsen und schlagen einen Kreis um den Nullpunkt durch den Eckpunkt auf der anderen Achse, so dass beide Seitenlängen auf der mit 0 und 1 markierten Achse liegen. Darauf führen wir die Multiplikation ab nach Lemma 25.8 durch. Aus diesem Produkt zieht man nun gemäß Lemma 26.1 die Quadratwurzel und erhält somit $\sqrt{ab}$. Mit dieser Streckenlänge konstruiert man ein Quadrat, dessen Flächeninhalt gleich dem Flächeninhalt des vorgegebenen Rechtecks ist. □

Man beachte, dass im Beweis der vorstehenden Aussage die Zahl ab von der Wahl der 1 abhängt, nicht aber $\sqrt{ab}$ und damit natürlich auch nicht die Seitenlänge des konstruierten Quadrats.

Konstruierbare und algebraische Zahlen

Wir wollen nun die konstruierbaren Zahlen algebraisch mittels quadratischer Körpererweiterungen charakterisieren. Unter einer reell-quadratischen Körpererweiterung eines Körpers $K \subseteq \mathbb{R}$ verstehen wir eine quadratische Körpererweiterung $K \subseteq K'$ mit $K' \subseteq \mathbb{R}$, die sich also innerhalb der reellen Zahlen abspielt. Eine solche Körpererweiterung ist nach Lemma 24.2 gegeben durch die Adjunktion einer Quadratwurel einer positiven reellen Zahl $\sqrt{c}$ mit $c \in K$, $\sqrt{c} \notin K$. Es gilt die Isomorphie

$$K[\sqrt{c}] \cong K[X]/(X^2 - c)\,.$$

Lemma 26.3. *Sei $K \subseteq \mathbb{R}$ ein Körper. Es sei $P \in \mathbb{C}$ ein Punkt, der sich aus $K^2 = K + Ki$ in einem Schritt konstruieren lässt. Dann liegen die Koordinaten von P in einer reell-quadratischen Körpererweiterung von K.*

Beweis. Wir gehen die drei Möglichkeiten durch, einen Punkt aus K^2 in einem Schritt zu konstruieren. Es sei P der Schnittpunkt von zwei verschiedenen Geraden G_1 und G_2, die über K definiert sind. Es sei also $G_1 = \{(x,y)|\, a_1x + b_1y + c_1 = 0\}$ und $G_2 = \{(x,y)|\, a_2x + b_2d + c_2 = 0\}$ mit a_1, b_1, $c_1, a_2, b_2, c_2 \in K$. Dann gehört der Schnittpunkt zu K^2 und seine Koordinaten gehören zu K. Sei G eine über K definierte Gerade und C ein über K definierter Kreis. Dann ist $G = \{(x,y)|\, ax + by + c = 0\}$ und $C = \{(x,y)|\, (x-r)^2 + (y-s)^2 = d\}$ mit $a, b, c, r, s, d \in K$. Wir können annehmen, dass $b \neq 0$ ist, so dass die Geradengleichung auf die Form $y = ux + v$ gebracht werden kann. Einsetzen von dieser Gleichung in die Kreisgleichung ergibt eine quadratische Gleichung für x über K. Die reellen Koordinaten

der (eventuell komplexen) Lösungen davon liegen in einer quadratischen Erweiterung von K. Das gilt dann auch für die zugehörigen Lösungen für y. Seien nun C_1 und C_2 zwei über K definierte verschiedene Kreise. Es seien

$$C_1 = \left\{(x,y) | \, (x-r_1)^2 + (y-s_1)^2 - a_1 = 0\right\}$$

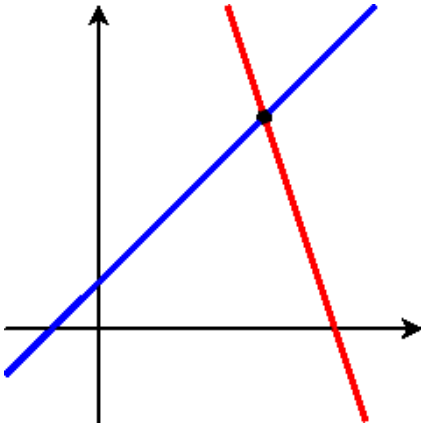
und

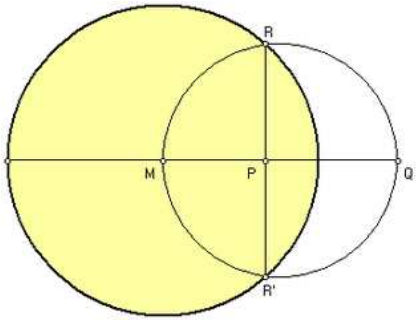
$$C_2 = \left\{(x,y) | \, (x-r_2)^2 + (y-s_2)^2 - a_2 = 0\right\}$$

die Kreisgleichungen. Ein Schnittpunkt der beiden Kreise muss auch jede Linearkombination der beiden Gleichungen erfüllen. Wir betrachten die Differenz der beiden Gleichungen, die die Gestalt

$$x(-2r_1 + 2r_2) + r_1^2 - r_2^2 + y(-2s_1 + 2s_2) + s_1^2 - s_2^2 - a_1 + a_2 = 0$$

besitzt. D.h. dies ist eine Geradengleichung, und die Schnittpunkte der beiden Kreise stimmen mit den Schnittpunkten eines Kreises mit dieser Geraden überein. Wir sind also wieder im zweiten Fall. □





Beispiel 26.4. Wir betrachten die beiden Kreise mit den Kreisgleichungen

$$x^2 + y^2 = 1 \text{ und } (x-2)^2 + y^2 = 3.$$

Die Differenz der beiden Gleichungen ist

$$x^2 - (x-2)^2 + 2 = 0$$

bzw.

$$4x = 2 \text{ und somit } x = \frac{1}{2}\,.$$

Die Schnittpunkte der beiden Kreise müssen also auch auf der durch $x = \frac{1}{2}$ gegebenen Geraden liegen. Setzt man diese Geradenbedingung in die erste Kreisgleichung ein, so erhält man

$$y^2 \;=\; 1 - x^2 \;=\; 1 - \frac{1}{4} \;=\; \frac{3}{4},$$

also

$$y = \pm\frac{\sqrt{3}}{2}\,.$$

Satz 26.5. *Es sei $P \in \mathbb{C}$ eine komplexe Zahl. Dann ist P eine konstruierbare Zahl genau dann, wenn es eine Kette von reell-quadratischen Körpererweiterungen*

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n$$

derart ibt, dass die Koordinaten von P zu K_n gehören.

