Einführung in die Algebra

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

Sommersemester 2009

Inhaltsverzeichnis

Vorwort

Dieses Skript gibt die Vorlesung Einführung in die Algebra wieder, die ich im Sommersemester 2009 an der Universität Osnabrück gehalten habe. Es handelt sich dabei im Wesentlichen um ausformulierte Manuskripttexte, die im direkten Anschluss an die einzelnen Vorlesungen öffentlich gemacht wurden. Ich habe diese Veranstaltung zum ersten Mal durchgeführt, bei einem zweiten Durchlauf würden sicher noch viele Korrekturen und Änderungen dazukommen. Dies bitte ich bei einer kritischen Durchsicht wohlwollend zu berücksichtigen.

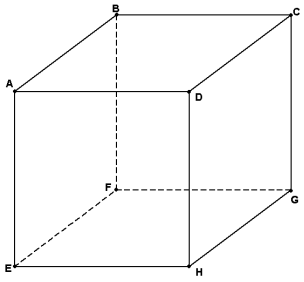
 Ich bedanke mich bei der Wikiversity Gemeinschaft und insbesondere bei Benutzer Exxu für die wichtigen Beiträge im Projekt semantische Vorlagen, die eine weitgehend automatische Erstellung des Latexcodes ermöglichen, bei den Studierenden für einzelne Korrekturen und erstellte Bilder und bei Frau Marianne Gausmann für die Erstellung des Pdf-Files.

Holger Brenner

1. Vorlesung

1.1. **Beispiele zu Symmetrien.**

Wir beginnen diese Vorlesung, indem wir am Beispiel der Symmetrien an einem Würfel den Gruppenbegriff in Erinnerung rufen.



Beispiel 1.1. Wir betrachten einen Würfel $W \subset \mathbb{R}^3$ mit der Seitenlänge 2 und dem Nullpunkt als Mittelpunkt. Die Eckpunkte sind also

$$(\pm 1, \pm 1, \pm 1)\,.$$

Wir fragen uns, welche Möglichkeiten es gibt, den Würfel in sich selbst zu überführen. Dabei soll der Würfel nicht in irgendeiner Form deformiert werden, es ist nur erlaubt, ihn als Ganzes zu bewegen, und zwar soll die Bewegung wirklich physikalisch durchführbar sein. Man spricht auch von einer (eigentlichen) *Bewegung* des Würfels. Bei einer solchen Bewegung verändert der Würfelmittelpunkt seine Lage nicht, und es werden Seiten auf Seiten, Kanten auf Kanten und Ecken auf Ecken abgebildet. Ebenso werden Seitenmittelpunkte auf Seitenmittelpunkte abgebildet, und gegenüberliegende Seitenmittelpunkte werden auf gegenüberliegende Seitenmittelpunkte abgebildet. Die Seitenmittelpunkte sind die sechs Punkte

$$(\pm 1, 0, 0),\ (0, \pm 1, 0),\ (0, 0, \pm 1)\,.$$

Wenn der Punkt $(1, 0, 0)$ auf den Seitenmittelpunkt S abgebildet wird, so wird $(-1, 0, 0)$ auf den gegenüberliegenden Punkt, also $-S$, abgebildet. Hierbei ist jede Vorgabe von S erlaubt, doch dadurch ist die Bewegung noch nicht eindeutig bestimmt. Für den Seitenmittelpunkt $(0, 1, 0)$ gibt es dann noch vier mögliche Bildpunkte (nur S und $-S$ sind ausgeschlossen), da man den Würfel um die durch S gegebene Achse um ein Vielfaches von 90 Grad drehen kann. Diese Drehungen entsprechen genau den Möglichkeiten, den Punkt $(0, 1, 0)$ auf einen der vier verbliebenen Seitenmittelpunkte abzubilden. Durch die Wahl des zweiten Seitenmittelpunktes T ist die Bewegung dann eindeutig festgelegt. Ist das völlig klar?

Um sich das klar zu machen, sind folgende Beobachtungen sinnvoll.

(1) Bewegungen lassen sich hintereinander ausführen, d.h. wenn man zwei Würfelbewegungen φ und ψ hat, so ist auch die *Hintereinanderausführung* $\psi \circ \varphi$, die zuerst φ und dann ψ durchführt, sinnvoll definiert.
(2) Die *identische Bewegung*, die nichts bewegt, ist eine Bewegung. Wenn man zu einer beliebigen Bewegung die identische Bewegung davor oder danach durchführt, so ändert das die Bewegung nicht.
(3) Zu einer Bewegung φ gibt es die *entgegengesetzte Bewegung* (oder „Rückwärtsbewegung“) φ^{-1}, die die Eigenschaft besitzt, dass die Hintereinanderausführungen $\varphi^{-1} \circ \varphi$ und $\varphi \circ \varphi^{-1}$ einfach die Identität sind.

Mit diesen Beobachtungen kann man sich das oben erwähnte Prinzip folgendermaßen klar machen: angenommen, es gibt zwei Bewegungen φ und ψ, die beide $(1,0,0)$ auf S und $(0,1,0)$ auf T abbilden. Es sei ψ^{-1} die umgekehrte Bewegung zu ψ. Dann betrachtet man die Gesamtbewegung

$$\theta = \psi^{-1} \circ \varphi\,.$$

Diese Bewegung hat die Eigenschaft, dass $(1,0,0)$ auf $(1,0,0)$ und dass $(0,1,0)$ auf $(0,1,0)$ abgebildet wird, da ja φ den Punkt $(1,0,0)$ auf S schickt und ψ^{-1} den Punkt S auf $(0,1,0)$ zurückschickt (und entsprechend für $(0,1,0)$). θ hat also die Eigenschaft, dass sowohl $(1,0,0)$ als auch $(0,1,0)$ auf sich selbst abgebildet werden, d.h., es handelt sich um *Fixpunkte* der Bewegung. Dann ist aber bereits die gesamte x,y-Ebene fix. Die einzige physikalisch durchführbare Bewegung des Würfels, die diese Ebene unbewegt lässt, ist aber die identische Bewegung. Daher ist $\psi^{-1} \circ \varphi = \mathrm{id}$ und damit $\varphi = \psi$. Man beachte, dass die *Spiegelung* an der x,y-Ebene die Punkte $(0,0,1)$ und $(0,0,-1)$ vertauscht, doch ist dies eine sogenannte *uneigentliche Bewegung*, da sie nicht physikalisch durchführbar ist.

Damit ergibt sich, dass es für den Basisvektor $(1,0,0)$ sechs mögliche Bildvektoren gibt, für den zweiten Basisvektor $(0,1,0)$ noch jeweils vier und dass dadurch die Abbildung eindeutig festgelegt ist. Insgesamt gibt es also 24 Transformationen des Würfels. Am einfachsten beschreibt man die Bewegungen durch eine 3×3-Matrix, wobei in den Spalten die Bildvektoren der Basisvektoren stehen. Wenn der erste Basisvektor festgehalten wird, so sind die vier möglichen Bewegungen durch die Matrizen

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

gegeben. Dies sieht man so: wenn eine Seitenmitte auf sich selbst abgebildet wird, so gilt das auch für die gegenüberliegende Seitenmitte und dann wird die dadurch definierte Achse nicht bewegt. Eine Bewegung, die eine solche *Seitenmittelpunktachse* fest hält, muss eine Drehung um diese Achse sein, und zwar eine um ein Vielfaches von 90 Grad. Eine solche Drehung ist eine

Bewegung in der Ebene (nämlich in der zur festen Achse senkrechten Ebene), und diese Beobachtung führt zu den angegebenen Matrizen.

Eine wichtige Eigenschaft dieser Bewegungen ist, dass es sich um Drehungen des Raumes um eine fixierte Achse handelt. Diese Eigenschaft zeichnet Raumbewegungen sogar aus, wie wir später noch sehen werden. Da die eben besprochenen Drehungen Vielfache einer Vierteldrehung sind, folgt, dass wenn man sie jeweils viermal hintereinander durchführt, dann wieder die Identität vorliegt. Bei der Halbdrehung führt natürlich schon die zweifache Ausführung zur Identität. Dies wird später mit dem Begriff der *Ordnung* einer Bewegung (eines Gruppenelementes) präzisiert.

Wir betrachten nun im Würfelbeispiel die Raumdiagonale D, die durch $(1,1,1)$ und durch $(-1,-1,-1)$ geht. Auch um diese Ache kann man den Würfel drehen, und zwar um Vielfache von 120 Grad. Man mache sich hierzu klar, wie der Würfel aussieht, wenn diese Achse zu einem Punkt im Gesichtsfeld wird. Die Dritteldrehung, die $(1,0,0)$ auf $(0,0,1)$ schickt, muss $(0,0,1)$ auf $(1,0,0)$ schicken. Die beiden Dritteldrehungen um diese Raumdiagonale sind daher in Matrixdarstellung durch

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

gegeben (die natürlich invers zueinander sind). Die Bewegungen am Würfel kann man dadurch verstehen, indem man untersucht, was eine Bewegung mit den Seitenmittelpunkten macht, wie sie also diese sechs Punkte ineinander überführt, welche sie fest lässt, etc. Eine Bewegung bestimmt dabei stets eine Bijektion dieser Punktmenge in sich selbst. Eine solche Bijektion nennt man auch eine *Permutation*. Es gibt aber auch andere charakteristische Punkte bzw. allgemeiner geometrische Teilobjekte des Würfels, die bei einer Würfelbewegung ineinander überführt werden, z.B. die Menge der Eckpunkte, die Menge der Kantenmittelpunkte, die Menge der Kanten, die Menge der Seiten, die Menge aller Raumdiagonalen, etc. Jede Bewegung hat auf diesen Objekten eine für sie charakteristische (Aus-)wirkung. Die mathematische Präzisierung dieser Beobachtung führt zum Begriff der *Gruppenwirkung* und des *Gruppenhomomorphismus*. Wenn man die Bezeichnung der Ecken vom obigen Bild übernimmt, so haben die oben an zweiter Stelle angeführte Vierteldrehung und die erste Dritteldrehung folgende Wirkung auf den Eckpunkten.

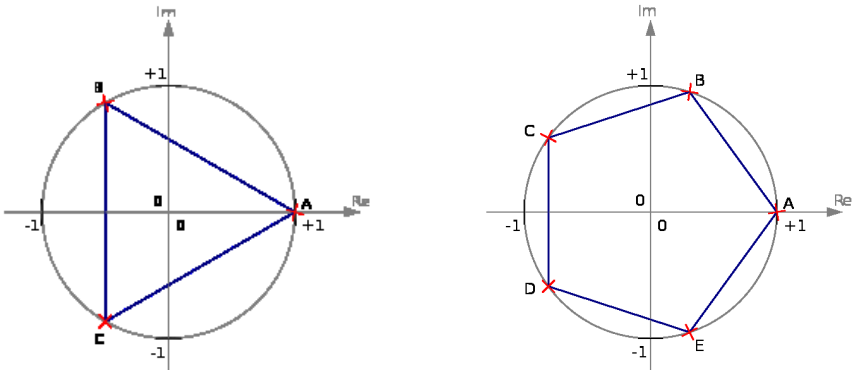
Vierteldrehung um Seitenmittelachse.

Punkt	A	A	C	D	E	F	G	H
Bildpunkt	E	A	D	H	F	B	C	G

Dritteldrehung um Raumdiagonale

Punkt	A	A	C	D	E	F	G	H
Bildpunkt	H	D	C	G	E	A	B	F

Wenn man eine Drehachse für eine Raumbewegung gefunden hat, so ist die Bewegung dadurch charakterisiert, wie sie auf der zur Achse senkrechten Ebene wirkt. Von daher ist es zuerst wichtig, die Bewegungen der Ebene mit einem fixierten Punkt zu verstehen.



Beispiel 1.2. Wir betrachten nun den Einheitskreis

$$S^1 = \{(x, y) \in \mathbb{R}^2 | \, x^2 + y^2 = 1\} \, .$$

Dieser wird bekanntlich parametrisiert durch die trigonometrischen Funktionen. Diese ordnen einem Winkel $\alpha \in [0, 2\pi)$ (bzgl. der x-Achse, gegen den Uhrzeigersinn) den zugehörigen Punkt

$$(\cos \alpha, \sin \alpha)$$

auf dem Kreisbogen zu. Eine gleichmäßige Unterteilung des Intervalls $[0, 2\pi]$ in n gleichgroße Stücke, die durch die Grenzen

$$0, \ \frac{2\pi}{n}, \ 2\frac{2\pi}{n}, \ 3\frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}, \ n\frac{2\pi}{n} = 2\pi$$

gegeben sind, führt zu einer gleichmäßigen Unterteilung des Kreises mit den Eckpunkten

$$(1,0), \ (\sin\frac{2\pi}{n}, \cos\frac{2\pi}{n}), \ (\cos 2\frac{2\pi}{n}, \sin 2\frac{2\pi}{n}), \ (\cos 3\frac{2\pi}{n}, \sin 3\frac{2\pi}{n}), \ldots,$$
$$(\cos(n-1)\frac{2\pi}{n}, \sin(n-1)\frac{2\pi}{n}).$$

Diese Punkte sind die Eckpunkte eines *regelmäßigen n-Ecks*. Das regelmäßige „Zweieck“ besitzt die Ecken $(1, 0)$ und $(-1, 0)$, das regelmäßige (= *gleichseitige*) Dreieck besitzt die Ecken

$$(1,0), \ (-\frac{1}{2}, \frac{\sqrt{3}}{2}), \ (-\frac{1}{2}, -\frac{\sqrt{3}}{2}) \, ,$$

das regelmäßige Viereck (Quadrat) besitzt die Ecken

$$(1,0), \ (0,1), \ (-1,0), \ (0,-1) \, ,$$

usw. Wir fassen ein solches reguläres n-Eck auf als ein in sich starres Gebilde und interessieren uns dafür, wie man es in sich selbst überführen kann. Der Nullpunkt ist der Mittelpunkt (Schwerpunkt) des n-Eckes, und bleibt bei einer Bewegung des n-Eckes auf sich selbst unverändert. Da eine solche Bewegung die Längen nicht ändert, muss der Punkt $(1, 0)$ auf einen der Eckpunkte abgebildet werden, da nur diese Punkte des n-Eckes vom Nullpunkt den Abstand eins besitzen. Da eine Bewegung auch die Winkel nicht verändert, muss der Nachbarpunkt $(\sin \frac{2\pi}{n}, \cos \frac{2\pi}{n})$ auf einen Nachbarpunkt des Bildpunktes von $(1, 0)$ abgebildet werden. Bei einer eigentlichen (physikalisch in der Ebene!) durchführbaren Bewegung bleibt auch die Reihenfolge (die „Orientierung“) der Ecken erhalten, so dass die einzigen eigentlichen Bewegungen eines regulären n-Eckes die Drehungen um ein Vielfaches von $2\pi/n$ sind.

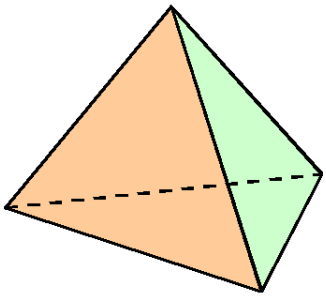
Wenn man auch noch uneigentliche Bewegungen zulässt, so gibt es noch die Spiegelungen an einer Achse, und zwar geht bei n gerade die Achse durch zwei gegenüberliegende Eckpunkte oder zwei gegenüberliegende Seitenmittelpunkte, und bei n ungerade durch einen Eckpunkt und einen gegenüberliegenden Seitenmittelpunkt.

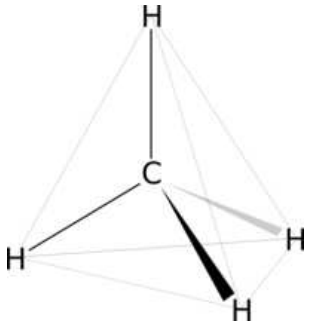
Sei n fixiert, und setze $\alpha = 2\pi/n$ und sei φ die Drehung des n-Eckes um α gegen den Uhrzeigersinn. Dann kann man jede Drehung am n-Eck schreiben als φ^k mit einem eindeutig bestimmten k zwischen 0 und $n - 1$. Dabei ist $\varphi^0 = \mathrm{id}$ die Nulldrehung (die identische Bewegung), bei der nichts bewegt wird. Wenn man φ n-mal ausführt, so hat man physikalisch gesehen eine volle Umdrehung durchgeführt. Vom Ergebnis her ist das aber identisch mit der Nulldrehung. Allgemeiner gilt, dass wenn man φ m-mal ausführt, dass dann das Endergebnis (also die effektive Bewegung) nur vom *Rest* $m \mod n$ abhängt. Die inverse Bewegung zu φ^k ist φ^{-k}, also k-mal wieder zurück, oder gleichbedeutend $\varphi^{(n-k)}$.

Sei nun ψ eine bestimmte Drehung am n-Eck, also $\psi = \varphi^k$ mit einem eindeutig bestimmten k, $0 \leq k \leq n - 1$. Dann kann man sich überlegen, welche Drehungen sich als Hintereinanderausführung von ψ schreiben lassen, also zur Menge

$$\psi^0 = \mathrm{id}\,, \psi^1 = \psi, \psi^2, \psi^3, \ldots$$

gehören. Da die Menge der Drehungen endlich ist, muss es eine Wiederholung geben. Wie sieht diese aus, wann durchlaufen die Hintereinanderausführungen von ψ sämtliche Drehungen am n-Eck? Dafür gibt es recht einfache Antworten im Rahmen der elementaren Gruppentheorie.





Beispiel 1.3. Wir betrachten einen *Tetraeder*, also eine Pyramide mit vier gleichseitigen Dreiecken als Flächen. Das einfachste Modell dafür ergibt sich, wenn man bei einem Würfel jeden „zweiten“ Punkt nimmt, also beispielsweise die Eckpunkte

$$(1,1,1),\ (-1,-1,1),\ (1,-1,-1),\ (-1,1,-1)\,.$$

Der Abstand der Eckpunkte zum Nullpunkt ist dann $\sqrt{3}$ und die Kantenlängen sind $\sqrt{2}$. Eine eigentliche Bewegung des Tetraeders ist auch eine eigentliche Bewegung des zugehörigen Würfels.

1.2. **Der Gruppenbegriff.**

In den angeführten Beispielen haben wir gesehen, dass man die Bewegungen an einem der geometrischen Objekte hintereinander ausführen kann und wieder eine Bewegung erhält, dass es die identische Bewegung gibt, und dass es zu einer gegebenen Bewegung die umgekehrte Bewegung gibt, die sie neutralisiert. Diese Eigenschaften werden durch den Begriff der Gruppe mathematisch präzisiert.

Definition 1.4. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

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

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

Wenn X ein geometrisches Objekt ist, und $M = \mathrm{Bew}\,(X)$ die Menge der Bewegungen auf X (also die bijektiven Abbildungen von X nach X, die die geometrische Struktur von X respektieren), so ist die Hintereinanderschaltung von Bewegungen, also

$$\mathrm{Bew}\,(X) \times \mathrm{Bew}\,(X) \longrightarrow \mathrm{Bew}\,(X),\ (f,g) \longmapsto g \circ f,$$

eine Verknüpfung.

Definition 1.5. 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 $x \in M$.

Die Hintereinanderausführung von Bewegungen ist assoziativ, da es allgemeiner bei der Hintereinanderausführung von Abbildungen nicht auf die Klammerung ankommt. Die identische Bewegung ist die neutrale Bewegung. 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 1.6. Ein Monoid $(G, \circ, e)$ heißt *Gruppe*, wenn jedes Element ein *inverses Element* besitzt, d.h. wenn es zu jedem $x \in G$ ein $y \in G$ gibt mit $x \circ y = e = y \circ x$.

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

2. Vorlesung

2.1. **Beispiele für Gruppen.**

Aus der Vorlesung Mathematik I 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 bspw. 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 in der ersten Vorlesung besprochenen *Symmetriegruppen* zu geometrischen Figuren sind sehr häufig nicht kommutativ. Wir haben die (eigentliche) Würfelgruppe (mit 24 Elementen), also die Gruppe der Bewegungen an einem Würfel, und die Tetraedergruppe (mit 12 Elementen) ausführlich besprochen. 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.

Die Menge der invertierbaren $n \times n$-Matrizen (also diejenigen mit Determinante $\neq 0$) über $\mathbb{R}$ bilden mit der Matrizenmultiplikation als Verknüpfung ebenfalls eine Gruppe, die mit $\mathrm{Gl}_n(\mathbb{R})$ bezeichnet wird.

2.2. **Lösbarkeit von Gleichungen.**

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

Satz 2.1. *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.

2.3. **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 2.2. *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 5.5.

2.4. **Gruppenordnung und Elementordnung.**

Definition 2.3. 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 2.4. 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 2.5. *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. □

2.5. **Untergruppen.**

Definition 2.6. 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 $g^{-1} \in H$.

Lemma 2.7. *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. Offenbar gehört das neutrale Element zum Durchschnitt. Seien $g, h \in \bigcap_{i\in I} H_i$. Dann ist $g, h \in H_i$ für alle i und daher auch $g + h \in H_i$ für alle i. Damit gehört $g + h$ zum Durchschnitt, d.h. der Durchschnitt ist ein Untermonoid. Sei nun h ein Element im Durchschnitt. Dann ist $h \in H_i$ für alle i und daher auch $h^{-1} \in H_i$ für alle i, also $h^{-1} \in \bigcap_{i\in I} H_i$. □

Man hat bspw. 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.

Beispiel 2.8. Wir betrachten einen Würfel mit den Eckpunkten $(\pm 1, \pm 1, \pm 1)$ und den darin enthaltenen Tetraeder mit den vier Eckpunkten

$$(1, 1, 1),\ (-1, -1, 1),\ (1, -1, -1),\ (-1, 1, -1)\,.$$

Dann ist jede Bewegung des Tetraeders auch eine Bewegung des Würfels: Eine Drehung des Tetraeders um eine Eck-Seitenmittelpuntkache ist eine Drehung des Würfels um eine Raumdiagonale. Eine Drehung des Tetraeders um eine Kantenmittelpunktachse ist eine (Halb-)drehung des Würfels um eine Seitenmittelpunktachse. Dies sind alle zwölf Tetraederbewegungen. Die Vierteldrehungen des Würfels um eine Seitenmittelpunktsachse und die Halbdrehungen um eine Würfelkantenmittelpunktachse bilden den Tetraeder nicht auf sich ab.

Warnung: das vorstehende Beispiel bedeutet keineswegs, dass die Symmetriegruppen eines geometrischen Teilobjektes immer eine Untergruppe der Symmetriegruppe des umfassenden geometrischen Objektes ist.

Definition 2.9. 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“ (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. Gruppen, die von einem Element erzeugt werden, heißen zyklisch.

2.6. **Zyklische Gruppen.**

Definition 2.10. 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 2.11. *Eine zyklische Gruppe ist kommutativ.*

Beweis. Das ist trivial. □

Eine zyklische Blüte der Ordnung fünf.

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

Beispiel 2.12. Sei $n \in \mathbb{N}$. Dann bilden die ebenen Drehungen um Vielfache des Winkels $360/n$ Grad eine zyklische Gruppe der Ordnung n.

Beispiel 2.13. Sei $n \in \mathbb{N}$. Wir betrachten innerhalb der komplexen Zahlen $\mathbb{C}$ die Lösungen der Gleichung

$$x^n = 1\,.$$

Da $\mathbb{C}$ algebraisch abgeschlossen ist, gibt es genau n verschiedene Zahlen, die diese Gleichung erfüllen. Man nennt sie die n-ten *Einheitswurzeln*. Wegen $(xy)^n = x^n y^n = 1 \cdot 1 = 1$ ist diese Menge multiplikativ abgeschlossen, und wegen $(x^{-1})^n = x^{-n} = (x^n)^{-1} = e^{-1} = e$ gehören auch die multiplikativen Inverse dazu. Durch Betrachten des Betrages folgt aus $x^n = 1$ direkt $|x| = 1$, d.h. x liegt auf dem Einheitskreis. Aufgrund der Eulerschen Formel

$$e^{iz} = \cos z + i \sin z$$

ist $x = e^{iz}$ mit $z \in \mathbb{R}$, und wegen $e^{iz} \cdot e^{iw} = e^{i(z+w)}$ folgt

$$x = e^{\frac{k2\pi i}{n}}$$

für ein k, d.h. die n-ten Einheitswurzeln bilden die Ecken eines regulären n-Ecks.

Beispiel 2.14. 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 2.11, mit 1 als Erzeuger.

3. Vorlesung

3.1. **Division mit Rest.**

In dieser und der nächsten Vorlesung stehen die ganzen Zahlen $\mathbb{Z}$ im Vordergrund, wobei wir uns insbesondere für die Gruppenstruktur $(\mathbb{Z}, 0, +)$ interessieren. 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 3.1. *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. Zur Existenz. Bei $n = 0$ ist $q = r = 0$ eine Lösung. Sei n positiv. Da d positiv ist, gibt es ein Vielfaches $ad \geq n$. Daher gibt es auch eine Zahl q mit $qd \leq n$ und $(q+1)d > n$. Sei $r := n - qd$. Dann ist

$$qd \leq qd + r < qd + d$$

und daher ist $0 \leq r < d$ wie gewünscht. Bei n negativ kann man schreiben $-n = \tilde{q}d + \tilde{r}$ nach dem Resultat für positive Zahlen. Daraus ergibt sich

$$n = (-\tilde{q})d - \tilde{r} = \begin{cases} (-\tilde{q})d + 0 \text{ bei } \tilde{r} = 0 \\ (-\tilde{q}-1)d + d - \tilde{r} \text{ sonst}\,. \end{cases}$$

Im zweiten Fall erfüllen $q = -\tilde{q} - 1$ und $r = d - \tilde{r}$ die Bedingungen.

Zur Eindeutigkeit. Sei $qd + r = n = \tilde{q}d + \tilde{r}$, wobei die Bedingungen jeweils erfüllt seien. Es sei ohne Einschränkung $\tilde{r} \geq r$. Dann gilt $(q-\tilde{q})d = \tilde{r} - r$. Diese Differenz ist nichtnegativ und kleiner als d, links steht aber ein Vielfaches von d, so dass die Differenz null sein muss und die beiden Darstellungen überein stimmen. □

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 schreiben kann als

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

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 3.2. *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 3.1 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 $H \subseteq \mathbb{Z}d$. □

Bevor wir uns fragen, wie man zu einer durch verschiedene Zahlen erzeugte Untergruppe einen einzigen Erzeuger findet, besprechen wir einige Folgerungen für endliche Gruppen.

Lemma 3.3. *Es sei G eine Gruppe und $x \in G$ ein Element mit endlicher Ordnung $d = \operatorname{ord}(x)$. Dann ist die Menge*

$$M = \{k \in \mathbb{Z} |\, x^k = e_G\}$$

eine Untergruppe von $\mathbb{Z}$, die von d erzeugt wird.

Beweis. Es ist einfach zu sehen, dass M eine Untergruppe von $\mathbb{Z}$ ist. Da d die Ordnung von x ist, gilt $d \in M$ und damit $\mathbb{Z}d \subseteq M$. Nach Satz 3.2 ist $M = \mathbb{Z}a$ mit $0 \leq a \leq d$. Bei $a < d$ wäre aber $x^a = e$ nach Definition von M und d könnte nicht die Ordnung sein. □

3.2. **Endliche zyklische Gruppen.**

Satz 3.4. *Sei G eine zyklische Gruppe. Dann ist auch jede Untergruppe von G zyklisch.*

Beweis. Sei u ein Erzeuger von G, d.h. jedes Element $z \in G$ lässt sich darstellen als ku mit $k \in \mathbb{Z}$. Es sei $H \subseteq G$ eine Untergruppe. Dazu definieren wir die Menge

$$M = \{k \in \mathbb{Z} |\, ku \in H\}\,.$$

Dies ist eine Untergruppe von $\mathbb{Z}$. Aus $ku \in H$ und $mu \in H$ folgt sofort aufgrund von Lemma 2.2

$$(k + m)u \;=\; ku + mu \;\in\; H,$$

also $k + m \in M$. Ebenso gehört wegen

$$(-k)u \;=\; -(ku) \;\in\; H$$

auch das Negative zu M. Daher ist nach Satz 3.2 $M = \mathbb{Z}d$ mit einem eindeutig bestimmten $d \geq 0$. Wir behaupten, dass

$$H = (du)$$

ist, dass also das d-Fache von u die Untergruppe erzeugt. Wegen $d \in M$ ist $du \in H$ und die Inklusion $(du) \subseteq H$ klar. Sei umgekehrt $h \in H$ und $h = ku$. Dann ist $k = rd$ für ein $r \in \mathbb{Z}$ und daher

$$h \;=\; ku \;=\; (rd)u \;=\; r(du).$$

□

Die folgende Aussage gilt allgemeiner in jeder endlichen Gruppe und für jede Untergruppe, der Beweis braucht dann aber das Konzept der Nebenklassen.

Korollar 3.5. *Sei G eine endliche zyklische Gruppe und $x \in G$ ein Element. Dann teilt die Ordnung* $\operatorname{ord}(x)$ *die Gruppenordnung* $\operatorname{ord}(G)$.

Beweis. Sei u ein Erzeuger von G. Dann ist die Ordnung von u gleich der Ordnung n von G. Wir schreiben $x = u^m$. Dann ist

$$x^n = (u^m)^n = u^{mn} = (u^n)^m = e^m = e.$$

Daher gehört die Gruppenordnung n zur Menge

$$M = \{k \in \mathbb{Z} |\, x^k = e\}.$$

Diese hat nach Lemma 3.3 die Gestalt $M = \mathbb{Z}d$, wobei d die Ordnung von x ist. Also ist $n \in \mathbb{Z}d$ und d ist ein Teiler von n. □

3.3. **Teilbarkeitsbegriffe.**

Es sei $d_1, \ldots, d_n$ eine Menge von ganzen Zahlen und $H \subseteq \mathbb{Z}$ die dadurch erzeugte Untergruppe von $\mathbb{Z}$, also

$$H = (d_1, \ldots, d_n) = \{a_1 d_1 + \ldots + a_n d_n |\, a_i \in \mathbb{Z}\}.$$

Nach den obigen Resultaten gibt es ein eindeutig bestimmtes $d \in \mathbb{N}$ mit $H = \mathbb{Z}d$. Wie findet man dieses d? Hierzu muss man vor allem den Fall von zwei Erzeugern verstehen. Denn wenn $(d_1, d_2) = \mathbb{Z}d$ ist, so ist auch

$$(d_1, \ldots, d_n) = (d, d_3, \ldots, d_n),$$

und die Anzahl der Erzeuger ist um eins reduziert. In diesem Zusammenhang erinnern wir an verschiedene Sprechweisen, die schon aus der Schule bekannt sind.

Definition 3.6. Man sagt, dass die ganze Zahl a die ganze Zahl b *teilt* (oder dass b von a *geteilt* wird, oder dass b ein *Vielfaches* von a ist), wenn es eine ganze Zahl c gibt derart, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Lemma 3.7. *(Teilbarkeitsregeln)*

In $\mathbb{Z}$ gelten folgende Teilbarkeitsbeziehungen.

(1) *Für jede ganze Zahl a gilt $1 \,|\, a$ und $a \,|\, a$*
(2) *Für jede ganze Zahl 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 jede ganze Zahl c.*
(6) *Gilt $a \,|\, b$ und $a \,|\, c$, so gilt auch $a \,|\, rb + sc$ für beliebige ganze Zahlen r, s.*

Beweis. Siehe Aufgabe 3.6. □

Definition 3.8. Seien $a_1, \ldots, a_k$ ganze Zahlen. Dann heißt eine ganze Zahl t *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn t jedes a_i teilt ($i = 1, \ldots, k$).

Eine ganze Zahl g 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.

Lemma 3.9. *Seien $a_1, \ldots, a_k$ ganze Zahlen und $H = (a_1, \ldots, a_k)$ die davon erzeugte Untergruppe. Eine ganze Zahl t ist ein gemeinsamer Teiler der $a_1, \ldots, a_k$ genau dann, wenn $H \subseteq \mathbb{Z}t$ ist, und t ist ein größter gemeinsamer Teiler genau dann, wenn $H = \mathbb{Z}t$ ist.*

Beweis. Aus $H = (a_1, \ldots, a_k) \subseteq (t)$ folgt sofort $a_i\mathbb{Z} \subseteq t\mathbb{Z}$ für jedes $i = 1, \ldots k$, was gerade bedeutet, dass t diese Zahlen teilt, also ein gemeinsamer Teiler ist. Sei umgekehrt t ein gemeinsamer Teiler. Dann ist $a_i \in t\mathbb{Z}$ und da $H = (a_1, \ldots, a_k)$ die kleinste Untergruppe ist, die alle a_i enthält, muss $H \subseteq t\mathbb{Z}$ gelten.

Aufgrund von Satz 3.2 wissen wir, dass es eine ganze Zahl g gibt mit $H = \mathbb{Z}g$. Für einen anderen gemeinsamen Teiler t der a_i gilt $\mathbb{Z}g = H \subseteq \mathbb{Z}t$, so dass g von allen anderen gemeinsamen Teilern geteilt wird, also ein größter gemeinsamer Teiler ist. □

4. Vorlesung

4.1. **Das Lemma von Bezout.**

Satz 4.1. *Jede Menge von ganzen Zahlen $a_1, \ldots, a_n$ besitzt einen größten gemeinsamen Teiler d, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt ganze Zahlen $r_1, \ldots, r_n$ mit*

$$r_1a_1 + r_2a_2 + \ldots + r_na_n = d\,.$$

Insbesondere gibt es zu teilerfremden ganzen Zahlen $a_1, \ldots, a_n$ eine Darstellung der 1.

Beweis. Dies folgt direkt aus Lemma 3.9 und Satz 3.2. □

Man beachte, dass ein größter gemeinsamer Teiler, der nach dem Lemma von Bézout existiert, nicht eindeutig bestimmt ist. Denn ebenso ist mit g auch das Negative $-g$ ein größter gemeinsamer Teiler. Häufig wählt man den Vertreter ≥ 0, um Eindeutigkeit zu erreichen, und spricht dann von *dem größten gemeinsamer Teiler* der $a_1, \ldots, a_n$. Diese Zahl wird dann mit

$$\mathrm{ggT}\,(a_1, \ldots, a_n)$$

bezeichnet. Wir besprechen nun, wie man algorithmisch zu vorgegebenen ganzen Zahlen den ggT finden kann.

4.2. **Der Euklidische Algorithmus.**

Es seien a, b ganze Zahlen, $b \neq 0$. Dann kann man die Division mit Rest durchführen und erhält $a = qb + r$ mit $0 \leq r < b$. Danach kann man (bei $r \neq 0$) die Division mit Rest von b durch r durchführen, d.h. b nimmt die Rolle von a und r die Rolle von b ein und erhält einen neuen Rest. Dies kann man fortsetzen, und da dabei die Reste immer kleiner werden bricht das Verfahren irgendwann ab.

Euklid (4. Jahrhundert v. C.)

Definition 4.2. Seien zwei ganze Zahlen a, b (mit $b \neq 0$) gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels Satz 3.1

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

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

Satz 4.3. *Seien zwei ganze Zahlen $r_0 = a$ und $r_1 = b \neq 0$ 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 $r_{i+2} < r_{i+1}$.*
(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 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

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

□

Beispiel 4.4. Aufgabe: Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 71894 und 45327.

Lösung:

Der Euklidischen Algorithmus liefert:

$$71894 = 1 \cdot 45327 + 26567$$

$$45327 = 1 \cdot 26567 + 18760$$

$$26567 = 1 \cdot 18760 + 7807$$

$$18760 = 2 \cdot 7807 + 3146$$

$$7807 = 2 \cdot 3146 + 1515$$

$$3146 = 2 \cdot 1515 + 116$$

$$1515 = 13 \cdot 116 + 7$$

$$116 = 16 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1\,.$$

Die Zahlen 71894 und 45327 sind also teilerfremd.

Bei kleinen Zahlen sieht man häufig relativ schnell direkt, was ihr größter gemeinsamer Teiler ist, da man die Primfaktorzerlegung kennt bzw. mögliche gemeinsame Teiler schnell übersehen kann. Bei zwei größeren Zahlen müssten aber viel zu viele Probedivisionen durchgeführt werden! Der euklidische Algorithmus ist also zur Bestimmung des größten gemeinsamen Teilers ein sehr effektives Verfahren!

4.3. **Darstellung des größten gemeinsamen Teilers.**

Mit dem euklidischen Algorithmus kann man auch durch Zurückrechnen eine Darstellung des größten gemeinsamen Teilers als Linearkombination der beiden vorgegebenen Zahlen erhalten. Dazu seien

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

die Gleichungen im euklidischen Algorithmus und $r_{k-1} = \mathrm{ggT}\,(r_0, r_1)$. Aus der letzten Gleichung

$$r_{k-3} = q_{k-3} r_{k-2} + r_{k-1}$$

erhält man die Darstellung

$$r_{k-1} = r_{k-3} - q_{k-3} r_{k-2}$$

von r_{k-1} als Linearkombination mit r_{k-3} und r_{k-2}. Mit der vorhergehenden Zeile

$$r_{k-4} = q_{k-4} r_{k-3} + r_{k-2}$$

bzw.

$$r_{k-2} = r_{k-4} - q_{k-4} r_{k-3}$$

kann man in dieser Darstellung r_{k-2} ersetzen und erhält eine Darstellung von r_{k-1} als Linearkombination von r_{k-3} und r_{k-4}. So fortfahrend erhält man schließlich eine Darstellung von $r_{k-1} = \mathrm{ggT}\,(r_0, r_1)$ als Linearkombination von r_0 und r_1.

Beispiel 4.5. Wir wollen für 52 und 30 eine Darstellung des größten gemeinsamen Teilers finden. Wir führen dazu den euklidischen Algorithmus durch.

$$52 = 1 \cdot 30 + 22$$

$$30 = 1 \cdot 22 + 8$$

$$22 = 2 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0\,.$$

D.h. 2 ist der größte gemeinsame Teiler von 52 und 30. Rückwärts gelesen erhält man daraus die Darstellung

$$\begin{aligned} 2 &= 8-6 \\ &= 8-(22-2\cdot 8) \\ &= 3\cdot 8-22 \\ &= 3\cdot(30-22)-22 \\ &= 3\cdot 30-4\cdot 22 \\ &= 3\cdot 30-4\cdot(52-30) \\ &= 7\cdot 30-4\cdot 52. \end{aligned}$$

4.4. **Gemeinsame Vielfache.**

Nachdem wir schon die gemeinsamen Teiler von ganzen Zahlen behandelt haben, wenden wir uns einem verwandten Begriff zu, der ebenfalls aus der Schule bekannt ist, nämlich dem des kleinsten gemeinsamen Vielfachen von ganzen Zahlen. In der Schule wird dabei „kleinste“ in Bezug auf die $\leq$-Ordnung verstanden. Wir benutzen einen äquivalenten Begriff, der sich besser auf eine weit allgemeinere Situation übertragen lässt.

Definition 4.6. Zu einer Menge von ganzen Zahlen

$$a_1,\ldots,a_n$$

heißt eine ganze Zahl b ein *gemeinsames Vielfaches*, wenn b ein Vielfaches von jedem a_i ist, also von jedem a_i geteilt wird. Die Zahl 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.

Wir werden gleich sehen, dass es stets ein kleinstes gemeinsames Vielfaches gibt, und dass dieses, wenn man es ≥ 0 wählt, auch eindeutig bestimmt ist. Man spricht dann einfach von *dem* kleinsten gemeinsamen Vielfachen, geschrieben $\mathrm{kgV}\,(a_1,\ldots,a_n)$.

Satz 4.7. *Zu einer Menge von ganzen Zahlen*

$$a_1,\ldots,a_n$$

existiert genau ein kleinstes gemeinsames Vielfaches ≥ 0*, und zwar ist* $\mathrm{kgV}\,(a_1,\ldots,a_n)$ *der eindeutig bestimmte Erzeuger* $b\geq 0$ *der Untergruppe*

$$\mathbb{Z}a_1\cap\ldots\cap\mathbb{Z}a_n\,.$$

Beweis. Es ist klar, dass eine ganze Zahl b ein gemeinsames Vielfaches der $a_1,\ldots,a_n$ ist genau dann, wenn

$$b\in\mathbb{Z}a_1\cap\ldots\cap\mathbb{Z}a_n \text{ bzw. } \mathbb{Z}b\subseteq\mathbb{Z}a_1\cap\ldots\cap\mathbb{Z}a_n$$

gilt. Nach Satz 3.2 gibt es ein eindeutig bestimmtes $c\geq 0$ mit

$$\mathbb{Z}c=\mathbb{Z}a_1\cap\ldots\cap\mathbb{Z}a_n\,.$$

Nach der Vorüberlegung ist daher c ein gemeinsames Vielfaches und für jedes weitere gemeinsame Vielfache b gilt

$$\mathbb{Z}b \subseteq \mathbb{Z}c\,.$$

Dies bedeutet, dass b ein Vielfaches von c ist. □

Lemma 4.8. *Für ganze Zahlen a, b, g mit $g \geq 0$ gelten folgende Aussagen.*

(1) *Für teilerfremde a, b ist* $\mathrm{kgV}\,(a,b) = ab$.
(2) *Es gibt $c, d \in \mathbb{Z}$ mit $a = c \cdot \mathrm{ggT}\,(a,b)$ und $b = d \cdot \mathrm{ggT}\,(a,b)$, wobei c, d teilerfremd sind.*
(3) *Es ist* $\mathrm{kgV}\,(ga, gb) = g \cdot \mathrm{kgV}\,(a,b)$.
(4) *Es ist* $\mathrm{ggT}\,(a,b)\,\mathrm{kgV}\,(a,b) = ab$.

Beweis. (1) Zunächst ist natürlich das Produkt ab ein gemeinsames Vielfaches von a und b. Sei also f irgendein gemeinsames Vielfaches, also $f = ua$ und $f = vb$. Nach Satz 4.1 gibt es im teilerfremden Fall Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$. Daher ist

$$f \;=\; f \cdot 1 \;=\; f(ra + sb) \;=\; fra + fsb \;=\; vbra + uasb \;=\; (vr + us)ab$$

ein Vielfaches von ab.

(2) Die Existenz von c und d ist klar. Hätten c und d einen gemeinsamen Teiler $e \neq 1, -1$, so ergebe sich sofort der Widerspruch, dass $e \cdot \mathrm{ggT}\,(a,b)$ ein (größerer) gemeinsamer Teiler wäre.

(3) Die rechte Seite ist offenbar ein gemeinsames Vielfaches von ga und gb. Sei n ein Vielfaches der linken Seite, also ein gemeinsames Vielfaches von ga und gb. Dann kann man schreiben $n = uga$ und $n = vgb$. Damit ist $uga = vgb$ und somit ist $k := ua = vb$ (bei $n \neq 0$; $n = 0$ ist erst recht ein Vielfaches der rechten Seite) ein gemeinsames Vielfaches von a und b. Also ist $n = gk$ ein Vielfaches der rechten Seite.

(4) Wir schreiben unter Verwendung der ersten Teile

$$\begin{aligned}
\mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(a,b) &= \mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(c \cdot (\mathrm{ggT}\,(a,b)), d \cdot (\mathrm{ggT}\,(a,b))) \\
&= \mathrm{ggT}\,(a,b) \cdot \mathrm{ggT}\,(a,b) \cdot \mathrm{kgV}\,(c,d) \\
&= \mathrm{ggT}\,(a,b) \cdot \mathrm{ggT}\,(a,b) \cdot cd \\
&= c \cdot \mathrm{ggT}\,(a,b) \cdot d \cdot \mathrm{ggT}\,(a,b) \\
&= ab.
\end{aligned}$$

□

5. Vorlesung

5.1. Gruppenhomomorphismen.

Definition 5.1. 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.

Die Menge der Gruppenhomomorphismen von G nach H wird mit

$$\mathrm{Hom}\,(G, H)$$

bezeichnet. Aus der linearen Algebra sind vermutlich die linearen Abbildungen zwischen Vektorräume bekannt, welche insbesondere Gruppenhomomorphismen sind, darüber hinaus aber auch noch mit der skalaren Multiplikation verträglich sind. Die folgenden beiden Lemmata folgen direkt aus der Definition.

Lemma 5.2. *Es seien G und H Gruppen und $\varphi : G \to H$ 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 $e_H = \varphi(e_G)$. Für die zweite Behauptung gilt

$$\varphi(g^{-1})\varphi(g) \ = \ \varphi(g^{-1}g) \ = \ \varphi(e_G) \ = \ e_H.$$

Das heißt, dass $\varphi(g^{-1})$ die Eigenschaft besitzt, die für das Inverse von $\varphi(g)$ charakteristisch ist. Da das Inverse in einer Gruppe eindeutig bestimmt ist, muss $\varphi(g^{-1}) = (\varphi(g))^{-1}$ gelten. □

Lemma 5.3. *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. Das ist trivial. □

Beispiel 5.4. Betrachte die additve 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

$$\exp : \mathbb{R} \longrightarrow \mathbb{R}_+,\ x \longmapsto \exp(x),$$

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 5.5. *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

$$\varphi_g : \mathbb{Z} \longrightarrow G,\ n \longmapsto g^n,$$

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. □

Man kann den Inhalt dieses Lemmas auch kurz durch $G \cong \mathrm{Hom}\,(\mathbb{Z}, G)$ ausdrücken. 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

$$\mathbb{Z} \longrightarrow \mathbb{Z},\ x \longmapsto ax.$$

5.2. **Gruppenisomorphismen.**

Definition 5.6. Seien G und H Gruppen. Einen bijektiven Gruppenhomomorphismus

$$\varphi : G \longrightarrow H$$

nennt man einen *Isomorphismus* (oder eine *Isomorphie*). Die beiden Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

Lemma 5.7. *Seien G und H Gruppen und sei*

$$\varphi : G \longrightarrow H$$

ein Gruppenisomorphismus. Dann ist auch die Umkehrabbildung

$$\varphi^{-1} : H \longrightarrow G,\ h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus.

Beweis. Dies folgt aus $\varphi^{-1}(e_H) = e_G$ und aus

$$\begin{array}{rcl} \varphi^{-1}(h_1h_2) & = & \varphi^{-1}\left(\varphi(\varphi^{-1}(h_1))\varphi(\varphi^{-1}(h_2))\right) \\ & = & \varphi^{-1}\left(\varphi(\varphi^{-1}(h_1)\varphi^{-1}(h_2))\right) \\ & = & \varphi^{-1}(h_1)\varphi^{-1}(h_2). \end{array}$$

□

Isomorphe Gruppen sind bezüglich ihrer gruppentheoretischen Eigenschaften als gleich anzusehen. Isomorphismen einer Gruppe auf sich selbst nennt man auch *Automorphismen*. Wichtige Beispiele für Automorphismen sind die sogenannten inneren Automorphismen.

Definition 5.8. Sei G eine Gruppe und $g \in G$. Die durch g definierte Abbildung

$$\kappa_g : G \longrightarrow G,\ x \longmapsto gxg^{-1},$$

heißt *innerer Automorphismus*.

Lemma 5.9. *Ein innerer Automorphismus ist in der Tat ein Automorphismus. Die Zuordnung*

$$G \longrightarrow \mathrm{Aut}\ G,\ g \longmapsto \kappa_g,$$

ist ein Gruppenhomomorphismus.

Beweis. Es ist

$$\kappa_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y),$$

so dass ein Gruppenhomomorphismus vorliegt. Wegen

$$\kappa_g(\kappa_h(x)) = \kappa_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \kappa_{gh}$$

ist einerseits

$$\kappa_{g^{-1}} \circ \kappa_g = \kappa_{g^{-1}g} = \mathrm{id}_G,$$

so dass κ_g bijektiv, also ein Automorphismus, ist. Andererseits ist deshalb die Gesamtabbildung κ ein Gruppenhomomorphismus. □

Wenn G eine kommutative Gruppe ist, so ist wegen $gxg^{-1} = xgg^{-1} = x$ die Identität der einzige innere Automorphismus. Der Begriff ist also nur bei nicht kommutativen Gruppen von Interesse.

5.3. **Der Kern eines Gruppenhomomorphismus.**

Definition 5.10. Seien G und H Gruppen und sei

$$\varphi : G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann nennt man das Urbild des neutralen Elementes den *Kern* von φ, geschrieben

$$\text{kern } \varphi = \varphi^{-1}(e_H) = \{g \in G | \, \varphi(g) = e_H\} \, .$$

Lemma 5.11. *Seien G und H Gruppen und sei*

$$\varphi : G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern von φ eine Untergruppe von G.

