Einführung in die Algebra und Zahlentheorie

Dr. Stefan Kühnlein

Institut für Algebra und Geometrie, Karlsruher Institut für Technologie, Frühjahr 2012

Vorgeplänkel

Es ist das Hauptziel dieses Skriptums, die zentralen Objekte und Sichtweisen der Algebra und Elementaren Zahlentheorie einzuführen. Dabei habe ich mich überwiegend um algebraische Aspekte der Zahlentheorie gekümmert. Ich habe versucht, mich vom Gedanken leiten zu lassen, dass die strukturelle Sichtweise der Algebra und der oft mehr inhaltliche Ansatz der Zahlentheorie sich gegenseitig ergänzen. Nach langem Hin und Her habe ich mich schließlich dazu entschieden, zunächst die strukturellen Aspekte zu betonen und den zahlentheoretischen Inhalt erst nach und nach unterzuheben.

Ein zentrales algebraisches Objekt ist die Gruppe. Was hat das mit Arithmetik zu tun?

Algebra war von alters her die Lehre vom Lösen von Gleichungen. Schon die Babylonier konnten vor gut 4000 Jahren quadratische Gleichungen lösen, und wir haben es von ihnen gelernt. Die Technik ist die der quadratischen Ergänzung:

$$X^2 + bX + c = (X + \frac{b}{2})^2 + (c - \frac{b^2}{4}) = 0 \iff X = \frac{-b + \sqrt{b^2 - 4c}}{2},$$

wobei für die Quadratwurzel zwei Vorzeichenwahlen in Betracht zu ziehen sind.

Natürlich hat man das in Babylon nicht so aufgeschrieben, und man musste Fallunterscheidungen machen, denn so etwas abstruses wie negative Zahlen gab es ja noch nicht.

Dergleichen wurde viel später aufgeschrieben von al-Hwārizmī (ca. 780-850 n. Chr.), dessen Name in vielen verschiedenen Transkriptionen gehandelt wird. Ihm ist der Begriff *Algorithmus* gewidmet, denn er hat die seinerzeit bekannten Lösungswege für Gleichungen systematisiert und der Nachwelt hinterlassen, und zwar in einem Buch namens „Ein kurzgefasstes Buch über die Rechenverfahren durch Ergänzen und Ausgleichen“. Diese Ergänzen (al-ğabr) ist das, was al-Hwārizmī für entscheidend hält. Aus dem arabischen Wort wird unser Wort Algebra.

Aber inhaltlich sollte es natürlich noch weitergehen. Wie löst man kubische Gleichungen?

Hier gibt es noch mehr Vorzeichenverteilungsmöglichkeiten und damit auch noch mehr Fallunterscheidungen, die aber letztendlich doch von Leuten wie Cardano (1501-1576) und Tartaglia (ca. 1499-1557) zusammengefasst wurden. Zunächst eliminiert man aus

$$X^3 + aX^2 + bX + c = 0$$

den quadratischen Term, indem man X durch $X + \frac{a}{3}$ ersetzt. Zu lösen ist also ohne Einschränkung eine Gleichung der Form

$$X^3 + bX + c = 0.$$

Um dies zu machen könnte man etwa X durch $Y - Z$ ersetzen und hoffen, dass sich hierbei durch geschickte Wahlen etwas ergibt.

$$(Y - Z)^3 + b(Y - Z) + c = Y^3 - Z^3 - (Y - Z)(3YZ - b) + c = 0$$

wird einfacher, wenn man $3YZ = b$ setzt (was ja geht), und man löst also zwei Gleichungen in zwei Variablen:

$$Y^3 - Z^3 + c = 0, \quad 3YZ = b.$$

Das wiederum wird einfacher, wenn wir $U := Y^3$ und $V := Z^3$ setzen. Wir erhalten

$$U - V = -c, \quad UV = \big(\frac{b}{3}\big)^3.$$

Löst man hier die erste Gleichung nach U auf und setzt dies in die zweite ein, so erhalten wir

$$U = V - c, \quad V^2 - cV - \big(\frac{b}{3}\big)^3 = 0,$$

wobei wir die zweite Gleichung mit quadratischer Ergänzung lösen können, dann auch U erhalten und damit auch Y und Z durch Ziehen der dritten Wurzel; dies muss man dann konsistent machen, damit $X = Y - Z$ tatsächlich auch die ursprüngliche Gleichung löst. Das geht, und man erhält eine Lösungsformel, die man allerdings nicht unbedingt auswendig lernen sollte.

Auch Gleichungen vierten Grades konnte man schon im 16. Jhdt. lösen, sie lassen sich auf solche vom Grad 3 zurückführen, die wir gerade wiederum auf solche vom Grad 2 zurückgeführt haben.

Klar wollte man Grad 4 nicht als Grenze akzeptieren, sondern bemühte sich redlich, bis sich zu Beginn des 19. Jhdts. aus den Arbeiten von Abel (1802-1829) und Galois (1811-1832) ergab, dass eine allgemeine Lösungsformel ab Grad 5 nicht mehr existieren kann.

Das wichtigste Werkzeug beim Beweis dieser Unmöglichkeit ist aus heutiger Sicht grob gesagt die Menge all solcher Permutationen der Lösungsmenge, die die arithmetischen Relationen zwischen den Koeffizienten der Gleichung und der Lösungen respektieren. Das ist die Galoisgruppe, deren Behandlung wir aus Zeitgründen der Algebravorlesung überlassen.

Jedenfalls tauchen Mengen von Permutationen auf, hier in der Algebra und – auch im frühen 19. Jhdt. – in der Geometrie. Isometrien, Symmetrien, Kollineationen, das sind so die Schlagwörter, die dabei eine Rolle spielen.

Diese beiden Quellen fließen zusammen, als der Gruppenbegriff in der zweiten Hälfte des 19. Jhdts. spätestens bei Cayley (1821-1895) zutage tritt. Auch die Grundlagenfragen der Mathematik (was sind zum Beispiel Zahlen?) spielen hier eine Rolle. Letztlich werden die Zahlen heute nicht mehr ontologisch eingeführt,

sondern sie werden nur noch als Elemente einer Menge gesehen, mit denen man dies oder das machen kann. Eine natürliche Zahl ist ein Element von $\mathbb{N}$, und $\mathbb{N}$ ist durch diese und jene Eigenschaften charakterisiert. Ob die dabei benutzten Axiome tatsächlich all das zum Ausdruck bringen, was man haben möchte, ist jeweils zu klären. Dafür muss man all die Sätze beweisen, die dem Novizen so selbstverständlich sind, weil er noch nicht axiomatisch denkt, sondern inhaltliche Vorurteile mitbringt.