Beweis. Es sei $P \in \mathbb{C}$ eine konstruierbare komplexe Zahl. D.h. es gibt eine Folge von Punkten $P_1, \ldots, P_n = P$ derart, dass P_{i+1} aus den Vorgängerpunkten $\{0, 1, P_1, \ldots, P_i\}$ in einem Schritt konstruierbar ist. Es sei $P_i = (a_i, b_i)$ und es sei

$$K_i \,=\, \mathbb{Q}(a_1, b_1, \ldots, a_i, b_i)$$

der von den Koordinaten der Punkte erzeugte Unterkörper von $\mathbb{R}$. Nach Lemma 26.3 liegt K_{i+1} in einer reell-quadratischen Körpererweiterung von K_i (und zwar ist $K_{i+1} = K_i$ oder K_{i+1} ist eine reell-quadratische Körpererweiterung von K_i). Die Koordinaten von P liegen also in K_n, und K_n ist das Endglied in einer Folge von quadratischen Körpererweiterungen von $\mathbb{Q}$. Sei umgekehrt angenommen, dass die Koordinaten eines Punktes $P = (a, b)$ in einer Kette von reell-quadratischen Körpererweiterungen von $\mathbb{Q}$ liegen. Wir zeigen durch Induktion über die Länge der Körperkette, dass die Zahlen in einer solchen Kette aus quadratischen Körpererweiterungen konstruierbar sind. Bei $n = 0$ ist $K_0 = \mathbb{Q}$, und diese Zahlen sind konstruierbar. Sei also schon gezeigt, dass alle Zahlen aus K_n konstruierbar sind, und sei $K_n \subset K_{n+1}$ eine reell-quadratische Körpererweiterung. Nach Lemma 24.2 ist $K_{n+1} = K_n[\sqrt{c}]$ mit einer positiven reellen Zahl $c \in K_n$. Nach Induktionsvoraussetzung ist c konstruierbar und nach Lemma 26.1 ist $\sqrt{c}$ konstruierbar. Daher ist auch jede Zahl $u + v\sqrt{c}$ mit $u, v \in K_n$, konstruierbar. Damit sind die Koordinaten von P konstruierbar und somit ist nach Lemma 25.7 auch P selbst konstruierbar. □

Man kann ebenfalls zeigen, dass eine komplex-algebraische Zahl z genau dann konstruierbar ist, wenn der Grad des Zerfällungskörpers des Minimalpolynoms von z eine Potenz von 2 ist. Dies erfordert jedoch die Galoistheorie. Für viele Anwendungen ist allerdings schon die oben vorgestellte Charakterisierung bzw. die folgenden Korollare ausreichend.

Korollar 26.6. *Eine mit Zirkel und Lineal konstruierbare Zahl ist algebraisch.*

Beweis. Dies folgt direkt aus Satz 26.5, aus Satz 24.4 und aus Satz 23.3. □

Korollar 26.7. *Sei $z \in \mathbb{C}$ eine konstruierbare Zahl. Dann ist der Grad des Minimalpolynoms von z eine Potenz von zwei.*

Beweis. Die Koordinaten der konstruierbaren Zahl z liegen nach Satz 26.5 in einer Folge von reell-quadratischen Körpererweiterungen

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n\,.$$

Diese Kette kann man um die komplex-quadratische Körpererweiterung $K_n \subset K_n[i] = L$ ergänzen mit $z \in L$. Nach der Gradformel ist der Grad von L über $\mathbb{Q}$ gleich 2^{n+1}. Dabei ist $\mathbb{Q}(z) = \mathbb{Q}[z] \subseteq L$ ein Unterkörper und daher ist, wieder nach der Gradformel, der Grad von $\mathbb{Q}[z]$ über $\mathbb{Q}$ ein Teiler von 2^{n+1}, also selbst eine Potenz von 2. □

26. Arbeitsblatt

Übungsaufgaben

Aufgabe 26.1. Ist die Zahl, die den „goldenen Schnitt“ beschreibt, eine konstruierbare Zahl?

Aufgabe 26.2. Zeige, dass man zu einem gegebenen Parallelogramm mit Zirkel und Lineal ein flächengleiches gleichseitiges Rechteck konstruieren kann.

Aufgabe 26.3. Zeige direkt, ohne Bezug auf Koordinaten, dass die Summe von zwei konstruierbaren komplexen Zahlen wieder konstruierbar ist.

Aufgabe 26.4. Sei $Z \in \mathbb{C}$ eine konstruierbare Zahl und r eine konstruierbare positive reelle Zahl. Zeige, dass dann auch der Kreis mit Mittelpunkt Z und Radius r konstruierbar ist.

Aufgabe 26.5. Betrachte ein DinA4-Blatt. Ist das Seitenverhältnis aus langer und kurzer Seitenlänge eine konstruierbare Zahl?

Aufgabe 26.6. Betrachte die Tastatur eines Klaviers. Ist das Schwingungsverhältnis von zwei nebeneinander liegendenTasten (bei „gleichstufiger Stimmung“) eine konstruierbare Zahl?

Aufgabe 26.7. Zeige, dass es kein gleichseitiges Dreieck gibt, dessen sämtliche Ecken rationale Koordinaten besitzen.

Aufgabe 26.8.*

Es seien $z, w \in \mathbb{C}$ konstruierbare Zahlen. Bestimme, ob die Zahl

$$z^2 - 3z\sqrt{w} + \sqrt{z + w^2} - \frac{5}{7} + 4\sqrt{\sqrt{z} + w} + \sqrt{11}$$

konstruierbar ist.

Aufgabe 26.9.*

Zeige, dass zu zwei konstruierbaren positiven reellen Zahlen a und b die Potenz a^b nicht konstruierbar sein muss.

Aufgabe 26.10. Zeige, dass es Geraden gibt, auf denen es keinen konstruierbaren Punkt gibt.

Aufgaben zum Abgeben

Aufgabe 26.11. (4 Punkte)

Es sei ein Kreis K und ein Punkt P außerhalb des Kreises gegeben. Konstruiere eine der Tangenten an den Kreis, die durch P läuft.

Aufgabe 26.12. (4 Punkte)

Zeige, dass man zu einem gegebenen Dreieck mit Zirkel und Lineal ein flächengleiches gleichseitiges Dreieck konstruieren kann.

Aufgabe 26.13. (2 Punkte)

Es seien P und Q zwei konstruierbare Punkte. Zeige, dass dann auch der Abstand $d(P, Q)$ konstruierbar ist.

Aufgabe 26.14. (3 Punkte)

Es seien P, Q_1, Q_2 drei konstruierbare Punkte derart, dass die Abstände $d(P, Q_1)$ und $d(P, Q_2)$ gleich 1 sind und dass der Winkel zwischen den dadurch definierten Halbgeraden 90 Grad beträgt. Zeige, dass es dann eine affin-lineare Abbildung

$$\varphi\colon\ E = \mathbb{R}^2 \longrightarrow E = \mathbb{R}^2$$

gibt, die 0 auf P, 1 auf Q_1 und i auf Q_2 schickt, und die konstruierbare Punkte in konstruierbare Punkte überführt.