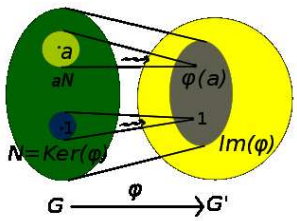
Beweis. Wegen $\varphi(e_G) = e_H$ ist $e_G \in \ker \varphi$. Seien $g, g' \in \ker \varphi$. Dann ist

$$\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$$

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 5.12. *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

$$\varphi(g\tilde{g}^{-1}) = \varphi(g)\varphi(\tilde{g})^{-1} = hh^{-1} = e_H$$

und damit ist $g\tilde{g}^{-1} \in \ker \varphi$, also $g\tilde{g}^{-1} = e_G$ nach Voraussetzung und damit $g = \tilde{g}$. □

5.4. **Das Bild eines Gruppenhomomorphismus.**

Lemma 5.13. *Seien G und H Gruppen und sei $\varphi : G \to H$ 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 5.14. 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 $(\mathbb{C}, \cdot, 1)$ vor. Wir bestimmen den Kern und das Bild dieser Abbildung. Für den Kern muss man diejenigen reellen Zahlen t bestimmen, für die

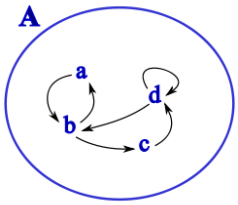
$$\cos t = 1 \text{ und } \sin t = 0$$

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.

6. Vorlesung

Bevor wir die Gruppentheorie weiter entwickeln und insbesondere die Restklassenbildung sinnvoll behandeln können ist es notwendig, einige grundlegende mengentheoretische Konzepte sich klar zu machen, insbesondere das Konzept der Äquivalenzrelation.

6.1. **Relationen auf einer Menge.**



Ein Pfeildiagramm ist eine Möglichkeit, eine Relation darzustellen.

Definition 6.1. Eine *Relation* R auf einer Menge M ist eine Teilmenge der Produktmenge $M \times M$, also $R \subseteq M \times M$.

Wenn ein Paar (x, y) zu R gehört, so sagt man auch, dass x und y in der Relation R stehen. Statt $(x, y) \in R$ verwendet man häufig suggestivere Schreibweisen wie xRy oder $x \sim y$ oder $x \leq y$. Dabei werden manche Symbole nur verwendet, wenn die Relation gewisse zusätzliche Eigenschaften erfüllt. Die wichtigsten Eigenschaften fasst die folgende Definition zusammen.

Definition 6.2. Sei M eine Menge und $R \subseteq M \times M$ eine Relation auf M. Man nennt R

• *reflexiv*, wenn $(x, x) \in R$ gilt für alle $x \in M$.

• *transitiv*, wenn für beliebige $x, y, z \in M$ aus $(x, y) \in R$ und aus $(y, z) \in R$ stets $(x, z) \in R$ folgt.

• *symmetrisch*, wenn für beliebige $x, y \in M$ aus $(x, y) \in R$ auch $(y, x) \in R$ folgt.

• *antisymmetrisch*, wenn für beliebige $x, y \in M$ aus $(x, y) \in R$ und $(y, x) \in R$ die Gleichheit $x = y$ folgt.

6.2. **Ordnungsrelationen.**

Eine reflexive, transitive und antisymmetrische Relation nennt man eine Ordnung, wofür man häufig ein Symbol wie $\geq, \leq, \preccurlyeq, \subseteq$ verwendet.

Definition 6.3. Eine Relation $\preccurlyeq$ auf einer Menge I heißt *Ordnungsrelation* oder *Ordnung*, wenn folgende drei Bedingungen erfüllt sind.

(1) Es ist $i \preccurlyeq i$ für alle $i \in I$.
(2) Aus $i \preccurlyeq j$ und $j \preccurlyeq k$ folgt stets $i \preccurlyeq k$.
(3) Aus $i \preccurlyeq j$ und $j \preccurlyeq i$ folgt $i = j$.

Eine Menge mit einer fixierten Ordnung darauf heißt *geordnete Menge*. Wenn zusätzlich gilt, dass für je zwei Elemente $x \leq y$ oder $y \leq x$ gilt, so spricht man von einer *total geordneten Menge*.

Beispiel 6.4. Die reellen Zahlen $\mathbb{R}$ (ebenso die rationalen Zahlen und die ganzen Zahlen) sind total geordnet durch die *Größergleichrelation* $\geq$. Dies gehört zum Begriff des angeordneten Körpers, der nicht nur verlangt, dass eine totale Ordnung erklärt ist, sondern auch, dass diese mit den algebraischen Operationen verträglich ist. Die strikte *Größerrelation* $>$ ist keine Ordnungsrelation, da sie nicht reflexiv ist. Der Körper der komplexen Zahlen $\mathbb{C}$ ist nicht angeordnet (und lässt sich auch nicht anordnen).

Beispiel 6.5. Wir betrachten die positiven ganzen Zahlen $\mathbb{N}_+$ zusammen mit der Teilbarkeitsbeziehung. Man sagt, dass eine Zahl k die Zahl n teilt, geschrieben

$$k|n\,,$$

wenn es eine weitere natürliche Zahl m gibt mit $n = km$. Die Bezeichnung ist nicht sonderlich glücklich gewählt, da ein symmetrisches Symbol für eine

nichtsymmetrische Relation verwendet wird. Die Teilbarkeitsrelation ist in der Tat reflexiv, da stets $n|n$ ist, wie $m = 1$ zeigt. Die Transitivität sieht man so: sei $k|n$ und $n|m$ mit $n = ak$ und $m = bn$. Dann ist $m = bn = bak$ und daher $k|m$. Die Antisymmetrie folgt so: aus $n = ak$ und $k = bn$ folgt $n = (ab)n$. Da wir uns auf positive natürliche Zahlen beschränken, folgt $ab = 1$ und daraus $a = b = 1$. Also ist $k = n$. Einfache Beispiele wie 2 und 3 zeigen, dass hier keine totale Ordnung vorliegt, da weder 2 von 3 noch umgekehrt geteilt wird.

Beispiel 6.6. Sei X eine beliebige Menge und $M = \mathfrak{P}(X)$ die Potenzmenge davon. Dann sind die Elemente aus $M = \mathfrak{P}(X)$ - also die Teilmengen von X - durch die Inklusionsbeziehung $\subseteq$ geordnet. Die Antisymmetrie ist dabei ein wichtiges Beweisprinzip für die Gleichheit von zwei Mengen: zwei Mengen T_1, T_2 sind genau dann gleich, wenn $T_1 \subseteq T_2$ und umgekehrt $T_2 \subseteq T_1$ gilt.

Beispiel 6.7. Sei X eine Menge (bspw. ein Intervall, oder ein topologischer Raum), so ist die Menge der (stetigen) Funktionen $f : X \to \mathbb{R}$ geordnet, indem man $f \geq g$ dadurch definiert, dass $f(x) \geq g(x)$ sein muss für jeden Punkt $x \in X$. Dies ist offensichtlich keine totale Ordnung.

6.3. **Äquivalenzrelationen.**

Definition 6.8. Eine *Äquivalenzrelation* auf einer Menge M ist eine Relation $R \subseteq M \times M$, die die folgenden drei Eigenschaften besitzt (für beliebige $x, y, z \in M$).

(1) $x \sim x$ (*reflexiv*),
(2) aus $x \sim y$ folgt $y \sim x$ (*symmetrisch*),
(3) aus $x \sim y$ und $y \sim z$ folgt $x \sim z$ (*transitiv*).

Dabei bedeutet $x \sim y$, dass das Paar (x, y) zu R gehört.

Beispiel 6.9. Das Urbeispiel für eine Äquivalenzrelation ist die Gleichheit auf einer beliebigen Menge. Unter der Gleichheit ist jedes Element nur mit sich selbst äquivalent.

Gnus bilden eine Äquivalenzklasse bzgl. der Äquivalenzrelation der Gleichartigkeit, ebenso Zebras.

Beispiel 6.10. Häufig interessiert man sich gar nicht so genau für einzelne Objekte, sondern nur für bestimmte Eigenschaften davon. Objekte, die sich

bezüglich einer bestimmten, genau definierten Eigenschaft gleich verhalten, kann man dann (bzgl. dieser Eigenschaft) als äquivalent betrachten. Offenbar handelt es sich dabei um eine Äquivalenzrelation. Wenn man sich beispielsweise nur für die Farbe von Objekten interessiert, so sind alle Objekte, die (exakt) gleichfarbig sind, äquivalent. Wenn man sich bei Tieren nicht für irgendwelche individuellen Eigenschaften interessiert, sondern nur für ihre Art, so sind gleichartige Tiere äquivalent, d.h. zwei Tiere sind genau dann äquivalent, wenn sie zur gleichen Art gehören. Studierende kann man als äquivalent ansehen, wenn sie die gleiche Fächerkombination studieren. Vektoren kann man als äquivalent ansehen, wenn sie zum Nullpunkt den gleichen Abstand besitzen, etc. Eine Äquivalenzrelation ist also ein bestimmter Blick auf bestimmte Objekte, der unter Bezug auf eine gewisse Eigenschaft gewisse Objekte als gleich ansieht.

Bei den zuletzt genannten „alltäglichen“ Beispielen muss man etwas vorsichtig sein, da im Allgemeinen die Eigenschaften nicht so genau definiert werden. Im Alltag spielt Ähnlichkeit eine wichtigere Rolle als Gleichheit hinsichtlich einer bestimmten Eigenschaft. Die Ähnlichkeit ist aber keine Äquivalenzrelation, da sie zwar reflexiv und symmetrisch ist, aber nicht transitiv. Wenn A und B zueinander (knapp) ähnlich sind und B und C ebenso, so kann A und C schon knapp unähnlich sein (ebenso: lebt in der Nachbarschaft von, ist verwandt mit, etc.).

Die Gleichheit bzgl. einer Eigenschaft wird durch folgende mathematische Konstruktion präzisiert.

Beispiel 6.11. Seien M und N Mengen und sei $f : M \to N$ eine Abbildung. In einer solchen Situation hat man immer eine Äquivalenzrelation auf dem Definitionsbereich M der Abbildung, und zwar erklärt man zwei Elemente $x, y \in M$ als äquivalent, wenn sie unter f auf das gleiche Element abgebildet werden, wenn also $f(x) = f(y)$ ist. Wenn die Abbildung f injektiv ist, so ist die durch f auf M definierte Äquivalenzrelation die Gleichheit. Wenn die Abbildung konstant ist, so sind unter der zugehörigen Äquivalenzrelation alle Elemente aus M untereinander äquivalent.

Zu einer Abbildung $f : M \to N$ nennt man übrigens die Menge aller Punkte $x \in M$, die auf einen bestimmten Punkt $z \in N$ abgebildet werden, die *Faser* über z. Die Äquivalenzklassen (s.u.) sind dann also die Fasern.

Beispiel 6.12. Wir betrachten die *Gaussklammer* (oder den „floor“) einer reellen Zahl, also die Abbildung

$$\lfloor\ \rfloor : \mathbb{R} \longrightarrow \mathbb{Z},\ t \longmapsto \lfloor t \rfloor.$$

Eine Zahl t wird also auf die größte ganze Zahl abgebildet, die kleiner oder gleich t ist (die „Vorkommazahl“). Dabei wird das gesamte ganzzahlige einseitig offene Intervall $[n, n+1)$ auf $n \in \mathbb{Z}$ abgebildet. Bezüglich dieser Abbildung sind also zwei reelle Zahlen genau dann äquivalent, wenn sie im gleichen Intervall liegen.

Statt der Vorkommazahl kann man auch die „Nachkommazahl“ betrachten. Das ist die Abbildung

$$\mathbb{R} \longrightarrow [0,1),\ t \longmapsto t - \lfloor t \rfloor .$$

Unter der durch diese Abbildung definierte Äquivalenzrelation sind zwei reelle Zahlen genau dann gleich, wenn sie die gleiche Nachkommazahl besitzen, und das heißt, wenn ihre Differenz eine ganze Zahl ist.

Unter der Äquivalenzrelation „erreichbar auf dem Landweg“ sind Inseln und Kontinente die Äquivalenzklassen.

Beispiel 6.13. Es sei eine Situation gegeben, wo gewisse Orte (oder Objekte) von gewissen anderen Orten aus erreichbar sind oder nicht. Die Erreichbarkeit kann dabei durch die Wahl eines Verkehrsmittels oder durch eine abstraktere (Bewegungs-)Vorschrift festgelegt sein. Solche Erreichbarkeitsrelationen liefern häufig eine Äquivalenzrelation. Dass ein Ort von sich selbst aus erreichbar ist, sichert die Reflexivität. Die Symmetrie der Erreichbarkeit besagt, dass wenn man von A nach B kommen kann, dass man dann auch von B nach A kommen kann. Das ist nicht für jede Erreichbarkeit selbstverständlich, für die meisten aber schon. Die Transitivität gilt immer dann, wenn man die Bewegungsvorgänge hintereinander ausführen kann, also zuerst von A nach B und dann von B nach C.

Wenn erreichbar bspw. dadurch gegeben ist, dass man auf dem Landweg von einem Ort zu einem anderen kommen kann, so sind zwei Ortspunkte genau dann äquivalent, wenn sie auf der gleichen Insel (oder dem gleichen Kontinent) liegen. Inseln und Kontinente sind dann die Äquivalenzklassen. In der Topologie spielt der Begriff des Wegzusammenhangs eine wichtige Rolle: zwei Punkte sind wegzusammenhängend, wenn man sie durch einen stetigen Weg verbinden kann. Oder: auf den ganzen Zahlen lebe eine Kolonie von Flöhen, und jeder Flohsprung geht fünf Einheiten weit (in beide Richtungen). Wie viele Flohpopulationen gibt es, welche Flöhe können sich begegnen?

6.4. Äquivalenzklassen, Quotientenmenge, kanonische Abbildung.

Eine Äquivalenzrelation $R \subseteq M \times M$ auf einer Menge M kann auch als Zerlegung der Menge M aufgefasst werden. Hierzu ist der Begriff der *Äquivalenzklasse* nützlich.

Definition 6.14. Sei $R \subseteq X \times X$ eine Äquivalenzrelation und $x \in X$. Dann ist $[x] := \{y \in X : (x, y) \in R\}$ die *Äquivalenzklasse* von x bezüglich R. Es ist $[x] \subseteq X$.

In Worten: $[x]$ ist die Teilmenge aller Elemente von M, die zu x äquivalent sind.

Definition 6.15. Sei $R \subseteq X \times X$ eine Äquivalenzrelation. Dann ist

$$X/R := \big\{[x] : x \in X\big\}$$

die *Quotientenmenge* von R.

Definition 6.16. Sei $R \subseteq X \times X$ eine Äquivalenzrelation und X/R die Quotientenmenge. Die Abbildung $q_R : X \to X/R$, die $x \in X$ auf $[x] \in X/R$ abbildet, heißt *kanonische Projektion* von R.

Lemma 6.17. *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M mit den Äquivalenzklassen $[x]$ und der Quotientenmenge $M/\sim$. Dann gelten folgende Aussagen.*

(1) *Es ist $x \sim y$ genau dann, wenn $[x] = [y]$ ist, und dies gilt genau dann, wenn $[x] \cap [y] \neq \emptyset$.*
(2) *$M = \bigcup_{x \in M/\sim} [x]$ ist eine disjunkte Vereinigung.*
(3) *Die kanonische Projektion $q : M \to M/\sim$ ist surjektiv.*
(4) *Es ist $q^{-1}([x]) = [x]$.*
(5) *Sei $f : M \to W$ eine Abbildung mit $f(x) = f(y)$ für alle $x, y \in M$ mit $x \sim y$. Dann gibt es eine eindeutig bestimmte Abbildung $\overline{\varphi} : M/\sim \to W$ mit $\overline{\varphi} = \varphi \circ q$.*

Beweis. (1) Seien x und y äquivalent und $u \in [x]$. Dann ist $x \sim u$ und nach der Transitivität auch $y \sim u$, also $u \in [y]$. Damit stimmen die Äquivalenzklasssen überein. Die Implikationen von der Mitte nach rechts ist klar, da wegen $x \sim x$ Äquivalenzklassen nicht leer sind. Sei nun $[x] \cap [y] \neq \emptyset$, und sei z ein Element im Durchschnitt. Dann ist $x \sim z$ und $y \sim z$ und wegen der Transitivität ist $x \sim y$.

(2) Wegen der Reflexivität ist $x \in [x]$ und daher ist $M = \bigcup_{[x] \in X/R} [x]$. Wegen Teil (1) ist die Vereinigung disjunkt.

(3) Die Surjektivität ist klar aufgrund der Definition der Quotientenmenge, und da x auf die Klasse $[x]$ geschickt wird.

(4) Es ist

$$\begin{aligned} q^{-1}([x]) &= \{y \in M \,|\, q(y) = [x]\} \\ &= \{y \in M \,|\, [y] = [x]\} \end{aligned}$$

$$\begin{aligned} &= \{y \in M |\, y \sim x\} \\ &= [x]. \end{aligned}$$

(5) Sei $[x] \in M/\sim$ gegeben. Die einzige Möglichkeit für $\overline{\varphi}$ ist $\overline{\varphi}([x]) = \varphi(x)$ zu setzen. Es muss aber gezeigt werden, dass diese Abbildung überhaupt wohldefiniert ist, also unabhängig von der Wahl des Repräsentanten ist. Sei hierzu $[x] = [y]$, also $x \sim y$. Dann ist nach der Voraussetzung an φ aber $\varphi(x) = \varphi(y)$.

□

Beispiel 6.18. Sei $n \in \mathbb{N}$ und $X = \mathbb{R}^{n+1} \setminus \{0\}$. Der $\mathbb{R}^{n+1}$ ist ein reeller Vektorraum, wobei die Skalarmultiplikation von $\lambda \in \mathbb{R}$ und $x \in \mathbb{R}^{n+1}$ mit $\lambda \cdot x$ bezeichnet wird. Sei weiter

$$R := \{(x, y) \in X \times X : \text{ es gibt ein } \lambda \in \mathbb{R} \setminus \{0\} \text{ mit } \lambda \cdot x = y\}.$$

Zwei Punkte werden also also äquivalent erklärt, wenn sie durch Skalarmultiplikation mit einem Skalar $\lambda \neq 0$ ineinander überführt werden können. Ebenso könnte man sagen, dass zwei Punkte als äquivalent gelten, wenn sie dieselbe Gerade durch den Nullpunkt definieren.

Dass wirklich eine Äquivalenzrelation vorliegt, sieht man so. Die Reflexivität folgt aus $x = 1x$ für jedes $x \in X$. Zur Symmetrie sei xRy, d.h. es gibt $\lambda \neq 0$ mit $\lambda x = y$. Dann gilt aber auch $y = \lambda^{-1}x$, da ja λ invertierbar ist. Zur Transitivität sei xRy und yRz angenommen, d.h. es gibt $\lambda, \delta \neq 0$ mit $\lambda x = y$ und $\delta y = z$. Dann ist insgesamt $z = \delta y = (\delta\lambda)x$ mit $\delta\lambda \neq 0$. Die Äquivalenzklassen zu dieser Äquivalenzrelation sind die einzelnen Geraden durch den Nullpunkt (aber ohne den Nullpunkt). Die Quotientenmenge heißt *reell-projektiver Raum* (der reellen Dimension n) und wird mit $\mathbb{P}^n_{\mathbb{R}}$ bezeichnet.

7. Vorlesung

7.1. **Nebenklassen.**

Definition 7.1. 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 7.2. 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 bzgl. 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

$$\begin{aligned}[x] &= \{y \in G | \, x \sim y\} \\ &= \{y \in G | \, x^{-1}y \in H\} \\ &= \{y \in G | \, \text{es gibt } h \in H \text{ mit } x^{-1}y = h\} \\ &= \{y \in G | \, \text{es gibt } h \in H \text{ mit } y = xh\} \\ &= xH\end{aligned}$$

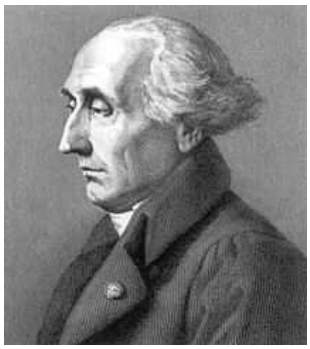
genau die Linksnebenklassen. Die Linksnebenklassen bilden somit eine disjunkte Zerlegung (eine *Partition*) von G. Dies gilt ebenso für die Rechtsnebenklassen. Im kommutativen Fall muss man nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

Lemma 7.3. *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 äquivalent. Da die Nebenklassen Äquivalenzklassen sind, ergibt sich die Äquivalenz von (5) und (7). □

7.2. **Der Satz von Lagrange.**



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Satz 7.4. *(Satz von Lagrange)*

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. □

Korollar 7.5. *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 2.3 ist $\operatorname{ord}(g) = \operatorname{ord}(H)$. Daher teilt diese Zahl nach Satz 7.4 die Gruppenordnung von G. □

Definition 7.6. 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*

$$\#(G) = \#(H) \cdot \operatorname{ind}_G H \, .$$

7.3. **Normalteiler.**

Definition 7.7. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Man nennt H einen *Normalteiler*, wenn

$$xH = Hx$$

ist für alle $x \in G$, 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*. Die Gleichheit $xH = Hx$ bedeutet *nicht*, dass $xh = hx$ ist für alle $h \in H$, sondern lediglich, dass es zu jedem $h \in H$ ein $\tilde{h} \in H$ gibt mit $xh = \tilde{h}x$. Statt xH oder Hx schreiben wir meistens $[x]$.

Lemma 7.8. *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 $xh = \tilde{h}x$ schreiben kann mit einem $\tilde{h} \in H$. 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 7.9. 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 7.10. *Seien G und H Gruppen und sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist der Kern $\ker\varphi$ ein Normalteiler in G.*

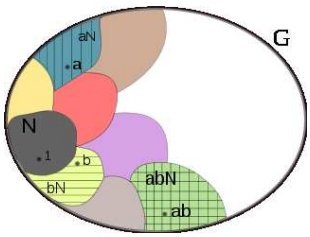
Beweis. Wir verwenden Lemma 7.8. Sei also $x \in G$ beliebig und $h \in \ker\varphi$. Dann ist

$$\varphi(xhx^{-1}) = \varphi(x)\varphi(h)\varphi(x^{-1}) = \varphi(x)e_H\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = e_H,$$

also gehört xhx^{-1} ebenfalls zum Kern. □

7.4. **Restklassenbildung.**

Wir zeigen nun umgekehrt, dass jeder Normalteiler sich als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt.



Die Multiplikation der Nebenklassen zu einem Normalteiler $N \subseteq G$.

Satz 7.11. *Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Es sei G/H die Menge der Nebenklassen (die Quotientenmenge) und*

$$q : G \longrightarrow G/H,\ g \longmapsto [g],$$

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 $hy' = \tilde{h}y = yh'$ schreiben mit $h, \tilde{h}, h' \in H$. 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 7.12. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 7.11 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 7.13. Die Untergruppen der ganzen Zahlen sind nach Satz 3.2 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.

8. Vorlesung

8.1. **Homomorphie- und Isomorphiesatz.**

Satz 8.1. *Seien G, Q und H Gruppen, es sei $\varphi : G \to H$ ein Gruppenhomomorphismus und $\psi : G \to Q$ 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. φ 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 8.2. *Seien G und H Gruppen und sei $\varphi : G \to H$ ein surjektiver Gruppenhomomorphismus. Dann gibt es eine kanonische Isomorphie*

$$\tilde{\varphi} : G/\operatorname{kern} \varphi \longrightarrow H.$$

Beweis. Wir wenden Satz 8.1 auf $Q = G/\operatorname{kern}\varphi$ und die kanonische Projektion $q : G \to G/\operatorname{kern}\varphi$ an. Dies induziert einen Gruppenhomomorphismus

$$\tilde{\varphi} : G/\operatorname{kern}\varphi \longrightarrow H$$

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 5.12 ist $\tilde{\varphi}$ auch injektiv. □

Satz 8.3. *Seien G und H Gruppen und sei $\varphi : G \to H$ 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 8.2 angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 8.4. *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 7.7. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

$$p \circ q : G \longrightarrow Q \longrightarrow Q/\overline{H}\,.$$

Wegen

$$\begin{aligned}\operatorname{kern}\, p \circ q &= \{x \in G |\, p \circ q(x) = e\}\\ &= \{x \in G |\, q(x) \in \operatorname{kern}\, p\}\\ &= \{x \in G |\, q(x) \in \overline{H}\}\\ &= H\end{aligned}$$

ist $\operatorname{kern}\, p \circ q = H$. Daher ergibt Korollar 8.2 die kanonische Isomorphie

$$G/H \longrightarrow Q/\overline{H}.$$

□

Kurz gesagt ist also

$$G/H = (G/N)/(H/N)\,.$$

8.2. **Permutationsgruppen.**

Seien M_1, M_2, M_3, M_4 Mengen und es seien Abbildungen

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} M_4$$

gegeben. Dann ist es egal, ob man die Hintereinanderschaltung der drei Abbildungen als $\varphi_3 \circ (\varphi_2 \circ \varphi_1)$ oder als $(\varphi_3 \circ \varphi_2) \circ \varphi_1$ auffasst. Das ist die natürliche Assoziativität für Abbildungen.

Definition 8.5. Sei M eine beliebige Menge. Dann ist die Menge

$$\mathrm{Abb}\,(M) = \mathrm{Abb}\,(M, M)$$

der Abbildungen von M in sich mit der Hintereinanderschaltung von Abbildungen als Verknüpfung und mit der Identität als neutralem Element ein Monoid, das man das *Abbildungsmonoid* zu M nennt.

Definition 8.6. Zu einer Menge M nennt man die Menge

$$\mathrm{Aut}\,(M) = \mathrm{Perm}\,(M) = \{\varphi : M \longrightarrow M | \, \varphi \text{ bijektiv}\}$$

der bijektiven Selbstabbildungen die *Automorphismengruppe* oder die *Permutationsgruppe* zu M.

Eine bijektive Selbstabbildung $\varphi : M \to M$ nennt man auch eine *Permutation*. Für eine endliche Menge $I = \{1, \ldots, n\}$ schreibt man $S_n = \mathrm{Perm}\,(I)$. Wir werden uns hauptsächlich auf endliche Permutationsgruppen beschränken. Eine endliche Permutation kann man bspw. mit einer (vollständigen) Wertetabelle oder mit einem Pfeildiagramm beschreiben.

Lemma 8.7. *Sei M eine endliche Menge mit n Elementen. Dann besitzt die Permutationsgruppe* $\mathrm{Perm}\,(M) \cong S_n$ *genau $n!$ Elemente.*

Beweis. Es sei $M = \{1, \ldots, n\}$. Für die 1 gibt es n mögliche Bilder, für 2 gibt es noch $n-1$ mögliche Bilder, für 3 gibt es noch $n-2$ mögliche Bilder, usw. Daher gibt es insgesamt

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

mögliche Permutationen. □

Lemma 8.8. *Sei M eine Menge und $N \subseteq M$ eine Teilmenge. Dann gibt es eine natürliche injektive Abbildung*

$$\mathrm{Perm}\,(N) \longrightarrow \mathrm{Perm}\,(M),\ \sigma \longmapsto \tilde{\sigma},$$

wobei $\tilde{\sigma}$ auf N gleich σ und auf $M \setminus N$ die Identität ist. Mittels dieser Abbildung ist $\mathrm{Perm}\,(N)$ *eine Untergruppe von* $\mathrm{Perm}\,(M)$.

Beweis. Offenbar ist die Abbildung wohldefiniert. Sie ist injektiv, da aus $\tilde{\sigma} = \tilde{\tau}$ sofort folgt, dass $\sigma = \tau$ ist. Die Abbildung liefert eine Bijektion zwischen $\mathrm{Perm}\,(N)$ und der Menge der Permutationen auf M, die $M \setminus N$ fest lassen. Diese Permutationen bilden eine Untergruppe. □

Bemerkung 8.9. Das vorstehende Lemma besagt bei $M = \{1, \ldots, n\}$ und $N = \{1, \ldots, n-1\}$, dass $S_{n-1} \subseteq S_n$ eine Untergruppe ist. Diese Untergruppe ist bei $n \geq 3$ kein Normalteiler. Sie hat den Index n, woraus sich erneut durch Induktion ergibt, dass die Permutationsgruppe S_n die Ordnung $n!$ besitzt.

Permutationsgruppen tauchen in vielen unterschiedlichen Situationen auf, und zwar häufig dann, wenn man sich die Wirkungsweise einer Gruppe auf einem geometrischen Objekt anschaut, wie im folgenden Beispiel (Zykel und Transposition werden sofort definiert).

Beispiel 8.10. Wir betrachten die Gruppe der eigentlichen Bewegungen an einem Würfel. Für eine fixierte Raumdiagonale W betrachten wir die Untergruppe H derjenigen Bewegungen, die diese Raumdiagonale in sich überführen. Das sind einerseits die drei Drehungen um diese Achse um $0, 120, 240$ Grad, andererseits aber auch die drei Halbdrehungen um diejenigen Kantenmittelpunktsachsen, deren Kanten nicht an den Ecken von W anliegen. Diese drei Halbdrehungen führen ebenfalls W in sich über, wobei allerdings die Eckpunkte vertauscht werden.

Es seien B, G und R die drei anderen Raumdiagonalachsen. Dann definiert jede Bewegung aus H eine Permutation der Menge $\{B, G, R\}$. Die beiden Dritteldrehungen definieren dabei die beiden Zykel $\langle B, G, R\rangle$ und $\langle B, R, G\rangle$, und die drei Halbdrehungen definieren jeweils eine Transposition. Damit ist H isomorph zu S_3 und somit ist S_3 eine Untergruppe der Würfelgruppe.

8.3. **Zykeldarstellung für Permutationen.**

Sei M eine endliche Menge, $\sigma \in \mathrm{Perm}\,(M)$ eine Permutation und $x \in M$. Dann kann man die Folge

$$\sigma^0(x) = \mathrm{id}\,(x) = x,\ \sigma^1(x) = \sigma(x),\ \sigma^2(x),\ \sigma^3(x) \ldots,$$

betrachten. Da M endlich ist, gibt es eine Wiederholung $\sigma^i(x) = \sigma^j(x)$ mit $i < j$. Durch Multiplikation mit σ^{-i} sieht man, dass es ein minimales $k \in \mathbb{N}_+$ gibt mit $\sigma^k(x) = \sigma^0(x) = x$, und dass alle $\sigma^j(x)$ für j, $1 \leq j < k$, verschieden sind. Ist $y = \sigma^j(x)$, so durchläuft auch $\sigma^i(y)$ dieselbe Teilmenge aus M.

Definition 8.11. Sei M eine endliche Menge und σ eine Permutation auf M. Man nennt σ einen *Zykel der Ordnung* r, wenn es eine r-elementige Teilmenge $Z \subseteq M$ gibt derart, dass σ auf $M \setminus Z$ die Identität ist und σ die Elemente aus Z zyklisch vertauscht. Wenn $Z = \{z, \sigma(z),\ \sigma^2(z), \ldots, \sigma^{r-1}(z)\}$ ist, so schreibt man einfach

$$\sigma = \langle z, \sigma(z),\ \sigma^2(z), \ldots, \sigma^{r-1}(z)\rangle\,.$$

Dabei kann man statt z jedes andere Element aus Z als Anfangsglied nehmen. Die Menge Z heißt auch der *Wirkungsbereich* des Zykels, und die (geordnete) Auflistung heißt die *Wirkungsfolge* des Zykels.

Definition 8.12. Eine *Transposition* auf einer endlichen Menge M ist eine Permutation auf M, die genau zwei Elemente miteinander vertauscht und alle anderen Elemente unverändert lässt.

Eine Transposition ist also ein besonders einfacher Zykel mit der Zyklendarstellung $\langle x, y\rangle$, wenn die Transposition die Punkte x und y vertauscht.

Lemma 8.13. *Jede Permutation auf einer endlichen Menge M kann man als Produkt von Transpositionen schreiben.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl der Menge M. Für $\#(M) = 1$ ist nichts zu zeigen, sei also $\#(M) \geq 2$. Die Identität ist das leere Produkt aus Transpositionen. Sei also σ nicht die Identität, und sei $\sigma(x) = y \neq x$. Es sei τ die Transposition, die x und y vertauscht. Dann ist y ein Fixpunkt von $\sigma\tau$, und man kann $\sigma\tau$ auffassen als eine Permutation auf $M' = M \setminus \{y\}$. Nach Induktionsvoraussetzung gibt es dann Transpositionen τ_j auf M' mit $\sigma\tau = \prod_j \tau_j$ auf M'. Dies gilt dann auch auf M, und daher ist $\sigma = \prod_j \tau_j\tau$. □

Satz 8.14. *Sei M eine endliche Menge und σ eine Permutation auf M. Dann gibt es eine Darstellung*

$$\sigma = \sigma_1 \cdots \sigma_k \,,$$

wobei die σ_i Zykel der Ordnung ≥ 2 sind mit disjunkten Wirkungsbereichen. Dabei ist die Darstellung bis auf die Reihenfolge eindeutig.

Beweis. Es sei F die Fixpunktmenge von σ und es seien $Z_1, \ldots, Z_k$ diejenigen Teilmengen von M mit mindestens zwei Elementen derart, dass σ die Elemente aus jedem Z_i zyklisch vertauscht. Dann ist M die disjunkte Vereinigung aus F und den Z_i. Zu i, $1 \leq i \leq k$ sei σ_i der Zykel auf M, der auf $M \setminus Z_i$ die Identität ist und auf Z_i mit σ übereinstimmt. Wir behaupten

$$\sigma = \sigma_1 \cdots \sigma_k \,.$$

Um dies einzusehen, sei $x \in M$ beliebig. Bei $x \in F$ ist x ein Fixpunkt für alle σ_i und daher kommt links und rechts wieder x raus. Sei also x kein Fixpunkt der Permutation. Dann gehört $x \in Z_i$ für genau ein i. Für alle $j \neq i$ ist x ein Fixpunkt von σ_j. Da $y = \sigma(x)$ ebenfalls zu Z_i gehört, ist auch y ein Fixpunkt von σ_j für alle $j \neq i$. Wendet man daher die rechte Seite auf x an, so wird x auf x abgebildet bis man zu σ_i kommt. Dieses bildet x auf y ab und die folgenden σ_j bilden y auf y ab, so dass die rechte Seite insgesamt x auf y schickt und daher mit σ übereinstimmt. □

Aufgrund von diesem Satz können wir allgemein eine Zyklendarstellung für eine beliebige Permutation definieren.

Definition 8.15. Sei M eine endliche Menge und σ eine Permutation auf M. Es seien $Z_1, \ldots, Z_k$ die Wirkungsbereiche der Zyklen von σ mit $n_i = \#(Z_i)$. Es sei $x_i \in Z_i$ und $Z_i = \{x_i, \sigma(x_i), \ldots, \sigma^{n_i-1}(x_i)\}$. Dann nennt man

$$\langle x_1, \sigma(x_1), \ldots, \sigma^{n_1-1}(x_1)\rangle\langle x_2, \sigma(x_2), \ldots, \sigma^{n_2-1}(x_2)\rangle \cdots \langle x_k, \sigma(x_k), \ldots, \sigma^{n_k-1}(x_k)\rangle$$

die *Zyklendarstellung* von σ.

Diese Schreibweise ist wie in Satz 8.14 zu verstehen, dass also σ das Produkt der k Zykel ist, die jeweils durch ihre Wirkungsfolge angegeben werden.

9. Vorlesung

9.1. Das Signum einer Permutation.

Definition 9.1. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Dann heißt die Zahl

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

das *Signum* (oder das *Vorzeichen*) der Permutation σ.

Das Signum ist 1 oder -1, da im Zähler und im Nenner die positive oder die negative Differenz $\pm(i - j)$ steht. Es gibt für das Signum also nur zwei mögliche Werte. Bei $\operatorname{sgn}(\sigma) = 1$ spricht man von einer *geraden Permutation* und bei $\operatorname{sgn}(\sigma) = -1$ von einer *ungeraden Permutation*.

Definition 9.2. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Dann heißt ein Indexpaar $i < j$ ein *Fehlstand*, wenn $\sigma(i) > \sigma(j)$ ist.

Lemma 9.3. *Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Es sei $k = \#(F)$ die Anzahl der Fehlstände von σ. Dann ist das Signum von σ gleich*

$$\operatorname{sgn}(\sigma) = (-1)^k .$$

Beweis. Wir schreiben

$$\begin{aligned}
\operatorname{sgn}(\sigma) &= \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \prod_{(i,j)\in F} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{(i,j)\notin F} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= (-1)^k \prod_{(i,j)\in F} \frac{\sigma(i) - \sigma(j)}{j - i} \prod_{(i,j)\notin F} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= (-1)^k,
\end{aligned}$$

da nach dieser Umordnung sowohl im Zähler als auch im Nenner das Produkt aller positiven Differenzen steht. □

Beispiel 9.4. Wir betrachten die Permutation

x	1	2	3	4	5	6
$\sigma(x)$	2	4	6	5	3	1

mit der Zyklendarstellung

$$\langle 124536 \rangle .$$

Die Fehlstände sind

$$(1,6),\ (2,5),\ (2,6),\ (3,4),\ (3,5),\ (3,6),\ (4,5),\ (4,6),\ (5,6)\,,$$

also 9 Stück. Das Signum ist also $(-1)^9 = -1$ und die Permutation ist ungerade.

Satz 9.5. *Sei $M = \{1, \ldots, n\}$. Dann ist die Zuordnung*

$$S_n \longrightarrow \{1, -1\},\ \sigma \longmapsto \operatorname{sgn}(\sigma),$$

ein Gruppenhomomorphismus.

Beweis. Zunächst ist das Signum wirklich gleich 1 oder -1. Dies beruht darauf, dass sowohl im Zähler als auch im Nenner der Definition des Signums zu jedem Indexpaar $i \leq j$ die positive oder die negative Differenz $\pm(i-j)$ vorkommt.

Das Signum der Identität ist natürlich 1. Seien zwei Permutationen σ und τ gegeben. Dann ist

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \prod_{i<j} \frac{(\sigma\circ\tau)(j) - (\sigma\circ\tau)(i)}{j-i} \\
&= \Big(\prod_{i<j} \frac{(\sigma\circ\tau)(j) - (\sigma\circ\tau)(i)}{\tau(j)-\tau(i)}\Big) \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \Big(\prod_{i<j,\,\tau(i)<\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)}\Big)\Big(\prod_{i<j,\,\tau(i)>\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)}\Big)\ \operatorname{sgn}(\tau) \\
&= \Big(\prod_{i<j,\,\tau(i)<\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)}\Big)\Big(\prod_{i<j,\,\tau(i)>\tau(j)} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)}\Big)\ \operatorname{sgn}(\tau) \\
&= \prod_{k<\ell} \frac{\sigma(\ell)-\sigma(k)}{\ell-k} \operatorname{sgn}(\tau) \\
&= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).
\end{aligned}$$

□

Lemma 9.6. *Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Es sei*

$$\sigma = \tau_1 \cdots \tau_r$$

geschrieben als ein Produkt von r Transpositionen. Dann gilt für das Signum die Darstellung

$$\operatorname{sgn}(\sigma) = (-1)^r\,.$$

Beweis. Die Transposition τ vertausche die beiden Zahlen $k < \ell$. Dann ist

$$\begin{aligned}
\operatorname{sgn}(\tau) &= \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{i,j\neq k,\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i=k,j\neq\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i\neq k,j=\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i=k,j=\ell} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{j>k,\, j\neq\ell} \frac{j-\ell}{j-k} \cdot \prod_{i\neq k,\, i<\ell} \frac{k-i}{\ell-i} \cdot \frac{k-\ell}{\ell-k} \\
&= \prod_{j>\ell} \frac{j-\ell}{j-k} \cdot \prod_{i<k} \frac{k-i}{\ell-i} \cdot \prod_{k<j<\ell} \frac{j-\ell}{j-k} \cdot \prod_{k<i<\ell} \frac{k-i}{\ell-i} \cdot (-1) \\
&= -1.
\end{aligned}$$

Die letzte Gleichung ergibt sich daraus, dass im ersten und im zweiten Produkt alle Zähler und Nenner positiv sind und dass im dritten und im vierten Produkt die Zähler negativ und die Nenner positiv sind, so dass sich diese (wegen der gleichen Indexmenge) Minuszeichen wegkürzen.

Die Aussage folgt dann aus der Gruppeneigenschaft. □

Bemerkung 9.7. Es sei I eine beliebige Menge mit n Elementen, die nicht geordnet sein muss. Dann kann man nicht von Fehlständen sprechen und die Definition des Signums ist nicht direkt anwendbar. Man kann sich jedoch an Lemma 9.12 orientieren, um das Signum auch in dieser leicht allgemeineren Situation zu erklären. Dazu schreibt man eine Permutation σ auf I als Produkt von r Transpositionen und definiert

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 \text{ falls } r \text{ gerade ist} \\ -1 \text{ falls } r \text{ ungerade ist.} \end{cases}$$

Um einzusehen, dass dies wohldefiniert ist, betrachtet man eine Bijektion

$$\varphi : I \longrightarrow \{1, \ldots, n\}.$$

Die Permutation σ auf I definiert auf $\{1, \ldots, n\}$ die Permutation $\sigma' = \varphi\sigma\varphi^{-1}$. Sei $\sigma = \tau_1 \cdots \tau_r$ eine Darstellung als Produkt von r Transpositionen auf I. Dann gilt

$$\sigma' = \varphi\sigma\varphi^{-1} = \varphi\tau_1 \cdots \tau_r\varphi^{-1} = \varphi\tau_1\varphi^{-1}\varphi\tau_2\varphi^{-1}\varphi \cdots \varphi^{-1}\varphi\tau_r\varphi^{-1} = \tau_1'\tau_2' \cdots \tau_r'$$

mit $\tau_j' = \varphi\tau_j\varphi^{-1}$. Dies sind ebenfalls Transpositionen, sodass die Parität von r durch das Signum von σ' festgelegt ist.

9.2. **Die alternierende Gruppe.**

Für $n \geq 2$ ist die Signumsabbildung $\operatorname{sgn} : S_n \to \{1, -1\}$ ein surjektiver Gruppenhomomorphismus, da ja Transpositionen auf -1 abgebildet werden. Der Kern dieses Homomorphismus besteht aus allen geraden Permutationen und ist ein Normalteiler in der Permutationsgruppe S_n. Diese Untergruppe bekommt einen eigenen Namen.

Definition 9.8. Zu $n \in \mathbb{N}$ heißt die Untergruppe

$$A_n = \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\} \subseteq S_n$$

der geraden Permutationen die *alternierende Gruppe*.

Die alternierende Gruppe besitzt ($n \geq 2$) den Index zwei, die beiden Nebenklassen sind die geraden Permutationen und die ungeraden Permutationen.

Für $n = 1, 2$ ist die alternierende Gruppe die triviale Gruppe. Für $n = 3$ ist $A_3 = \mathbb{Z}/(3)$. Die Gruppe A_4 ist isomorph zur Tetraedergruppe.

Beispiel 9.9. Wir betrachten die alternierende Gruppe A_4. Die vier Permutationen (in Zykeldarstellung)

$$\mathrm{id},\ \langle 1,2\rangle\langle 3,4\rangle,\ \langle 1,3\rangle\langle 2,4\rangle,\ \langle 1,4\rangle\langle 2,3\rangle$$

bilden darin eine kommutative Untergruppe V, in der jedes Element $\neq \mathrm{id}$ die Ordnung 2 besitzt. Sie ist isomorph zur Kleinschen Vierergruppe. Es handelt sich sogar um einen Normalteiler vom Index drei. Um dies einzusehen verwenden wir Lemma 7.8 und betrachten exemplarisch $\sigma = \langle 1,2\rangle\langle 3,4\rangle$ und $\tau = \langle 1,2,3\rangle$ mit dem Inversen $\tau^{-1} = \langle 1,3,2\rangle$. Wir erhalten

$$\langle 1,2,3\rangle\langle 1,2\rangle\langle 3,4\rangle\langle 1,3,2\rangle = \langle 1,4\rangle\langle 2,3\rangle\,,$$

was wieder zu V gehört. Die Restklassengruppe A_4/V muss isomorph zu $\mathbb{Z}/(3)$ sein, die beiden anderen (neben V) Nebenklassen sind einerseits die Dreierzykel

$$N = \langle 2,3,4\rangle,\ \langle 1,4,3\rangle,\ \langle 1,2,4\rangle,\ \langle 1,3,2\rangle$$

und andererseits die dazu inversen Dreierzykel

$$\langle 2,4,3\rangle,\ \langle 1,3,4\rangle,\ \langle 1,4,2\rangle,\ \langle 1,2,3\rangle\,.$$

Wenn man einen Tetraeder mit nummerierten Ecken anschaut, so entsprechen diese beiden Nebenklassen den Dritteldrehungen im Uhrzeigersinn oder entgegen dem Uhrzeigersinn um die Seiteneckachsen, wobei die Drehrichtung dadurch festgelegt ist, dass man auf den Eckpunkt schaut (welche Orientierung zu welcher Nebenklasse gehört, hängt dabei von der Nummerierung der Ecken ab).

Die Gruppe A_4 besitzt also einen nicht-trivialen Normalteiler. Sie ist damit unter den alternierenden Gruppen eine Ausnahme. Es gilt nämlich, und das werden wir hier nicht beweisen, dass die alternierenden Gruppen A_n, $n \geq 5$ einfach sind im Sinne der folgenden Definition.

Definition 9.10. Eine Gruppe heißt *einfach*, wenn sie genau zwei Normalteiler enthält (nämlich sich selbst und die triviale Gruppe).

Für eine Primzahl p sind die zyklischen Gruppen $\mathbb{Z}/(p)$ der Ordnung p einfach, da es in diesen Gruppen aufgrund des Satzes von Lagrange überhaupt nur die triviale und die ganze Gruppe als Untergruppe gibt. In einer nicht

kommutativen einfachen Gruppe gibt es im Allgemeinen sehr viele Untergruppen, aber eben keine nicht-trivialen Normalteiler. Die einfachen Gruppen sind in gewissem Sinne die einfachsten Bausteine für alle endlichen Gruppen. Die nicht einfachen Gruppen sind in einem gewissen Sinn „zusammengesetzt“, da es dort dann einen echten Normalteiler $N \subset G$, $N \neq 0, \neq G$ gibt und damit auch eine Restklassengruppe $G/N = Q$. Die Gruppe G ist dann aus den kleineren Gruppen N und Q irgendwie „zusammengebastelt“, wobei allerdings N und Q nicht die Struktur von G festlegen. Die Klassifikation aller einfachen endlichen Gruppen war ein schwieriges Problem der Gruppentheorie und ist inzwischen (seit ca. 1980) gelöst.

9.3. **Die Determinante.**

Wir erinnern noch kurz an die Determinante, die aus der Anfängervorlesung bekannt ist. Mittels Permutationen und deren Signa kann man eine geschlossene Definition für die Determinante geben. Zur Berechnung sind aber rekursive Verfahren sinnvoller.

Definition 9.11. Zu einer $n \times n$-Matrix

$$M = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ . & \dots & . \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

heißt

$$\det M = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

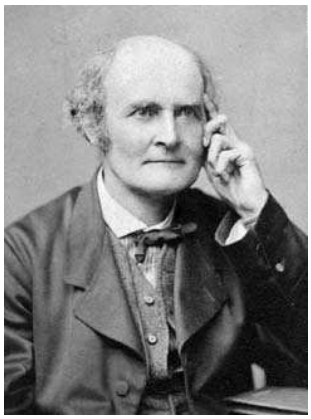
die *Determinante* von M.

9.4. **Der Satz von Cayley.**

Zu einer Gruppe G und einem Element $g \in G$ nennt man die Abbildung

$$L_g : G \longrightarrow G,\ x \longmapsto gx$$

die *Linksmultiplikation* mit g. Das ist in aller Regel *kein* Gruppenhomomorphismus, allerdings ist es eine bijektive Abbildung der Menge G in sich. Dieser Zusammenhang wird nun kurz thematisiert.



Arthur Cayley (1821-1895)

Lemma 9.12. *Sei G eine Gruppe und* $\mathrm{Perm}\,(G)$ *die Gruppe der Bijektionen auf G. Dann ist die Abbildung, die einem Gruppenelement die Linksmultiplikation zuordnet, also*

$$G \longrightarrow \mathrm{Perm}\,(G),\ g \longmapsto L_g,$$

ein injektiver Gruppenhomomorphismus.

Beweis. Die Linksmultiplikation ist eine Bijektion auf G, da aus $gx = gy$ durch Multiplikation von links mit g^{-1} sofort $x = y$ folgt. Wegen $ex = x$ geht das neutrale Element auf die Identität. Ferner ist für jedes $x \in G$

$$L_{g\tilde{g}}(x) = (g\tilde{g})x = g(\tilde{g}x) = g(L_{\tilde{g}}(x)) = L_g(L_{\tilde{g}}(x)) = (L_g L_{\tilde{g}})(x),$$

was $L_{g\tilde{g}} = L_g L_{\tilde{g}}$ bedeutet. Daher ist die Zuordnung ein Gruppenhomomorphismus. Zur Injektivität verwenden wir Lemma 5.12. Es sei also $L_g = \mathrm{id}\,$. Dann ist aber sofort

$$g = ge = L_g(e) = \mathrm{id}\,(e) = e.$$

□

Satz 9.13. *(Satz von Cayley)*

Jede Gruppe lässt sich als Untergruppe einer Permutationsgruppe realisieren. Jede endliche Gruppe lässt sich als Untergruppe einer endlichen Permutationsgruppe realisieren.

