Mathematik Kompakt

Gernot Stroth

Elementare Algebra und Zahlentheorie

Birkhäuser

Mathematik Kompakt

Herausgegeben von:

Martin Brokate
Heinz W. Engl
Karl-Heinz Hoffmann
Götz Kersting
Gernot Stroth
Emo Welzl

Die neu konzipierte Lehrbuchreihe *Mathematik Kompakt* ist eine Reaktion auf die Umstellung der Diplomstudiengänge in Mathematik zu Bachelor- und Masterabschlüssen. Ähnlich wie die neuen Studiengänge selbst ist die Reihe modular aufgebaut und als Unterstützung der Dozierenden sowie als Material zum Selbststudium für Studierende gedacht. Der Umfang eines Bandes orientiert sich an der möglichen Stofffülle einer Vorlesung von zwei Semesterwochenstunden. Der Inhalt greift neue Entwicklungen des Faches auf und bezieht auch die Möglichkeiten der neuen Medien mit ein. Viele anwendungsrelevante Beispiele geben den Benutzern Übungsmöglichkeiten. Zusätzlich betont die Reihe Bezüge der Einzeldisziplinen untereinander.

Mit *Mathematik Kompakt* entsteht eine Reihe, die die neuen Studienstrukturen berücksichtigt und für Dozierende und Studierende ein breites Spektrum an Wahlmöglichkeiten bereitstellt.

Elementare Algebra und Zahlentheorie

Gernot Stroth

Birkhäuser

Autor:
Gernot Stroth
Institut für Mathematik
Martin-Luther-Universität Halle-Wittenberg
Theodor Lieser Str. 5
06099 Halle
e-mail: gernot.stroth@mathematik.uni-halle.de

2011 Mathematical Subject Classification: 11-01, 12-01, 13-01, 20-01

ISBN 978-3-0346-0501-4 ISBN 978-3-0346-0502-1 (eBook)
DOI 10.1007/978-3-0346-0502-1

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Satz und Layout: Protago-TEX-Production GmbH, Berlin, www.ptp-berlin.eu
Einbandentwurf: deblik, Berlin

Gedruckt auf säurefreiem Papier, hergestellt aus chlorfrei gebleichtem Zellstoff. TCF ∞
Printed in Germany

Springer Basel AG ist Teil der Fachverlagsgruppe Springer Science+Business Media

www.birkhauser-science.com

Für Heike

Vorwort

Die Algebra-Vorlesung gehört zu den zentralen Vorlesungen eines Mathematikstudiums. Wir hatten uns daran gewöhnt, dass es eine zweisemestrige Vorlesung Algebra (Algebra I/II) gab. Sicherlich haben sich im Laufe der Jahre die Inhalte weiterentwickelt, aber es gab doch ein allgemein akzeptiertes Kerncurriculum mit einem zentralen Teil, der Galoistheorie. Je nach Ambition des Vorlesenden gab es diese am Ende des ersten Semesters oder im zweiten Semester. Mit der Einführung der Bachelor-/Masterstudiengänge hat sich da einiges geändert. Es gibt kaum noch das zweisemestrige Modul Algebra. Dieses ist häufig durch ein Modul Algebra und dann eine Sammlung von möglichen Vertiefungsmodulen ersetzt worden, letztere oft erst für den Master vorgesehen. Dazu kommt, dass man heute kaum noch erwarten kann, dass Studierenden im Bachelorstudium ein Modul Algebra und ein weiteres Modul Zahlentheorie besucht. Man kann das beklagen, und als Algebraiker mache ich das auch, man kann aber dennoch versuchen, wie seit einigen Jahren in Halle geschehen, ein Modul Algebra/Zahlentheorie mit Leben zu erfüllen, das den Studierenden so etwas wie eine Allgemeinbildung auf beiden Gebieten vermittelt: nicht mehr, aber auch nicht weniger. Dies bedeutet nicht „Algebra light“, der Qualitätsanspruch muss gewahrt bleiben. Aus diesen Vorlesungen, die ich seit ein paar Jahren halte, ist dieses Buch hervorgegangen. Nun ist es nachvollziehbar, dass jeder Algebraiker hier wesentliche Dinge vermissen wird, genauso wird es Zahlentheoretiker geben, denen wichtige Dinge fehlen. Das kann auch gar nicht anders sein, wenn man bedenkt, dass dies der Stoff eines Semesters ist. Es ist keine systematische Einführung in die Algebra, und es ist erst recht keine in die Zahlentheorie. Die Zahlentheorie in diesem Buch bewegt sich im Wesentlichen im Bereich der Kongruenzen, was dann mit den quadratischen Kongruenzen am Ende des Buches seinen Höhepunkt erreichen wird. So werden auch wichtige Gebiete wie z.B. Siebmethoden, Kettenbrüche oder Pellsche Gleichung nicht thematisiert. Aber ich hoffe, und darüber möge der Leser urteilen, dass das Buch gewisse Grundideen und ein grundlegendes Allgemeinwissen wiedergibt, das ein Mathematiker haben sollte. So sollte man wissen, was ein euklidischer Ring, ein Hauptidealring, eine algebraische Körpererweiterung ist. Man sollte die Idee der Galoistheorie kennen. Im Bereich der Zahlentheorie sollte man etwas über Primzahlen, Häufigkeit und Verteilung wissen, Kongruenzrechnung und Zahlbereichserweiterungen als Beweismittel sollten bekannt sein, und schließlich sollte man vielleicht grob wissen, was mit dem quadratischen Reziprozitätsgesetz verbunden wird. Genau dies versucht das vorliegende Buch zu leisten.

Eine kurze Beschreibung der Inhalte soll hier mehr Klarheit schaffen. Wir beginnen mit den Grundlagen sowohl der Körpertheorie, als das wird Algebra hier im Wesentlichen verstanden, als auch der Zahlentheorie. Der Begriff der Primfak-

torzerlegung steht im Vordergrund. Es werden euklidische Ringe, Hauptidealringe und Polynomringe behandelt. Für Studierende ist es immer wieder überraschend, dass $\mathbb{Z}[x]$ keine Division mit Rest hat, man aber dennoch gut mit ganzzahligen Polynomen rechnen kann. Woran liegt das eigentlich? Nach diesem grundlegenden Kapitel entwickeln wir die Körpertheorie ein Stück weit. Dies bedeutet in Kapitel II die Behandlung der algebraischen Körpererweiterungen bis hin zur Konstruktion des algebraischen Abschlusses und in Kapitel III die Klassifikation der endlichen Körper. Die Existenz eines algebraischen Abschlusses ist im Folgenden nicht mehr erforderlich. Was benötigt wird, sind die Existenz und Eindeutigkeit des Zerfällungskörpers eines Polynoms, die man in Satz II.13 und Folgerung II.20 findet. Wenn man will, kann man sich also den algebraischen Abschluss ersparen.

Nach diesem ersten algebraischen Abschnitt kommen wir zu der Zahlentheorie mit den Begriffen Primzahl, Primzahlformel, kleiner Satz von Fermat, Eulerfunktion φ bis hin zu Carmichealzahlen. Danach wird dann wieder als Teil der Algebra die Gruppentheorie bis zum Sylow-Satz entwickelt, Auflösbarkeit wird thematisiert und schließlich die Einfachheit der alternierenden Gruppen A_n, $n \geq 5$, bewiesen. Danach konnte ich trotz der eingangs gemachten Bemerkungen nicht umhin, doch etwas zur Galoistheorie zu sagen. Im Mittelpunkt steht hier die Symmetrie (Gruppe) eines Polynoms, was zur Definition der Galoisgruppe führt. Mit der nicht bewiesenen Galoiskorrespondenz kann dann wieder bewiesen werden, dass die Auflösbarkeit eines Polynoms (Charakteristik 0) äquivalent zur Auflösbarkeit der Gruppe ist. Dies, meine ich, sollte ein Gymnasiallehrer einmal in seinem Studium gesehen haben. Im folgenden Kapitel wenden wir die Resultate über die algebraischen Körpererweiterungen auf die Geometrie, also auf die Konstruktion mit Zirkel und Lineal an. Dies geht bis zum Gaußschen Satz der Konstruierbarkeit des regulären n–Ecks, wobei auch wieder der nicht bewiesene Teil der Galoistheorie eine Rolle spielt.

Danach kehren wir endgültig in die Zahlentheorie zurück. Mit unseren algebraischen Hilfsmitteln können wir leicht entscheiden, welche natürlichen Zahlen Summe von zwei Quadraten sind. Hierzu wird ein Beweis gewählt, der zeigt, wie man die Idee der Zahlbereichserweiterung gewinnbringend einsetzen kann, am Beispiel des Satzes von Fermat werden aber auch die Grenzen aufgezeigt. Es ergibt sich dann natürlich im letzten Kapitel die Frage nach quadratischen Resten mit dem quadratischen Reziprozitätsgesetz als Höhepunkt. Das Buch endet mit Betrachtungen zu den Fermatschen Primzahlen.

Inhaltlich gibt es im Algebra-Teil dieses Buches (Kapitel I–III, V und VII) Überschneidungen mit meinem Algebra-Buch von 1998, die sich nicht vermeiden lassen. Es wird weitgehend dem dortigen Aufbau gefolgt. Dem Verlag De Gruyter sei Dank für die Erlaubnis, dies zu verwenden.

Es wurde versucht, wo immer möglich, auch historische Bezüge herzustellen. Diese stammen aus den Büchern von E. Scholz [26] und B.L. von der Waerden [31], aber auch zu großen Teilen aus Wikipedia. Den unbekannten Autoren dieser Plattform gilt mein ausdrücklicher Dank.

Der Aufbau des Buches spiegelt noch eine Besonderheit hier in Halle wider. Wir lesen die Algebra für Bachelorstudierende mit 9CP[1], für Studierende mit dem Ziel Lehramt an Gymnasien mit 7CP und für die mit dem Ziel Lehramt an Sekundarschulen mit 5CP. Ein Kurs für letztere könnte aus den ersten vier Kapiteln und Teilen von Kapitel VII (ohne die Konstruierbarkeit des n-Eckes) bestehen. Für Studierende

[1] Credit points (Leistungspunkte) gemäß European Credit Transfer and Accumulation System (ECTS).

mit dem Ziel Lehramt an Gymnasien würde ein Kurs in Halle aus den Kapiteln I–VII bestehen. Aber auch andere Zusammensetzungen sind denkbar.

Vorausgesetzt werden natürlich die Inhalte einer Vorlesung über Lineare Algebra. Eine Besonderheit mag sein, dass das Lemma von Zorn an einigen Stellen eingesetzt wird, was vielleicht nicht überall zum Standardstoff der Linearen Algebra gehört.

Ich möchte mich bei den Hörern meiner Vorlesungen zur Algebra bedanken, durch deren Rückmeldungen übersteigerte Ambitionen vermieden wurden. Frau Rebecca Waldecker hat große Teile dieses Buches gelesen und sehr wertvolle Verbesserungshinweise gegeben, auch hierfür möchte ich mich an dieser Stelle bedanken. Mein besonderer Dank geht an Frau Helbich, die die nicht immer leichte Umsetzung des Manuskripts in den Stil der Birkhäuser-Reihe durchgeführt hat. Dem Verlag danke ich für die angenehme und sehr hilfreiche Zusammenarbeit.

Halle, im September 2010 Gernot Stroth

Inhaltsverzeichnis

I Arithmetik

Was meinen wir eigentlich, wenn wir „Rechnen“ sagen? Normalerweise denken wir an die ganzen Zahlen $\mathbb{Z}$. Diese können wir z.B. addieren und multiplizieren, und dabei gelten gewisse Regeln.

Das Gleiche gilt auch für die Menge der Polynome mit Koeffizienten in einem Körper K oder $\mathbb{Z}$. Aber auch in

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\},$$

den sogenannten Gaußschen Zahlen können wir so rechnen. Dies führt zu einer allgemeinen Definition von Rechenbereichen, den Ringen.

Definition

Ring. Sei R eine Menge mit zwei Verknüpfungen $+, \cdot$. Bezüglich $+$ sei R eine kommutative Gruppe mit neutralem Element 0. Weiter gelte für alle $a, b, c \in R$

a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

b) $a \cdot (b + c) = a \cdot b + a \cdot c$

c) $(a + b) \cdot c = a \cdot c + b \cdot c$

d) Es gibt ein Element $1 \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

Dann nennen wir R einen *Ring*. Ist $a \cdot b = b \cdot a$ für alle $a, b \in R$, so wird R ein *kommutativer Ring* genannt. Ein kommutativer Ring, in dem zusätzlich $(R \setminus \{0\}, \cdot)$ eine Gruppe ist, heißt *Körper*.

Statt $a \cdot b$ werden wir normalerweise kurz ab schreiben.

Alle eingangs genannten Beispiele sind Ringe, keines davon ist ein Körper. Beispiele für Körper sind $\mathbb{R}, \mathbb{C}, \mathbb{Q}$. Was ist mit $R = \{0\}$ mit der Addition und Multiplikation ganzer Zahlen als Verknüpfungen? Dies ist offenbar ein Ring. Hier gilt $1 = 0$, was durch die Axiome nicht verboten ist. Es ist aber kein Körper, da $R \setminus \{0\}$ die leere Menge ist. Insbesondere kann es bezüglich $\cdot$ keine Gruppe sein, da eine Gruppe stets eine nicht leere Menge ist.

In diesem Buch werden alle Ringe kommutativ sein. Es gibt aber auch interessante nicht kommutative Ringe, wie z.B.

$$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}.$$

Besonders wichtig wird die folgende Konstruktion sein: Ist R ein Ring, so bezeichnen wir mit $R[x]$ die Menge der Polynome mit Koeffizienten in R. Es ist $R[x]$ wieder ein Ring.

Eine weitere Rechenoperation, die wir in der Praxis häufig benutzen, ist das Dividieren. Dies führt uns zu der Definition des Teilers:

Definition

Teiler. Sei R ein kommutativer Ring und $a, b \in R$. Wir sagen a teilt b, in Zeichen $a|b$, falls es ein $c \in R$ gibt, so dass $b = ca$ ist.

Bemerkung. Es gilt $0|0$, da z.B. $0 = 1 \cdot 0$ ist. Für jedes a gilt $a|0$, da $0 = 0 \cdot a$ ist.

Achtung! Teiler und Division sind zwei verschiedene Dinge. Es ist zwar 0 ein Teiler von 0, aber die Division von 0 durch 0 ist nicht definiert. Hier muss man sich also vor der Alltagssprache hüten. Es gibt eben in R den Ausdruck $\frac{a}{b}$ nicht.

Kann in einem Ring eigentlich beides,

$$a \text{ teilt } b \quad \text{und} \quad b \text{ teilt } a,$$

gelten? Das ist z.B. sicherlich der Fall, wenn $a = b$ ist. Ist dies aber die einzige Möglichkeit?

Gilt $a|b$, so gibt es ein $c \in R$ mit $b = ca$. Gilt $b|a$, so gibt es ein $d \in R$ mit $a = db$. Also gilt

$$b = (cd)b.$$

Folgt hieraus $cd = 1$? In den reellen Zahlen wäre das so, falls $b \neq 0$ ist.

Wir betrachten also zunächst den Sonderfall $b = 0$. Ist 0 ein Teiler von a, so ist $a = 0$, also ist $a = b$.

Sei ab jetzt $b \neq 0$. Dann gilt immerhin

$$b(1 - cd) = 0.$$

Folgt hieraus $1 - cd = 0$?

Allgemein: Folgt aus $xy = 0$ stets $x = 0$ oder $y = 0$? In unseren eingangs erwähnten Beispielen scheint dies so zu sein.

Wir betrachten den folgenden Ring $R = \{0, 1, 2, 3\}$ (Reste modulo 4) mit den Operationen + und $\bullet$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\bullet$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition und Multiplikation ist die in $\mathbb{Z}$, nur wird vom Resultat nur der Rest bei Division durch 4 genommen. Dies ist ein Ring. Aber $2 \bullet 2 = 0$.

Dies führt zu folgender Definition:

Definition

Integritätsbereich. Sei R ein kommutativer Ring.

a) $0 \neq x \in R$ heißt ein *Nullteiler*, falls es ein $0 \neq y \in R$ gibt, so dass $xy = 0$ ist.

b) Ein kommutativer Ring ohne Nullteiler heißt *Integritätsbereich*.

Wir greifen nun unsere Frage wieder für Integritätsbereiche auf. Dann ist

$$1 - cd = 0.$$

Also haben wir $cd = 1$. Damit sind c und d Teiler der 1. Das liefert aber noch nicht $c = d = 1$, da z.B. auch -1 ein Teiler von 1 ist. Das führt zu folgender Definition:

Definition

Einheit. Sei R ein Integritätsbereich. Ein Element $c \in R$ heißt *Einheit*, falls c ein Teiler von 1 ist.

Wir hatten gesehen, dass aus a teilt b und b teilt a folgt, dass $b = ca$ mit einer Einheit c ist. Ist umkehrt $b = ca$, mit einer Einheit c, so gibt es ein $d \in R$ mit $dc = 1$. Also ist $db = (dc)a = a$, d.h., b teilt a. Damit haben wir:

Lemma I.1

Seien R ein Integritätsbereich und $a, b \in R$. Ist a ein Teiler von b und b ein Teiler von a, so ist $a = be$ mit einer Einheit e.

In $\mathbb{Z}$ sind die Einheiten 1 und -1. Wir werden später sehen, dass in $K[x]$, K Körper, die Einheiten genau die Elemente aus K sind.

Was sind die Einheiten von $\mathbb{Z}[i]$?
Man sieht, dass 1, -1 aber auch i, $-i$ Einheiten sind, da $i \cdot (-i) = 1$ ist. Gibt es weitere?

Sei $a + bi \in \mathbb{Z}[i]$ eine Einheit. Dann gibt es $c + di \in Z[i]$ mit

$$(a + bi)(c + di) = 1.$$

Wir wenden nun einen Trick an. Diesen werden wir im Verlauf noch häufig einsetzen, so dass man auch von einer Methode sprechen kann. Wir bilden konjugiert Komplexe. Da für $z_1, z_2 \in \mathbb{C}$ stets $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ und $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ gilt, erhalten wir

$$\overline{(a + bi)}\,\overline{(c + di)} = 1$$

also

$$(a - bi)(c - di) = 1.$$

Nun multiplizieren wir beide Gleichungen

$$1 = (a + bi)(a - bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2).$$

Dies ist eine Gleichung in $\mathbb{Z}$. Damit erhalten wir nun

$$a^2 + b^2 = 1 = c^2 + d^2.$$

Aus $a^2 + b^2 = 1$ mit $a, b \in \mathbb{Z}$, folgt $a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$. Also ist $a + bi \in \{1, -1, i, -i\}$. Damit haben wir die Einheiten von $\mathbb{Z}[i]$ bestimmt.

Besonders wichtig beim Rechnen in $\mathbb{Z}$ sind die Primzahlen. Diese wollen wir jetzt auch in Integritätsbereichen definieren. Dazu lassen wir uns von $\mathbb{Z}$ motivieren.

a) Eine Primzahl p in $\mathbb{Z}$ hat die Eigenschaft: *Ist $x \in \mathbb{Z}$ ein Teiler von p, so ist x eine Einheit oder $x = ep$ mit einer Einheit e ($x = \pm 1$ oder $x = \pm p$).*

b) Eine Primzahl p in $\mathbb{Z}$ hat die Eigenschaft: *Sind $a, b \in \mathbb{Z}$ und ist p ein Teiler von ab, so ist p ein Teiler von a oder von b.*

Üblicherweise nennt man ± 1 nicht Primzahl, obwohl beide Eigenschaften a) und b) erfüllt werden. Dies führt nun zu der folgenden Definition: Dabei wollen wir allerdings etwas vorsichtiger vorgehen und a) und b) zunächst getrennt betrachten. Wir werden erst einmal a) irreduzibel und b) prim nennen.

Definition

Primelement. Sei R ein Integritätsbereich. Sei $p \in R$, $p \neq 0$, p keine Einheit.

a) Folgt für $x \in R$ aus $x|p$ stets, dass x eine Einheit oder $x = ep$ mit einer Einheit e ist, so nennen wir p ein *irreduzibles Element*.

b) Folgt für $a, b \in R$ mit p teilt ab stets, dass p einen der Faktoren a oder b teilt, so nennen wir p ein *Primelement*.

In $\mathbb{Z}$ gibt es keinen Unterschied zwischen Primelement und irreduziblem Element. Vielleicht ist das ja immer so. Der nächste Satz gibt eine Teilantwort.

Satz I.2

Sei R ein Integritätsbereich, p ein Primelement, so ist p irreduzibel.

Beweis. Sei a ein Teiler von p, also $p = ab$, mit $b \in R$. Da p ein Primelement ist, ist p ein Teiler von a oder b. Sei p ein Teiler von a. Mit Lemma I.1 erhalten wir $a = pe$ mit einer Einheit e. Ist p ein Teiler von b, so ist $b = pt$. Also ist $p = p(ta)$ und dann $p(1 - at) = 0$. Da R ein Integritätsbereich ist und $p \neq 0$ ist, folgt $at = 1$, also ist a eine Einheit. Damit haben wir gezeigt, dass die Teiler von p entweder Einheiten oder von der Form pe mit einer Einheit e sind. Somit ist p irreduzibel. □

Dies macht Mut, nur ist leider nicht jedes irreduzible Element prim. Dazu betrachten wir eine Variante des Rings der Gaußschen Zahlen

$$R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}.$$

Da R eine Teilmenge von $\mathbb{C}$ ist, ist R ein Integritätsbereich. Es ist $3 \in R$. Sei $a + b\sqrt{-5}$ ein Teiler von 3. Dann ist

$$3 = (a + b\sqrt{-5})(c + d\sqrt{-5}), a, b.c, d \in \mathbb{Z}.$$

Wir wenden nun den gleichen Trick wie bei der Bestimmung der Einheiten in $\mathbb{Z}[i]$ an. Es gilt auch

$$3 = (a - b\sqrt{-5})(c - d\sqrt{-5}).$$

Also ist

$$\begin{aligned} 9 = 3 \cdot 3 &= (a - b\sqrt{-5})(a + b\sqrt{-5})(c - d\sqrt{-5})(c + d\sqrt{-5}) \\ &= (a^2 + 5b^2)(c^2 + 5d^2). \end{aligned}$$

Dies ist eine Gleichung in $\mathbb{Z}$ und somit ist

$$a^2 + 5b^2 = 1, 3 \text{ oder } 9.$$

Ist $a^2 + 5b^2 = 3$, so muss $b^2 = 0$ und $a^2 = 3$ sein, was in $\mathbb{Z}$ keine Lösung hat.
Ist $a^2 + 5b^2 = 9$, so ist $c^2 + 5d^2 = 1$. Also ist stets

$$a^2 + 5b^2 = 1 \quad \text{oder} \quad c^2 + 5d^2 = 1.$$

Wir können per Symmetrie $a^2 + 5b^2 = 1$ annehmen. Dies hat in $\mathbb{Z}$ nur die Lösungen $b = 0, a = 1$ oder -1.

Damit haben wir

$$3 \quad \text{ist irreduzibel in} \quad R.$$

Offenbar ist

$$3|9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Wäre 3 prim, so wäre $3|2 + \sqrt{-5}$ oder $3|2 - \sqrt{-5}$. Dann gibt es $a + b\sqrt{-5} \in R$ mit

$$(2 + \sqrt{-5}) = (a + b\sqrt{-5})3 \text{ oder } (2 - \sqrt{-5}) = (a + b\sqrt{-5})3.$$

In beiden Fällen folgt

$$3a = 2 \quad \text{mit} \quad a \in \mathbb{Z}.$$

Dies ist ein Widerspruch. Somit sind prim und irreduzibel verschiedene Begriffe. Bevor wir uns ansehen, wann diese Begriffe doch gleich sind (z.B. in $\mathbb{Z}$), wollen wir den Teilerbegriff noch etwas weiter studieren.

In $\mathbb{Z}$ haben wir eine „Divison mit Rest". Dies besagt: Sind $a, b \in \mathbb{Z}$, $a \neq 0$, so gibt es $q, r \in \mathbb{Z}$ mit

$$b = qa + r\,, \quad |r| < |a|.$$

Wenn wir diesen Begriff auf weitere Integritätsbereiche ausdehnen wollen, benötigen wir eine Definition des Restes r, d.h. von „klein". Wir werden dabei den Betrag $|\cdot|$ auf $\mathbb{Z}$ durch eine Abbildung φ ersetzen.

Euklidischer[1] Ring. Ein Integritätsbereich R wird *euklidischer Ring* genannt, falls es eine Abbildung $\varphi: R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ gibt, die die beiden folgenden Eigenschaften hat: **Definition**

[1] Euklid von Alexandria (* um 365 v. Chr., † um 300 v. Chr.) wirkte in Alexandria, Verfasser des für viele Jahrhunderte grundlegenden Mathematikwerkes „Elemente".

a) Sind a und b in R mit $ab \neq 0$, so ist $\varphi(ab) \geq \varphi(a)$.

b) Sind $a, b \in R$ mit $a \neq 0$, so gibt es $q, r \in R$, abhängig von dem Paar a, b, mit
$$b = qa + r, \quad \text{wobei} \quad r = 0 \quad \text{oder} \quad \varphi(r) < \varphi(a) \quad \text{ist.}$$

In diesem Sinne ist $\mathbb{Z}$ mit $\varphi = |\cdot|$ ein euklidischer Ring. Ist auch $\mathbb{Z}[i]$ euklidisch? Wir setzen $\varphi = |\cdot|^2$, also

$$\varphi(a + bi) = a^2 + b^2 = (a + bi)\overline{(a + bi)}.$$

a) Sei $(a + bi)(c + di) \neq 0$. Dann ist

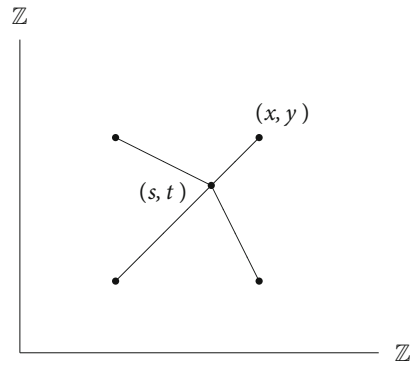
$$\begin{aligned} \varphi((a + ib)(c + id)) &= (a + ib)(c + id)\overline{(a + ib)(c + id)} \\ &= (a + ib)(\overline{a + ib})(c + id)(\overline{c + id}) \\ &= \varphi(a + ib)\varphi(c + id) \geq \varphi(a + bi). \end{aligned}$$

b) Sei $\alpha = a + bi$, $\beta = c + di \neq 0$. Für die komplexe Zahl $\frac{\alpha}{\beta}$ gilt dann:

$$\frac{\alpha}{\beta} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(a + bi)(c - di)}{c^2 + d^2} = s + it \quad \text{mit } s, t \in \mathbb{Q}.$$

Wir wählen nun ganze Zahlen x und y mit

$$|s - x| \leq \frac{1}{2} \quad \text{und} \quad |t - y| \leq \frac{1}{2}.$$



Wir haben damit $(a + ib) = (x + iy)(c + id) + r$, wobei

$$r = (c + id)[(s + it) - (x + iy)]$$

ist. Es ist $r \in \mathbb{Z}[i]$, da $r = (a+bi)-(c+di)(x+iy)$ ist, und $a+ib, x+iy$ und $c+id \in \mathbb{Z}[i]$ sind. Setze nun $q = x + iy$. Dann ist $a + bi = q(c + di) + r$. Weiter ist

$$\begin{aligned} \varphi(r) &= \varphi(c + di)\varphi((s - x) + i(t - y)) \\ &= \varphi(c + di)[(s - x)^2 + (t - y)^2] \\ &\leq \varphi(c + di)\left[\frac{1}{4} + \frac{1}{4}\right] = \frac{1}{2}\varphi(c + di) < \varphi(c + di). \end{aligned}$$

Somit ist $\mathbb{Z}[i]$ ein euklidischer Ring.

Ist auch $K[x]$, K ein Körper, ein euklidischer Ring? Dazu müssen wir etwas weiter ausholen. Sei zunächst R ein kommutativer Ring. Jedes Polynom in $R[x]$ hat einen Grad. Sei

$$f = \sum_{i=0}^{n} a_i x^i \quad \text{mit} \quad a_n \neq 0.$$

So ist

$$n = \operatorname{grad} f.$$

Es ist eine nützliche Konvention, $\operatorname{grad} 0 = -\infty$ zu setzen.

Lemma I.3

Sei R ein kommutativer Ring und $f, g \in R[x]$. Dann gilt

a) $\operatorname{grad}(fg) \leq \operatorname{grad} f + \operatorname{grad} g$.

b) Ist R ein Integritätsbereich, so ist $\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g$. *Insbesondere ist $R[x]$ ein Integritätsbereich.*

Beweis. Wir beweisen a) und b) gleichzeitig. Die Behauptungen sind klar für $f = 0$ oder $g = 0$. Sei also

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^i$$

mit $a_n \neq 0 \neq b_m$. Dann ist

$$fg = a_n b_m x^{n+m} + \sum_{i=0}^{n+m-1} c_i x^i.$$

Das ergibt $\operatorname{grad} fg \leq n+m = \operatorname{grad} f + \operatorname{grad} g$. Ist weiter R ein Integritätsbereich, so ist $a_n b_m \neq 0$, also gilt Gleichheit. Insbesondere ist $fg \neq 0$, d.h. $R[x]$ ist Integritätsbereich. □

Nun können wir zeigen, dass $K[x]$ euklidisch ist. Dabei werden wir die grad Funktion als φ benutzen. Also „klein“ bedeutet hier jetzt einfach „von kleinem Grad“.

Satz I.4

Sei K ein Körper

a) $K[x]$ ist ein euklidischer Ring.

b) Die Polynome vom Grad Null sind genau die Einheiten von $K[x]$.

Beweis. a) Für $f \in K[x], f \neq 0$, setze $\varphi(f) = \operatorname{grad} f$.

Ist $fg \neq 0$, so gilt nach Lemma I.3b)

$$\varphi(fg) = \operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g = \varphi(f) + \varphi(g) \geq \varphi(f).$$

Seien nun $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{j=0}^{m} b_j x^j$ mit $a_n b_m \neq 0$. Wir müssen q, r mit

$$f = qg + r$$

und $r = 0$ oder $\operatorname{grad} r < \operatorname{grad} g$ angeben.

Ist $\operatorname{grad} f < \operatorname{grad} g$, so setzen wir $q = 0$ und $r = f$ und sind fertig. Also können wir $\operatorname{grad} f \geq \operatorname{grad} g$ annehmen. Wir definieren nun f_1 durch

$$f_1 = f - x^{n-m} a_n b_m^{-1} g.$$

Dann ist $\operatorname{grad} f_1 \leq \operatorname{grad} f - 1 = n - 1$. Mit einer Induktion nach $\operatorname{grad} f$ erhalten wir

$$f_1 = q_1 g + r_1$$

mit $r_1 = 0$ oder $\operatorname{grad} r_1 < \operatorname{grad} g$.

Dann ist

$$f = (q_1 + x^{n-m} a_n b_m^{-1}) g + r_1$$

und wir setzen $q = q_1 + x^{n-m} a_n b_m^{-1}$ und $r = r_1$.

b) Sei f eine Einheit. Dann gibt es ein $g \in K[x]$ mit $fg = 1$. Also

$$0 = \operatorname{grad} 1 \underset{(I.3b)}{=} \operatorname{grad} f + \operatorname{grad} g.$$

Dies liefert $\operatorname{grad} f = 0$. □

Von unseren Beispielen zu Anfang dieses Kapitels bleibt $\mathbb{Z}[x]$. Der obige Beweis kann hier nicht verwendet werden, da wir b_m^{-1} in $\mathbb{Z}$ nicht bilden können. Dies sagt aber noch nicht, dass $\mathbb{Z}[x]$ kein euklidischer Ring ist. Es ist aber in der Tat so. $\mathbb{Z}[x]$ hat keine Division mit Rest, was immer φ auch sein mag. Es ist schwierig, die Nichtexistenz von etwas zu zeigen. Deshalb wollen wir zunächst euklidische Ringe eingehender studieren. Wir werden dann sehen, dass alle euklidischen Ringe eine gemeinsame Eigenschaft haben, die $\mathbb{Z}[x]$ offenbar nicht hat.

Der Begriff „euklidischer Ring“ leitet sich vom euklidischen Algorithmus zum Berechnen des ggT (a, b) her.

Seien $a, b \in R$. Wir teilen a durch b mit Rest, also

$$a = q_1 b + r_2 \quad \text{mit} \quad \varphi(r_2) < \varphi(b) \quad \text{oder} \quad r_2 = 0.$$

Ist $r_2 \neq 0$, so teile b durch r_2 mit Rest, also

$$b = q_2 r_2 + r_3 \quad \text{mit} \quad \varphi(r_3) < \varphi(r_2) \quad \text{oder} \quad r_3 = 0.$$

Dieses Verfahren setzen wir fort

$$r_i = q_{i+1} r_{i+1} + r_{i+2} \quad \varphi(r_{i+2}) < \varphi(r_{i+1}) \quad \text{oder} \quad r_{i+2} = 0.$$

Das endet mit

$$r_{n+2} = 0 \quad \text{also}$$
$$r_n = q_{n+1} r_{n+1}.$$

In $\mathbb{Z}$ kann man so den ggT $(a, b) = r_{n+1}$ berechnen. Wir zeigen dies durch Induktion nach n, also nach der Anzahl der Schritte. Ist $r_2 = 0$, so ist b ein Teiler von a und damit auch der größte gemeinsame Teiler von a und b. Sei also $r_2 \neq 0$. Dann besitzen per Induktion r_2 und b den größten gemeinsamen Teiler r_{n+1}. Dann ist aber auch r_{n+1} ein Teiler von a, da $a = q_1 b + r_2$ ist. Da der ggT (a, b) auch r_2 teilt, ist er ein Teiler von $r_{n+1} = \text{ggT}\,(b, r_2)$. Dies bedeutet dann, dass $r_{n+1} = \text{ggT}\,(a, b)$ ist. Eigentlich haben wir nur gezeigt, dass r_{n+1} und ggT (a, b) sich nur um ein Vorzeichen unterscheiden.

Sind a und b in $\mathbb{N}$, ist der ggT , wie wir ihn normalerweise benutzen, auch in $\mathbb{N}$. Wählt man bei der Division mit Rest immer den nicht negativen Rest, so ist auch $r_{n+1} \in \mathbb{N}$. Also ist dann wirklich $r_{n+1} = \text{ggT}\,(a, b)$.

Wir wollen den ggT nun auch in beliebigen Integritätsbereichen definieren. Dann haben wir aber keine natürliche Anordnung mehr. Wir gehen so wie in $\mathbb{Z}$ vor, also indem wir nur den Teilerbegriff benutzen.

Definition

Größter gemeinsamer Teiler (ggT). Sei R ein Integritätsbereich, $a, b \in R$. Wir nennen c einen *ggT* von a und b, falls gilt :

a) c teilt sowohl a als auch b.

b) Ist $d \in R$ ein Teiler sowohl von a als auch von b, so ist d ein Teiler von c.

Der ggT (a, b) ist allerdings jetzt nicht mehr eindeutig bestimmt. Sind c und d beides ggT von a und b, so ist c ein Teiler von d und d ein Teiler von c. Nach Lemma I.1 ist dann c bis auf eine Einheit gleich d. Also ist ggT (a, b) nur bis auf Einheiten bestimmt. Trotzdem werden wir im Folgenden $c = \text{ggT}\,(a, b)$ schreiben.

Wie in $\mathbb{Z}$ sieht man, dass in einem euklidischen Ring der euklidische Algorithmus einen ggT (a, b) berechnet. Dass die Existenz eines ggT (a, b) nicht selbstverständlich ist, zeigt folgendes Beispiel (siehe Schulze-Pillot [27] Aufgabe 3.4]:

Wir betrachten wieder

$$R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}.$$

Wir zeigen, dass $d = \text{ggT}\,(6, 4 + 2\sqrt{-5})$ nicht existiert. Sei dazu d ein größter gemeinsamer Teiler von 6 und $4 + 2\sqrt{-5}$. Offenbar ist 2 ein Teiler von 6 und von $4 + 2\sqrt{-5}$. Somit ist 2 ein Teiler von d. Weiter ist $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$ und $4 + 2\sqrt{-5} = -(1 - \sqrt{-5})^2$. Also ist auch $1 - \sqrt{-5}$ ein Teiler von d.

Ist a ein Teiler von d, so ist auch $|a|^2$ ein Teiler von $|d|^2$. Es ist $|2|^2 = 4$ und $|1-\sqrt{-5}|^2 = 6$. Damit sind sowohl 4 als auch 6 ein Teiler von $|d|^2$ in $\mathbb{Z}$. Also ist 12 ein Teiler $|d|^2$. Da d ein Teiler von 6 ist, ist $6 = de$, also $36 = |6|^2 = |d|^2|e|^2$.

Die einzige Lösung mit $12 \Big| |d|^2$ ist $|d|^2 = 36$ und $|e|^2 = 1$. Sei $e = a + b\sqrt{-5}$. Dann ist $1 = |e|^2 = a^2 + b^2 5$. Die einzige Lösung hiervon ist $b = 0$ und $a^2 = 1$. Also ist $d = 6$ oder -6. Damit wäre 6 ein Teiler von $4 + 2\sqrt{-5}$, was nicht geht. Also haben 6 und $4 + 2\sqrt{-5}$ keinen größten gemeinsamen Teiler in R.

Für feinere Untersuchungen in Ringen benötigen wir den Begriff des Ideals. Vergleiche hierzu auch die Bemerkungen auf Seite 126 am Ende von Kapitel VIII.

Definition

Ideal. Sei R ein Ring. Eine Teilmenge $\mathbf{i} \subseteq R$ heißt *Links- (Rechts-) Ideal*, falls gilt:

a) $(\mathbf{i}, +)$ ist eine Untergruppe von $(R, +)$.

b) Ist $a \in R$, so ist $a\mathbf{i} = \{ai | i \in \mathbf{i}\} \subseteq \mathbf{i}$, $(\mathbf{i}a = \{ia | i \in \mathbf{i}\} \subseteq \mathbf{i})$.

Ist $\mathbf{i}$ sowohl Rechts- als auch Linksideal, so nennen wir $\mathbf{i}$ 2-seitig.

Ist R kommutativ, so ist jedes Rechtsideal auch Linksideal und umgekehrt. In diesem Fall sprechen wir einfach von Idealen. So bilden z.B. die geraden Zahlen in $\mathbb{Z}$ ein Ideal.

Satz I.5

Sei R ein Ring, $\mathbf{i}$ ein 2-seitiges Ideal. Wir setzen $R/\mathbf{i} = \{a + \mathbf{i} | a \in R\}$.

(Da $(R, +)$ abelsch ist, ist jede Untergruppe Normalteiler, also ist $(R/\mathbf{i}, +)$ die Faktorgruppe. Siehe Seite 80.)

Wir definieren auf $R/\mathbf{i}$ eine Multiplikation durch

$$(a + \mathbf{i})(b + \mathbf{i}) = ab + \mathbf{i}, \quad a, b \in R.$$

Dann ist $R/\mathbf{i}$ ein Ring, der sogenannte Faktorring.

Beweis. Wir zeigen, dass die Multiplikation wohldefiniert ist. Der Rest sei dem Leser als Übung überlassen. Sei dazu $a' + \mathbf{i} = a + \mathbf{i}$ und $b' + \mathbf{i} = b + \mathbf{i}$. Dann ist $a' = a + i$ mit $i \in \mathbf{i}$ und $b' = b + j$ mit $j \in \mathbf{i}$. Es ist

$$(a' + \mathbf{i})(b' + \mathbf{i}) = [(a + i) + \mathbf{i}][(b + j) + \mathbf{i}] = ab + aj + ib + ij + \mathbf{i}.$$

Da $\mathbf{i}$ 2-seitig ist, ist $aj + ib + ij \in \mathbf{i}$, also ist $(a' + \mathbf{i})(b' + \mathbf{i}) = ab + \mathbf{i}$. □

Definition

Homomorphismus. Seien R_1, R_2 Ringe.

a) Eine Abbildung $\varphi: R_1 \to R_2$ heißt *Homomorphismus*, falls

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b) \qquad \text{und} \\ \varphi(ab) &= \varphi(a)\varphi(b) \end{aligned}$$

für alle $a, b \in R_1$ gilt.

Einen surjektiven Homomorphismus nennen wir *Epimorphismus*. Einen injektiven Homomorphismus nennen wir *Monomorphismus*. Einen bijektiven Homomorphismus nennen wir *Isomorphismus*. Ist $R_1 = R_2$, so nennen wir einen Isomorphismus auch *Automorphismus*. Ist φ ein Isomorphismus, so schreiben wir

$$R_1 \cong R_2.$$

b) Sei $\varphi: R_1 \to R_2$ ein Homomorphismus. Wir setzen

$$\ker \varphi = \{a | a \in R_1, \varphi(a) = 0\}$$

und nennen $\ker \varphi$ *den Kern des Homomorphismus* φ.

Lemma I.6

Seien R_1, R_2 Ringe und $\varphi: R_1 \to R_2$ ein Homomorphismus. Dann gilt:

a) $\varphi(0) = 0$.

b) Ist R_1 ein Körper, hat R_2 keine Nullteiler und gibt es ein $a \in R_1$ mit $\varphi(a) \neq 0$, so ist $\varphi(1) = 1$.

Beweis. a) Für alle $a \in R_1$ ist $\varphi(a) = \varphi(a+0) = \varphi(a) + \varphi(0)$, also gilt $\varphi(0) = 0$.

b) Sei nun R_1 ein Körper. Es ist $\varphi(a) = \varphi(1a) = \varphi(1)\varphi(a)$. Das liefert

$$0 = \varphi(a)(1 - \varphi(1)).$$

Da R_2 keine Nullteiler hat, ist also $0 = \varphi(1) - 1$ und somit $\varphi(1) = 1$. □

Lemma I.7

Seien R_1, R_2 Ringe und $\varphi: R_1 \to R_2$ ein Homomorphismus. Dann ist $\ker \varphi$ *ein 2-seitiges Ideal.*

Beweis. Wie in der Linearen Algebra sieht man, dass $\ker \varphi$ eine Untergruppe von $(R_1, +)$ ist. Seien $a \in R_1$ und $b \in \ker \varphi$. Dann ist $\varphi(ab) = \varphi(a)\varphi(b) = 0 = \varphi(b)\varphi(a) = \varphi(ba)$. Somit sind ab und ba in $\ker \varphi$, was zeigt, dass $\ker \varphi$ ein 2-seitiges Ideal ist. □

Satz I.8

Homomorphiesatz. *Seien R_1, R_2 Ringe und $\varphi: R_1 \to R_2$ ein Homomorphismus. Dann ist*

$$R_1/\ker \varphi \cong \text{Bild } \varphi.$$

Beweis. Wir definieren $\psi: \text{Bild } \varphi \to R_1/\ker \varphi$ durch $\psi(\varphi(a)) = a + \ker \varphi$.

Man beachte, dass nach Lemma I.7 $R_1/\ker \varphi$ ein Ring ist. Wie in der Linearen Algebra sieht man, dass ψ ein Isomorphismus bezüglich der addidiven Gruppen ist. Wir müssen also nur zeigen, dass ψ ein Homomorphismus ist. Dies sieht man wie folgt:

$$\psi(\varphi(a)\varphi(b)) = \psi(\varphi(ab)) = ab + \ker \varphi =$$
$$(a + \ker \varphi)(b + \ker \varphi) = \psi(\varphi(a))\psi(\varphi(b)).$$

□

Der nächste Satz erscheint zunächst etwas künstlich, wird uns später aber noch häufig gute Dienste leisten.

Satz I.9

Ein kommmutativer Ring R mit $|R| \geq 2$ ist genau dann ein Körper, wenn jedes Ideal gleich $\{0\}$ oder R ist.

Beweis. Es habe R nur die Ideale $\{0\}$ oder R. Wir zeigen, dass R ein Körper ist.

(1) Jedes $a \in R \setminus \{0\}$ hat ein Inverses.
Wir zeigen zunächst, dass

$$aR = \{ar | r \in R\}$$

ein Ideal ist. Seien dazu $ar_1, ar_2 \in aR$ und $b \in R$. Es ist

$$ar_1 + ar_2 = a(r_1 + r_2) \in aR$$

und

$$(ar_1)b = a(r_1 b) \in aR.$$

Also ist aR ein Ideal.

Es ist $a = a \cdot 1 \in aR$. Also ist $aR \neq \{0\}$. Somit ist nach der Annahme, dass es nur die Ideale $\{0\}$ und R gibt, $aR = R$. Da $1 \in R$ ist, gibt es ein $c \in R$ mit $ac = 1$, d.h., a ist invertierbar.

(2) $R \setminus \{0\}$ ist eine Gruppe.
Da $|R| \geq 2$ ist, ist $R \setminus \{0\} \neq \varnothing$. Somit haben wir wegen (1) nur zu zeigen, dass aus $a \neq 0 \neq b$ stets $ab \neq 0$ folgt.

Sei also $ab = 0$. Nach (1) gibt es ein c mit $bc = 1$. Also ist

$$0 = (ab)c = a(bc) = a,$$

ein Widerspruch zu $a \neq 0$.

Nach (2) ist nun R ein Körper.

Sei umgekehrt R ein Körper und $\mathbf{i} \neq \{0\}$ ein Ideal. Dann gibt es ein $a \in \mathbf{i}$, $a \neq 0$. Da R ein Körper ist, gibt es ein $b \in R$ mit $ab = 1$, d.h. $1 \in \mathbf{i}$. Dann ist

$$R = \{1 \cdot r | r \in R\} \subseteq \mathbf{i}.$$

□

Bemerkung. a) Im Beweis von Satz I.9 haben wir auch gezeigt: Ist $\mathbf{i}$ ein Ideal in R mit $1 \in \mathbf{i}$, so ist $\mathbf{i} = R$.

b) Der Ring $R = \{0\}$ hat nur die Ideale $\{0\}$ und R, ist aber kein Körper. Also ist die Voraussetzung $|R| \geq 2$ in Satz I.9 notwendig.

Folgerung I.10

Seien K_1, K_2 Körper und $\varphi: K_1 \to K_2$ ein Homomorphismus. Dann ist $\ker \varphi = \{0\}$ *oder* $\ker \varphi = K_1$.

Beweis. Nach Lemma I.7 ist $\ker \varphi$ ein Ideal. Nach Satz I.9 ist $\ker \varphi = K_1$ oder $\ker \varphi = \{0\}$. □

Definition

Primideal. Sei R ein kommutativer Ring. Ein Ideal $\mathbf{p} \neq R$ von R heißt *Primideal*, falls $R/\mathbf{p}$ ein Integritätsbereich ist.

Woher kommt der Name Primideal? Sei $R = \mathbb{Z}$ und $p \in \mathbb{Z}$ eine Primzahl. Wir behaupten, dass $p\mathbb{Z}$ ein Primideal ist. Wir nehmen dazu an, dass

$$ab + p\mathbb{Z} = (a + p\mathbb{Z})(b + p\mathbb{Z}) = p\mathbb{Z}$$

sei. Dann ist $ab \in p\mathbb{Z}$, d.h., p teilt ab. Also ist p ein Teiler von a oder b. Somit ist $a + p\mathbb{Z} = p\mathbb{Z}$ oder $b + p\mathbb{Z} = p\mathbb{Z}$. Das heißt, $\mathbb{Z}/p\mathbb{Z}$ ist ein Integritätsbereich.

Ist umgekehrt $m = n_1 n_2 \in \mathbb{Z}$, $n_1 \neq \pm m$, $n_2 \neq \pm m$. Dann sind beide $n_1 + m\mathbb{Z}$ und $n_2 + m\mathbb{Z}$ ungleich $m\mathbb{Z}$, aber $(n_1 + m\mathbb{Z})(n_2 + m\mathbb{Z}) = n_1 n_2 + m\mathbb{Z} = m\mathbb{Z}$.

Die von Null verschiedenen Ideale der Form $m\mathbb{Z}$, $m \in \mathbb{Z}$, sind somit genau dann Primideale, wenn m prim ist. Die Primideale sind somit eine Verallgemeinerung der Primzahlen in $\mathbb{Z}$.

Bemerkung. Satz I.9 zeigt, dass maximale Ideale $\mathbf{i}$ in kommutativen Ringen R prim sind, da $R/\mathbf{i}$ ein Körper ist.

Die Idee, wie wir gezeigt haben, dass $p\mathbb{Z}$ prim ist, kann man verallgemeinern.

Satz I.11

Sei R ein kommuntativer Ring und $\mathbf{i} \neq R$ ein Ideal. Es ist $\mathbf{i}$ genau dann ein Primideal, falls aus $a, b \in R$ mit $ab \in \mathbf{i}$ stets folgt, dass a oder b in $\mathbf{i}$ liegt.

Beweis. a) Sei $\mathbf{i}$ ein Primideal und $ab \in \mathbf{i}$. Dann ist

$$\mathbf{i} = ab + \mathbf{i} = (a + \mathbf{i})(b + \mathbf{i}).$$

Da $\mathbf{i}$ ein Primideal ist, ist $R/\mathbf{i}$ ein Integritätsbereich. Damit erhalten wir $a + \mathbf{i} = \mathbf{i}$ oder $b + \mathbf{i} = \mathbf{i}$, was gleichwertig zu $a \in \mathbf{i}$ oder $b \in \mathbf{i}$ ist.

b) Es gelte nun umgekehrt, dass aus $ab \in \mathbf{i}$ stets $a \in \mathbf{i}$ oder $b \in \mathbf{i}$ folgt. Wir wollen zeigen dass $R/\mathbf{i}$ ein Integritätsbereich ist. Seien dazu $a + \mathbf{i}$ und $b + \mathbf{i}$ Elemente aus $R/\mathbf{i}$ mit $(a + \mathbf{i})(b + \mathbf{i}) = \mathbf{i}$. Dann gilt $ab \in \mathbf{i}$. Nach Annahme ist nun $a \in \mathbf{i}$ oder $b \in \mathbf{i}$, also $a + \mathbf{i} = \mathbf{i}$ oder $b + \mathbf{i} = \mathbf{i}$. Somit ist $R/\mathbf{i}$ ist ein Integritätsbereich. □

Eine weitere Analogie zu den Verhältnissen in $\mathbb{Z}$, nämlich, dass prim und irreduzibel sich nicht unterscheiden, ist das nächste Resultat.

Lemma I.12

Seien R ein Integritätsbereich und $0 \neq p \in R$, so dass pR ein Primideal in R ist, so ist p irreduzibel.

Beweis. Sei $ab = p$ mit $a, b \in R$. Dann ist $ab \in pR$. Nach Satz I.11 ist $a \in pR$ oder $b \in pR$. Wir nehmen ohne Einschränkung $a \in pR$ an. Dann ist $a = px$ mit $x \in R$. Das liefert

$$p = pxb \quad \text{und} \quad p(1 - xb) = 0.$$

Da $p \neq 0$ ist, ist $1 = xb$, d.h., b ist eine Einheit. Da $pR \neq R$ ist, ist p keine Einheit. Also ist p irreduzibel. □

Wir wollen uns $\mathbb{Z}$ noch etwas genauer ansehen.

Sei $0 \neq \mathbf{i}$ ein Ideal in $\mathbb{Z}$. Dann gibt es ein $a \neq 0$ mit $a \in \mathbf{i}$. Wähle a mit $|a|$ minimal. Sei nun $b \in \mathbf{i}$, so teile b durch a mit Rest, also

$$b = qa + r, |r| < |a|.$$

Es ist $r = b - qa \in \mathbf{i}$. Die minimale Wahl von a liefert nun $r = 0$. Damit ist

$$\mathbf{i} = \{qa | q \in \mathbb{Z}\} = a\mathbb{Z}.$$

Somit haben alle Ideale von $\mathbb{Z}$ die Gestalt $a\mathbb{Z}$. Dies führt zu folgender Definition:

Definition

Hauptidealring. Sei R ein Integritätsbereich. Wir nennen R einen *Hauptidealring* (HIR), falls jedes Ideal $\mathbf{i}$ von R die Gestalt aR mit geeignetem $a \in R$ hat.

Was wir gerade gezeigt haben, ist:

Lemma I.13 *$\mathbb{Z}$ ist HIR.*

Die Idee von $\mathbb{Z}$ trägt aber weiter.

Satz I.14 *Jeder euklidische Ring R ist HIR.*

Beweis. Wir wiederholen einfach den Beweis für $\mathbb{Z}$. Sei $0 \neq \mathbf{i}$ ein Ideal von R, wähle $0 \neq a \in \mathbf{i}$ mit $\varphi(a)$ minimal. Sei $b \in \mathbf{i}$, so teile b durch a mit Rest, also

$$b = qa + r, \varphi(r) < \varphi(a) \text{ oder } r = 0.$$

Da $r = b - qa \in \mathbf{i}$ ist, folgt $r = 0$, d.h.

$$\mathbf{i} = \{qa | q \in R\} = aR.$$ □

Nun kommen wir wieder zu den Begriffen „prim“ und „irreduzibel“ zurück.

Satz I.15 *Sei R ein HIR. Dann sind 0 und pR mit irreduziblem p genau die Primideale in R. Weiter ist jedes von 0 verschiedene Primideal maximal, d.h., R/pR ist ein Körper.*

Beweis. Sei zunächst $\mathbf{p}$ ein Primideal. Da R ein Hauptidealring ist, gibt es ein $p \in R$ mit $\mathbf{p} = pR$. Ist $\mathbf{p} \neq 0$, so ist p nach Lemma I.12 irreduzibel.

Sei umgekehrt p irreduzibel. Wir zeigen, dass pR ein maximales Ideal ist. Sei $pR \subsetneqq aR \subsetneqq R$. Dann ist $p = ab$ mit geeignetem $b \in R$. Ist a eine Einheit, so ist $aR = R$, ein Widerspruch zur Annahme $aR \neq R$. Also ist a keine Einheit. Da p irreduzibel ist, ist dann b eine Einheit.

Es gibt also ein $c \in R$ mit $bc = 1$. Damit erhalten wir

$$a = abc = pc \in pR.$$

Also ist $aR \subseteq pR$ und dann $aR = pR$, ein Widerspruch zur Annahme $pR \neq aR$. Damit ist pR ein maximales Ideal. Nach Satz I.9 ist R/pR ein Körper, insbesondere ein Integritätsbereich. Somit ist pR ein Primideal. □

Wir wissen, dass $\mathbb{Z}$, $K[x]$ (K Körper) und $\mathbb{Z}[i]$ Hauptidealringe sind. Aber $\mathbb{Z}[x]$ ist keiner. Wir betrachten dazu das Ideal $x\mathbb{Z}[x]$. Offenbar ist

$$\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}.$$

Dies kann man wie folgt einsehen. Wir betrachten die Abbildung

$$\varphi: \mathbb{Z}[x] \to \mathbb{Z}$$

mit

$$\varphi(f) = f(0), f \in \mathbb{Z}[x].$$

Dann ist φ ein Homomorphismus. Es ist Bild $f = \mathbb{Z}$. Weiter ist $x\mathbb{Z}[x] = \ker f$. Der Homomorphiesatz I.8 liefert nun die Behauptung.

Somit ist $x\mathbb{Z}[x]$ ein Primideal, da $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$ ist, und $\mathbb{Z}$ ein Integritätsbereich ist. Da aber $\mathbb{Z}$ kein Körper ist, folgt mit Satz I.15, dass $\mathbb{Z}[x]$ kein Hauptidealring sein kann.

Damit haben wir auch die Frage beantwortet, ob es in $\mathbb{Z}[x]$ eine Division mit Rest gibt (was auch immer die Funktion φ sein mag). Diese gibt es nicht, da nach Satz I.14 jeder euklidische Ring ein Hauptidealring ist.