Aufgabe 26.15. (2 Punkte)

Zeige, dass die komplexe Zahl $re^{i\varphi} = r\,(\cos\varphi\,,\ \sin\varphi\,)$ genau dann konstruierbar ist, wenn r und $e^{i\varphi}$ konstruierbar sind.

Aufgabe 26.16. (4 Punkte)

Beweise auf zwei verschiedene Arten, dass die komplexe Quadratwurzel einer konstruierbaren komplexen Zahl wieder konstruierbar ist.

27. Vorlesung - Quadratur des Kreises

Das Delische Problem

Die Bewohner der Insel Delos befragten während einer Pestepidemie 430 v. Chr. das Orakel von Delphi. Sie wurden aufgefordert, den würfelförmigen Altar des Apollon zu verdoppeln.

Wir kommen zur ersten Konsequenz von unserer systematischen Untersuchung der konstruierbaren Zahlen auf die klassischen Konstruktionsprobleme.

Korollar 27.1. *Die Würfelverdopplung mit Zirkel und Lineal ist nicht möglich.*

Beweis. Wir betrachten einen Würfel mit der Kantenlänge 1 und dem Volumen 1. Die Konstruktion eines Würfels mit dem doppelten Volumen würde bedeuten, dass man die neue Kantenlänge, also $2^{1/3}$ mit Zirkel und Lineal konstruieren könnte. Das Minimalpolynom von $2^{1/3}$ ist $X^3 - 2$, da dieses offenbar $2^{1/3}$ annulliert und nach Lemma 6.9 irreduzibel ist, da in $\mathbb{Q}$ keine dritte Wurzel aus 2 existiert. Nach Korollar 26.7 ist $2^{1/3}$ nicht konstruierbar, da 3 keine Zweierpotenz ist. □

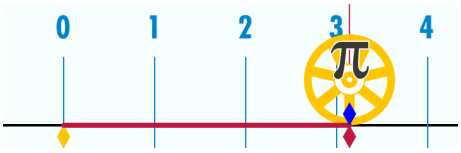
Die Quadratur des Kreises

Satz 27.2. *Es ist nicht möglich, zu einem vorgegebenen Kreis ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren.*

Beweis. Wenn es ein Konstruktionsverfahren gäbe, so könnte man insbesondere den Einheitskreis mit dem Radius 1 quadrieren, d.h. man könnte ein Quadrat mit der Seitenlänge $\sqrt{\pi}$ mit Zirkel und Lineal konstruieren. Nach Korollar 26.6 muss aber eine konstruierbare Zahl algebraisch sein. Nach dem Satz von Lindemann ist aber π und damit auch $\sqrt{\pi}$ transzendent. □

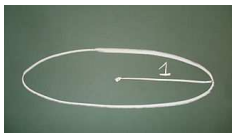
Es gibt natürlich einige geometrische Methoden die Zahl π zu erhalten, z.B. die Abrollmethode und die Schwimmbadmethode.

Beispiel 27.3. Die einfachste Art, die Zahl π geometrisch zu konstruieren, ist die *Abrollmethode*, bei der man einen Kreis mit Durchmesser 1 einmal exakt abrollt. Die zurückgeführte Entfernung ist genau der Kreisumfang, also π.

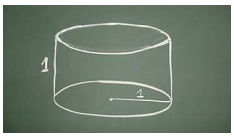


Beispiel 27.4.

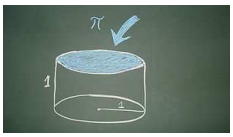
Wir starten mit einem Einheitskreis,



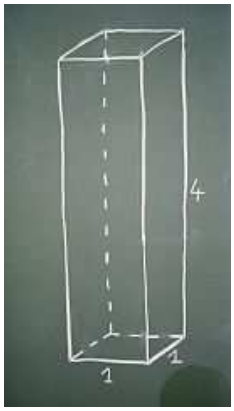
den wir als Grundfläche



eines Schwimmbeckens der Höhe 1 nehmen.

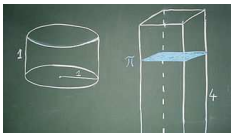


Das füllen wir randvoll mit Wasser auf.



Wir nehmen ein zweites Schwimmbecken mit quadratischer Grundfläche 1×1 und Höhe 4.

Der Inhalt des ersten Schwimmbeckens wird



in das zweite Schwimmbecken gegossen.

Der Wasserstand im zweiten Schwimmbecken ist exakt π.

Einheitswurzeln

Definition 27.5. Es sei K ein Körper und $n \in \mathbb{N}_+$. Dann heißen die Nullstellen des Polynoms

$$X^n - 1$$

in K die n-ten *Einheitswurzeln* in K.

Die 1 ist für jedes n eine n-te Einheitswurzel, und die -1 ist für jedes gerade n eine n-te Einheitswurzel. Es gibt maximal n n-te Einheitswurzel, da das Polynom $X^n - 1$ maximal n Nullstellen besitzt. Die Einheitswurzeln bilden also insbesondere eine endliche Untergruppe (mit $x^n = 1$ und $y^n = 1$ ist auch $(xy)^n = 1$, usw.) der Einheitengruppe des Körpers. Nach einem Satz, den wir nicht bewiesen haben, ist diese Gruppe zyklisch mit einer Ordnung, die n teilt.

Definition 27.6. Eine n-te Einheitswurzel heißt *primitiv*, wenn sie die Ordnung n besitzt.

Man beachte, dass ein Erzeuger der Gruppe der Einheitswurzeln nur dann primitiv heißt, wenn es n verschiedene Einheitswurzeln gibt. Wenn ζ eine primitive n-te Einheitswurzel ist, so sind genau die ζ^i mit $i < n$ und i teilerfremd

zu n die primitiven Einheitswurzeln. Insbesondere gibt es, wenn es überhaupt primitive Einheitswurzeln gibt, genau $\varphi(n)$ primitive Einheitswurzeln, wobei $\varphi(n)$ die eulersche φ-Funktion bezeichnet. Die komplexen Einheitswurzeln lassen sich einfach beschreiben.