Beweis. Dies folgt sofort aus Lemma 5.12. □

Bemerkung 9.14. Es gilt sogar, dass mit Ausnahme der Identität jede Linksmultiplikation fixpunktfrei ist. D.h. die Untergruppe der Permutationen, die isomorph zur vorgegebenen Gruppe ist, besitzt außer der Identität nur fixpunktfreie Abbildungen. Dies folgt aus $gx = L_g(x) = x$ durch Multiplikation mit x^{-1} von rechts.

Beispiel 9.15. Sei $G = \mathbb{Z}/(n)$ eine zyklische Gruppe, repräsentiert durch die Elemente $\{0, 1, \ldots, n-1\}$. Das Einselement 1 erzeugt die Gruppe, das muss dann auch für die zu G isomorphe Untergruppe von S_n gelten. Die Linksaddition mit 1 ist die Zuordnung

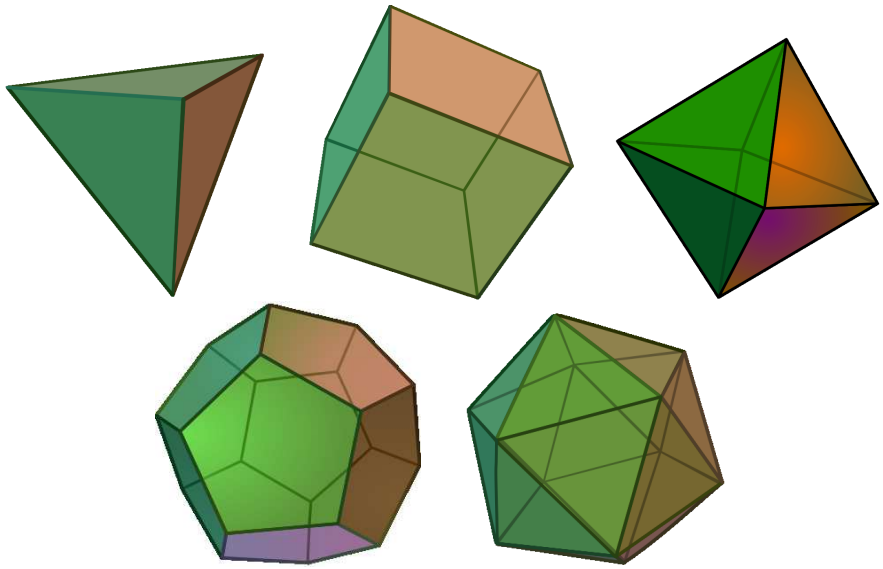
$$0 \mapsto 1,\ 1 \mapsto 2,\ 2 \mapsto 3, \ldots, n-2 \mapsto n-1,\ n-1 \mapsto 0\,.$$

Das ist also ein Zykel der Ordnung n. Das Element k geht auf die k-fache Hintereinanderausführung dieses Zykels.

10. Vorlesung

10.1. **Bewegungen.**

Wir haben schon mehrfach die Würfelgruppe betrachtet, also die Gruppe der eigentlichen Symmetrien an einem Würfel. Jeder dieser Symmetrien ist insbesondere eine abstandserhaltende lineare Abbildung des umgebenden Raumes um eine eindeutig bestimmte Drehachse. Die Gesamtmenge der abstandserhaltenden linearen (eigentlichen)Abbildungen des Raumes bildet die sogenannte *orthogonale Gruppe* O_3 (bzw. SO_3). Dies ist natürlich eine sehr große, unendliche Gruppe. Interessant ist aber, dass die endlichen Untergruppen darin übersichtlich beschrieben werden können. Diese endlichen Untergruppen lassen sich stets als Symmetriegruppe zu einem geeigneten geometrischen Objekt auffassen. Dass eine einfache Klassifikation dieser endlichen Bewegungsgruppen möglich ist, beruht auf intrinsischen Struktureigenschaften des Raumes und liefert unter Anderem eine präzise Version dafür, dass es nur fünf reguläre Polyder (die *platonischen Körper*) gibt.



Für die folgenden Überlegungen benötigen wir etwas lineare Algebra, insbesondere den Begriff des euklidischen Vektorraumes, siehe die Kurzübersicht auf der Kursseite unter „weitere Materialien“.

Definition 10.1. Eine lineare Abbildung

$$\varphi : V \longrightarrow V$$

auf einem euklidischen Vektorraum V heißt *Isometrie*, wenn für alle $v, w \in V$ gilt:

$$\langle \varphi(v), \varphi(w) \rangle = \langle v, w \rangle \, .$$

Definition 10.2. Eine Isometrie auf einem euklidischen Vektorraum heißt *eigentlich*, wenn ihre Determinante gleich 1 ist.

Die Gruppe, die aus allen Isometrien von V besteht, heißt *orthogonale Gruppe* zu V, und die eigentlichen Isometrien bilden die *spezielle orthogonale Gruppe*. Bei $V = \mathbb{R}^n$ schreibt man dafür

$$\mathrm{O}_n \text{ bzw. } \mathrm{SO}_n \, .$$

Satz 10.3. *Sei V ein euklidischer Vektorraum und sei*

$$\varphi : V \longrightarrow V$$

eine lineare Isometrie. Dann besitzt jeder Eigenwert von φ den Betrag 1.

Beweis. Es sei $\varphi(v) = \lambda v$ mit $v \neq 0$, d.h. v ist ein Eigenvektor zum Eigenwert λ. Wegen der Isometrieeigenschaft gilt

$$|| \, v \, || = || \, \varphi(v) \, || = || \, \lambda v \, || = \, |\lambda| \cdot || \, v \, || \, .$$

Wegen $|| \, v \, || \neq 0$ folgt daraus $|\lambda| = 1$, also $\lambda = \pm 1$. □

Im Allgemeinen muss es keine Eigenwerte geben (bei ungerader Dimension allerdings schon). Wir besprechen zunächst den zweidimensionalen Fall ausführlicher.

10.2. **Bewegungen in der Ebene.**

Satz 10.4. *Sei*

$$\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

eine eigentliche lineare Isometrie. Dann ist φ eine Drehung, und ihre Matrix hat die Gestalt

$$D(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} .$$

mit einem eindeutig bestimmten Drehwinkel $\theta \in [0, 2\pi)$.

Beweis. Es seien (x, y) und (u, v) die Bilder der Einheitsvektoren $(1, 0)$ und $(0, 1)$. Unter einer Isometrie wird die Länge eines Vektors erhalten, daher ist

$$|| \begin{pmatrix} x \\ y \end{pmatrix} ||= \sqrt{x^2 + y^2} = 1 \, .$$

Daher ist x eine reelle Zahl zwischen -1 und $+1$ und $y = \pm\sqrt{1 - x^2}$, d.h. (x, y) ist ein Punkt auf dem reellen Einheitskreis. Der Einheitskreis wird bekanntlich durch die trigonometrischen Funktionen parametrisiert, d.h. es gibt einen eindeutig bestimmten Winkel θ, $0 \leq \theta < 2\pi$, mit

$$(x, y) = (\cos \theta, \sin \theta) \, .$$

Da unter einer Isometrie die Senkrechtsbeziehung erhalten bleibt, muss

$$\langle \begin{pmatrix} x \\ y \end{pmatrix} , \begin{pmatrix} u \\ v \end{pmatrix} \rangle \; = \; xu + yv \; = \; 0$$

gelten. Bei $y = 0$ folgt daraus (wegen $x = \pm 1$) $u = 0$. Dann ist $v = \pm 1$ und wegen der Eigentlichkeit muss das Vorzeichen positiv sein. Sei also $y \neq 0$. Dann gilt

$$\begin{pmatrix} -v \\ u \end{pmatrix} = \frac{u}{y} \begin{pmatrix} x \\ y \end{pmatrix} \, .$$

Da die zwei Vektoren die Länge 1 haben, muss der skalare Faktor u/y den Betrag 1 haben. Bei $u = y$ wäre $v = -x$ und die Determinante wäre -1. Also muss $u = -y$ und $v = x$ sein, was die Behauptung ergibt. □

Satz 10.5. *Sei $G \subset \mathrm{SO}_2$ eine endliche Untergruppe der linearen Bewegungsgruppe der reellen Ebene. Dann ist G eine zyklische Gruppe.*

Beweis. Jedes Element aus G ist nach Satz 10.4 eine Drehung der Ebene um einen bestimmten Winkel θ. Wir betrachten den surjektiven Gruppenhomomorphismus

$$\mathbb{R} \longrightarrow \mathrm{SO}_2 \, , \, \theta \longmapsto D(\theta),$$

der einen Winkel auf die zugehörige Drehung abbildet. Es sei $H \subseteq \mathbb{R}$ das Urbild von G unter dieser Abbildung, d.h. H besteht aus allen Drehwinkeln zu Drehungen, die zu G gehören. Die Gruppe H wird von einem Repräsentantensystem für die Elemente aus G zusammen mit 2π erzeugt. Insbesondere ist also H eine endlich erzeugte Untergruppe von $\mathbb{R}$. Da jedes Gruppenelement aus G eine endliche Ordnung besitzt, muss jedes $\theta \in H$ die Gestalt $\theta = 2\pi q$ mit einer rationalen Zahl $q \in \mathbb{Q}$ haben. Dies bedeutet, dass H eine endlich erzeugte Untergruppe von $2\pi\mathbb{Q} \subseteq \mathbb{R}$ ist. Damit ist H isomorph zu einer endlich erzeugten Untergruppe der rationalen Zahlen. Nach Aufgabe 3.9 ist H zyklisch, sagen wir $H = \mathbb{Z}\alpha$ mit einem eindeutig bestimmten Winkel $\alpha \in [0, 2\pi)$. Dann ist die Gruppe G als Bild von H ebenfalls zyklisch. □

Wenn man auch noch uneigentliche Symmetrien, also Isometrien mit der Determinante -1 (etwa Achsenspiegelungen) zulässt, so gibt es noch eine weitere Familie von endlichen Untergruppen der O_2, nämlich die Diedergruppen.

Definition 10.6. Zu einem regelmäßigen n-Eck ($n \geq 3$) heißt die Gruppe der eigentlichen oder uneigentlichen linearen Symmetrien die *Diedergruppe* D_n.

Die Diedergruppe besteht aus den Drehungen des n-Ecks und aus den Achsenspiegelungen an den folgenden Achsen durch den Nullpunkt: bei n gerade die Achsen durch gegenüberliegende Eckpunkte und gegenüberliegende Kantenmittelpunkte, bei n ungerade die Achsen durch einen Eckpunkt und einen gegenüberliegenden Kantenmittelpunkt. In beiden Fällen besteht die Diedergruppe aus $2n$ Elementen.

10.3. **Bewegungen im Raum.**

Satz 10.7. *Sei*

$$\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine Isometrie. Dann gibt es einen Eigenvektor zum Eigenwert 1 *oder* -1.

Beweis. Das charakteristische Polynom P zu φ ist ein normiertes Polynom vom Grad drei. Für $t \mapsto +\infty$ geht $P(t) \mapsto +\infty$ und für $t \mapsto -\infty$ geht $P(t) \mapsto -\infty$. Nach dem Zwischenwertsatz besitzt daher P mindestens eine Nullstelle. Eine solche Nullstelle ist ein Eigenwert von φ. Nach Satz 10.3 ist der Eigenwert gleich 1 oder gleich -1. □

Satz 10.8. *Eine eigentliche Isometrie*

$$\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

besitzt einen Eigenvektor zum Eigenwert eins, d.h. es gibt eine Gerade (durch den Nullpunkt), die unter φ *fest bleibt.*

Beweis. Wir betrachten das charakteristische Polynom von φ, also

$$P(\lambda) = \det(\lambda E_3 - \varphi).$$

Dies ist ein normiertes reelles Polynom vom Grad drei. Für $\lambda = 0$ ergibt sich

$$P(0) \;=\; \det(-\varphi) \;=\; -\det(\varphi) \;=\; -1.$$

Da für $\lambda \mapsto \infty$ das Polynom $P(\lambda) \mapsto \infty$ geht, muss es für ein positives λ eine Nullstelle geben. Aufgrund von Satz 10.3 kommt dafür nur $\lambda = 1$ in Frage. □

Lemma 10.9. *Sei*

$$\varphi : V \longrightarrow V$$

eine lineare Isometrie und sei $U \subseteq V$ *ein invarianter Unterraum. Dann ist auch das orthogonale Komplement* $U^\perp$ *invariant. Insbesondere kann man* φ *schreiben als direkte Summe*

$$\varphi = \varphi_U \oplus \varphi_{U^\perp},$$

wobei die Einschränkungen φ_U *und* $\varphi_{U^\perp}$ *ebenfalls Isometrien sind.*

Beweis. Es ist

$$U^\perp = \{v \in V | \langle v, u\rangle = 0 \text{ für alle } u \in U\}\,.$$

Für ein solches $v \in U^\perp$ und ein beliebiges $u \in U$ ist

$$\langle \varphi(v), u\rangle \;=\; \langle \varphi^{-1}(\varphi(v)), \varphi^{-1}(u)\rangle \;=\; \langle v, u'\rangle \;=\; 0,$$

da $u' = \varphi^{-1}(u) \in U$ liegt wegen der Invarianz. Also ist wieder $\varphi(v) \in U^\perp$. □

Satz 10.10. *Sei*

$$\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine eigentliche Isometrie. Dann ist φ eine Drehung um eine feste Achse. Das bedeutet, dass φ in einer geeigneten Orthonormalbasis durch eine Matrix der Form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

beschrieben wird.

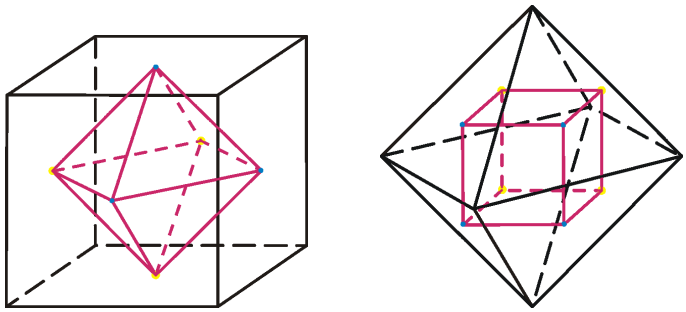
Beweis. Nach Satz 10.8 gibt es einen Eigenvektor u zum Eigenwert 1. Sei $U = \mathbb{R}u$ die davon erzeugte Gerade. Diese ist fix und insbesondere invariant unter φ. Nach Lemma 10.9 ist dann auch das orthogonale Komplement $U^\perp$ invariant unter φ, d.h. es gibt eine lineare Isometrie

$$\varphi_2 : U^\perp \longrightarrow U^\perp\,,$$

die auf $U^\perp$ mit φ übereinstimmt. Dabei muss φ_2 eigentlich sein, und daher muss nach Satz 10.4 φ_2 eine Drehung sein. Wählt man einen Vektor der Länge eins aus U und dazu eine Orthonormalbasis von $U^\perp$, so hat φ bzgl. dieser Basis die angegebene Gestalt. □

10.4. **Halbachsensysteme.**

Es sei $G \subseteq \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien. Jedes Element $g \in G$, $g \neq \mathrm{id}$, ist eine Drehung um eine eindeutig bestimmte Drehachse A. Insbesondere sind an einer endlichen Symmetriegruppe nur endlich viele Drehachsen beteiligt. Jedes Gruppenelement bewirkt dann eine Permutation der Drehachsenmenge, und diese Bedingung schränkt die möglichen Gruppen wesentlich ein. Eine Drehachse zerfällt in zwei Halbachsen, und es ist sinnvoll, die Wirkungsweise der Gruppe auf diesen Halbachsen zu untersuchen.



Bei einem Würfel gibt es drei verschiedene Arten von Drehachsen: es gibt drei Drehachsen, die durch die Seitenmittelpunkte gegeben sind, vier Drehachsen, die durch die Eckpunkte gegeben sind und sechs Drehachsen, die durch die Kantenmittelpunkte gegeben sind. Betrachtet man alle *Durchstoßungspunkte* dieser Achsen mit der Sphäre vom Radius eins, so ergeben sich $6 + 8 + 12 = 26$ Punkte. Diese Punkte entsprechen den *Halbachsen*. Dabei gibt es zu je zwei Eckpunkten (bzw. den zugehörigen Durchstoßungspunkten) (mindestens) eine Würfelbewegung, die sie ineinander überführt, ebenso zu je zwei Kantenmittelpunkten und zu je zwei Seitenmittelpunkten. Jede Bewegung permutiert diese charakteristischen Punkte. Wenn man eine Achse (oder einen Durchstoßungspunkt) fixiert, so kann man die Menge der Bewegungen betrachten, die diese Achse als Drehachse haben. Es kann natürlich auch die Achse zwar auf sich selbst abgebildet werden, aber nicht fix sein. Dann werden die gegenüberliegenden Durchstoßungspunkte ineinander überführt.

Definition 10.11. Es sei $G \subseteq \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien im $\mathbb{R}^3$. Dann nennt man jede Gerade durch den Nullpunkt, die als Drehachse eines Elementes $g \neq \mathrm{id}$ auftritt, eine *Achse* von G. Die Halbgeraden dieser Drehachsen nennt man die *Halbachsen* der Gruppe und die Gesamtmenge dieser Halbachsen nennen wir das zu G gehörige *Halbachsensystem*. Es wird mit $\mathfrak{H}(G)$ bezeichnet. Zwei Halbachsen $H_1, H_2 \in \mathfrak{H}(G)$ heißen *äquivalent*, wenn es ein $g \in G$ gibt mit $g(H_1) = H_2$. Die Äquivalenzklassen zu dieser Äquivalenzrelation nennt man *Halbachsenklassen*.

Da jede von id verschiedene Drehung genau eine Drehachse hat, ist das Halbachsensystem zu einer endlichen Symmetriegruppe endlich (und zwar ist die Anzahl maximal gleich $2(\mathrm{ord}\,(G)-1)$). Wenn H eine Halbachse ist und $g \in G$, so ist auch $g(H)$ eine Halbachse: wenn nämlich $h \in G$ die durch H definierte Achse als Drehachse besitzt, so ist

$$(ghg^{-1})(g(H)) = (gh)((gg^{-1})(H)) = (gh)(H)) = g(h(H)) = g(H).$$

Mit „äquivalenten Halbachsen“ ist also wirklich eine Äquivalenzrelation definiert.

Beispiel 10.12. Beim Würfel werden die Halbachsen repräsentiert durch die Eckpunkte, die Seitenmittelpunkte und die Kantenmittelpunkte. Diese drei

Arten bilden dann auch die Äquivalenzklassen, also die Halbachsenklassen. Der Vergleich mit dem Oktaeder zeigt, dass die Sprechweise mit den Halbachsen für die Bewegungsgruppe als solche angemessener ist als die Sprechweise mit Ecken, Kanten, Mittelpunkten.

Beispiel 10.13. Bei einem Tetraeder gibt es vier Eck-Seitenmittelpunkt-Achsen und vier Kantenmittelpunktachsen. Die Kantenmittelpunkthalbachsen sind dabei alle untereinander äquivalent, während die zuerst genannten Achsen in zwei Halbachsenklassen zerfallen, nämlich die Eckhalbachsen und die Seitenhalbachsen.

An diesem Beispiel sieht man auch, dass die beiden durch eine Drehachse gegebenen Halbachsen nicht zueinander äquivalent sein müssen.

11. Vorlesung

11.1. Numerische Bedingungen für endliche Symmetriegruppen im Raum.

Lemma 11.1. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$. Zu einer Halbachse H von G sei*

$$G_H = \{g \in G | \, g(H) = H\}\,.$$

Dann sind für zwei äquivalente Halbachsen H_1 und H_2 die Gruppen G_{H_1} und G_{H_2} isomorph. Insbesondere besitzen sie die gleiche Ordnung.

Beweis. Es sei $g(H_1) = H_2$, was es gibt, da die beiden Halbachsen nach Voraussetzung äquivalent sind. Dann hat man aber sofort den Gruppenisomorphismus

$$G_{H_1} \longrightarrow G_{H_2},\ f \longmapsto g \circ f \circ g^{-1}.$$

Wegen

$$(gfg^{-1})(H_2) = gf(g^{-1}(H_2)) = gf(H_1) = g(H_1) = H_2$$

führt dieser innere Automorphismus von G in der Tat die beiden Gruppen ineinander über. □

Bei G_H handelt es sich trivialerweise um eine Untergruppe von G. Man nennt sie die *Isotropiegruppe* zur Halbachse H. Das Lemma besagt also, dass äquivalente Halbachsen isomorphe Isotropiegruppen besitzen. Wenn $n = \#(G)$ ist und H eine Halbachse in der Halbachsenklasse K, und die Untergruppe G_H k Elemente besitzt, so gibt es in K genau n/k verschiedene Halbachsen. Die fixierte Halbachse H definiert nämlich eine surjektive Abbildung

$$G \longrightarrow K,\ f \longmapsto f(H).$$

Dabei geht $f \in G_H$ auf H, und ebenso gibt es für jede Halbachse $H' \in K$ genau k Urbilder.

Lemma 11.2. *Es sei $G \subseteq \mathrm{SO}_3$ eine endliche Untergruppe der Ordnung n in der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$. Es seien $K_1, \ldots, K_m$ die verschiedenen Halbachsenklassen zu G, und zu jeder dieser Klassen sei n_i, $i = 1, \ldots, m$, die Ordnung der Gruppe G_H, $H \in K_i$, die nach Lemma 11.1 unabhängig von $H \in K_i$ ist. Dann ist*

$$2(1 - \frac{1}{n}) = \sum_{i=1}^{m} (1 - \frac{1}{n_i})$$

Beweis. Für zwei gegenüberliegende Halbachsen H und $-H$ gilt $G_H = G_{-H}$. Dagegen gilt für zwei Halbachsen H_1 und H_2, die nicht zur gleichen Achse gehören (also insbesondere verschieden sind), die Beziehung $G_{H_1} \cap G_{H_2} = \{\mathrm{id}\}$, da eine Isometrie mit zwei Fixachsen die Identität sein muss. Da G die Vereinigung aller G_H, $H \in \mathfrak{H}(G)$, ist, liegt eine Vereinigung

$$G - \{\mathrm{id}\} = \bigcup_{H \in \mathfrak{H}(G)} (G_H - \{\mathrm{id}\})$$

vor, wobei rechts jedes Gruppenelement $g \neq \mathrm{id}$ genau zweimal vorkommt. Daher ist

$$2(n-1) = \sum_{H \in \mathfrak{H}(G)} (\mathrm{ord}\,(G_H) - 1)\,.$$

Die Halbachsenklasse K_i enthält n/n_i Elemente. Daher ist

$$2(n-1) \;=\; \sum_{H \in \mathfrak{H}(G)} (\mathrm{ord}\,(G_H) - 1) \;=\; \sum_{i=1}^{m} \frac{n}{n_i}(n_i - 1).$$

Mittels Division durch n ergibt sich die Behauptung. □

Lemma 11.3. *Die numerische Gleichung*

$$2(1 - \frac{1}{n}) = \sum_{i=1}^{m} (1 - \frac{1}{n_i})$$

mit $n \geq 2$, $m \in \mathbb{N}$ und mit $2 \leq n_1 \leq n_2 \leq \ldots \leq n_m$ besitzt folgende Lösungen.

(1) *$m = 2$ und $n = n_1 = n_2$.*
(2) *Bei $m = 3$ gibt es die Möglichkeiten*
   (a) *$n_1 = n_2 = 2$ und $n = 2n_3$,*
   (b) *$n_1 = 2$, $n_2 = n_3 = 3$ und $n = 12$,*
   (c) *$n_1 = 2$, $n_2 = 3$, $n_3 = 4$ und $n = 24$,*
   (d) *$n_1 = 2$, $n_2 = 3$, $n_3 = 5$ und $n = 60$.*

Beweis. Bei $m = 0$ ist die rechte Seite null und daher folgt $n = 1 < 2$ aus der linken Seite. Bei $m = 1$ muss gelten $n_1 = \frac{n}{-n+2}$, was bei $n \geq 2$ keine Lösung besitzt. Bei $m = 2$ erhält man die Bedingung

$$\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2}\,,$$

woraus sich $n_1 = n_2 = n$ ergibt. Bei $m = 3$ schreibt sich die Bedingung als

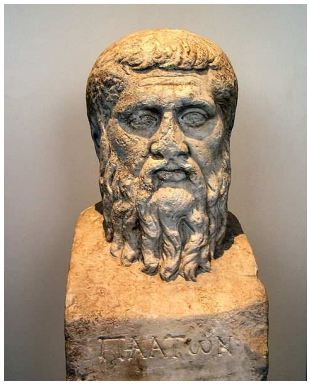
$$1 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

mit $n_1 \leq n_2 \leq n_3$. Die linke Seite ist > 1. Daher muss wegen $n_i \geq 2$ mindestens eines der $n_i = 2$ sein. Sei also $n_1 = 2$. Bei $n_2 = 2$ gibt es genau die Lösung $n = 2n_3$ mit beliebigem $n_3 \geq 2$. Sei also $n_2 \geq 3$. Bei $n_2 \geq 4$ wäre die rechte Seite wieder ≤ 1, so dass $n_2 = 3$ gelten muss. Der Wert $n_3 = 3$ führt zur Lösung $n = 12$, der Wert $n_3 = 4$ führt zur Lösung $n = 24$ und der Wert $n_3 = 5$ führt zur Lösung $n = 60$. Bei $n_3 \geq 6$ wird die rechte Seite wieder ≤ 1, so dass es keine weitere Lösung gibt. Bei $m \geq 4$ hat man eine Bedingung der Form

$$m - 2 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4} + \ldots + \frac{1}{n_m},$$

die keine Lösung besitzt, da die rechte Seite $\leq m - 2$ ist, da die ersten vier Summanden maximal 2 ergeben und die weiteren durch $m - 4$ abgeschätzt werden können. □

11.2. **Geometrische Realisierungen der endlichen Symmetriegruppen.**



Plato (427-347 v. C.) sagte: „die Bedeutung der Geometrie beruht nicht auf ihrem praktischen Nutzen, sondern darauf, daß sie ewige und unwandelbare Gegenstände untersucht und danach strebt, die Seele zur Wahrheit zu erheben“.

Das letzte Lemma enthält die entscheidenden numerischen Bedingungen, wie eine endliche Symmetriegruppe im $\mathbb{R}^3$ aussehen kann. Wenn man von der trivialen Gruppe absieht, bei der $m = 0$ gilt, so erfasst dieses Lemma alle endlichen Gruppen, da bei $m \geq 1$ für jedes i die Gruppe der Drehungen an einer Achse schon mindestens zwei Elemente besitzt. Jede der angegebenen Bedingungen lässt sich im Wesentlichen eindeutig durch eine endliche Symmetriegruppe realisieren. Das geometrische Objekt ist aber nicht eindeutig bestimmt, wie schon das „duale Paar“ Würfel und Oktaeder zeigen.

Lemma 11.4. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ mit einer fixierten Halbachsenklasse K. Dann ist die Abbildung*

$$G \longrightarrow \mathrm{Perm}\,(K),\ g \longmapsto \sigma_g : H \mapsto g(H),$$

ein Gruppenhomomorphismus.

Beweis. Nach der Definition von Halbachsenklasse ist mit $H \in K$ auch $g(H) \in K$ für alle $g \in G$. Daher ist die Abbildung σ wohldefiniert. Die Identität geht auf die Identität. Seien $f, g \in G$. Dann ist sofort

$$\sigma_{g \circ f}(H) = (g \circ f)(H) = g(f(H)) = g(\sigma_f(H)) = \sigma_g(\sigma_f(H)) = (\sigma_g \circ \sigma_f)(H).$$

□

Lemma 11.5. *Es sei $G \subseteq \mathrm{SO}_3$ eine endliche Untergruppe der Ordnung n der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ mit zwei verschiedenen Halbachsenklassen zu G. Dann ist G die zyklische Gruppe der Drehungen zum Winkel $2\pi/n$ um eine einzige fixierte Drehachse.*

Beweis. Aufgrund von Lemma 11.2 und Lemma 11.3 muss $n = n_1 = n_2$ sein und jede Halbachsenklasse enthält nur eine Halbachse. Daher gibt es überhaupt nur eine Drehachse und diese Bewegungsgruppe ist isomorph zu einer Bewegungsgruppe in der senkrechten Ebene, also nach Satz 10.5 isomorph zur zyklischen Gruppe der Ordnung n. □

In diesem Fall gibt es also zwei Halbachsenklassen, die jeweils aus nur einer Halbachse bestehen.

Lemma 11.6. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2, 2, k)$. Dann ist G isomorph zur Diedergruppe D_k.*

Beweis. Es gibt drei Halbachsenklassen, und zwar zwei mit der Ordnung zwei (und je k Halbachsen) und eine mit der Ordnung k und 2 Halbachsen (die Anzahlen der Halbachsen folgen mit $n_1 = n_2 = 2$ aus Lemma 11.3). Bei $k \geq 3$ müssen die zwei Halbachsen aus der dritten Klasse zueinander äquivalent sein, und bei $k = 2$ muss jede Halbachse zu ihrem Gegenüber äquivalent sein. Wir bezeichnen die Achse zu K_3 mit A_3. Jedes Gruppenelement mit einer anderen Drehachse muss die beiden Halbachsen aus K_3 ineinander überführen, so dass alle anderen Achsen senkrecht zu A_3 stehen. Es sei g eine erzeugende Drehung um A_3. Zu einer Halbachse H_1 aus K_1 sind die

$$g^i(H_1),\ i = 0, \ldots, k-1\,,$$

genau alle Halbachsen aus K_1. Diese bilden ein regelmäßiges k-Eck in der zu A_3 senkrechten Ebene. Entsprechendes gilt für $g^i(H_2)$ mit $H_2 \in K_2$. Jede Halbdrehung um eine der Achsen aus K_1 überführt die Halbachsen aus K_2 in ebensolche. Daher liefern die Halbachsen aus K_2 eine „Halbierung“ des k-Ecks. Somit handelt es sich insgesamt um die (uneigentliche) Symmetriegruppe eines regelmäßigen k-Ecks, d.h. um eine Diedergruppe D_k. □

In diesem Fall bestehen die beiden Halbachsenklassen der Ordnung zwei einerseits aus den Eckpunkten (oder Eckhalbachsen) und andererseits aus den

Seitenmittelpunkten (oder Seitenmittelhalbachsen) des zugrunde liegenden regelmäßigen $n/2$-Ecks. Bei $n/2$ gerade sind gegenüberliegende Halbachsen äquivalent, bei $n/2$ ungerade nicht. Bei $n = 4$ ist die Diedergruppe (also D_2) kommutativ und isomorph zur Kleinschen Vierergruppe.

Lemma 11.7. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2,3,3)$. Dann ist G die Tetraedergruppe und damit isomorph zur alternierenden Gruppe A_4.*

Beweis. Nach Voraussetzung gibt es drei Halbachsenklassen der Ordnung $2,3$ und 3, ihre Anzahl ist daher $6,4$ und 4. Betrachten wir eine Halbachsenklasse K der Ordnung 3 mit ihren vier äquivalenten Halbachsen und den zugehörigen Gruppenhomomorphismus ()

$$G \longrightarrow \mathrm{Perm}\,(K),\ g \longmapsto \sigma_g.$$

Sei $g \in G$ eine Dritteldrehung um eine Halbachse $H \in K$. Sie lässt H fest und bewirkt eine Permutation der drei anderen Halbachsen in der Klasse. Diese Permutation kann nicht die Identität sein, da sonst g mindestens zwei Achsen fest ließe und damit g die (Raum-)Identität wäre. Da g die Ordnung 3 besitzt, muss diese Permutation ein Dreierzykel sein. Insbesondere gehören die vier Halbachsen zu verschiedenen Achsen, und die Doppeldrehung g^2 bewirkt den anderen Dreierzykel. Da man diese Überlegung mit jeder der vier Halbachsen anstellen kann, sieht man, dass G sämtliche Dreierzykel der Permutationsgruppe der vier Halbachsen bewirkt. Das Bild des Gruppenhomomorphismus ist daher genau die alternierende Gruppe A_4 und damit ist $G \cong A_4$. Diese ist nach Aufgabe 10.5 isomorph zur Tetraedergruppe. □

In der vorstehenden Aussage kann man auch direkt erkennen, dass es sich um eine Tetradergruppe handeln muss. Dazu markieren wir auf jeder der vier Halbachsen den Punkt mit dem Abstand 1 zum Nullpunkt. Aus dem Beweis des Lemmas folgt, dass je zwei solche Punkte den gleichen Abstand voneinander haben (und dass die Winkel der Halbachsen zueinander alle gleich sind). Daher bilden diese vier Punkte die Eckpunkte eines Tetraeders. Die gegenüberliegenden Halbachsen entsprechen den Seitenmittelpunkten der Tetraederflächen. Das Halbachsensystem der Ordnung zwei enthält die Halbachsen zu den Drehachsen der Komposition von zwei Dritteldrehungen um zwei verschiedene Achsen. Diese Halbachsen entsprechen den Kantenmittelpunkten.

Lemma 11.8. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$ vom Typ $(2,3,4)$. Dann ist G die Würfelgruppe und damit isomorph zur Permutationsgruppe S_4.*

Beweis. Wir betrachten die Halbachsenklasse K der Ordnung drei, die also 8 zueinander äquivalente Halbachsen besitzt. Zu einer solchen Halbachse H muss die entgegengesetzte Halbachse ebenfalls in einer der Halbachsenklassen liegen, und zwar in einer mit der gleichen Ordnung. Daher gehört auch $-H$

zu K, so dass an K insgesamt vier Achsen beteiligt sind. Die Menge dieser Achsen nennen wir $\mathfrak{A}$. Wir betrachten den Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}\,(\mathfrak{A}),\ g \longmapsto \sigma_g : A \mapsto g(A).$$

Hier wird also nur geschaut, was mit den Achsen passiert, nicht mit den Halbachsen. Es können nicht drei dieser vier Achsen in einer Ebene liegen. Wären nämlich $A_1, A_2, A_3 \subset E$, so würde eine Dritteldrehung f um A_1 die äquivalenten Achsen $f(A_2)$ und $f(A_3)$ hervorbringen, die aber nicht in der Ebene E liegen können und die nicht beide gleich A_4 sein können. Das Element $g \in G$ habe die Eigenschaft, dass σ_g die Identität ist, dass also alle Geraden $A \in \mathfrak{A}$ auf sich abgebildet werden. Nach Aufgabe 11.5 muss g die Identität sein. Der Gruppenhomomorphismus ist also nach Lemma 5.12 injektiv und daher muss eine Isomorphie vorliegen. □

Mit einem ähnlichen, aber aufwändigeren Argument kann man zeigen, dass die verbleibende numerische Möglichkeit, also eine Gruppe mit 60 Elementen und mit den Klassenordnungen $2, 3$ und 5 wieder nur von einem Isomorphietyp realisiert wird, nämlich von der alternierenden Gruppe A_5, die zugleich isomorph zur Dodekaedergruppe und zur Ikosaedergruppe ist.

Insgesamt haben wir (bis auf den Ikosaederfall) den folgenden Hauptsatz über endliche (eigentliche) Symmetriegruppen im Raum bewiesen.

Satz 11.9. *Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$. Dann ist G eine der folgenden Gruppen.*

(1) *Eine zyklische Gruppe $(\mathbb{Z}/(n))$,*
(2) *Eine Diedergruppe (D_k),*
(3) *Die Tetraedergruppe (A_4),*
(4) *Die Würfelgruppe (S_4),*
(5) *Die Ikosaedergruppe (A_5).*

12. Vorlesung

12.1. **Ringe.**

Wir beginnen einen neuen Abschnitt dieser Vorlesung, in dem es um Ringe geht.

Definition 12.1. 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 12.2. 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 (im Arbeitsblatt zu den Peano-Axiomen stehen die wichtigsten Beweisschritte). 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 $a \in R$ bzgl. 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 $na = a + \ldots + a$ (n Summanden) und $a^n = a \cdots a$ (n Faktoren). Bei negativen $n \in \mathbb{Z}$ ist $na = (-n)(-a)$ zu interpretieren (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 12.3. 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 12.4. 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

$*$	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).

Lemma 12.5. *Sei R ein Ring und seien a, b, c, a_i, b_k 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.

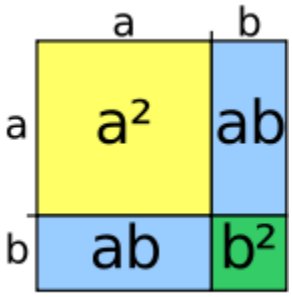
(1) Es ist $a0 = a(0+0) = a0 + a0$. Durch beidseitiges Abziehen von $a0$ ergibt sich die Behauptung.
(2)
$$(-a)b + ab = (-a+a)b = 0b = 0$$
nach Teil (1). Daher ist $(-a)b$ das (eindeutig bestimmte) Negative von ab.
(3) Nach (2) ist $(-a)(-b) = (-(-a))b$ und wegen $-(-a) = a$ (dies gilt in jeder Gruppe)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

□

12.2. **Die Binomialkoeffizienten.**

Definition 12.6. Es seien k und n natürliche Zahlen mit $k \le n$. Dann nennt man
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$
den *Binomialkoeffizienten* „n über k“.

Wenn $k > n$ ist oder wenn k negativ ist so setzt man den Binomialkoeffizienten gleich null.



Satz 12.7. *(Binomischer Lehrsatz)*

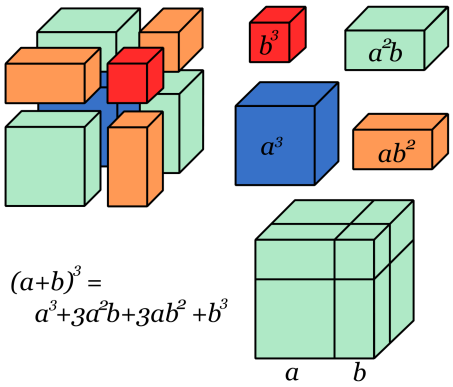
Es sei R ein kommutativer Ring und $a, b \in R$. Ferner sei n eine natürliche Zahl. Dann gilt

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

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

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

□



12.3. **Nichtnullteiler und Integritätsbereiche.**

Definition 12.8. Ein Element a in einem kommutativen Ring R heißt *Nullteiler*, wenn es ein von null verschiedenes Element b gibt mit $ab = 0$. Andernfalls heißt es ein *Nichtnullteiler*.

Im nicht kommutativen Fall hat man zwischen Links- und Rechtsnullteilern zu unterscheiden. 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.

Lemma 12.9. *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 umschreiben als

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

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 12.10. 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.

12.4. **Unterringe.**

Definition 12.11. 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. Wir haben die Kette von Unterringen

$$\mathbb{Z} \subset \mathbb{Q} \subseteq \mathbb{R} \subset \mathbb{C}\,.$$

12.5. **Endomorphismenringe.**

Definition 12.12. Es sei $(G, 0, +)$ eine kommutative Gruppe. Dann nennt man

$$\operatorname{End} G = \{\varphi : G \to G |\, \varphi \text{ ist ein Gruppenhomomorphismus}\}$$

den *Endomorphismenring* zu G. Er wird mit der *Addition*

$$(\varphi + \psi)(x) := \varphi(x) + \psi(x)$$

und der Hintereinanderschaltung als *Multiplikation*

$$\varphi\psi := \varphi \circ \psi$$

versehen.

Der Endomorphismenring zu einer Gruppe ist mit den angegebenen Verknüpfungen in der Tat ein Ring. Dabei folgt die kommutative Gruppenstruktur für die Addition aus einer direkten Rechnung. Die Hintereinanderschaltung von zwei Gruppenhomomorphismen ergibt nach Lemma 5.3 wieder einen Gruppenhomomorphismus. Die Assoziativität der Multiplikation und dass die Identität das neutrale Element ist, gilt allgemeiner für die Verknüpfung von Abbildungen. Für die Distributivität seien Gruppenhomomorphismen φ, ψ, θ gegeben. Dann gilt für jedes $x \in G$

$$((\psi+\theta)\circ\varphi)(x) = (\psi+\theta)(\varphi(x)) = \psi(\varphi(x))+\theta(\varphi(x)) = (\psi\circ\varphi)(x)+(\theta\circ\varphi)(x).$$

Beispiel 12.13. Es sei R ein kommutativer Ring und $n \in \mathbb{N}$. Wie aus der linearen Algebra bekannt (zumindest für den Fall $R = \mathbb{R}$) beschreiben $n \times n$-Matrizen lineare Abbildungen von R^n nach R^n. Die Matrizenverknüpfung

(gemäß der Regel „Zeile mal Spalte“) definiert dabei die Hintereinanderschaltung von linearen Abbildungen. Die Addition von Matrizen, die komponentenweise für jeden Eintrag erklärt ist, beschreibt die Summe von linearen Abbildungen. Mit diesen zwei Verknüpfungen und mit der Nullmatrix als Nullelement und der Einheitsmatrix als Einselement bildet die Menge der Matrizen einen (nicht-kommutativen) Ring, den sogenannten *Matrizenring* über R. Er wird mit $\mathrm{Mat}_n(R)$ bezeichnet.

Zu einem (sagen wir reellen) Vektorraum V der Dimension n hängen der Endomorphismenring zur additiven Gruppe $(V,+,0)$ und der Matrizenring $\mathrm{Mat}_n(\mathbb{R})$ in folgender Weise zusammen. Nach Wahl einer Basis von V entsprechen die $\mathbb{R}$-linearen Endomorphismen $V \to V$ den Matrizen, wobei sich die Additionen entsprechen und die Matrizenmultiplikation der Hintereinanderschaltung von linearen Abbildungen entspricht. Andererseits ist jede lineare Abbildung insbesondere ein Gruppenhomomorphismus von V nach V, so dass sich die Situation

$$\mathrm{Mat}_n(\mathbb{R}) \cong \mathrm{End}_{\mathbb{R}-\mathrm{lin}}(V) \subseteq \mathrm{End}(V)$$

ergibt, wobei hier ein Unterring vorliegt.

13. Vorlesung

13.1. **Einheiten.**

Definition 13.1. Ein Element u in einem Ring R heißt *Einheit*, wenn es ein Element $v \in R$ gibt mit

$$uv = vu = 1\,.$$

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 $uv = 1$ nennt man das (multiplikativ) *Inverse* zu u und bezeichnet es mit

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

Im kommutativen Fall muss man natürlich nur die Eigenschaft $uv = 1$ überprüfen. Eine Einheit ist stets ein Nichtnullteiler. Aus $ux = 0$ folgt ja sofort $x = u^{-1}ux = 0$.

Definition 13.2. 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 (bzgl. der Multiplikation mit 1 als neutralem Element). Wenn v und w die Inversen v^{-1} und w^{-1} haben, so ist das Inverse von vw gleich $w^{-1}v^{-1}$.

Zu einer Einheit $u \in R$ machen auch Potenzen mit einem negativen Exponenten Sinn, d.h. es ist dann u^n für $n \in \mathbb{Z}$ definiert. Die Zahl -1 (also das Negative zu 1) ist stets eine Einheit, da ja $(-1)(-1) = 1$ 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. 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.

13.2. **Körper.**

Viele wichtige Zahlbereiche 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 13.3. Ein kommutativer Ring R heißt *Körper*, wenn $R \neq 0$ ist und wenn jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.

Es sind also die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$ Körper, die ganzen Zahlen dagegen 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 null verschiedenen Elemente eine Gruppe (mit der Multiplikation) bilden.

Definition 13.4. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

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 13.5. 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*.

13.3. **Ringhomomorphismen.**

Definition 13.6. Seien R und S Ringe. Eine Abbildung

$$\varphi : R \longrightarrow S$$

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. Zu einem Unterring $S \subseteq R$ ist die natürliche Inklusion ein Ringhomomorphismus. 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.

Satz 13.7. *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 5.5 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 12.5. □

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 13.8. 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 13.9. *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 13.7 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. □

Satz 13.10. *Sei R ein Ring und sei* $\mathrm{End}(R)$ *der Endomorphismenring der additiven Gruppe $(R,+,0)$. Dann gibt es einen kanonischen injektiven Ringhomomorphismus*

$$R \longrightarrow \mathrm{End}(R),\ f \longmapsto (g \mapsto fg).$$

Beweis. Für jedes $f \in R$ ist die Multiplikation

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

ein Gruppenhomomorphismus, wie direkt aus der Distributivität und der Eigenschaft $f0 = 0$ folgt. Die Gesamtabbildung ist also wohldefiniert.

Für die Gesamtzuordnung $f \mapsto \mu_f$ gilt zunächst $\mu_0 = 0$ und $\mu_1 = \mathrm{id} = 1$. Wegen

$$\mu_{f_1+f_2}(g) = (f_1+f_2)g = f_1g + f_2g = \mu_{f_1}(g) + \mu_{f_2}(g) = (\mu_{f_1} + \mu_{f_2})(g)$$

für jedes $g \in R$ ist μ additiv. Die Multiplikativität folgt aus

$$\mu_{f_1f_2}(g) = f_1f_2g = \mu_{f_1}(f_2g) = \mu_{f_1}(\mu_{f_2}(g)) = (\mu_{f_1} \circ \mu_{f_2})(g).$$

Schließlich ist die Abbildung injektiv, da aus $\mu_f = 0$ folgt, dass insbesondere $f = f1 = 0$ sein muss. □

Lemma 13.11. *Seien R und S Ringe und sei*

$$\varphi : R \longrightarrow S$$

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. □

13.4. **Ideale.**

Wir beschränken uns im Folgenden auf kommutative Ringe, um nicht zwischen Linksidealen, Rechtsidealen und beidseitigen Idealen unterscheiden zu müssen.

Definition 13.12. 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 $ra \in \mathfrak{a}$.

Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich die zweite oben angeführte Eigenschaft erfüllt. Die einfachsten Ideale sind das *Nullideal* 0 und das *Einheitsideal* R.

Für den Ring der ganzen Zahlen $\mathbb{Z}$ sind Untergruppen und Ideale identische Begriffe. Dies folgt einerseits aus der Gestalt $H = \mathbb{Z}d$ für jede Untergruppe

von $\mathbb{Z}$ (die ihrerseits aus der Division mit Rest) aber ebenso direkt aus der Tatsache, dass für $k \in H$ und beliebiges $r \in \mathbb{N}$ gilt $rk = k + k + \ldots + k$ (r-mal) und entsprechend für negatives r. Die Skalarmultiplikation mit einem beliebigen Ringelement lässt sich also bei $\mathbb{Z}$ auf die Addition zurückführen.

Definition 13.13. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

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

heißt *Hauptideal*.

Wir werden auf Hauptideale im Rahmen der Teilbarkeitstheorie bald zurückkommen.

Definition 13.14. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \, ,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

Es handelt sich dabei um das kleinste Ideal in R, das alle a_j, $j \in J$, enthält. Dass ein solches Ideal existiert ist auch deshalb klar, weil der Durchschnitt von einer beliebigen Familie von Idealen wieder ein Ideal ist. Ein Hauptideal ist demnach ein Ideal, das von einem Element erzeugt wird.

Die Idealtheorie in einem Ring reflektiert viele Eigenschaften des Ringes, worauf wir im Rahmen der Teilbarkeitstheorie zurückkommen werden. Eine erste Beobachtung in diese Richtung kommt im folgenden Lemma zum Ausdruck.

Lemma 13.15. *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. $\square$

13.5. **Ideale unter einem Ringhomomorphismus.**

Der Zusammenhang zwischen Ringhomomorphismen und Idealen wird durch folgenden Satz hergestellt.

Satz 13.16. *Seien R und S kommutative Ringe und sei*

$$\varphi : R \longrightarrow S$$

ein Ringhomomorphismus. Dann ist der Kern

$$\text{kern } \varphi = \{f \in R | \, \varphi(f) = 0\}$$

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 13.17. *Es sei K ein Körper und S ein vom Nullring verschiedener Ring. Es sei*

$$\varphi : K \longrightarrow S$$

ein Ringhomomorphismus. Dann ist φ injektiv.

Beweis. Es genügt nach Lemma 5.12 zu zeigen, dass der Kern der Abbildung gleich null ist. Nach Satz 13.6 ist der Kern ein Ideal. Da die 1 auf $1 \neq 0$ geht, ist der Kern nicht ganz K. Da es nach Lemma 13.15 in einem Körper überhaupt nur zwei Ideale gibt, muss der Kern das Nullideal sein. □

14. Vorlesung

14.1. **Restklassenbildung.**

Nach Satz 13.6 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 null, 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 n zuordnet. Jeder Rest wird dann repräsentiert durch eine der Zahlen $0, 1, 2, \ldots, n-1$. Im Allgemeinen gibt es nicht immer ein solch übersichtliches Repräsentantensystem.