Die sich immer stärker vordrängende axiomatische Sichtweise fand einen ersten Höhepunkt in der damals so genannten modernen Algebra bei Emmy Noether (1882-1935) und Emil Artin (1898-1962), die in van der Waerdens (1903-1996) Lehrbuch aus dem Jahr 1930 vorbildlich dargestellt ist.

Mittlerweile ist das schon wieder etwas veraltet, und viele strukturelle Aspekte sind dort noch nicht im heute üblichen Maße zu finden. Lesenswert ist es allemal noch.

$\sim$

Am Anfang wird die Vorlesung relativ definitionslastig sein, ich hoffe, dass dies nicht zu dröge wird. Vieles haben Sie in der einen oder anderen Form auch schon gesehen, aber Wiedersehen macht Freude.

Ich werde in der Vorlesung einige Beweise ausführlicher darstellen als dies in dieser schriftlichen Fixierung der Fall ist. Da ich mein Skript nicht auswendig lerne und gerne relativ frei vortrage, wird die Notation oft nicht deckungsgleich sein. Bitte sehen Sie mir das nach!

Im Skript sind einige Nummern eingefügt, die ziemlich sicher dem Zeitmanagement zum Opfer fallen werden. Diese sind dann natürlich nicht prüfungsrelevant, könnten aber trotzdem nicht uninteressant sein.

Ich hoffe nun, der Spaß beim weiteren Verlauf der Vorlesung wird nicht mir allein vorbehalten sein, und will das mir mögliche tun, genau dazu beizutragen.

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Magmen

Obwohl die meisten Lehrbücher zur Algebra im Gegensatz zum Bourbaki nicht wirklich auf Magmen eingehen, dachte ich, dass das ein netter Ausgangspunkt ist. Hier wird es viel heiße Luft geben, die nachher dafür sorgen soll, dass der Ballon der Algebra ins Steigen kommt (und nicht etwa platzt...)

Definition/Bemerkung 1.1.1 Magma

a) Ein *Magma* (oder *Verknüpfungsgebilde*) ist eine Menge mit einer (fixierten) Verknüpfung. Streng genommen ist das also ein Paar $(M, *)$, wobei M eine Menge ist und

$$* : M \times M \longrightarrow M$$

eine Abbildung.

Statt (formal korrekt) $*(m, n)$ notiert man den Wert der Verknüpfung von $m, n \in M$ als $m * n := *(m, n)$. Dabei kommt es meistens auf die Reihenfolge an! Oft – wenn klar ist, welche Verknüpfung man meint – nennt man auch schon M das Magma. Man notiert die Verknüpfung auch oft als $(m, n) \mapsto mn$ ohne ein „Symbol“ für die Abbildung zu verwenden.

b) Ein Magma $(M, *)$ heißt *assoziativ*, wenn für alle $l, m, n \in M$ die Regel

$$(l * m) * n = l * (m * n)$$

gilt. Man nennt $(M, *)$ dann auch eine *Halbgruppe* (Vorsicht: das wird in der Literatur nicht absolut einheitlich gehandhabt!).

c) Ein Element $e \in M$ heißt ein (beidseitiges) *Neutralelement* des Magmas $(M, *)$, wenn für alle $m \in M$ die Regel

$$m * e = e * m = m$$

gilt. Wir werden immer nur beidseitige Neutralelemente betrachten und das Adjektiv „beidseitig“ oft weglassen, auch wenn es korrekter wäre.

Wenn es ein neutrales Element gibt, dann ist es eindeutig bestimmt. Sind nämlich $e, f \in M$ beides Neutralelemente, dann folgt

$$f = e * f = e,$$

wobei man bei der ersten Gleichung benutzt, dass e neutral ist, und bei der zweiten, dass f neutral ist.

Eine Halbgruppe mit Neutralelement nennt man auch ein *Monoid*.

d) Ein Magma $(M, *)$ heißt *kommutativ*, wenn für alle $m, n \in M$ die Regel

$$m * n = n * m$$

gilt.

Beispiel 1.1.2 Erste Beispiele

a) Die Abbildung

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}, \quad x * y := x + \sin y,$$

macht aus $\mathbb{R}$ ein Magma. Hier gilt zum Beispiel für die meisten x, y, z

$$(x * y) * z = (x + \sin y) * z = x + \sin y + \sin z \neq x + \sin(y + \sin z) = x * (y * z).$$

Also ist das Magma nicht assoziativ. Es ist offensichtlich auch nicht kommutativ, und besitzt kein beidseitiges Neutralelement.

b) Die natürlichen Zahlen $\mathbb{N} := \{1, 2, 3, \dots\}$ mit der Addition als Verknüpfung sind ein assoziatives und kommutatives Magma, besitzen aber kein neutrales Element – das liegt erst in $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

c) Man kann eine Verknüpfung natürlich durch ihre Verknüpfungstafel angeben. Zum Beispiel betrachten wir auf der dreielementigen Menge $M := \{a, b, c\}$ die Verknüpfung, die durch

$*$	a	b	c
a	c	c	c
b	c	c	c
c	c	c	a

gegeben ist. Diese ist kommutativ, es gibt kein Neutralelement, und die Assoziativität ist auch verletzt:

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

d) Ein **wichtiges Beispiel** ist das Magma $\mathrm{Abb}(D, D)$ aller Abbildungen von D nach D, wobei D eine beliebige Menge ist. Als Verknüpfung nimmt man

dabei die Komposition von Abbildungen. Dieses Magma ist assoziativ, hat ein neutrales Element (nämlich die Identität id_D), ist aber nicht kommutativ, wenn D mindestens zwei Elemente enthält.

e) Das *leere Magma* ist die leere Menge $\emptyset$ mit der einzig möglichen Abbildung $\emptyset \times \emptyset \longrightarrow \emptyset$ als Verknüpfung. Das *triviale Magma* ist eine einelementige Menge mit der einzig möglichen Verknüpfung.