Lemma 27.7. *Sei $n \in \mathbb{N}_+$. Die Nullstellen des Polynoms $X^n - 1$ über $\mathbb{C}$ sind*

$$e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, k = 0, 1, \ldots, n-1.$$

In $\mathbb{C}[X]$ gilt die Faktorisierung

$$X^n - 1 = (X-1)(X - e^{2\pi i/n})\cdots(X - e^{2\pi i(n-1)/n})$$

Beweis. Der Beweis verwendet einige Grundtatsachen über die komplexe Exponentialfunktion. Es ist

$$\left(e^{2\pi ik/n}\right)^n = e^{2\pi ik} = \left(e^{2\pi i}\right)^k = 1^k = 1.$$

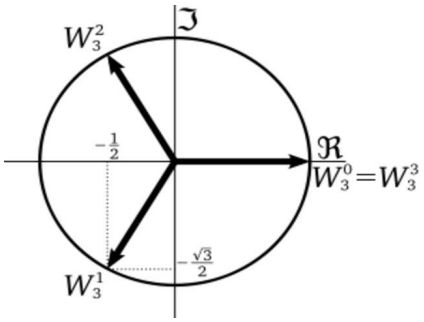
Die angegebenen komplexen Zahlen sind also wirklich Nullstellen des Polynoms $X^n - 1$. Diese Nullstellen sind alle untereinander verschieden, da aus

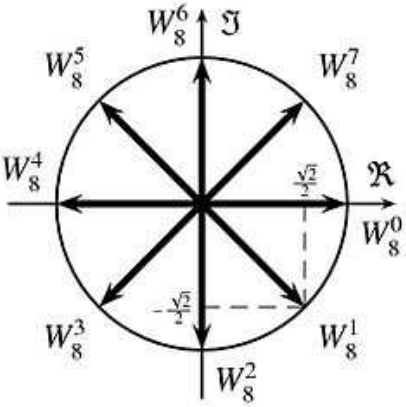
$$e^{2\pi ik/n} = e^{2\pi i\ell/n}$$

mit $0 \leq k \leq \ell \leq n-1$ sofort durch betrachten des Quotienten $e^{2\pi i(\ell-k)/n} = 1$ folgt, und daraus

$$\ell - k = 0.$$

Es gibt also n explizit angegebene Nullstellen und daher müssen dies alle Nullstellen des Polynoms sein. Die explizite Beschreibung in Koordinaten folgt aus der eulerschen Formel. □





Kreisteilungskörper

Definition 27.8. Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms

$$X^n - 1$$

über $\mathbb{Q}$.

Offenbar ist 1 eine Nullstelle von $X^n - 1$. Daher kann man $X^n - 1$ durch $X - 1$ teilen und erhält, wie man schnell nachrechen kann,

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Wegen $1 \in \mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1} + X^{n-2} + \cdots + X + 1\,.$$

Es gibt auch Kreisteilungskörper über anderen Körpern, da es ja stets Zerfällungskörper gibt. Wir beschränken uns aber auf die Kreisteilungskörper über $\mathbb{Q}$, die wir auch mit K_n bezeichnen. Da $X^n - 1$ in der oben explizit beschriebenen Weise über $\mathbb{C}$ in Linearfaktoren zerfällt, kann man K_n als Unterkörper von $\mathbb{C}$ realisieren, und zwar ist K_n der von allen n-ten Einheitswurzeln erzeugte Unterkörper von $\mathbb{C}$. Dieser wird sogar schon von einer einzigen primitiven Einheitswurzel erzeugt, wofür wir den folgenden Begriff einführen.

Definition 27.9. Eine Körpererweiterung $K \subseteq L$ heißt *einfach*, wenn es ein Element $x \in L$ gibt mit

$$L = K(x)\,.$$

Lemma 27.10. *Sei $n \in \mathbb{N}_+$. Dann wird der n-te Kreisteilungskörper über $\mathbb{Q}$ von $e^{2\pi i/n}$ erzeugt. Der n-te Kreisteilungskörper ist also*

$$K_n = \mathbb{Q}\left(e^{2\pi i/n}\right) = \mathbb{Q}[e^{2\pi i/n}].$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$

Beweis. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Wegen $\left(e^{2\pi i/n}\right)^n = 1$ ist $\mathbb{Q}[e^{2\pi i/n}] \subseteq K_n$. Wegen $\left(e^{2\pi i/n}\right)^k = e^{2\pi ik/n}$ gehören auch alle anderen Einheitswurzeln zu $\mathbb{Q}[e^{2\pi i/n}]$, also ist $\mathbb{Q}[e^{2\pi i/n}] = K_n$. □

Statt $e^{\frac{2\pi i}{n}}$ kann man auch jede andere n-te primitive Einheitswurzel als Erzeuger nehmen. Das Minimalpolynom zu einem Erzeuger von K_n heißt das n-te *Kreisteilungspolynom*. Der Grad des n-ten Kreisteilungspolynoms ist der Grad des n-ten Kreisteilungskörpers über $\mathbb{Q}$. Dieser Grad ist stets $\varphi(n)$, was wir aber nicht beweisen werden.

Beispiel 27.11. Wir bestimmen einige Kreisteilungskörper für kleine n. Bei $n = 1$ oder 2 ist der Kreisteilungskörper gleich $\mathbb{Q}$. Bei $n = 3$ ist

$$X^3 - 1 = (X-1)(X^2+X+1)$$

und der zweite Faktor zerfällt

$$X^2 + X + 1 = \left(X + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right).$$

Daher ist der dritte Kreisteilungskörper der von $\sqrt{-3} = \sqrt{3}i$ erzeugte Körper, es ist also $K_3 = \mathbb{Q}[\sqrt{-3}]$ eine quadratische Körpererweiterung der rationalen Zahlen.

Bei $n = 4$ ist natürlich

$$\begin{aligned} X^4 - 1 &= (X^2-1)(X^2+1) \\ &= (X-1)(X+1)(X^2+1) \\ &= (X-1)(X+1)(X-i)(X+i). \end{aligned}$$

Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

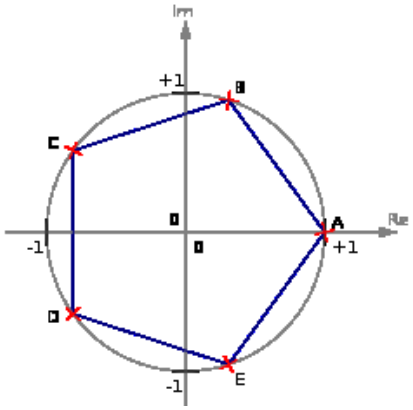
Der Beweis der folgenden wichtigen Aussage beruht auf Überlegungen, die wir nicht entwickelt haben.

Lemma 27.12. *Sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/(X^{p-1} + X^{p-2} + \cdots + X^1 + 1)$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p-1$ über $\mathbb{Q}$.

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □



Beispiel 27.13. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi i/5}$ erzeugt. Er hat aufgrund von Lemma 27.8 die Gestalt

$$K_5 \cong \mathbb{Q}[X]/(X^4+X^3+X^2+X+1)\,,$$

wobei die Variable X als $e^{2\pi i/5}$ (oder eine andere primitive Einheitswurzel) zu interpretieren ist. Sei $x = e^{2\pi i/5}$ und setze $u = 2x^4+2x+1$. Aus Symmetriegründen muss dies eine reelle Zahl sein. Es ist

$$\begin{aligned} u^2 &= 4x^8+4x^2+1+8x^5+4x^4+4x \\ &= 4x^3+4x^2+1+8+4x^4+4x \\ &= 5+4(x^4+x^3+x^2+x+1) \\ &= 5. \end{aligned}$$

Es ist also $u = \sqrt{5}$ (die positive Wurzel) und somit haben wir eine Folge von quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5\,.$$

Dies zeigt aufgrund von Satz 26.5, dass die fünften Einheitswurzeln konstruierbare Zahlen sind.