14.2. **Die Homomorphiesätze für Ringe.**

Für Ringe, ihre Ideale und Ringhomomorphismen gelten die analogen Homomorphiesätze wie für Gruppen, ihre Normalteiler und Gruppenhomomorphismen, siehe die achte Vorlesung. Wir beschränken uns auf kommutative Ringe.

Satz 14.3. *Seien R, S und T kommutative Ringe, es sei $\varphi : R \to S$ ein Ringhomomorphismus und $\psi : R \to T$ ein surjektiver Ringhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern} \psi \subseteq \operatorname{kern} \varphi$$

ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi} : T \longrightarrow S$$

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 8.1 gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi} : T \longrightarrow S,$$

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

$$\tilde{\varphi}(tt') = \psi(rr') = \psi(r)\psi(r') = \tilde{\varphi}(t)\tilde{\varphi}(t').$$

□

Die im vorstehenden Satz konstruierte Abbildung heißt wieder *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus*.

Korollar 14.4. *Es seien R und S kommutative Ringe und es sei*

$$\varphi : R \longrightarrow S$$

ein surjektiver Ringhomomorphismus. Dann gibt es eine kanonische Isomorphie von Ringen

$$\tilde{\varphi} : R/\operatorname{kern} \varphi \longrightarrow S.$$

Beweis. Aufgrund von Korollar 8.2 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 14.3 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

Satz 14.5. *Es seien R und S kommutative Ringe und es sei*

$$\varphi : R \longrightarrow S$$

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 Korollar 8.2 und Satz 14.3. □

Es gilt also wieder:

Bild = Urbild modulo Kern.

Satz 14.6. *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 14.3. □

Lemma 14.7. *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. □

14.3. $\mathbb{Z}$ ist ein Hauptidealbereich.

Wir wollen nun die Restklassenringe der ganzen Zahlen verstehen. Bei den ganzen Zahlen muss man nicht zwischen Untergruppen und Idealen unterscheiden, da jede Untergruppe von $\mathbb{Z}$ die Gestalt $n\mathbb{Z}$ mit $n \geq 0$ besitzt und daher ein (Haupt-)Ideal ist. Insbesondere hat überhaupt jedes Ideal in $\mathbb{Z}$ diese einfache Gestalt. Dass jede Untergruppe von $\mathbb{Z}$ eine besonders einfache Gestalt hat ist eine Besonderheit der ganzen Zahlen, dagegen ist die Eigenschaft, dass jedes Ideal ein Hauptideal ist, weiter verbreitet und verdient einen eigenen Namen.

Definition 14.8. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

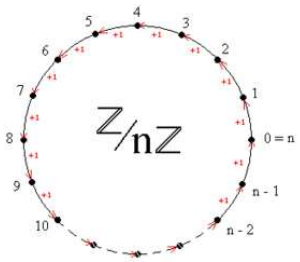
Ein kommutativer Ring, in dem jedes Ideal ein Hauptideal ist, der aber kein Integritätsbereich sein muss, heißt *Hauptidealring*.

Wir halten fest.

Satz 14.9. *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 3.2 die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal. □

14.4. Die Restklassenringe von $\mathbb{Z}$.



Die Restklassengruppen $\mathbb{Z}/(n)$ haben wir bereits kennengelernt, es handelt sich um zyklische Gruppen der Ordnung n. Diese Gruppen bekommen jetzt aber noch zusätzlich eine Ringstruktur.

Korollar 14.10. *Sei $n \geq 0$ eine natürliche Zahl. Dann gibt es eine eindeutig bestimmte Ringstruktur auf $\mathbb{Z}/(n)$ derart, dass die Restklassenabbildung*

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\ a \longmapsto \overline{a}\,,$$

ein Ringhomomorphismus ist. $\mathbb{Z}/(n)$ ist ein kommutativer Ring mit n Elementen (bei $n \geq 1$).

Beweis. Dies ist ein Spezialfall von Definition 14.2 und den sich daran anschließenden Überlegungen. □

Die Charakteristik von $\mathbb{Z}/(n)$ ist n. Dies zeigt insbesondere, dass es zu jeder Zahl n Ringe gibt mit dieser Charakteristik. Zu einem beliebigen Ring R der Charakteristik n faktorisiert der charakteristische Ringhomomorphismus $\mathbb{Z} \to R$ durch

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n) \longrightarrow R\,,$$

wobei die hintere Abbildung injektiv ist. Der Ring $\mathbb{Z}/(n)$, $n = \operatorname{char}(R)$, ist der kleinste Unterring von R, und wird der *Primring* von R genannt.

Korollar 14.11. *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

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/(k) \\ \phi\downarrow & & \\ \mathbb{Z}/(n) & & \end{array}$$

Aufgrund der Teilerbeziehung haben wir die Beziehung

$$\operatorname{kern}\,\phi = (n) \subseteq (k) = \operatorname{kern}\,\varphi\,.$$

Aufgrund des Homomorphisatzes hat man daher eine kanonische Abbildung von links unten nach rechts oben. □

Vor dem nächsten Satz erinnern wir der Vollständigkeit halber an die Definition einer Primzahl.

Definition 14.12. Eine natürliche Zahl $n \geq 2$ heißt eine *Primzahl*, wenn die einzigen natürlichen Teiler von ihr 1 und n sind.

Wir werden uns bald mit ähnlichen Begriffen in einem allgemeineren Kontext auseinandersetzen.

Satz 14.13. *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. (1) $\Rightarrow$ (2). Da jede Einheit ein Nichtnullteiler ist, ist jeder Körper insbesondere ein Integritätsbereich. (2) $\Rightarrow$ (3). Es ist $n = \operatorname{char}(\mathbb{Z}/(n))$ und dies ist im integren Fall eine Primzahl, wie in Lemma 13.9 gezeigt wurde. (3) $\Rightarrow$ (1). Sei also $n = p$ eine Primzahl und $\overline{a} \in \mathbb{Z}/(p)$ eine von null verschiedene Restklasse. Diese wird durch eine ganze Zahl a zwischen 1 und $p-1$ repräsentiert. Da p prim ist, ist $a = 1$ oder aber kein Teiler von p. In

jedem Fall sind a und p teilerfremd und nach Satz 4.1 gibt es eine Darstellung der 1. D.h. es gibt ganze Zahlen $r, s \in \mathbb{Z}$ mit

$$ra + sp = 1\,.$$

Diese Gleichung gilt auch, wenn man die Restklassenbildung modulo p darauf los lässt. Es gilt also

$$\overline{r}\,\overline{a} + \overline{s}\,\overline{p} = \overline{1}$$

in $\mathbb{Z}/(p)$. Dort ist aber $\overline{p} = \overline{0} = 0$, so dass man den zweiten Summanden ignorieren kann und lediglich

$$\overline{r}\,\overline{a} = \overline{1} = 1$$

übrig bleibt. Diese Gleichung zeigt, dass $\overline{a}$ eine Einheit ist (mit $\overline{r}$ als Inversem). □

Die vorstehende Aussage folgt auch aus Lemma 14.7. 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 (bzgl. der Multiplikation). Bei $p = 5$ hat man bspw.

$$\overline{2}^{\,0} = \overline{1}\,,\ \overline{2}^{\,1} = \overline{2}\,,\ \overline{2}^{\,2} = \overline{4} = \overline{-1}\,,\ \overline{2}^{\,3} = \overline{8} = \overline{3}\,,$$

d.h. die Potenzen von $\overline{2}$ durchlaufen sämtliche vier Elemente dieser Gruppe, die sich damit als zyklisch erweist. Wir werden in ein paar Wochen zeigen, 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)

Satz 14.14. *(Kleiner Fermat)*

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 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. □

15. Vorlesung

15.1. **Der Hauptsatz der elementaren Zahlentheorie.**

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

Satz 15.1. *Es sei p eine Primzahl und p teile ein Produkt ab von natürlichen Zahlen $a, b \in \mathbb{N}$. Dann teilt p einen der Faktoren.*

Beweis. Die Voraussetzung bedeutet, dass

$$\overline{a}\,\overline{b} = \overline{0} = 0$$

ist in $\mathbb{Z}/(p)$. Da p eine Primzahl ist, ist dieser Restklassenring nach Satz 14.13 ein Körper, so dass ein Faktor null sein muss. Sagen wir $\overline{a} = 0$. Dies bedeutet aber zurückübersetzt nach $\mathbb{Z}$, dass a ein Vielfaches von p ist. □

Satz 15.2. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1 \cdots p_r$$

mit Primzahlen p_i. Dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Wir beweisen die Existenz und die Eindeutigkeit jeweils durch Induktion. Für $n = 2$ liegt eine Primzahl vor. Bei $n \geq 3$ ist entweder n eine Primzahl, und diese bildet die Primfaktorzerlegung, oder aber n ist keine Primzahl. In diesem Fall gibt es eine nichttriviale Zerlegung $n = ab$ mit kleineren Zahlen $a, b < n$. Für diese Zahlen gibt es nach der Induktionsvoraussetzung eine Zerlegung in Primfaktoren, und diese setzen sich zu einer Primfaktorzerlegung für n zusammen. Zur Eindeutigkeit: Bei $n = 2$ ist die Aussage klar. Im Allgemeinen seien zwei Zerlegungen in Primfaktoren gegeben, sagen wir

$$n = p_1 \cdots p_r = q_1 \cdots q_s\,.$$

Insbesondere teilt die Primzahl p_1 dann das Produkt rechts, und damit nach Satz 15.1 einen der Faktoren. Nach Umordnung können wir annehmen, dass q_1 von p_1 geteilt wird. Da q_1 selbst eine Primzahl ist, folgt, dass $p_1 = q_1$ sein

muss. Da $\mathbb{Z}$ nullteilerfrei ist, kann man beidseitig durch $p_1 = q_1$ dividieren und erhält die Gleichung

$$n' = p_2 \cdots p_r = q_2 \cdots q_s \, .$$

Da $n' < n$ ist, können wir die Induktionsvoraussetzung der Eindeutigkeit auf n' anwenden. □

Zu einer Primzahl p und einer positiven ganzen Zahl n ist der *Exponent*, also die Vielfachheit, mit der p als Primfaktor in n auftritt, eindeutich festgelegt. Dieser Exponent wird mit $\nu_p(n)$ bezeichnet. Die eindeutige Primfaktorzerlegung kann man auch als

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

schreiben, wobei das Produkt in Wirklichkeit endlich ist, da in der Primfaktorzerlegung nur endlich viele Primfaktoren mit einem positiven Exponenten vorkommen.

Lemma 15.3. *Es seien n und k positive natürliche Zahlen. Dann wird n von k genau dann geteilt, wenn für jede Primzahl p die Beziehung*

$$\nu_p(n) \geq \nu_p(k)$$

gilt.

Beweis. (1) $\Rightarrow$ (2). Aus der Beziehung $n = kt$ folgt in Verbindung mit der eindeutigen Primfaktorzerlegung, dass die Primfaktoren von k mit mindestens ihrer Vielfachheit auch in n vorkommen müssen. (2) $\Rightarrow$ (1). Wenn die Exponentenbedingung erfüllt ist, so ist $t = \prod_p p^{\nu_p(n)-\nu_p(k)}$ eine natürliche Zahl mit $n = kt$. □

Korollar 15.4. *Es seien n und m positive natürliche Zahlen mit den Primfaktorzerlegungen $n = \prod_p p^{\nu_p(n)}$ und $m = \prod_p p^{\nu_p(m)}$. Dann ist*

$$\mathrm{kgV}(n,m) = \prod_p p^{\max(\nu_p(n),\nu_p(m))}$$

und

$$\mathrm{ggT}(n,m) = \prod_p p^{\min(\nu_p(n),\nu_p(m))}$$

Beweis. Dies folgt direkt aus Lemma 15.3. □

15.2. **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 15.5. 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 15.6. 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 bspw. $(1, 0)$. 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 15.7. *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. □

15.3. **Der Chinesische Restsatz für $\mathbb{Z}$.**

Satz 15.8. *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. 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 null wird, also modulo $p_i^{r_i}$ den Rest null 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., es ist ein gemeinsames Vielfaches dieser

Potenzen. Daraus folgt aufgrund von Lemma 4.8, dass x ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv. □

Beispiel 15.9. 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 15.10. *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 15.7. □

15.4. **Die Eulersche φ-Funktion.**

Satz 15.11. *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. Sind a und n teilerfremd, so gibt es nach Satz 4.1 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 15.12. 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 15.13. Die Eulersche Funktion $\varphi(n)$ gibt also nach Satz 15.10 an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

Für eine Primzahl ist $\varphi(n) = p - 1$. Eine Verallgemeinerung des *kleinen Fermat* ist der folgende Satz von Euler.

Satz 15.14. *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 7.4 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 15.15. *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 $\leq p^r$ 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 15.16. *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 15.10 und die zweite aus Lemma 15.15. □

16. Vorlesung

16.1. **Polynomringe.**

Definition 16.1. Der *Polynomring* über einem kommutativen Ring R besteht aus allen *Polynomen*

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

mit $a_i \in R$ $n \in \mathbb{N}$, 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 $P = \sum_{i=0}^{n} a_iX^i = a_0 + a_1X + \ldots + a_nX^n$ 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.

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:

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

Lemma 16.2. *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 $P = \sum_{i=0}^{n} a_iX^i$ und $Q = \sum_{j=0}^{m} b_jX^j$ zwei von null verschiedene Polynome. Wir können annehmen, dass a_n und b_m von null verschieden sind. Dann ist $a_nb_m \neq 0$ und dies ist der Leitkoeffizient des Produktes PQ, das damit nicht null sein kann.

□

16.2. **Der Einsetzungshomomorphismus.**

Satz 16.3. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei A ein weiterer kommutativer Ring und es sei $\varphi : R \to A$ ein Ringhomomorphismus und $a \in A$ ein Element. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\psi : R[X] \longrightarrow A$$

mit $\psi(X) = a$ und mit $\psi \circ i = \varphi$, wobei $i : R \to R[X]$ die kanonische Einbettung ist. Dabei geht das Polynom $P = \sum_{j=0}^{n} c_jX^j$ auf $\sum_{j=0}^{n} \varphi(c_j)a^j$.

Beweis. Bei einem Ringhomomorphismus

$$\psi : R[X] \longrightarrow A$$

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 Ringhomomorphismus 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 16.4. *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 Korollar 14.4 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 Korollar 14.4 die Identität sein. Dies gilt auch für die Hintereinanderschaltung in umgekehrter Reihenfolge, so dass ein Isomorphismus vorliegt. □

Korollar 16.5. *Sei R ein kommutativer Ring und sei $S \subseteq R$ ein Unterring Dann ist auch $S[X]$ ein Unterring von $R[X]$.*

Beweis. Wir betrachten den zusammengesetzten Ringhomomorphismus

$$S \longrightarrow R \longrightarrow R[X]\,.$$

Dann liefert der zu $X \mapsto X$ nach Korollar 14.4 gehörige Einsetzungshomomorphismus

$$S[X] \longrightarrow R[X]$$

die gewünschte Abbildung. □

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 bspw. die Eigenschaft, irreduzibel zu sein.

16.3. **Der Grad eines Polynoms.**

Definition 16.6. Der *Grad* eines von null verschiedenen Polynoms

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

mit $a_n \neq 0$ ist n.

In der Situation der vorstehenden Definition heißt a_n der *Leitkoeffizient* des Polynoms. Wenn der Leitkoeffizient 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.

Lemma 16.7. *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. Das ist trivial. □

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 $(K[X])[Y]$ bilden. Für diesen Ring schreibt man auch $R[X,Y]$. Ein Element darin hat die Gestalt

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

Bemerkung 16.8. Zu einem Ring A und einer beliebigen Teilmenge $T \subseteq A$ kann man den von T *erzeugten Unterring* betrachten. Das ist der kleinste Unterring von A, der T umfasst; man kann ihn einfach als den Durchschnitt aller T umfassenden Unterringe realisieren.

Häufig ist man in eine Situation interessiert, wo $R \subseteq A$ ein fixierter Unterring ist und eine weitere, typischerweise recht kleine Teilmenge $T \subseteq A$ gegeben ist. Dann wird der von R und T gemeinsam erzeugte Unterring von A mit $R[T]$ bezeichnet. Es sei vorausgesetzt, dass R mit allen Elementen aus T vertauschbar ist (was bei kommutativen A automatisch der Fall ist). Dann besteht dieser erzeugte Unterring aus allen polynomialen Ausdrücken

$$\sum_{\nu} r_\nu t^{\nu_1}\cdots t_k^{\nu_k}$$

mit $r_\nu \in R$ $t_1,\ldots,t_k \in T$ $\nu = (\nu_1,\ldots,\nu_k) \in \mathbb{N}^k$. Diese Ausdrücke bilden offensichtlich den durch R und T erzeugten Unterring. Bei $T = \{x\}$ schreibt man dafür $R[x] = \{\sum_{i=0}^n a_ix^i \,|\, a_i \in R\}$. Man beachte, dass im Gegensatz zum Polynomring dabei die Darstellung eines Elementes aus $R[T]$ als ein polynomialer Ausdruck keineswegs eindeutig bestimmt sein muss.

16.4. **Polynomringe über einem Körper.**

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.

Satz 16.9. *(Division mit Rest)*

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. Wir beweisen die Existenzaussage durch Induktion über den Grad von P. Wenn der Grad von T größer als der Grad von P ist, so ist $Q = 0$ und $R = P$ die Lösung, so dass wir dies nicht weiter betrachten müssen. Bei $\operatorname{grad}(P) = 0$ ist nach der Vorbemerkung auch $\operatorname{grad}(T) = 0$ und damit ist (da $T \neq 0$ und K ein Körper ist) $Q = P/T$ und $R = 0$ die Lösung. Sei nun $\operatorname{grad}(P) = n$ und die Aussage für kleineren Grad schon bewiesen. Wir schreiben $P = a_nX^n + \ldots + a_1X + a_0$ und $T = b_kX^k + \ldots + b_1X + b_0$ mit $a_n, b_k \neq 0$, $k \leq n$. Dann gilt mit $H = \frac{a_n}{b_k}X^{n-k}$ die Beziehung

$$\begin{aligned} P' = P - TH = 0X^n + (a_{n-1} - \frac{a_n}{b_k}b_{k-1})X^{n-1} + \ldots \\ + (a_{n-k} - \frac{a_n}{b_k}b_0)X^{n-k} + a_{n-k-1}X^{n-k-1} + \ldots + a_0. \end{aligned}$$

Dieses Polynom P' hat einen Grad kleiner als n und darauf können wir die Induktionsvoraussetzung anwenden, d.h. es gibt Q' und R' mit

$$P' = TQ' + R' \text{ mit } \operatorname{grad}(R') < \operatorname{grad}(T) \text{ oder } R' = 0\,.$$

Daraus ergibt sich insgesamt

$$P \;=\; P' + TH \;=\; TQ' + TH + R' \;=\; T(Q' + H) + R',$$

so dass also $Q = Q' + H$ und $R = R'$ die Lösung ist. Zur Eindeutigkeit sei $P = TQ + R = TQ' + R'$ mit den angegebenen Bedingungen. Dann ist $T(Q - Q') = R' - R$. Da die Differenz $R' - R$ einen Grad kleiner als $\operatorname{grad}(T)$ besitzt, und der Polynomring nullteilerfrei ist, ist diese Gleichung nur bei $R = R'$ und somit $Q = Q'$ lösbar. □

Bemerkung 16.10. Das in Satz 16.9 beschriebene Verfahren, um zu zwei gegebenen Polynomen P und T Polynome Q und R zu finden mit

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

ist konstruktiv und lässt sich rechnerisch einfach durchführen, wenn man die Arithmetik im Grundkörper K beherrscht. Dieses Verfahren heißt *Division mit Rest*.

Satz 16.11. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

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

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

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \text{grad}\,(F)$. Wir behaupten, dass $I = (F)$ ist. Sei hierzu $P \in I$ gegeben. Aufgrund von Satz 16.9 gilt

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

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

Definition 16.12. Es sei K ein Körper und seien $a_0, a_1, \ldots, a_n \in K$. Eine Funktion

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

mit

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

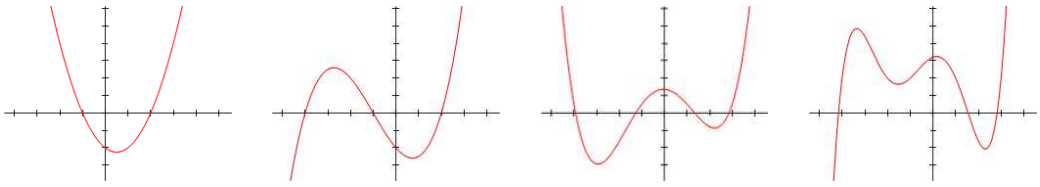
heißt *Polynomfunktion.*

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

$$X^p - X$$

hat bspw. nach dem kleinen Fermat (Satz 14.14) 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.



17. Vorlesung

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 Hauptidealbereich vorliegt, haben wir schon gesehen. Es gilt aber auch wieder der euklidische Algorithmus und die eindeutige Primfaktorzerlegung. Um diese adäquat formulieren zu können, brauchen wir einige Vorbereitungen zur allgemeinen Teilbarkeitslehre.

17.1. **Teilbarkeitsbegriffe.**

Definition 17.1. 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 $a|b$.

Lemma 17.2. *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 17.5. □

Mit dem Idealbegriff lassen sich Teilbarkeitsbeziehungen ausdrücken.

Lemma 17.3. *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. Das ist trivial. □

Definition 17.4. 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 17.2. In $R = \mathbb{Z}$ sind zwei Zahlen genau dann zueinander assoziiert, wenn ihr Betrag übereinstimmt. 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 17.5. *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 $(a) = (b)$ genau dann, wenn a und b assoziiert sind.*

Beweis. Siehe Aufgabe 17.6. □

Definition 17.6. 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.

Bemerkung 17.7. 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).

Lemma 17.8. *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. □

17.2. **Irreduzibel und prim.**

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

Definition 17.9. 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 17.10. 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 17.11. *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. □

17.3. **Teilbarkeitslehre in Hauptidealbereichen.**

Satz 17.12. *(Lemma von Bezout)*

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 $r_1a_1 + r_2a_2 + \ldots + r_na_n = d$.

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 $I = (a_1, \ldots, a_n) = R$. □

Bemerkung 17.13. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dies ist ein Hauptidealbereich und daher gibt es zu gegebenen Polynomen $P_1, P_2, \ldots, P_n$ einen größten gemeinsamen Teiler, und diesen kann man darstellen als Linearkombination der gegebenen Polynome. Es gibt sogar ein effektives Verfahren, eine solche Darstellung explizit zu finden, das man (wie bei den ganzen Zahlen $\mathbb{Z}$) den *euklidischen Algorithmus* nennt. Wir

beschränken uns auf den Fall von zwei Polynomen F und G. Man führt nun sukzessive eine Division mit Rest durch und erhält zunächst

$$F = Q_1 G + R_1 \, .$$

Dann erhält man

$$G = Q_2 R_1 + R_2, \; R_1 = Q_3 R_2 + R_3,$$

usw., bis schließlich der Rest $R_k = 0$ ist. Dieser Fall muss letztlich eintreten, da sich bei jedem Divisionsschritt der Grad der Reste reduziert. Der vorletzte Rest ist dann der größte gemeinsame Teiler, und man kann durch Zurückrechnen entlang der Gleichungen eine Darstellung dieses ggTs mit F und G finden.

Lemma 17.14. *(von Euklid)*

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

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 17.11 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 17.16. *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. □

18. Vorlesung

18.1. **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 Ringes

Definition 18.1. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Satz 18.2. *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 assoziiertes Element ergibt. Das gekürzte Element hat eine Faktorzerlegung mit $r-1$ 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 18.3. *Ein Hauptidelabereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Satz 17.15, Lemma 17.16 und Satz 18.2. □

Korollar 18.4. *Sei R ein faktorieller Ring und seien a und b zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

(wobei die u, v Einheiten sind und die Exponenten auch null sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ ist für alle Exponenten $i = 1, \ldots, k$.

Beweis. Wenn die Exponentenbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann schreiben

$$b = vu^{-1} p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k} ,$$

was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in einem faktoriellen Ring. □

18.2. **Restklassenringe von Hauptidealbereichen.**

Satz 18.5. *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 null 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. □

Für die Restklassenringe von Hauptidealbereichen gilt wieder der chinesische Restsatz (für beliebige faktorielle Bereiche gilt er nicht, da das Lemma von Bezout dafür im Allgemeinen nicht gilt).

Satz 18.6. *(Chinesischer Restsatz)*

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

$$R/(f) \longrightarrow R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k}),\ a \longmapsto (a \mod p_1^{r_1}, \ldots, a \mod p_1^{r_1}).$$

Wir müssen zeigen, dass dieser bijektiv ist. Zur Injektivität sei $a \in R$ derart, dass es in jeder Komponente auf null 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 Satz 17.12 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. □

18.3. **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 18.7. *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 16.11, aus Satz 18.3 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*. Diese Eigenschaft hängt wesentlich vom gewählten 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.

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. Ob ein lineares Polynom ein Faktor eines anderen Polynoms (und damit ein Primfaktor davon) ist, hängt direkt mit den Nullstellen des Polynoms zusammen.

18.4. **Nullstellen von Polynomen.**

Lemma 18.8. *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. Also ist $X - a$ ein Linearfaktor von P. □

Korollar 18.9. *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 18.8 das Polynom P genau dann, wenn $P(a) = 0$ ist. □

Korollar 18.10. *Es sei K ein Körper und $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom (ungleich null) 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 18.8 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 null sein, wenn einer der Faktoren null 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. □

Beispiel 18.11. 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.

19. Vorlesung

19.1. **Algebraisch abgeschlossene Körper.**

Wir haben zuletzt erwähnt, dass ein lineares Polynom $X - a$ über einem Körper stets irreduzibel ist, und dass es als Faktor in der Primfaktorzerlegung eines Polynoms F genau dann vorkommt, wenn a eine Nullstelle von F ist. Diejenigen Körper, für die es im Polynomring außer den linearen Polynomen keine weiteren irreduziblen Polynome gibt, bekommen einen eigenen Namen.

Definition 19.1. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom $F \in K[X]$ eine Nullstelle in K besitzt.

Lemma 19.2. *Sei K ein Körper. Dann sind die beiden folgenden Eigenschaften äquivalent.*

(1) *K ist algebraisch abgeschlossen.*
(2) *Jedes nicht-konstante Polynom $F \in K[X]$ zerfällt in Linearfaktoren.*

Beweis. Siehe Aufgabe 19.6. □

Wir erwähnen hier ohne Beweis den *Fundamentalsatz der Algebra*, der 1799 von Gauß bewiesen wurde.

Satz 19.3. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

19.2. **Endliche Untergruppen der Einheitengruppe eines Körpers.**

Wir wollen zeigen, dass die Einheitengruppe $\mathbb{Z}/(p)$, p Primzahl, zyklisch ist. Dafür brauchen wir neben den Aussagen der letzten Vorlesung über die Nullstellen von Polynomen noch einige gruppentheoretische Vorbereitungen.

Lemma 19.4. *Sei G eine kommutative Gruppe und $x, y \in G$ Elemente der endlichen Ordnungen $n = \operatorname{ord}(x)$ und $m = \operatorname{ord}(y)$, wobei n und m teilerfremd seien. Dann hat xy die Ordnung nm.*

Beweis. Sei $(xy)^k = 1$. Wir haben zu zeigen, dass k ein Vielfaches von nm ist. Es ist

$$1 = (x^k y^k)^n = x^{kn} y^{kn} = y^{kn}\,,$$

da ja n die Ordnung von x ist. Aus dieser Gleichung erhält man, dass kn ein Vielfaches der Ordnung von y, also von m sein muss. Da n und m teilerfremd sind, folgt aus Satz 17.14, dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, so dass k, wieder aufgrund der Teilerfremdheit, ein Vielfaches von nm sein muss. □

Definition 19.5. Der *Exponent* $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive Zahl n mit der Eigenschaft, dass $x^n = 1$ ist für alle $x \in G$.

Lemma 19.6. *Sei G eine endliche kommutative Gruppe und sei $\exp(G) = \operatorname{ord}(G)$, wobei $\exp(G)$ den Exponenten der Gruppe bezeichnet. Dann ist G zyklisch.*

Beweis. Sei $n = \operatorname{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

$$\exp(G) = \operatorname{kgV}(\operatorname{ord}(x) : x \in G)\,.$$

Sei p_i ein Primteiler von n. Wegen $\exp(G) = \operatorname{ord}(G)$ gibt es ein Element $x \in G$, dessen Ordnung ein Vielfaches von $p_i^{r_i}$ ist. Dann gibt es auch (in der von x erzeugten zyklischen Untergruppe) ein Element x_i der Ordnung $p_i^{r_i}$. Dann hat das Produkt $x_1 \cdots x_k \in G$ nach Lemma 19.4 die Ordnung n. □

Satz 19.7. *Sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Dann ist U zyklisch.*

Beweis. Sei $n = \operatorname{ord}(U)$ und $e = \exp(U)$ der Exponent dieser Gruppe. Dies bedeutet, dass alle Elemente $x \in U$ eine Nullstelle des Polynoms $X^e - 1$ sind. Nach Korollar 18.10 ist die Anzahl der Nullstellen aber maximal gleich dem Grad, so dass $n = e$ folgt. Nach Lemma 19.4 ist dann U zyklisch. □

Satz 19.8. *Sei p eine Primzahl. Dann ist die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch der Ordnung $p-1$. Es gibt also (sogenannte primitive) Elemente g mit der Eigenschaft, dass die Potenzen g^i, $i = 0, 1, \ldots, p-2$, alle Einheiten durchlaufen.*

Beweis. Dies folgt unmittelbar aus Satz 19.7, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

Definition 19.9. Eine Einheit $u \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitengruppe erzeugt.

Beispiel 19.10. Wir betrachten die Einheitengruppe des Restklassenkörpers $\mathbb{Z}/(23)$. Nach Satz 19.8 ist sie zyklisch und es gibt daher Erzeuger der Einheitengruppe, also primitive Elemente. Wie kann man diese finden? Man ist hierbei prinzipiell auf Probieren angewiesen, man kann dies allerdings deutlich vereinfachen. Man weiß, dass die Einheitengruppe 22 Elemente besitzt, als Ordnung von Elementen dieser Gruppe kommen also nur $1, 2, 11$ und 22 in Frage. Es gibt genau ein Element mit der Ordnung 1, nämlich 1, und ein Element mit der Ordnung 2, nämlich $-1 = 22$. Alle anderen Elemente haben also die Ordnung 11 oder 22, und genau die letzteren sind primitiv. Der erste Kandidat ist 2. Wir müssen also

$$2^{11} \mod 23$$

ausrechnen. Es ist $2^5 = 32 = 9$ und daher ist

$$2^{11} = 9 \cdot 9 \cdot 2 = 12 \cdot 2 = 24 = 1.$$

Die Ordnung ist also 11, und die 2 ist nicht primitiv. Betrachten wir die 3. Es ist $3^3 = 27 = 4$ und daher ist

$$3^{11} = 4 \cdot 4 \cdot 4 \cdot 9 = 18 \cdot 9 = 162 = 1,$$

also wieder nicht primitiv. Der nächste Kandidat 4 muss nicht gecheckt werden, denn wegen $4 = 2^2$ ist sofort $4^{11} = 2^{22} = 1$ (diese Beobachtung gilt für alle Quadratzahlen, und zwar auch für diejenigen Zahlen, die nur modulo 23 ein Quadrat sind). Betrachten wir also 5. Es ist $5^2 = 2$. Damit ist

$$5^{11} = 2^5 \cdot 5 = 9 \cdot 5 = 45 = -1 \neq 1.$$

Daher hat 5 die Ordnung 22 und ist ein primitives Element.

Man kann diesen Sachverhalt auch so ausdrücken, dass die Abbildung

$$\mathbb{Z}/(22) \longrightarrow (\mathbb{Z}/(23))^\times,\ k \longmapsto 5^k,$$

einen Gruppenisomorphismus definiert. Dieser übersetzt die Addition in die Multiplikation, daher spricht man von einer *diskreten Exponentialfunktion* und nennt die Umkehrabbildung auch einen *diskreten Logarithmus*. Solche Abbildungen spielen eine wichtige Rolle in der *Kryptologie*. Wenn man wie in diesem Beispiel einen solchen Isomorphismus gefunden hat, so kann man viele Eigenschaften der Einheitengruppe in der „einfacheren“ Gruppe entscheiden.

Z.B. sind in $\mathbb{Z}/(22)$ alle ungeraden Elemente außer 11 ein Gruppenerzeuger, daher sind in der Einheitengruppe alle Elemente der Form

$$5^u, u \text{ ungerade}, u \neq 11,$$

primitiv.

19.3. **Endliche Körper.**

Definition 19.11. Ein Körper heißt *endlich*, wenn er nur endlich viele Elemente besitzt.

Wir erinnern kurz an die Charakteristik eines Ringes. Zu jedem kommutativen Ring gibt es den kanonischen Ringhomomorphismus $\varphi : \mathbb{Z} \to R$, und der Kern davon ist ein Ideal $\mathfrak{a}$ in $\mathbb{Z}$ und hat daher die Form $\mathfrak{a} = (n)$ mit einem eindeutig bestimmten $n \geq 0$. Diese Zahl nennt man die Charakteristik von R. Ist R ein Körper, so ist dieser Kern $\mathfrak{a} = 0$ oder $\mathfrak{a} = (p)$ mit einer Primzahl p. Man spricht von Charakteristik null oder von positiver Charakteristik $p > 0$.

Wir haben bereits die endlichen Primkörper $\mathbb{Z}/(p)$ zu einer Primzahl p kennengelernt. Sie besitzen p Elemente, und ein Körper besitzt genau dann die Charakteristik p, wenn er diesen Primkörper enthält. Genau dann hat man auch eine Faktorisierung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(p) \longrightarrow K\,,$$

wobei die hintere Abbildung injektiv ist, d.h. es liegt eine Körpererweiterung

$$\mathbb{Z}/(p) \subseteq K$$

vor. Für eine Körpererweiterung gilt stets folgende Beobachtung.

Lemma 19.12. *Sei $K \subseteq L$ eine Körpererweiterung. Dann ist L in natürlicher Weise ein K-Vektorraum.*

Beweis. Die Skalarmultiplikation

$$K \times L \longrightarrow L,\ (\lambda, x) \longmapsto \lambda x,$$

wird einfach durch die Multiplikation in L gegeben. Die Vektorraumaxiome folgen dann direkt aus den Ringaxiomen. □

Über die Anzahl der Elemente in einem Körper gilt folgende wichtige Bedingung.

Lemma 19.13. *Sei K ein endlicher Körper. Dann besitzt K genau p^n Elemente, wobei p eine Primzahl ist und $n \geq 1$.*

Beweis. Der endliche Körper kann nicht Charakteristik null besitzen, und als Charakteristik eines Körpers kommt ansonsten nach Lemma 13.9 nur eine Primzahl in Frage. Diese sei mit p bezeichnet. Das bedeutet, dass K den Körper $\mathbb{Z}/(p)$ enthält. Damit ist aber K ein Vektorraum über $\mathbb{Z}/(p)$, und zwar, da K endlich ist, von endlicher Dimension. Sei n die Dimension, $n \geq 1$.

Dann hat man eine $\mathbb{Z}/(p)$-Vektorraum-Isomorphie $K \cong (\mathbb{Z}/(p))^n$ und somit besitzt K gerade p^n Elemente. □

Die vorstehende Aussage gilt allgemeiner für endliche Ringe, die einen Körper enthalten. Es sei schon jetzt erwähnt, dass es zu jeder Potenz p^n bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Dies werden wir in zwei Wochen beweisen. Für einige Beispiele siehe auch die Aufgaben.

Beispiel 19.14. Wir konstruieren einen Körper mit $23^2 = 529$ Elementen und knüpfen dabei an Beispiel 19.10 an. Da die $5 \in \mathbb{Z}/(23)$ primitiv ist, folgt, dass das Polynom $X^2 - 5 \in \mathbb{Z}/(23)[X]$ irreduzibel ist. Andernfalls müsste es eine Nullstelle haben und dann wäre $5 = a^2$ ein Quadrat mit $a \in \mathbb{Z}/(23)$. Doch dann wäre $5^{11} = a^{22} = 1$, was nicht der Fall ist.

Es folgt nach Satz 18.5, dass

$$K = \mathbb{Z}/(23)[X]/(X^2 - 5)$$

ein Körper ist. Dieser hat 23^2 Elemente, da man jede Restklasse auf genau eine Weise als $ax + b$ mit $a, b \in \mathbb{Z}/(23)$ schreiben kann (x bezeichne die Restklasse von X). Dieser Körper enthält $\mathbb{Z}/(23)$, und die Ordnungen dieser Elemente ändern sich nicht (und sie sind insbesondere nicht primitiv im größeren Körper).

Wir möchten eine primitive Einheit in diesem Körper finden. Die Ordnung von $K^\times$ ist $528 = 16 \cdot 3 \cdot 11$. Wir müssen für jede dieser Primzahlpotenzen ein Element mit dieser Ordnung finden. Die 2 hat die Ordnung 11. Das Element $11 - x$ hat die Ordnung 3, es ist nämlich

$$(11-x)^3 = 121 \cdot 11 - 3 \cdot 121x + 33x^2 - x^3 = 66 - 3 \cdot 6x + 50 - 5x = 116 - 23x = 1.$$

Um ein Element der Ordnung 16 zu finden, ziehen wir sukzessive Quadratwurzeln aus -1. Es ist

$$(3x)^2 = 9x^2 = 45 = -1.$$

Eine Quadratwurzel daraus ist $14 + 19x$, wegen

$$(14 + 19x)^2 = 196 + 361 \cdot 5 + 2 \cdot 14 \cdot 19x = 12 + 16 \cdot 5 + 5 \cdot 19x = 3x.$$

Um eine Quadratwurzel für $14+19x$ zu finden, setzen wir $(a+bx)^2 = 14+19x$ an, was zum Gleichungssystem $a^2+5b^2 = 14$ und $2ab = 19$ über $\mathbb{Z}/(23)$ führt. Es ist dann $a = 21 \cdot b^{-1}$, was zu $4b^{-2} + 5b^2 = 14$ bzw. zur *biquadratischen Gleichung*

$$5b^4 + 9b^2 + 4 = 0$$

führt. Normieren ergibt $b^4 + 11b^2 + 10 = 0$. *Quadratisches Ergänzen* führt zu

$$(b^2 + 17)^2 = 17^2 - 10 = 49.$$

Daher ist $b^2 = 13$ und somit $b = 6$ und $a = 15$, also ist $15 + 6x$ ein Element der Ordnung 16. Damit ist insgesamt

$$2(11 - x)(15 + 6x) = 2(165 - 30 + 51x) = 2(20 + 5x) = 17 + 10x$$

eine primitive Einheit nach Lemma 19.4.

Satz 19.15. *Sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedener Elemente aus K gleich -1.*

Beweis. Die Gleichung $x^2 = 1$ hat in einem Körper nur die Lösungen 1 und -1, die allerdings gleich sein können. Das bedeutet, dass für $x \neq 1, -1$ immer $x \neq x^{-1}$ ist. Damit kann man das Produkt aller Einheiten schreiben als

$$1(-1)x_1x_1^{-1}\cdots x_kx_k^{-1}\,.$$

Ist $-1 \neq 1$, so ist das Produkt -1. Ist hingegen $-1 = 1$, so fehlt in dem Produkt der zweite Faktor und das Produkt ist $1 = -1$. □

Korollar 19.16. *(Wilson)*

Sei p eine Primzahl. Dann ist

$$(p-1)! = -1 \mod p\,.$$

Beweis. Dies folgt unmittelbar aus Satz 19.15, da ja die Fakultät durch alle Zahlen zwischen 1 und $p-1$ läuft, also durch alle Einheiten im Restklassenkörper $\mathbb{Z}/(p)$. □

20. Vorlesung

20.1. **Multiplikative Systeme.**

Wir wollen zeigen, dass es zu jedem Integritätsbereich R einen Körper K gibt derart, dass R ein Unterring von K wird. Diesen Körper werden wir dann den *Quotientenkörper* von R nennen. Die Konstruktion ist dieselbe, mit der man aus den ganzen Zahlen $\mathbb{Z}$ die rationalen Zahlen $\mathbb{Q}$ gewinnt.

Definition 20.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

(1) $1 \in S$
(2) Wenn $f, g \in S$, dann ist auch $fg \in S$

gelten.

Wir erwähnen einige Beispiele von multiplikativen Systemen. Zunächst ist natürlich der Gesamtring, die Menge $\{1\}$ und die Einheitengruppe $R^\times$ ein multiplikatives System. Darüber hinaus erwähnen wir die folgenden Beispiele.

Beispiel 20.2. Sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n, $n \in \mathbb{N}$, ein multiplikatives System.

Beispiel 20.3. Die Nichtnullteiler bilden ein multiplikatives System in einem kommutativen Ring. Die 1 ist wie jede Einheit ein Nichtnullteiler, und wenn f und g Nichtnullteiler sind, so ist auch deren Produkt ein Nichtnullteiler, da aus $f(gh) = 0$ zunächst $gh = 0$ und daraus $h = 0$ folgt.

Beispiel 20.4. Sei R ein Integritätsbereich. Dann bilden alle von null verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R - \{0\}$ bezeichnet wird.

Definition 20.5. 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 $s \in \mathfrak{p}$.

Beispiel 20.6. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R - \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

Beispiel 20.7. Sei R ein faktorieller Bereich und sei M eine Menge von Primelementen. Dann ist die Menge aller Elemente aus R, in deren Primfaktorzerlegung ausschließlich Primelemente aus M vorkommen, ein multiplikatives System S. Es ist also

$$S = \{up_1^{r_1} \cdots p_k^{r_k} \,|\, u \in R^\times,\, p_i \in M\}\,.$$

Lemma 20.8. *Seien R und A kommutative Ringe und sei*

$$\varphi : R \longrightarrow A$$

ein Ringhomomorphismus. Dann ist das Urbild $\varphi^{-1}(A^\times)$ der Einheitengruppe ein multiplikatives System.

Beweis. Das ist trivial. □

20.2. **Nenneraufnahme.**

Unser nächstes Ziel ist es, zu einem multiplikativen System S einen Ring zu konstruieren mit der Eigenschaft, dass die Elemente aus S dort zu Einheiten werden, und dieser Ring minimal mit dieser Eigenschaft ist.

Definition 20.9. Sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann heißt die Menge der *formalen Brüche*

$$R_S := \left\{ \frac{f}{g} : \, f \in R,\, g \in S \right\}$$

die *Nenneraufnahme* zu S. Dabei werden zwei Brüche $\frac{f}{g}$ und $\frac{s}{t}$ identifiziert, wenn $ft = gs$ gilt. Die Nenneraufnahme ist ein kommutativer Ring mit der Addition

$$\frac{f}{g} + \frac{s}{t} = \frac{ft + gs}{tg}$$

und der Multiplikation

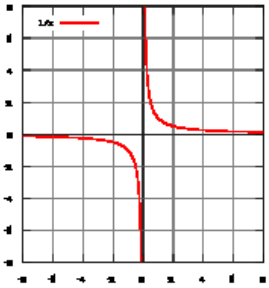
$$\frac{f}{g} \cdot \frac{s}{t} = \frac{fs}{tg}\,.$$

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n:n\in\mathbb{N}\}}$. Die Elemente $s \in S$ aus dem multiplikativen System werden in R_S zu Einheiten, und zwar ist $1/s$ das Inverse zu s. Die Nenneraufnahme an $R^* = R \setminus \{0\}$ in einem Integritätsbereich spielt für uns eine besondere Rolle. Dort werden sämtliche Elemente $\neq 0$ zu Einheiten und es entsteht somit ein Körper.

Definition 20.10. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

$$Q(R) = \{\frac{r}{s} : r, s \in R,\, s \neq 0\}$$

mit natürlichen Identifizierungen und Operationen.



Die einfachste rationale Funktion (von den Polynomen abgesehen)ist $1/X$.

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). 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 vorsichtig sein und darf nicht die formalen Brüche mit den dadurch definierten Funktionen gleichsetzen, auch wenn dies bei $K = \mathbb{R}$ die Vorstellung unterstützt.

Die folgende Aussage kann man so verstehen, dass der Quotientenkörper der minimale Körper ist, in dem man einen Integritätsbereich als Unterring realisieren kann.

Satz 20.11. *Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Es sei*

$$\varphi : R \longrightarrow K$$

ein injektiver Ringhomomorphismus in einen Körper K Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi} : Q(R) \longrightarrow K$$

mit $\varphi = \tilde{\varphi} \circ i$, wobei i die kanonische Einbettung

$$i : R \longrightarrow Q(R)$$

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

$$\begin{aligned}
\tilde{\varphi}(\frac{a}{b} + \frac{c}{d}) &= \tilde{\varphi}(\frac{ad+cb}{bd}) \\
&= \varphi(ad+bc)\varphi(bd)^{-1} \\
&= (\varphi(a)\varphi(d) + \varphi(b)\varphi(c))\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\
&= \tilde{\varphi}(\frac{a}{b}) + \tilde{\varphi}(\frac{c}{d}).
\end{aligned}$$

□

20.3. **Der Satz von Gauß.**

Wir wollen nun für einen faktoriellen Integritätsbereich R zeigen, dass auch der Polynomring $R[X]$ faktoriell ist. Speziell ergibt sich daraus induktiv, dass für einen Körper die Polynomringe in beliebig vielen Variablen faktoriell sind, obwohl sie nur bei einer Variablen Hauptidealbereiche sind. Es liegt nahe, dabei mit dem Quotientenkörper $Q(R)$ zu arbeiten und Teilbarkeitseigenschaften in $R[X]$ mit denen in $Q(R)[X]$ zu vergleichen. Da letzteres ein Hauptidealbereich ist, ist darüber viel bekannt.

In den folgenden Beweisen werden zwei einfache Beobachtungen wiederholt zur Anwendung kommen. Ein konstantes Polynom $c \in R$ teilt ein Polynom $P = \sum_{i=0}^{n} a_i X^i \in R[X]$ genau dann, wenn c jeden Koeffizienten a_i teilt. Und zu einem Polynom $F = \sum_{i=0}^{n} q_i X^i \in Q(R)[X]$ gibt es stets ein $a \in R$ (nämlich einen *Hauptnenner* der q_i) derart, dass aF zu $R[X]$ gehört.

Lemma 20.12. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei $p \in R$ ein Primelement. Dann ist p auch in $R[X]$ prim.*

Beweis. Sei $ph = fg$. Wir nehmen an, dass p weder f noch g teilt. Dann teilt p nicht alle Koeffizienten von f und von g. Es sei $f = \sum_{i=0}^{n} a_i X^i$ und $g =$

$\sum_{j=0}^{m} b_j X^j$ und es seien i_0 bzw. j_0 die kleinsten Indizes derart, dass a_{i_0} (bzw. b_{j_0}) kein Vielfaches von p ist (für alle kleineren Indizes sind die Koeffizienten also Vielfache von p). Wir betrachten den $(i_0 + j_0)$-ten Koeffizienten von fg, dieser ist

$$c_{i_0+j_0} = a_0 b_{i_0+j_0} + \ldots + a_{i_0-1} b_{j_0+1} + a_{i_0} b_{j_0} + a_{i_0+1} b_{j_0-1} + \ldots + a_{i_0+j_0} b_0$$

Die Summanden links sind Vielfache von p aufgrund der Wahl von i_0 und die Summanden rechts sind ebenso Vielfache von p. Da auch der Gesamtkoeffizient nach Voraussetzung ein Vielfaches von p ist, muss auch der mittlere Summand $a_{i_0} b_{j_0}$ ein Vielfaches von p sein. Da p prim ist, ist dies ein Widerspruch. □

Lemma 20.13. *(Lemma von Gauß)*

Es sei R ein faktorieller Bereich und $K = Q(R)$ der zugehörige Quotientenkörper. Es sei $f \in R[X]$ ein nicht-konstantes Polynom derart, dass in $R[X]$ nur Faktorzerlegungen $f = gh$ mit $g \in R$ oder $h \in R$ möglich sind. Dann ist f irreduzibel in $K[X]$.