Definition/Bemerkung 1.1.3 Untermagma

a) Eine Teilmenge U des Magmas M heißt ein *Untermagma*, wenn $U * U \subseteq U$ gilt. Die Einschränkung von $*$ auf $U \times U$ macht aus solch einem Untermagma selbst ein Magma.

Assoziativität und Kommutativität vererben sich von Magmen auf ihre Untermagmen. Ein neutrales Element muss natürlich nicht immer in einem Untermagma liegen – siehe $\mathbb{N} \subseteq \mathbb{N}_0$.

Der Durchschnitt einer beliebigen Familie $(U_i)_{i\in I}$ von Untermagmen (wobei I eine nichtleere Indexmenge ist) ist wieder ein Untermagma von M. Denn für alle $x, y,$ die im Durchschnitt liegen, gilt für alle $i \in I$:

$$x * y \in U_i,$$

denn U_i ist ein Untermagma. Daher liegt $x * y$ auch in $\bigcap_{i\in I} U_i$.

b) Für eine Teilmenge $X \subseteq M$ sei $\langle X\rangle_{Magma}$ der Durchschnitt aller Untermagmen von M, die X als Teilmenge enthalten. Das ist das *von X erzeugte Untermagma* von M. Etwas kürzer: das *Magmenerzeugnis* von X in M.

Vorsicht: selbst Magmen, die von einem Element erzeugt werden, müssen nicht notwendig assoziativ sein. Das Magma in Beispiel 1.1.2c) etwa ist von b erzeugt, denn $b * b = c$ und $c * c = a$, also liegen auch a und c in jedem Untermagma, das b enthält: $\langle b\rangle_{Magma} = \{a, b, c\}$.

c) Ein *Untermonoid* eines Monoids M ist ein Untermagma, das auch das neutrale Element von M enthält.

So ist etwa $\{0\} \subseteq \mathbb{Z}$ eine Teilmenge, die unter Multiplikation stabil ist, aber kein Untermonoid von $(\mathbb{Z}, \cdot)$.

Beispiel 1.1.4 symmetrische Gruppe

a) In einem assoziativen Magma $(M, *)$ ist für festes $X \subseteq M$ das von X erzeugte Magma gleich

$$\langle X\rangle_{Magma} = \bigcup_{n\in\mathbb{N}} X_n,$$

wobei rekursiv $X_1 = X, X_{n+1} := X * X_n$ gesetzt wird. Also ist

$$\langle X\rangle_{Magma} = \{x_1 * x_2 * \cdots * x_n \mid n \in \mathbb{N}, x_1, \ldots, x_n \in X\}.$$

Wegen der Assoziativität darf man hier die Klammern weglassen.

Besteht speziell X nur aus einem Element x, so finden wir $X_n = \{x^n\}$, wobei wie üblich $x^n = x * x * \cdots * x$ mit n Faktoren gesetzt ist.

b) Für eine Menge D ist die *symmetrische Gruppe*

$$\mathrm{Sym}(D) := \{\sigma \in \mathrm{Abb}(D, D) \mid \sigma \text{ ist bijektiv}\}$$

ein Untermagma von $\mathrm{Abb}(D, D)$. Es ist assoziativ und enthält ein neutrales Element. Wenn D mindestens 3 Elemente enthält ist $\mathrm{Sym}(D)$ nicht kommutativ.

Für $D = \{1, 2, \ldots, d\}$ schreibt man auch S_d anstatt $\mathrm{Sym}\,(D)$. Diese Magmen spielen eine besondere Rolle in der Gruppentheorie.

Eine *Transposition* ist ein Element von $\mathrm{Sym}\,(D)$, das alle bis auf zwei Elemente von X festlässt und die beiden anderen vertauscht. Genauer sei für zwei verschiedene Elemente $y, z \in D$ die Transposition $\tau_{y,z}$ definiert als die Bijektion von D mit

$$\forall x \in D : \tau_{y,z}(x) = \begin{cases} x, & x \notin \{y, z\}, \\ z, & x = y, \\ y, & x = z. \end{cases}$$

Nun sei $2 \leq d \in \mathbb{N}$ eine natürliche Zahl und $T_d \subseteq S_d$ die Menge aller Transpositionen in S_d. Wir zeigen:

$$\langle T_d \rangle_{Magma} = S_d.$$

Die Inklusion $\subseteq$ ist nach Definition klar. Wir zeigen noch die umgekehrte Inklusion, also dass sich jede Permutation aus S_d als Produkt von Transpositionen schreiben lässt.

Der **Beweis** geht per vollständiger Induktion nach d. Dabei fassen wir S_d als das Untermagma von S_{d+1} auf, dessen Elemente die Zahl $(d+1)$ auf sich selbst abbilden.

Für $d = 2$ ist die Behauptung klar, es gilt ja $\tau_{1,2}^2 = \mathrm{id}_{\{1,2\}}$, also $S_2 = \{\tau_{1,2}, \tau_{1,2}^2\}$.

Der Schritt von d nach $d+1$ geht zum Beispiel so: es sei $\sigma \in S_{d+1}$.

Fall 1: Wenn $\sigma(d+1) = d+1$ gilt, ist σ bereits in $S_d = \langle T_d \rangle_{Magma} \subseteq \langle T_{d+1} \rangle_{Magma}$.

Fall 2: Wenn $\sigma(d+1) = a \neq d+1$ gilt, dann liegt $\tau_{a,(d+1)} \circ \sigma$ in $S_d = \langle T_d \rangle_{Magma}$. Daher ist

$$\sigma = \tau_{a,(d+1)} \circ \tau_{a,(d+1)} \circ \sigma \in \tau_{a,(d+1)} \circ S_d \subseteq \langle T_d \cup \{\tau_{a,(d+1)}\} \rangle_{Magma} \subseteq \langle T_{d+1} \rangle_{Magma}.$$

Insgesamt sehen wir

$$\langle T_{d+1} \rangle_{Magma} \subseteq S_{d+1} \subseteq \langle T_{d+1} \rangle_{Magma}.$$

Man braucht übrigens gar nicht alle Transpositionen, es langen auch die, die jeweils benachbarte Zahlen vertauschen. Zum Beispiel gilt

$$\tau_{1,3} = \tau_{2,3} \circ \tau_{1,2} \circ \tau_{2,3}.$$

Definition/Bemerkung 1.1.5 Homomorphismus

Es seien $(M, *)$ und $(N, \diamond)$ zwei Magmen.