27. Arbeitsblatt

Übungsaufgaben

Aufgabe 27.1. Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Zeige, dass $K \subset L$ eine einfache, aber keine endliche Körpererweiterung ist.

Aufgabe 27.2. Sei $K \subseteq L$ eine endliche Körpererweiterung, deren Grad eine Primzahl sei. Zeige, dass dann eine einfache Körpererweiterung vorliegt.

Aufgabe 27.3. Es sei K ein Körper, $n \in \mathbb{N}$ und sei M die Menge der n-ten Einheitswurzeln in K. Zeige, dass M eine Untergruppe der Einheitengruppe $K^\times$ ist.

Aufgabe 27.4.*

Zeige, dass jede komplexe Einheitswurzel auf dem Einheitskreis liegt.

Aufgabe 27.5. Es sei p eine Primzahl und $K = \mathbb{Z}/(p)$. Zeige, dass es in K $p-1$ verschiedene $(p-1)$-te Einheitswurzeln gibt.

Finde für $p = 2, 3, 5, 7, 11, 13, 17, 19$ primitive $(p-1)$-te Einheitswurzeln in K.

Aufgabe 27.6. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Beweise die folgenden Aussagen.

(1) Wenn $b_1, b_2 \in K$ zwei Lösungen der Gleichung $X^n = a$ sind und $b_2 \neq 0$, so ist ihr Quotient b_1/b_2 eine n-te Einheitswurzel.
(2) Wenn $b \in K$ eine Lösung der Gleichung $X^n = a$ und ζ eine n-te Einheitswurzel ist, so ist auch ζb eine Lösung der Gleichung $X^n = a$.

Aufgabe 27.7. Bestimme das sechste Kreisteilungspolynom Φ_6 und beschreibe die Primfaktorzerlegung von $X^6 - 1$.

Aufgabe 27.8.*

Es sei p eine Primzahl. Finde die Partialbruchzerlegung von

$$\frac{1}{X^p - 1}$$

in $\mathbb{Q}(X)$.

Aufgabe 27.9. Bestätige folgende Aussagen.

(1) Die dritten Einheitswurzeln in $\mathbb{C}$ sind 1, $\epsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ und $\eta = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.
(2) Es ist $\epsilon^2 = \eta$ und $\eta^2 = \epsilon$.
(3) Es ist $1 + \epsilon + \epsilon^2 = 0$.
(4) Es ist $\epsilon + \epsilon^2 = -1$.

Aufgabe 27.10. Sei $n \in \mathbb{N}_+$. Zeige, dass die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ und die Gruppe $\mathbb{Z}/(n)$ isomorph sind.

Aufgabe 27.11. Seien $n \in \mathbb{N}_+$ und $j \in \mathbb{Z}$. Zeige

$$\sum_{k=0}^{n-1} e^{\frac{2\pi i j k}{n}} = \begin{cases} n, \text{ falls } j \text{ ein Vielfaches von } n \text{ ist,} \\ 0 \text{ sonst .} \end{cases}$$

Aufgabe 27.12.*

Es sei $n \in \mathbb{N}_+$ und es sei $\mu_n \subseteq \mathbb{C}$ die Menge der n-ten komplexen Einheitswurzeln. Es sei $F \in \mathbb{C}[X]$ ein Polynom. Zeige, dass $F \in \mathbb{C}[X^n]$ (d.h., dass F als Polynom in X^n geschrieben werden kann) genau dann gilt, wenn für jedes $z \in \mu_n$ die Gleichheit

$$F(zX) = F(X)$$

gilt.

Aufgaben zum Abgeben

Aufgabe 27.13. (3 Punkte)

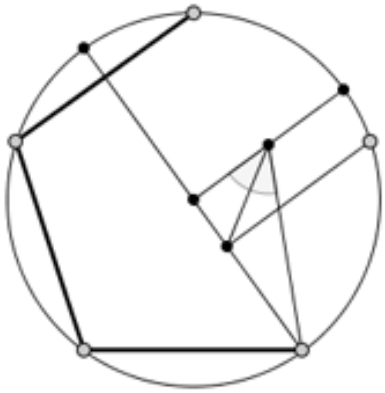
Es sei $n \in \mathbb{N}$ ungerade. Zeige, dass der n-te Kreisteilungskörper mit dem $2n$-ten Kreisteilungskörper übereinstimmt.

Aufgabe 27.14. (4 Punkte)

Bestimme die Koordinaten der fünften Einheitswurzeln in $\mathbb{C}$.

Aufgabe 27.15. (3 Punkte)

Beschreibe die Konstruktion mit Zirkel und Lineal eines regelmäßigen Fünfecks, wie sie in der folgenden Animation dargestellt ist.



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Aufgabe 27.16. (3 Punkte)

Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(23)$.

28. Vorlesung - Einheitswurzeln

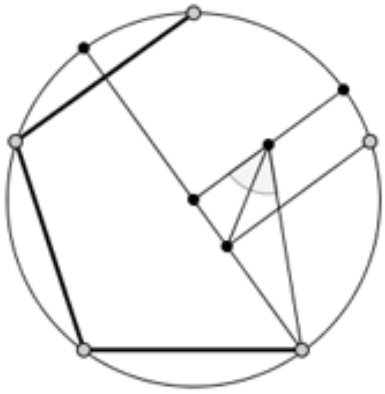
Konstruierbare Einheitswurzeln

Definition 28.1. Sei $n \in \mathbb{N}_+$. Man sagt, dass *das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar* ist, wenn die komplexe Zahl

$$e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

eine konstruierbare Zahl ist.