Beweis. Nehmen wir an, es gebe eine nicht-triviale Faktorzerlegung $f = gh$ mit nicht-konstanten Polynomen $g, h \in K[X]$. Sowohl in g als auch in h kommen nur endlich viele Nenner aus R vor, so dass man mit einem gemeinsamen Hauptnenner $r \in R$ multiplizieren kann und somit eine Darstellung $rf = \tilde{g}\tilde{h}$ mit $\tilde{g}, \tilde{h} \in R[X]$ erhält. Dabei haben sich die Grade der beteiligten Polynome nicht geändert. Es sei $r = p_1 \cdots p_n$ die Primfaktorzerlegung von r. Nach Lemma 20.12 ist p_1 auch im Polynomring $R[X]$ prim. Da es das Produkt $\tilde{g}\tilde{h}$ teilt, muss es einen der Faktoren teilen, sagen wir $\tilde{h}$. Dann kann man mit p_1 kürzen und erhält eine Gleichung der Form

$$r' f = \tilde{g}\tilde{h}' .$$

Dabei ändern sich wieder die Grade nicht. So kann man sukzessive alle Primfaktoren wegkürzen und erhält schließlich eine Zerlegung

$$f = g'h'$$

mit nicht konstanten Polynomen $h', g' \in R[X]$ im Widerspruch zur Voraussetzung. □

Satz 20.14. *Sei R ein faktorieller Bereich. Dann ist auch der Polynomring $R[X]$ faktoriell.*

Beweis. Wir zeigen, dass jedes irreduzible Element prim ist und dass jedes Polynom eine Zerlegung in irreduzible Polynome besitzt. Sei also $f \in R[X]$ irreduzibel und

$$fq = hg .$$

Bei $f \in R$ ist f prim nach Lemma 20.12, so dass wir $\operatorname{grad}(f) \geq 1$ annehmen können. Die Teilbarkeitsbeziehung gilt erst recht in $Q(R)[X]$. Nach Lemma 20.13 ist das Polynom f auch irreduzibel in $Q(R)[X]$ und damit darin prim

nach Satz 17.15. Daher teilt dieses Element in $Q(R)[X]$ einen der Faktoren, sagen wir h. Es ist also $fu = h$ mit $u \in Q(R)[X]$. Wir können mit einem Hauptnenner a von u multiplizieren und erhalten die Beziehung

$$fv = ha = hp_1 \cdots p_n$$

mit $v \in R[X]$, wobei a durch seine Primfaktorzerlegung ersetzt wurde. Da f irreduzibel ist, sind die Koeffizienten von f teilerfremd. Insbesondere ist p_1 kein Teiler von allen Koeffizienten von f. Da p_1 nach Lemma 20.12 auch in $R[X]$ prim ist, folgt, dass v ein Vielfaches von p ist. Man kann also durch p_1 kürzen. So kann man sukzessive die Primfaktorzerlegung von a abarbeiten und erhält schließlich, dass h ein Vielfaches von f ist.

Dass jedes Polynom $f \in R$ ein Produkt von irreduziblen Polynomen ist, beweisen wir durch Induktion über den Grad von f. Bei Grad null liefert die Primfaktorzerlegung in P sofort die gewünschte Zerlegung in $R[X]$. Sei also der Grad von f positiv. Wenn es eine Produktzerlegung in Polynome von kleinerem Grad gibt, so sind wir fertig aufgrund der Induktionsvoraussetzung. Andernfalls sei a der größte gemeinsame Teiler der Koeffizienten von f. Dann ist $f = a\tilde{f}$ mit $\tilde{f} \in R[X]$ und die Koeffizienten von $\tilde{f}$ sind teilerfremd. Dann ist aber $\tilde{f}$ irreduzibel, da es weder eine Zerlegung in Polynome mit kleinerem Grad noch eine nicht-triviale Zerlegung mit Konstanten geben kann. □

Korollar 20.15. *Der Polynomring $\mathbb{Z}[X]$ ist faktoriell.*

Beweis. Dies folgt aus Satz 14.9, Satz 18.3 und Satz 20.14. □

Korollar 20.16. *Es sei K ein Körper. Dann sind die Polynomringe $K[X_1, \ldots, X_n]$ faktoriell.*

Beweis. Dies folgt durch induktive Anwendung von Satz 20.14 auf die Kette

$$K \subset K[X_1] \subset (K[X_1])[X_2] \subset (K[X_1, X_2])[X_3] \subset \ldots$$

□

21. Vorlesung

21.1. **Algebren.**

Definition 21.1. 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 $\mathbb{Z} \to R$, $n \mapsto n_R$. Der Begriff der Algebra ist auch für nicht-kommutative Ringe A (bei kommutativem Grundring R) sinnvoll, wobei dann in aller Regel die Voraussetzung

gemacht wird, dass die Elemente aus R mit allen Elementen aus A vertauschen.

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 21.2. Seien R und S zwei kommutative K-Algebren über einem kommutativen Grundring K. Dann nennt man einen Ringhomomorphismus

$$\varphi : R \longrightarrow S$$

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 (siehe Vorlesung 16) 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.

21.2. 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 21.3. *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 $(P) = (\frac{P}{a_n})$, 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 null 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 21.4. Wir betrachten den Restklassenring

$$L = \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$

und bezeichnen die Restklasse von X mit x. Aufgrund von Proposition 21.3 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 null 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

$$\begin{aligned}(3x^2-2x+4)(2x^2+x-1) &= 6x^4+3x^3-3x^2-4x^3-2x^2+2x+8x^2+4x-4\\ &= 6x^4-x^3+3x^2+6x-4\\ &= 6(4x^2+5x-10)+2x^2-5+3x^2+6x-4\\ &= 29x^2+36x-69.\end{aligned}$$

21.3. **Endliche Körpererweiterungen.**

Wenn P in der vorstehenden Proposition irreduzibel ist, so ist $K[X]/(P)$ ein Körper und damit liegt eine Körpererweiterung

$$K \subseteq K[X]/(P) = L$$

vor. Bei einer K-Algebra und insbesondere einer Körpererweiterung hat man durch den Vektorraumbegriff sofort die folgenden Begriffe zur Verfügung.

Definition 21.5. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlich-dimensionaler Vektorraum über K ist.

Definition 21.6. 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 Satz 21.3(5) der Grad der Körpererweiterung gleich dem Grad von P.

21.4. **Minimalpolynom.**

Definition 21.7. 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 null verschiedenes Polynom $P \in K[X]$ gibt mit $P(f) = 0$.

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 21.8. 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 21.9. 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 bspw. $X - \sqrt{2}$ zwar ein annullierendes Polynom für $\sqrt{2}$ ist, dessen Koeffizienten aber nicht zu $\mathbb{Q}$ gehören.

Lemma 21.10. *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 13.6 und nach Satz 16.11 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. □

Definition 21.11. 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 $K[f] \subseteq K(f)$.

Satz 21.12. *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 Korollar 14.4 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 Satz 16.3 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 21.10 das vom Minimalpolynom erzeugte Hauptideal. □

Lemma 21.13. *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 null 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 21.10 ein Vielfaches des Minimalpolynoms P, sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad eins besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$.

□

22. Vorlesung

22.1. Algebraische Körpererweiterung.

Satz 22.1. *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*

$$f^0 = 1, f^1 = f, f^2, f^3, \dots .$$

(4) *Die von f über K erzeugte K-Algebra $K[f]$ hat endliche K-Dimension.*
(5) *f liegt in einer endlich-dimensionalen K-Algebra $M \subseteq L$.*

Beweis. (1) $\Rightarrow$ (2). Das ist trivial, da man ein von null verschiedenes Polynom stets normieren kann, indem man durch den Leitkoeffizienten durchdividiert. (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 null 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 endlich-dimensionalen Algebra $M \subseteq L$ liegt, so liegen darin auch alle Potenzen von f. Da es in einem endlich-dimensionalen Vektorraum keine unendliche Folge von linear unabhängigen Elementen geben kann, müssen diese Potenzen linear abhängig sein. □

Satz 22.2. *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 22.1 ist $M = K[f]$ eine endlich-dimensionale K-Algebra. Wir müssen zeigen, dass M ein Körper ist. Sei dazu $g \in M$ ein von null verschiedenes Element. Damit ist auch $K[g] \subseteq M = K[f]$, so dass $K[g]$ wieder eine endlich-dimensionale Algebra ist. Daher ist, wiederum nach Satz 22.1, das Element g algebraisch über K und es gibt ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(g) = 0$. Wir ziehen aus diesem Polynom die höchste Potenz von X heraus und schreiben

$$P = QX^k \, ,$$

wobei der konstante Term von Q von null verschieden sei. Die Ersetzung von X durch g ergibt

$$0 \, = \, P(g) \, = \, Q(g)g^k.$$

Da $g \neq 0$ ist und sich alles im Körper L abspielt, folgt $Q(g) = 0$. Wir können durch den konstanten Term von Q dividieren und erhalten die Gleichung

$$1 + c_1 g + \ldots + c_d g^d = 0\,.$$

Umstellen ergibt

$$g(-c_1 g^0 - \ldots - c_d g^{d-1}) = 1\,.$$

Das heißt, dass das Inverse zu g sich als Polynom in g schreiben lässt und daher zu $K[g]$ und erst recht zu $K[f]$ gehört. □

Korollar 22.3. *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 22.1 der Unterring $K[f]$ schon ein Körper. □

Bemerkung 22.4. 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 16.11 und Satz 17.12 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 $\overline{F} = z$.

22.2. **Algebraischer Abschluss.**

Definition 22.5. 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 22.6. *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 bzgl. 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 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 endlich-dimensionalen Unteralgebra ab. Daher sind Summe, Produkt und das Negative nach Satz 22.1 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 22.1 ein Körper von endlicher Dimension. Daher ist $z^{-1} \in K[z]$ selbst algebraisch. □

22.3. **Algebraische Zahlen.**

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 22.7. 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 22.8. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von null verschiedenes Polynom P mit rationalen Koeffizienten gibt mit $P(z) = 0$. 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.

22.4. **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 22.9. Eine endliche Körpererweiterung $K \subset L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Lemma 22.10. *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 schreiben

$$y^2 = a + by$$

bzw. (da 2 eine Einheit ist)

$$0 = y^2 - by - a = (y - \frac{b}{2})^2 - \frac{b^2}{4} - a.$$

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 22.11. *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 $\lambda_j = a_j + b_j i \in \mathbb{C}$. Das 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 Satz 21.12 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 $\mathbb{C} = L$ sein. □

22.5. **Das Irreduzibilitätskriterium von Eisenstein.**

Lemma 22.12. *(Eisenstein Irreduzibilitätskriterium)*

Sei R ein Integritätsbereich und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, alle anderen Koeffizienten teilt, aber dass p^2 nicht den

konstanten Koeffizienten c_0 teilt. Dann besitzt F keine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$.

Beweis. Sei angenommen, dass es eine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$ gäbe, und sei $G = \sum_{i=0}^{k} a_i X^i$ und $H = \sum_{j=0}^{m} b_j X^j$. Dann ist $c_0 = a_0 b_0$ und dies ist ein Vielfaches von p, aber nicht von p^2. Da p prim ist, teilt es einen der Faktoren, sagen wir a_0, aber nicht den anderen. Es ist nicht jeder Koeffizient von G ein Vielfaches von p, da sonst G und damit auch F ein Vielfaches von p wäre, was aber aufgrund der Bedingung an den Leitkoeffizienten ausgeschlossen ist. Es sei r der kleinste Index derart, dass a_r kein Vielfaches von p ist. Es ist $r \leq \operatorname{grad}(G) < \operatorname{grad}(F)$, da H nicht konstant ist. Wir betrachten den Koeffizienten c_r, für den

$$c_r = a_0 b_r + a_1 b_{r-1} + \ldots + a_{r-1} b_1 + a_r b_0$$

gilt. Hierbei sind c_r und alle Summanden $a_i b_{r-i}$, $i = 0, \ldots, r-1$, Vielfache von p. Daher muss auch der letzte Summand $a_r b_0$ ein Vielfaches von p sein. Dies ist aber ein Widerspruch, da $p \nmid a_r$ und $p \nmid b_0$. □

Satz 22.13. *Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$ und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, aber alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann ist F irreduzibel in $K[X]$.*

Beweis. Dies folgt aus Lemma 22.12 und Lemma 20.13. □

Korollar 22.14. *Sei p eine Primzahl und $n \geq 1$. Dann sind die Polynome $X^n - p$ irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Dies folgt direkt aus Satz 22.13 angewendet mit der Primzahl p. □

Korollar 22.15. *Es gibt endliche Körpererweiterungen von $\mathbb{Q}$ von beliebigem Grad.*

Beweis. Aufgrund von Satz 22.13 sind zu einer Primzahl p die Polynome $X^n - p \in \mathbb{Q}[X]$ irreduzibel und nach Satz 17.15 auch prim. Aufgrund von Satz 18.5 sind dann die Restklassenringe $\mathbb{Q}[X]/(X^n - p)$ Körper. Diese haben den Grad n nach Proposition 21.3. □

23. Vorlesung

23.1. **Die Gradformel.**

Satz 23.1. *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 aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j} x_1 + \ldots + a_{nj} x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= (a_{11} x_1 + \ldots + a_{n1} x_n) y_1 + \ldots + (a_{1m} x_1 + \ldots + a_{nm} x_n) y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

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 $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. 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. □

23.2. **Zerfällungskörper.**

Lemma 23.2. *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 18.5. 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 23.3. 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. 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 23.4. *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 23.5. *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 22.1 endliche Körpererweiterungen und nach Satz 23.1 ist dann die Gesamtkörpererweiterung ebenfalls endlich. □

Satz 23.6. *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*

$$\varphi : L_1 \longrightarrow L_2.$$

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 18.5

und nach Proposition 21.3 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 23.4 sind dann L_1 und L_2 Zerfällungskörper von $F \in K'[X]$. Nach Satz 23.1 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

$$\varphi : L_1 \longrightarrow L_2.$$

Dieser ist erst recht ein K-Algebra-Isomorphismus. □

23.3. **Konstruktion endlicher Körper.**

Endliche Körper mit der Anzahl p^n konstruiert man, indem man ein in $(\mathbb{Z}/(p))[X]$ irreduzibles Polynom vom Grad n findet. Ob ein gegebenes Polynom irreduzibel ist, lässt sich dabei grundsätzlich in endlich vielen Schritten entscheiden, da es ja zu jedem Grad überhaupt nur endlich viele Polynome gibt, die als Teiler in Frage kommen können. Zur Konstruktion von einigen kleinen endlichen Körpern siehe Aufgabe ***** und Aufgabe *****. Generell kann man einen Körper mit $q = p^n$ Elementen als Zerfällungskörper des Polynoms $X^q - X$ erhalten.

Lemma 23.7. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \left\{x \in K : x^q = x\right\}.$$

Dann ist M ein Unterkörper von K.

Beweis. Zunächst gilt für jedes Element $x \in \mathbb{Z}/(p) \subseteq K$, dass

$$x^{p^e} \;=\; (x^p)^{p^{e-1}} \;=\; x^{p^{e-1}} \;=\; \ldots \;=\; x$$

ist, wobei wir wiederholt den kleinen Fermat benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobenius

$$F : K \longrightarrow K,\ x \longmapsto x^p,$$

ist ein Ringhomomorphismus. Daher ist für $x, y \in M$ einerseits

$$(x+y)^q \;=\; F^e(x+y) \;=\; F^e(x) + F^e(y)$$

und andererseits

$$(xy)^q \;=\; x^q y^q \;=\; xy.$$

Ferner gilt für $x \in M$, $x \neq 0$, die Gleichheit

$$(x^{-1})^q = (x^q)^{-1} = x^{-1},$$

so dass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

Im Beweis der nächsten Aussage werden wir die Technik des *formalen Ableitens* verwenden. Ableiten ist eigentlich eine analytische Technik, und bekanntlich ist die Ableitung eines Monoms X^m gleich mX^{m-1}, und die Ableitung eines Polynoms ergibt sich durch lineare Fortsetzung dieser Regel. Da der Exponent der Variablen zum Vorfaktor wird, und da man jede ganze Zahl in jedem Körper eindeutig interpretieren kann, ergeben solche Ableitungen auch rein algebraisch für jeden Grundkörper Sinn. Wir definieren daher.

Definition 23.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zu einem Polynom

$$F = \sum_{i=0}^{n} a_i X^i \in K[X]$$

heißt das Polynom

$$F' = na_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + 3a_3X^2 + 2a_2X + a_1$$

die *formale Ableitung* von F.

Man beachte, dass, insbesondere bei positiver Charakteristik, das algebraische Ableiten einige überraschende Eigenschaften haben kann. In positiver Charakteristik p ist bspw.

$$(X^p)' = pX^{p-1} = 0.$$

Für einige grundlegende Eigenschaften des Ableitens siehe die Aufgaben. Wichtig ist für uns, dass man mit der formalen Ableitung testen kann, ob die Nullstellen eines Polynoms einfach oder mehrfach sind (eine Nullstelle a heißt *mehrfach*, wenn das zugehörige lineare Polynom $X-a$ das Polynom mehrfach teilt, d.h. wenn es in der Primfaktorzerlegung mit einem Exponenten ≥ 2 vorkommt).

Lemma 23.9. *Sei K ein Körper der Charakteristik $p > 0$, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K : x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 23.7 ist M ein Unterkörper von K, und nach Korollar 18.10 besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus $F' = -1$ und Aufgabe 23.14. □

Satz 23.10. *Sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Beweis. Existenz. Wir wenden Lemma 23.2 auf den Grundkörper $\mathbb{Z}/(p)$ und das Polynom $X^q - X$ an und erhalten einen Körper L der Charakteristik p, über dem $X^q - X$ in Linearfaktoren zerfällt. Nach Lemma 23.9 gibt es dann einen Unterkörper M von L, der aus genau q Elementen besteht.

Eindeutigkeit. Wir zeigen, dass ein Körper mit q Elementen der Zerfällungskörper des Polynoms $X^q - X$ sein muss, so dass er aufgrund dieser Eigenschaft nach Satz 23.6 eindeutig bestimmt ist. Sei also L ein Körper mit q Elementen, der dann $\mathbb{Z}/(p)$ als Primkörper enthält. Da $L^\times$ genau $q-1$ Elemente besitzt, gilt nach Satz 7.4 die Gleichung $x^{q-1} = 1$ für jedes $x \in L^\times$ und damit auch $x^q = x$ für jedes $x \in L$. Dieses Polynom vom Grad q hat also in L genau q verschiedene Nullstellen, so dass es also über L zerfällt. Zugleich ist der von allen Nullstellen erzeugte Unterkörper gleich L, so dass L der Zerfällungskörper ist. □

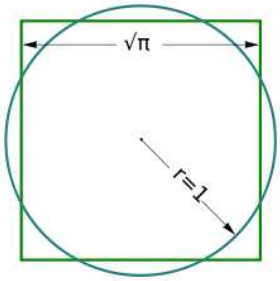
Notation 23.11. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 23.10 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Für $q = p$ ist $\mathbb{F}_p = \mathbb{Z}/(p)$. Dagegen sind für $q = p^e$, $e \geq 2$, die Ringe $\mathbb{F}_q$ und $\mathbb{Z}/(q)$ verschieden, obwohl beide Ringe q Elemente besitzen. Dies liegt einfach daran, dass $\mathbb{F}_q$ ein Körper ist, $\mathbb{Z}/(q)$ aber nicht.

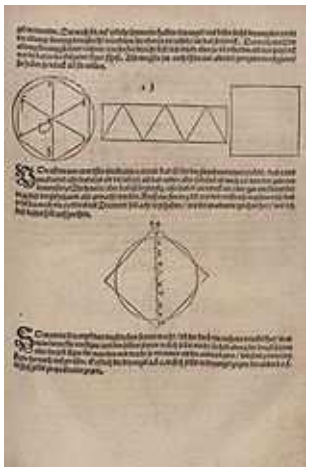
24. Vorlesung



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

24.1. **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 24.1. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Eine Gerade $G \subset E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $P, Q \in M$, $P \neq Q$, gibt derart, dass die Verbindungsgerade von P und Q gleich G ist. Ein Kreis $C \subseteq E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $Z, S \in M$, $Z \neq S$, gibt derart, 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 24.2. 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 24.3. 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.

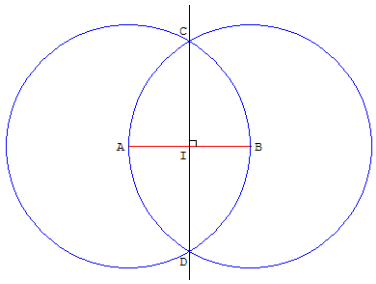
Definition 24.4. Eine Zahl $z \in \mathbb{C} \cong E$ heißt *konstruierbar* oder *konstruierbare Zahl*, wenn sie aus der Startmenge

$$\{0, 1\} \subset \mathbb{R} \subset \mathbb{C}$$

mit Zirkel und Lineal konstruierbar ist.

Bemerkung 24.5. 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 24.6. *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.

□

24.2. **Arithmetische Eigenschaften von konstruierbaren Zahlen.**

Lemma 24.7. *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 24.6 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 24.6 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 24.8. *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 24.9. *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 24.7 kann man sich beim Nachweis der Körpereigenschaften darauf beschränken, dass die reellen konstruierbaren Zahlen einen Körper bilden. Dies folgt aber aus Lemma 26.8. □

24.3. **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 24.10. *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 24.6 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

$$x^2 = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2 = \frac{a^2+2a+1-(a^2-2a+1)}{4} = \frac{4a}{4} = a.$$

Also repräsentiert x die Quadratwurzel aus a. □

Korollar 24.11. *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 auf einer der Achsen und schlagen einen Kreis um den Nullpunkt durch den Eckpunk 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 26.8 durch. Aus diesem Produkt zieht man nun gemäß Lemma 24.10 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.

25. Vorlesung

25.1. **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 immer gegeben durch die

Adjunktion einer Quadratwurel einer positiven reellen Zahl $\sqrt{c}$ mit $c \in K$, $\sqrt{c} \notin K$. Es gilt die Isomorphie

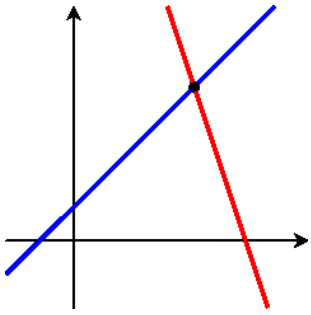
$$K[\sqrt{c}] \cong K[X]/(X^2 - c)\,.$$

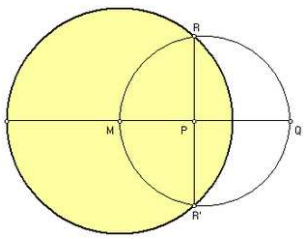
Lemma 25.1. *Sei $K \subseteq \mathbb{R}$ ein Körper. Es sei $P \in \mathbb{C}$ ein Punkt, der sich aus K^2 in einem Schritt konstruieren lässt. Dann liegen die Koordinaten von P in einer reell-quadratischen Körpererweiterung von K.*

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 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 $C_1 = \{(x,y)|\, (x-r_1)^2+(y-s_1)^2-a_1 = 0\}$ und $C_2 = \{(x,y)|\, (x-r_2)^2 + (y-s_2)^2 - a_2 = 0\}$ 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 25.2. 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 25.3. *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*

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n$$

gibt derart, 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 25.1 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 22.10 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 24.10 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 24.7 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 25.4. *Eine mit Zirkel und Lineal konstruierbare Zahl ist algebraisch.*

Beweis. Dies folgt direkt aus Satz 25.3, aus Satz 23.1 und aus Satz 22.1. □

Korollar 25.5. *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 25.3 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 $z \in L$. Dabei ist $\mathbb{Q}(z) = \mathbb{Q}[z] \subseteq L$ ein Unterkörper und daher ist nach Satz 23.1 der Grad von $\mathbb{Q}[z]$ über $\mathbb{Q}$ ein Teiler von 2^{n+1}, also selbst eine Potenz von 2. □

25.2. **Das Delische Problem.**

Die Bewohner der Insel Delos befragten während einer Pestepidemie 430 v. Chr. das Orakel von Delphi. Sie wurden aufgefordert, den wüürfelförmigen Altar des Apollon zu verdoppeln.

Korollar 25.6. *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 Satz 22.13 irreduzibel ist. Nach Korollar 25.5 ist $2^{1/3}$ nicht konstruierbar, da 3 keine Zweierpotenz ist. □

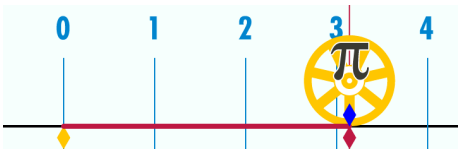
25.3. **Die Quadratur des Kreises.**

Satz 25.7. *Es ist nicht möglich, zu einem vorgegebenen Kreis ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren.*

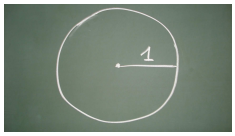
Beweis. Wenn es ein Konstruktionsverfahren gäbe, so könnte man insbesondere den Einheitskreis mit dem Radius 1 quadrieren, d.h. man könnte ein Quadrat mit der Seitenlänge $\sqrt{\pi}$ mit Zirkel und Lineal konstruieren. Nach Korollar 25.4 muss aber eine konstruierbare Zahl algebraisch sein. Nach dem 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.

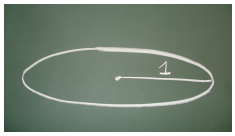
Beispiel 25.8. Die einfachste Art, die Zahl π geometrisch zu konstruieren, ist die *Abrollmethode*, bei der man einen Kreis mit Durchmesser 1 einmal exakt abrollt. Die zurückgeführte Entfernung ist genau der Kreisumfang, also π.



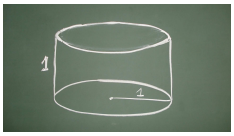
Beispiel 25.9.



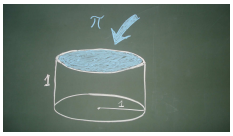
Wir starten mit einem Einheitskreis,



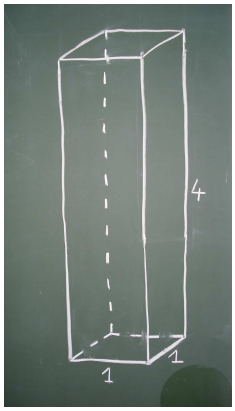
den wir als Grundfläche



eines Schwimmbeckens der Höhe 1 nehmen.

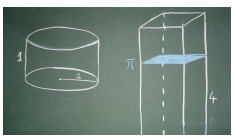


Das füllen wir randvoll mit Wasser auf.

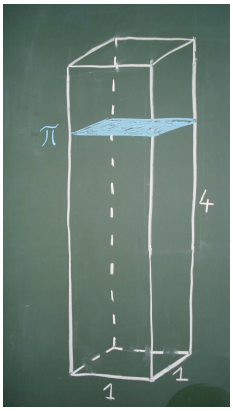


Wir nehmen ein zweites Schwimmbecken mit quadratischer Grundfläche 1×1 und Höhe 4.

Der Inhalt des ersten Schwimmbeckens wird



in das zweite Schwimmbecken gegossen.



Der Wasserstand im zweiten Schwimmbecken ist exakt π.

26. Vorlesung

26.1. **Einheitswurzeln.**

Definition 26.1. 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 Satz 19.7 ist diese Gruppe zyklisch mit einer Ordnung, die n teilt.

Definition 26.2. 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 26.3. *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

$$X^n - 1 = (X-1)(X - e^{2\pi i/n})\cdots(X - e^{2\pi i(n-1)/n})$$

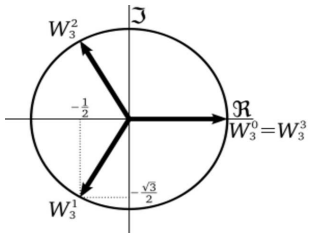
Beweis. Der Beweis verwendet einige Grundtatsachen über die *komplexe Exponentialfunktion*. Es ist

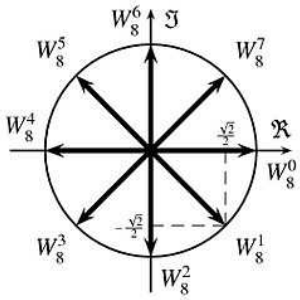
$$(e^{2\pi ik/n})^n = e^{2\pi ik} = (e^{2\pi i})^k = 1^k = 1.$$

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. □





26.2. **Kreisteilungskörper.**

Definition 26.4. 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,

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \ldots + X + 1)\,.$$

Wegen $1 \in \mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1} + X^{n-2} + \ldots + X + 1\,.$$

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 26.5. Eine Körpererweiterung $K \subseteq L$ heißt *einfach*, wenn es ein Element $x \in L$ gibt mit

$$L = K(x)\,.$$

Lemma 26.6. *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*

$$K_n = \mathbb{Q}(e^{2\pi i/n}) = \mathbb{Q}[e^{2\pi i/n}]\,.$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$

Beweis. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Wegen $(e^{2\pi i/n})^n = 1$ ist $\mathbb{Q}[e^{2\pi i/n}] \subseteq K_n$. Wegen $(e^{2\pi i/n})^k = e^{2\pi ik/n}$ 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.

Beispiel 26.7. 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

$$X^2 + X + 1 = (X + \frac{1}{2} - i\frac{\sqrt{3}}{2})(X + \frac{1}{2} + i\frac{\sqrt{3}}{2}) .$$

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

$$\begin{array}{rcl} X^4 - 1 & = & (X^2 - 1)(X^2 + 1) \\ & = & (X - 1)(X + 1)(X^2 + 1) \\ & = & (X - 1)(X + 1)(X - i)(X + i). \end{array}$$

Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

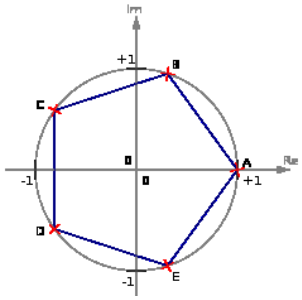
Lemma 26.8. *Sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/(X^{p-1} + X^{p-2} + \ldots + X^1 + 1)$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p - 1$ über $\mathbb{Q}$.

Beweis. Der p-te Kreisteilungskörper wird nach Lemma 26.6 von $e^{2\pi i/p}$ erzeugt, er ist also isomorph zu $\mathbb{Q}[X]/(P)$, wobei P das Minimalpolynom von $e^{2\pi i/p}$ bezeichnet. Als Einheitswurzel ist $e^{2\pi i/p}$ eine Nullstelle von $X^p - 1$ und wegen $e^{2\pi i/p} \neq 1$ ist $e^{2\pi i/p}$ eine Nullstelle von $X^{p-1} + X^{p-2} + \ldots + X^1 + 1$. Das Polynom $X^{p-1} + X^{p-2} + \ldots + X^1 + 1$ ist irreduzibel nach Aufgabe 22.12 und daher handelt es sich nach Lemma 21.13 um das Minimalpolynom von $e^{2\pi i/p}$. □

Weiter unten werden wir für jedes n die Minimalpolynome der primitiven n-ten Einheitswurzeln bestimmen.



Beispiel 26.9. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi i/5}$ erzeugt. Er hat aufgrund von Lemma 26.8 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 25.3, dass die fünften Einheitswurzeln konstruierbare Zahlen sind.

26.3. **Kreisteilungspolynome.**

Definition 26.10. Sei $n \in \mathbb{N}_+$ und seien $z_1, \ldots, z_{\varphi(n)}$ die primitiven komplexen Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i) \in \mathbb{C}[X]$$

das n-te *Kreisteilungspolynom*.

Nach Konstruktion hat das n-te Kreisteilungspolynom den Grad $\varphi(n)$.

Lemma 26.11. *Sei $n \in \mathbb{N}_+$. Dann gilt in $\mathbb{C}[X]$ die Gleichung*

$$X^n - 1 = \prod_{d|n} \Phi_d\,.$$

Beweis. Jede der n verschiedenen n-ten Einheitswurzeln besitzt eine Ordnung d, die ein Teiler von n ist. Eine n-te Einheitswurzel der Ordnung d ist eine primitive d-te Einheitswurzel. Die Aussage folgt daher aus

$$\begin{aligned} X^n - 1 &= \prod_{z \text{ ist } n\text{-te Einheitswurzel}} (X - z) \\ &= \prod_{d|n} \Big(\prod_{z \text{ ist primitive } d\text{-te Einheitswurzel}} (X - z) \Big) \\ &= \prod_{d|n} \Phi_d. \end{aligned}$$

□

Lemma 26.12. *Die Koeffizienten der Kreisteilungspolynome liegen in $\mathbb{Z}$.*

Beweis. Induktion über n. Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Für beliebiges n betrachten wir die in Lemma 26.11 bewiesene Darstellung

$$X^n - 1 = \prod_{d|n} \Phi_d = (\prod_{d|n,\, d\neq n} \Phi_d) \cdot \Phi_n \, .$$

Der linke Faktor ist ein normiertes Polynom und er besitzt nach der Induktionsvoraussetzung Koeffizienten in $\mathbb{Z}$. Daraus folgt mit Aufgabe 26.5, dass auch Φ_n Koeffizienten in $\mathbb{Z}$ besitzt. □

Grundlegend ist die folgende Aussage.

Satz 26.13. *Die Kreisteilungspolynome Φ_n sind irreduzibel über $\mathbb{Q}$.*

Beweis. Nehmen wir an, dass Φ_n nicht irreduzibel über $\mathbb{Q}$ ist. Dann gibt es nach Lemma 20.13 eine Zerlegung $\Phi_n = FG$ mit normierten Polynomen $F, G \in \mathbb{Z}[X]$ von kleinerem Grad. Wir fixieren eine primitive n-te Einheitswurzel ζ. Dann ist nach Definition der Kreisteilungspolynome $\Phi_n(\zeta) = 0$ und daher ist (ohne Einschränkung) $F(\zeta) = 0$. Wir können annehmen, dass F irreduzibel und normiert ist, also das Minimalpolynom von ζ ist.Wir werden zeigen, dass jede primitive n-te Einheitswurzel ebenfalls eine Nullstelle von F ist. Dann folgt aus Gradgründen $\operatorname{grad}(F) = \varphi(n) = \operatorname{grad}(\Phi_n)$ im Widerspruch zur Reduzibilität. Jede primitive Einheitswurzel kann man schreiben als ζ^k mit einer zu n teilerfremden Zahl k. Es genügt dabei, den Fall ζ^p mit einer zu n teilerfremden Primzahl p zu betrachten, da sich jedes ζ^k sukzessive als p-Potenz erhalten lässt (wobei man ζ sukzessive durch ζ^p ersetzt und $F(\zeta^p) = 0$ verwendet). Nehmen wir also an, dass $F(\zeta^p) \neq 0$ ist. Dann muss $G(\zeta^p) = 0$ sein. Daher ist ζ eine Nullstelle des Polynoms $G(X^p)$ und daher gilt $FH = G(X^p)$ mit $H \in \mathbb{Q}[X]$, da ja F das Minimalpolynom von ζ ist. Wegen Aufgabe 26.5 gehören die Koeffizienten von H zu $\mathbb{Z}$. Wir betrachten nun die Polynome Φ_n, F, G, H modulo p, also als Polynome in $\mathbb{Z}/(p)[X]$, wobei wir dafür $\overline{\Phi_n}, \overline{F}$ usw. schreiben. Aufgrund des Frobenius-Homomorphismus in Charakteristik p und Satz 14.14 gilt

$$\overline{G}(X^p) = (\overline{G}(X))^p \, .$$

Daher ist

$$\overline{FH} \, = \, \overline{G}(X^p) \, = \, (\overline{G}(X))^p .$$

Sei nun $\mathbb{Z}/(p) \subseteq L$ der Zerfällungskörper von $X^n - 1$ über $\mathbb{Z}/(p)$, so dass über L insbesondere auch $\overline{\Phi_n}$ und damit auch $\overline{F}$ in Linearfaktoren zerfällt. Sei $u \in L$ eine Nullstelle von $\overline{F}$. Dann ist u wegen der obigen Teilbarkeitsbeziehung auch eine Nullstelle von $\overline{G}$. Wegen $\overline{\Phi_n} = \overline{FG}$ ist dann u eine mehrfache Nullstelle von $\overline{\Phi_n}$. Damit besitzt auch $X^n - 1$ eine mehrfache Nullstelle in L. Nach dem formalen Ableitungskriterium ist aber $(X^n - 1)' = (n \bmod p)X^{n-1}$ und dieser Koeffizient ist nicht null. Also erzeugt das Polynom $X^n - 1$ und seine Ableitung das Einheitsideal, so dass es nach Aufgabe 23.14

keine mehrfache Nullstellen geben kann und wir einen Widerspruch erhalten. □

Korollar 26.14. *Der n-te Kreisteilungskörper K_n über $\mathbb{Q}$ hat die Beschreibung*

$$K_n = \mathbb{Q}[X]/(\Phi_n)\,,$$

wobei Φ_n das n-te Kreisteilungspolynom bezeichnet. Der Grad des n-ten Kreisteilungskörpers ist $\varphi(n)$.

Beweis. Es ist $K_n = \mathbb{Q}[\zeta]$, wobei ζ eine primitive n-te Einheitswurzel ist. Nach Definition des Kreisteilungspolynoms ist $\Phi_n(\zeta) = 0$ und nach Satz 26.13 ist das Kreisteilungspolynom irreduzibel, so dass es sich um das Minimalpolynom von ζ handeln muss. Also ist nach Satz 21.12 $K_n \cong \mathbb{Q}[X]/(\Phi_n)$. □

27. Vorlesung

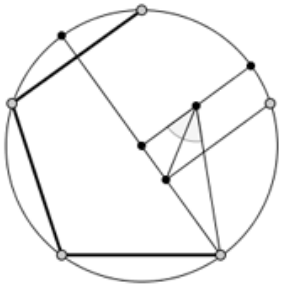
27.1. **Konstruierbare Einheitswurzeln.**

Definition 27.1. Sei $n \in \mathbb{N}_+$. Man sagt, dass *das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar* ist, wenn die komplexe Zahl

$$e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$$

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 26.7, 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 26.9 bzw. Aufgabe 26.9 gezeigt wurde. Wir werden im Folgenden sowohl positive als auch negative Resultate zur Konstruierbarkeit von regelmäßigen n-Ecken vorstellen.



Lemma 27.2. *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 24.9 die Potenz

$$(e^{\frac{2\pi i}{nk}})^n = e^{\frac{2\pi i}{k}}$$

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

$$(e^{\frac{2\pi i}{n}})^s (e^{\frac{2\pi i}{k}})^r = (e^{\frac{2\pi ik}{nk}})^s (e^{\frac{2\pi in}{nk}})^r = e^{\frac{2\pi isk}{nk}} e^{\frac{2\pi irn}{nk}} = e^{\frac{2\pi i(sk+rn)}{nk}} = e^{\frac{2\pi i}{nk}}$$

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 27.3. *Sei n eine natürliche Zahl derart, dass das regelmäßige n-Eck konstruierbar ist. Dann ist $\varphi(n)$ eine Zweierpotenz.*

Beweis. Die Voraussetzung besagt, dass die primitive Einheitswurzel $\zeta = e^{\frac{2\pi i}{n}}$ konstruierbar ist. Dann muss nach Korollar 25.5 der Grad des Minimalpolynoms von ζ eine Zweierpotenz sein. Nach Korollar 26.14 ist das Minimalpolynom von ζ das n-te Kreisteilungspolynom, und dieses hat den Grad $\varphi(n)$. Also muss $\varphi(n)$ eine Zweierpotenz sein. □

27.2. **Winkeldreiteilung.**

Wir sind nun in der Lage, das Problem der Winkeldreiteilung zu beantworten.

Korollar 27.4. *Das regelmäßige* 9*-Eck ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Wäre das regelmäßige 9-Eck konstruierbar, so müsste nach Satz 27.3 $\varphi(9)$ eine Zweierpotenz sein. Es ist aber $\varphi(9) = 2 \cdot 3 = 6$. □

Satz 27.5. *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 27.4 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 beruht.

Lemma 27.6. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes Polynom vom Grad ≤ 3 ohne Nullstelle in $\mathbb{Z}$. Dann ist F irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Aufgrund von Lemma 20.13 und der Gradvoraussetzung genügt es zu zeigen, dass es keine Faktorzerlegung $F = GH$ in $\mathbb{Z}[X]$ mit $\operatorname{grad}(G) = 1$ geben kann. Sei also angenommen, dass $G = aX + b \in \mathbb{Z}[X]$ ein Teiler von F ist. Der Leitkoeffizient a teilt den Leitkoeffizienten von F, also 1, daher muss $a \in \mathbb{Z}$ eine Einheit sein. Dann ist $a = \pm 1$ und somit ist $\pm b$ eine Nullstelle im Widerspruch zur Voraussetzung. □

Einfache Beispiele wie $F = (2X + 1)^2$ zeigen, dass ohne die Voraussetzung normiert die Aussage nicht stimmt. Dass ein ganzzahliges normiertes Polynom keine ganzzahligen Nullstellen besitzt, ist im Allgemeinen einfach zu zeigen. Für n betragsmäßig groß kann man durch eine einfache Abschätzung zeigen, dass es dafür keine Nullstelle geben kann, und für n in einem verbleibenden überschaubaren Bereich kann man durch explizites Ausrechnen feststellen, ob eine Nullstelle vorliegt oder nicht.

Bemerkung 27.7. 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

$$\begin{aligned}(2\cos 20^\circ)^3 - 3(2\cos 20^\circ) - 1 &= 2(4\cos^3 20^\circ - 3\cos 20^\circ - \frac{1}{2}) \\ &= 2(\cos 60^\circ - \frac{1}{2}) \\ &= 0.\end{aligned}$$

Also wird $2\cos 20^\circ$ vom Polynom $X^3 - 3X - 1$ annulliert. Dieses Polynom hat keine ganzzahlige Nullstelle und ist daher nach Lemma 27.6 irreduzibel. Also muss es nach Lemma 21.13 das Minimalpolynom von $2\cos 20^\circ$ sein. Daher kann $2\cos 20^\circ$ nach Korollar 25.5 nicht konstruierbar sein und damit ebensowenig $\cos 20^\circ$.

27.3. **Fermatsche Primzahlen.**

Die Frage der Konstruierbarkeit von regelmäßigen n-Ecken führt uns zu Fermatschen Primzahlen.

Definition 27.8. 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 27.9. *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

$$2^{2^k u} + 1 = (2^{2^k})^u + 1\,.$$

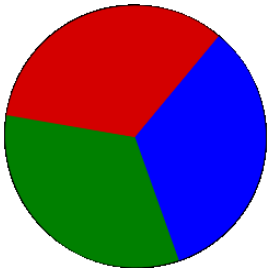
Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

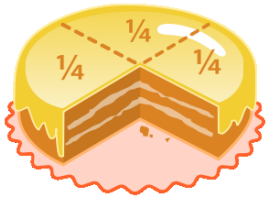
$$X^u + 1 = (X+1)(X^{u-1} - X^{u-2} + X^{u-3} - \ldots + X^2 - X + 1)\,.$$

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 $u = 1$. □

Eine Fermatsche Primzahl ist nach diesem Lemma also insbesondere eine Fermat-Zahl im Sinne der folgenden Definition.

Definition 27.10. Eine Zahl der Form $2^{2^r} + 1$, wobei r eine natürliche Zahl ist, heißt *Fermat-Zahl*.





Satz 27.11. *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat*

$$n = 2^\alpha p_1 \cdots p_k \,,$$

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 27.3 muss die eulersche Funktion eine Zweierpotenz sein, also

$$\varphi(n) = 2^t \,.$$

Andererseits gilt nach Korollar 15.16 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 27.2 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. □

Arbeitsblätter

1. Arbeitsblatt

Aufgabe 1.1. (2 Punkte)

Bestimme die vier Bewegungen an einem Würfel mit den Eckpunkten $(\pm 1, \pm 1, \pm 1)$ in Matrixschreibweise, die $(1, 0, 0)$ auf $(0, 0, -1)$ abbilden.

Aufgabe 1.2. (2 Punkte)

Wie viele (wesentlich verschiedene) Möglichkeiten gibt es, die Seiten eines Würfels von 1 bis 6 zu nummerieren, so dass die Summe gegenüberliegender Seiten stets 7 ergibt. Wie viele Möglichkeiten gibt es überhaupt?

Aufgabe 1.3. (3 Punkte)

Die Ecken $(\pm 1, \pm 1, \pm 1)$ eines Würfels seien mit $1, 2, 3, \ldots, 8$ (oder ähnlich) bezeichnet (Skizze!). Beschreibe durch Wertetabellen, wie die folgenden (eigentlichen oder uneigentlichen) Würfelsymmetrien die Eckpunkte permutieren:

(1) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$,

(2) $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$,

(3) $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$.

Was passiert mit den Kantenmittelpunkten unter diesen Bewegungen?

Aufgabe 1.4. (2 Punkte)

Sei W der Würfel mit den Eckpunkten $(\pm 1, \pm 1, \pm 1)$. Fixiere eine Kantenmittelpunktachse (durch den Nullpunkt). Welche Bewegungen des Würfels lassen sich als Drehung um diese Achse beschreiben? Wie sehen diese Bewegungen in Matrixschreibweise aus, und was passiert dabei mit den Eckpunkten des Würfels?

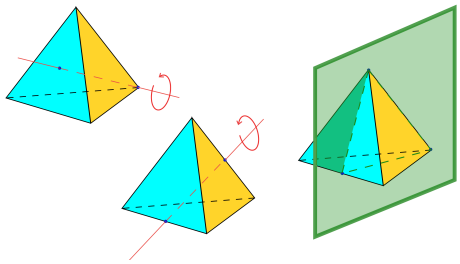
Aufgabe 1.5. (2 Punkte)

Es sei W der Würfel mit den Eckpunkten $(\pm 1, \pm 1, \pm 1)$. Es sei φ eine Dritteldrehung um die Raumdiagonale durch (1,1,1) *und* (-1,-1,-1) .Bestimme Ebenengleichungen für diejenigen Ebenen, auf denen je drei Eckpunkte liegen, die durch diese Drehung ineinander überführt werden.

Aufgabe 1.6. (3 Punkte)

Bestimme die Koordinaten eines Tetraeders, bei dem der Nullpunkt der Mittelpunkt ist, die vier Eckpunkte des Tetraeders vom Nullpunkt den Abstand eins besitzen, der Punkt $(0, 0, 1)$ ein Eckpunkt ist und ein weiterer Eckpunkt Koordinaten der Form $(u, 0, v)$ besitzt.

Aufgabe 1.7. (5 Punkte)



Man gebe für die in den obigen Skizzen angedeuteten Symmetrien des Tetraeders eine geeignete Matrixdarstellung.

Aufgabe 1.8. (3 Punkte)

Betrachte ein Rechteck in der Ebene, das kein Quadrat sei, und dessen Mittelpunkt der Nullpunkt sei und dessen Seiten parallel zu den Koordinatenachsen liegen mögen. Bestimme die Matrizen, die die (eigentlichen und uneigentlichen) Symmetrien des Rechteckes beschreiben. Erstelle eine Verknüpfungstafel für diese Symmetriegruppe.

2. Arbeitsblatt

Wir beginnen mit ein paar Aufwärmaufgaben, die nicht abzugeben sind.

Aufgabe 2.1. Sei G eine Gruppe und $x, y \in G$. Drücke das Inverse von xy durch die Inversen von x und y aus.

Aufgabe 2.2. 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 2.3. Man bringe für die Symmetrien am Würfel die Begriffe „Drehachse“, „Eigenvektor“ und „Eigenwert“ in Verbindung. Welche Eigenwerte können auftreten?

Aufgabe 2.4. 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.

Es folgen die Aufgaben, die man abgeben darf.

Aufgabe 2.5. (3 Punkte)

Man bestimme für jede natürliche Zahl, wie viele eigentliche Würfelsymmetrien es gibt, die diese Zahl als Ordnung besitzen. Man gebe für jede Zahl, die als Ordnung einer eigentlichen Würfelsymmetrie auftritt, eine Matrixdarstellung einer Symmetrie an, die diese Ordnung besitzt.

Aufgabe 2.6. (3 Punkte)

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

Aufgabe 2.7. (3 Punkte)

Sei G eine Gruppe, in der jedes Element die Ordnung zwei hat, d.h. für jedes Gruppenelement g gilt $g^2 = e$. Man zeige, dass die Gruppe G dann abelsch ist.

Aufgabe 2.8. (3 Punkte)

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

Aufgabe 2.9. (5 Punkte)

Betrachte die Gruppe der Bewegungen an einem Würfel W. Es sei φ eine Vierteldrehung um eine Seitenmittelpunktachse, β sei eine Halbdrehung um dieselbe Seitenmittelpunktachse, ψ sei eine Dritteldrehung um eine Diagonalachse und θ eine Halbdrehung um eine Kantenmittelpunktachse. Wie viele Elemente besitzen die von je zwei Elementen erzeugten Untergruppen?

Aufgabe 2.10. (3 Punkte)

Es seien φ und ψ Bewegungen am Würfel. Zeige, dass die Drehachse von φ und die Drehachse von ψ *nicht* die Drehachse der Komposition $\varphi \circ \psi$ bestimmen. (Man gebe ein Beispiel, in dem die Identität nicht vorkommt.)

Aufgabe 2.11. (3 Punkte)

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

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

die Verknüpfung

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

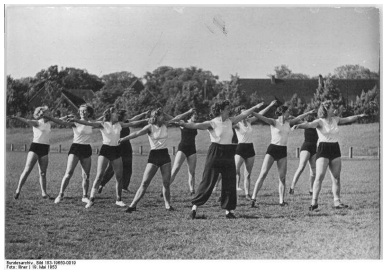
Zeige, dass dadurch eine assoziative Verknüpfung auf dieser Menge definiert ist, und dass damit sogar eine Gruppe vorliegt.