Ein *Homomorphismus* (oder auch *verknüpfungserhaltende Abbildung*) von M nach N ist eine Abbildung $\Phi : M \longrightarrow N$, sodass für alle $m_1, m_2 \in M$ die Gleichung

$$\Phi(m_1 * m_2) = \Phi(m_1) \diamond \Phi(m_2)$$

stimmt.

Das Bild $\Phi(M)$ ist dann ein Untermagma von N. Es ererbt vom Definitionsbereich gegebenenfalls die Assoziativität oder die Kommutativität.

Das Urbild $\Phi^{-1}(U)$ eines Untermagmas von N ist ein Untermagma von M.

Ist ein Homomorphismus Φ bijektiv, so nennt man ihn einen *Isomorphismus.* Dann ist auch die Umkehrabbildung Φ^{-1} ein Homomorphismus, denn für alle $n_1, n_2 \in N$ gilt

$$\begin{aligned}\Phi^{-1}(n_1 \diamond n_2) &= \Phi^{-1}\big(\Phi(\Phi^{-1}(n_1)) \diamond \Phi(\Phi^{-1}(n_2))\big) = \Phi^{-1}\big(\Phi(\Phi^{-1}(n_1) * \Phi^{-1}(n_2))\big) \\ &= \Phi^{-1}(n_1) * \Phi^{-1}(n_2).\end{aligned}$$

Mit $\mathrm{Hom}_{Magma}(M, N)$ bezeichnen wir die Menge aller Homomorphismen von M nach N. Streng genommen müssten hier auch die Verknüpfungen auf M und N in die Notation aufgenommen werden, das wird aber auf Dauer sehr schwerfällig.

Im Fall $M = N$ spricht man auch von *Endomorphismen* des Magmas $(M, *)$, und die Isomorphismen von M nach M heißen *Automorphismen* von M.

Die Menge aller Endomorphismen notieren wir als $\mathrm{End}_{Magma}(M)$ oder meistens einfacher als $\mathrm{End}(M)$; analog gibt es $\mathrm{Aut}_{Magma}(M)$.

Bei einem Monoidhomomorphismus wird man immer zusätzlich verlangen, dass das neutrale Element von M auf das von N abgebildet wird. Das ist keine notwendige Konsequenz aus der obigen Definition (aber siehe 1.3.3).

Beispiel 1.1.6 Beispiele

a) Es sei $N = \{x, y, z\}$ eine dreielementige Menge mit Verknüpfung $n_1 \diamond n_2 := n_2$, also Verknüpfungstafel

$\diamond$	x	y	z
x	x	y	z
y	x	y	z
z	x	y	z

Dann gibt es keinen Homomorphismus von N in das Magma M aus Beispiel 1.1.2c), denn für das Bild $\Phi(x)$ müsste ja gelten

$$\Phi(x) = \Phi(x \diamond x) = \Phi(x) * \Phi(x),$$

eine Bedingung, die von keinem Element von M erfüllt wird.

Die (drei) konstanten Abbildungen von M nach N sind dagegen allesamt Magmenhomomorphismen von M nach N, und sonst gibt es keinen.

b) Wenn M ein assoziatives Magma ist, dann gibt es eine Bijektion zwischen $\mathrm{Hom}_{Magma}(\mathbb{N}, M)$ und M. Ein Homomorphismus Φ von $\mathbb{N}$ nach M wird nämlich durch $\Phi(1)$ eindeutig bestimmt, und dieses lässt sich beliebig vorschreiben: für $m \in M$ ist $\Phi(k) := m^k$ offensichtlich ein Homomorphismus (wobei wir die Assoziativität brauchen – siehe Beispiel 1.1.4a)).

Allgemeiner gibt es eine Bijektion zwischen $\mathrm{Hom}_{Magma}(\mathbb{N}, M)$ und der Menge aller $m \in M$, für die $\langle m \rangle_{Magma}$ assoziativ ist.

Speziell sind Homomorphismen von $\mathbb{N}$ nach $\mathrm{Abb}(X, X)$ auch außerhalb der Mengenlehre interessant. Sie modellieren zum Beispiel (diskrete) dynamische Systeme.

c) Es sei M ein Magma. Dann wird durch

$$\Lambda : M \longrightarrow \mathrm{Abb}(M, M), \quad \Lambda(m) = [M \ni x \mapsto m * x \in M]$$

eine Abbildung definiert, die natürlich die Magmenstruktur von M codiert.

$\Lambda(m)$ ist die Abbildung, deren Wertetabelle gleich der Zeile in der Verknüpfungstafel ist, die m entspricht.

Λ ist genau dann ein Homomorphismus (wobei wir in $\mathrm{Abb}(M, M)$ die Komposition von Abbildungen als Verknüpfung verwenden), wenn M assoziativ ist, denn wir rechnen nach:

$$\begin{array}{ll} & \Lambda \text{ ist Homomorphismus} \\ \iff & \forall m_1, m_2 \in M : \Lambda(m_1 * m_2) = \Lambda(m_1) \circ \Lambda(m_2) \\ \iff & \forall m_1, m_2 \in M : \forall x \in M : (\Lambda(m_1 * m_2))(x) = (\Lambda(m_1) \circ \Lambda(m_2))(x) \\ \iff & \forall m_1, m_2 \in M : \forall x \in M : (m_1 * m_2) * x = m_1 * (m_2 * x). \end{array}$$

In diesem Fall heißt Λ die *linksreguläre Operation* von M.