Bevor wir uns wieder $\mathbb{Z}[x]$ zuwenden, wollen wir die Hauptidealringe noch näher studieren. Wir werden als Erstes zeigen, dass diese immer einen ggT haben. Allein davon ausgehend, werden wir zeigen, dass man in Hauptidealringen vernünftig rechnen kann, d.h. insbesondere, dass wir einen Ersatz für die eindeutige Primfaktorzerlegung aus $\mathbb{Z}$ finden werden.

Satz I.16

Seien R ein Hauptidealring und $a_1, \ldots, a_t \in R$. Dann existiert ein größter gemeinsamer Teiler d von $a_1, \ldots, a_t$. Weiter gibt es $b_1, \ldots, b_t \in R$ mit

$$d = a_1 b_1 + \ldots + a_t b_t.$$

Beweis. Es ist $a_1 R + \ldots + a_t R$ ein Ideal, wie man leicht nachrechnet. Da R ein HIR ist, ist dann $a_1 R + \ldots + a_t R = dR$ für geeignetes $d \in R$.

Dann gibt es $r_i \in R$, $i = 1, \ldots, t$ mit $a_i = r_i d$. Insbesondere ist d ein Teiler von a_i, $i = 1, \ldots, t$.

Auf der anderen Seite gilt auch

$$d = a_1 b_1 + \ldots + a_t b_t \text{ mit } b_i \in R \text{ geeignet.}$$

Sei nun s ein Teiler von a_i, $i = 1, \ldots, t$. Dann teilt s natürlich auch alle Produkte $a_i b_i$, $i = 1, \ldots, t$. Also ist s ein Teiler von d. Damit ist d ein ggT von $a_1, \ldots, a_t$. □

Dies ist an sich ein ganz überraschender Satz. Er zeigt, dass der ggT, der ja rein unter Benutzung der multiplikativen Struktur des Ringes definiert wurde, von der additiven Struktur nicht unabhängig ist.

In einem euklidischen Ring kann man die Zerlegung

$$d = a_1 b_1 + a_2 b_2$$

mit dem euklidischen Algorithmus berechnen. Wenn man den ggT (a_1, a_2) wie auf Seite 8 mit dem euklidischen Algorithmus bestimmt, so hat jede Zeile die Form $r_i = q_{i+1} r_{i+1} + r_{i+2}$. Das bedeutet, dass jedes r_{i+2} eine Linearkombination der vorhergehenden ist, sich also letztendlich in der Form $a_1 c_1 + a_2 c_2$ schreiben lässt. Der letzte Rest r_{n+1} ist der ggT. Also können wir rückwärts diese Linearkombination bestimmen. Das hat nicht nur theoretische, sondern auch praktische Bedeutung. Seien etwa $a, b, c \in \mathbb{Z}$ gegeben. Gesucht sind $x, y \in \mathbb{Z}$ mit

$$ax + by = c.$$

Offenbar ist ggT $(a, b) = d$ ein Teiler von c. Mit dem euklidischen Algorithmus finden wir $x_1, y_1 \in \mathbb{Z}$ mit

$$ax_1 + by_1 = d.$$

Ist $c = ud$, so ist $x = ux_1, y = uy_1$ eine Lösung.

Wir zeigen nun, dass Hauptidealringe die von uns gesuchte Verallgemeinerung der Situation in $\mathbb{Z}$ sind, und zwar in der Hinsicht, dass die Begriffe prim und irreduzibel zusammen fallen.

Satz I.17 *In einem Hauptidealring R ist jedes irreduzible Element prim.*

Beweis. Sei $p \in R$ irreduzibel. Seien weiter $a, b \in R$ und p ein Teiler von ab, also $ab = pr$. Sei $d = \text{ggT}(a, p)$. Da p durch d geteilt wird, ist d eine Einheit oder $d = ep$ mit einer Einheit e. Sei $d = ep$, so ist p ein Teiler von d. Da a von d geteilt wird, wird dann auch a von p geteilt. Ist also p kein Teiler von a, so muss d eine Einheit sein, also ist 1 ein ggT (a, p). Nach Satz I.16 gibt es $u, v \in R$ mit

$$1 = up + va.$$

Dann ist

$$b = upb + vab = upb + vpr = p(ub + vr).$$

Also ist p ein Teiler von b. Damit haben wir gezeigt, dass p ein Teiler von a oder b ist. Somit ist p prim. □

Das wohl wichtigste Hilfsmittel beim Rechnen in $\mathbb{Z}$ ist die eindeutige Primfaktorzerlegung. Wobei „eindeutig“ natürlich nur bis auf Multiplikation mit ± 1 bedeuten kann. Hier sieht man, warum man ± 1 nicht als prim bezeichnen sollte.

Definition **Eindeutige Primfaktorzerlegung.** Wir nennen einen Integritätsbereich R einen Ring mit *eindeutiger Primfaktorzerlegung* (EPZ-Ring), falls gilt:

a) Ist $0 \neq a \in R$, a keine Einheit, so ist $a = p_1 \cdots p_n$ mit irreduziblen $p_1, \ldots, p_n$.

b) Die p_i in a) sind bis auf Multiplikation mit Einheiten und Reihenfolge eindeutig durch a bestimmt.

Unser Ziel ist es nun zu zeigen, dass Hauptidealringe eine eindeutige Primfaktorzerlegung haben. Dabei ist weniger die Eindeutigkeit ein Problem als die Existenz.

Eindeutigkeit: Sei

$$a = p_1 \cdots p_u = q_1 \cdots q_r$$

mit irreduziblen Elementen $p_1, \ldots, p_u, q_1, \ldots, q_r$.

Es ist p_1 ein Teiler von a. Nach Satz I.17 ist p_1 prim. Also gibt es ein i, so dass q_i von p_1 geteilt wird, d.h. $q_i = p_1 d$, $d \in R$. Da q_i irreduzibel ist, ist d eine Einheit.

Bei geeigneter Anordnung können wir $i = 1$ annehmen. Also ist

$$p_1(p_2 \cdots p_u) = dp_1(q_2 \cdots q_r) \text{ d.h. } p_1[(p_2 \cdots p_u) - d(q_2, \cdots, q_r)] = 0.$$

Dann ist $p_2 \cdots p_u = dq_2 \cdots q_r$.

Setze $\tilde{q}_2 = dq_2$. Dann ist auch $\tilde{q}_2$ irreduzibel. Also haben wir

$$p_2 \cdots p_u = \tilde{q}_2 q_3 \cdots q_r.$$

Eine Induktion nach u liefert nun die Behauptung.

Es bleibt, die Existenz zu zeigen.

Ist $R = \mathbb{Z}$, so kann man wie folgt argumentieren: Sei $a \in R$ keine Einheit. Ist a irreduzibel, so sind wir fertig. Ist a nicht irreduzibel, so gibt es $a_1, a_2 \in R$ mit $a = a_1 a_2$ und $|a_1| < |a| > |a_2|$. Eine Induktion nach $|a|$ liefert nun die Behauptung.

Es ist klar, dass wir so in beliebigen euklidischen Ringen argumentieren können. In Hauptidealringen fehlt uns diese Möglichkeit. Ein Ersatz liefert folgendes Lemma:

Lemma I.18

Sei R ein kommutativer Ring. Gleichwertig sind

a) Jedes Ideal $\mathbf{i}$ ist endlich erzeugt, d.h., es gibt ein $r \in \mathbb{N}$ und $a_1, \ldots, a_r \in R$ mit

$$\mathbf{i} = a_1 R + \cdots + a_r R.$$

b) Jede nicht leere Teilmenge $\mathfrak{S}$ von Idealen in R besitzt ein maximales Element.

Beweis. a)$\Rightarrow$ b): Sei $\mathfrak{K}$ eine Kette in $\mathfrak{S}$, d.h. eine total geordnete Teilmenge bzgl. $\subseteq$. Setze

$$\mathbf{j} = \bigcup_{\mathbf{i} \in \mathfrak{K}} \mathbf{i}.$$

Sind $a_1, a_2 \in \mathbf{j}$, so gibt es $\mathbf{i}_1, \mathbf{i}_2 \in \mathfrak{K}$ mit $a_1 \in \mathbf{i}_1, a_2 \in \mathbf{i}_2$. Da $\mathfrak{K}$ total geordnet ist, können wir $\mathbf{i}_1 \subseteq \mathbf{i}_2$ annehmen, d.h. $a_1 + a_2 \in \mathbf{i}_2 \subseteq \mathbf{j}$. Genauso ist auch $ra_1 \in \mathbf{i}_1 \subseteq \mathbf{j}$ für $r \in R$.

Also ist $\mathbf{j}$ ein Ideal. Nach Annahme gibt es $a_1, \ldots, a_r \in R$ mit

$$\mathbf{j} = a_1 R + \cdots + a_r R.$$

Insbesondere sind $a_1, \ldots, a_r \in \mathbf{j}$. Das heißt, es gibt Ideale $\mathbf{i}_1, \ldots, \mathbf{i}_r \in \mathfrak{K}$ mit $a_i \in \mathbf{i}_i$, $i = 1, \ldots, r$. Die Totalordnung liefert wieder, dass es ein k gibt mit $a_1, \ldots, a_r \in \mathbf{i}_k$. Das heißt, $\mathbf{j} \subseteq \mathbf{i}_k$. Insbesondere ist dann $\mathbf{j} = \mathbf{i}_k \in \mathfrak{K}$. Damit hat jede Kette eine obere Schranke in $\mathfrak{S}$. Nach dem Zornschen[2] Lemma hat dann $\mathfrak{S}$ maximale Elemente.

b) $\Rightarrow$ a): Sei $\mathbf{i}$ ein Ideal. Setze

$$\mathfrak{S} = \{\mathbf{j} | \mathbf{j} \subseteq \mathbf{i}, \mathbf{j} \text{ endlich erzeugtes Ideal }\}.$$

Es ist $0 = 0R \in \mathfrak{S}$, d.h. $\mathfrak{S} \neq \varnothing$. Nach Annahme gibt es ein maximales Element $\mathbf{j}_0 \in \mathfrak{S}$. Es ist

$$\mathbf{j}_0 = a_1 R + \cdots + a_r R \text{ für geeignete } a_1, \ldots, a_r \in R.$$

[2] Max Zorn (*6.6.1906 Hamburg, †9.3.1993 Bloomington), Indiana, emigrierte 1933 in die USA, Professor in Yale und Indiana University Bloomington, Arbeitsgebiete Gruppentheorie, Mengenlehre. Besondere Berühmtheit erlangte er durch das Zornsche Lemma (Zorn 1935, [34]).

Ist $\mathbf{j}_0 \neq \mathbf{i}$, so gibt es ein $b \in \mathbf{i} \setminus \mathbf{j}_0$. Es ist $\mathbf{i} \supseteq \mathbf{j}_0 + bR = a_1R + \cdots + a_rR + bR$. Somit ist $\mathbf{j}_0 + bR \in \mathfrak{S}$, aber $\mathbf{j}_0 \neq \mathbf{j}_0 + bR$, ein Widerspruch zur Maximalität von $\mathbf{j}_0$. Also ist $\mathbf{j}_0 = \mathbf{i}$ endlich erzeugt. □

Nun wenden wir uns der Existenz einer Zerlegung in irreduzible Elemente in Hauptidealringen zu. Sei dazu $a \in R$, $a \neq 0$. Setze

$$\mathfrak{S} = \{bR | a = bp_1 \cdots p_n, \text{ mit endlich vielen irreduziblen Elementen } p_i\}.$$

Da $a = a$ ist, ist $aR \in \mathfrak{S}$, d.h. $\mathfrak{S} \neq \varnothing$ (beachte, dass endlich viel auch keines bedeuten kann). Nach Lemma I.18 hat $\mathfrak{S}$ ein maximales Element cR. Also

$$a = cp_1 \cdots p_k.$$

Wir zeigen, dass c eine Einheit ist. Dann haben wir unsere Zerlegung gefunden. Sei dazu c keine Einheit, also

$$cR \neq R.$$

Sei

$$\mathfrak{S}_1 = \{\mathbf{i} | \mathbf{i} \text{ Ideal }, cR \subseteq \mathbf{i} \subsetneq R\}.$$

Da $cR \in \mathfrak{S}_1$ ist, ist $\mathfrak{S}_1 \neq \varnothing$. Nach Lemma I.18 gibt es ein maximales Element $\mathbf{m}$ in $\mathfrak{S}_1$.

Es ist $\mathbf{m} = pR$, da R ein Hauptidealring ist. Da $\mathbf{m}$ insbesondere ein maximales Ideal in R ist, ist nach Satz I.9 $R/\mathbf{m}$ ein Körper. Also ist $\mathbf{m}$ prim. Nach Lemma I.12 ist dann p irreduzibel. Da $cR \subseteq \mathbf{m}$ ist, ist $c = pd$ mit geeignetem d. Somit ist

$$cR \subseteq dR.$$

Es ist nun

$$a = dpp_1 \cdots p_k.$$

Somit ist auch $dR \in \mathfrak{S}_1$. Die Maximalität von cR liefert dann $cR = dR$. Also ist $d = rc$ mit geeignetem $r \in R$. Das liefert nun

$$c = dp = crp, \text{ also } rp = 1,$$

ein Widerspruch, da $pR \neq R$ war. Somit ist c eine Einheit. Ist nun a keine Einheit, so ist $k \geq 1$. Setze $\tilde{p}_1 = cp_1$. Dann ist $a = \tilde{p}_1 p_2 \cdots p_k$ mit irreduziblen $\tilde{p}_1, p_2, \ldots, p_k$. Damit ist die Existenz bewiesen.

Wir haben zusammenfassend:

Satz I.19 *Jeder Hauptidealring ist ein EPZ-Ring.*

Da jeder euklidische Ring ein Hauptidealring ist, ist dann auch jeder euklidische Ring ein EPZ-Ring. Somit sind $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$ alles EPZ-Ringe. Jetzt können wir auch zeigen, dass in einem EPZ-Ring die Begriffe prim und irreduzibel gleichwertig sind.

Lemma I.20 *Sei R ein EPZ-Ring. Ist $p \in R$, so ist p genau dann prim, wenn p irreduzibel ist.*

Beweis. Nach Satz I.2 haben wir nur zu zeigen, dass irreduzible Elemente prim sind. Seien also $a, b \in R$, so dass p ein Teiler von ab ist. Das heißt, $ab = pc$. Ist a eine Einheit, so gibt es ein d mit $ad = 1$. Also ist $b = dpc$ und p ein Teiler von b. Genauso ist p ein Teiler von a, falls b eine Einheit ist. Seien also a und b beide keine Einheiten. Dann ist $a = p_1 \cdots p_r$ und $b = q_1 \cdots q_s$ mit irreduziblen $p_1, \ldots, p_r, q_1, \ldots, q_s$. Somit ist $ab = p_1 \cdots p_r q_1 \cdots q_s = pc$. Wegen der Eindeutigkeit der Zerlegung ist $p = ep_i$ oder $p = eq_i$ für eine Einheit e und geeignetes i, d.h. $p|a$ oder $p|b$. □

Bemerkung. Sei $m \in \mathbb{Z}$, m kein Quadrat. Wir setzen

$$M_m = \{a + b\sqrt{m} | a, b \in \mathbb{Q}\}.$$

Man kann zeigen, dass M_m ein Körper ist. Wir betrachten in M_m nun die Teilmenge

$$R_m = \{u | u \in M_m, u \text{ ist Nullstelle eines Polynoms } x^2 + cx + d,\ c, d \in \mathbb{Z}\}.$$

Dann ist R_m ein Integritätsbereich. Wir können R_m auch wie folgt beschreiben:

$$\begin{aligned} R_m &= \{r + s\sqrt{m} | r, s \in \mathbb{Z}\}, \text{ falls } m \equiv 2, 3 \pmod 4 \text{ ist.} \\ R_m &= \{(r + s\sqrt{m})/2 | r, s \in \mathbb{Z},\ r \equiv s \pmod 2\} \text{ sonst.} \end{aligned}$$

In dieser Sprache ist $\mathbb{Z}[i] = R_{-1}$.

Wie in $\mathbb{Z}[i]$ können wir in R_m auch eine Norm einführen. Sei $u = a + b\sqrt{m}$, so setze

$$N(u) = a^2 - mb^2 = (a + b\sqrt{m})(a - b\sqrt{m}).$$

Ist $m < 0$ und $m \neq -1, -2, -3, -7, -11$, so ist R_m kein euklidischer Ring. Für die restlichen Werte $m < 0$ ist R_m euklidisch mit $\varphi(r) = N(r)$. Der Beweis ist ähnlich wie bei $\mathbb{Z}[i]$.

Für R_{-5} hatten wir gezeigt, dass 3 irreduzibel, aber nicht prim ist, somit ist R_{-5} nach Lemma I.20 kein EPZ-Ring.

Man kann zeigen, dass R_{-19} ein Hauptidealring ist. Also ist nicht jeder Hauptidealring euklidisch.

Harold Stark (1967, [29]) hat bewiesen, dass für $m < 0$ R_m genau dann ein EPZ-Ring ist, falls

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

ist. Ist $m > 0$, so ist R_m euklidisch mit $\varphi(r) = |N(r)|$ genau für

$$m = 2, 3, 5, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Dies stammt im Wesentlichen von Harold Chatland und Harold Davenport (1990, [6]). Es ist eine offene Frage, für welche $m > 0$ R_m ein EPZ-Ring ist.

Ob $\mathbb{Z}[x]$ ein EPZ-Ring ist, können wir derzeit nicht klären, da, wie wir wissen, $\mathbb{Z}[x]$ kein Hauptidealring ist (siehe Seite 14). Wir müssen dies auf andere Art entscheiden.

Es ist $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Der Ring $\mathbb{Q}[x]$ ist ein Hauptidealring und damit auch ein EPZ-Ring. Dies werden wir benutzen, um zu zeigen, dass $\mathbb{Z}[x]$ ein EPZ-Ring ist.

Wir wollen dies gleich etwas allgemeiner machen. Die Einbettung von $\mathbb{Z}[x]$ in $\mathbb{Q}[x]$ wollen wir für jeden Integritätsbereich R nachvollziehen, also $R[x] \subseteq K[x]$ für einen geeigneten Körper K. Dazu wollen wir zunächst die Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$ für beliebige Integritätsbereiche nachvollziehen.

Satz I.21

Sei R ein Integritätsbereich.

a) Es gibt einen Körper K und einen Monomorphismus

$$\alpha: R \to K,$$

so dass jedes Element aus K als $\alpha(r_1)\alpha(r_2)^{-1}$ mit geeigneten $r_1, r_2 \in R$, $r_2 \neq 0$, dargestellt werden kann.

b) Der Körper K ist durch die in a) angegebene Eigenschaft bis auf Isomorphie eindeutig bestimmt.

c) Ist $\tilde{K}$ ein Körper und $\psi: R \to \tilde{K}$ ein Monomorphismus, so kann ψ zu einem Monomorphismus $\tilde{\psi}: K \to \tilde{K}$ mit $\tilde{\psi}\alpha = \psi$ erweitert werden.

Beweis. a) Wir definieren zunächst auf $R \times (R \setminus \{0\})$ eine Äquivalenzrelation $\sim$ durch $(r_1, s_1) \sim (r_2, s_2)$ genau dann, wenn $r_1 s_2 = r_2 s_1$ ist. Dies ist wie $\frac{2}{5} = \frac{4}{10}$ in $\mathbb{Q}$.

Man sieht leicht ein, dass $\sim$ reflexiv und symmetrisch ist.

Für die Transitivität sei $(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3)$, also $r_1 s_2 = r_2 s_1$ und auch $r_2 s_3 = s_2 r_3$. Dann ist

$$r_1 s_2 s_3 = r_2 s_1 s_3 = r_2 s_3 s_1 = r_3 s_2 s_1.$$

Da $s_2 \neq 0$ ist, ist dann $r_1 s_3 = r_3 s_1$, also $(r_1, s_1) \sim (r_3, s_3)$. Somit ist $\sim$ transitiv.

Sei K die Menge der Äquivalenzklassen $\overline{(r, s)}$ von $\sim$, also

$$K = \{\overline{(r, s)} | (r, s) \in R \times (R \setminus \{0\})\}.$$

In $\mathbb{Q}$ ist offenbar $\frac{2}{5}$ die Menge aller Brüche mit Wert $\frac{2}{5}$, also genau die Äquivalenzklasse von $\frac{2}{5}$. Wir definieren auf K eine Addition und Multiplikation, die auch wieder von $\mathbb{Q}$ motiviert ist, wie folgt:

$$\begin{aligned} \overline{(r_1, s_1)} + \overline{(r_2, s_2)} &= \overline{(r_1 s_2 + r_2 s_1, s_1 s_2)} \\ \overline{(r_1, s_1)}\,\overline{(r_2, s_2)} &= \overline{(r_1 r_2, s_1 s_2)}. \end{aligned}$$

Wie man nachrechnet, wird hiermit K zu einem Körper. Es ist $\overline{(0, 1)}$ das Nullelement, $\overline{(1, 1)}$ das Einselement und $\overline{(r, s)}^{-1} = \overline{(s, r)}$.

Wir definieren nun

$$\alpha: R \to K$$

durch

$$\alpha(r) = \overline{(r, 1)}.$$

Dies ist wie die Identifikation von 5 mit $\frac{5}{1}$.

Es ist

$$\alpha(r_1 r_2) = \overline{(r_1 r_2, 1)} = \overline{(r_1, 1)}\,\overline{(r_2, 1)} = \alpha(r_1)\alpha(r_2)$$

und

$$\alpha(r_1 + r_2) = \overline{(r_1 + r_2, 1)} = \overline{(r_1, 1)} + \overline{(r_2, 1)} = \alpha(r_1) + \alpha(r_2).$$

Somit ist α ein Homomorphismus.

Sei $r \in \ker \alpha$. Dann ist

$$\overline{(0, 1)} = \alpha(r) = \overline{(r, 1)}.$$

Das liefert $(0, 1) \sim (r, 1)$, d.h. $r = r \cdot 1 = 1 \cdot 0 = 0$. Somit ist α ein Monomorphismus.

Sei nun $\overline{(r, s)} \in K$. Dann ist

$$\overline{(r, s)} = \overline{(r, 1)}\,\overline{(1, s)} = \overline{(r, 1)}\,\overline{(s, 1)}^{-1} = \alpha(r)\alpha(s)^{-1}.$$

Damit haben wir a).

b) Sei K' ein Körper, der a) mit zugehörigem Monomorphismus β erfüllt.

Sei $\varphi: K \to K'$ definiert durch

$$\varphi(\overline{(r, s)}) = \beta(r)\beta(s)^{-1}.$$

(1) φ ist wohldefiniert.

Sei dazu $(r_1, s_1) \sim (r, s)$, also $r_1 s = r s_1$. Somit ist $\beta(r_1 s) = \beta(r s_1)$, d.h.

$$\beta(r_1)\beta(s_1)^{-1} = \beta(r)\beta(s)^{-1}.$$

(2) φ ist Homomorphismus.

Dies kann man leicht nachrechnen.

Nach a) ist

$$K' = \{\beta(r)\beta(s)^{-1} | (r, s) \in R \times (R \setminus \{0\})\}.$$

Also ist φ ein Epimorphismus.

Nach Folgerung I.10 ist $\ker \varphi = 0$, da $\varphi(\overline{(1, r)}) = 1 \neq 0$ ist. Also ist φ ein Isomorphismus.

c) Definiere $\tilde{\psi}: K \to \tilde{K}$ durch

$$\tilde{\psi}(\alpha(r)\alpha(s)^{-1}) = \psi(r)\psi(s)^{-1}.$$

Wir zeigen zunächst, dass $\tilde{\psi}$ wohldefiniert ist. Sei dazu

$$\alpha(r)\alpha(s)^{-1} = \alpha(r_1)\alpha(s_1)^{-1}.$$

Dann ist

$$\alpha(r)\alpha(s_1) = \alpha(r_1)\alpha(s) \text{ also } \alpha(r s_1) = \alpha(r_1 s).$$

Da α ein Monomorphismus ist, erhalten wir nun $r s_1 = r_1 s$. Somit ist

$$\psi(r)\psi(s_1) = \psi(r s_1) = \psi(r_1 s) = \psi(r_1)\psi(s),$$

was $\psi(r)\psi(s)^{-1} = \psi(r_1)\psi(s_1)^{-1}$ liefert. Also ist $\tilde{\psi}$ wohldefiniert.

Man rechnet nach, dass $\tilde{\psi}$ ein Homomorphismus ist. Wegen

$$\psi(\alpha(1)\alpha(1)^{-1}) = \psi(1)\psi(1)^{-1} = 1 \neq 0$$

ist nach Folgerung I.10 $\tilde{\psi}$ ein Monomorphismus.

Sei nun $r \in R$. Dann erhalten wir

$$\tilde{\psi}(\alpha(r)(\alpha(1))^{-1}) = \psi(r)\psi(1)^{-1} = \psi(r).$$

Somit ist $\psi = \tilde{\psi}\alpha$. □

Definition

Quotientenkörper. Den in Satz I.21 konstruierten Körper nennen wir den *Quotientenkörper* zu R. Der Quotientenkörper zu $R[x]$ wird mit $R(x)$ bezeichnet.

Die Elemente aus K bezeichnen wir üblicherweise mit $\frac{a}{b}$, d.h., wir identifizieren a mit $\alpha(a)$.

Wir betrachten nun Polynomringe $R[x]$, wobei R ein EPZ-Ring ist. Für

$$0 \neq f = \sum_{i=0}^{n} a_i x^i$$

setze $\operatorname{cont}(f) = \operatorname{ggT}(a_0, \ldots, a_n)$. Wie bei der Definition des ggT bereits festgestellt, ist auch $\operatorname{cont}(f)$ nur bis auf Einheiten bestimmt.

Lemma I.22

Gaußsches[3] Lemma. *Sei R ein EPZ-Ring und $f, g \in R[x] \setminus \{0\}$. Dann ist*

$$\operatorname{cont}(f)\operatorname{cont}(g) = \operatorname{cont}(fg).$$

Beweis. Es sind $f = cf_1$ und $g = dg_1$ mit $c = \operatorname{cont}(f)$, $d = \operatorname{cont}(g)$ und $\operatorname{cont}(f_1) = \operatorname{cont}(g_1) = 1$. Also genügt es, die Behauptung für den Fall $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$ zu beweisen.

Sei

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j.$$

[3] Carl Friedrich Gauß (*30.4.1777 Braunschweig, †23.2.1855 Göttingen), Professor in Göttingen, wird als der größte Mathematiker der Neuzeit bezeichnet. In seiner Doktorarbeit bewies er den Fundamentalsatz der Algebra (Jedes nicht konstante Polynom mit komplexen Koeffizienten hat eine Nullstelle in den komplexen Zahlen), mit 19 Jahren bewies er die Konstruierbarkeit mit Zirkel und Lineal des regelmäßigen 17-Ecks, ein Problem, das bis auf Euklid zurückgeht. Mit 24 Jahren schrieb er die „Disquisitiones Arithmeticae", eines der bedeutendsten Werke der Mathematik. Hier wurden die Grundlagen der Zahlentheorie, die bis daher aus vereinzelten Problemen bestand, gelegt. Er arbeitete auf vielen verschiedenen Gebieten (Geometrie, Algebra, Astronomie, Physik) und führte grundlegende Begiffe ein, z.B. die Gaußsche Glockenkurve und die erste geometrische Interpretation der komplexen Zahlen mit der Gaußschen Zahlenebene.

Wir müssen cont $(fg) = 1$ zeigen. Sei dazu p ein beliebiges irreduzibles Element in R. Da p weder cont (f) noch cont (g) teilt, kann p nicht alle Koeffizienten von f und auch nicht alle Koeffizienten von g teilen. Wähle nun r maximal in $0 \leq r \leq n$ mit $p \nmid a_r$ und s maximal in $0 \leq s \leq m$ mit $p \nmid b_s$. Wir betrachten den Koeffizienten in fg von x^{r+s}, also

$$c_{r+s} = a_0 b_{r+s} + \cdots + a_{r+s} b_0.$$

Da p für $i \geq 1$ alle $a_{r+i} b_{s-i}$ und $b_{s+i} a_{r-i}$ teilt, aber p nicht $a_r b_s$ teilt, teilt p auch nicht den Koeffizienten c_{r+s}. Also folgt $p \nmid$ cont (fg). Somit ist cont $(fg) = 1$, da p beliebig war. □

Das nächste Lemma gibt uns Kontrolle über die irreduziblen Elemente von $R[x]$.

Lemma I.23

Sei R ein EPZ-Ring und K der Quotientenkörper von R. Sei weiter $f \in R[x]$ mit cont $(f) = 1$. *Es ist f in $K[x]$ genau dann irreduzibel, wenn f in $R[x]$ irreduzibel ist.*

Beweis. Sei zunächst f irreduzibel in $K[x]$. Ist $f = gh$ mit $g, h \in R[x]$, so können wir annehmen, dass g eine Einheit in $K[x]$ ist. Nach Satz I.4 ist dann grad $g = 0$, d.h. $g \in R$. Da cont $(f) = 1$ ist, ist $g|1$, d.h., g ist eine Einheit in $R[x]$.

Sei nun f irreduzibel in $R[x]$ und $f = gh$ mit $g, h \in K[x]$, also

$$g = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i, \quad h = \sum_{j=0}^{m} \frac{c_j}{d_j} x^j \text{ mit } a_i, b_i, c_j, d_j \in R.$$

Wir bezeichen mit

$$b = \prod_{i=0}^{n} b_i \text{ und } d = \prod_{j=0}^{m} d_j$$

die Hauptnenner. Damit erhalten wir $bg = g_0 \in R[x]$ und $dh = h_0 \in R[x]$.

Seien nun $\alpha =$ cont (g_0) und $\beta =$ cont (h_0), also $g_0 = \alpha g_1$ und $h_0 = \beta h_1$ mit $g_1, h_1 \in R[x]$ und cont $(g_1) =$ cont $(h_1) = 1$. Das liefert

$$\alpha\beta g_1 h_1 = g_0 h_0 = bdgh = bdf.$$

Es ist $\alpha\beta =$ cont $(g_0 h_0)$ und nach Lemma I.22 cont $(bdf) = bd$, da cont $(f) = 1$ ist. Also ist $\alpha\beta = bde$ mit einer Einheit $e \in R$. Das liefert nun

$$f = g_1 h_1 e.$$

Da f irreduzibel ist, können wir annehmen, dass g_1 eine Einheit in $R[x]$ ist. Dann ist g_1 auch eine Einheit in $K[x]$ und nach Satz I.4 ist somit $g_1 \in K$. Dann ist aber $g = b^{-1}\alpha g_1 \in K$, d.h., g ist Einheit. Also ist f irreduzibel in $K[x]$. □

Für den Spezialfall $\mathbb{Z}$ haben wir

Folgerung I.24

Ist $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ irreduzibel und ggT $(a_0, \ldots, a_n) = 1$, *so ist f irreduzibel in $\mathbb{Q}[x]$.*

Nun können wir die Frage, ob $\mathbb{Z}[x]$ ein EPZ-Ring ist, beantworten.

Satz I.25 *Ist R ein EPZ-Ring, so ist auch $R[x]$ ein EPZ-Ring.*

Beweis. Nach Satz I.19 ist $K[x]$ ein EPZ-Ring, wobei K der Quotientenkörper von R ist.

Jedes $0 \neq f \in R[x]$ ist eindeutig als ein Produkt

$$f = p_1 \cdots p_r$$

mit irreduziblen $p_i \in K[x]$ schreibbar.

Sei a_i das Produkt der Nenner der Koeffizienten von p_i und $f_i = a_i p_i$. Dann ist $f_i \in R[x]$. Es ist

$$f_i = c_i q_i, \ c_i \in R, q_i \in R[x], \text{cont}\,(q_i) = 1.$$

Somit ist

$$p_i = \frac{c_i}{a_i} q_i.$$

Es ist

$$\Big(\prod_{i=1}^{r} a_i\Big) f = \Big(\prod_{i=1}^{r} c_i\Big) q_1 \cdots q_r.$$

Sei zunächst $\text{cont}\,(f) = 1$. Lemma I.22 liefert

$$\prod_{i=1}^{r} a_i = \Big(\prod_{i=1}^{r} c_i\Big) e$$

mit einer Einheit $e \in R$. Dann haben wir

$$f = e q_1 \cdots q_r.$$

Die p_i sind in $K[x]$ irreduzibel. Damit sind auch die f_i und daraus folgend die q_i irreduzibel in $K[x]$. Nach Lemma I.23 sind die q_i auch in $R[x]$ irreduzibel. Indem wir $\tilde{q}_1 = e q_1$ setzen, haben wir die Existenz einer Zerlegung nachgewiesen.

Wir müssen noch die Eindeutigkeit zeigen. Sei also

$$f = r_1 \cdots r_k$$

mit irreduziblen Elementen $r_1, \ldots, r_k \in R[x]$. Nach Lemma I.22 ist $\text{cont}\,(r_i) = 1$, $i = 1, \ldots, k$, da $\text{cont}\,(f) = 1$ ist. Nach Lemma I.23 sind die r_i irreduzibel in $K[x]$. Da $K[x]$ ein EPZ-Ring ist, gilt $k = r$ und

$$r_i = e_i p_i$$

bei geeigneter Nummerierung, wobei die e_i Einheiten in $K[x]$ sind, also $e_i \in K$. Das liefert nun

$$a_i r_i = e_i c_i q_i.$$

Nach Lemma I.22 ist dann $a_i = e_i c_i \tilde{e}_i$ mit einer Einheit $\tilde{e}_i \in R$. Also ist

$$e_i c_i (\tilde{e}_i r_i - q_i) = 0.$$

Das liefert

$$\tilde{e}_i r_i = q_i.$$

Damit ist die Zerlegung eindeutig.

Wir haben also gezeigt, dass sich jedes $0 \neq f \in R[x]$ mit $\operatorname{cont}(f) = 1$ eindeutig als Produkt irreduzibler Elemente schreiben lässt.

Sei nun $\operatorname{cont}(f) = d$ beliebig. Dann ist $f = d\tilde{f}$ mit $\operatorname{cont}(\tilde{f}) = 1$. Es ist $\tilde{f}$ eindeutig darstellbar. Da $d \in R$ ist, ist $d = d_1 \cdots d_k$ eindeutig mit irreduziblen $d_i \in R$ darstellbar. Also ist f als Produkt irreduzibler Elemente darstellbar.

Sei nun $f = q_1 \cdots q_r$ mit irreduziblen $q_i \in R[x]$. Sei $c_i = \operatorname{cont}(q_i)$. Somit ist $q_i = c_i \tilde{q}_i$ mit $\operatorname{cont}(\tilde{q}_i) = 1$. Dann ist

$$d\tilde{f} = f = \Big(\prod_{i=1}^{r} c_i\Big) \tilde{q}_1 \cdots \tilde{q}_r.$$

Nach Lemma I.22 ist $d = e \prod_{i=1}^{r} c_i$ mit einer Einheit $e \in R$. Also ist

$$\tilde{f} = \tilde{e}\tilde{q}_1 \cdots \tilde{q}_r$$

mit einer Einheit $\tilde{e}$. Nun sind die $\tilde{q}_i$ eindeutig bestimmt. Da auch $d = e \prod_{i=1}^{r} c_i$ eindeutig bestimmt ist, folgt, dass

$$f = q_1 \ldots q_r$$

eindeutig ist. □

Folgerung I.26

a) Ist K ein Körper, so ist $K[x_1, \ldots, x_n]$ ein EPZ-Ring.

b) $\mathbb{Z}[x]$ ist ein EPZ-Ring.

Folgerung I.26 b) zeigt, dass es EPZ-Ringe gibt, die keine Hauptidealringe sind.

Schon in $\mathbb{Z}$ ist es schwierig zu entscheiden, ob eine Zahl prim ist. In $\mathbb{Z}[x]$ kann dies noch schwieriger sein. Wir wollen dazu einige Methoden angeben.

Satz I.27

Sei $f \in K[x]$, K ein Körper.

a) Ist $a \in K$ mit $f(a) = 0$, so ist $x - a | f$. Insbesondere haben irreduzible Polynome vom Grad größer als 1 keine Nullstellen in K.

b) f hat höchstens grad f *viele verschiedene Nullstellen.*

Beweis. Sei $f = \sum_{i=0}^{n} a_i x^i$. Wir ersetzen f durch $g = f(x+a) = \sum_{i=0}^{n} b_i x^i$. Dann hat g die Nullstelle 0. Also ist

$$0 = g(0) = b_0.$$

Somit ist

$$g = x \sum_{i=0}^{n-1} c_i x^i \text{ mit } c_i = b_{i+1}.$$

Nun betrachte $f = g(x-a) = (x-a)\sum_{i=0}^{n-1} d_i x^i$. Dies ist a).

Da grad $(\sum_{i=0}^{n-1} d_i x^i) <$ grad f ist, folgt b) mit einer Induktion nach grad f. □

Das wohl bekannteste Irreduzibilitätskriterium ist der folgende Satz von Eisenstein[4].

Satz I.28

Sei R ein EPZ-Ring mit Quotientenkörper K und

$$f = a_0 + a_1 x + \cdots + a_n x^n \in R[x].$$

Für ein irreduzibles Element $p \in R$ teile p alle a_i, $i = 0, \ldots, n-1$, aber nicht a_n. Weiter sei a_0 nicht durch p^2 teilbar. Dann ist f irreduzibel in $K[x]$.

Beweis. Nach Voraussetzung ist p kein Teiler von cont (f). Also können wir annehmen, dass cont $(f) = 1$ ist. Dann genügt es nach Lemma I.23 zu zeigen, dass f irreduzibel in $R[x]$ ist. Sei dazu

$$f = gh \text{ mit}$$

$$g = \sum_{i=0}^{r} b_i x^i \text{ und } h = \sum_{j=0}^{t} c_j x^j,\ r, t > 0,\ b_r \neq 0 \neq c_t.$$

Es ist zunächst

$$a_0 = b_0 c_0.$$

Nach Lemma I.20 ist p prim. Da a_0 von p geteilt wird, folgt nun, dass b_0 oder c_0 von p geteilt wird. Da a_0 nicht durch p^2 teilbar ist, können wir annehmen, dass b_0 aber nicht c_0 von p geteilt wird. Da cont $(f) = 1$ ist, ist nach Lemma I.22 cont $(g) = 1$, also ist p kein Teiler von cont (g).

Damit gibt es ein k, das minimal ist, so dass b_k nicht durch p geteilt wird. Es ist

$$a_k = b_k c_0 + \cdots + b_0 c_k.$$

Angenommen, es ist $k < n$. Da p alle b_i, $i < k$ teilt, aber nicht $b_k c_0$, ist p auch kein Teiler von a_k, ein Widerspruch zu $k < n$.

[4] Ferdinand Gotthold M. Eisenstein (*16.4.1823 Berlin, †11.10.1852 Berlin) studierte ab 1843 an der Berliner Universität und erhielt dort den Doktorgrad ehrenhalber nach der Veröffentlichung von über 25 Arbeiten. Er habilitierte 1847 an der Berliner Universität und wurde 1852 Mitglied der Berliner Akademie. Eisenstein arbeitete auf Gebieten der Zahlentheorie, der Algebra sowie der elliptischen und abelschen Funktionen. Er beschäftigte sich mit quadratischen, kubischen und biquadratischen Reziprozitätsgesetzen. Herausragend sind seine Arbeiten zu quadratischen und kubischen Formen. Hier entstehen auch die später nach ihm benannten Eisenstein-Reihen.

Also ist $k = n$ und dann $k = r = n$. Somit haben wir

$$\operatorname{grad} g = \operatorname{grad} f.$$

Das liefert $\operatorname{grad} h = 0$, ein Widerspruch zur Annahme $t > 0$. □

Wir wollen nun an einigen Beispielen aufzeigen, mit welchen Methoden man die Frage nach der Irreduzibilität eines Polynoms angehen kann.

Beispiel

a) Sei $f = \frac{2}{25}x^6 + \frac{7}{5}x^5 + x^3 + \frac{1}{5} \in \mathbb{Q}[x]$. Ist f irreduzibel?

Es ist

$$25f = 2x^6 + 35x^5 + 25x^3 + 5 \in \mathbb{Z}[x].$$

Mit Satz I.28 und $p = 5$ sehen wir, dass

$$2x^6 + 35x^5 + 25x^3 + 5$$

irreduzibel ist, also auch f.

b) Das nächste Beispiel ist von zentraler Bedeutung. Sei

$$f = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1, \, p \text{ Primzahl.}$$

Wir wollen zeigen, dass f irreduzibel ist. Satz I.28 ist nicht direkt anwendbar. Aber wir können den Trick aus dem Beweis von Satz I.27 verwenden.

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} x^{i-1} = x^{p-1} + pxh + p \text{ mit } h \in \mathbb{Z}[x].$$

Nun liefert Satz I.28, dass $f(x+1)$ irreduzibel ist. Aber jede Zerlegung von $f(x)$ hätte auch eine von $f(x+1)$ geliefert, also ist f irreduzibel.

c) Eine weitere Möglichkeit ist, nicht x zu verändern, sondern die Koeffizienten des Polynoms. Ähnlich verfahren Computeralgebra-Systeme beim Testen von Irreduzibilität.

Sei $\bar{}$ die Abbildung von $\mathbb{Z}$ auf $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$. Diese erweitern wir zu einer Abbildung von $\mathbb{Z}[x]$ nach $(\mathbb{Z}/n\mathbb{Z})[x]$ durch

$$f = \sum_{i=0}^{m} a_i x^i \longrightarrow \bar{f} = \sum_{i=0}^{m} \bar{a}_i x^i.$$

Ist $n = p$ eine Primzahl, so ist $K = \mathbb{Z}/p\mathbb{Z}$ ein Körper und wir haben, dass $K[x]$ ein EPZ-Ring ist.

Zerfällt $f = gh$ in $\mathbb{Z}[x]$, so auch $\bar{f} = \bar{g}\bar{h}$ in $K[x]$. Dies ist eine echte Zerlegung, falls $p \nmid a_m$.

Somit gilt: Ist $\bar{f}$ irreduzibel in $K[x]$, so ist f irreduzibel in $\mathbb{Z}[x]$.

Der Vorteil von $K[x]$ ist die Endlichkeit von K. Es gibt also nur endlich viele Polynome $\bar{g} \in K[x]$ mit $\operatorname{grad} \bar{g} < \operatorname{grad} \bar{f}$. Damit ist das Entscheidungsproblem ein endliches Problem geworden. Wir wollen dies an folgendem Beispiel illustrieren.

Sei

$$f = x^4 + 5x^3 + 35x^2 + 10x + 7 \in \mathbb{Z}[x].$$

Setze $p = 5$. Dann ist

$$\bar{f} = x^4 + \bar{2}.$$

Indem man $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ einsetzt, sieht man, dass $\bar{f}$ keine Nullstelle in $\mathbb{Z}/5\mathbb{Z}$ hat. Ist $\bar{f}$ reduzibel, so ist

$$\bar{f} = \bar{g}\bar{h} \text{ mit } \operatorname{grad} \bar{g} = \operatorname{grad} \bar{h} = 2$$

und damit $x^4 + \bar{2} = (x^2 + \bar{a}x + \bar{b})(x^2 + \bar{c}x + \bar{d})$. Das liefert die Gleichungen $\bar{a} = -\bar{c}$, $\bar{a}\bar{c} + \bar{b} + \bar{d} = 0$, $\bar{b}\bar{d} = 2$. Somit $\bar{b} + \bar{d} = \bar{a}^2$. Da $\bar{a}^2 \in \{\bar{0}, \bar{1}, \bar{4}\}$ ist, folgt nun

$$\bar{b}(1 - \bar{b}) = \bar{2} \text{ oder } \bar{b}(4 - \bar{b}) = \bar{2}.$$

Einsetzen der Werte für $\bar{b}$ liefert einen Widerspruch. Also ist $\bar{f}$ irreduzibel in $(\mathbb{Z}/5\mathbb{Z})[x]$ und dann auch f in $\mathbb{Z}[x]$.

Wir hätten aber auch $p = 3$ betrachten können. Dann hätten wir

$$\bar{f} = x^4 - x^3 - x^2 + x + \bar{1}$$

erhalten. Aber jetzt gilt

$$x^4 - x^3 - x^2 + x + \bar{1} = (x^2 + x - \bar{1})^2.$$

Dies zeigt, dass $\bar{f}$ durchaus nicht irreduzibel sein muss, selbst wenn f irreduzibel ist. Man muss also bei der Verwendung von p etwas vorsichtig sein. Dazu später mehr. Zusammenfassend haben wir das folgende Verfahren zum Test der Irreduzibilität für $f \in \mathbb{Z}[x]$:

Sei $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$.

(1) Wir testen, ob f eine Nullstelle in $\mathbb{Z}$ hat:

Sei $f(a) = 0$. Dann ist $0 = \sum_{i=0}^{n} a_i a^i = a_0 + a \sum_{i=1}^{n} a_i a^{i-1}$. Also ist $a | a_0$.

Da a_0 nur endlich viele Teiler hat, ist dies ein endliches Problem.

(2) Wir testen, ob f quadratfrei ist:

Es ist $f' = \sum_{i=0}^{n} i a_i x^{i-1}$. Sei $f = g^2 h$. Dann ist $f' = 2gg'h + g^2 h'$.

Also ist $g | \mathrm{ggT}(f, f')$. Wir bestimmen mit dem euklidischen Algorithmus den $\mathrm{ggT}(f, f')$. Ist dieser ungleich 1, so ist f nicht irreduzibel.

(3) Wir faktorisieren in $(\mathbb{Z}/p\mathbb{Z})[x]$. Ist $\bar{f}$ irreduzibel, so ist f irreduzibel.

Das Problem liegt im Schritt (3). Es ist z.B. $x^4 - x^2 + 1$ irreduzibel in $\mathbb{Z}[x]$, aber niemals irreduzibel in $(\mathbb{Z}/p\mathbb{Z})[x]$. Ein Beispiel, das für unendlich viele Primzahlen irreduzibel und auch für unendlich viele reduzibel ist, werden wir auf Seite 127 sehen.

Angenommen, wir haben eine Primzahl p, so dass die Koeffizienten aller Teiler von f dem Betrag nach kleiner als $p/2$ sind. Ist dann $f = f_1 \cdots f_r$, so ist auch $\bar{f} = f_1 \cdots f_r$, da sich die Polynome nicht verändern. Ist nun $\bar{f} = g_1 \cdots g_t$ die Primfaktorzerlegung, so kann dies nur so gehen, dass die f_i Produkte einiger der g_j sind.

Insofern testen wir, ob die Produkte der g_j das Polynom f in $\mathbb{Z}[x]$ teilen. Das ist allerdings ein exponentieller Algorithmus.

Sei $f = x^4 - x^2 + 1$ und $p = 29$. Modulo 29 ist

$$\bar{f} = (x^2 + 12x - 1)(x^2 - 12x - 1).$$

Aber weder $x^2 + 12x - 1$ noch $x^2 - 12x - 1$ teilen f in $\mathbb{Z}[x]$, somit ist f irreduzibel.

Die Frage ist, woher wir p kennen, warum war $p = 29$ ausreichend? In der Tat gibt es solche Schranken. Es gilt die folgende Abschätzung (Landau-Mignotte-Ungleichung [16,19,20]).

Ist $g = \sum_{j=0}^{m} b_j x^j$ ein Teiler von $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0 \neq b_m$, so gilt

$$\sum_{j=0}^{m} |b_j| \leq 2^m \left| \frac{a_n}{b_m} \right| \sqrt{\sum_{i=0}^{n} a_i^2}.$$

In obigem Beispiel haben wir $|a_n| = 1 = |b_m|$. Also ist die Schranke

$$2^4 \sqrt{3} < 29.$$

Übungsaufgaben

I.1 Sei $(R, +, \cdot)$ ein Ring. Wir führen auf R zwei neue Verknüpfungen $\oplus$ und $\odot$ ein. Diese seien für $a, b \in R$ wie folgt definiert:

$$\begin{aligned} a \oplus b &= a + b - 1 \\ a \odot b &= a + b - a \cdot b. \end{aligned}$$

Zeige, dass auch $(R, \oplus, \odot)$ ein Ring ist, der sogar zu $(R, +, \cdot)$ isomorph ist.

I.2 Seien R ein Ring und $a, b \in R$ mit $a^2 = a, b^2 = b$ und $ab = ba$.

a) Es ist $(a - b)^4 = (a - b)^2$.

b) Ist $(a - b)^n = 0$ für ein $n \in \mathbb{N}$, so ist $a = b$.

c) Finde solche Elemente a, b mit $a \neq b$ in $R = \mathbb{R}_2$, dem Ring der 2×2–Matrizen über $\mathbb{R}$, beide nicht das Nullelement oder Einselement.

I.3 Sei R ein Integritätsbereich. Ist $2 \leq |R| < \infty$, so ist R ein Körper.

I.4 Sei p eine Primzahl und $\mathbb{Z}_p = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \text{ teilt nicht } b\}$.

a) Bestimme die Einheiten und Primelemente von $\mathbb{Z}_p$.

b) Ist $\mathbb{Z}_p$ ein euklidischer Ring?

I.5 Bestimme alle $q, r \in \mathbb{Z}[i]$ mit $1 + 25i = q(3 + 4i) + r$ und $|r| < |3 + 4i|$.

I.6 Zeige, dass $\mathbb{Z}[i]/3\mathbb{Z}[i] = K$ ein Körper ist. Bestimme $|K|$.

I.7 Bestimme die Primideale von $\mathbb{Z}/18\mathbb{Z}$.

I.8 Sei R ein kommutativer Ring, $\mathbf{i} \subseteq R$ ein Ideal und $S \subseteq R$ mit $\{s_1 s_2 \mid s_1, s_2 \in S\} \subseteq S$, so dass $S \cap \mathbf{i} = \varnothing$ ist. Setze

$$\mathcal{P} = \{\mathbf{p} \mid \mathbf{p} \text{ ist Ideal in } R \text{ mit } \mathbf{i} \subseteq \mathbf{p} \text{ und } \mathbf{p} \cap S = \varnothing\}.$$

a) Zeige mit dem Zornschen Lemma, dass $\mathcal{P}$ maximale Elemente bezüglich der Inklusion hat.

b) Zeige, dass maximale Elemente in $\mathcal{P}$ Primideale sind.

I.9 Finde ganze Zahlen x, y mit:

a) $754x + 221y = 13$.

b) $158x + 57y = 20000$.

I.10 Seien $f = x^3 + 2x^2 - x - 1$ und $g = x^2 + x - 3 \in \mathbb{Q}[x]$. Zeige:

a) f und g haben in $\mathbb{C}$ keine gemeinsamen Nullstellen.

b) Es gibt $a, b \in \mathbb{Q}[x]$ mit $af + bg = 1$.

c) Gib a und b aus b) explizit an.

I.11 Bestimme die Primfaktorzerlegung von $x^5 + x^3 + 2x^2 - x + 2$ in $\mathbb{Z}[x]$.

I.12 Betrachte das Polynom $x^q + 1 \in \mathbb{Z}[x]$ mit $q \in \mathbb{N}$. Zeige, dass $x^q + 1$ genau dann irreduzibel ist, falls $q = 2^m$ eine 2-Potenz ist.

I.13 Sei K ein Körper und $\varphi: K[x] \to K[x]$ ein Automorphismus. Ist $p \in K[x]$ ein Polynom, so ist p genau dann irreduzibel, wenn $\varphi(p)$ irreduzibel ist.

I.14 a) Seien $f, g \in K[x]$, K Körper, Polynome vom Grad $n > 0$. Gibt es $n+1$ paarweise verschiedene Elemente $a_1, \ldots, a_{n+1}$ in K mit

$$f(a_i) = g(a_i),\ i = 1, \ldots, n+1,$$

so ist $f = g$.

b) Bestimme alle Polynome $p \in \mathbb{Z}[x]$, die die Identität

$$p(x^2+1) = p(x)^2 + 1$$

für alle $x \in \mathbb{Z}$ erfüllen und für die $p(0) = 0$ gilt.

I.15 Sei f ein Polynom mit ganzzahligen Koeffizienten. Für vier paarweise verschiedene ganze Zahlen a, b, c, d sei

$$f(a) = f(b) = f(c) = f(d) = 7.$$

Zeige, dass es keine ganze Zahl k gibt, so dass $f(k) = 10$ ist.

I.16 Sei $p = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Zeige:

a) Ist $s \in \mathbb{Q}$ eine Nullstelle von p, so ist $s \in \mathbb{Z}$.

b) Ist $s \in \mathbb{Z}$ eine Nullstelle von p, so wird a_0 durch s geteilt.

c) Besitzt $x^{37} + 12x^{15} + x + 1$ rationale Nullstellen?

II Körper

Wir wollen uns jetzt mit Körpern beschäftigen, nachdem in Kapitel I Ringe und ihre Arithmetik mehr im Vordergrund standen.

Wir kennen bisher $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ und $\mathbb{Z}/p\mathbb{Z} = GF(p)$. Wir kennen aber sogar beliebig viele weitere. Ist nämlich $\mathbf{i}$ ein maximales Ideal in $K[x]$, K Körper, so ist $K[x]/\mathbf{i}$ nach Satz I.15 ein Körper. Ist f ein irreduzibles Polynom, so ist wieder nach Satz I.15 $\mathbf{i} = fK[x]$ ein maximales Ideal. Also gehört zu jedem irreduziblen Polynom ein Körper.

Den ersten Unterschied zwischen $\mathbb{Q}$ und $GF(p)$ sehen wir, wenn wir die 1 aufaddieren. In $GF(p)$ erhalten wir, wenn wir dies p-mal fortsetzen, die 0. In $\mathbb{Q}$ können wir dies beliebig oft fortsetzen und werden niemals die Null erhalten. Das führt zu folgender Definition:

Definition

Charakteristik. Sei K ein Körper. Die kleinste natürliche Zahl n mit $\underbrace{1 + \ldots + 1}_{n-mal} = 0$ nennen wir die *Charakteristik* von K. Schreibe dann $\operatorname{char} K = n$. Gibt es keine solche Zahl, so schreibe $\operatorname{char} K = 0$.

Also ist $\operatorname{char} \mathbb{Q} = 0$ und $0 < \operatorname{char} GF(p) \leq p$.

Lemma II.1

Ist K ein Körper mit $\operatorname{char} K \neq 0$, so ist $\operatorname{char} K = p$ eine Primzahl.

Beweis. Sei $\operatorname{char} K = n \neq 0$ und $n = pq$ mit einer Primzahl p. Dann ist

$$0 = n \cdot 1 = \underbrace{1 + \cdots + 1}_{n-mal} = \underbrace{(1 + \cdots + 1)}_{p-mal}\underbrace{(1 + \cdots + 1)}_{q-mal} = (p \cdot 1)(q \cdot 1).$$

Dann ist aber $(p \cdot 1) = 0$ oder $(q \cdot 1) = 0$. Die minimale Wahl von n liefert nun $n = p$. □

Definition

Primkörper, Teilkörper. Sei K ein Körper und k eine Teilmenge von K. Ist k mit der Einschränkung von Multiplikation und Addition von K wieder ein Körper, so nennen wir k einen *Teilkörper* von K. Den Durchschnitt aller Teilkörper von K nennen wir den *Primkörper* von K.

Der Primkörper ist somit der kleinste in einem Körper enthaltene Körper. Der nächste Satz sagt uns, dass wir alle Primkörper bereits kennen.