Aufgabe 2.12. (2 Punkte)

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

3. Arbeitsblatt

Wir beginnen mit Aufgaben zum Aufwärmen.



Aufgabe 3.1. Zeige, dass für zwei ganze Zahlen $a, b \in \mathbb{Z}$ die folgenden Beziehungen äquivalent sind.

(1) a teilt b (also $a|b$).
(2) $b \in \mathbb{Z}a$.
(3) $\mathbb{Z}b \subseteq \mathbb{Z}a$.

Aufgabe 3.2. 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 3.3. 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?

Die „echten“ Aufgaben.

Aufgabe 3.4. (2 Punkte)

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

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

Aufgabe 3.5. (2 Punkte)

Es sei G eine Gruppe, $x \in G$ ein Element und $H \subseteq G$ eine Untergruppe. Zeige, dass die Menge

$$M = \{k \in \mathbb{Z} :\ x^k \in H\}$$

die Form $M = \mathbb{Z}d$ besitzt mit einer eindeutig bestimmten ganzen Zahl $d \geq 0$.

Aufgabe 3.6. (3 Punkte)

Beweise die Teilbarkeitsregeln für ganze Zahlen, die in Lemma 3.7 aufgelistet sind.

Aufgabe 3.7. (2 Punkte)

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.

Aufgabe 3.8. (2 Punkte)

Sei K ein archimedisch angeordneter Körper. Dann gibt es für jedes $s \in K$ eine ganze Zahl q und ein $t \in K$ mit $0 \leq t < 1$ und mit

$$s = q + t\,.$$

Aufgabe 3.9. (3 Punkte)

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 3.10. (3 Punkte)

Es sei Z eine endliche zyklische Gruppe der Ordnung 12. Wie viele Untergruppen gibt es darin?

Aufgabe 3.11. (5 Punkte)

Betrachte ein gleichseitiges Dreieck in der x, y-Ebene mit $(0, 0)$ als Mittelpunkt und mit $(1, 0)$ als einem der Eckpunkte. Betrachte darüber die doppelte Pyramide D mit oberer Spitze $(0, 0, 2)$ und unterer Spitze $(0, 0, -2)$. Bestimme die Matrizen der (eigentlichen) Bewegungen, die D in sich überführen, ihre Drehachsen und erstelle eine Verknüpfungstabelle für diese Bewegungen.

Beschreibe ferner, was unter diesen Bewegungen mit den drei Eckpunkten des zugrundeliegenden Dreiecks geschieht.

4. Arbeitsblatt

Zwei Aufwärmaufgaben

Aufgabe 4.1. Geben Sie eine Darstellung des ggT von 5 *und* 7 an. Wie viele solche Darstellungen gibt es?

Aufgabe 4.2. Bestimme den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache von 105 *und* 150 .

Aufgabe 4.3. (3 Punkte)

Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 3711 und 4115.

Aufgabe 4.4. (4 Punkte)

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

Vor der nächsten Aufgabe erinnern wir an die Fibonacci-Zahlen.

Die Folge der *Fibonacci-Zahlen* f_n ist rekursiv definiert durch

$$f_1 := 1\,, f_2 := 1 \text{ und } f_{n+2} := f_{n+1} + f_n\,.$$

Aufgabe 4.5. (2 Punkte)

Wende auf zwei aufeinander folgende Fibonacci-Zahlen den euklidischen Algorithmus an. Welche Gesetzmäßigkeit tritt auf?

Aufgabe 4.6. (3 Punkte)

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 4.7. (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 4.8. (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 4.9. (2 Punkte)

Sei $a_1, \ldots, a_n$ eine Menge von ganzen Zahlen. Zeige, dass das nichtnegative kleinste gemeinsame Vielfache der a_i mit demjenigen gemeinsamen Vielfachen übereinstimmt, das bezüglich der Ordnungsrelation „$\leq$“ das kleinste gemeinsame Vielfache ist.

Aufgabe 4.10. (2 Punkte)

Zeige, dass die Verknüpfung

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

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

5. Arbeitsblatt

Wir beginnen mit drei Aufwärmaufgaben.

Aufgabe 5.1. Beweise Lemma 5.3.

Aufgabe 5.2. Sei G eine Gruppe und sei $\varphi : G \to G$ ein Gruppenhomomorphismus. Zeige, dass die Menge der Fixpunkte von φ eine Untergruppe von G bildet.

Aufgabe 5.3. 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 5.4. (2 Punkte)

Betrachte die Matrix

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}.$$

Zeige, dass diese Matrix einen Gruppenhomomorphismus von $\mathbb{Q}^2$ nach $\mathbb{Q}^2$ und ebenso von $\mathbb{Z}^2$ nach $\mathbb{Z}^2$ definiert. Untersuche diese beiden Gruppenhomomorphismen in Hinblick auf Injektivität und Surjektivität.

Aufgabe 5.5. (3 Punkte)

Es seien $G_1, \ldots, G_n$ Gruppen. Definiere eine Gruppenstruktur auf dem Produkt

$$G_1 \times \cdots \times G_n\,.$$

Es sei H eine weitere Gruppe. Zeige, dass eine Abbildung

$$\varphi : H \longrightarrow G_1 \times \cdots \times G_n,\ x \longmapsto \varphi(x) = \varphi_1(x), \ldots, \varphi_n(x)\,,$$

genau dann ein Gruppenhomomorphismus ist, wenn alle Komponenten φ_i Gruppenhomomorphismen sind.

Aufgabe 5.6. (1 Punkt)

Sei G eine (multiplikativ geschriebene) kommutative Gruppe und sei $n \in \mathbb{N}$. Zeige, dass dann das Potenzieren

$$G \longrightarrow G,\, x \longmapsto x^n\,,$$

ein Gruppenhomomorphismus ist.

Aufgabe 5.7. (3 Punkte)

Bestimme die Gruppenhomomorphismen von $(\mathbb{Q}, +, 0)$ nach $(\mathbb{Z}, +, 0)$.

Aufgabe 5.8. (2 Punkte)

Stifte einen surjektiven Gruppenhomomorphismus von der Gruppe der komplexen Zahlen ohne null $(\mathbb{C}, 1, \cdot)$ und der multiplikativen Gruppe der positiven reellen Zahlen $(\mathbb{R}_+, 1, \cdot)$.

Aufgabe 5.9. (3 Punkte)

Betrachte die Gruppe der komplexen Zahlen ohne null, $\mathbb{C}^\times = (\mathbb{C}, 1, \cdot)$. Bestimme für jedes $n \in \mathbb{N}$ den Kern des Potenzierens

$$\mathbb{C}^\times \longrightarrow \mathbb{C}^\times,\, z \longmapsto z^n\,.$$

Sind diese Gruppenhomomorphismen surjektiv?

Aufgabe 5.10. (3 Punkte)

Seien V *und* W zwei $\mathbb{Q}$-Vektorräume und sei

$$\varphi : V \longrightarrow W$$

ein Gruppenhomomorphismus. Zeige, dass φ bereits $\mathbb{Q}$-linear ist.

Die letzte Aufgabe ist eher zum Nachdenken als zum Lösen gedacht und ist nicht abzugeben.

Aufgabe 5.11. Gibt es Gruppenhomomorphismen

$$(\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}, +, 0)\,,$$

die nicht $\mathbb{R}$-linear sind?

6. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 6.1. Skizziere ein Inklusionsdiagramm für sämtiche Teilmengen einer dreielementigen Menge.

Aufgabe 6.2. Skizziere ein Teilerdiagramm für die Zahlen $25, 30, 36$ sowie all ihrer positiven Teiler.

Aufgabe 6.3. Sei G eine Gruppe. Betrachte die Relation $\sim$ auf G, die durch

$x \sim y$ genau dann, wenn $x = y$ oder $x = y^{-1}$

erklärt ist. Zeige, dass $\sim$ eine Äquivalenzrelation ist.

Aufgabe zum Abgeben

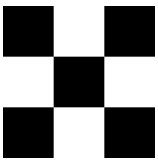
Aufgabe 6.4. (2 Punkte)

Es sei M eine Menge mit n Elementen. Bestimme die Anzahl der Relationen auf M, die

(1) reflexiv
(2) symmetrisch
(3) reflexiv und symmetrisch

sind.

Aufgabe 6.5. (2 Punkte)
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 6.6. (2 Punkte)

Sei G eine Gruppe und betrachte die Relation R auf G, wobei xRy bedeutet, dass es einen inneren Automorphismus κ_g gibt mit $x = \kappa_g(y)$. Zeige, dass diese Relation eine Äquivalenzrelation ist.

Die Äquivalenzklassen zu dieser Äquivalenzrelation bekommen einen eigenen Namen:

Zu einer Gruppe G nennt man die Äquivalenzklassen zur Äquivalenzrelation, bei der zwei Elemente als äquivalent (oder *konjugiert*) gelten, wenn sie durch einen inneren Automorphismus ineinander überführt werden können, die *Konjugationsklassen*.

Aufgabe 6.7. (3 Punkte)

Bestimme die Konjugationsklassen der Würfelgruppe.

Aufgabe 6.8. (2 Punkte)

Es sei S_3 die Gruppe der bijektiven Abbildungen der Menge $\{1, 2, 3\}$ in sich selbst. Bestimme die Konjugationsklassen dieser Gruppe.

Aufgabe 6.9. (3 Punkte)

Es sei $\mathrm{Mat}_n(\mathbb{R})$ die Menge der reellen invertierbaren $n \times n$-Matrizen. Zeige, dass für konjugierte Matrizen M *und* N die folgenden Eigenschaften bzw. Invarianten übereinstimmen: die Determinante, die Eigenwerte, die Dimension der Eigenräume zu einem Eigenwert, die Diagonalisierbarkeit, die Trigonalisierbarkeit.

Aufgabe 6.10. (2 Punkte)

Es sei $U \subseteq \mathbb{R}^n$ eine Teilmenge mit der induzierten Metrik. Betrachte die Relation R auf U, wobei xRy bedeutet, dass es eine stetige Abbildung

$$\gamma : [0,1] \longrightarrow \mathbb{R},\, t \longmapsto \gamma(t)\,,$$

gibt mit $\gamma(0) = x$ und $\gamma(1) = y$. Zeige, dass dies eine Äquivalenzrelation auf U ist.

7. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 7.1. Seien G *und* H Gruppen und sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Ist das Bild von φ ein Normalteiler in H?

Aufgabe 7.2. Sei G eine Gruppe und sei $g \in G$ ein Element und sei

$$\varphi : G \longrightarrow G,\, h \longmapsto hg,$$

die Multiplikation mit g. Zeige, dass φ bijektiv ist und dass φ genau dann ein Gruppenhomomorphismus ist, wenn $g = e_G$ ist.

Aufgabe 7.3. Sei p eine Primzahl und sei G eine Gruppe der Ordnung p. Zeige, dass G eine zyklische Gruppe ist.

Aufgabe 7.4. Seien G *und* H Gruppen und sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Zeige, dass das Urbild $\varphi^{-1}(N)$ eines Normalteilers $N \subseteq H$ ein Normalteiler in G ist.

Aufgabe 7.5. Zeige, dass der Durchschnitt von Normalteilern N_i, $i \in I$, in einer Gruppe G ein Normalteiler ist.

Aufgaben zum Abgeben

Aufgabe 7.6. (2 Punkte)

Bestimme die Untergruppen von $\mathbb{Z}\,\mathrm{mod}\,15$.

Aufgabe 7.7. (2 Punkte)

Seien G *und* H Gruppen und sei $\varphi : G \to H$ ein surjektiver Gruppenhomomorphismus. Zeige, dass das Bild $\varphi(N)$ eines Normalteilers $N \subseteq G$ ein Normalteiler in H ist.

Aufgabe 7.8. (2 Punkte)

Zeige, dass jede Untergruppe vom Index zwei in einer Gruppe G ein Normalteiler in G ist.

Aufgabe 7.9. (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 7.10. (2 Punkte)

Sei G eine Gruppe und sei M eine Menge mit einer Verknüpfung. Es sei

$$\varphi : G \longrightarrow M$$

eine surjektive Abbildung mit $\varphi(gh) = \varphi(g)\varphi(h)$ für alle $g, h \in G$. Zeige, dass M eine Gruppe und dass φ ein Gruppenhomomorphismus ist.

Aufgabe 7.11. (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.

8. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 8.1. Sei G eine Gruppe und $g \in G$ ein Element mit dem (nach Lemma 5.5) zugehörigen Gruppenhomomorphismus

$$\varphi : \mathbb{Z} \longrightarrow G,\ n \longmapsto g^n.$$

Beschreibe die kanonische Faktorisierung von φ gemäß Satz 8.3.

Aufgabe 8.2. Zeige mit Hilfe der Homomorphiesätze, dass zyklische Gruppen mit der gleichen Ordnung isomorph sind.

Aufgabe 8.3. Seien G, H *und* F Gruppen und seien $\varphi : G \to H$ und $\psi : G \to F$ Gruppenhomomorphismen mit ψ surjektiv und mit $\ker \psi \subseteq \ker \varphi$. Bestimme den Kern des induzierten Homomorphismus

$$\tilde{\varphi} : F \longrightarrow H.$$

Aufgabe 8.4. 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.

Aufgabe 8.5. Berechne für die Permutation σ mit

P	1	2	3	4	5	6	7	8	9	10
$\sigma(P)$	7	10	3	9	5	2	4	1	8	6

die Potenzen σ^2 und σ^3 und gebe die Zyklendarstellung für diese drei Permutationen an.

Aufgabe 8.6. Sei M eine Menge und sei $\sigma : M \to M$ eine Permutation. Definiere auf M die Relation R durch

$$xRy \text{ genau dann, wenn es ein } n \in \mathbb{Z} \text{ gibt mit } y = \sigma^n(x)\,.$$

Zeige, dass R eine Äquivalenzrelation auf M ist. Wie sieht es aus, wenn man nur $n \in \mathbb{N}$ zulässt, und wie, wenn M endlich ist.

Aufgaben zum Abgeben

Aufgabe 8.7. (3 Punkte)

Bestimme die Gruppenhomomorphismen zwischen zwei zyklischen Gruppen. Welche sind injektiv und welche sind surjektiv?

Aufgabe 8.8. (2 Punkte)

Bestimme sämtliche Gruppen mit vier Elementen.

In der folgenden Aufgabe wird das *Zentrum* einer Gruppe verwendet.

Sei G eine Gruppe. Das *Zentrum* $Z = Z(G)$ von G ist die Teilmenge

$$Z = \{g \in G : \; gx = xg \text{ für alle } x \in G\}\,.$$

Aufgabe 8.9. (3 Punkte)

Sei G eine Gruppe. Zeige, dass das Zentrum $Z \subseteq G$ ein Normalteiler in G ist. Man bringe das Zentrum in Zusammenhang mit dem Gruppenhomomorphismus

$$\kappa : G \longrightarrow \mathrm{Aut}\,(G),\ g \longmapsto \kappa_g.$$

Was ist das Bild von diesem Homomorphismus, und was besagen die Homomorphiesätze in dieser Situation?

Aufgabe 8.10. (3 Punkte)

Sei W die Gruppe der eigentlichen Bewegungen an einem Würfel. Man gebe eine möglichst lange Kette von sukzessiven Untergruppen

$$\{\mathrm{id}\} \subset G_1 \subset G_2 \subset \ldots \subset G_n = W$$

an derart, dass zwischen G_i und G_{i+1} keine weitere Untergruppe liegen kann.

Aufgabe 8.11. (2 Punkte)

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 8.12. (2 Punkte)

Sei M eine Menge und sei $M = \biguplus_{i\in I} M_i$ eine Partition von M, d.h. jedes M_i ist eine Teilmenge von M und M ist die disjunkte Vereinigung der M_i. Zeige, dass die Produktgruppe

$$\prod_{i\in I} \mathrm{Perm}(M_i)$$

eine Untergruppe von $\mathrm{Perm}\,(M)$ ist.

9. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 9.1. Was bedeutet das linke Bild auf der Kursseite?

Aufgabe 9.2. Berechne für die Permutation

x	1	2	3	4	5	6	7	8
$\sigma(x)$	2	5	7	3	1	4	8	6

die Anzahl der Fehlstände und das Vorzeichen.

Sei G eine Gruppe. Zwei Elemente $g, h \in G$ heißen *vertauschbar*, wenn $gh = hg$ gilt.

Aufgabe 9.3. Zeige, dass zwei Permutationen mit disjunktem Wirkungsbereich vertauschbar sind.

Aufgabe 9.4. Sei G eine zyklische Gruppe der Ordnung 6. Für welche $n \in \mathbb{N}$ lässt sich G realisieren als Untergruppe der Permutationsgruppe S_n?

Aufgabe 9.5. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Die zugehörige *Permutationsmatrix* M_σ ist dadurch gegeben, dass

$$a_{\sigma(i),i} = 1$$

ist und alle anderen Einträge null sind. Zeige, dass

$$\det(M_\sigma) = \operatorname{sgn}(\sigma)$$

ist.

Aufgaben zum Abgeben

Aufgabe 9.6. (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 9.7. (3 Punkte)

Zeige, dass die (eigentliche) Würfelgruppe isomorph zur Permutationsgruppe S_4 ist.

Aufgabe 9.8. (2 Punkte)

Sei $G = \mathbb{Z}/(n)$ eine zyklische Gruppe der Ordnung n. Bestimme für jedes Element $g \in G$ das Signum der zugehörigen Permutation (der Addition mit g).

(Vergleiche hierzu Beispiel 9.15)

Aufgabe 9.9. (3 Punkte)

Für eine Gruppe G bezeichne $T(G)$ die Menge aller Elemente mit endlicher Ordnung in G. Zeige folgende Aussagen.

(1) Ist G abelsch, so ist $T(G)$ eine Untergruppe von G.
(2) Ist $T(G)$ eine Untergruppe, so ist $T(G)$ ein Normalteiler in G.
(3) Es gibt eine Gruppe G, für die $T(G)$ keine Untergruppe von G ist.

Aufgabe 9.10. (5 Punkte)

Sei σ ein Zykel der Ordnung n. Zeige, dass man σ als Produkt von $n-1$ Transpositionen schreiben kann, aber nicht mit einer kleineren Anzahl von Transpositionen.

Aufgabe 9.11. (3 Punkte)

Sei $m \geq n$. Wie viele injektive Abbildungen gibt es von $\{1, \ldots, n\}$ nach $\{1, \ldots, m\}$ und wie viele surjektiven Abbildungen gibt es von $\{1, \ldots, m\}$ nach $\{1, \ldots, n\}$?

Für die nächste Vorlesung empfehlen wir, sich an die Begriffe *Skalarprodukt* und *euklidischer Vektorraum* zu erinnern, siehe die Kursseite unter "weitere Materialien".

10. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 10.1. Sei A_n eine alternierende Gruppe mit $n \geq 4$. Zeige, dass A_n nicht kommutativ ist.

Aufgabe 10.2. Bestimme die Ordnung der ebenen Drehung um 291 Grad.

Aufgabe 10.3. Führe folgendes Gedankenexperiment durch: Gegeben sei eine Kugeloberfläche aus Metall und n gleiche Teilchen mit der gleichen positiven Ladung. Die Teilchen stoßen sich also ab. Diese Teilchen werden auf die Kugeloberfläche gebracht, wobei sie sich nach wie vor gegenseitig abstoßen, aber auf der Kugel bleiben. Welche Konfiguration nehmen die Teilchen ein? Müsste sich nicht „aus physikalischen Gründen“ eine „gleichverteilte“ Konfiguration ergeben, in der alle Teilchen gleichberechtigt sind? Müsste es nicht zu je zwei Teilchen P, Q eine Kugelbewegung geben, die eine Symmetrie der Konfiguration ist und die P in Q überführt?

Die nächste Aufgabe verwendet die sogenannte *Kleinsche Vierergruppe*. Dies ist einfach die Produktgruppe $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Aufgabe 10.4. Zeige, dass die Kleinsche Vierergruppe zu einer Untergruppe der Permutationsgruppe S_4 isomorph ist. Wie sieht eine Realisierung als Untergruppe der Würfelgruppe aus?

Aufgaben zum Abgeben

Aufgabe 10.5. (2 Punkte)

Zeige, dass jede gerade Permutation ein Produkt aus Dreierzykeln ist.

Aufgabe 10.6. (2 Punkte)

Betrachte die Wirkung der Tetraedergruppe auf den vier Eckpunkten eines Tetraeders. Zeige, dass dies eine Isomorphie zwischen der Tetraedergruppe und der alternierenden Gruppe A_4 ergibt.

Aufgabe 10.7. (2 Punkte)

Wie viele Elemente besitzt die von der Drehung um 51 Grad, von der Drehung um 99 Grad und von der Siebteldrehung erzeugte Untergruppe der Drehgruppe SO_2.

Aufgabe 10.8. (3 Punkte)

Betrachte ein regelmäßiges n-Eck und die zugehörige Gruppe der (eigentlichen und uneigentlichen) Symmetrien, also die Diedergruppe D_n. Beschreibe D_n als Untergruppe der Permutationsgruppe S_n. Durch welche Permutationen wird sie erzeugt? Für welche n handelt es sich um eine Untergruppe der alternierenden Gruppe?

Aufgabe 10.9. (2 Punkte)

Sei $G \subset \mathrm{O}_2$ eine endliche Untergruppe der (eigentlichen und uneigentlichen) Bewegungsgruppe der reellen Ebene, und sei $G \not\subseteq \mathrm{SO}_2$. Zeige, dass es einen surjektiven Gruppenhomomorphismus

$$G \longrightarrow \mathbb{Z}/(2)$$

gibt, dessen Kern eine zyklische Gruppe ist. Schließe, dass die Ordnung von G gerade ist.

Aufgabe 10.10. (3 Punkte)

Sei G eine Gruppe mit Zentrum $Z(G)$. Zeige:

(1) G ist genau dann abelsch, wenn $G/Z(G)$ zyklisch ist.

(2) $Z(G)$ hat niemals eine Primzahl als Index in G.
(3) Ist G von der Ordnung pq für zwei Primzahlen p und q, so ist G abelsch oder $Z(G)$ trivial.

Die folgende Aufgabe verwendet den topologischen Begriff der Dichtheit.

Eine Teilmenge $T \subseteq \mathbb{R}$ heißt *dicht*, wenn es zu jeder reellen Zahl $x \in \mathbb{R}$ und jedem $\epsilon > 0$ Elemente $t \in T$ gibt mit $d(t,x) < \epsilon$.

Aufgabe 10.11. (3 Punkte)

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.

11. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 11.1. Betrachte den Beweis zu Lemma 11.2 mit der dortigen Notation. Begründe die folgenden Aussagen.

(1) Eine eigentliche Isometrie mit zwei Fixachsen ist die Identität.
(2) G ist die Vereinigung aller G_H.
(3) Sei $g \neq \mathrm{id}$. Das Element g kommt in genau zwei der G_H vor. In welchen?
(4) Die Halbachsenklasse K_i enthält n/n_i Elemente.

Aufgabe 11.2. Überprüfe die Formel

$$2(1 - \frac{1}{n}) = \sum_{i=1}^{m} (1 - \frac{1}{n_i})$$

für den Oktaeder, den Dodekaeder und den Ikosaeder.

Aufgabe 11.3. Sei G eine Gruppe, M eine Menge und

$$G \longrightarrow \mathrm{Perm}\,(M),\ g \longmapsto \sigma_g,$$

ein Gruppenhomomorphismus in die Permutationsgruppe von M. Zeige, dass dies in natürlicher Weise einen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}(\mathfrak{P}\,(\mathrm{M}))\ ,\ g \longmapsto (N \mapsto g(N)),$$

in die Permutationsgruppe der Potenzmenge induziert.

Aufgabe 11.4. Bestimme sämtliche Matrizen, die den Symmetrien eines Quadrates mit den Eckpunkten $(\pm 1, \pm 1)$ entsprechen. Sehen diese Matrizen für jedes Quadrat (mit dem Nullpunkt als Mittelpunkt) gleich aus?

Aufgaben zum Abgeben

Aufgabe 11.5. (4 Punkte)

Es seien A_1, A_2, A_3 und A_4vier Geraden im $\mathbb{R}^3$ durch den Nullpunkt mit der Eigenschaft, dass keine drei davon in einer Ebene liegen. Es sei

$$f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

eine lineare Isometrie mit $f(A_i) = A_i$ für $i = 1, 2, 3, 4$. Zeige, dass f die Identität ist. Man gebe ein Beispiel an, dass diese Aussage ohne die Ebenenbedingung nicht gilt.

Aufgabe 11.6. (2 Punkte)

Betrachte ein gleichseitiges Dreieck mit dem Nullpunkt als Mittelpunkt und mit $(1, 0)$ als einem Eckpunkt. Bestimme die (eigentlichen und uneigentlichen) Matrizen, die den Symmetrien an diesem Dreieck entsprechen.

Aufgabe 11.7. (2 Punkte)

Zeige, dass sich jede endliche Gruppe als Untergruppe der $\mathrm{SO}_n(\mathbb{R})$ realisieren lässt.

Aufgabe 11.8. (4 Punkte)

Es seien $\varphi_1, \varphi_2, \varphi_3$ Drehungen um die x-Achse, die y-Achse und die z-Achse mit den Ordungen n_1, n_2, n_3 (φ_1 ist also eine Drehung um den Winkel $360/n_1$ Grad um die x-Achse, etc.). Es sei $1 \leq n_1 \leq n_2 \leq n_3$. Für welche Tupel (n_1, n_2, n_3) ist die von diesen drei Drehungen erzeugte Gruppe endlich?

Aufgabe 11.9. (2 Punkte)

Man gebe ein Beispiel einer Raumdrehung, bei der sämtiche Matrixeinträge $\neq 0, 1$ sind.

Aufgabe 11.10. (3 Punkte)

Es sei G eine Gruppe und seien U, V Untergruppen von G. Zeige folgende Aussagen.

(1) $UV = \{uv \mid u \in U, v \in V\}$ ist genau dann eine Gruppe, wenn $UV = VU$ gilt.
(2) Ist G endlich, so gilt $\#(UV) = \#(U) \cdot \#(V)/\#(U \cap V)$.
(3) Sind U und V echte Untergruppen von G, so gilt $U \cup V \neq G$.

Die nächste Aufgabe verwendet das Konzept einer exakten Sequenz.

Seien $G_0, \ldots, G_n$ Gruppen und $f_i : G_{i-1} \to G_i$ Gruppenhomomorphismen derart, dass kern $f_{i+1} =$ bild f_i für $i = 1, \ldots, n$. Dann heißt

$$G_0 \to G_1 \to \ldots \to G_{n-1} \to G_n$$

eine *exakte Sequenz von Gruppen*.

Aufgabe 11.11. (3 Punkte)

Sei

$$G_0 \to G_1 \to \ldots \to G_{n-1} \to G_n$$

eine exakte Sequenz von Gruppen, wobei alle beteiligten Gruppen endlich seien und $G_0 = G_n$ die triviale Gruppe sei. Zeige, dass dann gilt

$$\prod_{i=0}^{n} \#(G_i)^{(-1)^i} = 1\,.$$

Aufgabe 11.12. (3 Punkte)

Zeige: Keine der alternierenden Gruppen A_n besitzt eine Untergruppe vom Index zwei.

Für die folgende Aufgabe gibt es keinen festen Abgabetermin. Sie gilt so lange, bis eine befriedigende Lösung auf Commons hochgeladen wurde.

Aufgabe 11.13. (10 Punkte)

Schreibe eine Computeranimation, die zeigt, wie sich fünf auf einer Kugeloberfläche platzierte Teilchen mit der gleichen positiven Ladung aufgrund ihrer gegenseitigen Abstoßung bewegen (wobei sie aber auf der Kugeloberfläche bleiben), und welche Endposition (?) sie einnehmen.

12. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 12.1. Zeige, dass ein Ring mit $0 = 1$ der Nullring ist.

Aufgabe 12.2. Zeige, dass es keinen echten Zwischenring zwischen $\mathbb{R}$ und $\mathbb{C}$ gibt.

Aufgabe 12.3. Formuliere und beweise das allgemeine Distributivitätsgesetz für einen Ring.

Aufgabe 12.4. 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.

Aufgabe 12.5. 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.

Aufgaben zum Abgeben

Aufgabe 12.6. (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 12.7. (2 Punkte)

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 12.8. (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.

Die nächste Aufgabe ist online abzugeben. Legen Sie dazu eine Benutzerseite auf Wikiversity an.

Aufgabe 12.9. (3 (=2+1) Punkte)

Es sei R ein Ring und es seien $a, b \in R$ Elemente, die *vertauschbar* sind, d.h. es ist $ab = ba$. Zeigen Sie, dass die Binomische Formel auch unter dieser Voraussetzung gilt, indem Sie die Einzelschritte in der Gleichungskette im Beweis zu Satz 12.7 begründen. Sagen Sie jeweils, auf welchem Ringaxiom die Gleichung beruht und wo die Voraussetzung eingeht.

Gehen Sie dabei folgendermaßen vor.

(1) Legen Sie auf Ihrer Benutzerseite (oder Gruppenseite) eine Unterseite an, indem Sie die Zeile
[[/Binomischer Lehrsatz/Vergleichskette/Einzelbegründungen]]
schreiben (d.h. Bearbeiten, Schreiben, Abspeichern; das / vorne ist wichtig).
(2) Es erscheint ein roter Link. Gehen Sie auf den roten Link und geben Sie dort
:Binomischer Lehrsatz/Vergleichskette/Begründungsfenster
ein.
(3) Es erscheint der Beweis der Binomischen Formel. Wenn Sie auf eines der Gleichheitszeichen gehen, erscheint ein roter Link. Gehen Sie auf diesen roten Link und geben Sie dort die Begründung für dieses Gleichheitszeichen ein.
(4) Die Abgabe erfolgt online, indem Sie auf der Abgabeseite(die Sie von der Kursseite auf Wikiversity aus erreichen können) einen Link zu Ihrer Lösung hinterlassen, also dort
[[Ihr Benutzername/Binomischer Lehrsatz/Vergleichskette/Einzelbegründungen]]
hinschreiben.

Aufgabe 12.10. (2 Punkte)

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

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

eine Ringstruktur.

Die nächste Aufgabe verwendet einige topologische Begriffe. Man kann dabei einen topologischen Raum durch einen metrischen Raum oder eine Teilmenge des $\mathbb{R}^n$ ersetzen.

Aufgabe 12.11. (3 Punkte)

Es sei X ein topologischer Raum und

$$R = C(X, \mathbb{R}) = \{f : X \longrightarrow \mathbb{R} | \, f \text{ stetige Abbildung}\}.$$

Zeige, dass R ein kommutativer Ring ist. Man gebe auch ein Beispiel an, das zeigt, dass R im Allgemeinen nicht nullteilerfrei ist.

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 12.12. (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.

Die folgende Aufgabe richtet sich vor allem an diejenigen, die im Proseminar den Begriff einer *trigonalisierbaren Matrix* kennengelernt haben.

Aufgabe 12.13. (2 Punkte)

Es sei

$$f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

eine eigentliche Isometrie. Es sei vorausgesetzt, dass f trigonalisierbar ist. Zeige, dass dann f sogar diagonalisierbar ist.

Auf welche Matrixgestalt kann man in Dimension zwei und drei eine trigonalisierbare eigentliche Isometrie bringen?

13. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 13.1. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 13.2. Zeige, dass ein Unterring eines Körpers ein Integritätsbereich ist.

Aufgabe 13.3. Es sei R ein Ring, bei dem das multiplikative Monoid eine Gruppe ist. Welche Möglichkeiten gibt es da?

Aufgabe 13.4. Es sei A eine Menge mit zwei Verknüpfungen, die beide für sich ein Monoid bilden. Ferner seien beide Verknüpfungen miteinander distributiv verbunden. Gibt es (interessante) Beispiele für eine solche algebraische Struktur? Kann ein Ring diese doppelte Distributivität besitzen?

Aufgabe 13.5. Zeige, dass die Umkehrabbildung eines Ringisomorphismus wieder ein Ringhomomorphismus ist.

Aufgabe 13.6. 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.

Aufgaben zum Abgeben

Aufgabe 13.7. (2 Punkte)

Studiere den kanonischen Ringhomomorphismus in den Endomorphismenring für $R = \mathbb{Z}$.

Aufgabe 13.8. (2 Punkte)

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

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

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 13.9. (2 Punkte)

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

Aufgabe 13.10. (2 Punkte)

Sei R ein Ring und seien L und M zwei Mengen mit den in Aufgabe 12.10 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 13.11. (4 Punkte)

Es sei K ein Körper und es sei V ein endlichdimensionaler K-Vektorraum. Es sei

$$\varphi : V \longrightarrow V$$

eine nilpotente lineare Abbildung. Zeige, dass $\varphi^n = 0$ ist, wobei n die Dimension von V bezeichnet.

In der folgenden Aufgabe muss man mittels einiger topologischer Eigenschaften der reellen Zahlen argumentieren.

Aufgabe 13.12. (5 Punkte)

Sei X eine Teilmenge von $\mathbb{R}$ und $C(X, \mathbb{R})$ der Ring der stetigen Funktionen von X nach $\mathbb{R}$. Dann ist durch

$$\varphi : C(\mathbb{R}, \mathbb{R}) \longrightarrow C(X, \mathbb{R}),\, f \longmapsto f|_X,$$

ein Ringhomomorphismus gegeben.

(1) Zeige, dass φ genau dann surjektiv ist, wenn X abgeschlossen ist.
(2) Für welche Mengen X ist φ injektiv?

In der letzten Aufgabe geht es nochmal „nur“ um Gruppen. Die darin verwendete Konstruktion spielt bei „elliptischen Kurven“ eine wichtige Rolle.

Aufgabe 13.13. (5 Punkte)

Es sei M eine Menge mit einer Verknüpfung

$$* : M \times M \longrightarrow M,\ (P, Q) \longmapsto P * Q,$$

die für alle Elemente $P, Q, R, S \in M$ folgende Eigenschaften erfüllt.

(1) $P * Q = Q * P$
(2) $(P * Q) * P = Q$
(3) $((P * Q) * R) * S = P((Q * S) * R)$.

Es sei O ein beliebiges aber fest gewähltes Element aus M. (a) Zeige, dass die Verknüpfung

$$P + Q := (P * Q) * O$$

eine kommutative Gruppenstruktur auf M mit O als neutralem Element definiert.

(b) Es sei nun O' ein zweites Element aus M. Zeige, dass die durch O und durch O' definierten Gruppen isomorph sind.

14. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 14.1. Zeige, dass das Bild unter einem Ringhomomorphismus ein Unterring ist.

Aufgabe 14.2. Zeige, dass das Bild eines Ideals unter einem Ringhomomorphismus nicht unbedingt wieder ein Ideal ist.

Aufgabe 14.3. Sei R ein kommutativer Ring mit endlich vielen Elementen. Zeige, dass R genau dann ein Integritätsbereich ist, wenn R ein Körper ist.

Aufgabe 14.4. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

Aufgaben zum Abgeben

Aufgabe 14.5. (3 Punkte)

Zeige direkt, ohne mit Restklassen zu argumentieren, dass eine Primzahl p die Eigenschaft besitzt, dass wenn p ein Produkt teilt, dass sie dann einen der Faktoren teilt.

Aufgabe 14.6. (3 Punkte)

Studiere den kanonischen Ringhomomorphismus in den Endomorphismenring für $R = \mathbb{Z}/(n)$ für $n > 0$.

Aufgabe 14.7. (3 Punkte)

Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 14.8. (3 Punkte)

Berechne 3^{1571} in $\mathbb{Z}/(13)$.

Aufgabe 14.9. (2 Punkte)

Sei R ein kommutativer Ring und sei f_j, $j \in J$, eine Familie von Elementen in R. Es sei angenommen, dass die f_j zusammen das Einheitsideal erzeugen. Zeige, dass es dann bereits eine endliche Teilfamilie f_j, $j \in J_0 \subseteq J$ gibt, die ebenfalls das Einheitsideal erzeugt.

Aufgabe 14.10. (4 Punkte)

Sei R ein kommutativer Ring und sei I ein Ideal mit dem Restklassenring $S = R/I$. Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die I umfassen.

Aufgabe 14.11. (3 Punkte)

Zeige, dass jeder Restklassenring eines Hauptidealringes selbst wieder ein Hauptidealring ist. Man gebe ein Beispiel, dass ein Restklassenring eines Hauptidealbereiches kein Hauptidealbereich sein muss.

In der folgenden Aufgabe darf man wieder den topologischen Raum X durch einen metrischer Raum bzw. eine offene Teilmenge des $\mathbb{R}^n$ ersetzen.

Aufgabe 14.12. (5 Punkte)

Sei X ein topologischer Raum und $R = \operatorname{Cont}(X, \mathbb{R})$ der Ring der stetigen Funktionen auf X. Es sei $T \subseteq X$ eine Teilmenge. Zeige, dass die Teilmenge

$$I = \{f \in R : \ f|_T = 0\}$$

ein Ideal in R ist. Definiere einen Ringhomomorphismus

$$R/I \longrightarrow \operatorname{Cont}(T, \mathbb{R}).$$

Ist dieser immer injektiv? Surjektiv?

15. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 15.1. Zeige, dass es unendlich viele Primzahlen gibt.

Aufgabe 15.2. Berechne die Werte der Eulerschen Funktion $\varphi(n)$ für $n \leq 20$.

Aufgabe 15.3. Finde einen Restklassenring $\mathbb{Z}/(n)$ derart, dass die Einheitengruppe davon nicht zyklisch ist.

Aufgabe 15.4. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(100)$.

Aufgaben zum Abgeben

Aufgabe 15.5. (3 Punkte)

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

Aufgabe 15.6. (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 15.7. (3 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.

Aufgabe 15.8. (2 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 15.9. (2 Punkte)

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 15.10. (3 Punkte)

Sei p eine Primzahl. Zeige, dass

$$\binom{p}{k} \equiv 0 \mod p$$

ist für alle $k = 1, \ldots, p-1$.

Aufgabe 15.11. (2 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.

Aufgabe 15.12. (2 Punkte)

Sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p ist für jede ganze Zahl a.

Aufgabe 15.13. (8 Punkte)

(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

$$\mathrm{Folg}_{\mathrm{Cauchy}}(\mathbb{Q}) \longrightarrow \mathbb{R}$$

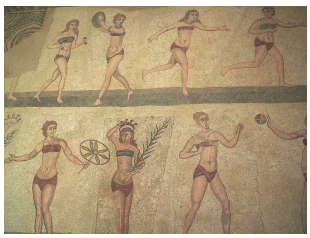
derart, dass eine Ringisomorphie

$$\mathrm{Folg}_{\mathrm{Cauchy}}(\mathbb{Q})/N \longrightarrow \mathbb{R}$$

entsteht.

16. Arbeitsblatt

Aufwärmaufgaben



Aufgabe 16.1. 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 16.2. Berechne das Produkt

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

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

Aufgabe 16.3. Man begründe, dass Satz 16.3 auch unter der schwächeren Bedingung gilt, dass die Elemente aus dem kommutativen Ring R mit dem Element $a \in A$ vertauschbar sind, d.h. dass für alle $r \in R$ gilt $\varphi(r) \cdot a = a \cdot \varphi(r)$.

Aufgabe 16.4. 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 16.5. 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 16.6. Führe in $\mathbb{Z}/(5)[X]$ die Division mit Rest P/T für die beiden Polynome $P = X^3 + 4X^2 + 3X - 1$ und $T = 3X^2 + 2X + 1$ durch.

Aufgaben zum Abgeben

Aufgabe 16.7. (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 16.8. (5 Punkte)

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. Zeige, dass bei $\operatorname{grad}(P) \geq 2$ ein echter Unterring $K[P] \subset K[X]$ vorliegt.

Aufgabe 16.9. (3 Punkte)

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

Aufgabe 16.10. (3 Punkte)

Führe in $\mathbb{C}[X]$ die Division mit Rest P/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 16.11. (2 Punkte)

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 16.12. (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 16.13. (4 Punkte)

Bestimme sämtliche konstante und lineare Einheiten im Polynomring $\mathbb{Z}/(9)[X]$. Begründe, dass es sich um eine Untergruppe der Einheitengruppe handelt. Welche Struktur hat diese Gruppe?

Aufgabe 16.14. (4 Punkte)

Es sei K ein Körper. Betrachte den Matrizenring $\mathrm{Mat}_3(K)$ und darin die Matrix

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

Definiere einen Ringhomomorphismus

$$K[X] \longrightarrow \mathrm{Mat}_3(K),$$

der X auf M schickt. Bestimme den Kern dieser Abbildung.

Aufgabe 16.15. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $A = \mathrm{Abb}\,(K, K)$ der Ring der Abbildungen von K nach K. Definiere einen Ringhomomorphismus

$$K[X] \longrightarrow A.$$

17. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 17.1. 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 17.2. Zeige, dass die Assoziiertheit in einem kommutativen Ring eine Äquivalenzrelation ist.

Aufgabe 17.3. 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 17.4. 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?

Aufgaben zum Abgeben

Aufgabe 17.5. (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 17.6. (2 Punkte)

Zeige, dass in einem Integritätsbereich R zwei Elemente a *und* b genau dann assoziiert sind, wenn für die Hauptideale $Ra = Rb$ gilt.

Aufgabe 17.7. (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 17.8. (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 17.9. (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 17.10. (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 17.11. (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, die sich mit einer Potenz von 3 im Nenner schreiben lassen, enthält.

18. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 18.1. Bestimme in $\mathbb{Z}/(3)[X]$ die Primfaktorzerlegung des Polynoms $P = X^4 + 2X^3 + 2X^2 + 2X + 1$. Man beschreibe ferner die Produktzerlegung des Restklassenrings $\mathbb{Z}/(3)[X]/(P)$.

Aufgabe 18.2. Bestimme im Polynomring $\mathbb{Z}/(2)[X]$ alle irreduziblen Polynome vom Grad $2, 3, 4$.

Aufgabe 18.3. Zeige, dass ein reelles Polynom von ungeradem Grad nicht irreduzibel ist. Hinweis: Der Zwischenwertsatz hilft.

Aufgabe 18.4. 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 18.5. 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.

Aufgaben zum Abgeben

Aufgabe 18.6. (4 Punkte)

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 18.7. (4 Punkte)

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 18.8. (4 Punkte)

Bestimme in $\mathbb{Z}/(5)[X]$ die Primfaktorzerlegung des Polynoms $P = X^6 + 3X^4 - 4$. Man beschreibe ferner die Produktzerlegung des Restklassenrings $\mathbb{Z}/(5)[X]/(P)$.

Aufgabe 18.9. (4 Punkte)

Sei $Q \in \mathbb{R}[X]$ ein quadratisches irreduzibles Polynom. Zeige, dass der Restklassenkörper $\mathbb{R}[X]/(Q)$ isomorph zu $\mathbb{C}$ ist.

Aufgabe 18.10. (4 Punkte)

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

Aufgabe 18.11. (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 18.12. (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.

Aufgabe 18.13. (5 Punkte)

Seien R ein kommutativer Ring und I, J Ideale in R. Sei weiter

$$\varphi : R \longrightarrow R/I \times R/J,\ r \longmapsto (r+I, r+J).$$

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.

19. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 19.1. Finde primitive Elemente in den Restklassenkörpern $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(5)$, $\mathbb{Z}/(7)$ und $\mathbb{Z}/(11)$.

Aufgabe 19.2. Es seien $n_1, \ldots, n_k$ positive natürliche Zahlen und es sei

$$G = \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_k)$$

die Produktgruppe. Bestimme den Exponenten von G.

Aufgabe 19.3. Konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen.

Aufgabe 19.4. Bestimme in $\mathbb{F}_9$ für jedes Element die multiplikative Ordnung. Gib insbesondere die primitiven Elemente an.

Aufgabe 19.5. Es sei $\mathbb{F}_9 = \mathbb{Z}/(3)[Z]/(Z^2+1)$ der Körper mit 9 Elementen (z bezeichne die Restklasse von Z). Führe in $\mathbb{F}_9[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = X^3 + zX^2 + 1 + z$ und $T = zX^2 + (z+2)X + 2$ durch.

Aufgaben zum Abgeben

Aufgabe 19.6. (2 Punkte)

Sei K ein Körper. Zeige, dass die beiden folgenden Eigenschaften äquivalent sind:

(1) K ist algebraisch abgeschlossen.
(2) Jedes nicht-konstante Polynom $F \in K[X]$ zerfällt in Linearfaktoren.

Aufgabe 19.7. (3 Punkte)

Sei K ein algebraisch abgeschlossener Körper. Zeige, dass K nicht endlich sein kann.

Aufgabe 19.8. (3 Punkte)

Finde primitive Elemente in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 19.9. (4 Punkte)

Zeige, dass für natürliche Zahlen k und n mit $k \mid n$ der kanonische Homomorphismus

$$(\mathbb{Z}/(n))^\times \to (\mathbb{Z}/(k))^\times$$

surjektiv ist.

Aufgabe 19.10. (5 Punkte)

Konstruiere zu einer Primzahl p einen Körper mit p^2 Elementen.

Aufgabe 19.11. (4 Punkte)

Es sei p eine Primzahl und F ein Körper mit p^2 Elementen. Welche Ringhomomorphismen zwischen $\mathbb{Z}/(p^2)$ und F gibt es? Man betrachte beide Richtungen.

Aufgabe 19.12. (4 Punkte)

Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32$ und 49 Elementen.

Aufgabe 19.13. (4 Punkte)

Es sei $\mathbb{F}_9 = \mathbb{Z}/(3)[Z]/(Z^2+1)$ der Körper mit 9 Elementen (z bezeichne die Restklasse von Z). Führe in $\mathbb{F}_9[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = X^4 + (1+2z)X^3 + zX^2 + 2X + 2 + z$ und $T = (z+1)X^2 + zX + 2$ durch.

Aufgabe 19.14. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 25 Elementen. Wie viele solche Erzeuger gibt es?

20. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 20.1. Sei R ein kommutativer Ring und I ein Ideal. Dann ist $\{1+x : x \in I\}$ ein multiplikatives System in R.

Aufgabe 20.2. 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 20.3. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal. Genau dann ist $\mathfrak{p}$ ein Primideal, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.

Aufgabe 20.4. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X,Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 20.5. Man mache sich anhand des Einsetzungshomomorphismus

$$\mathbb{R}[X] \longrightarrow \mathbb{C},\ X \longmapsto i,$$

klar, dass die Anzahl der Primideale in $K[X]$ stark vom Grundkörper K abhängt.

Aufgaben zum Abgeben

Aufgabe 20.6. (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

$$f = up_1^{r_1} \cdots p_n^{r_n}$$

mit einer Einheit $u \in R$ und ganzzahligen Exponenten r_i besitzt.

Aufgabe 20.7. (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 20.8. (2 Punkte)

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

Aufgabe 20.9. (4 Punkte)

Sei $\mathfrak{a}$ ein Ideal in einem kommutativen Ring R. Zeige, dass $\mathfrak{a}$ ein Primideal ist genau dann, wenn $\mathfrak{a}$ der Kern eines Ringhomomorphismus $\varphi : R \to K$ in einen Körper K ist.

Die folgende Aufgabe verwendet den Begriff des maximalen Ideals.

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.

Aufgabe 20.10. (3 Punkte)

Seien R ein kommutativer Ring und sei $\mathfrak{a} \neq R$ ein Ideal in R. Zeige: $\mathfrak{a}$ ist ein maximales Ideal genau dann, 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 20.11. (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 20.12. (2 Punkte)

Sei R ein kommutativer Ring. Zeige die Äquivalenz folgender Aussagen.

(1) R hat genau ein maximales Ideal
(2) Die Menge der Nichteinheiten $R \setminus R^\times$ bildet ein Ideal in R.

Aufgabe 20.13. (4 Punkte)

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.

21. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 21.1. 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 21.2. 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 21.3. Berechne im Körper $\mathbb{Q}[\sqrt{7}]$ das Produkt

$$(-2+\sqrt{7}) \cdot (4-\sqrt{7}) .$$

Aufgabe 21.4. Bestimme das Inverse von

$$1+\sqrt{2}+3\sqrt{10}$$

im Körper $\mathbb{Q}[\sqrt{2},\sqrt{5}]$.

Aufgaben zum Abgeben

Aufgabe 21.5. (2 Punkte)

Bestimme in $\mathbb{Q}[\sqrt{11}]$ das Inverse von $3+5\sqrt{11}$.

Aufgabe 21.6. (4 Punkte)

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 21.7. (5 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 21.8. (5 Punkte)

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 21.9. (4 Punkte)

Bestimme das Inverse von

$$2 + 3\sqrt{5} + \sqrt{7} + 3\sqrt{35}$$

im Körper $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$.

Aufgabe 21.10. (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 21.11. (4 Punkte)

Bestimme das Minimalpolynom von

$$\sqrt{3}+\sqrt{5}$$

über $\mathbb{Q}$.