Wenn M sogar assoziativ mit einem Einselement ist (also ein Monoid), dann ist Λ injektiv, denn für beliebige $m_1, m_2 \in M$ gilt

$$\Lambda(m_1) = \Lambda(m_2) \Rightarrow (\Lambda(m_1))(e_M) = (\Lambda(m_2))(e_M) \Rightarrow m_1 = m_2.$$

Damit ist das Monoid $(M, *)$ zu seinem Bild $\Lambda(M) \subseteq \mathrm{Abb}(M, M)$ isomorph, man kann also jedes Monoid als Untermagma eines Magmas $\mathrm{Abb}(X, X)$ für eine geeignete Menge X auffassen. Noch anders gesagt: um eine Übersicht über alle Monoide zu bekommen, die es überhaupt geben kann, muss man „nur“ alle Untermonoide der Magmen $\mathrm{Abb}(X, X)$ (für alle Mengen X) angeben.

Naja – ob man das Übersicht nennen kann?

Wie dem auch sei – diese Art von Wirkung eines Objekts auf sich selbst werden wir noch verschiedentlich zu sehen bekommen und auch zum Beweis von Strukturaussagen benutzen. Siehe zum Beispiel 1.5.3!

d) Zwei einelementige Magmen sind immer isomorph. Daher hatten wir diese auch das triviale Magma genannt.

e) Für ein beliebiges Magma M gibt es genau einen Homomorphismus des leeren Magmas $\emptyset$ nach M, und genau einen Homomorphismus von M in das triviale Magma. Man sagt daher: das leere Magma ist ein *initiales Objekt* und das triviale Magma ein *finales Objekt* in der „Kategorie der Magmen“.

f) Wenn $(L,\diamond),(M,*),(N,\bullet)$ Magmen sind und $\Phi : L \longrightarrow M$, $\Psi : M \longrightarrow N$ Magmenhomomorphismen, dann ist auch

$$\Psi \circ \Phi : L \longrightarrow N$$

ein Magmenhomomorphismus. Denn für alle $l_1, l_2 \in L$ gilt

$$\begin{aligned}(\Psi \circ \Phi)(l_1 \diamond l_2) &= \Psi(\Phi(l_1 \diamond l_2) = \\ &= \Psi(\Phi(l_1) * \Phi(l_2)) = \\ &= \Psi(\Phi(l_1)) \bullet \Psi(\Phi(l_2)). \\ &= (\Psi \circ \Phi)(l_1) \bullet (\Psi \circ \Phi)(l_2).\end{aligned}$$

g) Sind X und Y zwei Mengen und $F : X \longrightarrow Y$ eine Bijektion, dann „induziert“ F einen Isomorphismus $F_* : \mathrm{Abb}(X,X) \longrightarrow \mathrm{Abb}(Y,Y)$ auf folgende Art:

$$\forall \Phi \in \mathrm{Abb}(X,X) : F_*(\Phi) := F \circ \Phi \circ F^{-1}.$$

Als Diagramm malt man sich das so hin:

$$\begin{array}{ccc} X & \stackrel{\Phi}{\longrightarrow} & X \\ {\scriptstyle F^{-1}}\uparrow & & \downarrow{\scriptstyle F} \\ Y & \stackrel{F_*(\Phi)}{\longrightarrow} & Y \end{array}$$

Es ist klar, dass F_* ein Homomorphismus ist:

$$F_*(\Phi_1 \circ \Phi_2) = F \circ \Phi_1 \circ \Phi_2 \circ F^{-1} = F \circ \Phi_1 \circ F^{-1} \circ F \circ \Phi_2 \circ F^{-1} = F_*(\Phi_1) \circ F_*(\Phi_2).$$

Die Umkehrabbildung F^{-1} induziert $(F_*)^{-1} = (F^{-1})_*$, daher ist F_* ein Isomorphismus... erinnern Sie sich an Abbildungsmatrizen aus der LA!

Bemerkung 1.1.7 Bemerkung

a) Ein Homomorphismus $\Phi : M \longrightarrow N$ wird durch seine Einschränkung auf ein Erzeugendensystem von M festgelegt.

Denn: Sind Φ und Ψ zwei Homomorphismen von M nach N, so ist die Menge

$$U := \{m \in M \mid \Phi(m) = \Psi(m)\}$$

ein Untermagma von M.

b) Es sei M ein Magma. Dann ist wegen Beispiel 1.1.6 f) $\mathrm{End}(M)$ ein Untermagma von $\mathrm{Abb}(M, M)$.

Auch die Automorphismen $\mathrm{Aut}(M)$ sind ein Untermagma; sie sind ja der Durchschnitt von $\mathrm{Sym}(M)$ und $\mathrm{End}(M)$.

$\mathrm{Aut}(M)$ ist niemals leer, denn id_M liegt immer darin. Auch ist $\mathrm{Aut}(M)$ als Teilmagma von $\mathrm{Abb}(M, M)$ assoziativ. Das Novum ist, dass nach der Rechnung aus Definition 1.1.5 zu jedem Automorphismus von M auch die inverse Abbildung ein Automorphismus ist, d.h.

$$\forall \Phi \in \mathrm{Aut}(M) : \exists \Psi \in \mathrm{Aut}(M) : \Phi \circ \Psi = \Psi \circ \Phi = \mathrm{id}_M.$$

Damit sind wir endlich bei den Gruppen angekommen (naja, wir waren auch in Beispiel 1.1.4 schon mal dort).

1.2 Der Gruppenbegriff

Definition 1.2.1 Gruppe

a) Es sei $(M, *)$ ein Magma. Dann heißt das Paar $(M, *)$ eine *Gruppe*, wenn es assoziativ ist, ein beidseitig neutrales Element (siehe 1.1.1) e existiert und schließlich für jedes $x \in M$ (mindestens) ein $y \in M$ existiert, sodass

$$x * y = y * x = e$$

gilt.

Bemerkung: Wenn $\tilde{y}$ ein weiteres Element in M mit der Eigenschaft

$$x * \tilde{y} = \tilde{y} * x = e$$

ist, dann folgt unter Ausnutzung der Assoziativität:

$$y = y * e = y * (x * \tilde{y}) = (y * x) * \tilde{y} = e * \tilde{y} = \tilde{y}.$$

Also ist y eindeutig durch die charakterisierende Gleichung festgelegt. Man nennt es das zu x *inverse Element* in $(M, *)$. Speziell ist zum Beispiel e zu sich selbst invers.

b) Ist $(M, *)$ eine Gruppe, so nennt man sie *kommutativ* oder auch *abelsch*[1], wenn sie als Magma kommutativ ist.