Die Menge der komplexen Einheitswurzeln $e^{\frac{2\pi ik}{n}}$, $k = 0, \ldots, n-1$, bilden die Eckpunkte eines regelmäßigen n-Ecks, wobei 1 eine Ecke bildet. Alle Eckpunkte liegen auf dem Einheitskreis. Die Ecke $e^{\frac{2\pi i}{n}}$ ist eine primitive Einheitswurzel; wenn diese mit Zirkel und Lineal konstruierbar ist, so sind auch alle weiteren Eckpunkte konstruierbar. Bei $n = 1, 2$ kann man sich darüber streiten, ob man von einem regelmäßigen n-Eck sprechen soll, jedenfalls gibt es die zugehörigen Einheitswurzeln und diese sind aus $\mathbb{Q}$, also erst recht konstruierbar. Das regelmäßige Dreieck ist ein gleichseitiges Dreieck und dieses ist konstruierbar nach Beispiel 27.7, da der dritte Kreisteilungskörper eine quadratische Körpererweiterung von $\mathbb{Q}$ ist (man kann einfacher auch direkt zeigen, dass ein gleichseitiges Dreieck aus seiner Grundseite heraus konstruierbar ist). Das regelmäßige Viereck ist ein Quadrat mit den Eckpunkten $1, i, -1, -i$, und dieses ist ebenfalls konstruierbar. Das regelmäßige Fünfeck ist ebenfalls konstruierbar, wie in Beispiel 27.9 bzw. Aufgabe 27.16 gezeigt wurde. Wir werden im Folgenden sowohl positive als auch negative Resultate zur Konstruierbarkeit von regelmäßigen n-Ecken vorstellen.



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Lemma 28.2. *Sei $m = kn$, $m, k, n \in \mathbb{N}_+$. Dann gelten folgende Aussagen.*

(1) *Das regelmäßige 2^r-Eck, $r \in \mathbb{N}$, ist konstruierbar.*
(2) *Wenn das regelmäßige m-Eck konstruierbar ist, so sind auch das regelmäßige n-Eck und das regelmäßige k-Eck konstruierbar.*
(3) *Wenn n und k teilerfremd sind und wenn das regelmäßige n-Eck und das regelmäßige k-Eck konstruierbar sind, so ist auch das regelmäßige m-Eck konstruierbar.*

Beweis. (1) folgt daraus, dass eine Winkelhalbierung stets mit Zirkel und Lineal durchführbar ist. (2). Nach Voraussetzung ist $e^{\frac{2\pi i}{nk}}$ konstruierbar. Dann ist auch nach Satz 25.9 die Potenz

$$\left(e^{\frac{2\pi i}{nk}}\right)^n = e^{\frac{2\pi i}{k}}$$

konstruierbar. (3). Seien nun $e^{\frac{2\pi i}{n}}$ und $e^{\frac{2\pi i}{k}}$ konstruierbar und n und k teilerfremd. Nach dem Lemma von Bezout gibt es dann ganze Zahlen r, s mit $rn + sk = 1$. Daher ist auch

$$\left(e^{\frac{2\pi i}{n}}\right)^s \left(e^{\frac{2\pi i}{k}}\right)^r = \left(e^{\frac{2\pi ik}{nk}}\right)^s \left(e^{\frac{2\pi in}{nk}}\right)^r = e^{\frac{2\pi isk}{nk}} e^{\frac{2\pi irn}{nk}} = e^{\frac{2\pi i(sk+rn)}{nk}} = e^{\frac{2\pi i}{nk}}$$

konstruierbar. □

Aus diesem Lemma kann man in Zusammenhang mit den oben erwähnten Konstruktionsmöglichkeiten folgern, dass die regelmäßigen $3 \cdot 2^r$-Ecke, die regelmäßigen $5 \cdot 2^r$-Ecke und die regelmäßigen $15 \cdot 2^r$-Ecke für jedes r konstruierbar sind.

Satz 28.3. *Sei n eine natürliche Zahl derart, dass das regelmäßige n-Eck konstruierbar ist. Dann ist $\varphi(n)$ eine Zweierpotenz.*

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Er beruht darauf, dass der n-te Kreisteilungskörper den Grad $\varphi(n)$ besitzt und dass im konstruierbaren Fall der Grad einer Körpererweiterung eine Zweierpotenz sein muss.

Winkeldreiteilung

Wir sind nun in der Lage, das Problem der Winkeldreiteilung zu beantworten.

Korollar 28.4. *Das regelmäßige 9-Eck ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Wäre das regelmäßige 9-Eck konstruierbar, so müsste nach Satz 28.3 $\varphi(9)$ eine Zweierpotenz sein. Es ist aber $\varphi(9) = 2 \cdot 3 = 6$. □

Satz 28.5. *Es ist nicht möglich, einen beliebig vorgegebenen Winkel mittels Zirkel und Lineal in drei gleich große Teile zu unterteilen.*

Beweis. Es genügt, einen (konstruierbaren) Winkel α anzugeben derart, dass $\alpha/3$ nicht konstruierbar ist. Wir betrachten $\alpha = 120°$ Grad, welcher konstruierbar ist, da die dritten Einheitswurzeln konstruierbar sind, weil sie nämlich in einer quadratischen Körpererweiterung von $\mathbb{Q}$ liegen. Dagegen ist der Winkel $\alpha/3 = 120°/3 = 40°$ nicht konstruierbar, da andernfalls das regelmäßige 9-Eck konstruierbar wäre, was nach Korollar 28.4 aber nicht der Fall ist. □

Wir geben noch einen weiteren Beweis, dass die Winkeldreiteilung mit Zirkel und Lineal nicht möglich ist, der nicht auf der allgemeinen Irreduzibilität der Kreisteilungspolynome (die wir nicht bewiesen haben) beruht.

Bemerkung 28.6. Wir zeigen direkt, dass man den Winkel 20° Grad nicht konstruieren kann (obwohl man 60° Grad konstruieren kann). Aufgrund der *Additionstheoreme für die trigonometrischen Funktionen* gilt

$$\cos 3\alpha \ = \ 4\cos^3 \alpha - 3\cos\alpha$$

und damit

$$\begin{aligned}(2\cos 20^\circ)^3 - 3(2\cos 20^\circ) - 1 &= 2\left(4\cos^3 20^\circ - 3\cos 20^\circ - \frac{1}{2}\right) \\ &= 2\left(\cos 60^\circ - \frac{1}{2}\right) \\ &= 0.\end{aligned}$$

Also wird $2\cos 20^\circ$ vom Polynom $X^3 - 3X - 1$ annulliert. Dieses Polynom ist nach Aufgabe 28.3 irreduzibel. Also muss es nach Lemma 23.2 das Minimalpolynom von $2\cos 20^\circ$ sein. Daher kann $2\cos 20^\circ$ nach Korollar 26.7 nicht konstruierbar sein und damit ebensowenig $\cos 20^\circ$.

Fermatsche Primzahlen

Die Frage der Konstruierbarkeit von regelmäßigen n-Ecken führt uns zu Fermatschen Primzahlen.

Definition 28.7. Eine Primzahl der Form $2^s + 1$, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Es ist noch nicht mal bekannt, ob es außer den ersten fünf Fermat-Zahlen

$$3, 5, 17, 257, 65537$$

überhaupt weitere Fermatsche Primzahlen gibt.