Satz II.2

Sei K ein Körper.

a) Ist char $K = 0$, *so ist der Primkörper zu $\mathbb{Q}$ isomorph.*

b) Ist char $K = p \neq 0$, *so ist der Primkörper zu $GF(p)$ isomorph.*

Beweis. Wir wollen mit k den Primkörper von K bezeichnen.

a) Sei $\psi\colon \mathbb{N} \to k$ mit $\psi(n) = n \cdot 1 = \underbrace{(1 + \cdots + 1)}_{n-mal}$. Sei $\psi(n) = \psi(m)$ für $n, m \in \mathbb{N}$. Wir können $n \geq m$ annehmen. Dann ist $0 = n \cdot 1 - m \cdot 1 = (n - m) \cdot 1$. Da char $K = 0$ ist, ist dann $n = m$. Also ist ψ eine injektive Abbildung. Somit ist ohne Einschränkung $\mathbb{N} \subseteq k$. Da k ein Körper ist, ist nun auch $\mathbb{Z} \subseteq k$. Nach Satz I.21c) enthält k einen zu $\mathbb{Q}$ isomorphen Teilkörper, also ist $k \cong \mathbb{Q}$.

b) Sei nun die Charakteristik von K endlich. Setze $K_1 = \{0, 1, \ldots, p-1\} \subseteq k$, wobei hier i für $\underbrace{1 + \cdots + 1}_{i-mal}$ steht. Sei $i = j$ in K_1 mit $0 \leq i \leq j \leq p - 1$. Dann ist $j - i = 0$. Da char $K = p$ ist, ist dann $j = i$ in $\mathbb{Z}$. Also ist $|K_1| = p$.
Sei nun $0 \neq x \in K_1$. Dann ist ggT $(x, p) = 1$ in $\mathbb{Z}$. Nach Satz I.16 gibt es $a, b \in \mathbb{Z}$ mit

$$ax + bp = 1.$$

Sei $a = \tilde{a} + kp$ mit $0 \leq \tilde{a} \leq p - 1$. Dann ist $1 = \tilde{a}x + (b + kx)p$. Also können wir $a \in K_1$ annehmen. Da $bp = 0$ in K ist, folgt $ax = 1$ und K_1 ist ein Körper, da K_1 gegen Addition ohnehin abgeschlossen war. Nach Definition von k ist $K_1 = k$.
Sei nun

$$\tau\colon GF(p) \to k \text{ mit } \tau(i + p\mathbb{Z}) = i.$$

Dann ist τ ein Isomorphismus. Also ist $k \cong GF(p)$. □

Das Potenzieren mit p in einem Körper der Charakteristik p gestaltet sich besonders einfach.

Lemma II.3

Ist char $K = p \neq 0$, *und sind $a, b \in K$, so ist*

$$(a + b)^p = a^p + b^p.$$

Beweis. Es ist $(a + b)^p = \sum_{i=0}^{p} a^i b^{p-i} \binom{p}{i}$. Hierbei bedeutet $\binom{p}{i}$, dass die Eins aus K genau $\binom{p}{i}$-mal aufaddiert wird. Ist $1 \leq i < p$, so ist $p | \binom{p}{i}$ also ist $\binom{p}{i} = 0$ in K und dann

$$(a + b)^p = b^p + a^p.$$

□

Wir hatten $GF(p)$ als $\mathbb{Z}/p\mathbb{Z}$ konstruiert. Sei nun k ein Körper und $f = \sum_{i=0}^{n} a_i x^i$ ein Polynom in $k[x]$ mit $a_n \neq 0$. Genauso konstruieren wir nun auch

$$K = k[x]/fk[x].$$

Ist f irreduzibel, so ist K nach Satz I.15 ein Körper. Es ist

$$K = \{g + fk[x] | g \in k[x]\}.$$

Da wir in $k[x]$ eine Division mit Rest haben, ist $g = fq + r$, grad $r <$ grad f. Dann ist

$$g + fk[x] = r + fk[x].$$

Somit ist

$$K = \{g + fk[x] | g \in k[x], \text{grad}\, g < \text{grad}\, f\}.$$

Als k-Vektorraum wird K von $\{x^i + fk[x] | 0 \leq i \leq n-1\}$ erzeugt.

Sei $\sum_{i=0}^{n-1} b_i(x^i + fk[x]) = fk[x]$ für geeignete $b_i \in k$. Dann ist $\sum_{i=0}^{n-1} b_i x^i \in fk[x]$, d.h.

$$f \Big| \sum_{i=0}^{n-1} b_i x^i.$$

Aber grad $f = n$ und damit ist $\sum_{i=0}^{n-1} b_i x^i = 0$ nach Lemma I.3, was $b_i = 0$ für alle i liefert. Somit bilden die $x^i + fk[x]$, $i = 0, \ldots, n-1$, eine Basis. Also ist $\dim_k K = n$.

Wenn wir k mit $\{b(1 + fk[x]) | b \in k\}$ identifizieren, können wir $k \subseteq K$ annehmen. Dann können wir f als Polynom in $K[y]$ betrachten. Dabei werden die a_i mit $a_i + fk[x]$ identifiziert. Also

$$f = \sum_{i=0}^{n} (a_i + fk[x]) y^i.$$

(Beachte, die „Variable“ x hat keine besondere Bedeutung.)

In dieses Polynom können wir nun $x + fk[x] \in K$ einsetzen. Das ergibt

$$f(x + fk[x]) = \sum_{i=0}^{n} (a_i + fk[x])(x + fk[x])^i$$

$$= \sum_{i=0}^{b} a_i x^i + fk[x] = f + fk[x] = fk[x] = 0.$$

Also ist $x + fk[x]$ eine Nullstelle von f in K. Insbesondere ist f in $K[y]$ nicht irreduzibel. Dies ist für das Folgende eine ganz wichtige Feststellung.

Sei z.B. $\mathbb{Q}$ gegeben. Wir suchen einen Körper K mit $\mathbb{Q} \subseteq K$, der $\sqrt{2}$ enthält. Angenommen, wir kennen weder $\mathbb{R}$ noch $\mathbb{C}$, sondern nur $\mathbb{Q}$. Wir können $\sqrt{2}$ allein aus $\mathbb{Q}$ heraus als Nullstelle von $x^2 - 2$ definieren. Dann ist

$$K = \mathbb{Q}[x]/(x^2 - 2)\mathbb{Q}[x]$$

der gesuchte Körper. Diese Konstruktion, die nicht die Existenz irgendwelcher Oberkörper voraussetzt, wird im Folgenden noch eine wichtige Rolle spielen.

Definition

Körpererweiterung. Sei K ein Körper. Ist k ein Teilkörper von K, so nennen wir K eine *Körpererweiterung* von k.

Definition

Algebraisch. Seien k und K Körper, K eine Körpererweiterung von k.

a) Setze $[K:k] = \dim_k K$. Wir nennen $[K:k]$ den Grad von K über k.

b) Ist $a \in K$ und gibt es ein $f \in k[x], f \neq 0$ mit $f(a) = 0$, so nennen wir a *algebraisch* über k. Ansonsten nennen wir a *transzendent*. Ist jedes Element aus K algebraisch über k, so nennen wir die Erweiterung $k \subseteq K$ algebraisch.

c) Ist U eine Teilmenge von K, so bezeichnen wir mit $k(U)$ den Durchschnitt aller Unterkörper von K, die U enthalten. Statt $k(\{x_1, \ldots, x_n\})$ schreiben wir auch $k(x_1, \ldots, x_n)$.

d) Gibt es $\{x_1, \ldots, x_n\} \subseteq K$ mit $K = k(x_1, \ldots, x_n)$, so nennen wir die Erweiterung endlich erzeugt. Einen Körper K nennen wir endlich erzeugt, wenn er über seinem Primkörper endlich erzeugt ist.

Es ergeben sich nun gleich einige Fragen. Wie erkennen wir, dass $k \subseteq K$ algebraisch ist? Folgt aus u, v beide algebraisch über k, dass auch $u + v$ oder uv algebraisch sind? Um diese Fragen beantworten zu können, müssen wir aber zunächst algebraische Körpererweiterungen näher studieren.

Der nächste Satz gibt ein gutes Kriterium dafür, dass gewisse Körpererweiterungen algebraisch sind.

Satz II.4

Sei $k \subseteq K$ eine Körpererweiterung mit $[K:k] < \infty$. Dann ist die Erweiterung algebraisch.

Beweis. Setze $[K:k] = n$. Wähle $a \in K$. Wir wollen zeigen, dass a Nullstelle eines Polynoms $p \in k[x]$ mit $p \neq 0$ ist. Da K ein k-Vektorraum der Dimension n ist, sind $1, a, a^2, \ldots, a^n$ linear abhängig. Also gibt es geeignete $a_i \in k$ nicht alle gleich Null, so dass gilt:

$$\sum_{i=0}^{n} a_i a^i = 0.$$

Setze nun

$$p = \sum_{i=0}^{n} a_i x^i \in k[x].$$

Dann ist $p \neq 0$ und $p(a) = 0$. Somit ist a algebraisch über k. □

Der nächste Satz beschreibt die Struktur von Körpern der Form $k(a)$.

Satz II.5

Seien k, K Körper mit $K = k(a)$ für ein $a \in K$. Ist a transzendent über k, so ist K zu dem Quotientenkörper $k(x)$ des Polynomrings $k[x]$ isomorph. Weiter ist $[K:k] = \infty$.

Ist a algebraisch über k, so existiert ein eindeutig bestimmtes normiertes irreduzibles Polynom $m_a \in k[x]$, das a als Nullstelle hat. Es ist $[K:k] = \operatorname{grad} m_a$ und

$$K \cong k[x]/m_a k[x].$$

Beweis. Wir betrachten den Einsetzungungshomomorphismus $\sigma: k[x] \to K$ mit

$$\sigma(p) = p(a), \text{ für } p \in k[x].$$

Setze $M = \text{Bild } \sigma$. Es ist $M = \{\sum_{i=0}^{n} a_i a^i | a_i \in k, n \in \mathbb{N} \cup \{0\}\}$. Offenbar ist M ein Ring. Da M in K enthalten ist, ist M ein Integritätsbereich.

Ist $p \in \ker \sigma$, so ist $0 = \sigma(p) = p(a)$.

Ist a transzendent, so folgt $p = 0$, d.h., σ ist ein Monomorphismus. Dann ist $k[x] \cong M$. Nach Satz I.21 enthält $k(a) = K$ einen Quotientenkörper von M, der dann zu dem Quotientenkörper von $k[x]$ also $k(x)$ isomorph ist. Da $a \in M$, und $k(a)$ minimal mit $a \in k(a)$ ist, folgt $k(a)$ ist der Quotientenkörper, d.h. $k(x) \cong k(a)$.

Sei nun a algebraisch über k. Dann gibt es ein Polynom $p \in k[x]$, $p \neq 0$ und $p(a) = 0$. Also ist $\ker \sigma \neq \{0\}$. Es ist $\ker \sigma$ ein Ideal nach Lemma I.7. Nach Satz I.4 und Satz I.14 gibt es ein $m_a \in k[x]$ mit $\ker \sigma = m_a k[x]$. Wir können m_a normiert wählen. Dann ist m_a eindeutig bestimmt. Da $\sigma \neq 0$ ist, ist $m_a k[x] \neq k[x]$, also ist m_a keine Einheit. Es ist $k[x]/m_a k[x] \cong M$, d.h. $k[x]/m_a k[x]$ ist ein Integritätsbereich. Nach Lemma I.12 ist dann m_a irreduzibel. Das liefert mit Satz I.15, dass M ein Körper ist. Somit ist $M = k(a)$. Die Behauptung $[k(a):k] = \operatorname{grad} m_a$ hatten wir bereits gezeigt. □

Minimalpolynom. Seien k, K Körper, K eine Körpererweiterung von k und $a \in K$ algebraisch über k. Das Polynom m_a aus Satz II.5 nennen wir das *Minimalpolynom* von a. — Definition

Bemerkung. Seien k, K Körper mit $k \subseteq K$. Dann ist K ein k-Vektorraum. Angenommen, es ist $K = k(a)$ mit algebraischem a. Wir betrachten die lineare Abbildung

$$\alpha_a: v \to av, v \in K.$$

Dann ist m_a das Minimalpolynom von α_a im Sinne der linearen Algebra.

Ein überaus wichtiger Satz, der bei der Beantwortung unserer Fragen eine fundamentale Rolle spielen wird, ist der folgende:

Gradsatz. *Seien k, K, L Körper, K eine Körpererweiterung von k und L eine Körpererweiterung von K. Dann gilt* — Satz II.6

$$[L:k] = [L:K][K:k].$$

Beweis. Sei $\{x_i | i \in I\}$ eine Basis von K als k-Vektorraum, $\{y_j | j \in J\}$ eine Basis von L als K-Vektorraum. Wir zeigen, dass

$$B = \{x_i y_j | i \in I, j \in J\}$$

eine Basis von L als k-Vektorraum ist. Dann folgt die Behauptung. Zunächst zeigen wir die lineare Unabhängigkeit über k. Sei dazu

$$\sum_{\substack{i \in I \\ j \in J}} a_{ij}(x_i y_j) = 0, \text{ mit } a_{ij} \in k, \text{ wobei nur endlich viele der } a_{ij} \text{ ungleich Null sind.}$$

Wir schreiben dies um als

$$\sum_{j \in J} \left\{ \sum_{i \in I} a_{ij} x_i \right\} y_j = 0.$$

Die $\sum_{i \in I} a_{ij} x_i$ sind Elemente in K. Da die y_j über K linear unabhängig sind, erhalten wir somit, dass

$$\sum_{i \in I} a_{ij} x_i = 0 \quad \text{für alle } j \text{ ist.}$$

Die lineare Unabhängigkeit der x_i liefert dann

$$a_{ij} = 0 \quad \text{für alle } i \text{ und } j.$$

Nun zeigen wir, dass B den Körper L als k-Vektorraum erzeugt. Sei dazu $a \in L$. Dann gibt es $\lambda_j \in K$ mit

$$a = \sum_{j \in J} \lambda_j y_j.$$

Weiter gibt es $\lambda_{ij} \in k$ mit

$$\lambda_j = \sum_{i \in I} \lambda_{ij} x_i.$$

Damit erhalten wir

$$a = \sum_{\substack{i \in I \\ j \in J}} \lambda_{ij} x_i y_j.$$

□

Wie wir in Satz II.4 gesehen haben, sind endliche Körpererweiterungen algebraisch. Wir wollen nun zeigen, dass für endlich erzeugte algebraische Erweiterungen die Umkehrung gilt.

Satz II.7

Sei $K = k(a_1, \ldots, a_n)$ eine endlich erzeugte Körpererweiterung. Dann sind gleichwertig

a) Die Elemente a_i, $i = 1, \ldots, n$, sind algebraisch über k.

b) Der Körpergrad $[K : k]$ ist endlich.

c) Die Erweiterung $k \subseteq K$ ist algebraisch.

Beweis.

a) $\Rightarrow$ b): Wir beweisen die Behauptung durch Induktion nach n.

Für $n = 1$ ist dies die Aussage von Satz II.5.

Sei $n > 1$. Wir haben $K = k(a_1, \ldots, a_{n-1})(a_n)$. Weiter ist nach Satz II.6

$$[K\colon k] \quad = \quad [k(a_1, \ldots, a_{n-1})(a_n)\colon k(a_1, \ldots, a_{n-1})][k(a_1, \ldots, a_{n-1})\colon k].$$

Per Induktion ist $[k(a_1, \ldots, a_{n-1})\colon k]$ endlich. Da a_n algebraisch über k ist, gibt es ein $p \in k[x], p \neq 0$, mit $p(a_n) = 0$. Es ist

$$k[x] \subseteq k(a_1, \ldots, a_{n-1})[x],$$

also ist a_n auch algebraisch über $k(a_1, \ldots, a_{n-1})$. Damit ist

$$[k(a_1, \ldots, a_{n-1})(a_n)\colon k(a_1, \ldots, a_{n-1})] \text{ endlich.}$$

Somit ist $[K\colon k] < \infty$.

b) $\Rightarrow$ c): Dies ist die Aussage von Satz II.4.

c) $\Rightarrow$ a): Per Definition sind alle Elemente in K algebraisch über k. □

Damit haben wir auch gezeigt, dass aus $a, b \in K$, a, b algebraisch über k, stets $a + b$ und $a \cdot b$ algebraisch über k folgt, denn nach Satz II.7 ist $k(a, b)$ algebraisch über k und es sind $a + b$ und ab in $k(a, b)$. Das Kernargument war die endliche Dimension der Körpererweiterung. Wir haben nicht versucht, aus den Polynomen für a und b eines für $a + b$ zu konstruieren. Beachte, dass wir mit Hilfe von Satz II.5 $k(a, b)$ direkt aus k konstruieren können.

Wir wollen nun noch Satz II.7 etwas verallgemeinern, indem wir Körper betrachten, die von beliebigen Mengen algebraischer Elemente erzeugt werden.

Definition

Algebraisch erzeugt. Seien k, K Körper mit $k \subseteq K$ und M eine Teilmenge von über k algebraischen Elementen von K. Ist $K = k(M)$ so nennen wir K *algebraisch erzeugt* über k.

Satz II.8

Seien k, K Körper, K eine Körpererweiterung von k. Ist K algebraisch erzeugt über k, so ist die Erweiterung $k \subseteq K$ algebraisch.

Beweis. Sei M die Menge aller über k algebraischen Elemente von K. Dann ist $k(M) = K$. Also ist K Quotientenkörper des Ringes

$$R = \{\sum_{j=1}^{m} a_j \prod_{i=1}^{n_j} m_i | m, n_j \in \mathbb{N} \cup \{0\}, m_i \in M, a_j \in k\}.$$

Es ist jedes Element $u \in K$ von der Gestalt ab^{-1}, $a, b \in R$. In der Darstellung von a und der von b kommen nur endlich viele Elemente aus M vor. Diese fassen wir zu M_u zusammen. Dann ist $u \in k(M_u)$, $|M_u| < \infty$, $M_u \subseteq M$. Nach Satz II.7 ist dann u algebraisch über k. □

Folgerung II.9 *Sei $\mathbb{A}$ die Menge der über $\mathbb{Q}$ algebraischen Zahlen in $\mathbb{C}$. Dann ist $\mathbb{A}$ ein Körper.*

Es ist $\mathbb{Q}$ abzählbar und damit auch $\mathbb{Q}[x]$. Da jedes Polynom nur endlich viele Nullstellen in $\mathbb{C}$ hat, gibt es nun abzählbar viele algebraische Zahlen. Da $\mathbb{C}$ überabzählbar ist, gibt es überabzählbar viele transzendente Zahlen. Es ist überraschend, dass wir davon nur wenige konkret kennen, z.B. π, e.

Folgerung II.10 *Seien k, K und L Körper, K eine Körpererweiterung von k und L eine Körpererweiterung von K. Ist $k \subseteq K$ algebraisch und $K \subseteq L$ algebraisch, so ist $k \subseteq L$ algebraisch.*

Beweis. Sei $a \in L$. Da a algebraisch über K ist, gibt es ein Polynom $p \in K[x]$, $p = \sum_{i=0}^{n} a_i x^i$, mit $p \neq 0$ und $p(a) = 0$. Dann ist offenbar a algebraisch über $k(a_0, \ldots, a_n)$. Nach dem Gradsatz II.6 ist

$$[k(a_0, \ldots, a_n, a) : k] = [k(a_0, \ldots, a_n, a) : k(a_0, \ldots, a_n)][k(a_0, \ldots, a_n) : k].$$

Nach Satz II.7 sind beide Körpergrade endlich. Also ist auch

$$[k(a_0, \ldots, a_n, a) : k] < \infty.$$

Nach Satz II.7 ist dann a algebraisch über k. □

Wir wollen nun Automorphismen ins Spiel bringen. Zunächst erweitern wir Isomorphismen auf die zugehörigen Polynomringe. Dazu die folgende Definition:

Definition **Automorphismen von Polynomen.** Seien k_1 und k_2 Körper. Weiter seien $\sigma : k_1 \to k_2$ ein Isomorphismus und $f \in k_1[x]$, $f = \sum_{i=0}^{n} a_i x^i$. Dann setzen wir $\sigma(f) = \sum_{i=0}^{n} \sigma(a_i) x^i$.

Der folgende Satz wird uns noch viele gute Dienste leisten. Seine wirkliche Stärke kommt erst im Rahmen der Galoistheorie zum Tragen, die aber nicht mehr Gegenstand dieses Buches ist.

Satz II.11 *Seien k_1 und k_2 Körper und K_1, K_2 Körpererweiterungen. Für geeignete $u_i \in K_i$, $i = 1, 2$, gelte $K_1 = k_1(u_1)$ und $K_2 = k_2(u_2)$. Sei weiter $\sigma : k_1 \to k_2$ ein Isomorphismus und $m_1 = \sum_{i=0}^{n} a_i x^i$ ein irreduzibles Polynom in $k_1[x]$ mit $m_1(u_1) = 0$. Genau dann gibt es eine Fortsetzung $\tau : K_1 \to K_2$ von σ mit $\tau(u_1) = u_2$, falls u_2 eine Nullstelle von $\sigma(m_1)$ ist. In diesem Fall ist τ eindeutig bestimmt.*

Beweis. Angenommen τ sei eine Fortsetzung mit $\tau(u_1) = u_2$. Dann ist

$$0 = \tau(0) = \tau\Big(\sum_{i=0}^{n} a_i u_1^i\Big) = \sum_{i=0}^{n} \tau(a_i) u_2^i = \sum_{i=0}^{n} \sigma(a_i) u_2^i = \sigma(m_1)(u_2).$$

Sei nun umgekehrt u_2 eine Nullstelle von $\sigma(m_1)$. Angenommen, es wäre auch

$$\sum_{i=0}^{n-1} c_i u_1^i = 0, \text{ mit } c_i \in k_1 \text{ geeignet, nicht alle gleich Null.}$$

Dann ist u_1 Nullstelle des Polynoms $g = \sum_{i=0}^{n-1} c_i x^i \in k_1[x]$. Dann ist u_1 auch Nullstelle des ggT (m_1, g). Also ist m_1 ein Teiler von g. Da m_1 den Grad n hat, folgt $g = 0$, also $c_i = 0$ für $i = 0, \ldots, n-1$. Somit ist $\{1, \ldots, u^{n-1}\}$ linear unabhängig. Nach Satz II.5 ist $[k_1(u_1): k_1] = \operatorname{grad} m_1 = n$. Also ist $\{1, \ldots, u_1^{n-1}\}$ eine Basis von $k_1(u_1)$ als k_1-Vektorraum.

Sei $u \in k_1(u_1)$ beliebig gewählt. Dann gibt es eindeutig bestimmte Elemente $b_i \in k_1$, $i = 0, \ldots, n-1$, mit

$$u = \sum_{i=0}^{n-1} b_i u_1^i.$$

Definiere nun τ durch

$$\tau(u) = \sum_{i=0}^{n-1} \sigma(b_i) u_2^i.$$

Klar ist, dass τ ein Homomorphismus ist. Da $\tau(1) = \sigma(1) = 1 \neq 0$ ist, ist τ nach Folgerung I.10 ein Monomorphismus. Weiter ist $\sigma = \tau_{|k_1}$ und $\tau(u_1) = u_2$.

Wir müssen noch zeigen, dass τ ein Epimorphismus ist. Es ist $m_{u_2} | \sigma(m_1)$. Dann ist $t = \operatorname{grad} m_{u_2} \leq n$. Genauso wie eben folgt, dass $\{1, \ldots, u_2^{t-1}\}$ eine k_2-Basis von $k_2(u_2)$ ist. Sei also $v = \sum_{i=0}^{t-1} d_i u_2^i \in k_2(u_2)$ ein beliebiges Element. Wähle $c_i \in k_1$ mit $\sigma(c_i) = d_i$. Dann ist $v = \tau(\sum_{i=0}^{t-1} c_i u_1^i)$. Also ist τ ein Epimorphismus.

Die Eindeutigkeit von τ ist klar. □

Als erste Anwendung von Satz II.11 erhalten wir den folgenden Satz:

Satz II.12

Seien k ein Körper und $q \in k[x]$ ein irreduzibles Polynom. Dann gibt es einen bis auf Isomorphie eindeutig bestimmten Erweiterungskörper K von k der Form $K = k(a)$, wobei $q(a) = 0$ gilt. Für diesen Körper gilt $[K: k] = \operatorname{grad} q$. Ist insbesondere L ein Körper mit $k \subseteq L$ und sind $a_1, a_2 \in L$ mit $q(a_1) = q(a_2) = 0$, so ist $k(a_1) \cong k(a_2)$.

Beweis. Wir haben nur noch $k(a_1) \cong k(a_2)$ zu zeigen. Dies folgt aus Satz II.11 mit $k_1 = k_2 = k$ und $\sigma = id$. □

Indem wir dies fortsetzen, erhalten wir:

Satz II.13

Seien k ein Körper und $f \in k[x]$ mit $\operatorname{grad} f = n \geq 1$. Dann gibt es einen Erweiterungskörper K von k, so dass $[K: k] \leq n!$ ist, und f über K in Linearfaktoren zerfällt.

Beweis. Nach Satz II.12 gibt es einen Erweiterungskörper k_1 von k, in dem f eine Nullstelle a hat. Es ist $k_1 = k(a)$ und $[k_1 : k] \leq n$. Nun wenden wir Induktion nach dem Grad auf $g = (x-a)^{-1}f$ und den Körper k_1 an. □

Dies führt zu folgender Definition:

Definition

Zerfällungskörper. Seien k ein Körper und K eine Körpererweiterung von k.

a) Sei $F \subseteq k[x]$ eine Menge nicht konstanter Polynome. Wir nennen K einen *Zerfällungskörper* von F, wenn jedes Polynom $f \in F$ in $K[x]$ in Linearfaktoren zerfällt und weiter $k(W) = K$ ist, wobei W die Menge der Nullstellen der Polynome von $f \in F$ ist.

b) Ein Körper K heißt *algebraisch abgeschlossen*, falls es für jedes Polynom $f \in K[x]$ mit $\operatorname{grad} f \geq 1$ ein $a \in K$ mit $f(a) = 0$ gibt.

c) Ein algebraischer Abschluss $\bar{k}$ von k ist eine algebraische Erweiterung von k, die algebraisch abgeschlossen ist.

Bemerkung. $\mathbb{Q}(\sqrt{2})$ ist ein Zerfällungskörper von $F = \{x^2 - 2\}$.

$\mathbb{C}$ ist algebraisch abgeschlossen, aber nicht der algebraische Abschluss von $\mathbb{Q}$, wie wir gleich sehen werden.

Unser Ziel ist es, für jeden Körper einen algebraischen Abschluss zu konstruieren. Dazu müssen wir aber algebraisch abgeschlossene Körper zunächst etwas näher betrachten.

Satz II.14

Sei k ein Körper. Gleichwertig sind

a) $k = \bar{k}$.

b) Ist $f \in k[x]$ *mit* $\operatorname{grad} f \geq 1$, *so gibt es ein* $a \in k$ *mit* $f(a) = 0$.

c) Ist $k \subseteq K$ *eine Körpererweiterung mit* $[K : k] < \infty$, *so ist* $K = k$.

d) Ist $f \in k[x]$ *ein irreduzibles Polynom, so ist* $\operatorname{grad} f = 1$.

Beweis.

a) $\Rightarrow$ *b*): Dies ist die Definition des algebraischen Abschlusses.

b) $\Rightarrow$ *c*): Falls k eine Erweiterungen K von endlichem Grad hat, so sind nach Satz II.4 alle Elemente in K algebraisch über k. Es genügt also zu zeigen, dass jedes algebraische Element schon in k liegt. Sei dazu a algebraisch über k. Betrachte das Minimalpolynom m_a zu a. Nach Voraussetzung gibt es ein $u \in k$ mit $m_a(u) = 0$. Da m_a irreduzibel ist, ist dann $m_a = x - u$. Wegen $m_a(a) = 0$ ist $a = u$, also ist $a \in k$.

c) $\Rightarrow$ *d*): Sei f irreduzibel, $\operatorname{grad} f = n$. Anwendung von Satz II.12 liefert, dass k einen Erweiterungskörper K besitzt, so dass $[K : k] = n$ gilt. Nach Voraussetzung ist $K = k$, also $n = 1$.

d) $\Rightarrow$ a): Sei f ein nicht konstantes Polynom in $k[x]$. Wir wissen, dass f als Produkt irreduzibler Polynome p_i geschrieben werden kann, also $f = p_1 \cdots p_r$. Nach Voraussetzung ist nun grad $p_1 = 1$, also ist $p_1 = ax + b$. Nun ist $-a^{-1}b$ eine Nullstelle von p_1 in k. Dies ist auch eine Nullstelle von f in k. Damit hat jedes nicht konstante Polynom $f \in k[x]$ eine Nullstelle in k, was per Definition liefert, dass k algebraisch abgeschlossen ist. □

Folgerung II.15

Ist K ein Zerfällungskörper aller nicht konstanten Polynome von $k[x]$, so ist K ein algebraischer Abschluss von k.

Beweis. Da K ein Zerfällungskörper ist, ist K algebraisch über k. Um zu zeigen, dass K ein algebraischer Abschluss von k ist, genügt es $K = \bar{K}$ zu zeigen. Dazu wenden wir Satz II.14c) an. Sei L eine Erweiterung von K mit $[L\colon K] < \infty$. Dann ist L algebraisch über K. Nach Folgerung II.10 ist L auch algebraisch über k. Sei $a \in L$ und $m_a \in k[x]$ das Minimalpolynom. Da $m_a \in k[x]$ ist, zerfällt nach Annahme m_a in $K[x]$ in Linearfaktoren, also

$$m_a = \prod (x - a_i)^{n_i}.$$

Dabei sind alle a_i in K. Da $m_a(a) = 0$ ist, ist a eines der a_i, also ist $a \in K$. Somit ist jedes Element aus L in K, was $L = K$ bedeutet. Nach Satz II.14 ist K algebraisch abgeschlossen. □

Lemma II.16

Sei k ein Körper und K eine algebraische Erweiterung von k. Ist $|k|$ endlich, so hat K abzählbar viele Elemente. Ist $|k|$ unendlich, so haben k und K die gleiche Mächtigkeit. Stets hat $K = \bar{k}$ unendlich viele Elemente.

Beweis. Es ist $|k[x]| = |k|\aleph_0$, da $k[x]$ die abzählbare k-Basis $\{x^i \mid i \in \mathbb{N} \cup \{0\}\}$ hat. Ist also $|k|$ endlich, so ist $|k[x]|$ abzählbar. Ist $|k|$ unendlich, so haben $k[x]$ und k die gleiche Mächtigkeit.

Jedes Polynom aus $k[x]$ kann nur endlich viele Nullstellen in K haben, da die Anzahl der Nullstellen eines Polynoms durch den Grad beschränkt ist. Also ist die Anzahl der Nullstellen von Polynomen aus $k[x]$, die in K liegen, durch $\aleph_0|k[x]|$ also $|k[x]|$ beschränkt. Da K algebraisch über k ist, ist jedes Element in K eine Nullstelle eines Polynoms aus $k[x]$. Somit ist $|K|$ durch $|k[x]|$ beschränkt. Ist also $|k|$ unendlich, so sehen wir, dass K und k die gleiche Mächtigkeit haben. Sei nun $|k|$ endlich. Da $|k[x]|$ abzählbar ist, ist dann auch $|K|$ abzählbar.

Wäre $|\bar{k}|$ endlich, so betrachten wir das folgende Polynom

$$f = \prod_{x \in \bar{k}} (x - a) + 1.$$

Es ist $f(a) = 1$ für alle $a \in \bar{k}$ und somit hat f keine Nullstelle in $\bar{k}$, ein Widerspruch. Also hat $\bar{k}$ immer unendlich viele Elemente. □

Nun sieht man auch, dass $\overline{\mathbb{Q}} \neq \mathbb{C}$ ist. Nach Lemma II.16 ist $|\overline{\mathbb{Q}}|$ abzählbar (siehe auch Folgerung II.9), aber $|\mathbb{C}|$ ist überabzählbar.

Wir können jetzt die Existenz eines algebraischen Abschlusses des Körpers k beweisen. Anschaulich ist ein algebraischer Abschluss von k so etwas wie eine größte algebraische Körpererweiterung von k. Es liegt also nahe, hier mit dem Zornschen Lemma zum Erfolg zu kommen. Das Problem ist nur, dass die algebraischen Körpererweiterungen von k keine Menge bilden. Also muss man vorsichtiger vorgehen. Wir werden deshalb zunächst eine Menge definieren, von der wir sicher sein können, dass ihre Kardinalität größer als die eines potenziellen algebraischen Abschlusses ist. Dabei hilft Lemma II.16. Dann werden wir nur alle die algebraischen Erweiterungen betrachten, die in dieser Menge liegen. Hierauf ist das Zornsche Lemma anwendbar, was uns dann einen algebraischen Abschluss liefern wird.

Satz II.17 **Steinitz[1] (1910).** *Jeder Körper hat einen algebraischen Abschluss.*

Beweis. Wir wählen eine Menge S, die k enthält und eine Kardinalität hat, die größer als die jeder algebraischen Erweiterung von k ist. Nach Lemma II.16 erfüllt dies z.B. die Menge $S = k \cup \mathfrak{P}(k) \cup \mathbb{R}$.

Wir betrachten alle Körper $K = (K, +_K, \cdot_K)$, die die folgenden Bedingungen erfüllen:

- Die Menge K ist eine Teilmenge von S, die k enthält.
- Die Addition $+_K$ und Multiplikation $\cdot_K$ auf K seien jeweils Fortsetzungen der Addition und Multiplikation auf k. Damit ist $k \subseteq K$ eine Körpererweiterung.
- Die Körpererweiterung $k \subseteq K$ ist algebraisch.

Diese bilden offenbar eine Menge, die wir mit $\mathfrak{S}$ bezeichnen wollen. Da $k \in \mathfrak{S}$ ist, ist $\mathfrak{S}$ nicht leer.

Als Nächstes definieren wir auf $\mathfrak{S}$ eine Halbordnung $\leq_{\mathfrak{S}}$ durch die Festsetzung

$$K_1 = (K_1, +_{K_1}, \cdot_{K_1}) \leq_{\mathfrak{S}} (K_2, +_{K_2}, \cdot_{K_2}) = K_2,$$

falls $K_1 \subseteq K_2$ und $+_{K_1}, \cdot_{K_1}$ Einschränkungen von $+_{K_2}$ bzw. $\cdot_{K_2}$ sind, also $K_1 \subseteq K_2$ eine Körpererweiterung ist.

Wir wollen zeigen, dass ein maximales Element in $\mathfrak{S}$ der gesuchte algebraische Abschluss ist. Die Existenz solcher Elemente wollen wir mit dem Zornschen Lemma zeigen. Sei dazu $\mathfrak{K}$ eine Kette in $\mathfrak{S}$. Wir müssen eine obere Schranke für $\mathfrak{K}$ in $\mathfrak{S}$ finden. Setze dazu

$$L = \bigcup_{K \in \mathfrak{K}} K.$$

[1] Ernst Steinitz (*13.6.1871 Laurahütte, †29.9.1928 Kiel), Studium in Breslau und Berlin, ab 1894 Privatdozent an der TH Berlin, ab 1910 Professor in Breslau, ab 1920 in Kiel. Er verfasste grundlegende Arbeiten zur Algebra. In dem 1910 veröffentlichten Artikel *Algebraische Theorie der Körper* definierte er wichtige Konzepte der Körpertheorie, wie Primkörper, transzendente Erweiterungen, perfekte Körper, und bewies die Existenz eines algebraischen Abschlusses. Außer seinen algebraischen Arbeiten schrieb Steinitz auch wichtige Arbeiten über Polyeder.

Dann ist $L \subseteq S$. Sind $x, y \in L$, so gibt es ein $K \in \mathfrak{K}$ mit $x, y \in K$, da $\mathfrak{K}$ total geordnet ist. Wir definieren nun eine Addition und Multiplikation auf L durch

$$\begin{aligned} x +_L y &= x +_K y \\ x \cdot_L y &= x \cdot_K y. \end{aligned}$$

Für $K_1, K_2 \in \mathfrak{K}$ gilt stets $K_1 \leq_{\mathfrak{S}} K_2$ oder $K_2 \leq_{\mathfrak{S}} K_1$. Also ist $x +_{K_1} y = x +_{K_2} y$ und $x \cdot_{K_1} y = x \cdot_{K_2} y$. Damit ist die Definition der Addition und Multiplikation in L von der Wahl des Körpers K unabhängig.

In jedem Körperaxiom kommen nur endlich viele Elemente des Körpers vor, welche dann gemeinsam in einem Körper $K \in \mathfrak{K}$ liegen. Hier gelten aber die Axiome. Also ist $(L, +_L, \cdot_L)$ ein Körper.

Wir müssen jetzt noch zeigen, dass $k \subseteq L$ algebraisch ist. Wähle dazu $a \in L$ beliebig. Dann gibt es ein $K \in \mathfrak{K}$ mit $a \in K$. Da K algebraisch über k ist, ist a algebraisch über k. Also ist $k \subseteq L$ eine algebraische Erweiterung und somit ist

$$L \in \mathfrak{S}.$$

Nach dem Lemma von Zorn gibt es nun ein maximales Element $M \in \mathfrak{S}$. Wir zeigen, dass M ein algebraischer Abschluss von k ist.

Zunächst ist $k \subseteq M$ algebraisch, da $M \in \mathfrak{S}$ ist. Sei N eine Erweiterung von M mit $[N\colon M] = n < \infty$. Das Problem ist nun, dass N keine Teilmenge von S sein muss. Wir werden versuchen, einen zu N isomorphen Körper in $\mathfrak{S}$ zu finden.

Nach Lemma II.16 wissen wir, dass $|N| = |k|$ ist, falls $|k|$ unendlich ist, bzw. $|N|$ abzählbar ist, falls $|k|$ endlich ist. Insbesondere ist die Kardinalität von S größer als die von N. Das bedeutet, dass es eine Injektion

$$\sigma\colon N \to S$$

mit $\sigma_{|M} = id$ gibt.

Sei F=Bild σ. Wir definieren auf F eine Addition und Multiplikation, wobei wir die Abbildung σ benutzen.

$$\begin{aligned} x + y &= \sigma(\sigma^{-1}(x) + \sigma^{-1}(y)) \\ xy &= \sigma(\sigma^{-1}(x)\sigma^{-1}(y)). \end{aligned}$$

Man rechnet nach, dass F dadurch ein Körper wird. Die Definition ist gerade so gemacht, dass σ dadurch ein Isomorphismus wird, wie man sofort sieht:

$$\begin{aligned} \sigma(a)\sigma(b) &= \sigma(\sigma^{-1}(\sigma(a))\sigma^{-1}(\sigma(b))) = \sigma(ab) \\ \sigma(a) + \sigma(b) &= \sigma(\sigma^{-1}(\sigma(a)) + \sigma^{-1}(\sigma(b))) = \sigma(a + b). \end{aligned}$$

Also ist σ ein Isomorphismus zwischen N und F. Da $\sigma_{|M} = id$ ist, ist $M \subseteq F$ eine Körpererweiterung. Wir zeigen, dass diese algabraisch ist. Sei dazu $a \in F$. Dann ist $\sigma^{-1}(a) \in N$. Da $M \subseteq N$ algebraisch ist, gibt es ein nicht triviales Polynom $f = \sum_{i=0}^{m} a_i x^i \in M[x]$ mit $f(\sigma^{-1}(a)) = 0$. Da σ ein Homomorphismus ist, erhalten wir

$$0 = \sum_{i=0}^{m} a_i \sigma^{-1}(a)^i = \sum_{i=0}^{n} \sigma^{-1}(a_i)\sigma^{-1}(a)^i = \sigma^{-1}\left(\sum_{i=0}^{m} a_i a^i\right).$$

Da σ bijektiv ist, folgt dann $f(a) = 0$. Dies zeigt, dass a algebraisch über M ist. Insgesamt haben wir $M \subseteq M(a) \subseteq S$ und $M \subseteq M(a)$ ist algebraisch. Nach Folgerung II.10 ist dann auch $k \subseteq M(a)$ algebraisch. Also haben wir $M(a) \in \mathfrak{S}$ gezeigt. Es war aber M ein maximales Elememt in $\mathfrak{S}$, was dann $M(a) = M$ und somit $a \in M$ liefert. Somit ist $F = M$, was $M = N$ zur Folge hat. Nach Satz II.14c) ist dann M algebraisch abgeschlossen. □

Als Spezialfall erhalten wir

Satz II.18 *Seien k ein Körper und $F \subseteq k[x]$ eine Menge nicht konstanter Polynome. Dann existiert ein Zerfällungskörper zu F über k.*

Beweis. Nach Satz II.17 existiert ein algebraischer Abschluss $\bar{k}$ von k. Sei W die Menge der Nullstellen von F in $\bar{k}$. Dann ist $k(W) \subseteq \bar{k}$ ein Zerfällungskörper. □

Wir wollen uns am Ende dieses Kapitels mit der Eindeutigkeit von Zerfällungskörpern beschäftigen. Hierbei wird Satz II.11 eine wichtige Rolle spielen.

Satz II.19 *Seien k_1, k_2 Körper und $\sigma: k_1 \to k_2$ ein Isomorphismus. Sei $m_1 = \sum_{i=0}^{n} a_i x^i$ ein Polynom aus $k_1[x]$. Setze $m_2 = \sigma(m_1) \in k_2[x]$. Wir betrachten Zerfällungskörper K_i von m_i über k_i, $i = 1, 2$. Dann gibt es einen Isomorphismus $\Theta: K_1 \to K_2$, der σ erweitert.*

Beweis. Wir werden die Behauptung durch Induktion nach $n = \operatorname{grad} m_1$ beweisen. Hierbei ist Satz II.11 der Induktionsanfang.

Sei nun $p = \sum_{i=0}^{t} b_i x^i$ ein irreduzibler Teiler von m_1 in $k_1[x]$. Wir setzen $q = \sigma(p)$. Dann ist $q | m_2$.

Es enthält K_1 einen Zerfällungskörper von p und K_2 einen von q. Also gibt es eine Nullstelle u_1 von p in K_1 und eine Nullstelle u_2 von q in K_2. Nach Satz II.11 gibt es eine Fortsetzung τ von σ

$$\tau: k_1(u_1) \to k_2(u_2)$$

mit

$$\tau(u_1) = u_2.$$

Da u_1 auch eine Nullstelle von m_1 ist, gilt

$$m_1 = (x - u_1) \sum_{i=0}^{n-1} c_i x^i \in k_1(u_1)[x].$$

Da $u_2 = \tau(u_1)$ auch eine Nullstelle von m_2 ist, gilt

$$m_2 = (x - \tau(u_1)) \sum_{i=0}^{n-1} \tau(c_i) x^i \in k_2(u_2)[x].$$

Wir setzen $g_1 = \sum_{i=0}^{n-1} c_i x^i$ und $g_2 = \tau(g_1)$. Damit sind dann $m_1 = (x - u_1)g_1$ und $m_2 = (x - u_2)g_2$. Dann ist K_i Zerfällungskörper von g_i über $k_i(u_i)$, $i = 1, 2$. Weiter ist grad $g_1 < n$. Nun liefert die Induktion angewandt auf g_1 und g_2 eine Fortsetzung $\Theta: K_1 \to K_2$ von τ. □

k-isomorph. Seien k, K_1, und K_2 Körper mit $k \subseteq K_i$, $i = 1, 2$. Wir nennen K_1 und K_2 *k-isomorph*, falls es einen Isomorphismus $\sigma: K_1 \to K_2$ mit $\sigma_{|k} = id$ gibt. **Definition**

Seien k ein Körper und $f \in k[x]$ mit f nicht konstant. Sind K_1, K_2 Zerfällungskörper von f über k, so sind sie k-isomorph. **Folgerung II.20**

Beweis. Setze in Satz II.19 $k = k_1 = k_2, f = m_1$ und $\sigma = id$. □

Seien k_1, k_2 Körper und $\sigma: k_1 \to k_2$ ein Isomorphismus. Sei weiter F_1 eine Menge nicht konstanter Polynome aus $k_1[x]$. Setze $F_2 = \{\sigma(f) | f \in F_1\} \subseteq k_2[x]$. Sei K_1 ein Zerfällungskörper von F_1 über k_1 und entsprechend K_2 ein Zerfällungskörper von F_2 über k_2. Dann gibt es einen Isomorphismus $\phi: K_1 \to K_2$, der eine Erweiterung von σ ist. **Satz II.21**

Beweis. Wir betrachten die Körper, die zwischen k_1 und K_1 liegen, zusammen mit allen Einbettungen in K_2, die Erweiterungen von σ sind, also die Menge

$$\mathfrak{S} = \{(k_\alpha, \phi_\alpha) | k_1 \subseteq k_\alpha \subseteq K_1, k_\alpha \text{ Körpererweiterung von } k_1, \phi_\alpha: k_\alpha \to K_2$$

ein Monomorphismus mit $\phi_{\alpha|k_1} = \sigma\}$.

Insbesondere ist $(k_1, \sigma) \in \mathfrak{S}$. Somit ist $\mathfrak{S} \neq \emptyset$. Wir definieren nun auf $\mathfrak{S}$ eine Halbordnung durch

$$(k_\alpha, \phi_\alpha) \leq (k_\beta, \phi_\beta),$$

falls $k_\alpha \subseteq k_\beta$ und $\phi_{\beta|k_\alpha} = \phi_\alpha$ ist. Wenn wir ϕ_α und ϕ_β als Teilmengen von $K_1 \times K_2$ betrachten, so bedeutet dies $\phi_\alpha \subseteq \phi_\beta$.

Wir wollen zeigen, dass $\mathfrak{S}$ maximale Elemente besitzt. Sei dazu $\mathfrak{K}$ eine Kette in $\mathfrak{S}$. Dann definieren wir (k, τ) durch

$$k = \bigcup_{(k_\alpha, \phi_\alpha) \in \mathfrak{K}} k_\alpha \ , \qquad \tau = \bigcup_{(k_\alpha, \phi_\alpha) \in \mathfrak{K}} \phi_\alpha \ ,$$

wobei wir wieder ϕ_α als Teilmenge von $K_1 \times K_2$ auffassen.

Es ist offenbar $(k, \tau) \in \mathfrak{S}$. Damit hat $\mathfrak{K}$ eine obere Schranke in $\mathfrak{S}$. Nach dem Lemma von Zorn gibt es ein maximales Element $(k_0, \Theta) \in \mathfrak{S}$.

Wir wollen $k_0 = K_1$ und $\Theta(K_1) = K_2$ zeigen. Sei dazu zunächst $K_1 \neq k_0$. Wegen der minimalen Eigenschaft von K_1 als Zerfällungskörper ist dann k_0 nicht Zerfällungskörper von F_1. Also gibt es ein $f_1 \in F_1$, so dass nicht alle Nullstellen von f_1 in k_0 liegen. Sei W die Menge der Nullstellen von f_1 in K_1. Setze $L_1 = k_0(W)$. Dann ist L_1 ein Zerfällungskörper von f_1 über k_0.

Setze $f_2 = \Theta(f_1)$. Da $\Theta_{|k_1} = \sigma$ ist, ist $\Theta(f_1) = \sigma(f_1) \in F_2$. Dann gibt es mit gleicher Konstruktion wie vorher in K_2 einen Zerfällungskörper L_2 von f_2 über $\Theta(k_0)$. Nach Satz II.19 gibt es eine Erweiterung Θ_1 von Θ mit $\Theta_1: L_1 \to L_2$. Also ist

$$(k_0, \Theta) \leq (L_1, \Theta_1) \in \mathfrak{S}.$$

Da $k_0 \neq L_1$ ist, widerspricht dies der Maximalität von (k_0, Θ). Also ist $k_0 = K_1$. Dann ist $\Theta(K_1)$ ein Zerfällungskörper von

$$\{\Theta(f) | f \in F_1\} = \{\sigma(f) | f \in F_1\} = F_2.$$

Nach Definition des Zerfällungskörpers ist $\Theta(K_1) = K_2$. □

Folgerung II.22

a) Seien K_1, K_2 algebraische Abschlüsse von k. Dann gibt es einen Isomorphismus $\Theta: K_1 \to K_2$ mit $\Theta(a) = a$ für alle $a \in k$.

b) Sei F eine Menge nicht konstanter Polynome in $k[x]$. Dann sind alle Zerfällungskörper von F k-isomorph.

Beweis. Nach Folgerung II.15 genügt es, b) zu beweisen. Das ist aber die Aussage von Satz II.21 mit $k = k_1 = k_2, F = F_1$ und $\sigma = id$. □

Beispiel

a) Sei $f = (x^2 - 7)(x^2 + x + 2) \in \mathbb{Q}[x]$. In $\mathbb{C}$ berechnen wir

$$f = (x - \sqrt{7})(x + \sqrt{7})\left(x - \frac{-1 + i\sqrt{7}}{2}\right)\left(x - \frac{-1 - i\sqrt{7}}{2}\right).$$

Also ist $\mathbb{Q}(\sqrt{7}, \frac{-1-i\sqrt{7}}{2}) = \mathbb{Q}(\sqrt{7}, i)$ ein Zerfällungskörper von f in $\mathbb{C}$.

b) Sei $f = (x^2 - 2x - 6)(x^2 + 1) \in \mathbb{Q}[x]$. Die Nullstellen von f in $\mathbb{C}$ sind $1 \pm \sqrt{7}, \pm i$. Also ist wieder $\mathbb{Q}(\sqrt{7}, i)$ ein Zerfällungskörper von f in $\mathbb{C}$.

c) Sei nun $f = x^2 + x + 1 \in GF(2)[x]$. Um den Zerfällungskörper zu bestimmen, steht nun eine Einbettung in den bekannten Körper $\mathbb{C}$ nicht mehr zur Verfügung.

Es ist $f(0) = 1 = f(1)$. Damit hat f zunächst einmal keine Nullstelle in $GF(2)$. Da f den Grad zwei hat, ist dann f irreduzibel.

Sei nun α eine Nullstelle von f in $\overline{GF(2)}$. Dann ist $\alpha^2 = 1 + \alpha$. Einsetzen in f liefert

$$(\alpha + 1)^2 + \alpha + 1 + 1 = 0.$$

Also ist auch $\alpha + 1$ eine Nullstelle von f. Das heißt, $GF(2)(\alpha)$ ist ein Zerfällungskörper.

Es ist $[GF(2)(\alpha): GF(2)] = 2$ nach Satz II.12. Somit ist $|GF(2)(\alpha)| = 4$. Das heißt, $GF(2)(\alpha) = \{0, 1, \alpha, 1 + \alpha\}$ ist ein Körper mit 4 Elementen.

d) Sei $f \in K[x]$ ein nicht konstantes Polynom. Wir können f auch als Polynom aus $\bar{K}[x]$ auffassen. Hier zerfällt f in Linearfaktoren. Es gibt ein einfaches Verfahren, in $K[x]$ festzustellen, ob f in $\bar{K}[x]$ mehrfache Nullstellen hat.

Sei $f = (x-a)^2 g \in \bar{K}[x]$ und $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. Setze $f' = \sum_{i=0}^{n} i a_i x^{i-1}$. Dann gelten für f' die üblichen Regeln von Ableitungen. Siehe hierzu auch das Beispiel am Ende von Kapitel I. Insbesondere gilt: Sind $h, r \in K[x]$, so ist

$$(hr)' = h'r + hr'.$$

Dies wenden wir nun auf unser f an.

$$f' = 2(x-a)g + (x-a)^2 g'.$$

Also ist $x - a$ ein Teiler von f' in $\bar{K}[x]$. Das heißt, ggT $(f, f') \neq 1$ in $\bar{K}[x]$. Ist ggT $(f, f') = 1$ in $K[x]$, so gibt es nach Satz I.16 $a, b \in K[x]$ mit

$$af + bf' = 1.$$

Dies ist aber auch eine Gleichung in $\bar{K}[x]$, was dann ggT $(f, f') = 1$ in $\bar{K}[x]$ liefern würde.

Ist

$$f = \prod_{i=1}^{n} (x - a_i) \in \bar{K}[x]$$

mit paarweise verschiedenen a_i, so ist

$$f' = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ j \neq i}}^{n} (x - a_i).$$

Wäre $(x - a_j)$ ein Teiler von f' für ein j, so würde $(x - a_j)$ auch $\prod_{\substack{i=1 \\ i \neq j}}^{n} (x - a_i)$ teilen, ein Widerspruch, da alle a_i verschieden sind. Also ist ggT $(f, f') = 1$, falls f nur einfache Nullstellen in $\bar{K}$ hat.

Es genügt also, den ggT (f, f') in $K[x]$ zu berechnen. Wir fassen zusammen:

Satz II.23

Sei $f \in K[x]$.

a) Es hat f mehrfache Nullstellen in $\bar{K}[x]$ genau dann, wenn ggT $(f, f') \neq 1$ *ist.*

b) Ist f irreduzibel, so ist entweder $f' = 0$ oder ggT $(f, f') = 1$.

Beweis.

a) steht im Teil d) des vorhergehenden Beispiels.

b) Da f irreduzibel ist, ist ggT $(f', f) = f$ oder 1. Ist ggT $(f', f) = f$, so ist f ein Teiler von f'. Da grad $f' <$ grad f ist, ist dann $f' = 0$. □

Übungsaufgaben

II.1 Betrachte $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ als Teilkörper von $\mathbb{C}$. Zeige, dass sie nicht isomorph sind.

II.2 Bestimme folgende Körpergrade der Teilkörper von $\mathbb{C}$

a) $[\mathbb{Q}(\sqrt{15}):\mathbb{Q}]$.

b) $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{7}):\mathbb{Q}]$.

c) $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$.

II.3 Sei $K \subseteq L$ eine Körpererweiterung mit $[L:K] = 2$. Zeige:

a) Ist $\alpha \in L \setminus K$, so ist $L = K(\alpha)$.

b) Ist char $K \neq 2$, so gibt es ein $\alpha \in L$, so dass $m_\alpha = x^2 - a$ für ein geeignetes $a \in K$ gilt.

c) Ist char $K = 2$, und gibt es ein $\alpha \in L \setminus K$, so dass $m_\alpha \neq x^2 + a$ für irgendein $a \in K$ ist, so gibt es ein α mit $m_\alpha = x^2 + x + a$ für ein geeignetes $a \in K$.

II.4 Sei $f = x^3 + px + q \in \mathbb{Q}[x]$. In $\mathbb{C}$ habe f die Nullstellen $\alpha_1, \alpha_2, \alpha_3$. Setze

$$d = \Big((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)\Big)^2.$$

a) Bestimme d als Funktion von p und q.

b) Sei L ein Zerfällungskörper von $x^3 - 4x - 1$ über $\mathbb{Q}$. Zeige $[L:\mathbb{Q}] = 6$.

II.5 Sei $f = x^4 + x^2 + 1 \in K[x]$. Bestimme einen Zerfällungskörper von f über K für

a) $K = \mathbb{Q}$.

b) $K = \mathrm{GF}(2)$.

II.6 Sei $k \subseteq K$ eine Körpererweiterung mit $[K:k] = p, p$ eine Primzahl. Zeige:

a) Ist $a \in K \setminus k$, so ist $K = k(a)$.

b) Sei $f \in k[x]$ mit $\operatorname{grad} f = p$. Gibt es ein $a \in K \setminus k$ mit $f(a) = 0$, so ist f irreduzibel über k.

II.7 Sei $K \subseteq L$ eine Körpererweiterung und f ein irreduzibles Polynom aus $K[x]$ vom Grad n. Ist $[L:K]$ endlich und n teilerfremd zu $[L:K]$, so ist f auch in $L[x]$ irreduzibel.

II.8 Es ist bekannt, dass e und π beide transzendent sind. Folgere daraus, dass nicht beide $e + \pi$ und $e \cdot \pi$ algebraisch sein können. (Es ist allerdings eine offene Frage, ob einer, und wenn ja, wer von beiden, $e + \pi$ oder $e \cdot \pi$ algebraisch ist!)

III Endliche Körper

In diesem Kapitel wollen wir uns mit einer speziellen Klasse von Körpern, den endlichen Körpern, beschäftigen. Davon kennen wir bisher $GF(p) = \mathbb{Z}/p\mathbb{Z}$, p Primzahl. Weiter hatten wir am Ende von Kapitel II (siehe Seite 48) einen Körper mit vier Elementen konstruiert. Wir wollen zunächst alle endlichen Körper angeben.