[1] Niels Henrik Abel, 1802-1829

Schreibweisen: Oft benutzt man als Zeichen für die Verknüpfung einen Malpunkt (und lässt dann meistens auch diesen noch weg) und schreibt x^{-1} für das Inverse zu x.

Die „additive Schreibweise“ mit $+$ als Symbol für die Verknüpfung (und $-x$ als zu x inversem Element), benutzt man höchstens für kommutative Gruppen. Das neutrale Element wird dann mit 0 bezeichnet.

Wenn klar ist, welche Verknüpfung man auf M betrachtet, so sagt man meistens, dass M eine Gruppe ist, ohne explizit die Verknüpfung mit zu erwähnen. Außerdem heißt eine typische Gruppe eher G als M.

Beispiel 1.2.2 (Zahlen, symmetrische Gruppe)

a) Die ganzen Zahlen $\mathbb{Z}$ mit der Addition bilden eine Gruppe.

Wie $\mathbb{Z}$ so bilden auch die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ mit der Addition als Verknüpfung eine Gruppe.

Bezüglich der (wie üblich definierten) Multiplikation muss man etwas mehr aufpassen. Wir finden aber zum Beispiel die Gruppen

$$(\{\pm 1\},\cdot),\quad (\mathbb{Q}\smallsetminus\{0\},\cdot),\quad (\mathbb{R}\smallsetminus\{0\},\cdot).$$

b) Während $\mathrm{Abb}(M,M)$ keine Gruppe ist, sobald M mehr als ein Element enthält, ist $\mathrm{Sym}(M)$ immer eine Gruppe. Das neutrale Element ist die Identität auf M, zu $\sigma\in\mathrm{Sym}(M)$ invers ist die Umkehrabbildung.

c) Eine Menge M mit genau einem Element m wird durch die einzig mögliche Verknüpfung darauf – $m*m=m$ – zu einer Gruppe; diese Gruppe heißt eine *triviale Gruppe*. Sie kennen zwei Beispiele hierfür: $(\{0\},+)$ und $(\{1\},\cdot)$.

Für jede Gruppe $(G,*)$ ist $(\{e_G\},*)$ eine (oft sagt man auch die) triviale Gruppe.

d) Nun habe die Menge M genau zwei Elemente e und m. Wenn wir festlegen, dass e neutrales Element sein soll, so gibt es nur eine Möglichkeit der Gruppenstruktur auf M:

$$e*e=e,\ e*m=m*e=m,\ m*m=e.$$

Die ersten drei Gleichungen werden von den Eigenschaften des neutralen Elements erzwungen, die letzte von der Existenz eines zu m inversen Elements. Die Assoziativität ist offensichtlich erfüllt.

e) Es sei $n\geq 1$ eine natürliche Zahl. Auf $\mathbb{Z}$ haben wir die Äquivalenzrelation

$$x\equiv y\ (\mathrm{mod}\ n)\iff n \text{ teilt } (x-y).$$

Man sagt dann, die Zahlen x und y seien *modulo n kongruent*.

Es sei $\mathbb{Z}/n\mathbb{Z}$ die Menge aller Äquivalenzklassen dieser Äquivalenzrelation:

$$\mathbb{Z}/n\mathbb{Z} := \{[k] \mid k \in \mathbb{Z}\} = \{[0], [1], [2], \ldots, [n-1]\}.$$

Auf dieser Menge definieren wir eine Verknüpfung $+_n$ mittels

$$[k] +_n [l] := [k + l].$$

Damit dies wirklich eine Verknüpfung ist, darf die Zuordnung nur von den jeweiligen Äquivalenzklassen, nicht aber von der konkreten Wahl von k oder l abhängen. Man muss also Folgendes überprüfen: wenn für $\tilde{k}, \tilde{l} \in \mathbb{Z}$ die Voraussetzung erfüllt ist, dass $[k] = [\tilde{k}]$ und $[l] = [\tilde{l}]$, dann gilt $[k + l] = [\tilde{k} + \tilde{l}]$. Dies verifiziert man wie folgt: $[k] = [\tilde{k}]$ bedeutet, dass eine ganze Zahl a mit $\tilde{k} = k + an$ existiert; genauso gibt es eine ganze Zahl b mit $\tilde{l} = l + bn$. Dann ist aber

$$\tilde{k} + \tilde{l} = k + an + l + bn = k + l + (a + b) \cdot n,$$

also sind $\tilde{k} + \tilde{l}$ und $k + l$ kongruent modulo n, und ihre Äquivalenzklassen stimmen überein.

Nun ist wegen

$$([k] +_n [l]) +_n [m] = [k + l + m] = [k] +_n ([l] +_n [m])$$

die Verknüpfung assoziativ, $[0]$ ist ein neutrales Element, und für $[k] \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$[k] +_n [-k] = [0].$$

Also ist $(\mathbb{Z}/n\mathbb{Z}, +_n)$ eine Gruppe.

Definition 1.2.3 Untergruppe

Es sei $(G, *)$ eine Gruppe. Dann ist eine *Untergruppe* von G ein nichtleeres Untermagma U, das unter Inversenbildung abgeschlossen ist.

Wir schreiben dafür: $U \leq G$. (Die Verknüpfung denken wir uns fixiert.)

Da U nichtleer ist, liegt ein x und damit auch x^{-1} darin, also auch deren Produkt, und damit das neutrale Element von G.

Insbesondere ist dann U mit der auf $U \times U$ eingeschränkten Verknüpfung aus G eine Gruppe.

$U \subseteq G$ ist genau dann eine Untergruppe, wenn U nicht leer ist und

$$\forall x, y \in U : xy^{-1} \in U.$$

Beispiel 1.2.4 Untergruppen

$(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$, $(\{\pm 1\}, \cdot)$ ist eine Untergruppe von $(\mathbb{Q} \setminus \{0\}, \cdot)$.

In 1.1.4 haben wir stillschweigend und mit nachhaltigem Erfolg S_d als Untergruppe von S_{d+1} aufgefasst.

Beispiel 1.2.5 Untergruppen der ganzen Zahlen

Wenn wir von $\mathbb{Z}$ als Gruppe sprechen, meinen wir immer die Addition als Verknüpfung. In diesem Beispiel wollen wir alle Untergruppen von $\mathbb{Z}$ kennenlernen.