Lemma 28.8. *Bei einer Fermatschen Primzahl $2^s + 1$ hat der Exponent die Form $s = 2^r$ mit einem $r \in \mathbb{N}$.*

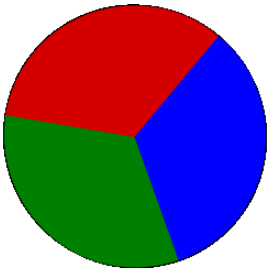
Beweis. Wir schreiben $s = 2^k u$ mit u ungerade. Damit ist

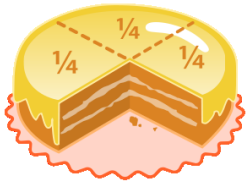
$$2^{2^k u} + 1 \ = \ \left(2^{2^k}\right)^u + 1.$$

Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

$$X^u + 1 \ = \ (X+1)\left(X^{u-1} - X^{u-2} + X^{u-3} - \ldots + X^2 - X + 1\right).$$

Also ist $2^{2^k} + 1 \geq 3$ ein Teiler von $2^{2^k u} + 1$. Da diese Zahl nach Voraussetzung prim ist, müssen beide Zahlen gleich sein, und dies bedeutet $u = 1$. □





Diese Torte wurde nicht mit Zirkel und Lineal geteilt.

Satz 28.9. *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt*

$$n = 2^\alpha p_1 \cdots p_k$$

hat, wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. Wir zeigen nur die eine Richtung, dass bei einem konstruierbaren regelmäßigen n-Eck die Zahl n die angegebene numerische Bedingung erfüllen muss.

Es sei $n = 2^\alpha p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung von n mit den verschiedenen ungeraden Primzahlen p_i, $i = 1, \ldots, k$, und positiven Exponenten $r_i \geq 1$ (und $\alpha \geq 0$). Nach Satz 28.3 muss die eulersche Funktion eine Zweierpotenz sein, also

$$\varphi(n) = 2^t .$$

Andererseits gilt nach Korollar 16.9 die Beziehung

$$\varphi(n) = 2^{\alpha-1}(p_1 - 1)p_1^{r_1-1} \cdots (p_k - 1)p_k^{r_k-1}$$

(bei $\alpha = 0$ ist der Ausdruck $2^{\alpha-1}$ zu streichen). Da dies eine Zweierpotenz sein muss, dürfen die ungeraden Primzahlen nur mit einem Exponenten 1 (oder 0) auftreten. Ferner muss jede beteiligte Primzahl p die Gestalt $p = 2^s + 1$ haben, also eine Fermatsche Primzahl sein.

Für die andere Richtung muss man aufgrund von Lemma 28.2 lediglich zeigen, dass für eine Fermatsche Primzahl p das regelmäßige p-Eck konstruierbar ist. Dies haben wir für $p = 3, 5$ explizit getan. Gauss selbst hat eine Konstruktion für das reguläre 17-Eck angegeben. Für die anderen Fermatschen Primzahlen (bekannt oder nicht) folgt die Konstruierbarkeit aus der Galoistheorie. □

28. Arbeitsblatt

Übungsaufgaben

Aufgabe 28.1.*

Zeige, dass es auf dem Einheitskreis unendlich viele konstruierbare Punkte gibt.

Aufgabe 28.2.*

Zeige, dass das Polynom

$$X^3 - 3X - 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 28.3. Bestimme für alle $n \leq 30$, ob das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist oder nicht.

Aufgabe 28.4. Gib eine Liste aller natürlichen Zahlen n zwischen 100 und 200 mit der Eigenschaft, dass das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist.

Aufgabe 28.5. Konstruiere mit Zirkel und Lineal ein regelmäßiges Zwölfeck.

Aufgabe 28.6. Welche der Winkel

$$10^\circ,\ 20^\circ,\ 30^\circ,\ 40^\circ, \ldots, 350^\circ$$

sind mit Zirkel und Lineal konstruierbar?

Aufgabe 28.7.*

Es sei n eine zu 360 teilerfremde natürliche Zahl. Zeige, dass der Winkel n° nicht mit Zirkel und Lineal konstruierbar ist.

Aufgabe 28.8.*

Man gebe einen Winkel a°, $0 < a < 1$, an, der mit Zirkel und Lineal konstruierbar ist.

Aufgabe 28.9. Es sei β ein Winkel, der durch zwei konstruierbare (Halb)-Geraden durch den Nullpunkt gegeben ist. Zeige, dass die Drehung um den Nullpunkt um den Winkel β konstruierbare Punkte in konstruierbare Punkte überführt.

Aufgabe 28.10.*

Es sei $P \in \mathbb{R}^2$ und

$$\varphi\colon\ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

eine Drehung um den Drehpunkt P um den Winkel β, $0° < \beta < 360°$, mit der Eigenschaft, dass konstruierbare Punkte in konstruierbare Punkte überführt werden.

a) Zeige, dass P ein konstruierbarer Punkt ist.

b) Zeige, dass der Drehwinkel β in dem Sinne konstruierbar ist, dass er als Winkel zwischen zwei konstruierbaren Geraden realisiert werden kann.

Aufgaben zum Abgeben

Aufgabe 28.11. (2 Punkte)

Beweise die Formel

$$\cos 3\alpha \ = \ 4\cos^3 \alpha - 3\cos\alpha$$

aus den Additionstheoremen für die trigonometrischen Funktionen.

Aufgabe 28.12. (5 Punkte)

Es sei $n \in \mathbb{N}$ eine natürliche Zahl, für die das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar sei. Es sei eine Strecke S durch zwei Punkte $P, Q \in E$ gegeben. Konstruiere mit Zirkel und Lineal ein regelmäßiges n-Eck R derart, dass S eine der Kanten von R wird.

Tipp: Aufgabe 25.15 kann helfen.

Aufgabe 28.13. (4 Punkte)

Welche der Winkel

$$1°,\ 2°,\ 3°,\ 4°, \ldots, 10°$$

sind mit Zirkel und Lineal konstruierbar?

Anhang A: Bildlizenzen

Die Bilder dieses Textes stammen aus Commons (also http://commons.wikimedia.org), und stehen unter unterschiedlichen Lizenzen, die zwar alle die Verwendung hier erlauben, aber unterschiedliche Bedingungen an die Verwendung und Weitergabe stellen. Es folgt eine Auflistung der verwendeten Bilder dieses Textes (nach der Seitenzahl geordnet, von links nach rechts, von oben nach unten) zusammen mit ihren Quellen, Urhebern (Autoren) und Lizenzen. Dabei ist *Quelle* so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/File:

unmittelbar davor setzt, die entsprechende Datei auf Commons ergibt. *Autor* benennt den Urheber des Werkes, falls dieser bekannt ist. *Benutzer* meint den Hochlader der Datei; wenn keine weitere Information über den Autor vorliegt, so gilt der Benutzer als Urheber. Die Angabe des Benutzernamen ist so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/User:

unmittelbar davor setzt, die Benutzerseite ergibt. Wenn das Bild ursprünglich in einem anderen Wikimedia-Projekt hochgeladen wurde, so wird die Domäne (bspw. *de.wikipedia.org*) explizit angegeben.