Endliche Körper spielen in vielen Bereichen eine Rolle, so z.B. in der Informatik. Eine besonders wichtige Rolle spielen sie aber in der Codierungstheorie. Einzelheiten hierzu kann man in Willems (2008, [32]) aus der gleichen Lehrbuchreihe finden. Aber auch wir haben endliche Körper bereits auf Seite 27 angewandt, um die Irreduzibiltät eines Polynoms mit ganzzahligen Koeffizienten zu entscheiden.

Das erste Lemma sagt, dass es Körper nicht zu jeder Ordnung gibt. So gibt es z.B. keinen Körper mit genau 6 Elementen.

Lemma III.1 *Sei K ein Körper, $|K| < \infty$. Dann gibt es eine Primzahl p mit $|K| = p^f$ für ein geeignetes $f \in \mathbb{N}$.*

Beweis. Sei k der Primkörper. Nach Satz II.2 ist $k \cong GF(p)$ für eine Primzahl p. Es ist $[K:k] = f$ für ein f. Das heißt, K ist ein f-dimensionaler Vektorraum über $GF(p)$ und somit ist $|K| = p^f$. □

Wir wollen nun umgekehrt zeigen, dass es für jede Primzahlpotenz p^f bis auf Isomorphie genau einen endlichen Körper K mit $|K| = p^f$ gibt. Dazu benötigen wir ein wenig Gruppentheorie.

Satz III.2 **Lagrange**[1]**.** *Sei G eine endliche Gruppe und U eine Untergruppe von G. Dann ist $|U| \Big| |G|$.*

Beweis. Sei $g \in G$. Setze

$$gU = \{gu | u \in U\}.$$

[1] Joseph-Louis Lagrange (*25.1.1736 Turin, †10.4. 1813 Paris), Professor in Turin, Berlin und Paris. Lagrange verfasste grundlegende Arbeiten zur Variationsrechnung, Zahlentheorie und Differentialrechnung. Er gilt als Begründer der analytischen Mechanik.

Seien $g, h \in G$, mit $gU \cap hU \neq \varnothing$. Wähle $x \in gU \cap hU$. Dann ist $x = gu_1 = hu_2$ mit $u_1, u_2 \in U$ geeignet. Somit ist

$$h = gu_1u_2^{-1} \in gU.$$

Sei nun $u \in U$ beliebig, so ist

$$hu \in gU,$$

also ist

$$hU \subseteq gU.$$

Genauso erhält man auch

$$gU \subseteq hU.$$

Somit ist stets $gU = hU$ oder $gU \cap hU = \varnothing$. Weiter ist $G = \bigcup_{g \in G} gU$. Damit gibt es $r_1, \ldots, r_t \in G$ mit $r_iU \cap r_jU = \varnothing$ für $i \neq j$ und

$$G = \bigcup_{i=1}^{t} r_iU.$$

Da die Multiplikation mit Gruppenelementen eine bijektive Abbildung ist, haben wir

$$|r_iU| = |U|, \quad i = 1, \ldots, t.$$

Das liefert

$$|G| = \sum_{i=0}^{t} |r_iU| = t|U|.$$

□

Die Menge gU aus dem Beweis von Satz III.2 spielt in vielen Zusammenhängen eine wichtige Rolle. Wir wollen ihr einen Namen geben.

Definition

Nebenklassenvertretersystem. Seien G eine Gruppe, U eine Untergruppe von G und $g \in G$. Dann nennen wir die Menge $gU = \{gu | u \in U\}$ eine *Rechtsnebenklasse* von U in G. Sei R eine Teilmenge von G mit $r_1U \cap r_2U = \varnothing$ für $r_1, r_2 \in R, r_1 \neq r_2$ und $G = \bigcup_{r \in R} rU$, so nennen wir R ein *Rechtsnebenklassenvertretersystem* von U in G. Entsprechendes gilt für *Linksnebenklassen* Ug.

Lemma III.3

Seien G eine Gruppe und $g \in G$. Sei $n \in \mathbb{N}$ minimal mit $g^n = 1$. Ist $m \in \mathbb{N}$ mit $g^m = 1$, so ist n ein Teiler von m.

Bemerkung. Ist n wie in Lemma III.3, so sagen wir, dass g die Ordnung n hat, und schreiben $o(g) = n$.

Beweis. Wir teilen m durch n mit Rest, also $m = xn + r$ mit $0 \leq r < n$. Nun gilt

$$1 = g^m = (g^n)^x g^r = g^r.$$

Da $r < n$ ist und n minimal war, ist $r = 0$, d.h., n teilt m. □

Lemma III.4

Sei G eine endliche abelsche Gruppe und seien $a, b \in G$.

a) Sind $o(a)$ und $o(b)$ teilerfremd, so ist $o(ab) = o(a)o(b)$.

b) Sei $\langle a, b\rangle$ die kleinste Untergruppe von G, die a und b enthält. Dann gibt es ein $d \in \langle a, b\rangle$ mit $o(d) = \mathrm{kgV}\,(o(a), o(b))$.

Beweis.

a) Es ist

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

Nach Lemma III.3 ist dann

$$m = o(ab) | o(a)o(b).$$

Es ist

$$a^m b^m = (ab)^m = 1.$$

Somit ist

$$1 = (a^m)^{o(a)} = (b^{-m})^{o(a)},$$

also

$$b^{mo(a)} = 1.$$

Nach Lemma III.3 ist $o(b)$ ein Teiler von $mo(a)$. Da $\mathrm{ggT}\,(o(a), o(b)) = 1$ ist, ist

$$o(b) \text{ ein Teiler von } m.$$

Genauso gilt auch

$$o(a) \text{ ist ein Teiler von } m.$$

Dann ist

$$o(a)o(b) \text{ ein Teiler von } m.$$

Insgesamt erhalten wir

$$o(a)o(b) = o(ab).$$

b) Seien

$$o(a) = p_1^{a_1} \cdots p_r^{a_r} \cdots p_t^{a_t} \text{ und } o(b) = p_1^{b_1} \cdots p_r^{b_r} q_{r+1}^{b_{t+1}} \cdots q_s^{b_s}$$

die Primfaktorzerlegungen von $o(a)$ bzw. $o(b)$, wobei $p_1, \ldots, p_r$ die gemeinsamen Primteiler seien. Dabei wollen wir die Anordnung noch so wählen, dass für ein w und $1 \le i \le w$ stets $a_i \ge b_i$ und für $w+1 \le i \le r$ stets $b_i > a_i$ sei. Wir betrachten die zwei natürlichen Zahlen $x = \prod_{i=w+1}^{r} p_i^{a_i}$ und $y = \prod_{i=1}^{w} p_i^{b_i}$. Dann setzen wir

$$d_1 = a^x, \quad d_2 = b^y.$$

Es ist $o(d_1) = p_1^{a_1} \cdots p_w^{a_w} p_{r+1}^{a_{r+1}} \cdots p_t^{a_t}$ und $o(d_2) = p_{w+1}^{b_{w+1}} \cdots p_r^{b_r} q_{r+1}^{b_{r+1}} \cdots q_s^{b_s}$. Wir sehen nun, dass $\mathrm{ggT}\,(o(d_1), o(d_2)) = 1$ ist. Mit a) erhalten wir

$$o(d_1 d_2) = o(d_1)o(d_2) = \mathrm{kgV}\,(o(a), o(b)) \text{ und } d = d_1 d_2 \in \langle a, b\rangle. \qquad \square$$

Lemma III.5 *Seien G eine Gruppe und $a \in G$. Sei weiter $o(a) = t < \infty$. Dann ist $\{1, a, \ldots, a^{t-1}\}$ eine Untergruppe von G, die wir mit $\langle a \rangle$ bezeichnen. Es ist $|\langle a \rangle| = t$. Ist $|G| < \infty$, so ist $o(a)$ ein Teiler von $|G|$.*

Beweis. Offenbar ist $\langle a \rangle \neq \emptyset$. Seien a^i und a^j Elemente aus $\langle a \rangle$. Dann ist

$$a^i a^j = a^{i+j}.$$

Sei $i + j = xt + r$ mit $0 \leq r \leq t - 1$. Dann ist

$$a^i a^j = a^{xt+r} = (a^t)^x a^r = a^r \in \langle a \rangle.$$

Sei a^i mit $0 < i < t$ ein Element von $\langle a \rangle$. Dann ist auch $a^{t-i} \in \langle a \rangle$ und

$$a^i a^{t-i} = a^t = 1.$$

Also ist $\langle a \rangle$ eine Untergruppe. Da $o(a) = t$ ist, sind alle Elemente in $\langle a \rangle$ paarweise verschieden, also $|\langle a \rangle| = t$.

Ist $|G| < \infty$, so ist $o(a)$ ein Teiler von $|G|$ nach dem Satz von Lagrange III.2. □

Nun können wir die angekündigte Klassifikation beweisen.

Satz III.6 *Zu jeder Primzahlpotenz $q = p^f$ gibt es bis auf Isomorphie genau einen Körper K mit $|K| = q$.*

Beweis. Sei K ein Körper mit $|K| = q$. Dann hat die multiplikative Gruppe K^* von K die Ordnung $q - 1$. Sei $a \in K^*$ und $o(a) = t$. Nach Lemma III.5 ist t ein Teiler von $q - 1$. Insbesondere ist dann $a^{q-1} = 1$ für alle $a \in K^*$. Somit ist dann sogar $a^q = a$ für alle $a \in K$. Damit ist jedes Element aus K Nullstelle des Polynoms $x^q - x$. Also ist K im Zerfällungskörper F von $x^q - x$ über $GF(p)$ enthalten. Es hat $x^q - x$ nach Satz I.27 höchstens q Nullstellen. Also enthält K alle Nullstellen, was $K = F$ liefert.

Sei jetzt umgekehrt F der Zerfällungskörper von $f = x^q - x$ über $GF(p)$. Sind a, b Nullstellen von f, so gilt

$$a^q = a, \quad b^q = b.$$

Nach Lemma II.3 ist $(a + b)^p = a^p + b^p$, da $\operatorname{char} F = p$ ist. Also ist auch

$$(ab)^q = a^q b^q = ab \quad \text{und} \quad (a + b)^q = a^q + b^q = a + b.$$

Somit bilden die Nullstellen von f einen Körper. Wir wollen nun zeigen, dass f genau q verschiedene Nullstellen hat.

Es ist $(x^q - x)' = qx^{q-1} - 1 = -1$, also $\operatorname{ggT}(x^q - x, (x^q - x)') = 1$. Nach Satz II.23 hat $f = x^q - x$ genau q paarweise verschiedene Nullstellen und damit ist $|F| = q$.

Wir haben gezeigt, dass es einen Körper mit q Elementen gibt, und jeder solche ist ein Zerfällungskörper von $x^q - x$. Die Eindeutigkeit folgt nun mit Folgerung II.22. □

Wir wollen jetzt noch zeigen, dass es in einem endlichen Körper K mit $|K| = q$ stets ein Element a gibt, so dass $o(a) = q - 1$ ist. Eine Gruppe G, die wie in Lemma III.5 aus den Potenzen eines einzelnen Elements besteht, nennen wir *zyklisch*. Wir wollen also zeigen, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Wir zeigen etwas mehr.

Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch. **Satz III.7**

Beweis. Seien K ein Körper und G eine endliche Untergruppe von K^*. Setze $t = \text{kgV}\,(o(a)|a \in G)$. Sei $a \in G$ beliebig. Dann ist $o(a)$ ein Teiler von t. Also ist $a^t = 1$ für alle Elemente a von G. Somit sind alle Elemente von G Nullstellen von $x^t - 1$. Es hat aber $x^t - 1$ höchstens t verschiedene Nullstellen, was $|G| \leq t$ liefert. Mit Lemma III.4b) erhalten wir, dass G ein Element a der Ordnung t enthält. Somit ist $G = \{1, a, a^2, \ldots, a^{t-1}\}$, d.h. zyklisch. □

Als Anwendung sehen wir, dass endliche Erweiterungen endlicher Körper stets einfach sind, d.h., von einem Element erzeugt werden.

Ist K eine endliche Erweiterung eines endlichen Körpers k, so wird K über k von einem Element erzeugt, d.h., es gibt ein $a \in K$ mit $K = k(a)$. **Lemma III.8**

Beweis. Es ist $[K:k] = n < \infty$. Also ist $|K| = |k|^n < \infty$. Die Anwendung von Satz III.7 liefert die Existenz eines Elementes $a \in K$ mit $\langle a \rangle = K^*$. Insbesondere ist dann $K = k(a)$. □

Übungsaufgaben

III.1 Seien K ein endlicher Körper mit $|K| = p^f$, p Primzahl, und L ein Teilkörper von K mit $|L| = p^t$. Zeige, dass f von t geteilt wird.

III.2 Gib einen Körper mit 27 Elementen an.

III.3 Sei $q = p^f$ eine Primzahlpotenz, K ein endlicher Körper mit $|K| = q$ und k sein Primkörper. Zeige:

a) Sind K_1 und K_2 Teilkörper von K mit $|K_1| = |K_2|$, so ist $K_1 = K_2$.

b) $x^q - x \in k[x]$ ist das Produkt aller normierten irreduziblen Polynome in $k[x]$, deren Grad f teilt.

III.4 Sei $K = GF(2)$ der Körper mit zwei Elementen. Seien $p_1, p_2, q \in K[x]$ Polynome mit $p_1 = x^4 + x^3 + 1$, $p_2 = x^4 + x + 1$ und $q = x^2 + x + 1$.

a) Zeige, dass q das einzige irreduzible Polynom vom Grad zwei über K ist.

b) Zeige, dass beide Polynome p_1, p_2 über K irreduzibel sind.

c) Sei $p_1(\alpha_1) = 0 = p_2(\alpha_2)$ für $\alpha_1, \alpha_2 \in \bar{K}$, wobei $\bar{K}$ ein algebraischer Abschluss von K ist. Zeige, dass $K(\alpha_1)$ und $K(\alpha_2)$ isomorph sind.

IV Primzahlen

Wir kehren nun wieder zur Arithmetik zurück. In diesem Kapitel wollen wir uns den ganzen Zahlen $\mathbb{Z}$ widmen. Da sich jede ganze Zahl als Produkt von Primzahlen schreiben lässt, wollen wir auf diese ein Hauptaugenmerk lenken. Primzahlen sind üblicherweise Primelemente p mit $p > 0$. Zunächst ein Klassiker:

Es gibt unendlich viele Primzahlen. **Satz IV.1**

Beweis. **Euklid.** Seien $p_1, \ldots, p_r$ sämtliche Primzahlen. Da 2 eine Primzahl ist, ist $r \geq 1$. Betrachte $n = 1 + p_1 \cdots p_r$. Es ist n keine Einheit, da $n > 1$ ist. Also gibt es eine Primzahl p, die n teilt. Dann ist $p \neq p_1, \cdots, p_r$, da p nicht 1 teilt. Somit erhalten wir einen Widerspruch dazu, dass $p_1, \cdots, p_r$ die sämtlichen Primzahlen sind.

Wir wollen noch einen weiteren Beweis geben.

Sei $\{p_i | i \in I\}$, $I \subseteq \mathbb{N}$, die Menge aller Primzahlen. Betrachte die Reihe

$$\sum_{i \in I} \frac{1}{p_i}.$$

Wir zeigen, dass diese Reihe divergiert. Diese Aussage wurde zuerst von Euler gemacht. Der hier gegebene Beweis der Divergenz stammt von Paul Erdös [7]. Dann gibt es insbesondere unendlich viele Primzahlen. Angenommen, die Reihe konvergiert. Sei

$$a_n = \sum_{i=1}^{n} \frac{1}{p_i}$$

die n-te Partialsumme. Die Konvergenz liefert ein k mit

$$a_i - a_k < 1/2 \quad \text{für alle} \quad i \geq k + 1.$$

Also gilt für beliebiges $N \in \mathbb{N}$

$$N(a_i - a_k) < N/2.$$

Sei nun N_s die Anzahl der natürlichen Zahlen $n \leq N$, die nur durch die Primzahlen $p_1, \ldots, p_k$ teilbar sind, und sei N_b die Anzahl der restlichen $n \leq N$. Also

$$N_b + N_s = N.$$

Es ist $\lfloor \frac{N}{p_i} \rfloor$ die Anzahl der natürlichen Zahlen $n \leq N$, die durch p_i teilbar sind. Ist $p_i > N$, so ist $\lfloor \frac{N}{p_i} \rfloor = 0$. Also gibt es ein r mit

$$N_b \leq \sum_{i=k+1}^{r} \left\lfloor \frac{N}{p_i} \right\rfloor \leq N \sum_{i=k+1}^{r} \frac{1}{p_i} = N(a_r - a_k) < N/2.$$

Betrachte $n \leq N$. Es ist

$$n = q_n s_n^2, \quad q_n \text{ quadratfrei.}$$

Also ist q_n ein Produkt von paarweise verschiedenen Primzahlen.

Sei nun n nur durch Primzahlen aus $\{p_1, \ldots, p_k\}$ teilbar. Dann gibt es für q_n maximal 2^k Möglichkeiten. Es ist weiter

$$s_n \leq \sqrt{n} \leq \sqrt{N}.$$

Also gibt es höchstens $\sqrt{N}$ Möglichkeiten für s_n. Das liefert

$$N_s \leq 2^k \sqrt{N}.$$

Setze nun $N = 2^{2k+2}$. Dann ist $\sqrt{N} = 2^{k+1}$ und

$$N_s \leq 2^{2k+1} = \frac{N}{2}.$$

Damit haben wir

$$N = N_b + N_s < \frac{N}{2} + \frac{N}{2} = N,$$

ein Widerspruch. Also konvergiert $\sum_{i \in I} \frac{1}{p_i}$ nicht. □

Es ist offen, ob es unendlich viele Primzahlzwillinge, also Primzahlen im Abstand zwei wie 5,7 oder 11,13 gibt. Sei $\mathcal{P}_2$ die Menge der Primzahlzwillinge. Immerhin hat Brun[1] 1919 gezeigt, dass $\sum_{p \in \mathcal{P}_2} \frac{1}{p}$ konvergiert, so dass ein ähnlicher Beweis wie eben nicht existiert. Der Wert der Summe wird die *Brunsche Konstante B* genannt. Er liegt bei 1, 902160583104.....

Wir wollen uns nun die Verteilung der Primzahlen ansehen. Wenn man sich die ersten 1000 Zahlen ansieht, so erhält man die Vorstellung, dass pro hundert Zahlen zwischen 20 und 25 davon Primzahlen sind. Es gilt aber:

Lemma IV.2

Es gibt beliebig lange Primzahllücken, d.h., für vorgegebenes n gibt es n aufeinander folgende Zahlen, die keine Primzahlen sind.

Beweis. Sei $n \in \mathbb{N}$. Dann gibt es zwischen $(n+1)! + 2$ und $(n+1)! + (n+1)$ keine Primzahlen. □

[1] Viggo Brun (*13.10.1885 Lier, †15.8.1978 Drobak), norwegischer Mathematiker, Professor an den Universitäten Trondheim und Oslo. Brun arbeitete über Primzahlzwillinge und die Goldbach-Vermutung.

Andererseits gibt es zwischen n und $2n$ immer eine Primzahl, wie wir jetzt in einer Folge von Lemmata zeigen wollen.

Lemma IV.3

Für alle $x \in \mathbb{R}$, $x \geq 2$, gilt

$$\prod_{\substack{p \text{ Primzahl} \\ p \leq x}} p < 4^x.$$

Beweis. Es genügt, x ungerade und $x \in \mathbb{N}$ zu betrachten. Also $x = 2m + 1$, $m \in \mathbb{N}$. Ist $x = 3$, so ist $2 \cdot 3 < 4^3$. Also können wir $x > 3$ annehmen. Setze $k = m$ für m ungerade und $k = m + 1$ für m gerade.

Sei $k < p \leq x$. Dann ist p ein Teiler von $x!$, aber p teilt nicht $k!$. Ist m ungerade, so ist $m \geq 3$. Es ist weiter $x - k = k + 1$ gerade. Da $p > k$ ist, ist p kein Teiler von $(x - k)!$. Ist m gerade, so ist $x - k = k - 1$ gerade. Also ist stets

$$p \text{ kein Teiler von } (x - k)!\,,$$

was

$$\prod_{k < p \leq x} p \leq \frac{x!}{k!(x-k)!} = \binom{x}{k}$$

liefert. Nun gilt

$$2^x = (1+1)^x = \sum_{t=1}^{x} \binom{x}{t} > \binom{x}{k} + \binom{x}{x-k} = 2\binom{x}{k}.$$

Beachte, dass k ungerade und $(x - k)$ gerade ist. Somit sind $\binom{x}{k}$ und $\binom{x}{x-k}$ zwei verschiedene Summanden. Also ist

$$2^{x-1} > \binom{x}{k}.$$

Eine Induktion liefert nun

$$\prod_{p \leq x} p = \prod_{p \leq k} p \prod_{k < p \leq x} p < 4^k 2^{x-1} = 2^{2k+x-1} \leq 2^{2x} = 4^x.$$

□

Lemma IV.4

Sei $n \in \mathbb{N}$ und $n = a_0 + a_1 p + \cdots + a_r p^r$ mit $0 \leq a_i \leq p-1$. Setze $S_p(n) = a_0 + \cdots + a_r$. Sei $n! = p^{e_p(n!)} t$, wobei p kein Teiler von t sei. Dann ist

$$e_p(n!) = \frac{n - S_p(n)}{p - 1}.$$

Beweis. Von den n Faktoren in $n!$ enthalten genau $\lfloor \frac{n}{p} \rfloor$ den Faktor p, von diesen dann $\lfloor \frac{n}{p^2} \rfloor$ den Faktor p^2 usw. Also ist

$$e_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor.$$

Ist $i > r$, so ist $\lfloor \frac{n}{p^i} \rfloor = 0$. Für $0 < i \leq r$ ist

$$\lfloor \frac{n}{p^i} \rfloor = a_i + a_{i+1}p + \cdots + a_{r-1}p^{r-i-1} + a_r p^{r-i}.$$

Also ist

$$\begin{aligned} e_p(n!) = a_1 &+ a_2 p &&+ a_3 p^2 + \cdots + a_r p^{r-1} \\ &+ a_2 &&+ a_3 p + \cdots + a_r p^{r-2} \\ &&&+ a_3 + \cdots + a_r p^{r-3} \\ &&&\ddots \\ &&&+ a_r \end{aligned}$$

$$= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_r(p^{r-1} + p^{r-2} + \cdots + 1)$$

$$= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + a_3 \frac{p^3-1}{p-1} + \cdots + a_r \frac{p^r-1}{p-1}$$

$$= \frac{(a_0 + a_1 p + \cdots + a_r p^r) - (a_0 + a_1 + \cdots + a_r)}{p-1} = \frac{n - S_p(n)}{p-1}.$$

□

Lemma IV.5

Sei $n \in \mathbb{N}$ und $n = a_0 + a_1 p + \cdots + a_r p^r$, mit $0 \leq a_i \leq p-1$. Sei weiter $S_p(n) = a_0 + a_1 + \cdots + a_r$. Ist

$$\binom{2n}{n} = p^{e_p\left(\binom{2n}{n}\right)} t, \text{ wobei } p \text{ kein Teiler von } t \text{ sei,}$$

so ist $p^{e_p\left(\binom{2n}{n}\right)} \leq 2n$ und

$$e_p\left(\binom{2n}{n}\right) = \frac{2S_p(n) - S_p(2n)}{p-1}.$$

Beweis. Nach Lemma IV.4 gilt

$$e_p\left(\binom{2n}{n}\right) = e_p\left(\frac{(2n)!}{(n!)^2}\right) = \frac{2n - S_p(2n)}{p-1} - 2\left(\frac{n - S_p(n)}{p-1}\right) = \frac{2S_p(n) - S_p(2n)}{p-1}.$$

Sei nun

$$2n = b_0 + b_1 p + \ldots + b_u p^u, 0 \leq b_i \leq p-1.$$

Sei v die Anzahl der Ziffernübertragungen, die bei der Addition von $n + n = 2n$ auftreten. Es ist $v \leq u$. Jede Ziffernübertragung trägt höchstens den Wert $p-1$ bei.

Also

$$2S_p(n) - S_p(2n) \le v(p-1) \le u(p-1).$$

Also ist $e_p(\binom{2n}{n}) \le u$. Das liefert $p^{e_p(\binom{2n}{n})} \le p^u \le 2n$. □

Jetzt können wir das angekündigte Resultat beweisen.

Bertrand-Postulat[2]. *Für jedes $n > 1$ existiert eine Primzahl p mit $n < p < 2n$.* Satz IV.6

Beweis. **Erdös**[3]**.** Sei zunächst $n < 128$. Setze

$$p_i = 2, 3, 5, 7, 13, 23, 43, 83, 163,\ i = 1, \dots, 10.$$

Dann ist stets $p_i < 2p_{i-1}$. Also erhält jedes Intervall $n < y < 2n$ eine dieser Primzahlen.

Sei ab jetzt $n \ge 128$. Wir nehmen weiter an, dass es für ein n keine Primzahl p zwischen n und $2n$ gibt. Dann ist

$$\binom{2n}{n} = \prod_{p \le n} p^{e_p(\binom{2n}{n})}.$$

Sei zunächst p eine Primzahl mit $\frac{2}{3}n < p \le n$. Dann ist $n = p + a_0$, $0 \le a_0 \le p-1$. Also ist $S_p(n) = 1 + a_0$ und $S_p(2n) = 2 + 2a_0$, da $2n = 2p + 2a_0$ und $2n < 3p$, also $2a_0 < p$ ist. Also ist

$$2S_p(n) = S_p(2n).$$

Nach Lemma IV.5 ist dann $e_p\left(\binom{2n}{n}\right) = 0$, d.h., ein solches p kommt in der Primfaktorzerlegung von $\binom{2n}{n}$ nicht vor.

Betrachte nun Primzahlen p mit $\sqrt{2n} < p \le \frac{2}{3}n$. Dann ist $n = a_1 p + a_0$ mit $1 \le a_1 < \frac{p}{2}$ und $0 \le a_0 < p$. Es ist

$$2n = 2a_1 p + 2a_0 < p^2.$$

Es kann somit bei der Addition $n + n$ höchstens eine Ziffernübertragung auftreten. Also ist

$$2S_p(n) - S_p(2n) \le p - 1.$$

Mit Lemma IV.5 erhalten wir

$$e_p\left(\binom{2n}{n}\right) \le 1.$$

[2] Joseph L.F. Bertrand (*11.3.1822, †5.4.1900, beides Paris), Professor an der École Polytechnique und am Collège de France, war 26 Jahre Sekretär der Akademie der Wissenschaften. Bertand arbeitete in Zahlentheorie, Differentialgeometrie, Wahrscheinlichkeitrechnung, Ökonomie und Thermodynamik. Das Postulat wurde von ihm vermutet, aber erst 1850 von Chebyshev bewiesen. Er ist berühmt für das Bertrand-Paradox in der Wahrscheinlichkeitstheorie.

[3] Paul Erdös, *26.3.1913 Budapest, †20.9.1996 Warschau, ist für seine brillianten Beweise und seine scheinbar unlösbaren Probeme, für die er Preisgelder aussetzte, bekannt. Sein Hauptarbeitsgebiet war die Zahlentheorie. Er war einer der kreativsten Mathematiker des letzten Jahrhunderts. Sein Werk umfasst mehr als 1500 Arbeiten mit mehr als 450 Koautoren. Paul Erdös wurde mit vielen Preisen ausgezeichnet unter anderem dem Cole Preis und dem Wolf Preis. Paul Erdös promovierte im Alter von 19 Jahren mit einem Beweis von Bertrand's Postulat [8], auf den sich der hier gegebene bezieht. Eine schöne Biographie findet man in "The man, who loved only numbers" [12].

Diese Primzahlen kommen also höchstens mit der Vielfacheit 1 in der Primfaktorzerlegung von $\binom{2n}{n}$ vor.

Sei zuletzt p eine Primzahl mit $p \leq \sqrt{2n}$. Nach Lemma IV.5 ist $e_p\left(\binom{2n}{n}\right) \leq 2n$. Also ist

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Im ersten Produkt kommen höchstens $\frac{1}{2}\sqrt{2n}$ Faktoren vor, da 1 und die geraden Zahlen $\neq 2$ keine Primzahlen sind. Da $n \geq 128$ ist, ist $\sqrt{2n} \geq 16$. Dann sind auch 9 und 15 keine Primzahlen, also kommen weniger als $\frac{1}{2}\sqrt{2n} - 1$ viele Faktoren vor.

Nach Lemma IV.3 ist

$$\prod_{p \leq \frac{2}{3}n} p < 4^{\frac{2}{3}n}.$$

Also ist

$$\binom{2n}{n} < (2n)^{\frac{1}{2}\sqrt{2n}-1} 4^{\frac{2}{3}n}.$$

Es ist $(1+1)^{2n} = \sum_{i=1}^{2n} \binom{2n}{i} < 2n\binom{2n}{n}$. Das liefert $2^{2n} < 2n\binom{2n}{n}$. Also ist

$$\frac{2^{2n}}{2n} < (2n)^{\frac{1}{2}\sqrt{2n}-1} 4^{\frac{2}{3}n}$$

und dann

$$2^{\frac{2}{3}n} < (2n)^{\frac{1}{2}\sqrt{2n}}$$

und

$$\frac{2}{3}n \log 2 < \frac{1}{2}\sqrt{2n} \log 2n$$

oder anders ausgedrückt

$$\frac{4n}{\sqrt{2n}} \log 2 - 3 \log 2n < 0 \text{ bzw. } \sqrt{8n} \log 2 - 3 \log 2n < 0.$$

Wir betrachten die Abbildung

$$f: x \to \sqrt{8x} \log 2 - 3 \log 2x.$$

Es ist

$$f'(x) = \frac{1}{x}(\sqrt{2x} \log 2 - 3) > 0, \quad \text{für } x \geq 128 \quad \text{und}$$
$$f(128) = 32 \log 2 - 24 \log 2 = 8 \log 2 > 0.$$

Somit erhalten wir

$$f(x) > 0, \quad \text{für alle} \quad x \geq 128,$$

ein Widerspruch zu $\sqrt{8n} \log 2 - 3 \log 2n < 0$. Somit gibt es zwischen n und $2n$ eine Primzahl. □

Eine offene Frage ist, ob es stets eine Primzahl zwischen n^2 und $(n+1)^2$ gibt.

Trotz all dieser Resultate sind die Primzahlen doch nicht ganz wild verteilt. 1792 hat C.F. Gauß den folgenden Satz vermutet:

Primzahlsatz. *Sei $\pi(x)$ die Anzahl der Primzahlen kleiner gleich x. Dann ist $\pi(x)$ asymptotisch gleich $\frac{x}{lnx}$, d.h.* Satz IV.7

$$\lim_{x\to\infty} \frac{\pi(x)}{(\frac{x}{lnx})} = 1.$$

Dieser Satz wurde erst 1896 von Hadamard[4] und unabhängig auch von de la Vallée-Poussin[5] bewiesen. Der Beweis benutzt analytische Hilfsmittel, die den Rahmen dieses Buches sprengen würden.

Eine weitere, immer wieder gestellte Frage ist die nach einer Primzahlformel. Es fragt sich zunächst, welche Art Formel man meint. Stellt man sich die Primzahlen $p_1, p_2, \ldots$ in einer Reihenfolge, z.B. der Größe nach, geordnet vor, so ist

$$f(n) = p_n \text{ (die } n\text{-te Primzahl)}$$

sicherlich eine Formel. Man kann auch zeigen, dass die folgende Reihe konvergiert (siehe [11] Satz 419):

$$\sum_{n=1}^{\infty} p_n 10^{-2^n} = a.$$

Dann ist

$$p_n = \lfloor 10^{2^n} a \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} a \rfloor.$$

Diese Formel ist allerdings zur Berechnung von p_n ziemlich nutzlos.

Wie sieht es aber aus, wenn wir uns auf Polynome beschränken? Betrachten wir erst einmal Formeln der Form

$$f(n) = an + b.$$

Damit $f(n)$ Primzahlen darstellt, sollte zumindest ggT $(a, b) = 1$ sein. Sei für ein n

$$an + b = p$$

eine Primzahl. Setze $n_k = n + kp$, $k = 0, 1, \cdots$. Dann ist

$$an_k + b = a(n + kp) + b = an + b + akp = (ak + 1)p.$$

[4] Jacques S. Hadamard (*8.12.1865 Versailles, †17.10.1963 Paris), arbeitete zunächst als Lehrer, promovierte über Taylorreihen, wurde 1896 Professor für Astronomie und Mechanik in Bordeaux und wechselte 1897 an die Sorbonne. Hadamard war in die Dreyfus-Affäre verstrickt, dessen Schwager er war. Er wurde 1906 Präsident der Société Mathématique de France, 1912 Professor für Analysis an der École Polytechnique (Nachfolge Camille Jordan). Er war Mitglied der Akademie der Wissenschaften. Hadamard schrieb bahnbrechende Arbeiten im Bereich der partiellen Differentialgleichungen und Geodäsie. Er arbeitete auf den Gebieten der Optik, Hydrodynamik und Grenzwertprobleme.

[5] Charles de la Vallée-Poussin (*14.8.1866 Löwen, †2.3.1962 Brüssel), Professor in Löwen, Harvard, Paris und Genf. Er arbeitete über Differentialgleichungen, Funktionentheorie und Potentialtheorie.

Somit kann $an + b$ niemals nur Primzahlen darstellen. Immerhin können so aber unendlich viele Primzahlen dargestellt werden.

Lemma IV.8

a) Die Folge $4n + 3$, $n \in \mathbb{N}$, enthält unendlich viele Primzahlen.

b) Die Folge $8n \pm 3$, $n \in \mathbb{N}$, enthält unendlich viele Primzahlen.

Beweis. Wir beweisen a) und b) gleichzeitig. Seien $p_1, \ldots, p_r$ sämtliche Primzahlen, die durch $4n + 3$ bzw. $8n \pm 3$ dargestellt werden können. Es gibt solche Primzahlen, z.B. 7, 11, 5. Wir verfahren nun ähnlich wie in Satz IV.1. Ist $x \in \mathbb{N}$ ungerade, so ist

$$8 | x^2 - 1.$$

Also ist

$$8 | p_1^2 \cdots p_r^2 - 1.$$

Setze $x = p_1^2 \cdot \cdots \cdot p_r^2 - 2$ in a) und $x = p_1^2 \cdot \cdots \cdot p_r^2 - 4$ in b).

Für alle i gilt:

$$p_i \text{ teilt nicht } x.$$

Also ist jede Primzahl, die x teilt, von der Form $4n + 1$ in a) bzw. $8n \pm 1$ in b). Da

$$(4n_1 + 1)(4n_2 + 1) = 4m + 1 \qquad \text{bzw.} \qquad (8n_1 \pm 1)(8n_2 \pm 1) = 8m \pm 1$$

ist, ist also in a) $x = 4t + 1$ bzw. in b) $x = 8t \pm 1$ für geeignetes t.

Es war aber 8 ein Teiler von $p_1^2 \cdots p_r^2 - 1$, d.h., 8 teilt $x + 1 = 4t + 2$ in a) bzw. $x + 3 = 8t + 4$ oder $8t + 2$ in b), was offenbar nicht möglich ist. □

Lemma IV.8 ist nur ein Spezialfall eines allgemeinen Satzes.

Satz IV.9

Dirichlet[6]. *Ist* ggT $(a, b) = 1$, *so enthält die Folge $an + b$, $n \in \mathbb{N}$, unendlich viele Primzahlen.*

Auch die Bemerkung, dass $an + b$ nicht nur Primzahlen darstellen kann, gilt allgemeiner.

Satz IV.10

Sei f ein Polynom. Ist $n \in \mathbb{N}$ mit $f(n) = p$, p eine Primzahl, so ist $p | f(n + kp)$ für alle $k \in \mathbb{N}$.

Beweis. Sei $f(n) = \sum_{i=0}^{r} a_i n^i$. Dann ist

$$f(n + kp) = \sum_{i=0}^{r} a_i (n + kp)^i = \sum_{i=0}^{r} a_i n^i + tp.$$

□

[6] Johann Peter Gustave Lejeune Dirichlet (*13.2.1805 Düren, †5.5.1859 Göttingen), Professor in Berlin und Göttingen, dort Nachfolger von Gauß. Hauptarbeitsgebiete waren partielle Differentialgleichungen, Zahlentheorie und Integraltheorie.

Euler hat festgestellt, dass $n^2 + n + 41$ für $-40 \leq n \leq 39$ immer eine Primzahl ist, also für 80 aufeinander folgende Werte prim ist. Dies ist bisher der Rekord für quadratische Polynome. Natürlich kann man mittels Interpolation bei genügend großem Grad erreichen, dass für beliebig viele aufeinander folgende n ein Polynom f mit $f(n)$ prim existiert.

Ein ähnlicher Satz wie IV.9 für Polynome höheren Grades ist nicht bekannt. Es ist z.B. offen, ob es unendlich viele Primzahlen der Form $n^2 + 1$ gibt.

Vielleicht gibt es ja Polynome, die nur Primzahlen darstellen. Diese sind dann notwendigerweise in mehreren Variablen. Es sind allerdings keine einfachen Polynome bekannt. Im Rahmen der Lösung des 10. Hilbert-Problems hat Matijassewitsch (1970, [17]) ein Polynom in 26 Variablen angegeben. Falls bei einer Belegung der Variablen der Wert dieses Polynoms positiv ist, so ist er immer eine Primzahl.

In Kapitel I Seite 12 hatten wir uns die Ringe $\mathbb{Z}/m\mathbb{Z}$ angesehen. Wir wollen jetzt in diesen ein wenig rechnen. Zur Vereinfachung der Sprechweise führen wir die folgende Notation ein. Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, so schreibe

$$a \equiv b (\mathrm{mod}\, m) \text{ (in Worten: } a \text{ kongruent } b \text{ modulo } m),$$

falls

$$a + m\mathbb{Z} = b + m\mathbb{Z} \text{ ist, oder anders ausgedrückt } m \text{ teilt } a - b.$$

Wie man schnell sieht, kann mit den Kongruenzen fast wie mit Gleichungen gerechnet werden.

Lemma IV.11

Seien $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$. Dann gilt

a) Ist $a \equiv b (\mathrm{mod}\, m)$, so auch $b \equiv a (\mathrm{mod}\, m)$.

b) Ist $a \equiv b (\mathrm{mod}\, m)$ und $c \equiv d (\mathrm{mod}\, m)$, so ist $a + c \equiv b + d (\mathrm{mod}\, m)$.

c) Ist $a \equiv b (\mathrm{mod}\, m)$ und $c \equiv d (\mathrm{mod}\, m)$, so ist $ac \equiv bd (\mathrm{mod}\, m)$.

Beweis. a) und b) sind klar.

c) Es ist $ac - bd = (a - b)c + b(c - d)$. Da m sowohl $a - b$ also auch $c - d$ teilt, gilt m teilt $ac - bd$. □

Allerdings ist im Allgemeinen nicht richtig, dass aus $ca \equiv cb (\mathrm{mod}\, m)$ stets $a \equiv b (\mathrm{mod}\, m)$ folgt. Es ist $6 \equiv 2 (\mathrm{mod}\, 4)$, aber nicht $3 \equiv 1 (\mathrm{mod}\, 4)$.

Wir wissen, dass $\mathbb{Z}/m\mathbb{Z}$ kein Körper ist, falls m keine Primzahl ist. Also gibt es nicht invertierbare Elemente. Wir können kürzen, falls $c + m\mathbb{Z}$ eine Einheit in $\mathbb{Z}/m\mathbb{Z}$ ist. Dies ist richtig, falls $\mathrm{ggT}(c, m) = 1$ ist. Dann ist nämlich $cx + my = 1$ für geeignete $x, y \in \mathbb{Z}$, also $(c + m\mathbb{Z})(x + m\mathbb{Z}) + (my + m\mathbb{Z}) = 1 + m\mathbb{Z}$, d.h.

$$(c + m\mathbb{Z})(x + m\mathbb{Z}) = 1 + m\mathbb{Z}.$$

Somit haben wir:

Lemma IV.12

Seien $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\mathrm{ggT}(c, m) = 1$. Dann folgt aus $ac \equiv bc (\mathrm{mod}\, m)$ stets $a \equiv b (\mathrm{mod}\, m)$.

Satz IV.13 **Wilson**[7]. *Sei p eine Primzahl. Dann ist*

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

Beweis. Es ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper nach Lemma I.13 und Satz I.15. Also gibt es zu jedem $1 \leq x \leq p-1$ ein $1 \leq y \leq p-1$ mit

$$xy \equiv 1 (\mathrm{mod}\, p).$$

Ist $x = y$, so ist $x^2 \equiv 1 (\mathrm{mod}\, p)$. D.h. p teilt $x^2 - 1 = (x-1)(x+1)$.

Da p eine Primzahl ist, ist p ein Teiler von $x-1$ oder $x+1$. Somit ist $x \equiv 1 (\mathrm{mod}\, p)$ oder es ist $x \equiv -1 \equiv p-1 (\mathrm{mod}\, p)$. Für alle anderen x ist $x \neq y$. Damit ist $(p-1)! \equiv p-1 \equiv -1 (\mathrm{mod}\, p)$. □

Ist übrigens $p > 2$ keine Primzahl, so ist $\mathrm{ggT}(p, (p-1)!) \neq 1$. Da aber stets $\mathrm{ggT}(-1, p) = 1$ ist, ist dann $(p-1)! \not\equiv -1 (\mathrm{mod}\, p)$.

Dennoch eignet sich der Satz von Wilson nicht, um zu zeigen, dass p eine Primzahl ist. Besser steht es da schon um den folgenden Satz:

Satz IV.14 **Fermat**[8]. *Sei p eine Primzahl und $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, p) = 1$. Dann ist*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Beweis. Wir betrachten $\bar{a} = a + p\mathbb{Z}$ als Element in $\mathbb{Z}/p\mathbb{Z}$.. Nach Lemma III.5 ist $o(\bar{a})$ ein Teiler von $p-1$. Also ist $\bar{a}^{p-1} = \bar{1}$, was $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$ liefert. Dann ist

$$a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$$

also

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$ □

Was passiert, wenn p keine Primzahl ist?

Sei z.B. $p = 6$ und $a = 5$. Dann ist $\mathrm{ggT}(p, a) = 1$.

Aber es gilt

$$5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 1 \cdot 1 \cdot 5 \equiv 5 \equiv -1 (\mathrm{mod}\, 6).$$

[7] John Wilson (*6.8.1741 Applethwaite, †18.10. 1793, Kendal), britischer Mathematiker. Waring veröffentlichte den Satz 1770 als Satz von Wilson, aber ohne Beweis. Der erste Beweis wurde 1773 von Lagrange gegeben.

[8] Pierre de Fermat (*20.8.1601 Beaumont-de-Lomagne, †12.1.1665 Castres), Jurist und Mathematiker, war Mitglied des obersten Gerichtshofs in Toulouse. Fermat beschäftigte sich mit Mathematik nur als Hobby. Er lieferte wesentliche Beiträge zur Geometrie, Analysis und Wahrscheinlichkeitstheorie. Berühmt sind seine Beiträge zur Zahlentheorie und hier insbesondere der „Große Fermatsche Satz". Die Versuche, diesen Satz zu beweisen, führten zur Entwicklung der algebraischen Zahlentheorie. Schließlich wurde der Satz 1995 von A. Wiles bewiesen.

Das Einsetzen kleiner Zahlen zeigt, dass es für zusammengesetzte Zahlen n stets ein a mit ggT $(n, a) = 1$ gibt, so dass $a^{n-1} \not\equiv 1 (\mathrm{mod}\ n)$ ist. Zahlen n mit $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ für alle a mit ggT $(a, n) = 1$ wollen wir *Carmichaelzahlen*[9] nennen. Die Frage ist nun:

Sind Carmichaelzahlen prim?

Lemma IV.15

Sei $n = p_1 \cdots p_r$, alle p_i verschiedene ungerade Primzahlen. Ist $p_i - 1 | n - 1$ für alle i, so ist n eine Carmichaelzahl.

Beweis. Wir halten i fest. Dann ist $n - 1 = (p_i - 1)r$. Sei $a \in \mathbb{N}$ mit ggT $(a, n) = 1$. Nach dem Satz von Fermat IV.14 ist p_i ein Teiler von $a^{p_i - 1} - 1$. Also ist

$$a^{n-1} = a^{(p_i-1)r} = (a^{p_i-1})^r \equiv 1^r \equiv 1 (\mathrm{mod}\ p_i).$$

Dann ist p_i ein Teiler von $a^{n-1} - 1$ für alle i. Also ist

$$n = p_1 \cdots p_r \quad \text{ein Teiler von} \quad a^{n-1} - 1$$

und dann

$$a^{n-1} \equiv 1 (\mathrm{mod}\ n).$$

□

Damit haben wir ein Verfahren, wie wir Carmichaelzahlen finden können. Es gilt aber auch noch:

Lemma IV.16

Sei n eine ungerade Carmichaelzahl und n nicht prim. Dann ist $n = p_1 \cdots p_r$, wobei alle p_i prim und paarweise verschieden sind. Weiter ist $p_i - 1$ ein Teiler von $n - 1$ und $r \geq 3$.

Um dieses Lemma beweisen zu können, benötigen wir allerdings noch mehr Resultate über Kongruenzen, die wir im Folgenden entwickeln wollen.

Immerhin können wir nun mit Lemma IV.15 und Lemma IV.16 die kleinste Carmichaelzahl n finden, die keine Primzahl ist. Sie muss durch mindestens drei verschiedene Primzahlen p_1, p_2 und p_3 teilbar sein. Weiter muss $p_i - 1$, $i = 1, 2, 3$, stets $n - 1$ teilen. Dies liefert schnell $n = 561$. Somit gibt es Carmichaelzahlen, die nicht prim sind. Da der Satz von Fermat für Primzahltests eine zentrale Bedeutung hat, hoffte man, dass es nur endlich viele Carmichaelzahlen gibt. Dies ist aber falsch, wie W.R. Alford, A. Granville und C. Pomerance (1994, [2]) zeigen konnten. Jeder Primzahltest, der auf dem Satz von Fermat beruht, muss irgendwie die Carmichaelzahlen umgehen.

Wir wollen nun zunächst den Satz von Fermat verallgemeinern.

Definition

Eulerfunktion. Sei $n \in \mathbb{N}$. Mit $\varphi(n)$ bezeichne die Anzahl der Einheiten in $\mathbb{Z}/n\mathbb{Z}$. Wir nennen φ die *Eulerfunktion*.

[9] Robert D. Carmichael (*1.3.1879 Goodwater, Alabahma, †1967), amerikanischer Mathematiker, Professor an der University of Illinois. Seine Arbeitsgebiete waren Zahlentheorie und Relativitätstheorie.

Es ist $\varphi(n)$ auch die Anzahl der $x \in \mathbb{N}$ mit $1 \leq x \leq n$, so dass ggT $(x, n) = 1$ ist.

Sei ggT $(x, n) = 1$. Dann gibt es $a, b \in \mathbb{Z}$ mit $ax + bn = 1$, also

$$(a + n\mathbb{Z})(x + n\mathbb{Z}) = 1 + n\mathbb{Z},$$

was besagt, dass $x + n\mathbb{Z}$ eine Einheit ist.

Ist umgekehrt $x + n\mathbb{Z}$ eine Einheit, so gibt es ein $a + n\mathbb{Z}$ mit

$$(a + n\mathbb{Z})(x + n\mathbb{Z}) = 1 + n\mathbb{Z},$$

also

$$ax + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Dann ist ggT $(x, n) = 1$.

Satz IV.17

Euler[10]**.** *Seien $a, n \in \mathbb{N}$. Ist* ggT $(a, n) = 1$, *so ist*

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n).$$

Beweis. Wir folgen dem Beweis von Lemma IV.14. Nach der Vorbemerkung ist $a + n\mathbb{Z}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$. Also folgt, dass $o(a + n\mathbb{Z})$ die Ordnung der Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ teilt. Dies liefert

$$(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$$

und dann

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n). \qquad \square$$

Wie kann man $\varphi(n)$ berechnen?

Es ist $\varphi(1) = 1$. Ist p eine Primzahl, so ist $\varphi(p) = p - 1$. Was ist $\varphi(p^a)$? Es hat p und auch jedes Vielfache von p einen nicht trivialen Teiler mit p^a und dies sind auch genau alle solche Zahlen. Davon gibt es p^{a-1} viele zwischen 1 und p^a. Also ist

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1).$$

Wäre $\varphi(p^a q^b) = \varphi(p^a)\varphi(q^b)$ für verschiedene Primzahlen p und q, so hätten wir eine Formel für $\varphi(n)$. Genau das wollen wir jetzt beweisen. Dazu beweisen wir zunächst einen Satz, der auch von unabhängiger Bedeutung ist.

[10] Leonhard Euler (*15.4.1707 Basel, †18.9.1783 St. Petersburg), Professor in Berlin und St. Petersburg, bedeutendster Mathematiker des 18. Jahrhunderts, lieferte auf fast allen damals zur Mathematik gehörenden Gebieten grundlegende Beiträge. Er publizierte über 500 Arbeiten und ca. 350 tauchten noch nach seinem Tode auf. Bedeutend waren nicht nur seine erzielten Sätze, sondern auch seine Fähigkeit, die ihm bekannte Mathematik zu vereinheitlichen und zu systematisieren.

Chinesischer Restsatz[11]. *Seien $m_1, \ldots, m_k$ paarweise teilerfremde natürliche Zahlen und, $a_1, \ldots, a_k$ ganze Zahlen. Dann hat*

$$x \equiv a_i (\mathrm{mod}\, m_i),\ i = 1, \ldots, k \qquad (\star)$$

eine Lösung $x \in \mathbb{Z}$.

Lemma IV.18

Beweis. Es gibt eine Lösung $x \equiv a_1 (\mathrm{mod}\, m_1)$, nämlich $x = a_1$. Alle Lösungen dieser Kongruenz sind von der Form $a_1 + ym_1$ mit y beliebig.

Nun betrachten wir das System

$$ym_1 \equiv a_i - a_1 (\mathrm{mod}\, m_i),\ i = 2, \ldots, k. \qquad (\star\star)$$

Da ggT $(m_1, m_i) = 1$ für alle $i = 2, \ldots, k$ ist, gibt es t_i mit $m_1 t_i \equiv 1 (\mathrm{mod}\, m_i)$. Wir betrachten jetzt

$$y \equiv ym_1 t_i \equiv (a_i - a_1) t_i (\mathrm{mod}\, m_i),\ i = 2, \ldots, k. \qquad (\star\star\star)$$

Per Induktion nach k gibt es eine Lösung y von $(\star\star\star)$. Wegen $(\star\star)$ ist dann $a_1 + ym_1$ eine Lösung des Systems $(\star)$. □

Sind a, b teilerfremd, so ist $\varphi(ab) = \varphi(a)\varphi(b)$.

Lemma IV.19

Beweis. Wir betrachten die Menge

$$E = \{(x, y) | 1 \leq x \leq a, 1 \leq y \leq b, \text{ggT}\,(x, a) \neq 1 \text{ oder ggT}\,(y, b) \neq 1\}.$$

Es ist

$$|E| = ab - \varphi(a)\varphi(b).$$

Wir wollen nun E noch auf eine andere Art abzählen. Dabei wird der Wert $\varphi(ab)$ eingehen, was uns dann die Formel liefert. Sei $1 \leq t \leq ab$ mit ggT $(t, ab) \neq 1$. Dann ist ggT $(t, a) \neq 1$ oder ggT $(t, b) \neq 1$.

Sei t_1 der Rest von t modulo a, $1 \leq t_1 \leq a$, und r_1 der von t modulo b, $1 \leq r_1 \leq b$. Also

$$t \equiv t_1 (\mathrm{mod}\, a)$$
$$t \equiv r_1 (\mathrm{mod}\, b).$$

Dabei ist ggT $(t_1, a) \neq 1$ oder ggT $(r_1, b) \neq 1$. Also ist $(t_1, r_1) \in E$. Somit können wir jedem t, $1 \leq t \leq ab$ mit ggT $(t, ab) \neq 1$ ein $(t_1, r_1) \in E$ zuordnen. Wir zeigen, dass diese Zuordnung injektiv ist.

[11] Der Chinesische Restsatz wurde von den Chinesen im 13. Jahrhundert zur Berechnung der Planetenbahnen benutzt. Es wurde hierbei allerdings angenommen, dass sich die Planeten auf Kreisbahnen bewegen.

Seien $1 \leq t, \tilde{t} \leq ab$, $\mathrm{ggT}(t, ab) \neq 1$ und $\mathrm{ggT}(\tilde{t}, ab) \neq 1$. Sei $t \to (t_1, r_1)$ und $\tilde{t} \to (t_1, r_1)$. Dann sind a und b Teiler von $t - \tilde{t}$. Da $\mathrm{ggT}(a, b) = 1$ ist, ist auch ab ein Teiler von $t - \tilde{t}$. Da $t, \tilde{t} \leq ab$ sind, ist $t = \tilde{t}$. Damit ist die Zuordnung injektiv. Also ist

$$(1) \qquad |E| \geq ab - \varphi(ab).$$

Sei nun $(x, y) \in E$. Nach dem Chinesischen Restsatz IV.18 gibt es ein $t_1 \in \mathbb{Z}$ mit

$$t_1 \equiv x (\mathrm{mod}\, a)$$
$$t_1 \equiv y (\mathrm{mod}\, b).$$

Betrachte t mit $t_1 \equiv t (\mathrm{mod}\, ab)$ und $1 \leq t \leq ab$. Da $\mathrm{ggT}(x, a) \neq 1$ oder $\mathrm{ggT}(y, b) \neq 1$ ist, ist $\mathrm{ggT}(t_1, a) \neq 1$ oder $\mathrm{ggT}(t_1, b) \neq 1$. Also ist $\mathrm{ggT}(t, ab) \neq 1$. Somit ist (x, y) ein t, $1 \leq t \leq ab$ mit $\mathrm{ggT}(t, ab) \neq 1$ zugeordnet. Wir zeigen, dass diese Zuordnung injektiv ist.

Sei dazu $(\tilde{x}, \tilde{y}) \in E$ mit

$$t_1 \equiv \tilde{x} (\mathrm{mod}\, a)$$
$$t_1 \equiv \tilde{y} (\mathrm{mod}\, b).$$

Dann teilt a sowohl $\tilde{x} - t_1$ als auch $x - t_1$, also auch $x - \tilde{x}$. Genauso ist b ein Teiler von $y - \tilde{y}$. Da $1 \leq x, \tilde{x} \leq a$ und $1 \leq y, \tilde{y} \leq b$ ist, ist dann $x = \tilde{x}$ und $y = \tilde{y}$. Also ist die Zuordnung injektiv und damit

$$(2) \qquad |E| \leq ab - \varphi(ab).$$

Das liefert $|E| = ab - \varphi(ab)$. Da wir bereits $|E| = ab - \varphi(a)\varphi(b)$ gezeigt haben, folgt $\varphi(ab) = \varphi(a)\varphi(b)$. □

Eine Konsequenz ist nun:

Folgerung

Sei $n = p_1^{a_1} \dots p_r^{a_r}$ die Primfaktorzerlegung von n. Dann ist

$$\varphi(n) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1).$$

Der Satz von Euler spielt in der Kryptographie eine wichtige Rolle. Die tragende Idee ist, eine Art der Verschlüsselung zu benutzen, die von der Methode her bekannt ist, aber in der Praxis kaum von Unberechtigten entschlüsselt werden kann.