Die triviale Untergruppe (1.2.2 e)) ist $\{0\}$. Es ist außerdem klar, dass für jede natürliche Zahl n die Teilmenge

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$$

eine Untergruppe ist, denn diese Menge ist nicht leer und mit nk und nl ist auch $nk - nl = n(k - l)$ in $n\mathbb{Z}$ enthalten. Für $n = 0$ erhalten wir wieder die triviale Untergruppe.

Wir zeigen nun umgekehrt, dass jede Untergruppe von $\mathbb{Z}$ eine der eben genannten ist. Es sei also $H \subseteq \mathbb{Z}$ eine Untergruppe, und H sei nicht die triviale Untergruppe (sonst wählen wir $n = 0$ und sind fertig). Dann gibt es in H ein von 0 verschiedenes Element x. Mit diesem liegt auch $-x$ in H, und es gibt demnach ein positives x in H. Die Menge $H \cap \mathbb{N}$ ist also nicht leer, und enthält damit auch ein kleinstes Element, welches wir n nennen. Die Behauptung ist nun, dass $H = n\mathbb{Z}$. Die Inklusion $\supseteq$ ist klar. Wenn umgekehrt $h \in H$ beliebig gewählt ist, so gilt für die größte Zahl k mit der Eigenschaft $kn \leq h$ die Ungleichung

$$0 \leq h - nk < n.$$

Da mit h und nk auch $h - nk$ in H liegt, muss nach Wahl von n die Differenz $h - nk$ gleich Null sein, also $h \in n\mathbb{Z}$.

Wir halten fest: Die Untergruppen von $\mathbb{Z}$ sind genau die Mengen $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$.

Hilfssatz 1.2.6 Durchschnitt von Untergruppen

Es seien G eine Gruppe, I eine nichtleere Menge, und für jedes $i \in I$ eine Untergruppe U_i von G gegeben. Dann ist auch $\cap_{i\in I} U_i$ eine Untergruppe von G.

Beweis. Der Durchschnitt ist ein nichtleeres Untermagma (1.1.3a), da er das neutrale Element e enthält. Mit $x \in \bigcap U_i$ liegt auch x^{-1} in jedem einzelnen U_i, und damit auch in deren Durchschnitt. ◯

Definition 1.2.7 Gruppenerzeugnis, zyklische Gruppe

a) Für eine Teilmenge M der Gruppe G sei I die Menge aller Untergruppen von G, die M enthalten. Dazu gehört zum Beispiel G selbst. Dann ist aber nach dem Vorhergehenden auch

$$\langle M \rangle := \bigcap_{i\in I} i$$

eine Gruppe, sie heißt das *(Gruppen-)Erzeugnis von* M oder die *von* M *erzeugte Untergruppe von* G. Es ist offensichtlich die kleinste Untergruppe von G, die M enthält.

Offensichtlich gilt

$$\langle M\rangle = \{x_1 \cdot x_2 \cdot \ldots \cdot x_k \mid k \in \mathbb{N}_0, x_i \in M \text{ oder } x_i^{-1} \in M\}.$$

b) Eine Gruppe G heißt *zyklisch*, wenn es ein Element $a \in G$ gibt, sodass $G = \langle\{a\}\rangle$. Hierfür schreibt man kürzer auch $G = \langle a\rangle$.

Beispiel 1.2.8 zyklische Gruppen

a) Für jede natürliche Zahl n ist die Gruppe $\mathbb{Z}/n\mathbb{Z}$ von [1] erzeugt.

b) Für beliebiges $g \in G$ und für $n \in \mathbb{N}$ setzen wir $g^0 := e_G$ und für $n > 0$ schreiben wir

$$g^n := g * g * \cdots * g \ (n \text{ Faktoren}), \quad g^{-n} := (g^{-1})^n.$$

Dann ist

$$\langle g\rangle = \{g^k \mid k \in \mathbb{Z}\}$$

die von g erzeugte zyklische Gruppe.

c) Wir wissen schon (seit 1.2.5), dass auch alle Untergruppen von $\mathbb{Z}$ zyklisch sind.

Trotzdem erzeugen auch zwei ganze Zahlen a, b immer eine Untergruppe H in $\mathbb{Z}$, konkreter gilt:

$$H = \{ra + sb \mid r, s \in \mathbb{Z}\}.$$

Da auch H zyklisch ist, gibt es also ein $g \in \mathbb{N}_0$ mit $H = \mathbb{Z}g$.

Da a und b in H liegen, ist g ein gemeinsamer Teiler von a und b.

Umgekehrt ist g von der Gestalt $ra+sb$, und damit teilt jeder gemeinsame Teiler von a und b auch g. Daher ist g der größte gemeinsame Teiler von a und b, siehe 3.1.1.

Definition 1.2.9 Ordnung

Die Kardinalität einer Gruppe nennt man auch ihre *Ordnung*. Die *Ordnung eines Elementes* $g \in G$ ist definiert als die Ordnung der von g erzeugten Untergruppe.

Bemerkung 1.2.10 Wenn $g \in G$ endliche Ordnung hat, dann ist diese gleich der kleinsten natürlichen Zahl k, für die $g^k = e_G$ gilt.

Denn: Es existieren ein $l > 0$ und ein $r \geq 0$ mit $g^r = g^{r+l}$, da die von g erzeugte Gruppe endlich ist. Daher ist (nach Kürzen von g^r aus der Gleichung) auch

$e_G = g^l$, und es gibt überhaupt ein kleinstes k mit der genannten Eigenschaft. Mit einem ähnlichen Argument sieht man ein, dass $e_G, g, g^2, \ldots, g^{k-1}$ paarweise verschiedene Elemente sind, was dann die Behauptung zeigt.

Satz 1.2.11 von Lagrange[2]

Es sei G eine endliche Gruppe und H eine Untergruppe von G. Dann ist die Ordnung von H ein Teiler der Ordnung von G.

Beweis. Wir definieren auf G die Relation $\sim$ durch

$$g_1 \sim g_2 : \Longleftrightarrow \; g_1 g_2^{-1} \in H.$$

Dann ist $\sim$ eine Äquivalenzrelation, wie man leicht nachrechnet.