Aufgabe 21.12. (2 Punkte)

Sei K ein endlicher Körper mit $q=p^n$ Elementen. Zeige, dass es in K genau $\varphi(q-1)$ primitive Elemente gibt, wobei φ die Eulersche Funktion bezeichnet.

22. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 22.1. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad 1. Zeige, dass dann $L=K$ ist.

Aufgabe 22.2. Beweise die Lösungsformel für eine quadratische Gleichung

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

mit $a,b,c \in K$ für einen Körper K der Charakteristik $\neq 2$.

Aufgabe 22.3. 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-Homomorphismus $L \to L$ gibt.

Aufgabe 22.4. Zeige, dass die Menge der algebraischen Zahlen $\mathbb{A}$ keine endliche Körpererweiterung von $\mathbb{Q}$ ist.

Aufgabe 22.5. Zeige, dass es nur abzählbar viele algebraische Zahlen gibt.

Aufgaben zum Abgeben

Aufgabe 22.6. (3 Punkte)

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 22.7. (3 Punkte)

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 22.8. (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 22.9. (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 $L \to L$ gibt derart, dass $L \subseteq L$ eine endliche Körpererweiterung vom Grad n ist.

Aufgabe 22.10. (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 22.11. (2 Punkte)

Formuliere und beweise das „verschobene Eisensteinkriterium“. Man gebe auch ein Beispiel eines Polynoms $P \in \mathbb{Q}[X]$, wo man die Irreduzibilität nicht mit dem Eisensteinkriterium, aber mit dem verschobenen Eisensteinkriterium nachweisen kann.

Aufgabe 22.12. (6 Punkte)

Es sei p eine Primzahl. Betrachte das Polynom

$$P = X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1\,.$$

Zeige, dass P irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 22.13. (4 Punkte)

Formuliere und beweise das *umgekehrte Eisensteinkriterium*, bei dem die Rollen des Leitkoeffizienten und des konstanten Koeffizienten vertauscht werden.

Aufgabe 22.14. (3 Punkte)

Wende eine Form des *Eisensteinkriteriums* an, um die Irreduzibilität der folgenden Polynome aus $\mathbb{Q}[X]$ nachzuweisen.

(1) $X^4 + 2X^2 + 2$,
(2) $20X^5 - 15X^4 + 125X^3 - 10X + 4$,
(3) $X^4 + 9$.

23. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 23.1. 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 23.2. 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 23.3. Seien $K \subseteq L \subseteq M$ Körpererweiterungen derart, dass M über K endlich ist. Zeige, dass dann auch M über L und L über K endlich sind.

Aufgabe 23.4. Zeige, dass der Körper der komplexen Zahlen $\mathbb{C}$ der Zerfällungskörper des Polynoms $X^2 + 1 \in \mathbb{R}[X]$ ist.

Aufgabe 23.5. Sei K ein Körper der positiven Charakteristik p. Sei $F : K \to K$ der Frobenius-Homomorphismus. Zeige, dass genau die Elemente aus $\mathbb{Z}/(p)$ invariant unter F sind.

Aufgabe 23.6. Es sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Es sei

$$f : V \longrightarrow V$$

eine lineare Abbildung, also $f \in \operatorname{End}(V)$. Zeige, dass die von f erzeugte K-Algebra $K[f]$ kommutativ ist, und zeige, dass f algebraisch ist, ohne den Satz von Cayley-Hamilton zu verwenden.

Aufgaben zum Abgeben

Aufgabe 23.7. (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 23.8. (4 Punkte)

Konstruiere endliche Körper mit $64, 81, 121, 125$ und 128 Elementen.

Aufgabe 23.9. (4 Punkte)

Sei q eine echte Primzahlpotenz und $\mathbb{F}_q$ der zugehörige endliche Körper. Zeige, dass in $\mathbb{F}_{q^2}$ jedes Element aus $\mathbb{F}_q$ ein Quadrat ist.

Aufgabe 23.10. (4 Punkte)

Sei p eine Primzahl und $e, d \in \mathbb{N}_+$. Zeige: $\mathbb{F}_{p^d}$ ist ein Unterkörper von $\mathbb{F}_{p^e}$ genau dann, wenn e ein Vielfaches von d ist.

Aufgabe 23.11. (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.

Aufgabe 23.12. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 27 Elementen. Wie viele solche Erzeuger gibt es?

Aufgabe 23.13. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Beweise die folgenden Rechenregeln für das formale Ableiten $F \mapsto F'$:

(1) Die Ableitung eines konstanten Polynoms ist null.
(2) Die Ableitung ist K-linear.
(3) Es gilt die *Produktregel*, also

$$(FG)' = FG' + F'G\,.$$

Es sei K ein Körper. Ein Element $a \in K$ heißt *mehrfache Nullstelle* eines Polynoms $P \in K[X]$, wenn in der Primfaktorzerlegung von P das lineare Polynom $X - a$ mit einem Exponenten ≥ 2 vorkommt.

Aufgabe 23.14. (4 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a eine mehrfache Nullstelle von F genau dann ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

24. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 24.1. 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 24.2. Rekapituliere die Strahlensätze.

Aufgabe 24.3. Erläutere geometrisch, warum die 0 das neutrale Element der geometrischen Addition von reellen Zahlen ist.

Aufgabe 24.4. 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.

Aufgaben zum Abgeben

Aufgabe 24.5. (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 24.6. (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 24.7. (12 Punkte)

Schreibe Computeranimationen, die die in Lemma 24.6 beschriebenen Konstruktionen veranschaulichen (über Commons hochladen).

Aufgabe 24.8. (2 Punkte)

Konstruiere mit Hilfe von Zirkel und Lineal eine reelle Zahl x, deren Abweichung von $\sqrt{\pi}$ kleiner als $0,00001$ ist.

Aufgabe 24.9. (2 Punkte)

Erläutere geometrisch, warum die 1 das neutrale Element der geometrischen Multiplikation von reellen Zahlen ist.

Aufgabe 24.10. (2 Punkte)

Erläutere geometrisch, woran die geometrische Division von reellen Zahlen durch 0 scheitert.

Aufgabe 24.11. (3 Punkte)

Bestimme alle Lösungen der Kreisgleichung

$$x^2 + y^2 = 1$$

für die Körper $K = \mathbb{Z}/(2)$, $\mathbb{Z}/(5)$ und $\mathbb{Z}/(11)$.

Aufgabe 24.12. (2 Punkte)

Es seien P und Q zwei konstruierbare Punkte. Zeige, dass dann auch der Abstand $d(P,Q)$ konstruierbar ist.

25. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 25.1. Es sei $K \subseteq \mathbb{R}$ ein Unterkörper. Zeige, dass dann auch $K[i]$ ein Unterkörper von $\mathbb{C}$ ist.

Aufgabe 25.2. 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 25.3. Ist die Zahl, die den „goldenen Schnitt“ beschreibt, eine konstruierbare Zahl?

Aufgabe 25.4. Zeige direkt, ohne Bezug auf Koordinaten, dass die Summe von zwei konstruierbaren komplexen Zahlen wieder konstruierbar ist.

Aufgaben zum Abgeben

Aufgabe 25.5. (2 Punkte)

Sei $Z \in \mathbb{C}$ eine konstruierbare Zahl und r eine konstruierbare positive reelle Zahl. Dann ist auch der Kreis mit Mittelpunkt Z und Radius r konstruierbar.

Aufgabe 25.6. (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

$$\varphi : E = \mathbb{R}^2 \longrightarrow E = \mathbb{R}^2$$

gibt, die 0 auf P, 1 auf Q_1 und i auf Q_2 schickt, und die konstruierbare Punkte in konstruierbare Punkte überführt.

Aufgabe 25.7. (2 Punkte)

Betrachte ein DinA4-Blatt. Ist das Seitenverhältnis aus langer und kurzer Seitenlänge eine konstruierbare Zahl?

Aufgabe 25.8. (2 Punkte)

Betrachte die Tastatur eines Klaviers. Ist das Schwingungsverhältnis von zwei nebeneinander liegendenTasten (bei „gleichstufiger Stimmung“) eine konstruierbare Zahl?

Aufgabe 25.9. (2 Punkte)

Zeige, dass die komplexe Zahl $re^{i\varphi}$ genau dann konstruierbar ist, wenn r und $e^{i\varphi}$ konstruierbar sind.

Aufgabe 25.10. (4 Punkte)

Beweise auf zwei verschiedene Arten, dass die komplexe Quadratwurzel einer konstruierbaren komplexen Zahl wieder konstruierbar ist.

Aufgabe 25.11. (4 Punkte)

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.

26. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 26.1. 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 26.2. Sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 26.3. Sei $K \subseteq L$ eine endliche Körpererweiterung, deren Grad eine Primzahl sei. Zeige, dass dann eine einfache Körpererweiterung vorliegt.

Aufgabe 26.4. Bestimme das sechste Kreisteilungspolynom Φ_6 und beschreibe die Primfaktorzerlegung von $X^6 - 1$.

Aufgaben zum Abgeben

Aufgabe 26.5. (2 Punkte)

Es seien $F, G \in \mathbb{Z}[X]$ normierte Polynome mit der Eigenschaft, dass $F = GH$ ist mit $H \in \mathbb{Q}[X]$. Zeige, dass $H \in \mathbb{Z}[X]$ ist.

Aufgabe 26.6. (5 Punkte)

Bestimme die Kreisteilungspolynome Φ_n für $n \leq 15$.

Aufgabe 26.7. (3 Punkte)

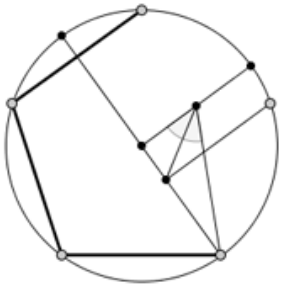
Es sei $n \in \mathbb{N}$ ungerade. Zeige, dass der n-te Kreisteilungskörper mit dem $2n$-ten Kreisteilungskörper übereinstimmt.

Aufgabe 26.8. (4 Punkte)

Bestimme die Koordinaten der fünften Einheitswurzeln in $\mathbb{C}$.

Aufgabe 26.9. (3 Punkte)

Beschreibe die Konstruktion mit Zirkel und Lineal eines regelmäßigen Fünfecks, wie sie in der Animation (siehe Arbeitsblatt auf Wikiversity) dargestellt ist.



27. Arbeitsblatt

Aufwärmaufgaben

Aufgabe 27.1. Es sei ein Kreis K und ein Punkt $P \in K$ gegeben. Konstruiere die Tangente an den Kreis durch P.

Aufgabe 27.2. Zeige, dass es auf dem Einheitskreis unendlich viele konstruierbare Punkte gibt.

Aufgabe 27.3. Bestimme für alle $n \leq 30$, ob das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist oder nicht.

Aufgabe 27.4. Zeige mit Hilfe des verschobenen Eisensteinkriteriums, dass das Polynom $X^3 - 3X - 1$ irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 27.5. Zeige, dass das Polynom $X^3 + 2X^2 - 5$ in $\mathbb{Q}[X]$ irreduzibel ist.

Aufgaben zum Abgeben

Aufgabe 27.6. (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 27.7. (2 Punkte)

Beweise die Formel

$$\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$$

aus den Additionstheoremen für die trigonometrischen Funktionen.

Aufgabe 27.8. (2 Punkte)

Beweise die Formel

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

für u ungerade.

Anhang A. Reflexionsaufgaben

Diese Aufgaben sind Reflexionsaufgaben. Es geht dabei jeweils um einen bestimmten Aspekt, der sich durch die Algebra-Vorlesung zieht. Es kann zu einem gewählten Thema eine Ausarbeitung in Form eines schriftlichen Essays im Umfang von 2 bis 3 Seiten bis zum Ende des Semesters abgegeben werden (Postkasten des Dozenten). Es soll dabei gezeigt werden, dass man durchgängige Prinzipien erkennen bzw. Querverbindung zu anderen Bereichen herstellen konnte. Es können maximal 10 Punkte erreicht werden.

Aufgabe A.1. Wo findet sich *schulrelevanter Stoff* in der Algebra-Vorlesung? Wie unterscheidet sich die wissenschaftliche Darstellung vom Schulunterricht?

Aufgabe A.2. Welche algebraischen Konstruktionen spielen beim *Aufbau des Zahlensystems* eine Rolle?

Aufgabe A.3. Beschreiben Sie Querverbindungen zwischen der Algebra und Ihrem *Neben-* oder *Zweitfach*.

Aufgabe A.4. Welche *Beweisprinzipien* finden sich häufig in der Algebra? Diskutieren Sie typische Beispiele.

Aufgabe A.5. Diskutieren Sie den Begriff *Symmetrie* und wie er algebraisch gefasst werden kann.

Aufgabe A.6. Diskutieren Sie den Begriff der *Äquivalenzrelation*.

Aufgabe A.7. Erläutern Sie die Bedeutung der *Division mit Rest*, und zwar sowohl für die ganzen Zahlen als auch für einen Polynomring über einem Körper.

Aufgabe A.8. Schildern Sie den Übergang von *Primzahlen* hin zu *Primelementen* in einem kommutativen Ring.

Aufgabe A.9. Inwiefern ist die Algebra *geometrisch*?

Aufgabe A.10. Beschreiben Sie das Problem der *Quadratur des Kreises*.

Aufgabe A.11. Vergleichen Sie *Algebra* und *Analysis*.

Anhang B. Probeklausur

Dauer: Zwei volle Stunden + 10 Minuten Orientierung, in denen noch nicht geschrieben werden darf.

Hilfsmittel: Erlaubt ist lediglich ein DinA4-Blatt (zweiseitig) mit beliebigem Inhalt. Taschenrechner oder sonstige Hilfsmittel sind nicht erlaubt.

Alle Antworten sind zu begründen.

Es gibt insgesamt 64 Punkte. Zum Bestehen braucht man 16 Punkte und für eine Eins braucht man 32 Punkte. Es gilt die 1-Punkt-Sockelregelung, d.h. die Bewertung pro Aufgabe beginnt bei einem Punkt. Viel Erfolg!

Aufgabe B.1. (3 Punkte)

Bestimmen Sie den größten gemeinsamen Teiler von 3146 und 1515 und geben Sie eine Darstellung des ggT von 3146 und 1515 an.

Aufgabe B.2. (2 Punkte)

Sei p eine Primzahl. Man gebe einen Körper der Charakteristik p an, der unendlich viele Elemente besitzt.

Aufgabe B.3. (3 Punkte)

Es sei M eine Menge mit n Elementen. Bestimme die Anzahl der Relationen auf M, die

(1) reflexiv
(2) symmetrisch
(3) reflexiv und symmetrisch

sind.

Aufgabe B.4. (3 Punkte)

Sei p eine Primzahl und $x \in (\mathbb{Z}/(p))^\times$ eine Einheit. Es sei a die Ordnung von x in der additiven Gruppe $(\mathbb{Z}/(p), +, 0)$ und es sei b die Ordnung von x in der multiplikativen Gruppe $((\mathbb{Z}/(p))^\times, \cdot, 1)$. Zeige, dass a und b teilerfremd sind.

Aufgabe B.5. (3 Punkte)

Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Aufgabe B.6. (5 Punkte)

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Erläutere die Begriffe „Linksnebenklasse“, „Index“ und „Normalteiler“. Zeige, dass eine Untergruppe vom Index 2 ein Normalteiler ist.

Aufgabe B.7. (3 Punkte)

(a) Bestimme für die Zahlen 3, 4 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(4) \times \mathbb{Z}/(7)$$

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

$$x = 2 \mod 3,\ x = 3 \mod 4 \text{ und } x = 1 \mod 7\,.$$

Aufgabe B.8. (3 Punkte)

Betrachte die beiden Permutationen

x	1	2	3	4	5	6	7	8
$\sigma(x)$	2	5	3	7	1	4	8	6

und

x	1	2	3	4	5	6	7	8
$\tau(x)$	4	5	2	8	6	7	1	3

Berechne $\sigma\tau$ und $\tau\sigma$. Bestimme die Anzahl der Fehlstände und das Vorzeichen von τ. Gebe die Zyklendarstellung von σ und von σ^3 an. Was ist die Ordnung von σ?

Aufgabe B.9. (5 Punkte)

Formuliere und beweise den Satz von Cayley für endliche Gruppen.

Aufgabe B.10. (5 Punkte)

Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$. Definiere die Begriffe „Halbachse von G“ und erläutere, wann zwei Halbachsen „äquivalent“ sind. Zu einer Halbachse H sei

$$G_H = \{g \in G : \, g(H) = H\} \, .$$

Zeige, dass zu zwei äquivalenten Halbachsen H_1 und H_2 die Gruppen G_{H_1} und G_{H_2} isomorph sind.

Aufgabe B.11. (4 Punkte)

Es sei K ein Körper, R ein Ring mit $0 \neq 1$ und

$$\varphi : K \longrightarrow R$$

ein Ringhomomorphismus. Zeige direkt (ohne Bezug auf Sätze der Vorlesung), dass φ injektiv ist.

Aufgabe B.12. (3 Punkte)

Beweise mit Hilfe der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$, dass $9^{1/3}$ irrational ist.

Aufgabe B.13. (3 Punkte)

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.

Aufgabe B.14. (3 Punkte)

Bestimme in $\mathbb{Q}[X]/(X^3 - 7)$ das Inverse von $3x + 4$ (x bezeichnet die Restklasse von X).

Die folgende Aufgabe verwendet den Begriff der algebraischen Körpererweiterung.

Eine Körpererweiterung $K \subseteq L$ heißt *algebraisch*, wenn jedes Element $f \in L$ algebraisch über K ist.

Aufgabe B.15. (5 Punkte)

Es seien $K \subseteq L$ und $L \subseteq M$ algebraische Körpererweiterungen. Zeige, dass dann auch $K \subseteq M$ eine algebraische Körpererweiterung ist.

Aufgabe B.16. (4 Punkte)

Es sei $z = a + bi \in \mathbb{C}$ 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

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}\,.$$

($\mathbb{A}$ bezeichnet dabei den Körper der algebraischen Zahlen.)

Aufgabe B.17. (4 Punkte)

Es sei eine Gerade G gegeben, auf der zwei Punkte als 0 und 1 ausgezeichnet seien, so dass man diese Gerade mit den reellen Zahlen $\mathbb{R}$ identifizieren kann. Es seien zwei Zahlen a und b auf G gegeben. Beschreibe, wie man die beiden Zahlen durch eine geometrische Konstruktion mit Zirkel und Lineal miteinander multiplizieren kann, so dass das Produkt wieder auf G liegt (dabei darf die Konstruktion von Parallelen und Senkrechten verwendet werden). Skizziere die Situation.

Aufgabe B.18. (3 Punkte)

Beschreibe die wesentlichen mathematischen Schritte, mit denen man beweisen kann, dass die „Quadratur des Kreises“ nicht möglich ist.

Anhang C. Probeklausur mit Lösungen

Aufgabe C.1. Bestimmen Sie den größten gemeinsamen Teiler von 3146 und 1515 und geben Sie eine Darstellung des ggT von 3146 und 1515 an.

Lösung:

Der euklidische Algorithmus liefert:

$$3146 = 2 \cdot 1515 + 116$$

$$1515 = 13 \cdot 116 + 7$$

$$116 = 16 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1\,.$$

Die Zahlen 3146 und 1515 sind also teilerfremd und 1 ist ihr größter gemeinsamer Teiler. Eine Darstellung der 1 erhält man, indem man diese Division mit Rest rückwärts liest, also

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - (7 - 1 \cdot 4) \\ &= 2 \cdot 4 - 7 \\ &= 2(116 - 16 \cdot 7) - 7 \\ &= 2 \cdot 116 - 33 \cdot 7 \\ &= 2 \cdot 116 - 33(1515 - 13 \cdot 116) \\ &= -33 \cdot 1515 + (2 + 13 \cdot 33) \cdot 116 \\ &= -33 \cdot 1515 + 431 \cdot 116. \end{aligned}$$

Aufgabe C.2. Sei p eine Primzahl. Man gebe einen Körper der Charakteristik p an, der unendlich viele Elemente besitzt.

Lösung:

Wir starten mit $K = \mathbb{Z}/(p)$, das ist ein Körper der Charakteristik p. Dazu betrachten wir den Quotientenkörper $K(X) = Q(K[X])$ des Polynomrings $K[X]$. Der Polynomring und sein Quotientenkörper enthalten K, so dass $K(X)$ ebenfalls die Charakteristik p besitzt. Ferner enthält $K(X)$ die unendlich vielen Potenzen X^n, $n \in \mathbb{N}$, die alle untereinander verschieden sind.

Aufgabe C.3. Es sei M eine Menge mit n Elementen. Bestimme die Anzahl der Relationen auf M, die

(1) reflexiv
(2) symmetrisch
(3) reflexiv und symmetrisch

sind.

Lösung:

Sei $M = \{1, \ldots, n\}$. Eine Relation R ist gegeben durch eine bestimmte Menge von geordneten Paaren (x, y), $x, y \in M$. Daher kann man sich eine Relation auf M so vorstellen, dass in einer $n \times n$-Tabelle gewisse Stellen angekreuzt werden und andere nicht.

Bei einer beliebigen Relation gibt es keine weiteren Bedingungen, so dass es 2^{n^2} Relationen gibt (das war nicht gefragt).

Bei einer reflexiven Relation muss auf der Diagonalen immer ein Kreuz sein, ansonsten hat man keine Bedingung, es gibt also $n^2 - n = n(n-1)$ freie Stellen und daher $2^{n(n-1)}$ reflexive Relationen.

Bei einer symmetrischen Relation hat man oberhalb der Diagonalen (einschließlich dieser) volle Freiheiten (unterhalb der Diagonalen muss sich der Eintrag wiederholen). Da gibt es $\frac{n^2-n}{2} + n = \frac{n^2+n}{2}$ Plätze und somit gibt es $2^{\frac{n^2+n}{2}}$ symmetrische Relationen.

Bei einer symmetrischen und reflexiven Relation hat man echt oberhalb der Diagonalen volle Wahlfreiheiten. Davon gibt es $\frac{n^2-n}{2}$ Plätze, so dass es $2^{\frac{n^2-n}{2}}$ symmetrische und reflexive Relationen gibt.

Aufgabe C.4. Sei p eine Primzahl und $x \in (\mathbb{Z}/(p))^\times$ eine Einheit. Es sei a die Ordnung von x in der additiven Gruppe $(\mathbb{Z}/(p), +, 0)$ und es sei b die Ordnung von x in der multiplikativen Gruppe $((\mathbb{Z}/(p))^\times, \cdot, 1)$. Zeige, dass a und b teilerfremd sind.

Lösung:

Da x eine Einheit ist, gibt es eine natürliche Zahl n mit $nx = 1 \mod p$. Damit durchlaufen die Vielfachen von x die ganze Gruppe $\mathbb{Z}/(p)$, d.h. x ist ein (additiver) Erzeuger dieser Gruppe. Damit ist die additive Ordung von x genau p. Da die Einheitengruppe $p-1$ Elemente besitzt, ist die multiplikative Ordnung von x kleiner als p. Damit sind die beiden Ordnungen teilerfremd.

Aufgabe C.5. Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Lösung:

Die multiplikative Ordnung ist ein Teiler von 12. Wir bestimmen zuerst die Ordnung von 2. Es ist

$$2^2 = 4 \neq 1,\ 2^3 = 8 \neq 1,\ 2^4 = 16 = 3 \neq 1,\ 2^6 = 64 = -1\,.$$

Daher muss die Ordnung 12 sein und 2 ist eine primitive Einheit. Daher gibt es einen Gruppenisomorphismus

$$(\mathbb{Z}/(12), +, 0) \longrightarrow \mathbb{Z}/(13)^\times,\ n \longmapsto 2^n,$$

der Erzeuger auf Erzeuger abbildet. Die Erzeuger links sind $1, 5, 7, 11$ (die zu 12 teilerfremden Zahlen), und diese werden auf die primitiven Einheiten

$$2^1 = 2,\ 2^5 = 32 = 6,\ 2^7 = 6 \cdot 4 = 11,\ 2^{11} = 2^{-1}2^{12} = 2^{-1} = 7$$

abgebildet.

Aufgabe C.6. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Erläutere die Begriffe „Linksnebenklasse“, „Index“ und „Normalteiler“. Zeige, dass eine Untergruppe vom Index 2 ein Normalteiler ist.

Lösung:

Zu einer Untergruppe $H \subseteq G$ heißt eine Teilmenge der Form $gH = \{gh |\, h \in H\}$ mit $g \in G$ eine Linksnebenklasse. Die Anzahl der Linksnebenklassen heißt der Index von H in G. Eine Untegruppe heißt Normalteiler, wenn $gH = Hg$ ist für jedes $g \in G$.

Sei nun H eine Untergruppe von G vom Index zwei. D.h. es gibt zwei Linksnebenklassen, nämlich $H = e_G H$ und eine weitere Klasse $K = fH$ mit $f \notin H$. Für zwei Elemente $u, v \notin H$ ist $uH = fH$ und $uv \in H$, da andernfalls $uvH = uH$ und somit durch Kürzen doch $v \in H$ gelten würde.

Sei nun $g \in G$ beliebig. Bei $g \in H$ ist natürlich $gH = H = Hg$, sei also $g \notin H$. Dann ist $gH = fH = G \setminus H$, da es sonst keine weitere Linksnebenklassen gibt. Wegen $Hg \subseteq G \setminus H$ ist $Hg \subseteq gH$. Umgekehrt sei gh mit $h \in H$ gegeben. Dann ist $(gh)(g^{-1}h) = h' \in H$ nach der Vorüberlegung und daraus folgt $gh = h'h^{-1}g$, also auch $gH \subseteq Hg$.

Aufgabe C.7. (a) Bestimme für die Zahlen 3, 4 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(4) \times \mathbb{Z}/(7)$$

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

$$x = 2 \mod 3, x = 3 \mod 4 \text{ und } x = 1 \mod 7$$

Lösung:

Für die Basislösung zu $(1,0,0)$ müssen wir die Vielfachen von 28 betrachten. Da $28 = 1 \mod 3$ ist, ist 28 die erste Basislösung. Ebenso repräsentiert wegen $21 = 1 \mod 4$ die 21 das Restetupel $(0,1,0)$. Die Vielfachen von 12 haben modulo 7 die Reste

$$12 = 5 \mod 7, 24 = 3 \mod 7 \text{ und } 36 = 1 \mod 7$$

also repräsentiert 36 das Restetupel $(0,0,1)$.

Das Tupel $(2,3,1)$ wird daher von (beachte $3 \cdot 4 \cdot 7 = 84$)

$$2 \cdot 28 + 3 \cdot 21 + 36 \;=\; 56 + 63 + 36 \;=\; 155 \;=\; 71$$

repräsentiert.

Aufgabe C.8. Betrachte die beiden Permutationen

x	1	1	3	4	5	6	7	8
$\sigma(x)$	2	5	3	7	1	4	8	6

und

x	1	1	3	4	5	6	7	8
$\tau(x)$	4	5	2	8	6	7	1	3

Berechne $\sigma\tau$ und $\tau\sigma$. Bestimme die Anzahl der Fehlstände und das Vorzeichen von τ. Gebe die Zyklendarstellung von σ und von σ^3 an. Was ist die Ordnung von σ?

Lösung:

Die Produkte der beiden Permutationen sind als Wertetabellen geschrieben

x	1	1	3	4	5	6	7	8
$\tau\sigma(x)$	5	6	2	1	4	8	3	7

und

x	1	1	3	4	5	6	7	8
$\sigma\tau(x)$	7	1	5	6	4	8	2	3

Die Fehlstände von τ sind

$$(1,3),\ (1,7),\ (1,8),\ (2,3),\ (2,7),\ (2,8),\ (3,7),\ (4,5),\ (4,6),\ (4,7),\ (4,8),\ (5,7),\ (5,8),\ (6,7),\ (6,8).$$

Das sind also 15 Fehlstände und damit ist das Vorzeichen -1.

Die Zyklendarstellung von σ ist (wir führen auch die Fixpunkte aus)

$$\langle 1,\, 2,\, 5\rangle\langle 3\rangle\langle 4,\, 7,\, 8,\, 6\rangle\,.$$

Daher hat σ^3 die Zyklendarstellung

$$\langle 1\rangle\langle 2\rangle\langle 5\rangle\langle 3\rangle\langle 4,\, 6,\, 8,\, 7\rangle\,.$$

Die Ordnung von σ ist 12, da ein Dreierzyklus und ein Viererzyklus beteiligt sind.

Aufgabe C.9. Formuliere und beweise den Satz von Cayley für endliche Gruppen.

Lösung:

Der Satz von Cayley für endliche Gruppen besagt, dass sich jede endliche Gruppe als Untergruppe einer endlichen Permutationsgruppe auffassen lässt. Zum Beweis geht man wie folgt vor. Zur Gruppe G bezeichnet $\mathrm{Perm}\,(G)$ die Gruppe der Permutationen auf der Menge G. Man betrachtet die Abbildung

$$L : G \longrightarrow \mathrm{Perm}\,(G),\; g \longmapsto L_g : (h \mapsto gh),$$

d.h. dem Gruppenelement g wird die Multiplikation mit g zugeordnet. Dabei ist diese Multiplikation wirklich eine Bijektion auf G (mit der Multiplikation mit g^{-1} als inverser Abbildung). Wir zeigen, dass die Zuordnung $g \mapsto L_g$ ein injektiver Gruppenhomomorphismus ist. Offenbar ist L_{e_G} die Identität, also das neutrale Element der Permutationsgruppe. Seien $g, g' \in G$ und $h \in G$. Dann ist

$$L_{gg'}(h) \,=\, (gg')h \,=\, g(g'h) \,=\, L_g(g'h) \,=\, L_g(L_{g'}(h)) \,=\, (L_g \circ L_{g'})(h),$$

so dass ein Gruppenhomomorphismus vorliegt. Aus $L_g = \mathrm{id}$ folgt sofort $g = L_g(e_G) = e_G$, so dass die Abbildung auch injektiv ist. Daher ist G isomorph zur Bildgruppe, die eine Untergruppe der endlichen Permutationsgruppe ist.

Aufgabe C.10. Es sei $G \subset \mathrm{SO}_3$ eine endliche Untergruppe der Gruppe der eigentlichen linearen Isometrien des $\mathbb{R}^3$. Definiere die Begriffe „Halbachse von G“ und erläutere, wann zwei Halbachsen „äquivalent“ sind. Zu einer Halbachse H sei

$$G_H = \{g \in G |\, g(H) = H\}\,.$$

Zeige, dass zu zwei äquivalenten Halbachsen H_1 und H_2 die Gruppen G_{H_1} und G_{H_2} isomorph sind.

Lösung:

Eine Halbachse zu G ist eine Halbgerade, die durch die Drehachse eines Elementes $g \in G$, $g \neq \mathrm{id}$, gegeben ist. Zwei Halbachsen H und H' heißen

äquivalent, wenn es ein $f \in G$ gibt mit $f(H) = H'$. Seien zwei äquivalente Halbachsen H, H' gegeben und seien $G_H = \{g \in G | \, g(H) = H\}$ und $G_{H'} = \{g \in G | \, g(H') = H'\}$ die zugehörigen Isotropiegruppen. Dann definiert $f \in G$ mit $f(H) = H'$ durch

$$G_H \longrightarrow G_{H'},\, g \longmapsto fgf^{-1},$$

einen Isomorphismus der beiden Gruppen. Als ein innerer Automorphismus ist diese Zuordnung ein Isomorphismus auf G, man muss also nur noch zeigen, dass G_H nach $G_{H'}$ abgebildet wird. Für $g \in G_H$ ist aber

$$(fgf^{-1})(H') \,=\, (fg)f^{-1}(H') \,=\, (fg)(H) \,=\, f(g(H)) \,=\, f(H) \,=\, H',$$

so dass $fgf^{-1} \in G_{H'}$ ist.

Aufgabe C.11. Es sei K ein Körper, R ein Ring mit $0 \neq 1$ und

$$\varphi : K \longrightarrow R$$

ein Ringhomomorphismus. Zeige direkt, dass φ injektiv ist.

Lösung:

Es seien $a, b \in K$ vorgegeben, und sei angenommen, dass $\varphi(a) = \varphi(b)$ ist. Dann ist

$$\varphi(a - b) \,=\, \varphi(a) - \varphi(b) \,=\, 0.$$

Wenn $a - b \neq 0$ wäre, so wäre dies eine Einheit, d.h. es gäbe ein $x \in K$ mit $x(a - b) = 1$. Dann wäre

$$\varphi(x)0 \,=\, \varphi(x)\varphi(a - b) \,=\, \varphi(x(a - b)) \,=\, \varphi(1) \,=\, 1.$$

Aus $\varphi(x)0 = \varphi(x)(0 + 0) = \varphi(x)0 + \varphi(x)0$ folgt daraus $\varphi(x)0 = 0$, also $0 = 1$ im Widerspruch zur Voraussetzung an R. Also ist $a - b = 0$ und $a = b$.

Aufgabe C.12. Beweise mit Hilfe der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$, dass $9^{1/3}$ irrational ist.

Lösung:

Nehmen wir an, dass es eine Darstellung

$$9^{1/3} = \frac{a}{b}$$

mit positiven natürlichen Zahlen a, b gibt. Wenn a und b einen gemeinsamen Teiler ≥ 2 hat, so können wir mit diesem kürzen und erhalten dann eine Bruchdarstellung mit teilerfremden Zähler und Nenner. Seien also a und b teilerfremd. Wir nehmen die dritte Potenz der Anfangsgleichung und erhalten

$$9 = \frac{a^3}{b^3}$$

bzw.

$$3^2 b^3 = a^3 \,.$$

Diese Zahl hat eine eindeutige Primfaktorzerlegung. In ihr kommt 3 vor, so dass $3|a^3$ und daher $3|a$ ist, da 3 eine Primzahl ist. Also kommt rechterseits 3 mit einem Exponenten ≥ 3 in der Primfaktorzerlegung vor, linkerseits aber nur mit dem Exponenten 2, da b kein Vielfaches von 3 ist. Dies ist ein Widerspruch.

Aufgabe C.13. 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.

Lösung:

Zunächst ist 1 eine Nullstelle und daher ist $X - 1$ ein Linearfaktor. Division mit Rest ergibt

$$(X^3 - 1) = (X - 1)(X^2 + X + 1) \,.$$

Wir müssen also noch die komplexen Nullstellen von $X^2 + X + 1$ bestimmen. Dazu ist

$$X^2 + X + 1 \;=\; (X + \frac{1}{2})^2 - \frac{1}{4} + 1 \;=\; (X + \frac{1}{2})^2 + \frac{3}{4}.$$

Damit ist

$$X + \frac{1}{2} = \pm i\sqrt{\frac{3}{4}}$$

und somit sind die weiteren Nullstellen

$$x_2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \text{ und } x_3 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \,.$$

Aufgabe C.14. Bestimme in $\mathbb{Q}[X]/(X^3 - 7)$ das Inverse von $3x + 4$ (x bezeichnet die Restklasse von X).

Lösung:

Wir machen Division mit Rest von $X^3 - 7$ durch $3X + 4$. Das ergibt

$$X^3 - 7 = (3X + 4)(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{16}{27}) - \frac{253}{27} \,.$$

Also ist

$$(3x + 4)(\frac{1}{3}x^2 - \frac{4}{9}x + \frac{16}{27}) = \frac{253}{27} \mod X^3 - 7$$

und daher ist das Inverse von $3x + 4$ gegeben durch

$$\frac{27}{253}(\frac{1}{3}x^2 - \frac{4}{9}x + \frac{16}{27}) = \frac{9}{253}x^2 - \frac{12}{253}x + \frac{16}{253} \,.$$

Die folgende Aufgabe verwendet den Begriff der algebraischen Körpererweiterung.

Eine Körpererweiterung $K \subseteq L$ heißt *algebraisch*, wenn jedes Element $f \in L$ algebraisch über K ist.

Aufgabe C.15. Es seien $K \subseteq L$ und $L \subseteq M$ algebraische Körpererweiterungen. Zeige, dass dann auch $K \subseteq M$ eine algebraische Körpererweiterung ist.

Lösung:

Es ist zu zeigen, dass jedes Element $f \in M$ algebraisch über K ist. Nach Voraussetzung ist f algebraisch über L, d.h. es gibt ein normiertes Polynom $P \in L[X]$ mit $P(f) = 0$. Es seien $a_0, \ldots, a_n \in L$ die Koeffizienten von P. Da L über K algebraisch ist, sind all diese Koeffizienten algebraisch über K. Wir betrachten die Kette von K-Algebren

$$K \subseteq K[a_0] \subseteq K[a_0, a_1] \subseteq K[a_0, a_1, a_2] \subseteq \ldots \subseteq K[a_0, \ldots, a_n] =: K' .$$

Dabei ist jeweils a_i über $K[a_0, \ldots, a_{i-1}]$ algebraisch und daher handelt es sich jeweils um endliche Körpererweiterungen. Nach der Gradformel ist dann auch $K \subseteq K'$ endlich. Weiterhin ist $P \in K'[X]$, da ja nach Konstruktion die Koeffizienten von P zu K' gehören. Also ist f algebraisch über K' und damit zeigt wieder die Kette $K \subseteq K' \subseteq K'[f]$, dass $K'[f]$ und erst recht $K[f]$ endlich über K ist. Also ist f algebraisch über K.

Aufgabe C.16. 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

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A} .$$

Lösung:

Sei $P \in \mathbb{Q}[X]$, $P \neq 0$, mit $P(z) = 0$. Die komplexe Konjugation ist ein $\mathbb{R}$-Algebra-Homomorphismus, daher ist

$$P(\overline{z}) = \overline{P}(\overline{z}) = \overline{P(z)} = \overline{0} = 0.$$

Der Realteil von z lässt sich als $a = \frac{z+\overline{z}}{2}$ erhalten und der Imaginärteil als $b = \frac{z-\overline{z}}{2i}$. Da die Summe, die Differenz und das Produkt von algebraischen Zahlen wieder algebraisch ist, und da i algebraisch ist (als Nullstelle von X^2+1), folgt, dass Real- und Imaginärteil auch algebraisch sind. D.h. zu jeder algebraischen Zahl $z = a + bi$ sind die reellen Koordinaten auch algebraisch.

Wir setzen $T = \mathbb{A} \cap \mathbb{R}$ und behaupten, dass $\mathbb{A} = T + Ti$ ist und der Grad daher zwei ist (da $i \notin \mathbb{R}$ ist). Die Inklusion „ $\subseteq$ “ haben wir soeben gezeigt. Die andere Inklusion folgt daraus, dass i algebraisch ist.

Aufgabe C.17. Es sei eine Gerade G gegeben, auf der zwei Punkte als 0 und 1 ausgezeichnet seien, so dass man diese Gerade mit den reellen Zahlen $\mathbb{R}$ identifizieren kann. Es seien zwei Zahlen a und b auf G gegeben. Beschreibe, wie man die beiden Zahlen durch eine geometrische Konstruktion mit Zirkel und Lineal miteinander multiplizieren kann, so dass das Produkt wieder auf G liegt (dabei darf die Konstruktion von Parallelen und Senkrechten verwendet werden). Skizziere die Situation.

Lösung:

Man zeichnet eine senkrechte Gerade H zu G durch den Nullpunkt. Mit dem Zirkel schlägt man Kreise mit dem Nullpunkt als Mittelpunkt durch 1, a und b und markiert 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. Jetzt zeichnet man die Gerade P durch a und $1'$ und dazu die parallele Gerade P' durch b'. Diese Gerade schneidet G in genau einem Punkt x. Für diesen Punkt gilt nach dem Strahlensatz das Streckenverhältnis

$$x : a \;=\; b' : 1' \;=\; b : 1.$$

Also ist $x = ab$.

Aufgabe C.18. Beschreibe die wesentlichen mathematischen Schritte, mit denen man beweisen kann, dass die „Quadratur des Kreises“ nicht möglich ist.

Lösung:

Das Problem der Quadratur des Kreises bedeutet die Fragestellung, ob man aus einem durch den Radius gegebenen Kreis ein flächengleiches Quadrat mit Hilfe von Zirkel und Lineal konstruieren kann. Den Radius kann man dabei zu 1 normieren und durch zwei Punkte 0 und 1 repräsentieren. Da der Kreisinhalt π ist, muss die Seitenlänge des zu konstruierenden Quadrates $\sqrt{\pi}$ sein. Damit ist die Frage äquivalent dazu, ob man aus zwei Punkten mit Abstand 1 mittels Zirkel und Lineal den Abstand $\sqrt{\pi}$ konstruieren kann.

Der entscheidende Schritt ist, die Menge aller aus 0 und 1 konstruierbaren Punkte in der Ebene mathematisch zu erfassen. Dabei ergibt sich, dass bei jedem elementaren Schritt (wie dem Durchschnitt von einem Kreis und einer Geraden) der neue Punkt in einer quadratischen Körpererweiterung der schon konstruierten Punkte liegt. Daraus ergibt sich induktiv, dass jeder konstruierbare Punkt eine algebraische Zahl ist. Der Satz von Lindemann besagt allerdings, dass π und damit auch $\sqrt{\pi}$ keine algebraische Zahl ist, und damit auch nicht konstruierbar.

Anhang D. Klausur

Dauer: Zwei volle Stunden + 10 Minuten Orientierung, in denen noch nicht geschrieben werden darf.

Hilfsmittel: Erlaubt ist lediglich ein DinA4-Blatt (zweiseitig) mit beliebigem Inhalt. Taschenrechner oder sonstige Hilfsmittel sind nicht erlaubt.

Alle Antworten sind zu begründen.

Es gibt insgesamt 64 Punkte. Zum Bestehen braucht man 16 Punkte und für eine Eins braucht man 32 Punkte. Es gilt die 1-Punkt-Sockelregelung, d.h. die Bewertung pro Aufgabe beginnt bei einem Punkt. Viel Erfolg!

Aufgabe D.1. (4 Punkte)

Beweise mittels der Division mit Rest, dass jede Untergruppe H von $\mathbb{Z}$ die Gestalt $H = \mathbb{Z}d$ mit einem $d \in \mathbb{N}$ besitzt.

Aufgabe D.2. (4 Punkte)

Es seien $n, m \in \mathbb{Z}$ ganze Zahlen. Zeige, dass n genau dann ein Teiler von m ist, wenn es einen Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

gibt. Zeige durch ein Beispiel, dass es einen injektiven Gruppenhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

geben kann, ohne dass n ein Teiler von m ist.

Aufgabe D.3. (3 Punkte)

(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 D.4. (3 Punkte)

Wie viele Elemente besitzt die von der Drehung um 45 Grad, von der Drehung um 99 Grad und von der Zwölfteldrehung erzeugte Untergruppe der Drehgruppe SO_2?

Aufgabe D.5. (3 Punkte)

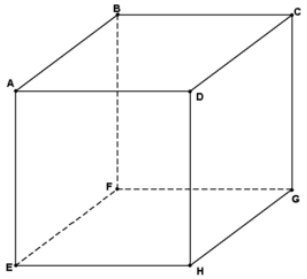
Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

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

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe D.6. (6 Punkte)

Betrachte den Würfel



Es sei α diejenige Drehung am Würfel um die Achse durch die Eckpunkte A und G, die den Eckpunkt B auf D schickt, und es sei β die Halbdrehung um die vertikale Achse (also die Gerade, die durch den Mittelpunkt der Seitenfläche A, B, C, D und den Mittelpunkt der Seitenfläche E, F, G, H läuft).

a) Man gebe eine Wertetabelle für die Permutationen auf der Eckpunktmenge $\{A, B, C, D, E, F, G, H\}$, die durch $\alpha, \beta, \alpha\beta$ und $\beta\alpha$ bewirkt werden.

b) Bestimme die Drehachse von $\alpha\beta$ und von $\beta\alpha$ sowie die Ordnung dieser Drehungen.

c) Man gebe die Zykeldarstellung der von α^2 bewirkten Permutation auf der Eckpunktmenge an. Was ist α^{1001}?

d) Man betrachte die Permutation σ, die auf der Eckpunktmenge durch die Wertetabelle

x	A	A	C	D	E	F	G	H
$\sigma(x)$	B	C	D	A	G	H	E	F

gegeben ist. Gibt es eine Drehung des Würfels, die diese Permutation bewirkt? Berechne das Signum von σ.

Die nächste Aufgabe verwendet die folgende Definition.

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 Schreibweise $a > b$ bedeutet $a \geq b$ und $a \neq b$. Die Schreibweise $a \leq b$ bedeutet $b \geq a$.

Aufgabe D.7. (10 Punkte)

Es sei R ein angeordneter Integritätsbereich.

a) Zeige, dass aus $ca \geq cb$ mit $c > 0$ folgt, dass $a \geq b$ ist.

b) Zeige, dass $1 > 0$ in R gilt.

c) Zeige, dass aus $a < 0$ die Eigenschaft $-a > 0$ folgt.

d) Es sei $K = Q(R)$ der Quotientenkörper von R. Definiere eine Ordnungsrelation $\geq$ auf K, die auf $R \subseteq K$ mit der vorgegebenen Ordnung übereinstimmt, und die K zu einem angeordneten Körper macht.

(Tipp: es empfiehlt sich, die Nenner positiv anzusetzen).

Aufgabe D.8. (5 Punkte)

Bestimme die Primfaktorzerlegung des Polynoms $X^6 - 1$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Aufgabe D.9. (3 Punkte)

Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2 + U + 1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u + 1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Aufgabe D.10. (6 Punkte)

Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Aufgabe D.11. (4 Punkte)

Beschreibe den Körper mit neun Elementen $\mathbb{F}_9$ als einen Restklassenkörper von $\mathbb{Z}/(3)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_9$ an.

Aufgabe D.12. (3 Punkte)

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 D.13. (5 Punkte)

Formuliere und beweise die „Gradformel“ für eine Kette von endlichen Körpererweiterungen $K \subseteq L \subseteq M$.

Aufgabe D.14. (3 Punkte)

Es seien zwei verschiedene Punkte M, P in der Ebene gegeben. Es bezeichne K den Kreis mit Mittelpunkt M durch den Punkt P. Konstruiere (ohne andere Konstruktionen zu verwenden) die Tangente an den Kreis K durch P. Skizziere die Situation.

Aufgabe D.15. (2 Punkte)

Charakterisiere mit Hilfe von Fermatschen Primzahlen (ohne Beweis) diejenigen natürlichen Zahlen n, für die das reguläre n-Eck konstruierbar ist. Wende diese Charakterisierung für n zwischen 30 und 40 an.

Anhang E. Klausur mit Lösungen

Aufgabe E.1. Beweise mittels der Division mit Rest, dass jede Untergruppe H von $\mathbb{Z}$ die Gestalt $H = \mathbb{Z}d$ mit einem $d \in \mathbb{N}$ besitzt.

Lösung:

Sei $H \subseteq \mathbb{Z}$ 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 3.1 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 $H \subseteq \mathbb{Z}d$.

Aufgabe E.2. Es seien $n, m \in \mathbb{Z}$ ganze Zahlen. Zeige, dass n genau dann ein Teiler von m ist, wenn es einen Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

gibt. Zeige durch ein Beispiel, dass es einen injektiven Gruppenhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

geben kann, ohne dass n ein Teiler von m ist.

Lösung:

Wenn n ein Teiler von m ist, so ist $m = an$ und daher ist $m \in \mathbb{Z}n$ und somit gilt die Idealinklusion $\mathbb{Z}m \subseteq \mathbb{Z}n$. Unter dem kanonischen Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n)$$

wird also $\mathbb{Z}m$ auf null abgebildet und daher gibt es nach dem Satz vom induzierten Homomorphismus einen Ringhomomorphismus

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

Wenn es umgekehrt einen solchen Ringhomomorphismus φ gibt, so betrachten wir insgesamt den Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(m) \xrightarrow{\varphi} \mathbb{Z}/(n)\,.$$

Die Gesamtabbildung muss also m auf null schicken, d.h. $m \mod n = 0$, und m ist ein Vielfaches von n.

Für das Beispiel betrachten wir $n = 4$ und $m = 2$. In $\mathbb{Z}/(4)$ bildet die Menge $\{\bar{0}, \bar{2}\}$ eine Untergruppe, die zu $\mathbb{Z}/(2)$ isomorph ist, so dass ein injektiver Gruppenhomomorphismus $\mathbb{Z}/(2) \to \mathbb{Z}/(4)$ vorliegt.

Aufgabe E.3. (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

$$x = 0 \mod 2, x = 3 \mod 9 \text{ und } x = 5 \mod 25$$

Lösung:

(a) Modulare Basislösungen. Es ist $9 \times 25 = 225$, und dies hat modulo 2 den Rest 1.

Es ist $2 \times 25 = 50$, und 50 hat modulo 9 den Rest 5, und 100 hat modulo 9 den Rest 1.

Es ist $2 \times 9 = 18$. Wir gehen die Vielfachen von 18 durch und berechnen die Reste modulo 25:

$$18,\ 36 = 11,\ 54 = 4,\ 72 = 22,\ 90 = 15,\ 108 = 8,\ 126 = 1\,.$$

Die Basislösungen sind also $225, 100, 126$.