Hier ist die Idee eines solchen Systems. Jeder Nutzer $A, B, \dots$ hat einen individuellen Schlüssel $f_A, f_B, \dots$. Diese Schlüssel werden allen Nutzern bekannt gegeben. Zum Entschlüsseln benötigt man die inverse Funktion $g_A = f_A^{-1}, g_B = f_B^{-1}, \dots$. Die Sicherheit des Systems ist dann gegeben, wenn g_A selbst unter Kenntnis von f_A nur sehr schwer berechenbar ist. Die Nachrichtenübertragung geht nun wie folgt vor:

Wir nehmen an, dass A eine Nachricht N an B senden möchte. Hierzu benutzt er den öffentlich zugänglichen Schlüssel f_B und sendet

$$f_B(N).$$

B wendet auf diese Nachricht, die er empfängt, seinen Schlüssel g_B an und erhält

$$g_B(f_B(N)) = N.$$

Eine Variante hiervon ist die elektronische Unterschrift. Wie kann B sicher sein, dass die Nachricht N wirklich von A gekommen ist? Dazu wählt A die folgende Variante. Er wendet zunächst g_A auf N an und berechnet dann wie oben

$$f_B(g_A(N)).$$

Der Empfänger B wendet g_B hierauf an, was $g_A(N)$ ergibt. Da er eine Nachricht von A erwartet, wendet er nun das öffentlich bekannte f_A an und erhält N.

Es sind also solche Funktionen f_A gesucht, für die g_A nur mit großem Aufwand berechenbar ist. Eine mögliche Funktion ist die Eulerfunktion $\varphi(n)$.

Seien p, q zwei verschiedene Primzahlen. Bilde

$$n = pq.$$

Es ist

$$\varphi(n) = (p-1)(q-1) = n - p - q + 1.$$

Kennt man p und q, so kann man also leicht $\varphi(n)$ berechnen. Sind umgekehrt n und $\varphi(n)$ gegeben, so können p und q leicht bestimmt werden.

$$n = pq,\ p + q = n - \varphi(n) + 1.$$

Also sind p, q Lösungen der quadratischen Gleichung

$$t^2 - (n - \varphi(n) + 1)t + n.$$

Die Berechnung von $\varphi(n)$ direkt aus n ist also genauso schwierig wie die Bestimmung der Primteiler p und q. Solange wir davon ausgehen können, dass die Primfaktorzerlegung schwierig ist, ist auch die Berechnung der Eulerfunktion schwierig. Eine systematische Behandlung dieser Fragen findet man, wie erwähnt, in Willems (2008, [32]).

Beispiel

a) Wir wollen zeigen, dass es keine ganzzahligen Lösungen x, y von

$$x^2 + y^2 = 1203$$

gibt. Seien also x und y solche. Wir rechnen modulo 4. Es ist

$$x^2 + y^2 \equiv 3 (\mathrm{mod}\ 4).$$

Für jede ganze Zahl gilt $x^2 \equiv 0, 1 (\mathrm{mod}\ 4)$. Also ist $x^2 + y^2 \equiv 0, 1, 2 (\mathrm{mod}\ 4)$. Das heißt, es gibt keine ganzzahlige Lösung von

$$x^2 + y^2 = 1203.$$

Beispiel

b) Was sind die letzten beiden Ziffern von 3^{1234}?

Wir rechnen jetzt modulo 100. Es ist $\varphi(100) = \varphi(2^2 \cdot 5^2) = 2 \cdot 5 \cdot 4 = 40$. Also ist nach dem Satz IV.17 von Euler

$$3^{40} \equiv 1 (\mathrm{mod}\ 100).$$

Es ist $1234 = 30 \cdot 40 + 34$. Also $3^{1234} \equiv 3^{34} (\mathrm{mod}\ 100)$. Es ist

$$\begin{array}{rcrcl} 3^4 & & & \equiv & 81 \quad (\mathrm{mod}\ 100) \\ 3^8 & \equiv & 81 \cdot 81 & \equiv & 61 \quad (\mathrm{mod}\ 100) \\ 3^{10} & \equiv & 9 \cdot 61 & \equiv & 49 \quad (\mathrm{mod}\ 100) \\ 3^{20} & \equiv & 49 \cdot 49 & \equiv & 1 \quad (\mathrm{mod}\ 100). \end{array}$$

Somit ist

$$3^{1234} \equiv 3^{14} \equiv 49 \cdot 81 \equiv 69 (\mathrm{mod}\ 100).$$

Die beiden letzten Ziffern sind also 69.

c) Sei $n \in \mathbb{N}$, $n = a_0 + a_1 \cdot 10 + \ldots a_k \cdot 10^k$ die Dezimaldarstellung, also $0 \leq a_i \leq 9$, $i = 0, \ldots, k$.

Da $10 \equiv 1 (\mathrm{mod}\ 3)$ ist, ist

$$n \equiv a_0 + \cdots + a_k (\mathrm{mod}\ 3).$$

Somit ist 3 genau dann ein Teiler von n, wenn 3 die Quersumme $a_0 + \cdots + a_k$ teilt. Da auch $10 \equiv 1 (\mathrm{mod}\ 9)$ ist, gilt dies für 9 entsprechend.

Da $10 \equiv -1 (\mathrm{mod}\ 11)$, $100 \equiv 1 (\mathrm{mod}\ 11)$ ist, gilt: 11 teilt n genau dann, wenn 11 die alternierende Quersumme $a_0 - a_1 + a_2 \cdots (-1)^k a_k$ teilt.

d) Es gibt offenbar zwei aufeinander folgende Zahlen, die einen quadratischen Faktor haben: 8,9. Es gibt auch drei aufeinander folgende Zahlen: 48, 49, 50. Wie ist dies mit 100000 aufeinander folgenden? Wir betrachten dazu die ersten 100000 Primzahlen $p_1, \ldots, p_{100000}$. Nun lösen wir mit dem Chinesischen Restsatz IV.18

$$x \equiv -i (\mathrm{mod}\ p_i^2),\ i = 1, \ldots, 100000.$$

Die gesuchten Zahlen sind:

$$x + 1, x + 2, \ldots, x + 100000.$$

Wir kommen nun zum

Beweis von Satz IV.16: Sei p eine Primzahl, so dass n von p^2 geteilt wird. Zunächst eine Vorbetrachtung.

Es ist

$$(1 + p)^p = \sum_{i=0}^{p} \binom{p}{i} p^i.$$

Ist i verschieden von 0 und p, so ist p ein Teiler von $\binom{p}{i}$. Also ist

$$(1 + p)^p \equiv 1 + p^p \equiv 1 (\mathrm{mod}\ p^2).$$

Sei

$$(1+p)^y \equiv 1 (\mathrm{mod}\, p^2) \qquad \text{für ein } 1 \leq y < p.$$

Da ggT $(y, p) = 1$ ist, gibt es nach Satz I.16 $a, b \in \mathbb{Z}$ mit $1 = ap + by$. Also ist

$$p + 1 \equiv (p+1)^{ap+by} \equiv (p+1)^{pa}(p+1)^{yb} \equiv 1 (\mathrm{mod}\, p^2).$$

Aber p^2 teilt nicht p, ein Widerspruch. Also ist $o(1+p) = p$ in $\mathbb{Z}/p^2\mathbb{Z}$.

Nach Satz III.7 gibt es in $\mathbb{Z}/p\mathbb{Z}$ ein Element g, dessen Potenzen genau die Elemente in $(\mathbb{Z}/p\mathbb{Z})^*$ sind, d.h., $(\mathbb{Z}/p\mathbb{Z})^*$ ist zyklisch. Also gibt es ein $g \in \mathbb{N}$ mit

$$g^{p-1} \equiv 1 (\mathrm{mod}\, p),$$

aber

$$g^x \not\equiv 1 (\mathrm{mod}\, p) \text{ für } 1 \leq x < p-1.$$

Da g und $p+1$ teilerfremd zu p^2 sind, ist nach dem Satz IV.17 von Euler

$$(g(p+1))^{p(p-1)} = (g(p+1))^{\varphi(p^2)} \equiv 1 (\mathrm{mod}\, p^2).$$

Sei y die Ordnung von g modulo p^2. Dann ist $g^y \equiv 1 (\mathrm{mod}\, p^2)$, also auch $g^y \equiv 1 (\mathrm{mod}\, p)$. Da g modulo p die Ordnung $p-1$ hat, ist nach Lemma III.3 $p-1$ ein Teiler von y. Weiter ist auch y ein Teiler von $\varphi(p^2)$. Damit ist $o(g) = p-1$ oder $o(g) = \varphi(p^2)$. Betrachte g^p. Es ist $g^p \equiv g (\mathrm{mod}\, p)$. Also ist $p-1$ ein Teiler der Ordnung von g^p modulo p^2. Wir können $o(g) = p-1$ annehmen, indem wir notfalls g durch g^p ersetzen. Nun folgt aber mit Lemma III.4 $o((p+1)g) = \varphi(p^2)$.

Setze $h = (p+1)g$. Dann ist mit $x = \varphi(p^2)$

$$h^x \not\equiv 1 (\mathrm{mod}\, p^2) \text{ für alle } 1 \leq x < \varphi(p^2). \qquad (*)$$

Sei $n = p^\alpha \cdot r$ mit ggT $(p, r) = 1$ und $\alpha > 1$. Nach dem Chinesischen Restsatz IV.18 hat

$$\begin{aligned} b &\equiv h (\mathrm{mod}\, p^\alpha) \\ b &\equiv 1 (\mathrm{mod}\, r) \end{aligned} \qquad (+)$$

eine Lösung $b \in \mathbb{Z}$.

Sei $1 \leq x < \varphi(p^2)$. Dann ist $b^x \equiv h^x (\mathrm{mod}\, p^2)$ und somit $b^x \not\equiv 1 (\mathrm{mod}\, p^2)$ nach $(*)$. Somit hat $b + p^2\mathbb{Z}$ die Ordnung $\varphi(p^2)$ in der Einheitengruppe von $\mathbb{Z}/p^2\mathbb{Z}$.

Da ggT $(h, p) = 1$ ist, ist auch ggT $(b, p) = 1$. Also ist ggT $(b, n) = 1$, da wegen $(+)$ ggT $(r, b) = 1$ ist. Mit diesem b gilt nun die Formel für die Carmichaelzahl n

$$b^{n-1} \equiv 1 (\mathrm{mod}\, n).$$

Dann ist insbesondere

$$b^{n-1} \equiv 1 (\mathrm{mod}\, p^2).$$

Also ist $\varphi(p^2)$ ein Teiler von $n-1$. Aber p teilt stets $\varphi(p^2)$. Da p ein Teiler von n war, kann p nicht gleichzeitig auch $n-1$ teilen.

Dieser Widerspruch zeigt, dass Carmichaelzahlen quadratfrei sind.

Wir zeigen nun, dass, falls p ein Teiler von n ist, stets $n-1$ von $p-1$ geteilt wird.

Sei g wie eben. Nach dem Chinesischen Restsatz IV.18 gibt es ein $b \in \mathbb{Z}$ mit

$$b \equiv g (\mathrm{mod}\, p)$$
$$b \equiv 1 (\mathrm{mod}\, \frac{n}{p}).$$

Wie eben folgt ggT $(b, n) = 1$. Also ist

$$b^{n-1} \equiv 1 (\mathrm{mod}\, n)$$

und dann auch

$$b^{n-1} \equiv 1 (\mathrm{mod}\, p).$$

Da aber die Ordnung von g und b modulo p gleich sind, folgt $\varphi(p) = p - 1 | n - 1$.

Schließlich bleibt noch zu zeigen, dass r, die Anzahl der Primteiler von n, mindestens 3 ist. Sei dazu $n = pq$. Wir können $p > q$ annehmen. Es ist, wie wir gerade gezeigt haben, $p - 1$ ein Teiler von $n - 1$. Nun ist

$$p - 1 | (p - 1)(q - 1) - (n - 1) = (p - 1)(q - 1) - (pq - 1) = -(p - 1) - (q - 1).$$

Dann ist aber $p - 1$ ein Teiler von $q - 1$, was $p > q$ widerspricht. □

Übungsaufgaben

IV.1 Bestimme alle $n \in \boldsymbol{N}$, so dass $2^{11} + 2^8 + 2^n = m^2$ für ein $m \in \boldsymbol{N}$ gilt.

IV.2 Seien A und B disjunkte nicht leere Mengen von Primzahlen. Setze

$$a = \prod_{p \in A} p \quad \text{und} \quad b = \prod_{p \in B} p.$$

Dann wird $a + b$ von einer Primzahl geteilt, die nicht in $A \cup B$ liegt. Insbesondere zeigt dies, dass es unendlich viele Primzahlen gibt. Kann man das gleiche Resultat auch mit $a - b$ erreichen?

IV.3 Für $m, n \in \mathbb{N}$ setze $B_{m,n} = m(n + 1) - (n! + 1)$ und

$$f(m, n) = \frac{n - 1}{2}(|(B_{m,n}^2 - 1)| - (B_{m,n}^2 - 1)) + 2.$$

Zeige, dass $f(m, n)$ immer eine Primzahl ist, dass jede Primzahl vorkommt und dass jede Primzahl ungleich 2 genau einmal vorkommt.

IV.4 Ist p eine Primzahl, so ist jeder Primteiler von $2^p - 1$ größer als p.

IV.5 Sei $p > 5$ eine Primzahl. Dann ist $p^4 - 1$ durch 240 teilbar.

IV.6 Bestimme für $i = 0, 2, 3$ und 4 jeweils das kleinste $x_i \in \mathbb{N}$, so dass die Gleichung $\varphi(n) = x_i$ genau i Lösungen n hat[12].

IV.7 Die Gleichung $\varphi(n^2) = k^2$ ist außer für $\varphi(1) = 1$ nicht lösbar.

IV.8 Sei $t = \varphi(5^{2n})$, $n \in \boldsymbol{N}$. Zeige, dass 2^{t+2n} in der Dezimaldarstellung mindestens n aufeinander folgende Nullen hat.

[12] Der Fall $i = 1$ ist offen. Die Vermutung ist, dass $\varphi(n) = x$ entweder keine oder mindestens zwei Lösungen hat.

IV.9 Sei p eine Primzahl, so dass $2p+1$ keine Primzahl ist. Dann hat $\varphi(x) = 2p$ keine Lösung x.

IV.10 a) Bestimme die letzten zwei Ziffern von $2^{1000000}$.

b) Auf welche Ziffer endet die Dezimaldarstellung von $2^{2^n} + 1$, für $n > 1$?

c) Wie lauten die beiden letzten Ziffern der Dezimaldarstellung von $3^{999} - 2^{999}$?

IV.11 a) Welchen Rest hat 4^{100} bei Division durch 7?

b) Welchen Rest hat 9! bei Division durch 10, und 10! bei Division durch 11, und 11! bei Division durch 12?

c) Sei $n + 1$ keine Primzahl. Was ist der Rest von $n!$ bei Division durch $n + 1$?

IV.12 Bestimme alle $x \in \mathbb{Z}$, die das folgende System von simultanen Kongruenzen lösen

$$\begin{aligned} x &\equiv 7 \pmod 8 \\ x &\equiv 2 \pmod 9 \\ x &\equiv -1 \pmod 5. \end{aligned}$$

V Gruppen

In diesem Kapitel beschäftigen wir uns mit einem zentralen Begriff der Algebra: den Gruppen. In den danach folgenden zwei Kapiteln werden wir an zwei Beispielen das Zusammenspiel der Begriffe „Gruppe“ und „Körper“ sehen. Wir setzen Kenntnisse der Gruppentheorie voraus, wie sie in einer Vorlesung über Lineare Algebra üblicherweise vermittelt werden. Weiter sind unsere Gruppen, wenn nicht ausdrücklich anders gesagt, stets endlich.

Definition

Index. Sei G eine Gruppe, U eine Untergruppe. Die Anzahl der Nebenklassen (siehe Seite 52) gU von U in G wird mit $|G\colon U|$ bezeichnet und *Index* von U in G genannt.

Im Satz III.2 von Lagrange, hatten wir gesehen, dass $|G| = |U||G\colon U|$ ist.

Das Analogon zum Gradsatz ist

Satz V.1

1. Kürzungssatz. *Seien G eine Gruppe und U eine Untergruppe von G. Ist weiter V eine Untergruppe von U, so gilt*

$$|G\colon V| = |G\colon U||U\colon V|.$$

Beweis. Es ist $|G\colon V| = \frac{|G|}{|V|}$, $|G\colon U| = \frac{|G|}{|U|}$ und $|U\colon V| = \frac{|U|}{|V|}$ nach Satz III.2. □

Wir wollen nun nicht nur Elemente, sondern auch Teilmengen in einer Gruppe multiplizieren. Dazu definieren wir:

Definition

Multiplikation. Seien $A, B \subseteq G$. Setze

$$AB = \{ab | a \in A, b \in B\}.$$

Die Frage ist, ob AB eine Untergruppe von G ist. Dies ist im Allgemeinen nicht so. Selbst wenn A und B Untergruppen von G sind, muss AB keine Untergruppe sein. Sei dazu G die Menge der bijektiven Abbildungen von $\{1, 2, 3\}$. Sei

$$f\colon 1 \to 1, 2 \to 3, 3 \to 2$$
$$g\colon 1 \to 2, 2 \to 1, 3 \to 3$$

und $A = \{id, f\}$, $B = \{id, g\}$. Dann sind A und B Untergruppen von G. Es ist $AB = \{id, fg, f, g\}$.

Dabei ist

$$fg\colon 1 \to 3, 3 \to 2, 2 \to 1.$$
$$gf = (fg)^{-1}\colon 1 \to 2, 2 \to 3, 3 \to 1, \text{ aber } (fg)^{-1} \notin AB.$$

Also ist AB keine Untergruppe von G.

Der nächste Satz gibt uns ein Kriterium, wann genau AB eine Untergruppe ist.

Lemma V.2 *Sind A, B Untergruppen von G, so ist AB genau dann eine Untergruppe von G, wenn $AB = BA$ ist.*

Beweis. Da $1 \cdot 1 \in AB$ ist, ist $AB \neq \varnothing$. Sei $AB = BA$. Weiter sei $a \in A$ und $b \in B$, also $ab \in AB$. Wir haben

$$(ab)^{-1} = b^{-1}a^{-1} \in BA = AB.$$

Also ist AB gegen Inversenbildung abgeschlossen.

Wir zeigen nun, dass AB auch gegen Multiplikation abgeschlossen ist. Seien dazu $a_1b_1 \in AB$ und $a_2b_2 \in AB$. Dann ist $a_1b_1a_2b_2 = a_1(b_1a_2)b_2$. Da $BA = AB$ ist, ist $b_1a_2 = a_3b_3$ mit geeigneten $a_3 \in A$, $b_3 \in B$.

Das liefert

$$a_1b_1a_2b_2 = (a_1a_3)(b_3b_2) \in AB.$$

Somit ist AB gegen Multiplikation abgeschlossen und dann eine Untergruppe.

Für die andere Richtung sei AB eine Untergruppe von G. Wir wählen $ab \in AB$ beliebig. Da AB eine Gruppe ist, ist $(ab)^{-1} \in AB$. Damit gilt $b^{-1}a^{-1} = a_1b_1$, mit geeigneten $a_1 \in A$, $b_1 \in B$, also $ab = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in BA$. Damit ist $AB \subseteq BA$.

Sei nun $b \in B$, $a \in A$. Dann sind

$$b = 1 \cdot b \in AB \quad \text{und} \quad a = a \cdot 1 \in AB.$$

Da AB nach Voraussetzung eine Untergruppe ist, ist auch

$$ba = (1 \cdot b)(a \cdot 1) \in AB.$$

Also ist $BA \subseteq AB$. □

Auch wenn AB keine Untergruppe ist, können wir dennoch die Anzahl der Elemente in AB bestimmen, was häufig sehr nützlich ist.

Lemma V.3 *Seien A, B Untergruppen von G. Dann gilt*

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Beweis. Sei

$$\dot{\bigcup_{r\in R}} r(A\cap B) = A$$

die Nebenklassenzerlegung nach den Nebenklassen von $A\cap B$ in A. Also $RB\subseteq AB$.

Sei $x = ab \in AB$, $a\in A$, $b\in B$, ein beliebiges Element. Es gibt ein $r\in R$ mit $a\in r(A\cap B)$. Damit ist $a = ry$, $y\in A\cap B\leq B$. Insgesamt haben wir

$$x = ab = r(yb)\in rB.$$

Das liefert

$$AB = \bigcup_{r\in R} rB.$$

Wir wollen zeigen, dass dies eine disjunkte Zerlegung ist. Seien dazu $r_1, r_2\in R$ und $r_1B\cap r_2B\neq\varnothing$. Dann ist

$$r_1b_1 = r_2b_2 \quad \text{für geeignete} \quad b_1, b_2\in B.$$

Also ist

$$r_2^{-1}r_1 = b_2b_1^{-1}\in A\cap B.$$

Das liefert

$$r_1(A\cap B) = r_2(A\cap B)$$

und dann

$$r_1 = r_2,$$

da die r_i in einem Nebenklassenvertretersystem von $A\cap B$ in A sind. Also ist die Zerlegung disjunkt.

Da die Multiplikation mit Gruppenelementen eine bijektive Abbildung ist, ist $|rB| = |B|$. Damit erhalten wir

$$|AB| = \sum_{r\in R}|rB| = |R||B| = |A\colon A\cap B||B| \underset{(3.2)}{=} \frac{|A||B|}{|A\cap B|}.$$

□

Wie in der Theorie der Vektorräume können wir auch bei Gruppen Faktorstrukturen einführen.

Definition

Normalteiler, Faktorgruppe. Sei G eine Gruppe und $N\leq G$.

a) Gilt für alle $g\in G$ stets $gN = Ng$, so nennen wir N einen *Normalteiler* von G. Wir schreiben dann $N\trianglelefteq G$.

b) Sei N ein Normalteiler von G. Setze $G/N = \{gN | g\in G\}$. Wir definieren auf G/N eine Verknüpfung $\circ$ durch

$$(g_1N)\circ(g_2N) = (g_1N)(g_2N) = (g_1g_2)N.$$

Wir nennen G/N die *Faktorgruppe* von G nach N.

In der Tat ist G/N eine Gruppe, wie man leicht nachrechnet. Das einzige Bemerkenswerte ist, dass die Verknüpfung wohldefiniert ist. Es ist mit der eingangs definierten Multiplikation von Mengen

$$g_1Ng_2N = \{g_1n_1g_2n_2 | n_1, n_2 \in N\}.$$

Da $N \trianglelefteq G$ ist, ist $n_1g_2 = g_2\tilde{n}_1$ mit geeignetem $\tilde{n}_1 \in N$. Also ist

$$g_1Ng_2N = \{g_1g_2\tilde{n}_1n_2 | \tilde{n}_1, n_2 \in N\} = (g_1g_2)N.$$

Dies zeigt auch, dass die Eigenschaft, Normalteiler zu sein, notwendig ist, damit die Menge $\{gN | g \in G\}$ mit der Multiplikation von Mengen eine Gruppe ist. Wir können auf diese Weise nicht eine Faktorgruppe für beliebige Untergruppen N definieren. Dies wird keine Gruppe sein. Bei Vektorräumen werden in der Linearen Algebra für beliebige Unterräume Faktorräume definiert. Dass dies möglich ist, liegt daran, dass die additive Gruppe eines Vektorraumes abelsch ist, also jede Untergruppe ein Normalteiler ist.

Satz V.4

Sei G eine Gruppe, $N \trianglelefteq G$. Dann ist

$$|G/N| = |G:N|$$

Beweis. Dies folgt aus der Definition von G/N. □

Die Menge der Normalteiler verhält sich besser als die Menge der Untergruppen. Sie ist nicht nur gegen Durchschnittsbildung, sondern auch gegen Multiplikation abgeschlossen, wie der nächste Satz zeigt:

Satz V.5

Sei G eine Gruppe. Dann gilt:

a) Sind $N_i \trianglelefteq G$, $i \in I$, so ist $\bigcap_{i\in I} N_i \trianglelefteq G$.

b) Ist $N \trianglelefteq G$ und $U \leq G$, so ist $N \cap U \trianglelefteq U$ und NU ist eine Untergruppe von G.

c) Sind $N_1, N_2 \trianglelefteq G$, so ist $N_1N_2 \trianglelefteq G$.

Beweis.

a) Sei $n \in \bigcap_{i\in I} N_i$, $g \in G$. Dann haben wir

$$g^{-1}ng \in N_i, \quad \text{für alle} \quad i.$$

Dies liefert

$$g^{-1}ng \in \bigcap_{i\in I} N_i,$$

also

$$\left(\bigcap_{i\in I} N_i\right) g = g\left(\bigcap_{i\in I} N_i\right).$$

Damit ist $\bigcap_{i\in I} N_i$ ein Normalteiler.

b) Sei $u \in U$. Wir zeigen $u(U \cap N) = (U \cap N)u$. Sei dazu $n \in U \cap N$. Dann ist $un = n'u$ mit geeignetem $n' \in N$. Nun ist $n' = unu^{-1} \in U \cap N$, d.h. $u(U \cap N) = (U \cap N)u$. Also ist $U \cap N \trianglelefteq U$.

Da $uN = Nu$ für alle $u \in U$ ist, ist $UN = NU$. Nach Lemma V.2 ist damit UN eine Untergruppe von G.

c) Nach b) ist N_1N_2 eine Untergruppe von G. Sei $g \in G$. Dann ist

$$g(N_1N_2) = (N_1g)N_2 = (N_1N_2)g,$$

also ist N_1N_2 ein Normalteiler. □

Der nächste Satz ist fundamental für die Konstruktion von Normalteilern.

Satz V.6

Seien G, H Gruppen und $f: G \to H$ ein Homomorphismus. Dann ist

$$\ker f := \{x | x \in G, f(x) = 1\}$$

ein Normalteiler von G.

Beweis. Da $f(1) = 1$ ist, ist $\ker f \neq \varnothing$. Sind $a, b \in \ker f$, so ist

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

Also ist $ab^{-1} \in \ker f$ und damit ist $\ker f$ eine Untergruppe von G. Seien nun $x \in \ker f$ und $g \in G$. Dann ist

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g) = f(g^{-1})f(g) = f(g^{-1}g) = 1.$$

Das liefert $g^{-1}xg \in \ker f$ und somit ist $\ker f \trianglelefteq G$. □

Lemma V.7

Seien G, H Gruppen, $f: G \to H$ ein Homomorphismus. Dann ist f genau dann ein Monomorphismus, wenn $\ker f = \{1\}$ ist.

Beweis. Ist f ein Monomorphismus, so hat $1 \in H$ nur $1 \in G$ als Urbild, also ist $\ker f = \{1\}$.

Sei umgekehrt $\ker f = \{1\}$. Seien $a, b \in G$ mit

$$f(a) = f(b).$$

Dann ist $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1$, also $ab^{-1} \in \ker f$ und damit $ab^{-1} = 1$, d.h.

$$a = b.$$

□

Genau wie bei Ringen haben wir auch bei Gruppen einen Homomorphiesatz, auf dessen Beweis wir hier aber verzichten wollen.

Satz V.8

Homomorphiesatz. *Seien G, H Gruppen und $f: G \to H$ ein Homomorphismus. Dann ist*

$$\text{Bild } f \cong G/\ker f.$$

Wir wollen jetzt zwei schöne Anwendungen des Homomorphiesatzes beweisen.

Satz V.9

a) Seien G eine Gruppe, U eine Untergruppe von G und N ein Normalteiler von G. Dann ist

$$U/U \cap N \cong UN/N.$$

b) (2. Kürzungssatz) *Seien G eine Gruppe und M und N Normalteiler von G mit $N \leq M$. Dann ist*

$$(G/N)\big/(M/N) \cong G/M.$$

Beweis. Die Idee in beiden Teilen ist gleich. Wir definieren eine Abbildung von U bzw. G/N auf die Gruppe auf der rechten Seite von $\cong$ mit Kern $U \cap N$ bzw. M/N. Die Behauptung folgt dann mit dem Homomorphiesatz.

a) Wir definieren zunächst durch $f(u) = uN$ für $u \in U$. eine Abbildung

$$f\colon U \to NU/N.$$

Da $uNvN = uvN$ für alle $u, v \in U$ ist, ist f ein Homomorphismus. Weiter ist

$$\text{Bild}\, f = NU/N.$$

Ist $u \in \ker f$, so gilt

$$N = f(u) = uN.$$

Also ist $u \in N$ und dann $\ker f \leq U \cap N$. Sei nun umgekehrt $u \in U \cap N$. Dann erhalten wir $f(u) = uN = N$. Zusammen ergibt dies

$$\ker f = U \cap N.$$

Nun folgt die Behauptung mit dem Homomorphiesatz.

b) Entsprechend wie eben definieren wir durch $f(gN) = gM$ für $g \in G$ eine Abbildung

$$f\colon G/N \to G/M.$$

Da gN das Element g nicht eindeutig bestimmt, müssen wir zeigen, dass f eine Abbildung ist.

Sei dazu $g_1N = g_2N$. Dann ist $g_1^{-1}g_2 \in N \subseteq M$, also ist dann $g_1M = g_2M$, und somit erhalten wir

$$f(g_1N) = g_1M = g_2M = f(g_2N).$$

Damit ist gezeigt, dass $f(gN)$ von der Auswahl von g unabhängig ist.Dass f ein Homomorphismus mit Bild $f = G/M$ ist, ist per Definition von f klar.

Es bleibt zu zeigen, dass $\ker f = M/N$ ist.

Sei zuerst $gN \in \ker f$. Wir erhalten

$$M = f(gN) = gM.$$

Das liefert $g \in M$, also $gN \in M/N$.
Sei jetzt umgekehrt $mN \in M/N$, $m \in M$. Dann erhalten wir

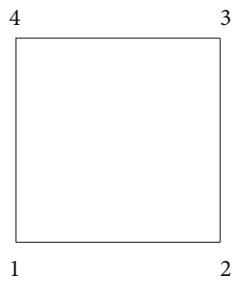
$$f(mN) = mM = M.$$

Somit ist $mN \in \ker f$ und dann $\ker f = M/N$. Nun folgt die Behauptung mit dem Homomorphiesatz. □

Bemerkung.

a) Sei U eine Untergruppe von G mit $|G:U| = 2$. Dann ist $G = U \cup Ug$ für $g \in G \backslash U$.
Es ist aber auch $G = U \cup gU$, da $|G| - |U| = |U|$ ist, also $|gU| = |G| - |U|$ und $gU \cap U = \varnothing$.
Somit ist $Ug = gU$ für alle $g \in G$. Das heißt $U \trianglelefteq G$.

b) Wir werden jetzt sehen, dass der Normalteilerbegriff nicht transitiv ist. Dies bedeutet, dass aus $N_1 \trianglelefteq N_2 \trianglelefteq G$, nicht notwendig folgt, dass $N_1 \trianglelefteq G$ ist!
Dazu betrachten wir ein konkretes Beispiel. Wir bestimmen zunächst die Gruppe G der Symmetrien des Quadrates.



Drehung	d:	$1 \to 2 \to 3 \to 4 \to 1$
	d^2:	$1 \to 3 \to 1,2 \to 4 \to 2$
	d^3:	$1 \to 4 \to 3 \to 2 \to 1$
Spiegelung	s:	$1 \to 1,3 \to 3,2 \to 4 \to 2$
	ds:	$1 \to 2 \to 1,3 \to 4 \to 3$
	d^2s:	$1 \to 3 \to 1,2 \to 2,4 \to 4$
	d^3s:	$1 \to 4 \to 1,2 \to 3 \to 2$
	id:	$1 \to 1,2 \to 2,3 \to 3,4 \to 4$

Dies sind alle Symmetrien. Warum?
Es ist $U = \{id, s, d^2, sd^2\}$ eine Untergruppe von G. Da $|G:U| = 2$ ist, ist $U \trianglelefteq G$ nach a). Da U abelsch ist, ist $V = \{id, s\} \trianglelefteq U$. Aber $dV = \{d, ds\} \neq Vd = \{d, sd\}$, da $sd = d^3s \neq ds$ ist. Somit ist V nicht normal in G.

Wie in der Linearen Algebra für Vektorräume definieren wir nun auch für Gruppen G das Erzeugnis einer Teilmenge von G.

Definition

Erzeugnis. Sei G eine Gruppe und $M \subseteq G$. Setze

$$\langle M\rangle = \bigcap_{\substack{M \subseteq U \\ U \leq G}} U.$$

Wir nennen $\langle M\rangle$ das *Erzeugnis* von M. Es ist die kleinste Untergruppe von G, die M enthält.

Man sieht leicht

$$\langle M\rangle = \{1, x_1 \cdots x_n | x_i \in M \text{ oder } x_i^{-1} \in M,\ n \in \mathbb{N}\}.$$

Definition

Zyklisch. Eine Gruppe G nennen wir *zyklisch*, falls es ein $g \in G$ mit $G = \langle g\rangle$ gibt. Das Element g nennen wir dann auch ein erzeugendes Element.

Wir hatten in Kapitel III für endliches G diese Definition bereits gegeben (siehe Lemma III.5). Wir sind jetzt in der Lage, alle zyklischen Gruppen anzugeben, auch die unendlichen.

Satz V.10

Sei G eine zyklische Gruppe, so gilt:

a) Ist $|G| = \infty$, so ist $G \cong \mathbb{Z}$.

b) Ist $|G| = n < \infty$, so ist $G \cong \mathbb{Z}/n\mathbb{Z}$.

Beweis. Da G zyklisch ist, ist $G = \langle g\rangle = \{g^i | i \in \mathbb{Z}\}$. Sei

$$f: \mathbb{Z} \to G \text{ mit } f(i) = g^i.$$

Offenbar ist f ein Epimorphismus. Sei $0 \neq i \in \ker f$. Dann erhalten wir

$$1 = f(i) = g^i,$$

also ist $o(g)|i$, d.h., G ist endlich. Ist also G nicht endlich, so ist f ein Isomorphismus. Das ist a).

Sei nun $|G| = n$. Nach Lemma III.3 ist $o(g) = n|i$. Also ist $i \in n\mathbb{Z}$. Sei nun $i \in n\mathbb{Z}$, d.h. $i = nj$. Dann ist $f(i) = g^{nj} = 1$. Also ist $\ker f = n\mathbb{Z}$. Die Behauptung b) folgt nun mit dem Homomorphiesatz. □

Dieser Satz ist typisch für weite Bereiche der Gruppentheorie. Wir haben eine Eigenschaft, hier „zyklisch“, und wir klassifizieren alle Gruppen, die diese Eigenschaft haben, in Form einer Aufzählung. Danach können wir Fragen über zyklische Gruppen beantworten, indem wir diese in den Beispielen beantworten.

Wir wollen jetzt noch eine besonders wichtige Gruppe, die symmetrische Gruppe, eingehend studieren.

Definition

Symmetrische Gruppe. Sei $\Omega = \{1, \ldots, n\}$ und Σ_n die Menge aller bijektiven Abbildungen von Ω. Die Menge Σ_n nennen wir die *symmetrische Gruppe* auf Ω und ihre Elemente Permutationen. Für die Abbildung $g \in \Sigma_n$ führen wir die folgende Schreibweise ein

$$g = \begin{pmatrix} i_1 & \cdots & \cdots & i_n \\ g(i_1) & \cdots & \cdots & g(i_n) \end{pmatrix}, \{i_1, \cdots, i_n\} = \Omega.$$

Satz V.11

$|\Sigma_n| = n!$

Beweis. Sei $g \in \Sigma_n$. Offenbar kann $g(1)$ jede der Zahlen $1, \ldots, n$ sein, also gibt es für $g(1)$ genau n Möglichkeiten. Da g injektiv ist, ist $g(1) \neq g(2)$. Also kann $g(2)$ jeden Wert außer $g(1)$ annehmen. Somit gibt es für $g(2)$ genau $n-1$ Möglichkeiten. Allgemein liefert nun die Injektivität, dass

$$g(i) \in \Omega \setminus \{g(1), \ldots, g(i-1)\}$$

ist. Damit gibt es $n - (i-1)$ viele Möglichkeiten für $g(i)$. Somit gibt es zusammen $\prod_{i=1}^{n} i = n!$ viele Möglichkeiten für g. □

Definition

Zyklus. Kann man die Zahlen $1, \ldots, n$ so als $m_1, m_2, \ldots m_k, \ldots m_n$ anordnen, dass die Permutation z die Form

$$z = \begin{pmatrix} m_1 & m_2 & \cdots & m_{k-1} & m_k & m_{k+1} & \cdots & m_n \\ m_2 & m_3 & \cdots & m_k & m_1 & m_{k+1} & \cdots & m_n \end{pmatrix}$$

hat, so nennen wir z einen *k-Zyklus*. Wir schreiben dafür vereinfachend

$$z = (m_1, m_2, \ldots, m_k).$$

Ein 2-Zyklus heißt auch *Transposition*.

Satz V.12

Zyklenzerlegung. *Sei $g \in \Sigma_n$.*

a) Wir können $\{1, \ldots, n\}$ als disjunkte Vereinigung von Mengen $M_1, \ldots, M_t$ schreiben, so dass bei geeigneter Anordnung der Elemente $m_{i_1}, \ldots, m_{i_{k_i}}$ in M_i das Element g als Produkt der Zyklen $(m_{i_1}, \ldots, m_{i_{k_i}})$, $i = 1, \ldots, t$, geschrieben werden kann.

b) Ist $n \geq 2$, so ist g ein Produkt von Transpositionen.

Beweis. Wir führen eine Relation $\sim$ auf $\{1, \ldots, n\}$ ein:

$i \sim j$ genau dann, falls es ein $k \in \mathbb{N} \cup \{0\}$ gibt, so dass $g^k(i) = j$ ist.

$\sim$ ist eine Äquivalenzrelation: Klar ist $i \sim i$. Weiter ist auch klar, dass aus $i \sim j$ und $j \sim k$, sofort $i \sim k$ folgt.

Sei nun $i \sim j$. Wir wollen $j \sim i$ zeigen. Es ist dann $g^k(i) = j$ für ein $k \in \mathbb{N} \cup \{0\}$. Dann gilt natürlich $j = g^{-k}(i)$. Allerdings ist für $k \neq 0$ dann $-k \notin \mathbb{N} \cup \{0\}$. Um diesem Problem aus dem Weg zu gehen, wenden wir einen kleinen Trick an. Sei $m = o(g)$ und $s \in \mathbb{N}$ mit $sm > k$. Dann ist $sm - k \in \mathbb{N}$ und $g^{sm-k}(j) = g^{-k}(j) = i$. Also ist $j \sim i$.

Seien $M_1, \ldots, M_t$ die Äquivalenzklassen von $\sim$. Wähle $m_{i_1} \in M_i$. Dann ist $M_i = \{g^s(m_{i_1}) | s \in \mathbb{N} \cup \{0\}\}$.

Die Behauptung folgt jetzt mit $g = \prod_{i=1}^{t} g_{|M_i}$.

b) Es genügt nach a), die Behauptung für einen Zykel $(m_1, \ldots, m_k)$ zu zeigen.
Ist $k = 1$, so ist $(m_1) = (m_1, m_2)(m_1, m_2)$.
Ist $k > 1$, so ist

$$(m_1, \ldots, m_k) = (m_1, m_k)(m_1, m_{k-1}) \cdots (m_1, m_2). \qquad \square$$

Die letzte Zeile des Beweises bedarf noch eines Kommentars. Ein Produkt von Permutationen lesen wir wie eine Hintereinanderausführung von Abbildungen, also von rechts nach links, während wir einen Zyklus von links nach rechts lesen. Dies ist nicht in allen Büchern so. Es beeinflußt zwar nicht die qualitativen, aber die quantitativen Resultate.

Die Anzahl der Zyklen in der Zyklenzerlegung a) ist eindeutig durch g bestimmt, es ist ja die Anzahl der Äquivalenzklassen. Das Gleiche gilt für die Zyklen selbst. Die Zyklenzerlegung ist also bis auf die Reihenfolge eindeutig. Anders sieht das mit den Transpositionen aus. Die Anzahl der Transpositionen in b) ist nicht eindeutig.

$$(1, 3) = (1, 2)(1, 3)(2, 3).$$

Den nachfolgenden schönen Beweis findet man in Neumann et al. (1994, [21]).

Satz V.13

Seien $h_1, \ldots, h_r \in \Sigma_n$ Transpositionen und $g \in \Sigma_n$.

a) Hat $h_1 h_2 \cdots h_r$ in der Zyklenzerlegung genau c Zyklen (Zyklen der Länge 1 zählen mit), so ist

$$r \equiv n - c \pmod 2.$$

b) Setze

$$\operatorname{sgn}(g) = (-1)^{x(g)},$$

wobei $x(g)$ die Anzahl der Transpositionen in einer Darstellung von g als Produkt von Transpositionen ist. Dann ist

$$\operatorname{sgn} : \Sigma_n \to \{1, -1\}$$

ein Epimorphismus. Dabei ist $\{1, -1\}$ mit der Multiplikation reeller Zahlen eine Gruppe.

Beweis.

a) Wir beweisen die Behauptung durch Induktion nach r. Ist $r = 0$, so ist die Behauptung offenbar richtig, da das Produkt von Null-Transpositionen die Identität ist. Also gilt $c = n$.

Sei $r > 0$. Setze $f = h_1 h_2 \cdots h_r$ und $g = h_2 \cdots h_r$. Sei

$$g = (\alpha_1, \ldots, \alpha_{b_1})(\beta_1, \cdots, \beta_{b_1}) \ldots (\lambda_1, \ldots, \lambda_{b_d})$$

die Zyklenzerlegung von g, d.h., g hat genau d Zyklen. Per Induktion ist

$$r - 1 \equiv n - d \pmod 2.$$

Die Zyklen können in jeder Reihenfolge geschrieben werden und jeder Zyklus kann an jeder Stelle starten. Also können wir $h_1 = (\alpha_1, \alpha_{s+1})$ annehmen, falls beide Einträge im gleichen Zykel liegen, und anderenfalls $h_1 = (\alpha_1, \beta_1)$.

Im ersten Fall ist

$$f = h_1 g = (\alpha_1, \ldots, \alpha_s)(\alpha_{s+1}, \ldots, \alpha_{b_1})(\beta_1, \ldots, \beta_{b_2}) \ldots$$

also $c = d + 1$ und dann $r \equiv n - d - 1 \equiv n - c \pmod 2$.

Im zweiten Fall ist

$$f = h_1 g = (\alpha_1, \ldots, \alpha_{b_1}, \beta_1, \ldots, \beta_{b_2})(\gamma_1, \ldots, \gamma_{b_3}) \ldots$$

also $c = d - 1$ und dann $r \equiv n - d + 1 \equiv n - c \pmod 2$.

b) Sei $f \in \Sigma_n$. Ist f das Produkt von r und auch von s vielen Transpositionen, so ist nach a)

$$r \equiv n - c \equiv s \pmod 2.$$

Also ist $x(f)$ modulo 2 eindeutig bestimmt. Dies bedeutet, sgn ist eine Abbildung. Da $\operatorname{sgn}(1, 2) = -1$ ist, ist sgn surjektiv.

Seien $g, h \in \Sigma_n$. Dann kann gh als Produkt von $x(g) + x(h)$ vielen Transpositionen geschrieben werden, indem man die entsprechenden Darstellungen einfach aneinanderhängt. Also ist

$$\operatorname{sgn} gh = (-1)^{x(g)+x(h)} = (-1)^{x(g)}(-1)^{x(h)} = \operatorname{sgn} g \operatorname{sgn} h. \qquad \square$$

Definition

Signum. Die Abbildung aus Satz V.13 b) wird *Signumsabbildung* genannt. Eine Permutation g mit $\operatorname{sgn} g = 1$ nennen wir eine gerade Permutation, eine mit $\operatorname{sgn} g = -1$ ungerade. Für den Kern der Signumsabbildung schreiben wir A_n und nennen ihn die *alternierende Gruppe*.

Das nächste Lemma liefert eine einfache Methode, um das Signum einer Permutation zu berechnen.

Lemma V.14

Ist $g = z_1, \cdots z_t \in \Sigma_n$, wobei die z_i Zyklen der Länge k_i sind, so ist

$$\operatorname{sgn} g = \prod_{i=1}^{t} (-1)^{k_i - 1}.$$

Beweis. Wegen Satz V.13 genügt es, die Behauptung für einen Zyklus g der Länge k zu zeigen. Im Beweis von Satz V.12 b) haben wir gesehen, dass ein solcher ein Produkt von $k-1$ Transpositionen ist. Da die Signumsabbildung ein Homomorphismus ist und jede Transposition das Signum -1 hat, ist

$$\operatorname{sgn} g = (-1)^{k-1}. \qquad \square$$

Die Berechnung des Signums ist also ganz einfach. Ist die Anzahl der Zyklen gerader Länge ungerade, so ist das Signum gleich –1, sonst gleich +1.

Bemerkung.

a) Nach dem Homomorphiesatz V.8 ist $\Sigma_n/A_n \cong \text{Bild sgn}$. Also ist $|A_n| = \frac{n!}{2}$.

b) Ist $n \neq 1, 2, 4$, so sind $\{1\}$, A_n, Σ_n die einzigen Normalteiler von Σ_n. Siehe dazu auch Satz V.21 und Satz V.23.

Lemma V.15

a) Sei Ω eine Menge und G eine Gruppe von bijektiven Abbildungen von Ω. Für $a \in \Omega$ setze

$$G_a = \{g | g \in G, g(a) = a\}.$$

Dann ist G_a eine Gruppe und $|G: G_a| = |\{g(a) | g \in G\}|$. Wir nennen G_a den Stabilisator von a in G.

b) Ist G eine Gruppe und U eine Untergruppe von G, so setze

$$N_G(U) = \{g | g \in G, gUg^{-1} = U\}$$

(Normalisator von U in G). Es ist $N_G(U)$ eine Untergruppe von G. Für den Index erhalten wir

$$|G: N_G(U)| = |\{gUg^{-1} | g \in G\}|.$$

Beweis.

a) Sei 1 das Einselement von G. Dann ist $1 \in G_a$. Also ist $G_a \neq \varnothing$. Seien nun $g, h \in G_a$. Dann ist

$$gh(a) = g(a) = a.$$

Damit ist $gh \in G_a$. Weiter ist

$$a = g^{-1}g(a) = g^{-1}(a)$$

und dann $g^{-1} \in G_a$. Somit ist G_a eine Untergruppe von G. Damit ist die erste Behauptung bewiesen.

Zum Beweis der zweiten Behauptung definieren wir eine Abbildung τ von der Menge der Nebenklassen von G_a in G in die Menge $\{g(a) | g \in G\}$ durch

$$\tau(gG_a) = g(a), \quad g \in G.$$

Ist $gG_a = hG_a$, so ist $h = gx$ mit $x \in G_a$. Also ist $h(a) = g(a)$. Somit ist τ eine Abbildung.

Wir wollen zeigen, dass τ injektiv ist. Sei dazu $g(a) = h(a)$. Dann erhalten wir $h^{-1}g(a) = a$, was $h^{-1}g \in G_a$ liefert. Insbesondere haben wir $gG_a = hG_a$. Somit ist τ injektiv und damit

$$|G\colon G_a| = |\text{Bild } \tau| = |\{g(a)|g \in G\}|.$$

b) Wir betrachten die Menge $\Omega = \{gUg^{-1}|g \in G\}$. Für jedes $h \in G$ definieren wir eine Operation auf Ω durch

$$h(gU^{-1}g) = hgUg^{-1}h^{-1} = (hg)U(hg)^{-1}.$$

Dadurch wird G zu einer Gruppe bijektiver Abbildungen von Ω. Indem wir a) auf das Element $U \in \Omega$ anwenden, erhalten wir

$$G_U = \{g \mid g(U) = U\} = \{g \mid gUg^{-1} = U\} = N_G(U).$$

Damit folgen die Behauptungen mit a). □

Der folgende Satz ist für die endliche Gruppentheorie sehr wichtig und wird dann im nächsten Satz, dem fundamentalen Satz der endlichen Gruppentheorie schlechthin, fortgesetzt.

Cauchy[1]**.** *Sei G eine Gruppe und sei p eine Primzahl mit $p||G|$. Dann besitzt G ein Element x mit $o(x) = p$.* Satz V.16

Beweis. **James McKay [18].** Sei

$$E = \{(x_1, \ldots, x_p)|x_i \in G, x_1 \cdots x_p = 1 \text{ und } (x_1, \ldots, x_p) \neq (1, \ldots, , 1)\}.$$

Sei weiter $\langle g\rangle = \mathbb{Z}/p\mathbb{Z}$. Wir definieren eine Operation von g auf E durch

$$(x_1, \ldots, x_p)^g = (x_2, \ldots, x_p, x_1).$$

Dadurch wird $\langle g\rangle$ zu einer Gruppe bijektiver Abbildungen auf E. Denn ist $x_1 \cdots x_p = 1$, so ist $x_2 \cdots x_p = x_1^{-1}$ und dann auch $x_2 \cdots x_p x_1 = 1$, also ist $(x_2, \cdots, x_p, x_1) \in E$.

Sei $a \in E$. Dann ist $\langle g\rangle_a$ eine Untergruppe von $\langle g\rangle$ nach Lemma V.15 a). Nach dem Satz von Lagrange ist

$$|\langle g\rangle_a| \text{ ein Teiler } |\langle g\rangle| = p.$$

Also ist

$$\langle g\rangle_a = 1 \text{ oder } \langle g\rangle_a = \langle g\rangle.$$

Für $a \in E$ setze $a^{\langle g\rangle} = \{a^x \mid x \in \langle g\rangle\}$. Nach Lemma V.15b) ist $|a^{\langle g\rangle}| = 1$ oder p. Es ist $E = \dot{\bigcup}_{a\in E} a^{\langle g\rangle}$. Da $|E| = |G|^{p-1} - 1$ ist, ist $p \not| |E|$. Somit gibt es ein $a \in E$ mit $|a^{\langle g\rangle}| = 1$.

[1] Augustin Louis Cauchy (*21.8.1789 Paris, †23.5 1857 Sceaux) war Ingenieur zur Zeit Napoleons und Professor in Paris, mit Unterbrechungen, da er keinen Eid auf den König schwören wollte. Fundamentale Arbeiten zur Algebra, Infinitesimalrechnung und zur mathematischen Physik. Mit ca. 700 Arbeiten ist sein Werk außergewöhnlich umfangreich.

Nach Lemma V.15 ist $\langle g\rangle_a = \langle g\rangle$. Dann ist aber

$$a = (x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1),$$

was

$$a = (x, \ldots, x)$$

liefert. Da $a \in E$ ist, ist $x^p = 1$ und $x \neq 1$. □

Wir kommen nun zu dem fundamentalen Satz der endlichen Gruppentheorie.

Satz V.17

Sylowsatz[2]. *Sei G eine Gruppe und p eine Primzahl mit $|G| = p^a m$, wobei m nicht durch p geteilt wird. Dann gilt:*

a) Es gibt eine Untergruppe U von G mit $|U| = p^a$.

b) Alle Untergruppen U von G mit $|U| = p^a$ sind konjugiert (d.h., sind U_1, U_2 Untergruppen mit $|U_1| = |U_2| = p^a$, so gibt es ein $g \in G$ mit $gU_1g^{-1} = U_2$).

c) Ist V eine Untergruppe von G mit $|V| = p^b$ für ein b, so gibt es eine Untergruppe U mit $|U| = p^a$ und $V \leq U$.

d) Die Anzahl der Untergruppen U mit $|U| = p^a$ ist $|G\colon N_G(U)|$ und kongruent 1 modulo p.

Beweis. Der Beweis folgt der Darstellung von Aschbacher (1984, Seite 19 [3]).
Sei

$$\mathcal{P} = \{U | U \leq G, |U| = p^c \text{ für ein } c\}$$

und $\mathcal{M}$ die Menge der maximalen Elemente in $\mathcal{P}$ bezüglich Inklusion.

Es ist $\langle 1\rangle$ eine p-Gruppe der Ordnung p^0. Somit ist $\mathcal{P} \neq \varnothing$ und dann auch $\mathcal{M} \neq \varnothing$. Wir definieren eine Operation von G auf $\mathcal{M}$ durch $g(U) = gUg^{-1}$ für $U \in \mathcal{M}$. Diese Operation hatten wir schon einmal im Beweis von Lemma V.15 b) gesehen. Wir müssen uns jetzt aber überlegen, ob $\mathcal{M}$ bezüglich dieser Operation invariant ist. Sei $gUg^{-1} \notin \mathcal{M}$ für ein $U \in \mathcal{M}$ und ein $g \in G$. Dann gibt es eine p–Untergruppe V von G mit $gUg^{-1} < V$. Dann ist aber auch $U < g^{-1}Vg$. Da $|V| = |g^{-1}Vg|$ ist, wäre dann U nicht maximal, was der Wahl $U \in \mathcal{M}$ widerspricht. Also haben wir eine Operation auf $\mathcal{M}$ definiert.

Seien $U, V \in \mathcal{M}$, $U \neq V$. Da beide maximal sind, ist $U \neq U \cap V \neq V$. Wäre $V \leq N_G(U)$, so wäre nach Satz V.5 UV eine Untergruppe von G. Nach Lemma V.3 ist

$$|UV| = \frac{|U||V|}{|U \cap V|}$$

eine p–Potenz, was der Maximalität von U widerspricht. Also ist $V \not\leq N_G(U)$.

[2] Peter Ludwig Sylow (*12.12.1832 Christiana, †7.9.1918 Oslo) wirkte als Lehrer bis 1898, erhielt 1898 eine Professur an der Universität Christiana. Wichtigstes Arbeitsgebiet war die Gruppentheorie, daneben auch die Theorie der elliptischen Funktionen.

Sei $\mathcal{N}$ eine unter G invariante Teilmenge von $\mathcal{M}$. Ist also $H \in \mathcal{N}$, $g \in G$, so ist $gHg^{-1} \in \mathcal{N}$. Wir halten ein $H \in \mathcal{N}$ fest. Dann operiert H auf $\mathcal{M} \setminus \mathcal{N}$. Nun kann H keinen Fixpunkt auf $\mathcal{M} \setminus \mathcal{N}$ haben. Wäre U ein solcher, so wäre $hUh^{-1} = U$ für alle $h \in H$. Dann wäre aber $H \leq N_G(U)$. Da $H \neq U$ ist, geht dies nicht, wie wir vorhin gesehen haben. Nach Lemma V.15 b) sind die Längen der Bahnen von H auf $\mathcal{M} \setminus \mathcal{N}$ Teiler der Ordnung von H. Da H eine p–Gruppe ist, sind sie also Potenzen von p. Da alle nicht trivial sind, ist

$$p \text{ ein Teiler von } |\mathcal{M} \setminus \mathcal{N}|.$$

Sei nun $H_1 \in \mathcal{M} \setminus \mathcal{N}$. Dann folgt wie eben, dass H_1 der einzige Fixpunkt von H_1 auf $\mathcal{M} \setminus \mathcal{N}$ ist. Also ist wieder

$$p \text{ ein Teiler von } |\mathcal{M} \setminus \mathcal{N}| - 1.$$

Das ist aber nicht möglich.

Somit sehen wir, dass $\mathcal{M}$ die einzige G-invariante Teilmenge von $\mathcal{M}$ ist. Das heißt, alle Elemente in $\mathcal{M}$ sind konjugiert und haben somit die gleiche Ordnung. Weiter ist U der einzige Fixpunkt für $U \in \mathcal{M}$, d.h. $|\mathcal{M}| \equiv 1 (\mathrm{mod}\, p)$.

Nach Lemma V.15 ist $|\mathcal{M}| = |G : N_G(U)|$. Da $|\mathcal{M}|$ nicht durch p geteilt wird, ist $p^a || N_G(U)|$. Da U eine maximale p-Untergruppe war, folgt mit dem Satz von Cauchy, dass $|N_G(U)/U|$ nicht von p geteilt wird. Also ist $|U| = p^a$. □

Definition

Sylowgruppen. Die Gruppen U, deren Existenz wir in Satz V.17 nachgewiesen haben, nennen wir *Sylow p-Untergruppen* von G.