Die *Lizenz* ist die auf der Dateiseite auf Commons angegebene Lizenz. Dabei bedeuten

- GFDL: Gnu Free Documentation License (siehe den angehängten Text, falls diese Lizenz vorkommt)
- CC-BY-SA-2.5 (3.0): Creative Commons Attribution ShareAlike 2.5 (oder 3.0)
- PD: gemeinfrei (public domain)

Abbildungsverzeichnis

Quelle = 2007-07-09Aquilegia01.jpg , Autor = Benutzer Wildfeuer auf Commons, Lizenz = CC-BY-SA-3.0 10

Quelle = Bundesarchiv Bild 183-10308-0006, Calbe, DS-Sportschule, Lehrgang für Sportler.jpg , Autor = Benutzer auf Deutsches Bundesarchiv, Lizenz = 11

Quelle = Pascal triangle.svg , Autor = Benutzer Kazukiokumura auf Commons, Lizenz = CC-by-sa 3.0 18

Quelle = Yanghui triangle.gif , Autor = Benutzer Noe auf Commons, Lizenz = PD 18

Quelle = TrianguloPascal.jpg , Autor = Pascal (= Benutzer Drini auf Commons), Lizenz = PD 18

Quelle = A plus b au carre.svg , Autor = Benutzer Alkarex auf Commons, Lizenz = CC-by-sa 2.0 19

Quelle = Binomio al cubo.svg , Autor = Drini, Lizenz = PD 20

Quelle = Complex number illustration.svg , Autor = Benutzer Wolfkeeper auf en. Wikipedia, Lizenz = CC-by-sa 3.0 28

Quelle = Euler's formula.svg , Autor = Benutzer Wereon auf Commons, Lizenz = CC-by-sa 3.0 29

Quelle = Polynomialdeg2.png , Autor = Enoch Lau, Lizenz = CC-by-sa 2.5 40

Quelle = Polynomialdeg3.png , Autor = Enoch Lau, Lizenz = CC-by-sa 2.5 40

Quelle = Polynomialdeg4.png , Autor = Enoch Lau, Lizenz = CC-by-sa 2.5 41

Quelle = Polynomialdeg5.png , Autor = Enoch Lau, Lizenz = CC-by-sa 2.5 41

Quelle = Gaussian integer lattice.png , Autor = Gunther (= Benutzer Gunther auf Commons), Lizenz = CC-by-sa 3.0 50

Quelle = Group homomorphism.svg , Autor = Benutzer Cronholm 144 auf Commons, Lizenz = CC-by-Sa 2.5 84

Quelle = Chocolates.jpg , Autor = Benutzer Sujit kumar auf Commons, Lizenz = CC-by-sa 4.0 87

Quelle = Joseph-Louis Lagrange.jpeg , Autor = Benutzer Katpatuka auf Commons, Lizenz = PD 92

Quelle = Snijden kruisen evenwijdig.png , Autor = Benutzer MADe auf nl.wikipedia, Lizenz = cc-by-sa 3.0 94

Quelle = TwoTone.svg , Autor = Benutzer Stevo auf Commons, Lizenz = PD 96

Quelle = Coset multiplication.svg , Autor = Benutzer Cronholm 144 auf Commons, Lizenz = CC-by-sa 2.5 98

Quelle = Anillo cíclico.png , Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-BY-SA-3.0 113

Quelle = Pierre de Fermat.jpg , Autor = Benutzer Magnus Manske auf en.wikipedia.org, Lizenz = PD 120

Quelle = Leonhard Euler by Handmann .png , Autor = Emanuel Handmann (= Benutzer QWerk auf Commons), Lizenz = PD 129

Quelle = Function-1 x.svg , Autor = Benutzer Qualc1 auf Commons, Lizenz = CC-by-sa 3.0 134

Quelle = Vector Addition.svg , Autor = Benutzer Booyabazooka auf Commons, Lizenz = PD 150

Quelle = Vector space illust.svg , Autor = Benutzer Oleg Alexandrov auf Commons, Lizenz = PD 151

Quelle = VectorGenerado.gif , Autor = Benutzer Marianov auf Commons, Lizenz = PD 155

Quelle = Carl Louis Ferdinand von Lindemann.jpg , Autor = Benutzer JdH auf Commons, Lizenz = PD 182

Quelle = Squaring the circle.svg , Autor = Albrecht Dürer (= Benutzer SOP auf Commons), Lizenz = PD 193

Quelle = Dürer quadratur.jpg , Autor = Benutzer auf Commons, Lizenz = PD 193

Quelle = Mediatrice compas.gif , Autor = Benutzer Pdebart auf Commons, Lizenz = PD 195

Quelle = Spiral of Theodorus.svg , Autor = Benutzer Pbroks13 auf en Wikipedia, Lizenz = CC-by-sa 3.0 200

Quelle = Two Lines.svg , Autor = Benutzer Jim.belk auf Commons, Lizenz = PD 202

Quelle = Inversie.PNG , Autor = Benutzer Lymantria auf Commons, Lizenz = CC-by-sa 3.0 202

Quelle = My Keyboard.jpg , Autor = Paree, Lizenz = CC-by-sa 2.0 205

Quelle = Roman Statue of Apollo.jpg , Autor = Benutzer Stuart Yeates auf flickr, Lizenz = CC-by-sa-2.0 207

Quelle = Pi-unrolled-720.gif, Autor = John Reid (= Benutzer MGTom auf Commons), Lizenz = CC-by-sa 3.0 207

Quelle = 3rd roots of unity.svg , Autor = Benutzer Marek Schmidt und Nandhp auf Commons, Lizenz = PD 209

Quelle = 8th-root-of-unity.jpg , Autor = Benutzer Marek Schmidt auf Commons, Lizenz = PD 209

Quelle = Kreis5Teilung.svg , Autor = Benutzer Exxu auf Commons, Lizenz = CC-by-sa 3.0 211

Quelle = Pentagon construct.gif , Autor = TokyoJunkie (= Benutzer Mosmas auf en.wikiversity.org), Lizenz = PD 214

Quelle = Pentagon construct.gif , Autor = TokyoJunkie (= Benutzer Mosmas auf PD), Lizenz = en.wikipedia.org 215

Quelle = Pie 2.svg , Autor = Benutzer Cronholm 144 auf Commons, Lizenz = CC-by-sa 3.0 218

Quelle = Cake quarters.svg , Autor = Benutzer Acdx, R. S. Shaw auf Commons, Lizenz = PD 218

Quelle = Luxembourg Vianden Nut-fair 10.jpg , Autor = Benutzer PlayMistyForMe auf Commons, Lizenz = CC-by-sa 3.0 218