(b) Eine Lösung für die angegebenen simultanen Kongruenzen ist (modulo $2 \cdot 9 \cdot 25 = 450$)

$$0 \cdot 225 + 3 \cdot 100 + 5 \cdot 126 = 300 + 630 = 930 = 30\,.$$

Daher ist 30 die kleinste positive Lösung.

Aufgabe E.4. Wie viele Elemente besitzt die von der Drehung um 45 Grad, von der Drehung um 99 Grad und von der Zwölfteldrehung erzeugte Untergruppe der Drehgruppe SO_2?

Lösung:

Wir schreiben die Drehungen als Teildrehungen einer Volldrehung, also

$$\frac{45}{360} = \frac{1}{8},\ \frac{99}{360} = \frac{11}{40},\ \frac{1}{12}\,.$$

Mit dem Hauptnenner 120 sind dies die Drehungen

$$\frac{15}{120}, \frac{33}{120}, \frac{10}{120}.$$

Jede dieser Drehungen ist ein Vielfaches der $\frac{1}{120}$-Drehung. Andererseits sind die Zahlen $15, 33$ und 10 teilerfremd, so dass es eine Darstellung der 1 gibt. Daher ist die von den drei Drehungen erzeugte Untergruppe genau die von der $\frac{1}{120}$-Drehung erzeugte Untergruppe und enthält daher 120 Elemente.

Aufgabe E.5. Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

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

wann f ein Nichtnullteiler und wann f eine Einheit ist.

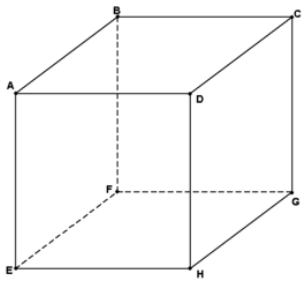
Lösung:

Die Multiplikationsabbildung ist ein Gruppenhomomorphismus, wie direkt aus dem Distributivitätsgesetz folgt. Es gilt:

f ist ein Nichtnullteiler genau dann, wenn für alle $g \in R$ aus $fg = 0$ folgt $g = 0$. Dies ist genau dann der Fall, wenn der Kern von μ_f nur aus 0 besteht, was genau dann gilt, wenn μ_f injektiv ist.

f ist eine Einheit genau dann, wenn es ein $g \in R$ gibt mit $fg = 1$, was genau dann der Fall ist, wenn 1 zum Bild von μ_f gehört. Dies wiederum ist äquivalent dazu, dass μ_f surjektiv ist, denn aus $fg = 1$ folgt sofort $h = (fg)h = f(gh)$ für jedes $h \in R$.

Aufgabe E.6. Betrachte den Würfel



Es sei α diejenige Drehung am Würfel um die Achse durch die Eckpunkte A und G, die den Eckpunkt B auf D schickt, und es sei β die Halbdrehung um die vertikale Achse (also die Gerade, die durch den Mittelpunkt der Seitenfläche A, B, C, D und den Mittelpunkt der Seitenfläche E, F, G, H läuft).

a) Man gebe eine Wertetabelle für die Permutationen auf der Eckpunktmenge $\{A, B, C, D, E, F, G, H\}$, die durch $\alpha, \beta, \alpha\beta$ und $\beta\alpha$ bewirkt werden.

b) Bestimme die Drehachse von $\alpha\beta$ und von $\beta\alpha$ sowie die Ordnung dieser Drehungen.

c) Man gebe die Zykeldarstellung der von α^2 bewirkten Permutation auf der Eckpunktmenge an. Was ist α^{1001}?

d) Man betrachte die Permutation σ, die auf der Eckpunktmenge durch die Wertetabelle

x	A	A	C	D	E	F	G	H
$\sigma(x)$	B	C	D	A	G	H	E	F

gegeben ist. Gibt es eine Drehung des Würfels, die diese Permutation bewirkt? Berechne das Signum von σ.

Lösung:

a) Die Wertetabellen für die angegebenen Permutationen sind

x	A	A	C	D	E	F	G	H
$\alpha(x)$	A	D	H	E	B	C	G	F

x	A	A	C	D	E	F	G	H
$\beta(x)$	C	D	A	B	G	H	E	F

x	A	A	C	D	E	F	G	H
$\alpha\beta(x)$	H	E	A	D	G	F	B	C

x	A	A	C	D	E	F	G	H
$\beta\alpha(x)$	C	B	F	G	D	A	E	H

b) Die Drehachse von $\alpha\beta$ ist die Gerade durch die beiden Eckpunkte D und F und die Drehachse von $\beta\alpha$ ist die Gerade durch die beiden Eckpunkte B und H. Beides sind Dritteldrehungen, ihre Ordnung ist 3.

c) Aus der Wertetabelle für α kann man leicht diejenige für α^2 errechnen, und damit auch die Zykledarstellung. Diese ist

$$\langle B, E, D\rangle\langle C, F, H\rangle\,.$$

Die Ordnung von α ist 3, daher ist $\alpha^{1001} = \alpha^2$.

d) σ stimmt auf den unteren Eckpunkten E, F, G, H mit der durch β definierten Permutation überein. Würde σ von einer Würfelbewegung γ herrühren,

so wäre $\beta\gamma^{-1}$ die Identität auf der unteren Ebenen und müßte dann überhaupt die Identität sein. Dann wäre $\beta = \gamma$, was aber wegen

$$\beta(A) \;=\; C \;\neq\; B \;=\; \gamma(A)$$

nicht der Fall ist.

σ hat die Zykeldarstelung

$$\sigma = \langle A, B, C, D\rangle\langle E, G\rangle\langle H, F\rangle\,,$$

die wir als Produktdarstellung lesen. Der vordere Zykel ist als Produkt geschrieben

$$\langle A, B, C, D\rangle = \langle B, C\rangle\langle C, D\rangle\langle D, A\rangle\,.$$

Insgesamt ist σ das Produkt von 5 Transpositionen und daher ist das Signum -1.

Die nächste Aufgabe verwendet die folgende Definition.

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 Schreibweise $a > b$ bedeutet $a \geq b$ und $a \neq b$. Die Schreibweise $a \leq b$ bedeutet $b \geq a$.

Aufgabe E.7. Es sei R ein angeordneter Integritätsbereich.

a) Zeige, dass aus $ca \geq cb$ mit $c > 0$ folgt, dass $a \geq b$ ist.

b) Zeige, dass $1 > 0$ in R gilt.

c) Zeige, dass aus $a < 0$ die Eigenschaft $-a > 0$ folgt.

d) Es sei $K = Q(R)$ der Quotientenkörper von R. Definiere eine Ordnungsrelation $\geq$ auf K, die auf $R \subseteq K$ mit der vorgegebenen Ordnung übereinstimmt, und die K zu einem angeordneten Körper macht.

Lösung:

a) Angenommen, unter den angegebenen Voraussetzungen wäre nicht $a \geq b$. Da eine totale Ordnung vorliegt, ist dann $a < b$. D.h. insbesondere $a \leq b$ und daraus folgt $ac \leq bc$. Wenn dies gleich wäre, würde wegen der Kürzbarkeit in einem Integritätsbereich und wegen $c \neq 0$ sofort $a = b$ folgen, was ausgeschlossen ist. Daher ist $ac < bc$ im Widerspruch zur Voraussetzung.

b) Die Eigenschaft $1 > 0$ ist aufgrund der ersten Eigenschaft äquivalent zu $0 > -1$, so dass wir $-1 \geq 0$ annehmen. Aufgrund der zweiten Eigenschaft ist dann $1 = (-1)(-1) \geq (-1)0 = 0$ und wegen $1 \neq 0$ in einem Integritätsbereich folgt doch $1 > 0$.

c) Aus $a < 0$ folgt durch beidseitige Addition mit $-a$ sofort $0 \leq -a$. Würde $0 = -a$ gelten, so folgt $a = 0$ im Widerspruch zur Voraussetzung, also ist $0 < -a$.

d) Ein Element im Quotientenkörper $K = Q(R)$ wird repräsentiert durch einen Bruch $\frac{a}{b}$ mit $a, b \in R$, $b \neq 0$. Dabei ist $\frac{a}{b} = \frac{c}{d}$ definitionsgemäß genau dann, wenn $ad = bc$ ist. Da eine totale Ordnung vorliegt, kann man stets annehmen, dass die Nenner positiv sind, da man mit -1 erweitern kann (nach Teil (c)). Im Folgenden nehmen wir alle Nenner als positiv an. Wir definieren

$$\frac{a}{b} \leq \frac{c}{d} \text{ wenn } ad \leq cb\,.$$

Man muss die Wohldefiniertheit dieser Definition nachweisen und dass die Eigenschaften eines geordneten Ringes erfüllt sind. Zur Wohldefiniertheit sei

$$\frac{a}{b} \leq \frac{c}{d}$$

und

$$\frac{a}{b} = \frac{a'}{b'} \text{ und } \frac{c}{d} = \frac{c'}{d'}\,.$$

Dann ist

$$a'd'cb \;=\; adb'c'.$$

Bei $c > 0$ ist

$$a'd'cb \;=\; adb'c' \;\leq\; c'b'cb$$

und daraus folgt durch kürzen (nach Teil (a)) $a'd' \leq c'b'$ wie gewünscht. Bei $c = 0$ ist auch $c' = 0$ und $\frac{a}{b} \leq 0$ bedeutet $a \leq 0$ und damit muss auch $a' \leq 0$ und $a'd' \leq 0$ sein. Bei $c < 0$ ist auch $c' < 0$. Dann ist $b'c' < 0$ und $-b'c' > 0$, also

$$a'd'(-cb) \;=\; ad(-b'c') \;\leq\; c'b'(-cb).$$

Daraus ergibt sich $a'd' \leq c'b'$. Daher ist die Ordnung wohldefiniert.

Jetzt sind die Ordnungseigenschaften zu testen. Es seien $x = \frac{a}{b}$, $y = \frac{c}{d}$ und $z = \frac{e}{f}$. Wir können stets zu einem Hauptnenner übergehen, also $b = d = f > 0$ annehmen. Aus dem bisher Bewiesenen folgt, dass $\frac{a}{b} \geq \frac{c}{b}$ genau dann gilt, wenn $a \geq c$ ist.

Die Reflexivität ist trivial. Zur Transitivität sei $x = \frac{a}{b} \leq y = \frac{c}{b}$ und $y = \frac{c}{b} \leq z = \frac{e}{b}$. Also ist $a \leq c$ und $c \leq e$ und daher ist $a \leq e$ und somit auch $x \leq z$.

Zur Antisymmetrie sei $\frac{a}{b} \leq \frac{c}{b}$ und $\frac{a}{b} \geq \frac{c}{b}$. Dann ist direkt $a = c$ und die Brüche stimmen überein.

Wir kommen nun zu den Eigenschaften eines geordneten Ringes.

(1). Aus $x = \frac{a}{b} \geq y = \frac{c}{b}$ folgt sofort $a \geq c$. Daher ist $a + e \geq c + e$ und somit wiederum

$$x + z \;=\; \frac{a+e}{b} \;\geq\; \frac{c+e}{b} \;=\; y + z.$$

(2). Sei $x \geq y$ und $z \geq 0$. Dann ist $a \geq c$ und $e \geq 0$ und somit $ae \geq ce$. Also ist

$$xz = \frac{a}{b}\frac{e}{b} = \frac{ae}{b^2} \geq \frac{ce}{b^2} = \frac{c}{b}\frac{e}{b} = yz.$$

Es ist trivial, dass eine Fortsetzung der Ordnung und eine totale Ordnung vorliegt.

Aufgabe E.8. Bestimme die Primfaktorzerlegung des Polynoms X^6-1 über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Lösung:

Es ist (über jedem Körper)

$$\begin{aligned} X^6-1 &= (X^2-1)(X^4+X^2+1) \\ &= (X-1)(X+1)(X^4+X^2+1) \\ &= (X-1)(X+1)(X^2+X+1)(X^2-X+1). \end{aligned}$$

Dies kann man direkt bestätigen, es ergibt sich aber auch aus der Produktzerlegung von X^6-1 mit Hilfe der Kreisteilungspolynome. Über den komplexen Zahlen ist

$$X^6-1 = \prod_{k=0}^{5}(X - e^{\frac{2\pi i k}{6}}).$$

Da davon vier Nullstellen imaginär sind, müssen die beiden quadratischen Polynome von oben über $\mathbb{Q}$ und über $\mathbb{R}$ irreduzibel sein, so dass die obige Faktorzerlegung über diesen Körpern die Primfaktorzerlegung ist.

Über $\mathbb{Z}/(7)$ gilt aufgrund des kleinen Fermat für jede Einheit $x^6 = 1$. Daher ist die Faktorzerlegung

$$X^6-1 = (X-1)(X-2)(X-3)(X-4)(X-5)(X-6).$$

Über $\mathbb{Z}/(5)$ haben die beiden Polynome X^2+X+1 und X^2-X+1 keine Nullstelle, sind also irreduzibel, und daher ist die obige Zerlegung auch die Primfaktorzerlegung über $\mathbb{Z}/(5)$.

Aufgabe E.9. Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2+U+1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4+uX^3+(u+1)X+1 \text{ durch } uX^2+X+u+1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Lösung:

Die Division mit Rest ergibt

$$X^4+uX^3+(u+1)X+1 = (uX^2+X+u+1)((u+1)X^2+(u+1)X+(u+1))+uX+u+1.$$

Aufgabe E.10. Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Lösung:

Wir betrachten die Abbildung

$$\mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times,\, x \longmapsto x^2,$$

der Einheitengruppe in sich. Diese schickt 1 auf 1 und wegen $(xy)^2 = x^2y^2$ handelt es sich um einen Gruppenhomomorphismus. Der Kern dieser Abbildung besteht aus den $x \in \mathbb{F}_q^\times$ mit $x^2 = 1$, also aus den Nullstellen des Polynoms $X^2 - 1$. Dessen Nullstellen sind gerade 1 und -1, weitere Nullstellen kann es nicht geben, da die Anzahl der Nullstellen durch den Grad des Polynoms beschränkt ist. Bei $1 = -1$ wäre $2 = 0$, was aufgrund der Charakteristik ausgeschlossen ist. Also besteht der Kern genau aus zwei Elementen. nach dem Isomorphiesatz ist das Bild isomorph zum Urbild modulo Kern. Das Bild ist genau die Menge der Quadrate in der Einheitengruppe, und diese ist isomorph zu $\mathbb{F}_q^\times/\{+1, -1\}$. Jede Nebenklasse besitzt daher zwei Elemente und die Anzahl der Nebenklassen ist daher $\frac{q-1}{2}$. Die Hälfte der Einheiten sind also Quadrate.

Aufgabe E.11. Beschreibe den Körper mit neun Elementen $\mathbb{F}_9$ als einen Restklassenkörper von $\mathbb{Z}/(3)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_9$ an.

Lösung:

In $\mathbb{Z}/(3)$ ist 2 kein Quadrat, wie man direkt nachrechnet. Daher ist $X^2 - 2 = X^2+1 \in \mathbb{Z}/(3)[X]$ ein irreduzibles Polynom und daher ist der Restklassenring

$$\mathbb{Z}/(3)[X]/(X^2 + 1)$$

ein Körper. Jedes Element wird dabei eindeutig geschrieben in der Form $ax + b$ (x bezeichnet die Restklasse von X) mit $a, b \in \mathbb{Z}/(3)$, so dass es sich um einen Körper mit 9 Elementen handelt.

Die Einheitengruppe von diesem Körper besitzt 8 Elemente. Alle Elemente haben also eine Zweierpotenz als Ordnung, und wir brauchen ein Element der Ordnung 8. Wir betrachten das Element $x + 1$. Es ist

$$(x + 1)^2 = x^2 + 2x + 1 = 2x + 3 = 2x \neq 1$$

und

$$(2x)^2 = 4x^2 = x^2 = 2 \neq 1.$$

Daher ist die Ordnung von $x + 1$ weder 1 noch 2 noch 4, also muss sie gleich 8 sein und es liegt ein primitives Element vor.

Aufgabe E.12. 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.

Lösung:

Es ist

$$X^4-1 \;=\; (X^2-1)(X^2+1) \;=\; (X+1)(X-1)(X^2+1)$$

und $X^2+1 \in \mathbb{Q}[X]$ ist irreduzibel, da es keine rationale Nullstelle besitzt. Es handelt sich also um die Primfaktorzerlegung, wobei die Faktoren paarweise nicht assoziiert sind, da sie ja alle normiert sind. Nach dem chinesischen Restsatz für Hauptidealbereiche gilt daher die Produktzerlegung

$$\mathbb{Q}[X]/(X^4-1) \;\cong\; \mathbb{Q}[X]/(X+1)\times\mathbb{Q}[X]/(X-1)\times\mathbb{Q}[X]/(X^2+1) \;\cong\; \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}[i],$$

wobei wir für das zweite Gleichheitszeichen die Einsetzungen $X \mapsto -1$ und $X \mapsto 1$ und die Isomorphie $\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[i]$ verwendet haben. Das Element $X^3+X = X(X^2+1)$ wird unter den drei Projektionen auf $-2, 2$ und 0 abgebildet, es ist also gleich

$$(-2, 2, 0)\,.$$

Aufgabe E.13. Formuliere und beweise die „Gradformel“ für eine Kette von endlichen Körpererweiterungen $K \subseteq L \subseteq M$.

Lösung:

Die Gradformel besagt

$$\operatorname{grad}_K M = (\operatorname{grad}_K L)(\operatorname{grad}_L M)\,.$$

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

$$x_i y_j, 1 \le i \le n, 1 \le j \le m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j}x_1 + \ldots + a_{nj}x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= (a_{11}x_1 + \ldots + a_{n1}x_n)y_1 + \ldots + (a_{1m}x_1 + \ldots + a_{nm}x_n)y_m \\ &= \sum_{1\le i\le n,\, 1\le j\le m} a_{ij} x_i y_j. \end{aligned}$$

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 $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. 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.

Aufgabe E.14. Es seien zwei verschiedene Punkte M, P in der Ebene gegeben. Es bezeichne K den Kreis mit Mittelpunkt M durch den Punkt P. Konstruiere (ohne andere Konstruktionen zu verwenden) die Tangente an den Kreis K durch P. Skizziere die Situation.

Lösung:

Wir zeichnen den Kreis C mit Mittelpunkt P durch den Punkt M. Die Verbindungsgerade G durch M und P hat mit C (neben M) noch einen weiteren Schnittpunkt, den wir mit S bezeichnen. Wir zeichnen Kreise K_1 und K_2 mit Mittelpunkt S durch M und mit Mittelpunkt M durch S. Die beiden Schnittpunkte von K_1 und K_2 definieren eine Gerade H, und diese verläuft durch P und steht senkrecht auf G (H ist die halbierende Senkrechte der Strecke von M nach S), so dass H die Tangente an P ist.

Aufgabe E.15. Charakterisiere mit Hilfe von Fermatschen Primzahlen (ohne Beweis) diejenigen natürlichen Zahlen n, für die das reguläre n-Eck konstruierbar ist. Wende diese Charakterisierung für n zwischen 30 und 40 an.

Lösung:

Zu einer natürlichen Zahl n ist das reguläre n-Eck genau dann konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat

$$n = 2^{\alpha} p_1 \cdots p_k$$

mit verschiedenen Fermatsche Primzahlen $p_1, \ldots, p_k$. Dabei ist eine Fermatsche Primzahl eine Primzahl der Form $p = 2^s + 1$. Für das Zahlenintervall von 30 bis 40 sind nur die Fermatschen Primzahlen $3, 5, 17$ relevant, und daher sind lediglich die regulären n-Ecke für

$$30 = 2 \cdot 3 \cdot 5,\ 32 = 2^5,\ 34 = 2 \cdot 17,\ 40 = 2^3 \cdot 5$$

konstruierbar.

Aufgabe F.1. (3 Punkte)

(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 F.2. (4 Punkte)

Bestimme in der Einheitengruppe $\mathbb{Z}/(17)^\times$ zu jeder möglichen Ordnung k ein Element $x \in \mathbb{Z}/(17)^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq \mathbb{Z}/(17)^\times$$

an, die aus vier Elementen besteht.

Aufgabe F.3. (5 Punkte)

Man berechne in $\mathbb{Z}/(80)$ die Elemente

(1) $3^{1234567}$,
(2) $2^{1234567}$,
(3) $5^{1234567}$.

Aufgabe F.4. (7 Punkte)

Betrachte auf der Produktmenge

$$\mathbb{N} \times \mathbb{N}$$

die Relation

$$(a,b) \sim (c,d) \text{ wenn } a + d = b + c\,.$$

Zeige, dass dies eine Äquivalenzrelation ist.

Es sei Z die Menge der Äquivalenzklassen. Definiere auf Z eine Addition $\oplus$, die die Eigenschaft

$$\overline{(a,0)} \oplus \overline{(b,0)} = \overline{(a+b,0)}$$

erfüllt (der Querstrich bedeutet dabei die zugehörige Äquivalenzklasse) und die Z zu einer kommutativen Gruppe macht.

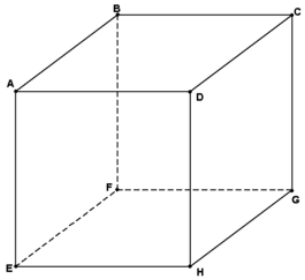
Aufgabe F.5. (4 Punkte)

Es sei $S = \{0, 1\}$. Betrachte das Monoid M, dass aus allen Abbildungen von S nach S besteht mit der Hintereinanderschaltung $\circ$ von Abbildungen als Verknüpfung.

(1) Beschreibe die Elemente in M und erstelle eine Verknüpfungstabelle für M.
(2) Bestimme sämtliche Untermonoide von M und entscheide jeweils, ob sie kommutativ sind und ob es sich um Gruppen handelt.

Aufgabe F.6. (5 Punkte)

Betrachte den Würfel



Es sei α die Gerade durch A und G, es sei β die Gerade durch B und H, es sei γ die Gerade durch C und E, es sei δ die Gerade durch D und F. Man beschreibe die Wirkungsweise der folgenden Würfelbewegungen auf der Menge $M = \{\alpha, \beta, \gamma, \delta\}$.

(1) Die Halbdrehung durch die vertikale Seitenmittelpunktsachse.
(2) Die Vierteldrehung durch die vertikale Seitenmittelpunktsachse, die A in B überführt.
(3) Die Halbdrehung um die Kantenmittelpunktsachse zur Kante A, E.
(4) Die Dritteldrehung um die Raumachse α, die B in D überführt.

Gibt es eine Würfelbewegung (wenn ja, welche?), die α auf α, β auf β abbildet und die γ und δ vertauscht?

Aufgabe F.7. (4 Punkte)

Betrachte die Permutation $\tau \in S_7$, die durch die Wertetabelle

x	1	1	3	4	5	6	7
$\tau(x)$	1	3	5	7	6	4	2

gegeben ist.

(1) Man gebe die Zyklendarstellung von τ an und bestimme den Wirkungsbereich.
(2) Berechne τ^3 und die Ordnung von τ^3.
(3) Bestimme die Fehlstände von τ und das Vorzeichen (Signum) von τ.
(4) Schreibe τ als Produkt von Transpositionen und bestimme erneut das Vorzeichen von τ.

Aufgabe F.8. (3 Punkte)

Es sei R ein kommutativer Ring. Zu jedem $f \in R$ sei

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

die Multiplikation mit f. Zeige, dass μ_f genau dann bijektiv ist, wenn es surjektiv ist.

Man zeige durch ein Beispiel, dass in dieser Situation aus der Injektivität nicht die Bijektivität folgt.

Aufgabe F.9. (3 Punkte)

Es sei K ein Körper. Zeige, dass in K die Differenz, also die Verknüpfung

$$K \times K \longrightarrow K,\, (a,b) \longmapsto a-b,$$

genau dann assoziativ ist, wenn die Charakteristik von K gleich 2 ist.

Aufgabe F.10. (4 Punkte)

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 F.11. (4 Punkte)

Bestimme eine Darstellung des größten gemeinsamen Teilers der beiden Polynome

$$4X^4 + 2X^2 + 3 \text{ und } X^2 + 3X + 1$$

in $\mathbb{Z}/(5)[X]$. Wie sieht es in $\mathbb{Z}/(2)[X]$ aus?

Aufgabe F.12. (3 Punkte)

Beschreibe den Körper mit acht Elementen $\mathbb{F}_8$ als einen Restklassenkörper von $\mathbb{Z}/(2)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_8$ an.

Aufgabe F.13. (4 Punkte)

Bestimme das Kreisteilungspolynom Φ_9.

Aufgabe F.14. (8 Punkte)

Sei $x = \sqrt{2} + \sqrt{5} \in \mathbb{R}$ und betrachte die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(x) = L\,.$$

Zeige, dass diese Körpererweiterung algebraisch ist und bestimme den Grad der Körpererweiterung, das Minimalpolynom von x und das Inverse von x. (Man darf dabei verwenden, dass $\sqrt{2}, \sqrt{5}, \sqrt{10}$ irrationale Zahlen sind.)

Aufgabe F.15. (3 Punkte)

Beschreibe die wesentlichen mathematischen Schritte, mit denen man beweisen kann, dass die „Quadratur des Kreises“ nicht möglich ist.

Anhang G. Nachklausur mit Lösungen

Aufgabe G.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

$$x = 2 \mod 3, x = 4 \mod 5 \text{ und } x = 3 \mod 7$$

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 $269 - 2 \cdot 105 = 59$.

Aufgabe G.2. Bestimme in der Einheitengruppe $\mathbb{Z}/(17)^\times$ zu jeder möglichen Ordnung k ein Element $x \in \mathbb{Z}/(17)^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq \mathbb{Z}/(17)^\times$$

an, die aus vier Elementen besteht.

Lösung:

Da 17 eine Primzahl ist, handelt es sich bei $\mathbb{Z}/(17)$ um einen Körper, so dass die Einheitengruppe aus 16 Elementen besteht. Aufgrund des Satzes von Lagrange kommen als Ordnung nur Teiler von 16 in Frage, also $1, 2, 4, 8, 16$. Aufgrund des Struktursatzes über multiplikative endliche Untergruppen von Körpern ist die Einheitengruppe zyklisch, so dass jede mögliche Ordnung

auch auftritt. Wir bestimmen zuerst ein primitives Element, also ein Element der Ordnung 16. Es ist

$$2^1 = 2,\ 2^2 = 4,\ 2^4 = 4^2 = 16 = -1,\ 2^8 = 1\,,$$

d.h. 2 hat die Ordnung 8 und ist nicht primitiv.

Es ist

$$3^1 = 3,\ 3^2 = 9,\ 3^4 = 9^2 = 81 = 13 = -4,\ 3^8 = (-4)^2 = 16 = -1\,.$$

Also ist 3 eine primitive Einheit modulo 17 und hat die Ordnung 16. Daher gilt:

$$3^2 = 9 \text{ hat die Ordnung } 8\,,$$

$$3^4 = 13 \text{ hat die Ordnung } 4\,,$$

$$3^8 = -1 \text{ hat die Ordnung } 2\,,$$

$$1 \text{ hat die Ordnung } 1\,.$$

Eine Untergruppe aus vier Elementen ist die Menge

$$\{3^0, 3^4, 3^8, 3^{12}\} = \{1, 13, -1 = 16, -13 = 4\}\,.$$

Aufgabe G.3. Man berechne in $\mathbb{Z}/(80)$ die Elemente

(1) $3^{1234567}$,
(2) $2^{1234567}$,
(3) $5^{1234567}$.

Lösung:

(1). Es ist $3^4 = 81 = 1$ und 3 ist eine Einheit. Daher hängt die Potenz nur von der Restklasse des Exponenten modulo 4 ab, also

$$3^{1234567} = 3^{67} = 3^7 = 3^3 = 27.$$

(2). Wir verwenden die Isomorphie des chinesischen Restsatzes, also

$$\mathbb{Z}/(80) \cong \mathbb{Z}/(16) \times \mathbb{Z}/(5)\,.$$

Das Element 2 entspricht bei dieser Zerlegung dem Paar $(2, 2)$. Die Potenz kann man komponentenweise ausrechnen, dabei erhält man vorne 0, da der Exponent ≥ 4 ist. Hinten ist 2 eine Einheit der Ordnung 4, daher ist in $\mathbb{Z}/(5)$

$$2^{1234567} = 2^3 = 3.$$

Das Ergebnis ist also das Paar $(0, 3)$. Diesem entspricht das Element 48.

(3). Wir verwenden wieder den chinesischen Restsatz, diesmal geht es um das Element $(5,0)$. Die Ordnung von 5 modulo 16 ergibt sich aus

$$5^2 = 25 = 9,\ 5^4 = 9^2 = 81 = 1\,,$$

die Ordnung ist also wieder 4. Daher ist in $\mathbb{Z}/(16)$

$$5^{1234567} \;=\; 5^3 \;=\; 125 \;=\; 13.$$

Dem Paar $(13,0)$ entspricht das Element 45.

Aufgabe G.4. Betrachte auf der Produktmenge

$$\mathbb{N} \times \mathbb{N}$$

die Relation

$$(a,b) \sim (c,d) \text{ wenn } a+d = b+c\,.$$

Zeige, dass dies eine Äquivalenzrelation ist.

Es sei Z die Menge der Äquivalenzklassen. Definiere auf Z eine Addition $\oplus$, die die Eigenschaft

$$\overline{(a,0)} \oplus \overline{(b,0)} = \overline{(a+b,0)}$$

erfüllt (der Querstrich bedeutet dabei die zugehörige Äquivalenzklasse) und die Z zu einer kommutativen Gruppe macht.

Lösung:

Die Relation ist trivialerweise reflexiv, da die Addition in $\mathbb{N}$ kommutativ ist. Auch die Symmetrie ist direkt klar. Zur Transitivität sei

$$(a,b) \sim (c,d) \text{ und } (c,d) \sim (e,f)\,,$$

d.h.

$$a+d = b+c \text{ und } c+f = d+e\,.$$

Damit ist insgesamt

$$a+d+f = b+c+f = b+d+e\,.$$

Hier können wir beidseitig d abziehen und erhalten $a+f = b+e$, was $(a,b) \sim (e,f)$ bedeutet.

Wir definieren nun die Addition durch

$$\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c,b+d)}\,.$$

Wir müssen zeigen, dass diese Addition wohldefiniert ist. Sei dazu

$$(a,b) \sim (a',b'),\ \text{also } a+b' = a'+b$$

und

$$(c,d) \sim (c',d'),\ \text{also } c+d' = c'+d\,.$$

Wir müssen zeigen, dass

$$(a+c,b+d) \sim (a'+c',b'+d')$$

ist. Dies folgt aber aus

$$a + c + b' + d' \;=\; a + b' + c + d' \;=\; a' + b + c' + d \;=\; a' + c' + b + d.$$

Wenn die hintere Komponente beidesmal 0 ist, so wird in der ersten Komponente einfach wie in $\mathbb{N}$ addiert. Die Verknüpfung ist assoziativ, da die komponentenweise Addition auf der Produktmenge assoziativ ist und sich dies auf die Verknüpfung auf den Äquivalenzklassen überträgt. Daraus folgt auch sofort, dass $\overline{(0,0)}$ das neutrale Element ist. Die Kommutativität der Verknüpfung ist ebenfalls klar. Zu einem Element $\overline{(a,b)}$ ist

$$\overline{(b,a)}$$

das inverse Element. Es ist ja

$$\overline{(a,b)} \oplus \overline{(b,a)} = \overline{(a+b,a+b)} = \overline{(0,0)}\,,$$

wobei die letzte Gleichung sich direkt aus der Definition der Relation $\sim$ ergibt.

Aufgabe G.5. Es sei $S = \{0,1\}$. Betrachte das Monoid M, dass aus allen Abbildungen von S nach S besteht mit der Hintereinanderschaltung $\circ$ von Abbildungen als Verknüpfung.

(1) Beschreibe die Elemente in M und erstelle eine Verknüpfungstabelle für M.
(2) Bestimme sämtliche Untermonoide von M und entscheide jeweils, ob sie kommutativ sind und ob es sich um Gruppen handelt.

Lösung:

(1). Es gibt vier Abbildungen der zweielementigen Menge in sich selbst, nämlich die Identität I, die Vertauschung V, die durch $V(0) = 1$ und $V(1) = 0$ festgelegt ist, und die beiden konstanten Abbildungen, die wir mit 0 bzw. 1 bezeichnen. Die Verknüpfungstabelle, bei der im Kreuzungspunkt von der φ-Zeile mit der ψ-Spalte die Verknüpfung $\varphi \circ \psi$ (also ψ zuerst angewendet) steht, sieht folgendermaßen aus:

$\circ$	I	V	0	1
I	I	V	0	1
V	V	I	1	0
0	0	0	0	0
1	1	1	1	1

(2). Die Identität I ist das neutrale Element des Monoids, jedes Untermonoid muss dieses Element enthalten.

Das kleinste Untermonoid ist $\{I\}$, das ist eine kommutative Gruppe.

$\{I, V\}$ ist ebenfalls eine kommutative Gruppe, da V zu sich selbst invers ist.

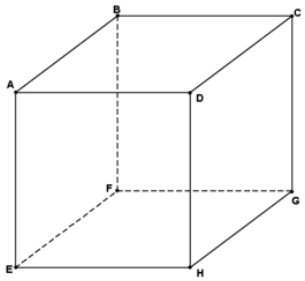
$\{I, 0\}$ ist ein kommutatives Untermonoid, wegen $I \circ 0 = 0 = 0 \circ I$ und $0 \circ 0 = 0$, aber keine Gruppe, da es kein inverses Element zu 0 gibt.

$\{I, 1\}$ ist ebenfalls ein kommutatives Untermonoid und keine Gruppe (gleicher Grund).

$\{I, 0, 1\}$ ist ein Untermonoid, da es unter der Operation abgeschlossen ist. Es ist keine Gruppe, da 0 und 1 nicht invertierbar sind. Es ist nicht kommutativ, da $0 \circ 1 = 0$ und $1 \circ 0 = 1$ ist.

Wenn man zu $\{I, V\}$ noch ein Element dazu tut, so ist wegen $V \circ 0 = 1$ auch das andere drin. Daher gibt es nur noch das volle Untermonoid $\{I, V, 0, 1\}$, das weder kommutativ noch eine Gruppe ist.

Aufgabe G.6. Betrachte den Würfel



Es sei α die Gerade durch A und G, es sei β die Gerade durch B und H, es sei γ die Gerade durch C und E, es sei δ die Gerade durch D und F. Man beschreibe die Wirkungsweise der folgenden Würfelbewegungen auf der Menge $M = \{\alpha, \beta, \gamma, \delta\}$.

(1) Die Halbdrehung durch die vertikale Seitenmittelpunktsachse.
(2) Die Vierteldrehung durch die vertikale Seitenmittelpunktsachse, die A in B überführt.
(3) Die Halbdrehung um die Kantenmittelpunktsachse zur Kante A, E.
(4) Die Dritteldrehung um die Raumachse α, die B in D überführt.

Gibt es eine Würfelbewegung (wenn ja, welche?), die α auf α, β auf β abbildet und die γ und δ vertauscht?

Lösung:

Die in Frage stehende Abbildung sei mit φ bezeichnet.

(1)

g	α	α	γ	δ
γ	δ	α	β	

(2)

g	α	α	γ	δ
β	γ	δ	α	

(3)

g	α	α	γ	δ
γ	β	α	δ	

(4)

g	α	α	γ	δ
α	δ	β	γ	

Es gibt eine solche Würfelbewegung: Die Halbdrehung um die Kantenmittelpunktsachse zur Kante C, D hat diese Eigenschaft.

Aufgabe G.7. Betrachte die Permutation $\tau \in S_7$, die durch die Wertetabelle

x	1	1	3	4	5	6	7
$\tau(x)$	1	3	5	7	6	4	2

gegeben ist.

(1) Man gebe die Zyklendarstellung von τ an und bestimme den Wirkungsbereich.
(2) Berechne τ^3 und die Ordnung von τ^3.
(3) Bestimme die Fehlstände von τ und das Vorzeichen (Signum) von τ.
(4) Schreibe τ als Produkt von Transpositionen und bestimme erneut das Vorzeichen von τ.

Lösung:

(1) Es geht $1 \mapsto 1$ und $2 \mapsto 3 \mapsto 5 \mapsto 6 \mapsto 4 \mapsto 7 \mapsto 2$, die Zyklendarstellung ist also

$$\langle 2, 3, 5, 6, 4, 7 \rangle$$

und der Wirkungsbereich ist $\{2, 3, 4, 5, 6, 7\}$.

(2) Die Permutation τ^3 ist gegeben durch die Wertetabelle

x	1	1	3	4	5	6	7
$\tau^3(x)$	1	6	4	3	7	2	5

Hier liegt die Zyklendarstellung

$$\langle 2, 6 \rangle \langle 3, 4 \rangle \langle 5, 7 \rangle$$

vor. Das Quadrat davon, also $(\tau^3)^2$ ist die Identität, so dass die Ordnung davon zwei ist.

(3) Die Fehlstände von τ sind

$$(2,7),\ (3,6),\ (3,7),\ (4,5),\ (4,6),\ (4,7),\ (5,6),\ (5,7),\ (6,7)\,.$$

Das sind insgesamt 9 Fehlstände, daher ist das Vorzeichen -1.

(4) Es ist, wie man leicht überprüft,

$$\tau = \langle 3,5\rangle \circ \langle 5,6\rangle \circ \langle 6,4\rangle \circ \langle 4,7\rangle \circ \langle 7,2\rangle\,.$$

Dies ist das Produkt von 5 Transpositionen, so dass sich erneut ergibt, dass das Vorzeichen -1 ist.

Aufgabe G.8. Es sei R ein kommutativer Ring. Zu jedem $f \in R$ sei

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

die Multiplikation mit f. Zeige, dass μ_f genau dann bijektiv ist, wenn es surjektiv ist.

Man zeige durch ein Beispiel, dass in dieser Situation aus der Injektivität nicht die Bijektivität folgt.

Lösung:

Die Bijektivität impliziert nach Definition stets die Surjektivität. Sei φ_f surjektiv. Dann gibt es insbesondere ein Urbild der 1, also ein Element $g \in R$ mit $fg = 1$. Dies bedeutet, dass f eine Einheit ist. Wegen der Distributivität ist die Abbildung φ_f ein Gruppenhomomorphismus der additiven Gruppe $(R, +, 0)$. Um die Injektivität zu zeigen wenden wir das Kernkriterium an. Sei also $fh = 0$. Dann ist aber

$$0 \;=\; g(fh) \;=\; (fg)h \;=\; h,$$

so dass der Kern nur aus einem Element besteht.

Sei $R = \mathbb{Z}$. Dann ist die Multiplikation mit $f = 2$ injektiv, aber nicht surjektiv, da nur gerade Zahlen im Bild liegen.

Aufgabe G.9. Es sei K ein Körper. Zeige, dass in K die Differenz, also die Verknüpfung

$$K \times K \longrightarrow K,\ (a,b) \longmapsto a - b,$$

genau dann assoziativ ist, wenn die Charakteristik von K gleich 2 ist.

Lösung:

Es sei zuerst die Charakteristik gleich 2. Dies bedeutet $1 + 1 = 0$ und damit $b + b = 0$ für jedes $b \in K$. Also ist $b = -b$ und damit $a + b = a - b$, d.h.

die Differenz stimmt mit der Summe überein, und diese ist in jedem Körper assoziativ.

Sei umgekehrt die Differenz assoziativ, d.h. es gilt

$$a - (b - c) = (a - b) - c$$

für beliebige $a, b, c \in K$. Wir wenden dies auf $a = b = 0$ und $c = 1$ an und erhalten $1 = -1$, also $2 = 0$, was Charakteristik 2 bedeutet.

Aufgabe G.10. 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.

Lösung:

Wir multiplizieren $\frac{3}{7} + \frac{2}{5}i$ mit seinem konjugierten Element und erhalten

$$(\frac{3}{7} + \frac{2}{5}i)(\frac{3}{7} - \frac{2}{5}i) = \frac{9}{49} + \frac{4}{25} = \frac{225 + 196}{1225} = \frac{421}{1225}\,.$$

Daher ist

$$(\frac{3}{7} + \frac{2}{5}i)^{-1} = \frac{1225}{421}(\frac{3}{7} - \frac{2}{5}i) = \frac{3675}{2947} - \frac{2450}{2105}i = \frac{3675}{2947} - \frac{490}{421}i.$$

Wir überprüfen mittels dem euklidischen Algorithmus, ob die Brüche gekürzt sind oder ob man sie noch vereinfachen kann. Rechts ergibt sich

$$490 = 1 \cdot 421 + 69$$

$$421 = 6 \cdot 69 + 7$$

$$69 = 9 \cdot 7 + 6$$

$$7 = 1 \cdot 6 + 1\,,$$

so dass Zähler und Nenner teilerfremd sind und die Darstellung gekürzt ist. Links ergibt sich

$$3675 = 1 \cdot 2947 + 728$$

$$2947 = 4 \cdot 728 + 35$$

$$728 = 20 \cdot 35 + 28$$

$$35 = 1 \cdot 28 + 7$$

$$28 = 4 \cdot 7 + 0\,.$$

Daher ist 7 der größte gemeinsame Teiler von Zähler und Nenner, und wir können durch 7 kürzen. Es ist

$$3675/7 = 525 \text{ und } 2947 = 7 \cdot 421\,,$$

also ist

$$(\frac{3}{7} + \frac{2}{5}i)^{-1} = \frac{525}{421} - \frac{490}{421}i.$$

Aufgabe G.11. Bestimme eine Darstellung des größten gemeinsamen Teilers der beiden Polynome

$$4X^4 + 2X^2 + 3 \text{ und } X^2 + 3X + 1$$

in $\mathbb{Z}/(5)[X]$. Wie sieht es in $\mathbb{Z}/(2)[X]$ aus?

Lösung:

Die Division mit Rest ergibt

$$(4X^4 + 2X^2 + 3) = (X^2 + 3X + 1)(4X^2 + 3X + 4) + 4\,.$$

Daher sind die beiden Polynome teilerfremd und es ist

$$4(4X^4 + 2X^2 + 3) + (4X^2 + 3X + 4)(X^2 + 3X + 1) = 1\,.$$

Über $\mathbb{Z}/(2)$ wird das erste Polynom zum konstanten Polynom 1, d.h. es ist automatisch zum zweiten Polynom teilerfremd und das erste Polynom für sich allein genommen ist schon die Darstellung der 1.

Aufgabe G.12. Beschreibe den Körper mit acht Elementen $\mathbb{F}_8$ als einen Restklassenkörper von $\mathbb{Z}/(2)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_8$ an.

Lösung:

Wir brauchen ein irreduzibles Polynom vom Grad drei in $\mathbb{Z}/(2)[X]$. Bei Grad drei kann man die Irreduzibilität dadurch nachweisen, dass keine Nullstelle vorliegt. Betrachten wir

$$F = X^3 + X + 1\,.$$

Weder 0 noch 1 sind Nullstellen, daher ist das Polynom irreduzibel und daher ist

$$K = \mathbb{Z}/(2)[X]/(X^3 + X + 1)$$

ein Körper mit 8 Elementen.

Da es in $\mathbb{F}_8$ genau 7 Einheiten gibt, und die Einheiten eine zyklische Gruppe bilden, ist jede Einheit außer 1 primitiv. Bspw. ist daher die Restklasse von X in K primitiv.

Aufgabe G.13. Bestimme das Kreisteilungspolynom Φ_9.

Lösung:

Es gilt die Gleichung

$$X^9 - 1 = \Phi_1\Phi_3\Phi_9$$

mit $\Phi_1 = X - 1$. Das dritte Kreisteilungspolynom errechnet sich aus

$$X^3 - 1 = (X - 1)\Phi_3$$

zu (Division mit Rest)

$$\Phi_3 = X^2 + X + 1\,.$$

Wegen $(X^9 - 1)/(X - 1) = X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ berechnet man das neunte Kreisteilungspolynom durch die Divison

$$(X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)/(X^2 + X + 1)\,.$$

Dies ergibt

$$\Phi_9 = X^6 + X^3 + 1\,.$$

Aufgabe G.14. Sei $x = \sqrt{2} + \sqrt{5} \in \mathbb{R}$ und betrachte die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(x) = L\,.$$

Zeige, dass diese Körpererweiterung algebraisch ist und bestimme den Grad der Körpererweiterung, das Minimalpolynom von x und das Inverse von x. (Man darf dabei verwenden, dass $\sqrt{2}, \sqrt{5}, \sqrt{10}$ irrationale Zahlen sind.)

Lösung:

Wir behaupten zunächst, dass

$$L = \mathbb{Q}[\sqrt{2}, \sqrt{5}] = (\mathbb{Q}[\sqrt{2}])[\sqrt{5}]$$

ist. Als eine Kette von quadratischen Körpererweiterungen ist dann $\mathbb{Q} \subseteq L$ algebraisch. Dabei ist die Inklusion $\subseteq$ klar. Es ist

$$x^2 = 7 + 2\sqrt{10},\ x^3 = 17\sqrt{2} + 11\sqrt{5}\,.$$

Daraus ergibt sich

$$\sqrt{2} = \frac{1}{6}(x^3 - 11x)\,,$$

so dass also $\sqrt{2}$ und damit auch $\sqrt{5}$ links dazu gehören, was die andere Inklusion ergibt.

Wir betrachten die Körperkette

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{5}] = L\,.$$

Dabei ist die Inklusion links echt, da $\sqrt{2}$ irrational ist, so dass links eine quadratische Körpererweiterung vorliegt. Aber auch die Inklusion rechts ist echt, denn anderfalls wäre

$$\sqrt{5} = a + b\sqrt{2} \text{ mit } a, b \in \mathbb{Q}\,,$$

was zu $5 = a^2 + 2b^2 + ab\sqrt{2}$ führt. Bei $a, b \neq 0$ ist das erneut im Widerspruch zur Irrationalität von $\sqrt{2}$. Bei $b = 0$ ist das ein Widerspruch zur Irrationalität von $\sqrt{5}$. Bei $a = 0$ ist das ein Widerspruch zur Irrationalität von $\sqrt{5/2} = \frac{1}{2}\sqrt{10}$.

Insgesamt liegt also eine Kette $\mathbb{Q} \subset K = \mathbb{Q}[\sqrt{2}] \subset L$ von quadratischen Körpererweiterungen vor, so dass aufgrund der Gradformel der Grad von $\mathbb{Q} \subset L$ gleich 4 ist.

Zur Bestimmung des Minimalpolynoms von x berechnen wir x^4, das ist

$$x^4 \;=\; (7 + 2\sqrt{10})^2 \;=\; 89 + 28\sqrt{10}.$$

Das Minimalpolynom ist gleich

$$F = X^4 - 14X^2 + 9\,.$$

Setzt man nämlich x ein, so erhält man 0. Da x den Körper L erzeugt, muss das Minimalpolynom den Grad 4 haben, so dass F das Minimalpolynom ist.

Zur Bestimmung des Inversen gehen wir von $x(x^3 - 14x) = -9$ aus. Daher ist das Inverse gleich

$$\begin{aligned} -\frac{1}{9}(x^3 - 14x) &= -\frac{1}{9}(17\sqrt{2} + 11\sqrt{5} - 14(\sqrt{2} + \sqrt{5})) \\ &= -\frac{1}{9}(3\sqrt{2} - 3\sqrt{5}) \\ &= -\frac{1}{3}\sqrt{2} + \frac{1}{3}\sqrt{5}. \end{aligned}$$

Aufgabe G.15. Beschreibe die wesentlichen mathematischen Schritte, mit denen man beweisen kann, dass die „Quadratur des Kreises“ nicht möglich ist.

Lösung:

Das Problem der Quadratur des Kreises bedeutet die Fragestellung, ob man aus einem durch den Radius gegebenen Kreis ein flächengleiches Quadrat mit Hilfe von Zirkel und Lineal konstruieren kann. Den Radius kann man dabei zu 1 normieren und durch zwei Punkte 0 und 1 repräsentieren. Da der Kreisinhalt π ist, muss die Seitenlänge des zu konstruierenden Quadrates $\sqrt{\pi}$ sein. Damit ist die Frage äquivalent dazu, ob man aus zwei Punkten mit Abstand 1 mittels Zirkel und Lineal den Abstand $\sqrt{\pi}$ konstruieren kann.

Der entscheidende Schritt ist, die Menge aller aus 0 und 1 konstruierbaren Punkte in der Ebene mathematisch zu erfassen. Dabei ergibt sich, dass bei

jedem elementaren Schritt (wie dem Durchschnitt von einem Kreis und einer Geraden) der neue Punkt in einer quadratischen Körpererweiterung der schon konstruierten Punkte liegt. Daraus ergibt sich induktiv, dass jeder konstruierbare Punkt eine algebraische Zahl ist. Der Satz von Lindemann besagt allerdings, dass π und damit auch $\sqrt{\pi}$ keine algebraische Zahl ist, und damit auch nicht konstruierbar.

Anhang H. 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