Beispiel

Wir wollen hier einige typische Anwendungen des Sylowsatzes aufzeigen.

a) Sei $|G| = 20 = 4 \cdot 5$. Sei S eine Sylow 5-Untergruppe von G. Dann ist

$$|G : N_G(S)| \text{ ein Teiler von } |G : S| = 4.$$

Da nach dem Sylowsatz $|G : N_G(S)| \equiv 1 (\mathrm{mod}\, 5)$ ist, folgt

$$S \lhd G.$$

b) Sei $|G| = 4 \cdot 5 \cdot 19 = 380$. Für $p \in \{2, 5, 19\}$ sei N_p eine Sylow p-Untergruppe von G. Es ist

$$|G : N_G(N_{19})| \text{ ein Teiler von } |G : N_{19}| = 20.$$

Mit dem Sylowsatz erhalten wir $|G : N_G(N_{19})| = 1$ oder 20. Sei $|G : N_G(N_{19})| = 20$. Dann ist wegen $N_{19}^g \cap N_{19} = 1$ für $N_{19} \neq N_{19}^g$, $g \in G$,

$$\Big| \bigcup_{g \in G} g N_{19} g^{-1} \Big| = 20 \cdot 18 + 1 = 361.$$

Es ist weiter

$$|G : N_G(N_5)| \text{ ein Teiler von } |G : N_5| = 4 \cdot 19 = 76.$$

Mit dem Sylowsatz folgt $|G: N_G(N_5)| = 1$ oder 76. Sei $|G: N_G(N_5)| = 76$, so erhalten wir mit dem gleichen Argument wie für N_{19}

$$|\bigcup_{g\in G} gN_5g^{-1}| = 76 \cdot 4 + 1 = 305.$$

Somit gibt es in G genau 360 Elemente der Ordnung 19 und 304 der Ordnung 5, was zusammen 664 Elemente ergibt. Aber $|G| = 380$.

Also ist $N_5 \lhd G$. Sei $\omega \in G$, $o(\omega) = 19$. Da $|N_5 \setminus \{1\}| = 4$ ist, folgt mit Lemma V.15 a), dass ω nur Bahnen der Länge 1 auf den Elementen von N_5 induziert, also $\omega x = x\omega$ für alle $x \in N_5$. Somit ist $N_5 \leq N_G(\langle\omega\rangle)$. Dann ist aber $|G: N_G(N_{19})| \leq 4$, ein Widerspruch zur Annahme $|G: N_G(N_{19})| = 20$.

Also haben wir $N_{19} \lhd G$ gezeigt. Nach Lemma V.15 a) hat N_5 Bahnen der Länge 1 oder 5 auf $N_{19} \setminus \{1\}$. Also gibt es ein $1 \neq \omega \in N_{19}$, das unter N_5 fest bleibt, d.h., $x\omega = \omega x$ für alle $x \in N_5$ oder $\omega \in N_G(N_5)$. Da N_{19} zyklisch von der Ordnung 19 ist, ist $\langle\omega\rangle = N_{19}$ und somit folgt $N_{19} \leq N_G(N_5)$ und dann auch $N_5 \lhd G$.

c) Sei $|G| = 36 = 2^2 \cdot 3^2$. Sei S eine Sylow 3-Untergruppe von G. Angenommen $S \not\lhd G$. Dann ist $|G: N_G(S)| = 4$ nach dem Sylowsatz. Es induziert G eine Gruppe von bijektiven Abbildungen auf $\Omega = \{gSg^{-1} \mid g \in G\}$. Da $|\Omega| = 4$ ist, gibt es einen Homomorphismus f von G in Σ_4. Dieser ist nicht trivial, da nach dem Sylowsatz G nicht trivial auf Ω operiert. Da $|G| > 24 = \Sigma_4$ ist, ist $\ker f \neq 1$. Also gibt es in jedem Fall einen Normalteiler $1 \neq N \lhd G$, $N \neq G$.

Satz V.18

Sei G eine p-Gruppe ($|G| = p^a$), $G \neq 1$. Dann gilt

a) $Z(G) := \{h | h \in G,\ gh = hg$ für alle $g \in G\} \neq 1$.

b) Es gibt einen Normalteiler G_1 von G mit $|G: G_1| = p$.

Beweis.

a) Wir betrachten die Gruppe G als Menge $M = \{x | x \in G\}$. Hierauf definieren wir eine Äquivalenzrelation $\sim$ durch

$$x \sim y, \text{ falls } y = g^{-1}xg \text{ mit geeignetem } g \in G \text{ gilt.}$$

Seien $M_1, \ldots, M_r$ die Äquivalenzklassen. Dann haben wir

$$|G| = \sum_{i=1}^{r} |M_i|.$$

Ist $m_i \in M_i$, so ist $G_{m_i} = \{g | g \in G, g^{-1}m_ig = m_i\}$. Es ist $|M_i| = |G: G_{m_i}|$ nach Lemma V.15 eine p–Potenz.

Wir wählen die Notation so, dass $M_1 = \{1\}$ die Äquivalenzklasse des neutralen Elementes ist. Dann gilt

$$|G| = 1 + \sum_{i=2}^{r} |M_i|.$$

Da $|G|$ eine p-Potenz ist, muss es ein $i \geq 2$ geben, so dass $|M_i| = 1$ ist. Also ist $M_i = \{m_i\}$, $m_i \neq 1$, und $g^{-1}m_i g = m_i$ für alle $g \in G$, d.h. $m_i \in Z(G)$.

b) Nach a) ist $Z(G) \neq 1$. Wir wählen $N \leq Z(G)$, $|N| = p$. Dann ist $N \trianglelefteq G$. Nun liefert eine Induktion angewandt auf G/N die Behauptung. □

Auflösbar. Eine Gruppe G heißt *auflösbar*, falls es eine Kette N_i, $i = 1, \ldots, k+1$, von Untergruppen von G so gibt, dass

$$1 = N_{k+1} \trianglelefteq \cdots \trianglelefteq N_2 \trianglelefteq N_1 = G \text{ und } N_i/N_{i+1} \text{ für alle } i = 1, \ldots, k \text{ abelsch ist.}$$

Definition

Normalteiler in endlichen Gruppen ermöglichen Induktionsbeweise, wie wir es bereits im Beweis von V.18b) gesehen haben. Sei N ein Normalteiler. Ist $1 \neq N$ und $N \neq G$, so sind beide $|N|$ und $|G/N|$ kleiner als $|G|$. Haben wir also eine Ausage, die wir beweisen wollen, und übertragen sich die Voraussetzungen auf Normalteiler und Faktorgruppen, so gilt unsere Aussage per Induktion in N und G/N. Wir müssen das dann nur noch zusammensetzen, um die Gültigkeit in G zu bekommen. Nicht jede Eigenschaft wird dies so einfach zulassen. Die Auflösbarkeit ist in dieser Hinsicht eine sehr angenehme Eigenschaft, wie der folgende Satz zeigt.

Sei G eine Gruppe.

a) Ist G auflösbar, so auch die Faktorgruppe G/N für jeden Normalteiler N von G.

b) Ist G auflösbar, so auch jede Untergruppe U von G.

c) Ist N ein auflösbarer Normalteiler von G, so dass auch die Faktorgruppe G/N auflösbar ist, so ist G auflösbar.

Satz V.19

Beweis.

a) Da G auflösbar ist, gibt es eine Kette $1 = N_{k+1} \trianglelefteq N_k \trianglelefteq \ldots \trianglelefteq N_1 = G$ mit N_i/N_{i+1} abelsch. Wähle $n_1N, n_2N \in N_iN/N$. Da N_i/N_{i+1} abelsch ist, ist $n_1n_2 = n_2n_1\tilde{n}$ mit geeignetem $\tilde{n} \in N_{i+1}$. Dann ist $(n_1N)(n_2N) = (n_1n_2)N = n_2n_1\tilde{n}N$ mit $\tilde{n} \in N_{i+1}$. Somit ist

$$(N_iN/N)/(N_{i+1}N/N) \text{ abelsch und}$$

$$N = N_{k+1}N/N \trianglelefteq N_kN/N \trianglelefteq \ldots N_1N/N = G/N.$$

Also ist G/N auflösbar.

b) Da G auflösbar ist, gibt es wieder eine Kette $1 = N_{k+1} \trianglelefteq \ldots \trianglelefteq N_1 = G$ mit N_i/N_{i+1} abelsch. Wir setzen $U_i = N_i \cap U$, $i = 1, \ldots, k+1$. Da nach Satz V.9 a) $U_i/U_{i+1} = N_i \cap U/N_{i+1} \cap U \cong (N_i \cap U)N_{i+1}/N_{i+1}$ ist, folgt für die Kette

$$1 = U_{k+1} \trianglelefteq \cdots \trianglelefteq U_1 = U,$$

dass U_i/U_{i+1} abelsch ist. Somit ist U auflösbar.

c) Da N und G/N auflösbar sind, gibt es Ketten $1 = N_{k+1} \trianglelefteq \cdots \trianglelefteq N_1 = N$ und $1 = M_{s+1}/N \trianglelefteq \cdots M_1/N = G/N$. Diese können wir zusammensetzen zu einer Kette $1 = N_{k+1} \trianglelefteq \cdots \trianglelefteq N_1 = M_{s+1} \trianglelefteq \cdots \trianglelefteq M_1 = G$. Da nach Satz V.9 b) $(M_i/N)/(M_{i+1}/N) \cong M_i/M_{i+1}$ ist, sind alle Faktoren abelsch, d.h., G ist auflösbar. □

Das folgende Lemma werden wir in Kapitel VI benötigen.

Lemma V.20 *Sei $1 \neq G$ eine auflösbare Gruppe. Dann gibt es einen Normalteiler N von G, so dass $|G/N|$ eine Primzahl ist.*

Beweis. Da G auflösbar ist, gibt es eine Kette von Untergruppen $N_1, \ldots, N_{k+1}$ mit $1 = N_{k+1} \trianglelefteq \cdots \trianglelefteq N_2 \trianglelefteq N_1 = G$ und N_i/N_{i+1} ist abelsch für $i = 1, \ldots, k$. Da $G \neq 1$ ist, können wir $N_2 \neq G$ annehmen. Also ist G/N_2 eine nicht triviale abelsche Faktorgruppe. Es genügt also, die Behauptung für abelsches G zu beweisen. Dann ist aber jede Untergruppe von G normal. Sei $N \neq G$ eine maximale Untergruppe von G. Dann hat G/N keine echten Untergruppen. Sei p ein Primteiler von $|G/N|$. Nach dem Satz von Cauchy gibt es ein Element $gN \in G/N$ mit $o(gN) = p$. Wegen der Maximalität von N ist $\langle gN \rangle = G/N$, also ist $|G/N| = p$, die Behauptung. □

Es könnte nun sein, dass jede Gruppe auflösbar ist. Dann wäre der Begriff Auflösbarkeit nicht sonderlich nützlich. Dass dem nicht so ist, werden wir in den nächsten zwei Sätzen zeigen.

Satz V.21 *Ist $n \geq 5$ und $1 \neq N \trianglelefteq A_n$, so ist $N = A_n$.*

Beweis. Wir zeigen zunächst, dass die Behauptung richtig ist, falls N einen 3-Zyklus enthält. Dazu können wir $(1, 2, 3) \in N$ annehmen. Für $k > 3$ ist dann

$$(3, 2, k)(1, 2, 3)(3, 2, k)^{-1} = (1, k, 2) \in N.$$

Also ist auch

$$(1, k, 2)^2 = (1, 2, k) \in N.$$

Es ist

$$\Sigma_n = \langle (i, j) | 1 \leq i < j \leq n \rangle$$

nach Satz V.12. Da $(i, j) = (1, i)(1, j)(1, i)$ ist, erhalten wir auch

$$\Sigma_n = \langle (1, i) | 1 < i \leq n \rangle.$$

Da $(1, j)(1, i) = (1, i, j), 1 \neq i \neq j \neq 1$, ist, ergibt das

$$A_n = \langle (1, i, j) | i, j = 2, \ldots, n, i \neq j \rangle.$$

Da $(1, i, j) = (1, 2, j)^{-1}(1, 2, i)(1, 2, j)$ ist, ist sogar

$$A_n = \langle (1, 2, k) | k \geq 3 \rangle.$$

Somit ist $N = A_n$. Enthält also N einen 3-Zyklus, so ist $N = A_n$.

Wir nehmen nun an, dass N keinen 3-Zyklus enthält. Dies wollen wir zum Widerspruch führen. Sei $x = abc\ldots \in N$, a, b, c Zyklus der Zyklenzerlegung. Sei $a = (a_1, \ldots, a_m)$, $m \geq 4$. Setze $t = (a_1, a_2, a_3)$. Dann ist $t^{-1}xt \in N$.

Es ist

$$t^{-1}xt = t^{-1}atbc\ldots = z \in N.$$

Nun ist

$$N \ni zx^{-1} = t^{-1}ata^{-1} = (a_1, a_3, a_4),$$

der gewünschte Widerspruch.

Also enthält x nur 2-Zyklus und 3-Zyklus in der Zyklenzerlegung. Angenommen, x enthalte zwei 3-Zyklen. Dann können wir

$$x = (1, 2, 3)(4, 5, 6)y.$$

annehmen.

Setze nun $t = (2, 3, 4)$. Dann erhalten wir

$$N \ni t^{-1}xtx^{-1} = (1, 5, 2, 4, 3),$$

ein Widerspruch, da Elemente aus N keine 5-Zyklen enthalten.

Sei nun

$$x = (1, 2, 3)p, \text{ wobei } p \text{ nur 2-Zyklen enthält.}$$

Dann ist $p^2 = 1$ und somit

$$x^2 = (1, 2, 3)^2 = (1, 3, 2) \in N,$$

ein Widerspruch, da wir keine 3-Zyklen in N haben. Somit enthält x nur 2-Zyklen. Wir können also

$$x = (1, 2)(3, 4)p, \text{ mit } p^2 = 1$$

annehmen. Setze jetzt $t = (2, 4, 3)$. Das liefert

$$N \ni t^{-1}xtx^{-1} = (1, 4)(2, 3) = y.$$

Da $n \geq 5$ ist, enthält A_n das Element $u = (1, 4, 5)$. Dann ist auch

$$N \ni u^{-1}yu = (1, 5)(2, 3) = z.$$

Aber

$$N \ni zy = (1, 4, 5)$$

und wieder haben wir einen Widerspruch dazu, dass N keine 3-Zyklen enthält. Das beweist den Satz. □

Gruppen, die genau zwei Normalteiler haben, nämlich $\{1\}$ und G, nennen wir einfach. Nach Satz V.21 ist somit A_n, $n \geq 5$, einfach. Sei $\mathrm{SL}(n, K)$ die Gruppe der linearen Abbildungen eines Vektorraumes der Dimension n über einem endlichen Körper K mit Determinante 1. Ist dann $n > 2$ oder $|K| > 3$ für $n = 2$, so ist stets $\mathrm{SL}(n, K)/Z(\mathrm{SL}(n, K))$ einfach. Es gibt noch weitere Serien einfacher Gruppen, die ähnlich gebildet sind. Hinzu kommen noch 26 sogenannte sporadische einfache Gruppen, die scheinbar kein gemeinsames Bildungsgesetz haben. Die erste davon

wurde von Emile Mathieu[3] 1860 gefunden, die letzte von Zvonimir Janko[4] 1976. Eine der großen Leistungen der Mathematik des letzten Jahrhunderts war die Klassifikation der endlichen einfachen Gruppen (ein guter Übersichtsartikel ist Solomon, 1995 [28]).

Satz V.22 *Für $n \geq 5$ ist Σ_n nicht auflösbar.*

Beweis. Es ist $A_n \trianglelefteq \Sigma_n$. Da A_n nicht abelsch ($(1,2,3)(1,2,4) \neq (1,2,4)(1,2,3)$) und einfach ist, ist A_n nicht auflösbar. Nun folgt die Behauptung mit Satz V.19 b). □

Satz V.23 *Für $n \leq 4$ ist Σ_n auflösbar.*

Beweis. Es ist Σ_2 abelsch und damit auflösbar. Es ist $|A_3| = 3$, also ist A_3 auflösbar. Da $|\Sigma_3/A_3| = 2$ ist, ist auch Σ_3/A_3 auflösbar. Somit ist nach Satz V.19 c) Σ_3 auflösbar.

Setze $V = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), id\}$. Dann besteht V aus allen Elementen aus A_4, die in der Zyklenzerlegung nur 2-Zyklen haben. Wir sehen somit, dass $V \trianglelefteq A_4$ ist. Es ist $|A_4/V| = 3$. Also ist A_4/V auflösbar. Offenbar ist V abelsch und damit auflösbar. Also ist nach Satz V.19 c) A_4 auflösbar. Da $|\Sigma_4/A_4| = 2$ ist, ist auch Σ_4/A_4 auflösbar und nach Satz V.19 c) ist dann Σ_4 auflösbar. □

Dieses unterschiedliche Verhalten von Σ_n für $n \geq 5$ und $n \leq 4$ ist letztlich der Grund dafür, warum es für die Nullstellen von Polynomen vom Grad n Auflösungsformeln für $n \leq 4$ gibt, die nur arithmetische Operationen und Wurzeln benutzen, und keine für $n \geq 5$. Das werden wir im nächsten Kapitel näher ausführen.

Wir wollen nun noch die bisher entwickelten Methoden benutzen, um zwei Resultate von Évariste Galois[5] zu beweisen: erstens, dass jede Gruppe der Ordnung kleiner als 60 auflösbar ist, und zweitens, dass A_5 die einzige einfache Gruppe der Ordnung 60 ist.

[3] Emile Leonard Mathieu (*15.5.1835 Metz, †19.10.1890 Nancy). Er endeckte zwischen 1860 und 1873 die ersten fünf sporadischen einfachen Gruppen, die später nach ihm benannt wurden. Mathieu war Professor in Besançon und ab 1874 in Nancy, wo er sich hauptsächlich mit mathematischer Physik beschäftigte. Neben den Mathieu-Gruppen sind auch die mathieuschen Differentialgleichungen nach ihm benannt.

[4] Zvonimir Janko (*26.7.1932 Bjelovar, Kroatien) studierte in Zagreb und wurde zunächst Gymnasiallehrer, promovierte 1960 an der Universität in Zagreb. Aus politischen Gründen konnte er keine Anstellung an einer Universität in Jugoslawien finden. Er ging 1962 nach Australien an die Universität in Canberra und später an die Monash University, 1968/69 an das Institute for Advanced Study in Princeton und war bis 1972 Professor an der Ohio State University in Columbus, ab 1972 bis zur Emeritierung 2000 war er Professor an der Universität Heidelberg. Er endeckte 90 Jahre nach Mathieu die erste neue sporadische einfache Gruppe J_1, danach 1968 die Gruppen J_2 und J_3 und 1976 die letzte sporadische einfache Gruppe J_4. Seit 2000 arbeitet Z. Janko erfolgreich auf dem Gebiet der p-Gruppen.

[5] Évariste Galois (*25.10.1811 Bologna, †31.5.1832 Paris) war Mathematiker und Begründer der Galoistheorie (detaillierte Information findet man in Kapitel VI auf Seite 110).

Beispiel

a) Ist $1 \neq |G| = p^\alpha, p$ Primzahl, so ist G auflösbar. Nach Satz V.18 gibt es einen abelschen Normalteiler $1 \neq N$ von G. Dann folgt die Behauptung mit Satz V.19 c) und Induktion.

b) Sei $|G| = p \cdot r$ mit verschiedenen Primzahlen p und r. Dann ist G auflösbar. Wäre G nicht auflösbar, so wäre G einfach nach Satz V.19 c). Dann ist nach dem Sylowsatz $p \equiv 1 (\mathrm{mod}\, r)$ und $r \equiv 1 (\mathrm{mod}\, p)$, was nicht möglich ist.

c) Sei $|G| \leq 59$. Dann ist G auflösbar. Per Induktion können wir für ein Gegenbeispiel G annehmen, dass G einfach ist.

α) Ist $|G|$ ungerade, so ist G auflösbar. Nach a) und b) können wir $|G| = p^2 \cdot r$ mit verschiedenen Primzahlen p und r annehmen. Also ist $|G| = 3^2 \cdot 5$. Aber $5 \not\equiv 1 (\mathrm{mod}\, 3)$, d.h., G hat eine normale Sylow 3-Untergruppe.

Nach α) ist ab jetzt $|G|$ gerade.

β) Sei $|G| = 2 \cdot u, u \neq 1$ ungerade. Sei $x \in G$, $o(x) = 2$. Dieses x existiert nach dem Satz von Cauchy. Wir lassen G auf G durch Multiplikation vermöge

$$g \to gh, \text{ für } h \in G$$

operieren. Dies liefert einen Homomorphismus von G in die $\Sigma_{|G|}$. Dabei induziert das Element x eine Permutation, die aus genau $|G|/2 = u$ vielen Transpositionen besteht, da $g \neq gx$ für alle $g \in G$ ist. Also ist $\operatorname{sgn} x = -1$, d.h., $x \notin A_{|G|}$. Da G einfach ist, ist $A_{|G|} \cap G = 1$. Nun ist aber $|\Sigma_{|G|}/A_{|G|}| = 2$, was $u \neq 1$ widerspricht.

γ) Sei $|G| = 4 \cdot u$, u ungerade, $u \neq 1$. Dann ist $u < 15$. Ist u prim, so können wir mit Satz V.19 c) wieder $4 \equiv 1 (\mathrm{mod}\, u)$ annehmen. Also ist $u = 3$, d.h. $|G| = 12$. Nun ist G isomorph in Σ_4 eingebettet, aber Σ_4 ist auflösbar nach Satz V.23.

Sei nun u nicht prim. Dann ist $u = 3^2$. Nach Beispiel c) auf Seite 92 ist dann G auflösbar.

δ) Sei $|G| = 8 \cdot u$, also $u \leq 7$. Dann ist $|G| = 8 \cdot 3, 8 \cdot 5, 8 \cdot 7$ oder $16 \cdot 3$. Ist $|G| = 8 \cdot 3$ oder $16 \cdot 3$, so hat G nach dem Sylow-Satz genau drei Sylow 2−Untergruppen. Dann gibt einen nicht trivialen Homomorphismus α von G in Σ_3. Aber jetzt ist $\ker \alpha \neq 1$ und auch $\ker \alpha \neq G$. Da $\ker \alpha \trianglelefteq G$ nach Satz V.6 ist, erhalten wir einen Widerspruch zur Einfachheit von G.

Da $8 \not\equiv 1 (\mathrm{mod}\, 5)$ ist, ist $|G| \neq 8 \cdot 5$. Es bleibt $|G| = 8 \cdot 7$. Dann gibt es 8 Sylow 7−Untergruppen. Sei T eine solche. Da T die Ordnung 7, also eine Primzahl, hat, ist $T \cap T^g = 1$ für $T \neq T^g, g \in G$. Also ist

$$\Big|\bigcup_{g \in G} T^g\Big| = 8 \cdot 6 + 1 = 49.$$

Es bleiben somit 7 Elemente übrig. Eine Sylow 2-Untergruppe enthält 8 Elemente. Also bilden die restlichen 7 Elemente und die Identität die einzige Sylow 2-Untergruppe, die damit normal in G ist.

d) Ist $|G| = 60$ und G einfach, so ist $G \cong A_5$.

Sei $S \in Syl_5(G)$ und $n_5 = |G : N_G(S)|$. Dann ist $n_5 \equiv 1 (\mathrm{mod}\, 5)$. Also ist $n_5 = 6$. Damit gibt es einen Monomorphismus

$$\alpha : G \to \Sigma_6.$$

Da G einfach ist, ist $\alpha(G) \leq A_6$. Wir können somit $G \leq A_6$ annehmen. Wir zeigen nun:

$$\text{Ist } G \leq A_6,\ |A_6 : G| = 6,\ G \text{ einfach, so ist } G \cong A_5.$$

Seien $Gh_1, \ldots, Gh_6$ die Nebenklassen von G in A_6. Es operiert A_6 auf diesen Nebenklassen durch

$$(Gh_i)g = G(h_i g).$$

Der Stabilisator der Nebenklasse G in A_6 ist G. Das heißt, G operiert auf den restlichen 5 Nebenklassen. Damit existiert ein Homomorphismus

$$\beta : G \to \Sigma_5.$$

Sei $\beta(G) = 1$. Dies bedeutet

$$Ghg = Gh$$

für alle $g \in G$ und $h \in A_6$, oder $hgh^{-1} \in G$ für alle $h \in A_6$. Also ist $G \lhd A_6$, was Satz V.21 widerspricht. Somit ist $\beta(G) \cong G$ einfach. Es ist $A_5 \cap \beta(G) \trianglelefteq \beta(G)$. Da $\beta(G) > 2$ ist, ist $A_5 \cap \beta(G) \neq 1$. Da $\beta(G)$ einfach ist, ist $A_5 \cap \beta(G) = \beta(G)$, also $\beta(G) \leq A_5$. Aber $|\beta(G)| = |A_5|$, d.h. $\beta(G) = A_5$. Somit ist $G \cong A_5$.

Übungsaufgaben

V.1 Jede Gruppe G mit $|G| = 4$ ist abelsch.

V.2 Sei G eine Gruppe, in der für ein $n \in \mathbb{N}$ die folgenden Gleichungen für ein Paar a, b von Elementen aus G gelten:

$$(ab)^n = a^n b^n,\ (ab)^{n+1} = a^{n+1} b^{n+1},\ (ab)^{n+2} = a^{n+2} b^{n+2}.$$

Dann ist $ab = ba$.

Gilt die Aussage $ab = ba$ auch noch, wenn wir nur noch die zwei Gleichungen $(ab)^n = a^n b^n$ und $(ab)^{n+1} = a^{n+1} b^{n+1}$ für ein $n \in \mathbb{N}$ haben?

V.3 Sei G eine endliche Gruppe.

a) Sei $n > 2$. Dann ist die Anzahl der Elemente der Ordnung n in G gerade.

b) Ist $|G|$ gerade, so ist die Anzahl der Elemente der Ordnung 2 in G ungerade (insbesondere existiert mindestens ein solches).

V.4 Seien G eine Gruppe und $a, b \in G$ mit $a^7 = 1$ und $aba^{-1} = b^2$. Bestimme die Ordnung von b.

V.5 Sei G eine Gruppe. Dann gilt:

a) Genau dann ist G abelsch, wenn die Abbildung $g \to g^{-1}$ ($g \in G$) ein Automorphismus ist.

b) Ist $g^2 = 1$ für alle $g \in G$, so ist G abelsch.

V.6 Seien G eine Gruppe und H eine Untergruppe von G. Für $g \in G$ setze $H^g = g^{-1}Hg$. Zeige:

a) Es ist $g \in HH^g$ genau dann, wenn $g \in H$ ist.

b) Ist $G = HH^g$ für ein $g \in G$, so ist $G = H$.

V.7 Seien G eine endliche Gruppe und U, V zwei Untergruppen von G. Sei $|G\colon U| = n$ und $|G\colon V| = m$. Zeige:

a) Es ist $|G\colon U \cap V| \geq \mathrm{kgV}(m, n)$.

b) Sind n und m teilerfremd, so ist $|G\colon U \cap V| = nm$.

V.8 Seien G eine endliche Gruppe, U eine Untergruppe und N ein Normalteiler. Zeige:

a) Aus $\mathrm{ggT}(|G/N|, |U|) = 1$ folgt $U \subseteq N$.

b) Aus $\mathrm{ggT}(|G\colon U|, |N|) = 1$ folgt $N \subseteq U$.

V.9 **Dedekind[6]-Identität.** Seien A, B, C Untergruppen der Gruppe G mit $A \subseteq C$. Dann gilt

$$AB \cap C = A(B \cap C).$$

V.10 (Alle Permutationen seien in Σ_9.)

a) Berechne

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 9 & 3 & 1 & 6 & 8 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 7 & 6 & 2 & 8 & 1 & 3 & 4 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 6 & 5 & 2 & 8 & 9 & 1 & 4 \end{pmatrix}^{-1}.$$

b) Schreibe als Produkt von elementfremden Zyklen $(1, 3, 6)(2, 5, 4)(4, 8)(6, 3, 7, 8, 9)$.

c) Schreibe als Produkt von Transpositionen $(1, 2, 4)^{-1}(5, 9)(7, 3, 6, 2)$.

d) Bestimme das Signum von $(3, 8, 4, 6, 5)^{-1}(1, 6)(1, 9)(1, 2)(9, 6, 7)^{-1}$.

V.11 a) Seien G eine Gruppe und U eine Untergruppe mit $|G\colon U| = n$. Dann gibt es einen Homomorphismus $\varphi\colon G \longrightarrow \Sigma_n$ mit $\ker \varphi = \bigcap_{g \in G} U^g$ (U^g wie in Aufgabe V.6).

b) Seien $|G| < \infty$ und p der kleinste Primteiler von $|G|$. Ist H eine Untergruppe von G mit $|G\colon H| = p$, so ist H ein Normalteiler von G.

V.12 Seien $|G| = p^3q$, p und q Primzahlen. Es habe G keine normale Sylow p–Untergruppe und auch keine normale Sylow q–Untergruppe. Dann ist $G \cong \Sigma_4$.

V.13 Zeige:

a) Es ist Σ_n zu einer Untergruppe von A_{n+2} isomorph.

b) Außer für $n = 1$ enthält A_{n+1} keine Untergruppe, die zu Σ_n isomorph ist.

[6] Julius Wilhelm Richard Dedekind (*6.10.1831 Braunschweig, †12.2.1916 Braunschweig) war Professor in Braunschweig. Er verfasste grundlegende Arbeiten in der Algebra und der Mengenlehre.

V.14 Seien A und B Normalteiler einer Gruppe G. Sind A und B beide auflösbar, so ist auch AB ein auflösbarer Normalteiler von G.

V.15 Seien G eine endliche Gruppe und N ein Normalteiler von G. Sei weiter P eine Sylow p-Untergruppe von N. Dann gilt $G = NN_G(P)$.

V.16 Sei G eine Gruppe mit $|G| = 168$. Wie viele Elemente der Ordnung 7 hat G, falls G keine normale Sylow 7–Untergruppe hat?

VI Symmetrien

Gruppen sind die Axiomatisierung des Begriffes der Symmetrie. Wo immer Symmetrien eine Rolle spielen, spielen auch Gruppen eine Rolle. Diese Sichtweise wollen wir jetzt in den Mittelpunkt stellen. Jeder kann sich unter einer Symmetrie eines geometrischen Körpers, also eines Würfels, Tetraeders usw. etwas vorstellen. Insbesondere ist klar, dass die Symmetrien eine Gruppe bilden. Auch spielen Symmetrien (Gruppen) bei der Abzählung von Mustern eine wichtige Rolle (siehe hierzu Polya, 1937 [24]).

Wir wollen im Folgenden einen völlig anderen Typ von Symmetrien betrachten und sehen, wie diese helfen können, gewisse Probleme zu lösen.

Wir betrachten zunächst Symmetrien von $\mathbb{C}$. Was bedeutet da aber Symmetrie? Bei der Symmetrie eines geometrischen Körpers, z.B. eines Würfels, denken wir an eine bijektive Abbildung, die die Struktur des Körpers erhält. Genau das Gleiche stellen wir uns unter einer Symmetrie von $\mathbb{C}$ vor, also eine bijektive Abbildung σ, die die Struktur von $\mathbb{C}$, nämlich Addition und Multiplikation erhält, d.h.

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = \sigma(a)\sigma(b)$$

für alle $a, b \in \mathbb{C}$. Dies haben wir unter dem Namen Automorphismus (siehe Seite 10) bereits kennengelernt.

Es ist $\sigma(1) = 1$ und $\sigma(0) = 0$ (siehe Lemma I.6). Ist $n \in \mathbb{N}$, so ist

$$n = \underbrace{1 + \cdots + 1}_{n-mal}.$$

Also ist $\sigma(n) = n$. Da $\sigma(0) = 0$ ist, ist

$$0 = \sigma(0) = \sigma(n + (-n)) = \sigma(n) + \sigma(-n) = n + \sigma(-n).$$

Somit ist $\sigma(z) = z$ für alle $z \in \mathbb{Z}$. Nun ist $\sigma(1) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1})$ für $a \in \mathbb{Z}$, $a \neq 0$. Dann ist $\sigma(a^{-1}) = a^{-1}$, also $\sigma_{|\mathbb{Q}} = id$. Als Ergebnis erhalten wir, dass jeder Automorphismus von $\mathbb{C}$ den Körper $\mathbb{Q}$ elementweise fest lässt.

Wir sind aber weniger an Symmetrien von $\mathbb{C}$ als an Symmetrien von Polynomen $f \in \mathbb{Q}[x]$ interessiert. Eine solche sollte das Polynom invariant lassen. Auf Seite 40 hatten wir $\sigma(f)$ definiert. Wir haben gerade gezeigt, dass wir für Automorphismen σ

von $\mathbb{C}$ stets $\sigma(f) = f$ haben. Somit induzieren Symmetrien von $\mathbb{C}$ auch Symmetrien jedes Polynoms $f \in \mathbb{Q}[x]$. Sie permutieren also die Nullstellen von f in $\mathbb{C}$. Also induziert σ einen Automorphismus des Zerfällungskörpers von f in $\mathbb{C}$.

Scheinbar kommt es somit nur auf die Automorphismen des Zerfällungskörpers an. Deshalb definieren wir etwas allgemeiner:

Definition

Galoisgruppe. Sei $f \in \mathbb{Q}[x]$ und K der Zerfällungskörper von f in $\mathbb{C}$. Setze $G_f = \mathrm{Aut}\,(K)$. Dann nennen wir G_f die *Galoisgruppe* von f.

Es ist G_f die gesuchte Gruppe von Symmetrien von f. Für die Berechnung von Galoisgruppen ist das folgende Resultat sehr hilfreich.

Satz VI.1

Ist $f \in \mathbb{Q}[x]$ irreduzibel, so operiert G_f transitiv auf den Nullstellen von f.

Beweis. Seien a_1, a_2 Nullstellen von f. Nach Satz II.11 gibt es einen Isomorphismus $\tau\colon \mathbb{Q}(a_1) \to \mathbb{Q}(a_2)$ mit $\tau(a_1) = a_2$. Nach Satz II.19 kann τ zu einem Automorphismus des Zerfällungskörpers K von f erweitert werden. □

Folgerung VI.2

Sei $f \in \mathbb{Q}[x]$, f irreduzibel, und $\operatorname{grad} f = n$. Dann ist G_f zu einer Untergruppe von Σ_n isomorph.

Beweis. Sei K der Zerfällungskörper von f in $\mathbb{C}$. Ist $\sigma \in \mathrm{Aut}\,(K)$ mit $\sigma(a) = a$ für alle Nullstellen a von f, so ist $\sigma = id$, da K von $\mathbb{Q}$ und den Nullstellen von f erzeugt wird. Also operiert G_f treu auf den Nullstellen. Da f höchstens n verschiedene Nullstellen hat, ist G_f zu einer Untergruppe von Σ_n isomorph. □

Beispiel

Sei $f = x^4 - 2 \in \mathbb{Q}[x]$. Nach dem Satz I.28 von Eisenstein mit $p = 2$ ist f irreduzibel. Die Nullstellen in $\mathbb{C}$ sind $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$, wobei $\sqrt[4]{2} \in \mathbb{R}$ sei. Also ist $K = \mathbb{Q}(\sqrt[4]{2}, i)$ der Zerfällungskörper.

Sei τ das Bilden des konjugiert Komplexen. Dann ist $\tau \in \mathrm{Aut}\,(K)$.

Nach Satz VI.1 gibt es ein $\sigma \in \mathrm{Aut}\,(K)$ mit

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}.$$

Es ist i eine Nullstelle von $x^2 + 1 = g$. Da $\sigma(g) = g$ ist, ist auch $\sigma(i)$ eine Nullstelle von g. Somit ist $\sigma(i) = i$ oder $\sigma(i) = -i$. Indem wir notfalls σ durch $\sigma\tau$ ersetzen (beachte $\sigma\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$) können wir $\sigma(i) = i$ annehmen. Dann ist

$$\sigma(i\sqrt[4]{2}) = i\sigma(\sqrt[4]{2}) = ii\sqrt[4]{2} = -\sqrt[4]{2}$$

und

$$\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}.$$

Damit entspricht σ einem 4-Zyklus auf den Nullstellen. Es ist

$$\tau\sigma\tau(\sqrt[4]{2}) = -i\sqrt[4]{2} = \sigma^{-1}(\sqrt[4]{2}).$$

Das liefert $\tau\sigma\tau = \sigma^{-1}$. Damit haben wir 8 Elemente aus G_f gefunden.

$$\{\sigma, \sigma^2, \sigma^3, id, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} = U.$$

Nach Folgerung VI.2 ist G_f eine Untergruppe von Σ_4.

Offenbar ist U eine Gruppe. Nach dem Satz von Lagrange ist $G_f = U$ oder $G_f = \Sigma_4$.

Sei $G_f = \Sigma_4$. Dann sind alle 3-Zyklen in G_f. Wir betrachten den 3-Zyklus ω aus Σ_4 mit

$$\omega(\sqrt[4]{2}) = \sqrt[4]{2}, \omega(-\sqrt[4]{2}) = i\sqrt[4]{2}, \omega(i\sqrt[4]{2}) = -i\sqrt[4]{2}, \omega(-i\sqrt[4]{2}) = -\sqrt[4]{2}.$$

Da $\omega \in G_f$ ist, ist $\omega_{|\mathbb{Q}} = id$, d.h. $\omega(-1) = -1$ und somit ist mit $\omega(\sqrt[4]{2}) = \sqrt[4]{2}$ auch $\omega(-\sqrt[4]{2}) = -\sqrt[4]{2}$, ein Widerspruch zur oben angenommenen Operation von ω. Dies zeigt

$$U = G_f.$$

Im Allgemeinen ist die Berechnung der Galoisgruppe eines Polynoms keine leichte Sache. Hier war uns zur Hilfe gekommen, dass wir die Nullstellen kannten. Wir werden am Ende dieses Kapitels sehen, dass man durchaus auch die Galoisgruppe berechnen kann, ohne auch nur eine einzige Nullstelle zu kennen.

Was haben wir von der Kenntnis der Galoisgruppe G_f? Galois beschäftigte sich mit der Frage nach der Auflösbarkeit von Polynomen durch sogenannte Radikale, dies bedeutet grob gesprochen, ob man die Nullstellen von Polynomen als Ausdrücke schreiben kann, die nur Addition, Subtraktion, Multiplikation, Division und Wurzelausdrücke benutzen. Bekannt ist sicherlich jedem die Lösungsformel für quadratische Gleichungen

$$x^2 + ax + b.$$

Die Nullstellen x_1, x_2 können wie folgt beschrieben werden:

$$x_1 = \frac{1}{2}(-a + \sqrt{a^2 - 4b}), \quad x_2 = \frac{1}{2}(-a - \sqrt{a^2 - 4b}).$$

Ähnliche Formeln gibt es auch für die Gleichungen vom Grad 3 und 4. Wir wollen hier nur noch Grad 3 betrachten, also

$$x^3 + ax^2 + bx + c.$$

Durch eine Transformation $x \to x - \frac{a}{3}$ kann man diese immer in die Form

$$x^3 + px + q$$

bringen. Hierfür wollen wir die Nullstellen bestimmen. Es gilt die folgende Identität:

$$(u + v)^3 - 3uv(u + v) - (u^3 + v^3) = 0.$$

Setzen wir $3uv = -p$ und $-(u^3 + v^3) = q$ dann ist $x = u + v$ eine Lösung von

$$x^3 + px + q = 0.$$

Das führt zu den beiden Gleichungen:

$$\begin{array}{lrcl} (1) & v^3 + u^3 & = & -q \\ (2) & -uv & = & \frac{p}{3}. \end{array}$$

Wir quadrieren (1) und bilden die dritte Potenz von (2), die dann noch mit 4 multipliziert wird. Das liefert

$$\begin{array}{lrcl} (1) & v^6 + 2u^3v^3 + u^3 & = & q^2 \\ (2) & -4u^3v^3 & = & \frac{4p^3}{27}. \end{array}$$

Addition der beiden Gleichungen liefert

$$(u^3 - v^3)^2 = q^2 + \frac{4p^3}{27}$$

und dann

$$u^3 - v^3 = \sqrt{\frac{27q^2 + 4p^3}{27}}.$$

Zusammen mit $v^3 + u^3 = -q$ erhalten wir dann

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{27q^2 + 4p^3}{108}}} \quad \text{und} \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{27q^2 + 4p^3}{108}}}.$$

Dies ist nicht eindeutig, da es mehr als eine dritte Wurzel gibt. Sei ω eine primitive dritte Einheitswurzel, also

$$\omega = \frac{-1 + i\sqrt{3}}{2}.$$

Dann ist $v^3 = (\omega v)^3 = (\omega^2 v)^3$. Damit haben wir jeweils drei dritte Wurzeln, was zunächst 9 Paare (u, v) ergibt. Wir wählen hiervon die 3 Paare (u, v), die zusätzlich

$$3uv = -p$$

erfüllen. Sei (u_1, v_1) ein solches zulässige Paar. Dann sind die Paare $(\omega u_1, \omega^2 v_1)$ und $(\omega^2 u_1, \omega v_1)$ auch zulässige Paare. Die Nullstellen der Gleichung $x^3 + px + q = 0$ sind nun

$$\begin{aligned} x_1 &= u_1 + v_1 \\ x_2 &= \omega u_1 + \omega^2 v_1 \\ x_3 &= \omega^2 u_1 + \omega v_1, \end{aligned}$$

die offenbar von der Auswahl von (u_1, v_1) unabhängig sind. Man nennt diese Form die Cardano[1]-Form.

[1] Gerolamo Cardano (*24.9.1501 Pavia, †21.9.1576 Rom) war Arzt, Philosoph, Techniker, Mathematiker, 1523 Gymnasiallehrer für Mathematik, 1525 Rektor der Universität Padua, 1543 Professor für Medizin in Pavia, 1562 Professor in Bologna, 1570 wegen Ketzerei eingesperrt. Sein mathematisches Hauptwerk besteht in den Auflösungsformeln für kubische Gleichungen, was ein 2000 Jahre altes Problem löste. Ein weiteres Arbeitsgebiet sind Anfänge der Wahrscheinlichkeitsrechnung. Philosophisch stand er Galilei sehr nahe. Er hat auch viele technische Erfindungen gemacht. Die kardanischen Aufhängungen sind nach ihm benannt, aber vermutlich älter.

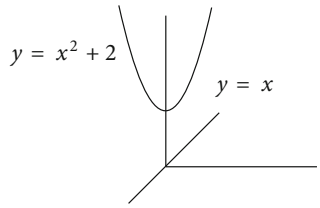
Interessant hierbei ist, dass die komplexen Zahlen (in ω) auftauchen. Zum ersten Mal wurden Mathematiker mit den komplexen Zahlen im 16. Jahrhundert konfrontiert, und zwar beim Lösen von Gleichungen. Die einfachste, bei denen man auf Wurzeln negativer Zahlen stößt, sind die quadratischen, z.B.

$$x^2 + 1 = 0.$$

Trotzdem waren es nicht die quadratischen, sondern die kubischen Gleichungen, die die Beschäftigung mit den komplexen Zahlen erzwungen haben. Betrachten wir z.B.

$$x^2 + 2 = x.$$

Wir interpretieren diese Gleichung als den Durchschnitt der Geraden $y = x$ mit der Parabel $y = x^2 + 2$.



Für die Lösung dieser Gleichung erhalten wir mit den obigen Formeln

$$x = \frac{1}{2}(1 \pm \sqrt{-7}).$$

Dies ist offenbar innerhalb der reellen Zahlen ein sinnloser Ausdruck, da man aus -7 in $\mathbb{R}$ keine Quadratwurzel ziehen kann. Diese Sinnlosigkeit ist aber nicht beunruhigend, da sich die beiden Kurven $y = x^2 + 2$ und $y = x$ in der Tat nicht schneiden. Die Idee, den Zahlenbereich zu erweitern, um auch in diesem Fall eine Lösung zu haben, ist eher ein moderner Ansatz, aber nicht der, der die Einführung komplexer Zahlen historisch nahegelegt hat.

Ganz anders sieht dies bei Gleichungen dritten Grades aus. Rafael Bombelli[2] beschäftigte sich 1572 mit der Gleichung

$$x^3 = 15x + 4.$$

Die Formel von Cardano liefert dann für eine Nullstelle

$$u = \sqrt[3]{2 + \sqrt{-121}},\ v = \sqrt[3]{2 - \sqrt{-121}}.$$

[2] Rafael Bombelli (*1526 Bologna, †1572 Rom) war Ingenieur und Mathematiker, gab 1572 ein fünfbändiges Werk zur Algebra heraus, das das mathematische Wissen seiner Zeit zusammenfasste, die beiden letzten Bände sind erst 1929 aus seinem Nachlass erschienen. Diese Bücher enthalten die Gleichungstheorie und zum ersten Mal sowohl negative als auch imaginäre Zahlen.

Also

$$x_1 = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}},$$

wobei zu beachten ist, dass $uv = 5$ sein muss.

Wieder haben wir den sinnlosen Ausdruck $\sqrt{-121}$. Allerdings entspricht x_1 der Lösung $x_1 = 4$. Die Kurven schneiden sich in der Tat. Hier hat man also ein Problem, da man bei Benutzung der Formeln auf Ausdrücke geführt wird, die Quadratwurzeln aus negativen Zahlen enthalten, aber durchaus reellen Lösungen der Gleichung entsprechen. Wenn man nun einfach so fortfährt und mit der „imaginären" Zahl $\sqrt{-121}$ so rechnet, wie man es von reellen Zahlen gewohnt ist, und $(\sqrt{-121})^2 = -121$ setzt, so kann man in der Tat

$$\sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}} = 4$$

nachrechnen. Auf diese Weise haben die italienischen Ingenieure des 16. Jahrhunderts erfolgreich mit den komplexen Zahlen gerechnet. Allerdings waren diese „imaginären" Zahlen zunächst nicht sonderlich beliebt. Man konnte sie zwar nicht einfach als Unfug abtun, man konnte damit ja reelle Lösungen von Gleichungen bekommen, auf der anderen Seite existierten sie aber nicht. Nicht alle Mathematiker haben solche Rechenausdrücke erlaubt. Erst durch Gauß und Hamilton[3] wurden sie allgemein anerkannt, nachdem sie als Paare reeller Zahlen mit gewissen Rechenregeln eingeführt wurden.

Die Frage, der wir jetzt nachgehen wollen, ist, ob solche Formeln auch für andere Grade als 2 oder 3 existieren bzw. für welche Polynome es diese gibt. Für manche gilt dies natürlich. Die Nullstellen von $x^6 - 1$ sind Wurzelausdrücke.

Niels Abel[4] hatte 1824 gezeigt, dass es für die allgemeine Gleichung vom Grad 5 keine solche Formeln gibt, und 1826 [1], dass dies auch für die allgemeine Gleichung vom Grad mindestens 5 richtig ist. Galois wollte aber darüber hinaus verstehen, warum es für manche Gleichungen solche Formeln gibt, für andere aber nicht. Hierauf gab er eine Antwort. Das Neue dabei war, dass die Antwort nicht irgendwelche Bedingungen an die Koeffizienten a_i des Polynoms f war, wie sie seine Vorgänger gesucht hatten, sondern eine Eigenschaft der Galoisgruppe G_f. Der Hauptsatz ist:

Satz VI.3

Die Gleichung $f = 0$ mit $f \in \mathbb{Q}[x]$ ist genau dann durch Radikale auflösbar, d.h., die Nullstellen lassen sich durch arithmetische Operationen und Wurzeln ausdrücken, falls G_f auflösbar ist.

Für den Beweis ist es sinnvoll, den Begriff der Galoisgruppe eines Polynoms etwas zu verallgemeinern.

[3] Sir William Rowen Hamilton (*4.8.1805 Dublin, †2.9 1865 in Dunsink bei Dublin) wurde bereits 1827 vor Beendigung seines Studiums Professor für Astronomie am Trinity College in Dublin. Sein Hauptarbeitsgebiet war die mathematische Physik, berühmt wurde er durch die nach ihm benannte Hamiltonsche Mechanik und die Entdeckung der Quaternionen.

[4] Niels Henrik Abel (*5.8.1802 Finnö (Norwegen), †6.4.1829 Froland) war als Stipendiat in Paris, Berlin und Italien. Er leistete bedeutende Beiträge auf den Gebieten der algebraischen Gleichungen, elliptischen Kurven und Reihenlehre.

Seien $L \subseteq \mathbb{C}$ ein Körper und $f \in L[x]$. Dann verstehen wir unter der Galoisgruppe G_f bezüglich L die Menge aller Automorphismen eines Zerfällungskörpers von f über L in $\mathbb{C}$, die L elementweise festlassen. Für $L = \mathbb{Q}$ ist dies genau unsere Definition der Galoisgruppe.

Die folgenden Aussagen sind zentral in der Galoistheorie. Ein Beweis würde den Rahmen dieses Buches allerdings sprengen.

Bemerkung. Seien $L \subseteq \mathbb{C}, f \in L[x]$ und K der Zerfällungskörper über L von f in $\mathbb{C}$. Sei G_f die zugehörige Galoisgruppe. Galois zeigte

a) Es gibt eine bijektive Beziehung zwischen den Untergruppen U von G_f und den Zwischenkörpern M mit $L \subseteq M \subseteq K$. Jeder Untergruppe U wird dabei $\mathrm{Fix}\,(U) = \{s \in K | u(s) = s \text{ für alle } u \in U\}$ zugeordnet.

b) Dass U normal in G_f ist, ist äquivalent dazu, dass es zu $M = \mathrm{Fix}\,(U)$ ein $g \in L[x]$ gibt, so dass M der Zerfällungskörper von g ist.

c) Ist U normal in G_f. So ist U die Galoisgruppe von f über $M = \mathrm{Fix}\,(U)$ und G_f/U ist die Galoisgruppe von g über L, wobei g das Polynom aus b) sei.

d) Ist $h \in L[x]$, so dass K ein Zerfällungskörper von h ist, so ist $G_f = G_h$.

Diese Aussagen werden zum Beweis von Satz VI.3 eingesetzt, den wir gleich skizzieren wollen. Dabei sind b) und c) wesentlich, da sie Induktionsbeweise ermöglichen.

Beweisskizze von VI.3. Sei K der Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$. Ist die Gleichung f auflösbar, so ist dies gleichwertig dazu, dass es eine Kette

$$\mathbb{Q} \subseteq K_1 \subseteq \cdots K_r = K$$

gibt, so dass $K_i = K_{i-1}(\sqrt[n_i]{b_i})$ für geeignete $b_i \in K_{i-1}$ ist. Man beachte, dass die Ausdrücke für die Lösungen ineinander geschachtelte Wurzelausdrücke sind. Indem wir die Kette noch verfeinern, können wir n_i als Primzahl wählen. Wir wollen nun noch $\mathbb{Q}$ um alle n_i-ten Einheitswurzeln vergrößern, also die Nullstellen von $x^{n_i} - 1$ (auch bei den Lösungsformeln für die Gleichung dritten Grades gehen ja dritte Einheitswurzeln ein, selbst wenn die Nullstellen alle reell sind). Also sei L dieser größere Körper und L_f der Zerfällungskörper von f über L in $\mathbb{C}$. Dann haben wir wieder eine Kette

$$L = L_1 \subseteq \cdots \subseteq L_r = L_f \text{ mit } L_i = L_{i-1}(\sqrt[n_i]{b_i}),\ b_i \in L_{i-1}.$$

Es hat $x^{n_i} - 1$ nach Satz II.23 paarweise verschiedene Nullstellen, also genau n_i viele. Da alle n_i-ten Einheitswurzeln in L_{i-1} liegen und die Nullstellen von

$$x^{n_i} - b_i$$

gerade $\epsilon \sqrt[n_i]{b_i}$ mit einer festen Nullstelle $\sqrt[n_i]{b_i}$ und beliebiger n_i-ter Einheitswurzel ϵ sind, ist L_i Zerfällungskörper von $x^{n_i} - b_i$ über L_{i-1}.

Die Elemente der Galoisgruppe von $x^{n_i} - b_i$ über L_i bilden $\sqrt[n_i]{b_i} \to \epsilon^j \sqrt[n_i]{b_i}$ für geeignetes j ab, also sind sie einfach die Multiplikation mit ϵ^j. Da $\epsilon^{i+j} = \epsilon^{j+i}$ ist, ist die Gruppe abelsch und damit auflösbar.

Wir setzen nun $i = 1$. Nach der obigen Bemerkung b) gibt es ein $M \trianglelefteq G_f$, so dass Fix $(M) = L_1$ ist. Nun ist nach Bemerkungen c) und d) G_f/M die Galoisgruppe von $x^{n_1} - b_1$ über L, d.h. abelsch, und M ist die Galoisgruppe von f über L_1. Da f auch über L_1 auflösbar ist, folgt per Induktion, dass M auflösbar ist. Nun folgt die Behauptung mit Satz V.19.

Wir betrachten nun die umgekehrte Richtung, also G_f ist auflösbar. Wie eben sei L der Körper, der alle notwendigen Einheitswurzeln enthält. Nach Lemma V.20 gibt es $M \trianglelefteq G$ mit $|G\colon M| = p$ prim. Sei $L_1 = \text{Fix}\,(M)$. Dann ist M die Galoisgruppe von f über L_1. Da M nach Satz V.19 auflösbar ist, gibt es per Induktion eine Kette

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r = L_f \text{ mit } L_i = L_{i-1}(\sqrt[n_i]{b_i}),\ b_i \in L_{i-1}.$$

Nach der Bemerkung c) ist G/M die Galoisgruppe eines Polynoms g über L, wobei L_1 der Zerfällungskörper von g über L ist. Also genügt es, die Behauptung für $L_1 = L_f$ und damit für $|G_f| = p$ zu zeigen.

Dies geht wie folgt: Sei ϵ eine primitive p-te Einheitswurzel in L, die per Konstruktion von L existiert, und $G_f = \langle\sigma\rangle$. Wir betrachten das lineare Gleichungssystem (auch Lagrange-Resolvente genannt):

$$(*)\quad \sum_{i=0}^{p-1} \epsilon^{ij}\sigma^i(x) = 0, j = 0, \ldots p-1.$$

Dieses System hat die Vandermonde[5] als Determinante, also nur triviale Lösungen.

In $(*)$ spielt die erste Gleichung eine besondere Rolle. Wir wollen annehmen, dass es ein b gibt, das alle Gleichungen bis auf die erste löst, und dies zum Widerspruch führen. Sei also $b \in L_1 \setminus L$ mit

$$\sum_{i=0}^{p-1} \epsilon^{ij}\sigma^i(b) = 0 \text{ für alle } j \neq 0.$$

Dann ist

$$\sum_{i=0}^{p-1} \sigma^i(b) = \sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1} \epsilon^{ij}\sigma^i(b)\right) = \sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-1} \epsilon^{ij}\right)\sigma^i(b).$$

Ist $i \neq 0$, so ist $\sum_{j=0}^{p-1} \epsilon^{ij}$ die Summe aller p–ten Einheitwurzeln, also der Koeffizient von x^{p-1} in $x^p - 1$. Dies ergibt $\sum_{j=0}^{p-1} \epsilon^{ij} = 0$ für alle $i \neq 0$. Also ist

$$\sum_{i=0}^{p-1} \sigma^i(b) = \left(\sum_{j=0}^{p-1} \epsilon^{j\cdot 0}\right)\sigma^0(b) = pb.$$

Da $\sigma(\sum_{i=0}^{p-1} \sigma^i(b)) = \sum_{i=0}^{p-1} \sigma^{i+1}(b) = \sum_{i=1}^{p} \sigma^i(b) = \sum_{i=0}^{p-1} \sigma^i(b)$ ist (beachte dabei $\sigma^0 = \sigma^p = id$), ist $\sum_{i=0}^{p-1} \sigma^i(b) \in \text{Fix}\,(G_f)$. Somit ist

$$pb \in \text{Fix}\,(G_f).$$

[5] Alexandre-Théophile Vandermonde (*28.2.1735 Paris, †1.1.1796 Paris) war Musiker, Mathematiker und Chemiker. Er wurde 1771 in die Académie de Sciences aufgenommen. Sein Name wird mit der Determinantentheorie verbunden.

Da wir nach der Bemerkung a) eine bijektive Zuordnung zwischen den Untergruppen und den Zwischenkörpern haben und nach dem Satz von Lagrange G_f nur die Untergruppen $\{id\}$ und G_f hat, gibt es auch nur die Zwischenkörper L und L_f, so dass

$$\sum_{i=0}^{p-1} \sigma^i(b) = pb \in L$$

ist. Aber b war nicht in L, ein Widerspruch.

Wähle nun $b \in L_1 \setminus L$ beliebig. Dann gibt es ein $j > 0$, so dass

$$\sum_{i=0}^{p-1} \epsilon^{ij} \sigma^i(b) \neq 0$$

ist. Indem wir notfalls ϵ durch eine geeignete Potenz ϵ^k ersetzen, können wir

$$c = \sum_{i=0}^{p-1} \epsilon^i \sigma^i(b) \neq 0$$

annehmen. Es ist

$$\sigma^j(c) = \sum_{i=0}^{p-1} \epsilon^i \sigma^{i+j}(b) = \sum_{i=0}^{p-1} \epsilon^{-j} \epsilon^{i+j} \sigma^{i+j}(b) = c\epsilon^{-j}.$$

Beachte $\sigma(\epsilon^i) = \epsilon^i$, da $\epsilon^i \in L$ ist. Also ist

$$\epsilon^j = c\sigma^j(c)^{-1}.$$

Es ist weiter

$$\sigma(\prod_{j=0}^{p-1} \sigma^j(c)) = \prod_{j=0}^{p-1} \sigma^{j+1}(c) = \prod_{j=0}^{p-1} \sigma^j(c).$$

Also ist wieder $\prod_{j=0}^{p-1} \sigma^j(c) \in L$. Weiter ist

$$L \ni \prod_{j=0}^{p-1} \epsilon^j = \prod_{j=0}^{p-1} c\sigma^j(c)^{-1} = c^p (\prod_{j=0}^{p-1} \sigma^j(c))^{-1}.$$

Dann ist aber auch

$$c^p \in L.$$

Da $1 \neq \epsilon = c\sigma(c)^{-1}$ ist, ist $\sigma(c) \neq c$, somit ist $c \notin L$. Dann ist $L(c)$ ein Zwischenkörper ungleich L und somit $L(c) = L_f$, d.h.

$$L_f = L(\sqrt[p]{c^p}) \text{ mit } c^p \in L.$$

Damit ist die Behauptung bewiesen. □

Die hier zum ersten Mal angewandte Methode war später noch in vielen anderen Gebieten fruchtbar. Man beweist Eigenschaften eines Objektes, indem man die Symmetrien dieses Objektes studiert und die gewünschten Resultate in Verbindung zu Eigenschaften der Symmetriegruppe setzt.

Nach Satz V.22 ist Σ_n für $n > 4$ nie mehr auflösbar. Man kann Polynome über $\mathbb{Q}$ konstruieren, die als Galoisgruppe die Σ_n haben, weshalb es für $n > 4$ keine allgemein gültigen Formeln geben kann. Wir wollen für $n = 5$ ein solches Polynom angeben.

Lemma VI.4 *Sei $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Dann ist $G_f \cong \Sigma_5$.*

Beweis. Nach dem Satz von Eisenstein mit $p = 3$ ist f irreduzibel. Es ist

$$f' = 5x^4 - 6 \neq 0$$

und somit hat nach Satz II.23 f fünf verschiedene Nullstellen. Nach Satz VI.1 ist G_f hierauf transitiv. Damit ist 5 ein Teiler von $|G_f|$. Nun ist weiter

$$f(-2) = -17, f(-1) = 8, f(0) = 3, f(1) = -2, f(2) = 23.$$

Also hat f mindestens drei reelle Nullstellen. Da die Nullstellen von f' nur $\pm\sqrt[4]{6/5}$ sind und diese die reellen Nullstellen von f trennen, hat f genau drei reelle Nullstellen. Somit hat f genau zwei komplexe Nullstellen x_1, x_2. Es ist $x_2 = \bar{x}_1$ das konjugiert Komplexe. Damit ist $^-$ ein nicht trivialer Automorphismus τ des Zerfällungskörpers von f. Wir identifizieren die Nullstellen x_1, x_2, x_3, x_4, x_5 mit 1, 2, 3, 4, 5. Dann können wir also annehmen

$$\tau = (1, 2) \in G_f, \sigma = (1, 2, 3, 4, 5) \in G_f.$$

Es ist

$$\begin{aligned} \sigma\tau\sigma^{-1} &= (2, 3) \\ \sigma^2\tau\sigma^{-2} &= (3, 4) \\ \sigma^3\tau\sigma^{-3} &= (4, 5) \\ \sigma^4\tau\sigma^{-4} &= (5, 1). \end{aligned}$$

In Σ_n haben wir

$$(1, m)(m, m + 1)(1, m) = (1, m + 1).$$

Also haben wir $(1, 2), (1, 3), (1, 4), (1, 5) \in G_f$. Es ist $(1, i)(1, j)(1, i) = (i, j)$. Damit sind alle Transpositionen in G_f. Nach Satz V.12 ist dann $G_f = \Sigma_5$. □

Zum Ende dieses Abschnittes noch ein paar Worte zu der Person Evariste Galois. Er wurde 1811 geboren und starb 1832 in einem Duell. Mit 15 Jahren publizierte er bereits seine ersten Arbeiten. Wie im politischen war er auch im mathematischen Denken revolutionär und hatte es schwer, von seinen Zeitgenossen verstanden zu werden. Seine erste Arbeit auf dem Gebiet der Auflösbarkeit von Polynomgleichungen reichte Galois 1829 bei der Akademie der Wissenschaften in Paris ein. Der Referent Cauchy lehnte diese und eine acht Tage später zum gleichen Thema eingereichte Arbeit ab. Die Manuskripte sind leider verschollen. Das gleiche Schicksal hatte auch die 1830 anläßlich des Wettbewerbs „Großer Preis der Mathematik“ eingereichte Arbeit. Im Jahre 1831 sandte Galois zum letzten Mal eine Arbeit an die Akademie. Zu Gutachtern wurden Poisson und Lacroix bestellt. Beide waren allerdings mehr an Physik als an Algebra interessiert. So lehnten sie nach fünf Monaten

die Arbeit mit der Begründung ab, dass sie die Bedeutung der Arbeit nicht sehen. Das Werk Galois wurde von seinen Zeitgenossen weder verstanden noch gewürdigt. Es wäre verlorengegangen, wenn er nicht am Vorabend seines Duells seine Resultate in einem Brief an seinen Freund Auguste Chevalier zusammengefasst hätte. Ob das Duell ein politisches war oder es um eine Frau ging, wird wohl nie geklärt werden. Erst 1846 wurde sein Nachlass herausgegeben. Als Cauchy seine im alt hergebrachten Stil verfassten Arbeiten zur Auflösbarkeit von Polynomgleichungen publizierte, erkannte Liouville die wesentliche Bedeutung der Galois'schen Arbeiten und gab sie 1846 heraus. Für weitere Informationen zu diesem Themenkreis sei auf die sehr lesenswerte Biographie von Rigatelli (1996, [25]) verwiesen.

Übungsaufgaben

VI.1 Bestimme die Symmetriegruppe des Tetraeders. Ist dies eine schon bekannte Gruppe?

VI.2 Seien $f \in \mathbb{Q}[x]$ und $K \subseteq \mathbb{C}$ der Zerfällungskörper von f. Es habe f paarweise verschiedene Wurzeln in K. Ist G_f transitiv auf den Nullstellen von f, so ist f irreduzibel über $\mathbb{Q}$.

VI.3 Sei $K \subseteq \mathbb{C}$ ein Zerfällungskörper von $f = x^3 - 2 \in \mathbb{Q}[x]$. Zeige, dass $G_f \cong \Sigma_3$ ist.

VI.4 Sei $K \subseteq \mathbb{C}$ der Zerfällungskörper von $f \in \mathbb{Q}[x]$. Weiter sei G_f eine endliche einfache Gruppe. Ist $\mathbb{Q} \subseteq M \subseteq K$ und M Zerfällungskörper eines Polynoms $g \in \mathbb{Q}[x]$, so ist $M = \mathbb{Q}$ oder $M = K$.

VII Konstruktion mit Zirkel und Lineal

In diesem Kapitel wollen wir die Resultate über algebraische Körpererweiterungen auf Probleme der Geometrie anwenden. Dazu gehört zunächst die Übersetzung geometrischer Fragestellungen in die Sprache der Algebra.

Sei $P_0 \subseteq \mathbb{R}^2$ eine Punktmenge. Wir betrachten die folgenden zwei Operationen:

(L): Durch zwei Punkte aus P_0 ziehe eine Gerade.

(Z): Schlage einen Kreis um einen Punkt aus P_0. Hierbei sei der Radius der Abstand zweier Punkte aus P_0.

Achtung! Unser Lineal (L) hat keine Einteilung. Man kann damit also keine Strecken fester Länge, z.B. 2 cm, abtragen.

Definition

Konstruierbar. Sei $P_0 \subseteq \mathbb{R}^2$ eine Punktmenge.

a) Die Schnittpunkte von Geraden und Kreisen, die mit (L) und (Z) konstruiert werden, nennen wir *im ersten Schritt aus P_0 konstruierbare Punkte*.

b) Ein Punkt $r \in \mathbb{R}^2$ wird *von P_0 aus konstruierbar* genannt, falls es eine Kette von Punkten $r_1, \ldots, r_n = r$ gibt, so dass jedes r_i, $i = 1, \ldots, n$, im ersten Schritt aus der Menge $P_0 \cup \{r_1, \ldots, r_{i-1}\}$ konstruierbar ist.

c) Mit K_0 bezeichnen wir den Unterkörper von $\mathbb{R}$, der von den Koordinaten der Punkte von P_0 erzeugt wird.

d) Sei $r_1, \ldots, r_n = r$, $r_i = (x_i, y_i)$, im ersten Schritt aus $P_0 \cup \{r_1, \ldots, r_{i-1}\}$ konstruierbar. Dann setze

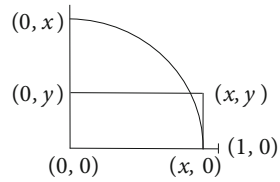
$$K_i = K_{i-1}(x_i, y_i),\ i = 1, \ldots, n.$$

Wir haben also in d) eine Kette $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$ von Körpern, die den Koordinaten der Punkte zugeordnet sind. Diese Kette spiegelt die einzelnen Schritte der Konstruktion des Punktes r wider.

Alles ist natürlich von der Startmenge P_0 abhängig. Wir werden ab jetzt stets annehmen, dass $(0, 0)$ und $(1, 0)$ in P_0 sind. Dadurch sind dann die Koordinatenachsen konstruierbar. Wir werden aber sehen, dass noch mehr gilt.

Lemma VII.1 *Sei $P_0 \subseteq P \subseteq \mathbb{R}^2$. Dann ist (x, y) genau dann aus P konstruierbar, wenn $(0, x)$ und $(0, y)$ aus P konstruierbar sind.*

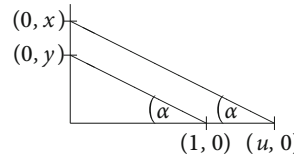
Beweis. Aus $(0, 0)$ und $(1, 0)$ können wir die Koordinatenachsen konstruieren. Ist (x, y) gegeben, so können wir die Parallelen durch (x, y) zu den Achsen konstruieren. Also können $(0, x)$ und $(0, y)$ konstruiert werden.



Sind umgekehrt $(0, x)$ und $(0, y)$ gegeben, so können wir daraus (x, y) konstruieren. Wir können zunächst $(x, 0)$ konstruieren. Der Schnittpunkt der Senkrechten durch $(x, 0)$ und $(0, y)$ liefert dann (x, y). □

Lemma VII.2 *Sei $P_0 \subseteq P \subseteq \mathbb{R}^2$. Sind $(0, x)$ und $(0, y)$ aus P konstruierbar, so auch die Punkte $(0, x \pm y)$, $(0, xy)$ und $(0, x/y)(y \neq 0)$.*

Beweis. Der Kreis um $(0, y)$ mit Radius $\overline{0x}$ schneidet die y-Achse in $(0, x + y)$ und $(0, x - y)$. Somit sind $(0, x \pm y)$ konstruierbar.



Sei $y \neq 0$. Verbinde $(0, y)$ mit $(1, 0)$. Danach ziehe eine Parallele zur Geraden $(0, y)(1, 0)$ durch $(0, x)$. Dann erhalten wir den Schnittpunkt $(u, 0)$ mit der x-Achse. Es ist $u/x = \tan\alpha = 1/y$. Das liefert $u = x/y$. Damit ist auch $(0, x/y)$ konstruierbar.

Wähle nun $x = 1$. Ist $y \neq 0$, so haben wir gerade gezeigt, dass $(0, 1/y)$ konstruierbar ist. Aus $(0, x)$ und $(0, 1/y)$ kann nun auch $(0, x(1/y)^{-1}) = (0, xy)$ konstruiert werden. □

Lemma VII.3 *Sei $P_0 \subseteq \mathbb{R}^2$ mit $(0, 0), (1, 0) \in P_0$. Sind $x, y \in K_0$, so ist (x, y) aus P_0 konstruierbar.*

Beweis. Wir wollen die Behauptung aus Lemma VII.1 und Lemma VII.2 folgern. Dazu setzen wir dort $P = P_0$. Sei zunächst $(x, y) \in P_0$. Nach Lemma VII.1 sind dann $(0, x)$ und $(0, y)$ aus P_0 konstruierbar. Es wird K_0 von den Koordinaten der Punkte aus P_0 erzeugt. Nach Lemma VII.2 sind somit alle $(0, k)$ mit $k \in K_0$ aus P_0 konstruierbar. Nach Lemma VII.1 sind dann alle (x, y) mit $x, y \in K_0$ aus P_0 konstruierbar. □

Da der Körper K_0 stets $\mathbb{Q}$ enthält, sind also alle Punkte mit rationalen Koordinaten konstruierbar.

Nun stellen wir den Zusammenhang zu algebraischen Körpererweiterungen her.

Lemma VII.4 *Sei $P_0 \subseteq \mathbb{R}^2$ und $r = (x, y)$ im ersten Schritt aus P_0 konstruierbar. Dann sind x und y Nullstellen quadratischer Polynome mit Koeffizienten in K_0.*

Beweis. Es gibt drei Fälle.

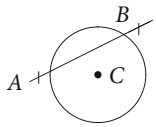
(1) r ist Schnittpunkt zweier Geraden.

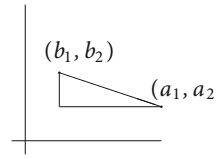
(2) r ist Schnittpunkt eines Kreises mit einer Geraden.

(3) r ist Schnittpunkt zweier Kreise.

Wir wollen nur den zweiten Fall betrachten. Die anderen seien dem Leser überlassen.

Wir haben eine Gerade durch die Punkte $A = (a, b)$ und $B = (c, d)$ und einen Kreis mit Mittelpunkt $C = (t, s)$ und Radius r, der der Abstand zwischen (a_1, a_2) und (b_1, b_2) ist, $a_1, a_2, b_1, b_2, t, s, a, b, c, d \in K_0$.





Es gilt nach Pythagoras

$$(b_1 - a_1)^2 + (a_2 - b_2)^2 = r^2 \in K_0.$$

Die Kreisgleichung ist

$$(x - t)^2 + (y - s)^2 = r^2.$$

Die Geradengleichung ist

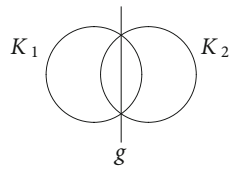
$$(x - a)(s - b) = (y - b)(t - a).$$

Das liefert für den Schnittpunkt (x-Koordinate)

$$(x - t)^2 + \left(\frac{(s - b)}{(t - b)}(x - a) + (b - s)\right)^2 = r^2.$$

Damit ist x Nullstelle einer quadratischen Gleichung. Genauso ist y Nullstelle einer quadratischen Gleichung.

Der Fall (3) kann auf Fall (2) zurückgeführt werden.



Statt K_1 schneidet K_2 kann auch K_1 schneidet g betrachtet werden. □

Als Konsequenz erhalten wir

Satz VII.5 *Sei $P_0 \subseteq \mathbb{R}$ und $r = (x, y)$ aus P_0 konstruierbar. Dann sind $[K_0(x): K_0]$ und $[K_0(y): K_0]$ 2-Potenzen.*

Beweis. Sei $r_1, \ldots, r_n = r$ eine Kette von Punkten im $\mathbb{R}^2$, wobei die $r_i = (x_i, y_i)$ im ersten Schritt aus $P_0 \cup \{r_1, \ldots, r_{i-1}\}$ konstruierbar seien. Nach Lemma VII.4 haben die x_i und y_i ein Minimalpolynom vom Grad höchstens zwei über K_{i-1}. Also ist nach Satz II.12 $[K_{i-1}(x_i): K_{i-1}] = 1$ oder 2 und $[K_{i-1}(y_i): K_{i-1}] = 1$ oder 2. Der Gradsatz liefert nun

$$[K_i: K_{i-1}] = [K_{i-1}(x_i, y_i): K_{i-1}] =$$

$$[K_{i-1}(x_i, y_i): K_{i-1}(x_i)][K_{i-1}(x_i): K_{i-1}] = 1, 2 \text{ oder } 4.$$

Dies bedeutet, dass $[K_i: K_{i-1}]$ eine 2-Potenz ist. Da nach dem Gradsatz

$$[K_n: K_0] = [K_n: K_{n-1}][K_{n-1}: K_{n-2}] \ldots [K_1: K_0]$$

ist, ist $[K_n: K_0]$ eine 2-Potenz. Wegen

$$[K_n: K_0(x)][K_0(x): K_0] = [K_n: K_0] \text{ und}$$
$$[K_n: K_0(y)][K_0(y): K_0] = [K_n: K_0]$$

sind $[K_0(x): K_0]$ und $[K_0(y): K_0]$ 2-Potenzen. □

Satz VII.5 kann schon benutzt werden, um zu zeigen, dass gewisse Dinge nicht konstruierbar sind.

Satz VII.6 *Die Verdoppelung des Würfels ist nicht möglich. Das heißt, ist der Einheitswürfel gegeben, so ist es nicht möglich, die Seite eines Würfels mit doppeltem Volumen aus den Daten des gegebenen Würfels, also $P_0 = \{(0, 0), (1, 0)\}$, zu konstruieren.*

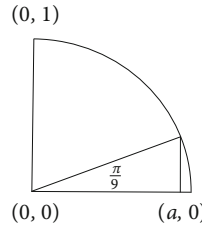
Beweis. Wir müssen aus einem Würfel mit einer Ecke auf $(0, 1)$ einen neuen konstruieren, der eine Ecke auf $(0, \sqrt[3]{2})$ hat. Also ist $r = (0, \sqrt[3]{2})$ aus $P_0 = \{(0.0), (1, 0)\}$ zu konstruieren. Das heißt, wir haben $\mathbb{Q} = K_0$. Ist r konstruierbar, so ist nach Satz VII.5 $[\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}]$ eine 2-Potenz. Aber $x^3 - 2$ ist nach Eisenstein irreduzibel, d.h.

$$[\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}] = 3$$

nach Satz II.12. Dies ist ein Widerspruch. □

Satz VII.7 *Der Winkel $60° = \pi/3$ kann nicht gedrittelt werden.*

Beweis. Ist die Drittelung des Winkels $\pi/3$ möglich, so kann auch der Punkt $(a, 0)$ mit $a = \cos \pi/9$ konstruiert werden. Es ist $(\cos \pi/3, 0) = (\frac{1}{2}, 0) \in P_0$.



Dann ist aber auch der Punkt $(y, 0)$ mit $y = 2\cos \pi/9$ konstruierbar. Mit Satz VII.5 erhalten wir, dass $[\mathbb{Q}(y):\mathbb{Q}]$ eine 2-Potenz ist. Es gilt die Formel

$$\cos \pi/3 = 4\cos^3 \pi/9 - 3\cos \pi/9,$$

also

$$\frac{1}{2} = \frac{1}{2}y^3 - \frac{3}{2}y$$

und dann auch

$$y^3 - 3y - 1 = 0.$$

Da ± 1 keine Nullstellen von $x^3 - 3x - 1$ sind, ist $x^3 - 3x - 1 \in \mathbb{Q}[x]$ irreduzibel. Also gilt nach Satz II.12 $[\mathbb{Q}(y):\mathbb{Q}] = 3$. Damit ist $(y, 0)$ nicht konstruierbar. □

Die Quadratur des Kreises ist nicht möglich. **Satz VII.8**

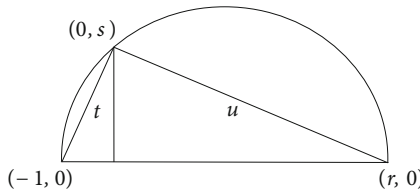
Beweis. Dies folgt aus der Tatsache, dass π nicht algebraisch ist. □

Diese Resultate waren alle von destruktiver Art. Wenn wir beweisen wollen, dass etwas konstruierbar ist, müssen wir also anders vorgehen, insbesondere eine Art Umkehrung von Satz VII.5 beweisen. Einen ersten Schritt in diese Richtung liefert der nächste Satz.

Sei P_0 eine Punktmenge mit $(0, 0), (1, 0) \in P_0$. Sei $K_0 \subseteq L \subseteq \mathbb{R}$ mit $[L:K_0] = 2$, so ist jeder Punkt $(x, y) \in L^2$ aus P_0 konstruierbar. **Satz VII.9**

Beweis. Es ist $L = K_0(\alpha)$, wobei α Nullstelle eines Polynoms $x^2 + px + q \in K_0[x]$ ist. Da $\alpha \in \mathbb{R}$ ist, ist $p^2 - 4q \geq 0$ und $\alpha = \frac{1}{2}(-p + \sqrt{p^2 - 4q})$. Kann man $(0, \sqrt{r})$ für alle $r \in K_0$, $r \geq 0$ aus P_0 konstruieren, so setze $P = P_0 \cup \{(0, \sqrt{p^2 - 4q})\}$. Dann ist L der von den Koordinaten der Punkte aus P erzeugte Körper. Nach Lemma VII.3 sind dann alle $(x, y) \in L^2$ aus P und damit auch aus P_0 konstruierbar.

Wir zeigen nun, dass $(0, \sqrt{r})$ für $r \in K_0$, $r \geq 0$, konstruierbar ist. Wieder können wir die Koordinatenachsen konstruieren. Da $r \in K_0$ ist, können wir nach Lemma VII.3 auch $(-1, 0)$ und $(r, 0)$ konstruieren.



Wir können die Strecke $\overline{(-1,0)(r,0)}$ halbieren und dann den Kreis um diesen Mittelpunkt mit $\overline{(-1,0)(r,0)}$ als Durchmesser konstruieren. Dieser trifft die y-Achse im Punkt $(0,s)$. Somit ist der Punkt $(0,s)$ konstruierbar. Wir zeigen jetzt, dass $s=\sqrt{r}$ gilt. Es sind $s^2+1=t^2$, $s^2+r^2=u^2$ und $t^2+u^2=(r+1)^2$. Also ist $(r+1)^2=2s^2+1+r^2$, d.h. $s=\sqrt{r}$. □

Wir wollen uns nun noch der Konstruktion des regulären n-Ecks zuwenden. Dabei sei immer $P_0\subseteq\mathbb{Q}^2$. Das n-Eck sei dem Einheitskreis einbeschrieben.

Satz VII.10

Es seien $n,m\in\mathbb{N}$.

a) Ist das reguläre n-Eck konstruierbar, so ist für jeden Teiler m von n auch das reguläre m-Eck konstruierbar.

b) Sind sowohl das reguläre n-Eck als auch das reguläre m-Eck konstruierbar und ist $\mathrm{ggT}(n,m)=1$, so ist das reguläre nm-Eck konstruierbar.

Beweis.

a) Setze $d=n/m$. Verbinden wir jede d-te Ecke des regulären n-Ecks, so erhalten wir ein reguläres m-Eck.

b) Nach Annahme ist $\mathrm{ggT}(n,m)=1$. Damit gibt es $a,b\in\mathbb{Z}$ mit $am+bn=1$. Dies können wir auch als

$$\frac{1}{mn}=a\frac{1}{n}+b\cdot\frac{1}{m}$$

schreiben.

Also können wir aus $2\pi/n$ und $2\pi/m$ auch $2\pi/nm$ konstruieren, indem wir zunächst den Winkel $2\pi/n$ genau a–mal und dann b–mal den Winkel $2\pi/m$ abtragen, wobei wir dies im Uhrzeigersinn oder Gegenuhrzeigersinn machen, je nachdem, ob a bzw. b positiv oder negativ ist. □

Folgerung VII.11

Sei $n\in\mathbb{N}$ und $p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung. Das reguläre n-Eck kann genau dann konstruiert werden, wenn jedes reguläre $p_i^{\alpha_i}$-Eck konstruierbar ist.

Lemma VII.12

Das reguläre 2^α-Eck ist konstruierbar.

Beweis. Dies geschieht durch fortgesetzte Halbierung des Winkels, die mit Zirkel und Lineal möglich ist. □

Wir müssen jetzt nur noch feststellen, wann das reguläre p^n–Eck, für ungerade Primzahlen p, konstruierbar ist. Es geht also darum, den Punkt

$$(x,y)=(\cos 2\pi/p^n,\sin 2\pi/p^n),$$

eine Ecke des regulären p^n–Ecks, zu konstruieren. Die Idee ist, den $\mathbb{R}^2$ als die Gaußsche Zahlenebene $\mathbb{C}$ zu betrachten. Dann entspricht (x, y) der komplexen Zahl $x + iy$. Es ist $\epsilon = \cos 2\pi/p^n + i \sin 2\pi/p^n = e^{2\pi i/p^n}$ eine p^n–te Einheitswurzel. Ist (x, y) konstruierbar, so ist nach Satz VII.5 $[\mathbb{Q}(x, y) : \mathbb{Q}]$ eine 2-Potenz. Weiter ist $[\mathbb{Q}(x, y, i) : \mathbb{Q}(x, y)] = 2$. Dann ist $[\mathbb{Q}(\epsilon) : \mathbb{Q}]$ nach dem Gradsatz II.6 eine 2-Potenz. Das liefert den folgenden Satz:

Satz VII.13

Für eine ungerade Primzahl p und eine natürliche Zahl n sei das reguläre p^n-Eck konstruierbar. Weiter sei ϵ eine primitive p^n-te Einheitswurzel in $\mathbb{C}$ und m_ϵ das Minimalpolynom von ϵ über $\mathbb{Q}$. Dann ist grad m_ϵ *eine 2-Potenz.*

Sei ϵ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Gemäß Satz VII.13 müssen wir uns mit dem Minimalpolynom m_ϵ beschäftigen und sehen, wann dieses einen Grad hat, der eine 2-Potenz ist.

Lemma VII.14

Seien p eine ungerade Primzahl, ϵ eine primitive p-te Einheitswurzel in $\mathbb{C}$ und m_ϵ das Minimalpolynom von ϵ über $\mathbb{Q}$. Dann ist

$$m_\epsilon = x^{p-1} + x^{p-2} + \cdots x + 1.$$

Beweis. Es ist ϵ Nullstelle von $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$. Nach Beispiel b) auf Seite 27 ist dieses Polynom irreduzibel. □

Lemma VII.15

Seien p eine ungerade Primzahl, ϵ eine primitive p^2-te Einheitswurzel in $\mathbb{C}$ und m_ϵ das Minimalpolynom von ϵ über $\mathbb{Q}$. Dann ist

$$m_\epsilon = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1.$$

Beweis. Es ist ϵ Nullstelle von $g = x^{p^2} - 1/x^p - 1 = x^{p(p-1)} + \cdots + x^p + 1$. Wir ersetzen x in g durch $1 + u$. Dann erhalten wir auf der linken Seite

$$g(x) = g(1 + u) = \frac{(1 + u)^{p^2} - 1}{(1 + u)^p - 1} = \frac{(1 + u^{p^2}) - 1}{(1 + u^p) - 1} \equiv u^{p(p-1)} \pmod{p}.$$

Beachte hierbei, dass das Potenzieren mit p modulo p nach Lemma II.3 ein Homomorphismus ist. Also erhalten wir

$$g(1 + u) = u^{p(p-1)} + pf(u), \text{ mit } f \in \mathbb{Z}[x].$$

Andererseits, wenn wir $1 + u$ in die rechte Seite einsetzen, erhalten wir

$$g(1 + u) = 1 + (1 + u)^p + \cdots + (1 + u)^{p(p-1)}.$$

Setzen wir jetzt $u = 0$ ein, so ergibt sich

$$p = g(1 + 0) = pf(0).$$

Das liefert $f(0) = 1$. Somit sind alle Koeffizienten von g, außer dem höchsten, durch p teilbar und das Absolutglied ist nicht durch p^2 teilbar. Mit dem Satz von Eisenstein erhalten wir, dass g irreduzibel ist. □

Dies zusammenfassend erhalten wir:

Satz VII.16 *Sei p eine ungerade Primzahl. Ist das reguläre p^n-Eck konstruierbar, so ist $n = 1$ und p eine Fermatzahl, d.h. $p = 2^m + 1$ für ein $m \in \mathbb{N}$.*

Beweis. Ist $n \geq 2$, so ist nach Satz VII.10 a) auch das reguläre p^2-Eck konstruierbar. Nach Satz VII.15 und Satz VII.13 ist dann $p(p-1)$ eine 2-Potenz, was nicht möglich ist. Also ist $n = 1$. Nach Satz VII.13 und Lemma VII.14 ist dann $p - 1$ eine 2-Potenz, also ist p eine Fermatzahl. □

Es gilt auch die Umkehrung, dass das reguläre p-Eck für p eine Fermatzahl konstruierbar ist. Der Beweis beruht wieder wesentlich auf Bemerkung a) aus Kapitel VI Seite 107.

Satz VII.17 *Ist p eine Fermatprimzahl, so ist das reguläre p-Eck konstruierbar.*

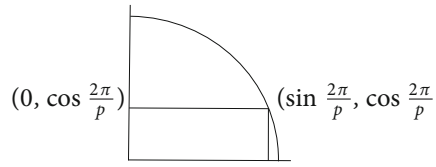
Beweis. Sei ϵ eine primitive p-te Einheitswurzel. Nach Lemma VII.14 ist dann $[\mathbb{Q}(\epsilon):\mathbb{Q}] = p - 1 = 2^n$. Es ist $\mathbb{Q}(\epsilon)$ Zerfällungskörper über $\mathbb{Q}$ von m_ϵ, da alle Einheitswurzeln Potenzen von ϵ sind. Sei G die zugehörige Galoisgruppe und $g, h \in G$. Dann ist $g(\epsilon) = \epsilon^i$ und $h(\epsilon) = \epsilon^j$ für i, j geeignet. Also ist $gh = hg$, d.h. G ist abelsch. Nach Satz VI.1 ist G transitiv auf den Nullstellen von m_ϵ. Ist $g \in G$ mit $g(\epsilon) = \epsilon$, so ist g die Identität auf $\mathbb{Q}(\epsilon)$. Also ist $G_\epsilon = 1$. Nach Lemma V.15 ist dann $|G| = p - 1$. Somit ist $|G|$ eine 2-Potenz. Nach Satz V.18 gibt es eine Kette von Normalteilern

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_n = G, \text{ mit } |N_{i+1}/N_i| = 2.$$

Zu jedem Normalteiler gehört nach der Bemerkung a) auf Seite 107 im vorherigen Kapitel ein Zwischenkörper. Also ist

$$\mathbb{Q} = K_0 \subseteq \cdots \subseteq K_n = \mathbb{Q}(\epsilon).$$

Dabei ist $K_i = \text{Fix}\,(N_{n-i})$. Da $N_i \neq N_{i+1}$ ist, ist $K_i \neq K_{i-1}$. Da $|G| = [\mathbb{Q}(\epsilon):\mathbb{Q}]$ ist, ist $[K_i : K_{i-1}] = 2$. Wir bilden nun $K_i \cap \mathbb{R}$. Dann ist $[K_i \cap \mathbb{R} : K_{i-1} \cap \mathbb{R}] \leq 2$. Also sind alle Elemente in $(\mathbb{Q}(\epsilon) \cap \mathbb{R})^2$ nach Satz VII.9 konstruierbar.



Es ist $\cos\frac{2\pi}{p} = (\epsilon+\bar{\epsilon})/2 \in \mathbb{Q}(\epsilon)\cap\mathbb{R}$. Damit ist $(0, \cos\frac{2\pi}{p})$ konstruierbar. Wenn wir die Senkrechte auf der y-Achse in $(0, \cos\frac{2\pi}{p})$ mit dem Einheitskreis schneiden, erhalten wir $(\sin\frac{2\pi}{p}, \cos\frac{2\pi}{p})$. □

Der hier gegebene Beweis geht auf Gauß zurück, der feststellte, dass das reguläre 17–Eck konstruierbar ist, und damit am 30.3.1796 ein 2000 Jahre altes Problem löste. Die allgemeine Theorie findet sich in den Disquisitiones Arithmeticae.

Es ist übrigens

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)$$

$$+\frac{1}{16}\left(\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}}\right).$$

Übungsaufgaben

VII.1 Die folgenden Konstruktionen sind mit Zirkel und Lineal durchzuführen:

a) Konstruiere aus $P_0 = \{(0,0),(1,0)\}$ den Punkt $(0,\sqrt{5})$.

b) Sei g eine Gerade und $P = (x,y)$ ein Punkt, der nicht auf g liegt. Konstruiere die Parallele zu g durch den Punkt P.

VII.2 Beschreibe eine Konstruktion des regulären 5-Ecks.

VII.3 Zeige, dass ein Winkel α mit $\cos(\alpha) = \frac{11}{16}$ mit Zirkel und Lineal in drei gleiche Teile geteilt werden kann.

VIII Summe von Quadraten

In diesem und dem nächsten Kapitel kommen wir wieder zur Zahlentheorie zurück. Wir werden sehen, dass wir unsere Resultate aus der Algebra gut anwenden können. Zunächst beschäftigen wir uns mit der folgenden Frage:

Welche natürlichen Zahlen n sind Summe von zwei Quadraten ganzer Zahlen, also

$$n = x^2 + y^2.$$

Wie wir bereits im Beispiel auf Seite 71 gesehen haben, ist $n \equiv 1 (\mathrm{mod}\ 4)$ notwendig. Wie wir an $n = 21$ sehen können, ist das nicht hinreichend.

Betrachten wir zunächst eine Variante

$$n = x^2 - y^2,$$

so sehen wir

$$n = x^2 - y^2 = (x - y)(x + y).$$

Ist $n = m_1 m_2$, so setze $m_1 = x - y$, $m_2 = x + y$. Dann ist $x = \frac{m_1 + m_2}{2}$, $y = \frac{m_2 - m_1}{2}$.

Die Idee hierbei war, aus der additiven Form des Problems eine multiplikative Form zu machen. Dann haben wir die Zahlentheorie mit der Primfaktorzerlegung zur Verfügung. Wir suchen somit eine Faktorisation von $x^2 + y^2$. Diese finden wir nicht in $\mathbb{Z}$. Ein allgemeines und sehr effektives Verfahren in der Zahlentheorie ist es, in solchen Fällen den Zahlbereich zu erweitern. Dies machen wir hier auch so und gehen zu $\mathbb{Z}[i]$ über, wo wir eine Faktorisation haben:

$$n = x^2 + y^2 = (x + iy)(x - iy).$$

Dies bedeutet, dass n eine Norm in $\mathbb{Z}[i]$ ist. Also ist unsere Frage jetzt:

Welche natürlichen Zahlen sind Normen in $\mathbb{Z}[i]$?

Es kommt uns zur Hilfe, dass die Norm multiplikativ ist. Ist also

$$n = x_1^2 + y_1^2,\ m = x_2^2 + y_2^2,$$

so ist

$$nm = |(x_1 + iy_1)(x_2 + iy_2)|^2 = x_3^2 + y_3^2$$

mit $x_3 = x_1 x_2 - y_1 y_2$ und $y_3 = x_1 y_2 + x_2 y_1$.

Ist umgekehrt $n = x^2 + y^2$ und m ein Teiler von n, so muss nicht $m = x_1^2 + y_1^2$ sein, wie das Beispiel $n = 21^2 = 21^2 + 0^2$ und $m = 21$ zeigt. Dennoch gibt es etwas, das annähernd einer Umkehrung gleichkommt.

Sei dazu zunächst p eine Primzahl, die auch in $\mathbb{Z}[i]$ prim ist. Sei weiter

$$p \text{ ein Teiler von } n = x^2 + y^2 = (x + iy)(x - iy).$$

Da p prim in $\mathbb{Z}[i]$ ist, ist p ein Teiler von $x + iy$ oder $x - iy$. Wir können annehmen, dass $x + iy$ von p geteilt wird. Dann ist

$$x + iy = p(a + ib).$$

Also ist $x = pa$ und $y = pb$, d.h., p teilt x und y. Dann teilt p^2 auch $x^2 + y^2 = n$. Nun ist

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2.$$

Damit ist auch $\frac{n}{p^2}$ eine Summe von zwei Quadraten. Indem wir dies so weiter fortsetzen, erhalten wir, dass die Primzahlen aus $\mathbb{Z}$, die prim in $\mathbb{Z}[i]$ bleiben, mit geradem Exponenten in der Primfaktorenzerlegung von n auftauchen. Dies hilft uns allerdings noch wenig, solange wir die Frage, welche Primzahlen in $\mathbb{Z}$ bleiben prim in $\mathbb{Z}[i]$, nicht beantworten können.

Schauen wir uns erst einmal den umgekehrten Fall an. Sei also p prim in $\mathbb{Z}$, aber nicht in $\mathbb{Z}[i]$.

Dann ist

$$p = (a + ib)(c + id),$$

wobei $a + id$ und $c + id$ keine Einheiten sind, d.h. $a^2 + b^2 \neq 1 \neq c^2 + d^2$. Dann erhalten wir mit unserem alten Trick

$$p^2 = p\bar{p} = (a + ib)(a - ib)(c + id)(c - id) = (a^2 + b^2)(c^2 + d^2).$$

Die Primfaktorenzerlegung in $\mathbb{Z}$ liefert mit $a^2 + b^2 \neq 1 \neq c^2 + d^2$ dann

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

Also ist $p = 2 = 1^2 + 1^2$ oder $p \equiv 1 \pmod 4$ nach dem Beispiel a) auf Seite 71 in Kapitel IV. Somit bleibt jede Primzahl, die kongruent 3 modulo 4 ist, prim in $\mathbb{Z}[i]$. Damit erhalten wir erstens

Lemma VIII.1 *Ist p eine Primzahl in $\mathbb{Z}$, die nicht prim in $\mathbb{Z}[i]$ ist, so ist p eine Summe von zwei Quadraten.*

und zweitens

Satz VIII.2 *Ist $n = x^2 + y^2$, so kommt jeder Primteiler $p \equiv 3 \pmod 4$ von n in der Primfaktorzerlegung von n mit geradem Exponenten vor.*

Es ist $2 = 1^2 + 1^2$. Um zu demonstrieren, dass die Bedingung in Satz VIII.2 auch hinreichend ist, wollen wir jetzt zeigen, dass jede Primzahl p mit $p \equiv 1 (\mathrm{mod}\, 4)$ eine Norm in $\mathbb{Z}[i]$ ist. Dazu machen wir folgende Überlegung:

Sei -1 ein Quadrat modulo p, also

$$x^2 \equiv -1 (\mathrm{mod}\, p)$$

hat eine Lösung $w \in \mathbb{Z}$. Dann ist

$$p \text{ ein Teiler von } w^2 + 1 = (w + i)(w - i).$$

Ist p prim in $\mathbb{Z}[i]$, so können wir ohne Einschränkung der Allgemeinheit annehmen, dass p ein Teiler von $w + i$ ist. Also $p(a + bi) = w + i$. Dann ist $pb = 1$ ein Widerspruch dazu, dass p eine Primzahl ist. Also ist p kein Primelement in $\mathbb{Z}[i]$. Nach Lemma VIII.1 ist dann $p = a^2 + b^2$ mit geeigneten a, b.

Es genügt also zu zeigen, dass für $p \equiv 1 (\mathrm{mod}\, 4)$ stets -1 ein Quadrat modulo p ist.

Wir betrachten dazu die multiplikative Gruppe von $\mathbb{Z}/p\mathbb{Z}$. Nach Satz III.7 ist diese zyklisch von der Ordnung $p - 1$. Sei g ein Erzeuger. Da $(p - 1)/4 \in \mathbb{N}$ ist, können wir $h = g^{p-1/4}$ bilden. Dann ist $o(h) = 4$, d.h., h ist Nullstelle von $x^4 - 1$, aber nicht von $x^2 - 1$. Also ist h Nullstelle von $x^2 + 1$. d.h. $h^2 = -1$. Damit haben wir, dass -1 ein Quadrat modulo p ist. Wir haben also bewiesen:

Ist p eine Primzahl mit $p \equiv 1 (\mathrm{mod}\, 4)$, so ist -1 ein Quadrat modulo p. **Lemma VIII.3**

Dies liefert jetzt das gewünschte Resultat:

Es ist $n = x^2 + y^2$ mit $n \in \mathbb{N}$ genau dann, wenn jede Primzahl p mit $p \equiv 3 (\mathrm{mod}\, 4)$ in der Primfaktorzerlegung von n mit geradem Exponenten vorkommt. **Satz VIII.4**

Dieses sehr effektive Verfahren, den Zahlenbereich zu erweitern, um multiplikative Darstellungen zu bekommen, kann man auch bei anderen Fragestellungen anwenden.

Betrachten wir die Fermat-Gleichung

$$x^p + y^p = z^p, x, y, z \in \mathbb{N}$$

mit einer ungeraden Primzahl p. Wir können diese umschreiben in der Form

$$x^p = z^p - y^p.$$

Sei nun ϵ eine p-te Einheitswurzel ungleich 1. Dann ist

$$z^p - y^p = (z - y)(z - \epsilon y)(z - \epsilon^2 y) \cdots (z - \epsilon^{p-1} y).$$

Also ist

$$x^p = (z-y)(z-\epsilon y)(z-\epsilon^2 y)\cdots(z-\epsilon^{p-1}y).$$

Dies ist eine Zerlegung in dem Ring

$$\mathbb{Z}[\epsilon] = \{a_0 + a_1\epsilon + a_2\epsilon^2 + \cdots + a_{p-2}\epsilon^{p-2} \mid a_i \in \mathbb{Z}\}.$$

Da $\epsilon^{p-1} = -(1\epsilon + \cdots + \epsilon^{p-2})$ ist, ist dies in der Tat ein Ring. Nun haben wir eine Zerlegung und können versuchen zu zeigen, dass die einzelnen Faktoren selbst p-te Potenzen sind, was gehen sollte, wenn wir die Primfaktoren (in $\mathbb{Z}[\epsilon]$) auf beiden Seiten vergleichen. Dies könnte dann einen Beweis für $p > 2$ liefern, dass die Fermat-Gleichung keine Lösungen $x, y, z \in \mathbb{N}$ hat. Leider hat dieser Ring im Allgemeinen für $p > 19$ keine eindeutige Primfaktorzerlegung mehr. Das führte Ernst Kummer[1] dazu, sogenannte *ideale Zahlen* einzuführen. Dies waren nicht mehr einzelne Elemente eines Ringes, sondern Teilmengen. Hieraus ist dann der Begriff *Ideal* entstanden. Kummer hat gezeigt, dass sich algebraische Zahlen, und $\mathbb{Z}[\epsilon]$ ist ein Beispiel dafür, wenn sie sich zwar nicht eindeutig in Primzahlen zerlegen lassen, doch eindeutig in diese idealen Zahlen faktorisieren lassen. Hiermit hat er dann den Satz von Fermat für sogenannte reguläre Primzahlen (unter 100 sind dies alle außer 37, 59 und 67) bewiesen. In der Welt der Ideale übernehmen die Primideale die Rolle der Primelemente, und die Begriffe irreduzibles Ideal und Primideal fallen hier wieder zusammen.

Wir haben gesehen, dass jede Primzahl p mit $p \equiv 1 \pmod 4$ eine Summe von zwei Quadraten ist. Es gilt aber sogar:

Satz VIII.5 *Sei $p \equiv 1 \pmod 4$, p prim. Dann ist die Darstellung $p = x^2 + y^2$ mit $x, y \in \mathbb{N} \cup \{0\}$ bis auf die Reihenfolge eindeutig.*

Beweis. Sei $p = x^2 + y^2 = a^2 + b^2$. Wir können x, b ungerade und y, a gerade annehmen. Es ist

$$x^2a^2 - y^2b^2 = (x^2 + y^2 - y^2)a^2 - y^2b^2 = (x^2 + y^2)(a^2 - y^2).$$

Da $p = x^2 + y^2$ ist, teilt p dann $x^2a^2 - y^2b^2$. Also ist

$$p \text{ ein Teiler von } (xa - yb)(xa + yb).$$

Es sind alle $x, y, a, b < \sqrt{p}$. Sei zunächst p ein Teiler von $ay + yp$. Wir haben dann $0 < xa + yb < 2p$. Also ist $p = xa + yb$. Aber 2 teilt $xa + yb$, ein Widerspruch zu $xa + yb < 2p$. Somit ist p ein Teiler von $xa - yb$. Ist $xa - yb > 0$, so erhalten wir wie eben $xa - yb = p$, aber $xa - yb$ ist gerade, ein Widerspruch. Das liefert $xa - yb = 0$. Da ggT $(x, y) = 1$ ist, folgt x teilt b und y teilt a, d.h. $x = b$, $y = a$. □

[1] Ernst Eduard Kummer (*29.1.1810 Sorau, †14.5.1893 Berlin) war zunächst 10 Jahre lang Lehrer an einem Gymnasium, bevor er Nachfolger von Dirichlet in Berlin wurde. Hauptarbeitsgebiete waren algebraische Geometrie und Zahlentheorie. Bekannt ist die Kummersche Fläche. Durch seine Beiträge zum Fermatschen Satz wurde er zum Wegbereiter der Klassenkörpertheorie und damit der algebraischen Zahlentheorie.

Interessant ist, dass auch die Umkehrung gilt. Der Beweis sei dem Leser überlassen.

Satz VIII.6 *Sei $g \in \mathbb{N}, g \equiv 1 (\mathrm{mod}\, 4), g \neq 1$. Ist g auf genau eine Art als Summe zweier Quadrate darstellbar, $g = x^2 + y^2,\ x, y \in \mathbb{N} \cup \{0\}, \mathrm{ggT}(x, y) = 1$, so ist g eine Primzahl.*

Man kann sich nun fragen, wie das mit der Summe von drei Quadraten aussieht. Die Antwort hierauf ist nicht ganz einfach. Überraschend ist aber, dass Lagrange 1770 zeigen konnte: *Jede natürliche Zahl ist Summe von vier Quadraten.*

Nun kann man ja auch anstelle Quadraten Kuben, Biquadrate oder allgemein n-te Potenzen betrachten. Sei $k \geq 2$. Bezeichne mit $g(k)$ die kleinste natürliche Zahl, so dass sich jede natürliche Zahl als Summe von $g(k)$ vielen, nicht negativen k–ten Potenzen schreiben läßt. Die Bestimmung dieser Funktion $g(k)$ ist als Waring[2]-Problem bekannt. Indem man die Zahl $n = 2^k \lfloor \left(\frac{3}{2}\right)^k \rfloor - 1$ als Summe von k-ten Potenzen schreibt, kann man elementar zeigen, dass

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

ist. Die Vermutung ist, dass hier immer Gleichheit besteht. Dies ist bewiesen für $k \leq 471600000$, also $g(2) = 4, g(3) = 9, g(4) = 19$ usw. Für $k > 471600000$ ist bekannt, dass es höchstens endlich viele k gibt, für die die Gleichheit nicht besteht.

Wir hatten in Lemma VIII.3 gesehen, dass für $p \equiv 1 (\mathrm{mod}\, 4)$ stets -1 ein Quadrat modulo p ist. Dies bedeutet, dass $x^2 + 1$ für diese p modulo p nicht irreduzibel ist. Ist aber $p \equiv 3 (\mathrm{mod}\, 4)$, so ist es irreduzibel. Anderenfalls wäre -1 ein Quadrat modulo p. Damit haben wir gesehen, dass der in Beispiel c) auf Seite 27 angegebene Algorithmus für das irreduzible Polynom $x^2 + 1 \in \mathbb{Z}[x]$ unendlich oft ein reduzibles Polynom liefert. Das heißt, es genügt dort nicht, die Primzahl möglichst groß zu wählen.

Die Frage, ob -1 ein Quadrat modulo p ist, ist nur ein Spezialfall der Frage, ob $x^2 \equiv a (\mathrm{mod}\, p)$ lösbar ist, wobei a vorgegeben ist.

Für ein konkretes p ist dies sicherlich kein Problem. Wir können die Frage durch Ausprobieren beantworten. Interessant ist aber die umgekehrte Frage. Für welche p ist a ein Quadrat modulo p. Für $a = -1$ hatten wir dies bereits beantwortet.

Lemma VIII.7 *Sei p eine ungerade Primzahl. Dann hat $x^2 \equiv -1 (\mathrm{mod}\, p)$ genau dann eine Lösung, falls $p \equiv 1 (\mathrm{mod}\, 4)$ ist.*

Im nächsten Kapitel wollen wir uns der allgemeineren Frage zuwenden. Wir werden dort einen der wichtigsten Sätze der Zahlentheorie beweisen, das quadratische Reziprozitätsgesetz, das besagt, dass dieses scheinbar unendliche Problem (für welche unendlich vielen p?) in Wirklichkeit ein endliches ist.

[2] Edward Waring (*1736 Old Heath, †15.8. 1798 Pontesbury) war ab 1760 Professor in Cambridge, seine Arbeitsgebiete waren Zahlentheorie und Geometrie.

Übungsaufgaben

VIII.1 a) Sei G eine endliche Gruppe. Zeige: Sind A, B Teilmengen von G mit $|A| > |G|/2 < |B|$, so ist $G = AB$. (Hinweis: für $g \in G$ ist $gB^{-1} \cap A \neq \varnothing$.)

b) In einem endlichen Körper ist jedes Element Summe von zwei Quadraten.

VIII.2 Zeige:

a) $n = 2^k$ und $n = 5 \cdot 2^k$ haben keine Darstellung als $n^2 = x^2 + y^2 + z^2$ mit $x, y, z \in \mathbb{Z}$, $xyz \neq 0$.

b) Es gibt keine allgemeingültige Gleichung der folgenden Form in $\mathbb{Z}$:

$$(x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) = z_1^2 + z_2^2 + z_3^2.$$

VIII.3 Zeige:

a) Sind $x, y \in \boldsymbol{N}$, so dass $x^2 + y^2$ von 4 geteilt wird, so sind x und y beide gerade.

b) Es gibt keine $x, y, z \in \boldsymbol{N}$ mit $x^2 + y^2 + z^2 = 2xyz$.

IX Das quadratische Reziprozitätsgesetz

In diesem Kapitel wollen wir uns mit der Lösung quadratischer Gleichungen modulo einer Primzahl p beschäftigen. Es ist klar, dass wir uns nur der Frage des Quadratwurzelziehens widmen müssen. Wir knüpfen an Lemma VIII.7 an und betrachten den allgemeinen Fall: Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(p, a) = 1$, wann hat

$$x^2 \equiv a (\mathrm{mod}\, p)$$

eine Lösung?

Dies ist nicht ganz eindeutig formuliert. Wir können z.B. p festhalten und dann nach den Zahlen a fragen. Dies ist sicherlich durch einfaches Probieren lösbar. Wir können aber auch a festhalten und nach den Primzahlen p fragen. Dies ist sicherlich nicht so einfach.

Weiter ist in dem Zusammenhang nur p ungerade sinnvoll, da modulo 2 jedes a ein Quadrat ist. Sei also ab jetzt stets p ungerade. Wir halten zunächst einmal p fest und betrachten die Quadrate

$$1^2, 2^2, \ldots, (p-1)^2.$$

Ist $1 \leq i \leq j \leq p-1$ und

$$i^2 \equiv j^2 (\mathrm{mod}\, p),$$

so ist p ein Teiler von $(i-j)(i+j)$. Also ist $i \equiv j (\mathrm{mod}\, p)$ oder $i \equiv p - j (\mathrm{mod}\, p)$. Somit kommt jedes Quadrat zweimal vor. Damit ist die Hälfte der Reste modulo p ein Quadrat.

Dies bedeutet, dass wir für die Hälfte der $1 \leq a \leq p-1$ eine Lösung von $x^2 \equiv a (\mathrm{mod}\, p)$ haben, für die andere nicht.

Ein erstes notwendiges Kriterium ist nun

Lemma IX.1

Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$. Hat

$$x^2 \equiv a (\mathrm{mod}\, p)$$

eine Lösung x, so ist $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$.

Beweis. $a^{\frac{p-1}{2}} \equiv x^{2\frac{p-1}{2}} \equiv x^{p-1} \underset{\text{(IV.14)}}{\equiv} 1 (\mathrm{mod}\, p)$. □

Gilt aber auch die Umkehrung? Folgt aus $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$, dass a ein quadratischer Rest ist?

Lemma IX.2

Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$. Hat

$$x^2 \equiv a (\mathrm{mod}\, p)$$

keine Lösung, so ist $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$.

Beweis. Nach dem kleinen Satz IV.14 von Fermat ist $(a^{\frac{p-1}{2}})^2 \equiv 1 (\mathrm{mod}\, p)$. Also ist $a^{\frac{p-1}{2}}$ eine Nullstelle von $x^2 - 1$ modulo p. Das liefert $a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$. Nun gilt aber bereits $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ für $\frac{p-1}{2}$ Werte von a. Da $x^{\frac{p-1}{2}} - 1$ modulo p höchstens $\frac{p-1}{2}$ viele Nullstellen hat, gilt für alle anderen Werte $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$. □

Damit haben wir nun ein notwendiges und hinreichendes Kriterium:

Lemma IX.3

Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$. Dann gibt es für $x^2 \equiv a (\mathrm{mod}\, p)$ genau dann eine Lösung x, falls $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ ist.

Beispiel

Betrachte $x^2 \equiv 7 (\mathrm{mod}\, 31)$. Es ist $7^{(31-1)/2} = 7^{15}$ zu berechnen.

$$\begin{aligned}
7^2 &= 49 \equiv 18 && (\mathrm{mod}\, 31)\\
7^4 &\equiv 18^2 \equiv 324 \equiv 14 && (\mathrm{mod}\, 31)\\
7^8 &\equiv 14^2 = 196 \equiv 10 && (\mathrm{mod}\, 31)\\
7^{16} &\equiv 10^2 = 100 \equiv 7 && (\mathrm{mod}\, 31).
\end{aligned}$$

Also ist $7^{15} \equiv 1 (\mathrm{mod}\, 31)$. Das heißt, $x^2 \equiv 7 (\mathrm{mod}\, 31)$ hat eine Lösung.

Eine Möglichkeit nun eine Lösung zu finden ist, stets p zu addieren, bis man ein Quadrat hat. Also

$$x^2 \equiv 7 \equiv 38 \equiv 69 \equiv 100 \equiv 10^2 (\mathrm{mod}\, 31).$$

Somit sind $x = 10$ und $x = 21$ die beiden Lösungen.

Definition

Legendre[1]-Symbol. Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$, so dass a nicht von p geteilt wird. Setze

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } x^2 \equiv a (\mathrm{mod}\, p) \text{ eine Lösung hat} \\ -1 & \text{falls } x^2 \equiv a (\mathrm{mod}\, p) \text{ keine Lösung hat} \end{cases}$$

Ist p ein Teiler von a, so setze $(\frac{a}{p}) = 0$. Wir nennen $(\frac{a}{p})$ das *Legendre-Symbol*.

[1] Adrien-Marie Legendre (*18.9.1752 Paris, †9.1.1833 Paris), Professor in Paris mit Arbeiten zur Zahlentheorie, Variationsrechnung, partiellen Differentialgleichungen, elliptischen Integralen.

Wir können nun Lemma IX.3 umformulieren als:

Lemma IX.4

Ist p ungerade, so ist

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Es ergibt sich die Frage, wie wir $(\frac{a}{p})$ effektiv berechnen können, und insbesondere, wie wir zu gegebenem a die p mit $(\frac{a}{p}) = 1$ bestimmen können. Dazu wollen wir zunächst einmal ein paar Rechenregeln für das Legendre-Symbol aufstellen.

Lemma IX.5

Seien p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Dann gilt

a) Ist $a \equiv b (\mathrm{mod}\, p)$, so ist $(\frac{a}{p}) = (\frac{b}{p})$.

b) Ist p kein Teiler von a, so ist $(\frac{a^2}{p}) = 1$.

c) Es ist $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Beweis.

a) Ist p ein Teiler von a, so ist p auch ein Teiler von b. Damit ist dann $(\frac{a}{p}) = 0 = (\frac{b}{p})$. Sei nun $\mathrm{ggT}(p, a) = 1$. Es hat $x^2 \equiv a (\mathrm{mod}\, p)$ genau dann eine Lösung, wenn $x^2 \equiv b (\mathrm{mod}\, p)$ eine hat, was $(\frac{a}{p}) = (\frac{b}{p})$ liefert.

b) $x^2 \equiv a^2 (\mathrm{mod}\, p)$ hat die Lösung $x = a$.

c) Ist p ein Teiler von a oder b, so ist $(\frac{ab}{p}) = 0 = (\frac{a}{p})$ bzw. $(\frac{ab}{p}) = 0 = (\frac{b}{p})$ und c) gilt. Sei also p kein Teiler von ab. Nach Lemma IX.4 ist

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\, p).$$

Da $(\frac{a}{b})(\frac{b}{p}) = \pm 1$ und $(\frac{ab}{p}) = \pm 1$ ist, folgt aus der Kongruenz modulo p die Gleichheit. □

Wir wollen nun den Hauptsatz dieses Paragraphen formulieren.

Satz IX.6

Quadratisches Reziprozitätsgesetz[2]. *Seien p, q ungerade Primzahlen. Dann ist*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

[2] Dies ist einer der wichtigsten Sätze. Gauß hat es theorema fundamentale genannt und selbst acht wesentlich verschiedene Beweise angegeben. Inzwischen sind mehr als 150 bekannt (siehe Pieper, 1978 [23]).

Sei q gegeben. Die Frage ist, für welche p die Zahl q ein Quadrat modulo p ist. Dies ist ein unendliches Problem. Aber Satz IX.6 besagt, dass dies nicht ganz stimmt, denn wir müssen nur feststellen, welche p für das gegebene q ein Quadrat sind. Davon gibt es aber nur endlich viele Kongruenzklassen, also doch ein endliches Problem.

Bevor wir Satz IX.6 beweisen, folgt ein Beispiel, das dessen Nutzen zeigt.

Beispiel

Hat $x^2 \equiv 85 (\mathrm{mod}\ 97)$ eine Lösung?

$$\left(\frac{85}{97}\right) = \left(\frac{17 \cdot 5}{97}\right) \underset{(IX.5)}{=} \left(\frac{17}{97}\right)\left(\frac{5}{97}\right).$$

Da 4 sowohl $17 - 1$ als auch $97 - 1$ teilt, ist nach Satz IX.6

$$\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right) \text{ und } \left(\frac{5}{97}\right) = \left(\frac{97}{5}\right).$$

Es ist

$$\left(\frac{97}{17}\right) \underset{(IX.5)}{=} \left(\frac{12}{17}\right) = \left(\frac{4 \cdot 3}{17}\right) \underset{(IX.5)}{=} \left(\frac{4}{17}\right)\left(\frac{3}{17}\right) \underset{(IX.5)}{=} \left(\frac{3}{17}\right)$$

$$\underset{(IX.6)}{=} \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

$$\left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Also ist $(\frac{85}{97}) = (-1)(-1) = 1$. Damit ist 85 ein Quadrat modulo 97.

Dieses Beispiel zeigt auch, warum Satz IX.6 „Reziprozitätsgesetz“ genannt wird.

Schneller wäre es wie folgt gegangen:

$$\left(\frac{85}{97}\right) = \left(\frac{-12}{77}\right) = \left(\frac{-1}{97}\right)\left(\frac{4}{97}\right)\left(\frac{3}{97}\right) = \left(\frac{-1}{97}\right)\left(\frac{3}{97}\right).$$

$$\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Also ist $\left(\frac{85}{97}\right) = \left(\frac{-1}{97}\right)$. Nach Lemma VIII.7 ist $(\frac{-1}{97}) = 1$.

Wir formulieren Lemma VIII.7 neu.

Lemma IX.7

$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, *d.h.*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1 (\mathrm{mod}\ 4) \\ -1 & \text{für } p \equiv 3 (\mathrm{mod}\ 4) \end{cases}$$

Wir wollen nun den Beweis von Satz IX.6 angehen. Dies geschieht in mehreren Schritten. Sei dazu a ein Rest modulo p mit ggT $(a, p) = 1$. Wir betrachten die Vielfachen

$$1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a$$

und definieren $1 \leq r_k \leq \frac{p-1}{2}$ durch

$$k \cdot a \equiv e_k r_k (\mathrm{mod}\, p), k = 1, \ldots, \frac{p-1}{2}, \text{ mit } e_k = \pm 1.$$

Wir wollen uns zunächst einmal ansehen, ob die r_k hierbei mehrmals vorkommen. Dieses könnte auf zweierlei Weise geschehen. Seien dazu $1 \leq k, l \leq (p-1)/2$.

Die eine Möglichkeit wäre

$$\begin{aligned} ka &\equiv \quad r_k (\mathrm{mod}\, p) \\ la &\equiv -r_k (\mathrm{mod}\, p). \end{aligned}$$

Dann ist aber p ein Teiler von $k+1$. Da $1 \leq k+l < p$ ist, kann das nicht sein.

Die andere Möglichkeit ist

$$\begin{aligned} ka &\equiv \quad r_k (\mathrm{mod}\, p) \\ la &\equiv \quad r_k (\mathrm{mod}\, p). \end{aligned}$$

Dann ist p ein Teiler von $k-l$, was $k = l$ liefert. Somit kommt jedes r_k mit geeignetem Vorzeichen genau einmal vor. Es sind $\pm a, \ldots, \pm\frac{p-1}{2}a$ alle möglichen Reste modulo p, die nicht Null sind. Also ist

$$\{r_1, \ldots, r_{\frac{p-1}{2}}\} = \{1, \ldots, \frac{p-1}{2}\}.$$

Wir erhalten jetzt mit diesen Bezeichnungen eine erste Formel für die Berechnung von $(\frac{a}{p})$.

Lemma IX.8 *Sei p eine Primzahl mit $\mathrm{ggT}(a, p) = 1$. Dann ist $(\frac{a}{p}) = e_1 e_2 \cdots e_{\frac{p-1}{2}}$.*

Beweis.

$$\begin{aligned} a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdots \tfrac{(p-1)}{2} &\equiv e_1 r_1 e_2 r_2 \cdots e_{\frac{p-1}{2}} r_{\frac{p-1}{2}} \\ &\equiv e_1 \cdots e_{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \tfrac{(p-1)}{2}\right) (\mathrm{mod}\, p). \end{aligned}$$

Somit ist

$$\left(\frac{a}{p}\right) \underset{(IX.4)}{\equiv} a^{\frac{p-1}{2}} \equiv e_1 \cdots e_{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Da die $e_i = \pm 1$ sind, ist Kongruenz dasselbe wie Gleichheit. □

Damit haben wir das Problem, das Legendre-Symbol zu berechnen, auf die Berechnung der e_k verlagert. Dies wollen wir nun angehen. Es ist

$$ak = u \cdot p + e_k r_k, 0 < r_k \leq \frac{p-1}{2}, \text{ mit geeignetem } u.$$

Also ist

$$2ak = 2up + 2e_k r_k$$

und

$$\frac{2ak}{p} = 2u + e_k \frac{2r_k}{p}.$$

Dabei ist

$$\frac{2r_k}{p} \leq \frac{p-1}{p} < 1.$$

Das liefert $\frac{2ak}{p} = 2u \pm \epsilon$ mit $0 < \epsilon < 1$, wobei das Plus-Zeichen für $e_k = 1$ und das Minus-Zeichen für $e_k = -1$ steht.

Somit haben wir

$$e_k = +1 \quad \text{für} \quad \left\lfloor \frac{2ak}{p} \right\rfloor \quad \text{gerade}$$

$$e_k = -1 \quad \text{für} \quad \left\lfloor \frac{2ak}{p} \right\rfloor \quad \text{ungerade.}$$

Also ist

$$e_k = (-1)^{\lfloor \frac{2ak}{p} \rfloor}.$$

Damit haben wir die e_k berechnet. Wir wollen nun das Legendre-Symbol berechnen. Sei dazu zunächst a ungerade. Dann gilt für das Legendre-Symbol:

$$\begin{aligned}\left(\frac{2a}{p}\right) &= \left(\frac{2a+2p}{p}\right) = \left(\frac{4(\frac{a+p}{2})}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) \\ &= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{(a+p)k}{p} \rfloor} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ak}{p} \rfloor + \sum_{k=1}^{\frac{p-1}{2}} k}.\end{aligned}$$

Es ist

$$\sum_{k=1}^{\frac{p-1}{2}} k = \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = \frac{p^2-1}{8}.$$

Also gilt für das Legendre-Symbol:

$$\left(\frac{2a}{p}\right) = (-1)^{\frac{p^2-1}{8} + \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ak}{p} \rfloor}.$$

Damit können wir nun zunächst den Spezialfall $a = 1$ behandeln.

Lemma IX.9

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \text{ also}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ für } p \equiv 1, 7 \pmod 8 \\ -1 \text{ für } p \equiv 3, 5 \pmod 8 \end{cases}$$

Beweis. Setze $a = 1$. Dann haben wir gerade gezeigt

$$\left(\frac{2}{p}\right) = \left(\frac{2 \cdot 1}{p}\right) = (-1)^{\frac{p^2-1}{8} + \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{k}{p} \rfloor}.$$

Da $k < p$ ist, ist $\lfloor \frac{k}{p} \rfloor = 0$. Das ist die Behauptung. □

Wir können Lemma IX.9 zur Berechnung von $(\frac{2a}{p})$ anwenden, indem wir die Multiplikativität des Legendre-Symbols benutzen

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right).$$

Damit haben wir eine neue Formel für $(\frac{a}{p})$.

Lemma IX.10

Sei p eine Primzahl mit ggT $(a, p) = 1$. *Dann ist*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ak}{p} \rfloor}.$$

Jetzt können wir den Beweis des Hauptsatzes angehen.

Beweis von Satz IX.6: Nach Lemma IX.10 ist

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor} = (-1)^{\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{p}{q} y \rfloor}.$$

Es ist $\lfloor \frac{p}{q} y \rfloor$ die Anzahl der ganzen Zahlen zwischen 1 und $\frac{p}{q} y$. Ist $y \leq \frac{q-1}{2}$, so ist $\frac{p}{q} y < \frac{p}{2}$. Also liegen die Zahlen, die kleiner oder gleich $\frac{p}{q} y$ sind, im Bereich zwischen 1 und $\frac{p-1}{2}$. Somit zählt $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$ die Paare (x, y) mit $x \in \{1, \ldots, \frac{p-1}{2}\}, y \in \{1, \ldots, \frac{q-1}{2}\}$, für die $x < \frac{p}{q} y$ ist, oder anders ausgedrückt, für die $qx < py$ ist. Sei N die Anzahl dieser Paare. Dann ist

$$\left(\frac{p}{q}\right) = (-1)^N.$$

Genauso ist

$$\left(\frac{q}{p}\right) = (-1)^M,$$

wobei M die Anzahl der Paare (x, y) mit $x \in \{1, \ldots, \frac{p-1}{2}\}$ und $y \in \{1, \ldots, \frac{q-1}{2}\}$ ist, so dass $py < qx$ ist. Somit ist

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N+M}.$$

Hierbei ist $N + M$ die Anzahl der Paare $(x, y) \in \{1, \ldots, \frac{p-1}{2}\} \times \{1, \ldots, \frac{q-1}{2}\}$ für die $py > qx$ oder $py < qx$ ist. Da aus $py = qx$ stets $q|y$ folgen würde, aber $y < q$ ist, sind dies aber alle Paare (x, y) mit $x = 1, \ldots, \frac{p-1}{2}$ und $y = 1, \ldots, \frac{q-1}{2}$. Also ist $N + M = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Damit ist Satz IX.6 bewiesen. □

Nun ist es sehr mühselig $(\frac{a}{p})$ zu berechnen, wenn man dazu zunächst a in seine Primfaktoren zerlegen muss, wie im Beispiel auf Seite 132 geschehen, was nicht einfach ist. Schließlich beruht die Sicherheit von gewissen Verschlüsselungssystemen darauf, dass die Primfaktorzerlegung ein schwieriges Problem ist, siehe Seite 71. Um diesem Problem aus dem Weg zu gehen, erweitern wir die Definition des Legendre-Symbols.

Definition

Jacobi[3]-Symbol. Sei n eine ungerade Zahl und sei $n = p_1 \cdots p_k$ mit Primzahlen p_i. Wir definieren das Jacobi-Symbol $(\frac{a}{n})$ für $a \in \mathbb{Z}$ durch

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right).$$

Hierbei sind die $(\frac{a}{p_i})$ die *Legendre-Symbole*.

Dies ist eine rein formale Definition. Obwohl sich das Jacobi-Symbol genauso wie das Legendre-Symbol verhält, wie wir gleich sehen werden, beantwortet es die Frage, ob a ein Quadrat modulo n ist, nicht. Betrachte dazu

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1.$$

Die Quadrate modulo 15 sind: $1^2, 2^2 = 4, 3^2 = 9, 4^2 \equiv 1 (\mathrm{mod}\ 15), 5^2 \equiv 10 (\mathrm{mod}\ 15), 6^2 \equiv 6 (\mathrm{mod}\ 15), 7^2 \equiv 4 (\mathrm{mod}\ 15)$. Also ist 2 kein Quadrat modulo 15.

Für das Jacobi-Symbol gelten die gleichen Rechenregeln wie für das Legendre-Symbol.

Lemma IX.11

Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ ungerade.

a) Ist $a \equiv b (\mathrm{mod}\ n)$, so ist $(\frac{a}{n}) = (\frac{b}{n})$.

b) $(\frac{1}{n}) = 1$, $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$.

c) Ist $\mathrm{ggT}(n, ab) = 1$, so ist $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.

d) Ist $\mathrm{ggT}(n, a) = 1$, so ist $(\frac{a^2}{n}) = 1$.

Beweis. a) Dies folgt direkt aus Lemma IX.5 a) und der Definition von $(\frac{a}{n})$.

[3] Carl Gustav Jacob Jacobi (*10.12.1804 Potsdam, †18.2.1851 Berlin) war Professor in Königsberg. Er arbeitete sowohl in der Analysis, mathematischen Physik als auch in der Zahlentheorie. Als Erster wendete er elliptische Funktionen in der Zahlentheorie an. Viele Begriffe in der Mathematik tragen seinen Namen, z.B Jacobi-Determinante, Jacobi-Theta-Funktion, Jacobi-Integral. Jacobi gab mehrere neue Beweise des quadratischen Reziprozitätsgesetzes. Auf dem Mond gibt es einen Krater, der nach ihm benannt wurde.

b) $(\frac{1}{n}) = (\frac{1}{p_1}) \cdots (\frac{1}{p_n}) = 1$.

Sind x, y ungerade, so ist stets 4 ein Teiler von $(x-1)(y-1) = xy - x - y + 1$. Also ist

$$xy \equiv x + y - 1 (\mathrm{mod}\, 4)$$

und dann

$$xy - 1 \equiv (x-1) + (y-1) (\mathrm{mod}\, 4).$$

Sei nun $n = p_1 \cdots p_k$. Dann ist

$$p_1 p_2 \cdots p_k - 1 \equiv p_1 - 1 + p_2 - 1 + \cdots p_k - 1 (\mathrm{mod}\, 4).$$

Also ist $\frac{n-1}{2} \equiv \sum_{i=1}^{k} \frac{p_i - 1}{2} (\mathrm{mod}\, 2)$.

Nun ist

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_k}\right) \underset{(IX.4)}{=} (-1)^{\sum_{i=1}^{k} \frac{p_i - 1}{2}} = (-1)^{\frac{n-1}{2}}.$$

c), d) Diese folgen aus Lemma IX.5 b) bzw. c). □

Sei $n \in \mathbb{N}$ ungerade. Dann ist $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$. **Satz IX.12**

Beweis. Sind x, y ungerade, so ist 16 ein Teiler von $(x^2 - 1)(y^2 - 1)$. Also ist

$$x^2 y^2 \equiv x^2 + y^2 - 1 (\mathrm{mod}\, 16)$$

und dann

$$x^2 y^2 - 1 \equiv (x^2 - 1) + (y^2 - 1) (\mathrm{mod}\, 16).$$

Sei nun $n = p_1 \cdots p_k$ mit Primzahlen p_i. Dann erhalten wir

$$n^2 - 1 \equiv (p_1^2 - 1) + \cdots + (p_k^2 - 1) (\mathrm{mod}\, 16).$$

Also ist $\frac{n^2-1}{8} \equiv \sum_{i=1}^{k} \frac{p_i^2 - 1}{8} (\mathrm{mod}\, 2)$. Damit erhalten wir

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_k}\right) \underset{(IX.9)}{=} (-1)^{\sum_{i=1}^{k} \frac{p_i^2 - 1}{8}} = (-1)^{\frac{n^2-1}{8}}.$$

□

Auch das Analogon zum quadratischen Reziprozitätsgesetz gilt.

Sind m und n ungerade und teilerfremd, so ist **Satz IX.13**

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{m}\right).$$

Beweis. Sei $m = q_1 \cdots q_t$ und $n = p_1 \cdots p_k$ mit Primzahlen p_i, q_i. Es ist

$$\begin{aligned}\left(\frac{m}{n}\right) &= \left(\frac{q_1 \cdots q_t}{p_1 \cdots p_k}\right) = \left(\frac{q_1 \cdots q_t}{p_1}\right) \cdots \left(\frac{q_1 \cdots q_t}{p_k}\right) \\ &= \prod_{i=1}^{t}\prod_{j=1}^{k}\left(\frac{q_i}{p_j}\right) \underset{(IX.6)}{=} \prod_{j=1}^{k}\prod_{i=1}^{t}\left(\frac{p_j}{q_i}\right)(-1)^{\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)} \\ &= \left(\frac{n}{m}\right)(-1)^{\sum_{j=1}^{k}\sum_{i=1}^{t}\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)} \\ &= \left(\frac{n}{m}\right)(-1)^{\left(\sum_{j=1}^{k}\frac{p_j-1}{2}\right)\left(\sum_{i=1}^{t}\frac{q_i-1}{2}\right)}.\end{aligned}$$

Wie wir im Beweis von Lemma IX.11 gesehen haben, ist

$$\begin{aligned}\textstyle\sum_{j=1}^{k}\left(\frac{p_j-1}{2}\right) &\equiv \tfrac{n-1}{2} \pmod 2 \text{ und} \\ \textstyle\sum_{i=1}^{t}\left(\frac{q_i-1}{2}\right) &\equiv \tfrac{m-1}{2} \pmod 2.\end{aligned}$$

Also ist $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$. □

Wir wollen nun das Jacobi-Symbol dazu benutzen, das Legendre-Symbol zu berechnen. Immerhin ist jedes Legendre-Symbol auch ein Jabobi-Symbol. Wir können daher die Regeln für Jacobi-Symbole benutzen, um $\left(\frac{a}{p}\right)$ zu berechnen, falls p eine Primzahl ist, ohne vorher die Primfaktorzerlegung von a bestimmen zu müssen.

Beispiel

Es soll das Legendre-Symbol $\left(\frac{28559}{46237}\right)$ berechnet werden.

$$\begin{aligned}&\left(\frac{28559}{46237}\right) \underset{(IX.13)}{=} \left(\frac{46237}{28559}\right) \underset{(IX.11)}{=} \left(\frac{17678}{28559}\right) \underset{(IX.11)}{=} \\ &\left(\frac{2}{28559}\right)\left(\frac{8839}{28559}\right) \underset{(IX.12)}{=} -\left(\frac{28559}{8839}\right) \\ = \; &-\left(\frac{2042}{8839}\right) = -\left(\frac{2}{8839}\right)\left(\frac{1021}{8839}\right) \\ = \; &-\left(\frac{1021}{8839}\right) = -\left(\frac{8839}{1021}\right) = -\left(\frac{671}{1021}\right) = -\left(\frac{1021}{671}\right) = -\left(\frac{350}{671}\right) \\ = \; &-\left(\frac{14}{671}\right) = -\left(\frac{2}{671}\right)\left(\frac{7}{671}\right) = -\left(\frac{7}{671}\right) = \left(\frac{671}{7}\right) = \left(\frac{-1}{7}\right) = -1.\end{aligned}$$

Also ist 28559 kein Quadrat modulo 46237.

Bisher haben wir nur die Frage betrachtet, ob a quadratischer Rest modulo einer Primzahl ist. Wir wollen dies nun darauf ausdehnen, dass n nicht prim ist. Das Jacobi-Symbol hilft dabei erst einmal nicht.

Es war $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ genau für einen quadratischen Rest a modulo p mit $\mathrm{ggT}(a, p) = 1$. Bei beliebigem n wird dann vermutlich (wie beim Satz von Euler) $p-1$ durch $\varphi(n)$ zu ersetzen sein. Wir können also erwarten, dass für a mit $\mathrm{ggT}(a, n) = 1$ wir genau dann einen quadratischen Rest haben, falls $a^{\varphi(n)/2} \equiv 1 (\mathrm{mod}\, n)$ ist. Wir werden sehen, dass das fast richtig ist. Um dies zu untersuchen, werden wir zwei Dinge tun. Ist $n = p_1^{n_1} \cdots p_r^{n_r}$ die Primfaktorzerlegung von n, so werden wir versuchen die Frage, ob a ein quadratischer Rest modulo n ist, auf die zurückzuführen, ob a quadratischer Rest modulo der $p_i^{n_i}$ ist. Wir werden also zunächst den Fall betrachten, dass n eine Primzahlpotenz ist. Für diese studieren wir die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$.

Satz IX.14 *Seien p eine ungerade Primzahl und $\alpha \in \mathbb{N}$. Dann gibt es ein $c \in \mathbb{N}$ mit $\mathrm{ggT}(c, p) = 1$ und $o_{p^\alpha}(c) = \varphi(p^\alpha)$, d.h., $c + p^\alpha\mathbb{Z}$ ist Erzeuger der Einheitengruppe von $\mathbb{Z}/p^\alpha\mathbb{Z}$.*

Beweis. Wie im Beweis von Lemma IV.16 wählen wir c mit

$$c^{p-1} \equiv 1 (\mathrm{mod}\, p),\ c^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$$

(z.B. mit g Erzeuger von $\mathbb{Z}/p\mathbb{Z}$ und $c = g(p+1)$).

Wir zeigen zunächst

$$(*) \qquad c^{(p-1)p^{\alpha-2}} \not\equiv 1 (\mathrm{mod}\, p^\alpha).$$

Dies geschieht mit Induktion nach α. Für $\alpha = 2$ ist das die obige Aussage.

Nach Euler ist

$$c^{(p-1)p^{\alpha-2}} = c^{\varphi(p^{\alpha-1})} \equiv 1 (\mathrm{mod}\, p^{\alpha-1}).$$

Das liefert

$$c^{(p-1)p^{\alpha-1}} = (1 + bp^{\alpha-1})^p = 1 + bp^\alpha + dp^{2\alpha-1},$$

da p stets $\binom{p}{r}, 0 < r < p$ teilt.

Per Induktionsannahme ist $p \nmid b$. Weiter ist $2\alpha - 1 \geq \alpha + 1$. Also ist

$$c^{(p-1)p^{\alpha-1}} \equiv 1 + bp^\alpha \not\equiv 1 (\mathrm{mod}\, p^{\alpha+1}).$$

Damit ist $(*)$ bewiesen.

Es ist $o_{p^\alpha}(c) | \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Da $o_p(c) = p - 1$ ist, folgt, dass $o_{p^\alpha}(c)$ durch $p - 1$ geteilt wird. Somit folgt mit $(*)$

$$o_{p^\alpha}(c) = p^{\alpha-1}(p-1). \qquad \square$$

Die Aussage von Satz IX.14 ist für $p = 2$ falsch. Es ist $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ die Einheitengruppe von $\mathbb{Z}/8\mathbb{Z}$ und $\varphi(8) = 4$. Es gilt aber $\bar{i}^2 \equiv 1 (\mathrm{mod}\, 8)$ für alle i. Somit haben alle Elemente die Ordnung 1 oder 2.

Der nächste Satz gibt über die Verhältnisse für $p = 2$ Auskunft.

Satz IX.15 *Sei $n = 2^m \geq 8$. Dann ist $o_n(5) = 2^{m-2}$. Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ besteht aus den Potenzen $5^i + n\mathbb{Z}$ und $-5^i + n\mathbb{Z}$.*

Beweis. Es ist $5^2 - 1 = 24$, also ist 2^3 ein Teiler von $5^2 - 1$. Wir zeigen mit Induktion

(+) $\quad 2^{t+2}$ teilt $5^{2^t} - 1, \quad t \geq 1.$

Es ist

$$(5^{2^t} - 1) = (5^{2^{t-1}} - 1)(5^{2^{t-1}} + 1).$$

Also ist $2^{t+1} \cdot 2 = 2^{t+2}$ ein Teiler von $5^{2^t} - 1$ per Induktion.

Nach (+) ist $o_n(5)$ ein Teiler von 2^{m-2}. Sei $o_n(5)$ ein Teiler von 2^{m-3}. Dann ist 2^m ein Teiler von $5^{2^{m-3}} - 1$. Das liefert dann, dass $5^{2^{m-4}} - 1$ durch 2^{m-1} teilbar ist, und schließlich, dass $5^2 - 1$ durch 16 geteilt wird, ein Widerspruch.

Also ist

$$o_n(5) = 2^{m-2}.$$

Ist $m = 3$, so ist $5 \not\equiv -1 (\mathrm{mod}\ 8)$, also ist 8 kein Teiler von $5^{2^{m-3}} + 1$.

Sei $m > 3$. Dann ist

$$5^{2^{m-3}} + 1 = (1+4)^{2^{m-3}} + 1 = 2 + \binom{2^{m-3}}{1} \cdot 4 + \cdots + 4^{2^{m-3}}.$$

Bis auf den ersten Summanden sind alle anderen durch 4 teilbar. Somit gilt:

(++) $\quad 2^m$ ist kein Teiler von $5^{2^{m-3}} + 1$.

Wäre $5^i \equiv -1 (\mathrm{mod}\ 2^m)$ für $i < 2^{m-2}$, so wäre $5^{2i} \equiv 1 (\mathrm{mod}\ 2^m)$. Da die Ordnung von 5 modulo 2^m gleich 2^{m-2} ist, wäre dann nach Lemma III.3 2^{m-2} ein Teiler von $2i$, d.h. $i = 2^{m-3}$, ein Widerspruch zu (++).

Ist $2^{m-2} \geq i > j$ und $5^i \equiv -5^j (\mathrm{mod}\ 2^m)$, so ist $5^{i-j} \equiv -1 (\mathrm{mod}\ 2^m)$ ein Widerspruch zu (++). Also sind 5^i und -5^i, $0 \leq i < 2^{m-2}$ die Einheiten modulo 2^m. □

Für den nächsten Satz vergleiche man Lemma IX.3.

Satz IX.16 *Seien $n \in \mathbb{N}$, $n \neq 2$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Es gebe ein c, dessen Ordnung modulo n gleich $\varphi(n)$ ist. Dann sind gleichwertig*

a) $x^2 \equiv a (\mathrm{mod}\ n)$ *hat eine Lösung x.*

b) $a^{\varphi(n)/2} \equiv 1 (\mathrm{mod}\ n)$.

Beweis.

a) $\Rightarrow$ b). Da $x^2 \equiv a \pmod{n}$ ist, ist auch $\mathrm{ggT}(x, n) = 1$. Nach dem Satz von Euler ist

$$a^{\varphi(n)/2} \equiv x^{\varphi(n)} \equiv 1 \pmod{n}.$$

b) $\Rightarrow$ a). Sei c mit $o_n(c) = \varphi(n)$. Dann ist c ein Erzeuger der Einheitengruppe modulo n. Da $\mathrm{ggT}(a, n) = 1$ ist, ist a eine Einheit modulo n. Somit gibt es ein j mit

$$c^j \equiv a \pmod{n}.$$

Es ist $c^{j\varphi(n)/2} \equiv a^{\varphi(n)/2} \equiv 1 \pmod{n}$. Also ist $\varphi(n) | j\varphi(n)/2$, d.h. $2|j$, und damit ist $j = 2i$. Dann ist

$$(c^i)^2 \equiv a \pmod{n}.$$

Mit $x = c^i$ erhalten wir $x^2 \equiv a \pmod{n}$. □

Damit haben wir das Problem nur verschoben. Wann gibt es denn ein c mit $o_n(c) = \varphi(n)$? Immerhin, wenn n eine ungerade Primzahlpotenz ist, so gibt es dies nach Satz IX.14. Der nächste Satz ist nun entscheidend, da er die angekündigte Reduktion des allgemeinen Problems auf das der Primzahlpotenzen liefert.

Satz IX.17

Seien $\mathrm{ggT}(a, m_1) = \mathrm{ggT}(a, m_2) = 1$ *und* $\mathrm{ggT}(m_1, m_2) = 1$. *Ist a ein Quadrat modulo m_1 und m_2, so ist a auch Quadrat modulo $m_1 m_2$.*

Beweis. Sei

$$x_1^2 \equiv a \pmod{m_1}$$
$$x_2^2 \equiv a \pmod{m_2}.$$

Nach dem Chinesischen Restsatz gibt es ein x mit

$$x \equiv x_1 \pmod{m_1}$$
$$x \equiv x_2 \pmod{m_2}.$$

Also ist $m_1 m_2 | x^2 - a$. □

Nun sind wir in der Lage, ein notwendiges und hinreichendes Kriterium dafür anzugeben, dass a ein Quadrat modulo n ist.

Satz IX.18

Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. *Sei $n = 2^{\alpha_0} \prod_{k=1}^{t} p_k^{\alpha_k}$ die Primfaktorzerlegung. Dann ist $x^2 \equiv a \pmod{n}$ genau dann lösbar, wenn*

$$a \equiv 1 \pmod{2^{\min(\alpha_0, 3)}}$$

ist, und

$$y_i^2 \equiv a \pmod{p_i},\ i = 1, \ldots, t$$

lösbar sind.

Beweis. Sei zunächst x eine Lösung von $x^2 \equiv a \pmod{n}$. Dann ist offenbar auch $x^2 \equiv a \pmod{p_i}$, $i = 1, \ldots, t$, und $x^2 \equiv a \pmod{2^{\alpha_0}}$. Somit gilt auch die Kongruenz $x^2 \equiv a \pmod{2^{\min(\alpha_0, 3)}}$. Ist $\alpha_0 \geq 1$, so ist n gerade und dann a ungerade. Damit ist auch x ungerade. Also ist $x^2 \equiv 1 \pmod{8}$ und damit $a \equiv 1 \pmod{2^{\min(\alpha_0, 3)}}$.

Wir betrachten nun die Umkehrung. Wir zeigen zunächst, dass a quadratischer Rest modulo 2^{α_0} ist. Dies ist richtig für $\alpha_0 \leq 2$. Sei $\alpha_0 \geq 3$, so ist $a \equiv 1 (\mathrm{mod}\ 8)$. Nach Satz IX.15 sind 5^i und -5^i die Einheiten modulo 2^{α_0}. Sei $a \equiv \pm 5^i (\mathrm{mod}\ 2^{\alpha_0})$. Dann ist $\pm 5^i \equiv 1 (\mathrm{mod}\ 8)$. Es ist $5^2 \equiv 1 (\mathrm{mod}\ 8)$. Also ist $a \equiv 5^{2j} (\mathrm{mod}\ 2^{\alpha_0})$, d.h. ein Quadrat.

Da a quadratischer Rest modulo p_i ist, folgt mit Lemma IX.1

$$a^{\frac{(p_i-1)}{2}} \equiv 1 (\mathrm{mod}\ p_i).$$

Also ist $a^{\frac{p_i-1}{2}} = 1 + \alpha p_i$ und dann

$$\left(a^{\frac{p_i-1}{2}}\right)^{p_i^{\alpha_i-1}} = 1 + \beta p_i^{\alpha_i}, \text{ d.h. } a^{\varphi(p_i^{\alpha_i})/2} \equiv 1 (\mathrm{mod}\ p_i^{\alpha_i}).$$

Nach Satz IX.14 und Satz IX.16 gilt, dass a ein Quadrat modulo $p_i^{a_i}$, $i = 1, \ldots, t$ ist. Mit Satz IX.17 folgt nun, dass a ein Quadrat modulo n ist. □

Beispiel

Hat die Kongruenz $x^2 \equiv 453 (\mathrm{mod}\ 1236)$ eine Lösung?

Wie oft bei Anwendungen schöner Theorien, geht dies nicht direkt. Wir müssen erst eine Situation herstellen, in der Satz IX.18 anwendbar ist. Zunächst ist die Voraussetzung der Teilerfremdheit nicht erfüllt, da ggT $(453, 1236) = 3$ ist. Gibt es eine Lösung x, so ist $3|x$. Dies ist äquivalent zu der Frage, ob es eine Lösung gibt von $3y^2 \equiv 151 (\mathrm{mod}\ 412)$.

Nun sind zwar 151 und 412 teilerfremd, mit $3y^2$ haben wir aber kein Quadrat mehr. Es ist $2 \cdot 412 = 3 \cdot 275 - 1$. Also ist

$$3^{-1} \equiv 275 (\mathrm{mod}\ 412).$$

Das liefert

$$y^2 \equiv -87 (\mathrm{mod}\ 412).$$

Nun können wir Satz IX.18 anwenden. Es ist $412 = 4 \cdot 103$. Nach Satz IX.18 gibt es genau dann eine Lösung y^2, falls

$$y^2 \equiv -87 (\mathrm{mod}\ 103)$$

lösbar ist.

Wir berechnen das Legendre-Symbol

$$\left(\frac{-87}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{3}{103}\right)\left(\frac{29}{103}\right) = (-1)\left(\frac{3}{103}\right)\left(\frac{29}{103}\right).$$

$$\left(\frac{3}{103}\right) = -\left(\frac{103}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

$$\left(\frac{29}{103}\right) = \left(\frac{103}{29}\right) = \left(\frac{3 \cdot 29 + 16}{29}\right) = \left(\frac{16}{29}\right) = 1.$$

Also ist $\left(\frac{-87}{103}\right) = 1$, d.h., es gibt eine Lösung y und dann auch eine Lösung x.

Wir wollen jetzt noch der Frage nachgehen, für wie viele Primzahlen eine Zahl a ein quadratischer Rest sein kann. Dazu definieren wir:

Extremalzahlen. Sei $a \in \mathbb{Z}$. Ist $x^2 \equiv a \pmod p$ für alle Primzahlen p, die a nicht teilen, lösbar, so nennen wir a eine *quadratische Extremalzahl*.

Hat $x^2 \equiv a \pmod p$ für alle ungeraden Primzahlen p, die a nicht teilen, niemals eine Lösung, so nennen wir a eine *nichtquadratische Extremalzahl*.

Definition

Es gibt keine nichtquadratischen Extremalzahlen.

Lemma IX.19

Beweis. Sei a eine nichtquadratische Extremalzahl. Wähle x mit $\mathrm{ggT}(a, x) = 1$, $x \neq a \pmod 2$ und $x^2 - a > 1$. Insbesondere ist $x^2 - a$ ungerade.

Es ist $x^2 \not\equiv a \pmod p$ für alle p, die a nicht teilen, da a nichtquadratische Extremalzahl ist. Da $\mathrm{ggT}(a, x) = 1$ ist, ist auch $x^2 \not\equiv a \pmod p$ für alle Primteiler p von a. Also hätte $x^2 - a$ keine Primteiler, ein Widerspruch. □

Es gilt aber sogar noch mehr:

Zu jeder Zahl a gibt es unendlich viele ungerade Primzahlen p, so dass a ein Quadrat modulo p ist.

Satz IX.20

Beweis. Nach Lemma IX.19 gibt es mindestens ein solches p. Seien nun $p_1, \ldots, p_t$ sämtliche ungerade Primzahlen mit

$$\left(\frac{a}{p_i}\right) = 1, \quad i = 1, \ldots, t.$$

Setze $Q = p_1 \cdots p_t$ und wähle n mit $Q^{2n} - 4a > 1$. Es ist Q ungerade. Sei q eine Primzahl, die $Q^{2n} - 4a$ teilt. Ist q ein Teiler von Q, so ist q eines der p_i. Dann teilt aber q nicht a. Also ist q kein Teiler von Q und somit $q \neq p_i$ für alle i. Dann ist $1 = (\frac{Q^{2n}}{q}) = (\frac{4a}{q}) = (\frac{a}{q})$. Also hat $Q^{2n} - 4a$ nur Primteiler, nach denen a ein Quadrat ist, aber diese sind genau $p_1, \ldots, p_t$, ein Widerspruch zu $q \neq p_i$, $i = 1 \ldots, t$. □

Ist a nicht selbst schon ein Quadrat, so gibt es immer Primzahlen modulo derer a kein quadratischer Rest ist.

a) Ist $a \in \mathbb{N}$ kein Quadrat, so gibt es unendlich viele Primzahlen p mit

$$\left(\frac{a}{p}\right) = -1.$$

b) Ist a eine quadratische Extremalzahl, so ist a ein Quadrat.

Satz IX.21

Beweis.

a) Ist $b \in \mathbb{N}$ mit $(\frac{b}{p}) = -1$, so ist auch $(\frac{bm^2}{p}) = -1$ für ggT $(m, p) = 1$. Also können wir annehmen, dass a quadratfrei ist. Sei

$$a = 2^{\epsilon} q_1 \dots q_n, \ \epsilon = 0, 1$$

die Primfaktorzerlegung von a. Es habe zunächst a mindestens einen ungeraden Primteiler. Wir wählen ein s mit

$$\left(\frac{s}{q_n}\right) = -1$$

Insbesondere ist q_n kein Teiler von s. Weiter wählen wir ungerade Primzahlen $r_1, \dots, r_k$, die verschieden von $q_1, \dots, q_n$ sind.

Nach dem Chinesischen Restsatz gibt es ein $b \in \mathbb{N}$ mit

$$\begin{aligned} & b \equiv 1 (\mathrm{mod}\, 8) \\ & b \equiv 1 (\mathrm{mod}\, r_i) \ i = 1, \dots, k \\ (+) \quad & b \equiv 1 (\mathrm{mod}\, q_i) \ i = 1, \dots, n-1 \\ & b \equiv s (\mathrm{mod}\, q_n) \end{aligned}$$

Sei $b = p_1 \cdots p_m$ die Primfaktorzerlegung von b. Dann sind die p_i ungleich 2, r_j, $j = 1, \dots k$, und q_j, $j = 1, \dots, n$, da ggT $(a, b) = 1$ ist. Wir zeigen $(\frac{a}{p_i}) = -1$ für ein $i \in \{1, \dots, m\}$. Da wir $\{r_1, \dots, r_k\}$ beliebig groß wählen können, folgt dann die Behauptung.

Wir betrachten dazu das Jacobi-Symbol $(\frac{a}{b})$. Es ist

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^{\epsilon} \left(\frac{q_1}{b}\right) \cdots \left(\frac{q_n}{b}\right).$$

Da $b \equiv 1 (\mathrm{mod}\, 8)$ ist, gilt nach Lemma IX.9 $(\frac{2}{b}) = 1$. Aus dem gleichen Grund folgt mit Satz IX.13 $(\frac{q_i}{b}) = (\frac{b}{q_i})$. Also ist

$$\left(\frac{a}{b}\right) = \left(\frac{b}{q_1}\right) \cdots \left(\frac{b}{q_n}\right) \underset{(+)}{=} \left(\frac{1}{q_1}\right) \cdots \left(\frac{1}{q_{n-1}}\right)\left(\frac{s}{q_n}\right) = -1.$$

Es gilt aber

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right).$$

Das liefert $(\frac{a}{p_i}) = -1$ für mindestens ein i.

Es bleibt der Fall $a = 2$ übrig. Es ist $(\frac{2}{p}) = -1$ für alle $p \equiv \pm 3 (\mathrm{mod}\, 8)$ nach Lemma IX.9. Nach Lemma IV.8 gibt es unendlich viele Primzahlen p mit $p \equiv \pm 3 (\mathrm{mod}\, 8)$.

b) Ist x kein Quadrat, so ist x keine quadratische Extremalzahl nach a). □

Dieser Satz ist ein Spezialfall eines allgemeineren Satzes.

Minkowski[4]-Hasse[5]. *Sei $f(x_1, \ldots, x_n)$ ein homogenes Polynom vom Grad 2 mit ganzen Koeffizienten. Dann ist $f(x_1, \ldots, x_n) = 0$ in $\mathbb{Z}$ genau dann nichttrivial lösbar, wenn die Gleichung in $\mathbb{R}$ und modulo jeder Primzahl nichttrivial lösbar ist. Hierbei meint nichttrivial, dass ein $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ eine Lösung ist.* Satz IX.22

Dies ist übrigens für höheren Grad falsch. Betrachte dazu

$$(x^2 - 2y^2)(x^2 + 7y^2)(x^2 + 14y^2) = 0.$$

Wir haben die Lösungen $x = \pm y\sqrt{2} \in \mathbb{R}$. Ist $p = 7$, so reduziert sich die Gleichung auf

$$x^2 - 2y^2 \equiv 0 (\mathrm{mod}\ 7).$$

Da $3^2 \equiv 2 (\mathrm{mod}\ 7)$ ist, hat die Gleichung die Lösung $x = 3, y = 1$.

Ist $p = 2$, so bleibt

$$x^2 + y^2 \equiv 0 (\mathrm{mod}\ 2).$$

Diese hat die Lösung $x = y = 1$.

Ist $p \neq 2, 7$, so ist

$$\left(\frac{-14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-7}{p}\right).$$

Also ist eine der Zahlen $2, -7, -14$ ein Quadrat modulo p, womit wir wieder eine Lösung haben. In $\mathbb{Z}$ gibt es aber nur die Lösung $(0, 0)$.

Wir wollen uns nun noch mit einem speziellen Typ von Zahlen, den Fermatzahlen $F_n = 2^{2^n} + 1$, beschäftigen. Diese sind für $n = 0, 1, 2, 3$ und 4 Primzahlen. Fermat vermutete, dass sie immer Primzahlen sind. Allerdings konnte schon Euler zeigen, dass F_5 keine Primzahl ist. Bis heute sind keine weiteren Fermatzahlen bekannt, die Primzahlen sind. Die kleinste Fermatzahl, für die nicht bekannt ist, ob sie eine Primzahl ist, ist derzeit F_{33}.

Ist $n \neq m$, so ist $\mathrm{ggT}(F_n, F_m) = 1$. Insbesondere gibt es unendlich viele Primzahlen. Lemma IX.23

Beweis. Wir zeigen:

$$(*) \qquad \prod_{k=0}^{n-1} F_k = F_n - 2.$$

Da offenbar $\mathrm{ggT}(F_n, F_n - 2) = 1$ ist, folgt dann die Behauptung.

[5]Hermann Minkowski (*22.6.1864 Alexota, †12.1.1909 Göttingen), Professor in Königsberg, Zürich und Göttingen, mit den Arbeitsgebieten Zahlentheorie und mathematische Grundlagen der speziellen Relativitätstheorie.

[5]Helmut Hasse (*25.8.1898 Kassel, †26.12.1979 Ahrensburg), Professor in Kiel, Halle, Marburg, Göttingen und Hamburg, mit den Arbeitsgebieten Algebra und Zahlentheorie. Der später sogenannte Satz von Minkowski-Hasse war seine Dissertation.

Wir beweisen $(*)$ durch Induktion nach n. Es ist $3 = F_0 = 5 - 2 = F_1 - 2$.

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n \underset{(Ind)}{=} (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

□

Um zu zeigen, dass F_5 keine Primzahl ist, betrachten wir zunächst mögliche Teiler von Fermatzahlen.

Satz IX.24

Sei p ein Primteiler von F_n, $n \geq 2$. Dann ist

$$p = 2^{n+2} \cdot k + 1 \text{ mit } k \in \mathbb{N}.$$

Beweis. Es ist $2^{2^n} \equiv -1 (\mathrm{mod}\, p)$. Damit erhalten wir $2^{2^{n+1}} \equiv 1 (\mathrm{mod}\, p)$. Dies zeigt, dass $o_p(2) = 2^{n+1}$ ist. Nach dem kleinen Satz IV.14 von Fermat gilt

$$2^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Also ist 2^{n+1} ein Teiler von $p-1$. Da $n \geq 2$ ist, ist $p \equiv 1 (\mathrm{mod}\, 8)$. Somit ist nach Lemma IX.9

$$\left(\frac{2}{p}\right) = 1.$$

Damit gibt es ein x mit $x^2 \equiv 2 (\mathrm{mod}\, p)$.

Das liefert

$$x^{2^{n+2}} \equiv 2^{2^{n+1}} \equiv 1 (\mathrm{mod}\, p).$$

Somit ist $o_p(x) = 2^j$ mit $j \leq n+2$. Wegen $o_p(x^2) = 2^{n+1}$, folgt $o_p(x) = 2^{n+2}$.

Es ist aber auch

$$x^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Also ist

$$2^{n+2} \text{ ein Teiler von } p - 1,$$

was die Behauptung ist. □

Mit diesem Satz IX.24 können wir nun zeigen, dass F_5 keine Primzahl ist.

Lemma IX.25

Euler. *F_5 ist keine Primzahl.*

Beweis. Nach Satz IX.24 müssen wir nur Primteiler der Form $128k + 1$ betrachten. Diese wären 129, 257, 385, 513, 641 usw.

Es sind 129, 385 und 513 keine Primzahlen. Es ist $257 = F_3$. Nach Lemma IX.23 ist $F_3 \nmid F_5$. Also müssen wir als erste Zahl 641 testen.

Es ist

$$641 - 1 = 640 = 5 \cdot 2^7.$$

Weiter ist

$$5^4 2^{28} = (641-1)^4 \equiv (-1)^4 \equiv 1 (\mathrm{mod}\, 641)$$

und dann

$$641 = 5^4 + 2^4 \text{ also } 5^4 \equiv -2^4 (\mathrm{mod}\, 641).$$

Das liefert

$$1 \equiv -2^4 2^{28} \equiv -2^{32} (\mathrm{mod}\, 641).$$

Somit ist $641 | 2^{32} + 1 = F_5$. □

In der Tat ist F_5 ein Produkt von zwei Primzahlen

$$F_5 = 641 \cdot 6700417.$$

Sei $F_n = 2^{2^n} + 1$ eine Primzahl. Dann ist 3 kein Quadrat modulo F_n, da

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$$

ist.

Ist also F_n eine Primzahl, so ist

$$3^{F_n - 1} \equiv 1 (\mathrm{mod}\, F_n) \text{ aber } 3^{\frac{F_n-1}{2}} \underset{(IX.2)}{\not\equiv} 1 (\mathrm{mod}\, F_n).$$

Also ist

$$o_{F_n}(3) = 2^{2^n}.$$

Sei umgekehrt $3^{2^{2^n}} \equiv 1 (\mathrm{mod}\, F_n)$ aber $3^{2^{2^n - 1}} \not\equiv 1 (\mathrm{mod}\, F_n)$. Dann erhalten wir $o_{F_n}(3) = 2^{2^n}$.

Nach dem Satz von Euler IV.17 gilt immer:

$$o_{F_n}(3) \text{ ist ein Teiler von } \varphi(F_n).$$

Somit ist $F_n - 1 = 2^{2^n}$ ein Teiler von $\varphi(F_n)$. Das liefert dann $\varphi(F_n) = F_n - 1$. Also sind alle Elemente in $\mathbb{Z}/F_n\mathbb{Z}$ invertierbar, was bedeutet, dass $\mathbb{Z}/F_n\mathbb{Z}$ ein Körper ist. Nach der Bemerkung auf Seite 12 ist dann F_n eine Primzahl. Damit haben wir

F_n ist genau dann Primzahl, wenn $o_{F_n}(3) = 2^{2^n}$ ist. **Lemma IX.26**

Unter den Primzahlen spielen noch die *Mersenne-Zahlen* $M_n = 2^n - 1$ eine wichtige Rolle. Es ist $M_2 = 3, M_3 = 7, M_4 = 15, M_5 = 31$. Ist $n = kr$, so ist $2^r - 1$ ein Teiler von M_n. Also ist M_n höchstens für $n = p$, p prim, eine Primzahl. Die Rekordprimzahlen sind häufig *Mersenne*[6]*-Primzahlen*. Wir wollen dies hier aber nicht weiter vertiefen.

[6] Marin Mersenne (*8.9.1588 Soultière, †1.9.1648 Paris) studierte zusammen mit René Descartes am Jesuitenkolleg in La Flèche und wurde 1611 Franziskanermönch. Mersenne gilt als wichtiger Vermittler von Informationen, da er Briefkontakt mit vielen führenden Wissenschaftlern seiner Zeit hatte. Er lieferte Beiträge zur Mathematik, Akustik, Optik und Musiktheorie.

Übungsaufgaben

IX.1 Sei $a = 849$. Haben die folgenden Kongruenzen eine Lösung?

a) $x^2 \equiv a \pmod{9800}$.

b) $x^2 \equiv a \pmod{10160}$.

IX.2 Sei $a \geq 2$ und $a^n + 1$ eine Primzahl. Dann ist a gerade und $n = 2^m$ für geeignetes m.

IX.3 Sei $n > 1$ und $a^n - 1$ eine Primzahl. Dann ist $a = 2$ und n eine Primzahl.

IX.4 Seien $M_p = 2^p - 1$ und $M_q = 2^q - 1$, p und q Primzahlen, $M_p \neq M_q$. Zeige:

$$\text{ggT}\,(M_p, M_q) = 1.$$

IX.5 Berechne das Legendre-Symbol $\left(\frac{2005}{44021}\right)$.

IX.6 Bestimme die letzten drei Ziffern von F_{73}.

IX.7 Bestimme alle Primzahlen p, für die -5 ein quadratischer Rest ist.

IX.8 Man bestimme die Lösungen von $x^2 + 12x + 11 \equiv 0 \pmod{23}$.

IX.9 Seien p eine ungerade Primzahl und $a, b \in \mathbb{Z}$ beide teilerfremd zu p. Dann hat $ax^2 + by^2 \equiv 0 \pmod{p}$ genau dann eine Lösung x, y, beide teilerfremd zu p, wenn $\left(\frac{a}{p}\right) = \left(\frac{-b}{p}\right)$ ist.

IX.10 Sei $a \in \mathbb{Z}$. Zeige $\left(\frac{a}{3}\right) \equiv a \pmod{3}$.

IX.11 Sei $p \neq 3$ eine ungerade Primzahl. Zeige, dass $\left(\frac{3}{p}\right) = 1$ für alle p mit $p \equiv \pm 1 \pmod{12}$ und $\left(\frac{3}{p}\right) = -1$ für alle p mit $p \equiv \pm 5 \pmod{12}$ ist.

IX.12 Sei $n > 1$. Zeige, dass das Jacobi-Symbol $\left(\frac{3}{3^n - 2}\right)$ den Wert $(-1)^{n+1}$ hat.

IX.13 Man bestimme alle $a \in \mathbb{N}$, so dass für ein $k \in \mathbb{Z}$ die Zahl $a + 29k$ eine Quadratzahl ist.

IX.14 Zeige, dass es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{4}$ gibt.
(Hinweis: Betrachte $n = (2p_1 \cdots p_m)^2 + 1$ und zeige, dass -1 ein Quadrat für jeden Primteiler p von n ist.)

Literaturverzeichnis

[1] N.H. Abel, Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré, Journal für die reine und angewandte Mathematik 1:66-87, 1826

[2] W.R. Alford & A. Granville, C. Pomerance, There are Infinitely Many Carmichael Numbers. Ann. Math. 139:703–722, 1994

[3] M. Aschbacher, Finite Group Theory, Cambridge University Press 1986

[4] B. Bundschuh, Einführung in die Zahlentheorie, Springer Verlag Heidelberg 1988, 6. überarbeitete Auflg. 2008

[5] G. Cardano, Ars Magna, or the Rules of Algebra, Dover Publications, Inc. New York 1993

[6] H. Chatland & H. Davenport, Euclid's algorithm in real quadratic fields, Canadian Journal of Math. 2:289–296, 1950

[7] P. Erdös, Über die Reihe $\sum \frac{1}{p}$, Mathematica, Zutphen B7, 1-2, 1938

[8] P. Erdös, Beweis eines Satzes von Tschebyschef, Acta Sci. Math. Szeged 5:194–198, 1930–1932.

[9] O. Forster, Algorithmische Zahlentheorie, Vieweg Verlag 1996

[10] I.N. Herstein, Topics in Algebra, John Wiley & Sons, Inc. New York 1975

[11] G.H. Hardy & E.M. Wright, Einführung in die Zahlentheorie, Oldenbourg 1958

[12] P. Hoffman, The man who loved only numbers, Hyperion 1998

[13] N. Jacobson, Basic Algebra I, II, Freeman & Co., San Francisco 1974, 1980

[14] I. Kaplansky, Fields and Rings, The University of Chicago Press, Chicago 1972

[15] N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag 1987

[16] E. Landau, Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques, Bull. Soc. Math. France 33:251–261, 1905

[17] J.W. Matijassewitsch, Enumerable sets are Diophantine. In: Soviet mathematics Doklady. American Mathematical Society, Providence RI 11, 1970.

[18] J. McKay, Another proof of Cauchy's group theorem, Americam Math. Monthly 66:119, 1959

[19] M. Mignotte, An inequality about factors of polynomials, Math. Comp. 28:1153–1157, 1974

[20] M. Mignotte, Some useful bounds, Symbolic & Algebraic Computation (Computing Supplementum 4) (ed. B. Buchberger, G.E. Collins, R. Loos), Springer Verlag, Wien, New York 1982, 259–263

[21] P.M. Neumann, G.A. Stoy & E.C. Thompson, Groups and Geometry, Oxford Science Publications 1994

[22] H. Opolka & W. Scharlau, Von Fermat bis Minkowski, Springer Verlag 1980

[23] H. Pieper, Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauß, Birkhäuser Verlag 1978

[24] G. Polya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, Acta Math. 68:145–254, 1937

[25] L. Toti Rigatelli, Evariste Galois 1811–1832, Birkhäuser Verlag, Basel 1996

[26] E. Scholz, Geschichte der Algebra, BI Wissenschaftsverlag, Mannheim-Wien-Zürich 1990

[27] R. Schulze-Pillot, Elementare Algebra und Zahlentheorie, Springer Verlag 2007

[28] R. Solomon, On finite simple groups and their classification, Notices of the American Mathematical Society 42:231–239, 1995

[29] H. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14:1–27, 1967

[30] G. Stroth, Algebra, De Gruyter Verlag, Berlin 1998

[31] B.L. van der Waerden, A History of Algebra, Springer-Verlag 1985

[32] W. Willems, Codierungstheorie und Krytographie, Birkhäuser Verlag 2008

[33] J. Wohlfart, Einführung in die Zahlentheorie und Algebra, Vieweg Verlag 1996

[34] M. Zorn, A remark on methods in transfinite algebra, Bull. Amer. Math. Soc. 41:667–670, 1935

Index