Die Äquivalenzklasse eines Elements g ist

$$[g] = Hg := \{hg \mid h \in H\}.$$

Nun ist G aber die disjunkte Vereinigung der Äquivalenzklassen, und wir sind fertig, wenn wir gezeigt haben, dass jede Äquivalenzklasse genauso viele Elemente hat wie H. Dies zeigen wir durch die Angabe einer Bijektion von $H = [e_G]$ nach $[g]$:

$$F : H \longrightarrow Hg, \; h \mapsto hg.$$

Diese Abbildung ist surjektiv, wie man der vorletzten Gleichung entnimmt. Sie ist injektiv, denn

$$\forall h_1, h_2 \in H : F(h_1) = F(h_2) \Rightarrow h_1 g = h_2 g \Rightarrow h_1 g g^{-1} = h_2 g g^{-1} \Rightarrow h_1 = h_2.$$

◯

Speziell ist in jeder endlichen Gruppe die Ordnung jedes Elements ein Teiler der Gruppenordnung. Zum Beispiel ist eine Gruppe G, deren Ordnung eine Primzahl ist, immer zyklisch, und es gilt für $g \in G$:

$$G = \langle g \rangle \iff g \neq e_G.$$

Definition 1.2.12 Index

Wenn $H \leq G$ zwei Gruppen sind, dann heißt die Anzahl der Äquivalenzklassen aus dem Beweis auch der *Index* von H in G. In Zeichen: $(G : H)$.

Es gilt demnach für endliche Gruppen:

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

[2] Joseph Louis Lagrange, 1736-1813

Beispiel 1.2.13 Es sei $G = S_3$, das ist eine Gruppe der Ordnung 6. Weiter sei $\tau = \tau_{12}$ die Transposition, die 1 und 2 vertauscht. Wegen $\tau \neq \tau^2 = \mathrm{Id}$ hat τ Ordnung 2 und daher hat $H := \langle \tau \rangle$ Index 3 in S_3. Die Äquivalenzklassen werden hier repräsentiert von

$$\mathrm{Id},\ \tau_{13},\ \tau_{23}.$$

1.3 Homomorphismen von Gruppen

Wir kennen schon Homomorphismen zwischen Magmen und wiederholen die Definition nun noch einmal für Gruppen.

Definition 1.3.1 Gruppenhomomorphismus

Es seien $(G, *)$ und $(H, \bullet)$ zwei Gruppen. Ein *(Gruppen-)Homomorphismus* von G nach H ist ein Magmenhomomorphismus zwischen den beiden Magmen, also eine Abbildung $f : G \longrightarrow H$, für die gilt:

$$\forall x, y \in G : f(x * y) = f(x) \bullet f(y).$$

Die Menge aller Homomorphismen von G nach H nennen wir $\mathrm{Hom}(G, H)$.

Beispiel 1.3.2 Gruppenhomomorphismen

a) Für beliebige Gruppen G und H ist die Abbildung

$$f : G \longrightarrow H,\ \ \forall x \in G : f(x) := e_H,$$

ein Gruppenhomomorphismus, der so genannte *triviale* Homomorphismus.

b) Für $G = \mathbb{Z}$ und beliebiges h in beliebigem H ist die Abbildung (mit Notation aus 1.2.8b))

$$f : \mathbb{Z} \longrightarrow H,\ \ \forall x \in \mathbb{Z} : f(x) := h^x,$$

ein Homomorphismus von $\mathbb{Z}$ nach H:

$$f(x + y) = h^{x+y} = h^x \bullet h^y = f(x) \bullet f(y).$$

c) Für $G = (\mathbb{R}, +)$ und $H = (\mathbb{R}_{>0}, \cdot)$ ist die e-Funktion

$$\forall x \in \mathbb{R} : x \mapsto \exp x$$

ein Gruppenhomomorphismus: $\exp x + y = \exp x \cdot \exp y$.

Wir wollen einige grundsätzliche Eigenschaften von Gruppenhomomorphismen kennenlernen.

Hilfssatz 1.3.3 Eigenschaften von Homomorphismen

Es sei $f : G \longrightarrow H$ ein Homomorphismus von Gruppen. Dann gelten die folgenden Aussagen:

a) $f(e_G) = e_H$.

b) $\forall g \in G : \ f(g^{-1}) = f(g)^{-1}$.

c) $f^{-1}(\{e_H\})$ *ist eine Untergruppe von* G.

d) $f(G)$ *ist eine Untergruppe von* H.

e) f *ist genau dann injektiv, wenn* $f^{-1}(\{e_H\}) = \{e_G\}$.

Beweis. a) Es gilt

$$f(e_G) = f(e_G * e_G) = f(e_G) \bullet f(e_G).$$

Diese Gleichung wird nun mit dem zu $f(e_G)$ inversen Element multipliziert, sodass

$$e_H = f(e_G)$$

übrig bleibt, was zu zeigen war.

b) Es gilt

$$f(g) \bullet f(g^{-1}) = f(g * g^{-1}) = f(e_G) = e_H.$$

Genauso gilt auch $f(g^{-1}) \bullet f(g) = e_H$.

Nach Definition des inversen Elements heißt das $f(g^{-1}) = f(g)^{-1}$.

c) Wegen Teil a) gilt $e_G \in f^{-1}(\{e_H\})$, also ist $f^{-1}(\{e_H\})$ nicht leer. Wegen b) ist es unter Inversenbildung abgeschlossen, und offensichtlich auch unter der Multiplikation.

d) Wegen a) ist $e_H = f(e_G) \in f(G)$. Wegen b) ist $f(G)$ unter Inversenbildung abgeschlossen, und wegen 1.1.5 ist es ein Untermagma.

e) Wenn f injektiv ist, dann liegt in $f^{-1}(\{e_H\})$ nicht mehr als ein Element, aber e_G liegt nach a) darin, also folgt

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

Wenn umgekehrt diese Mengengleichheit gilt, dann folgt für $x, y \in G$ aus $f(x) = f(y)$:

$$e_H = f(y) \bullet f(y)^{-1} = f(x) \bullet f(y^{-1}) = f(x * y^{-1})$$

und damit $x * y^{-1} \in f^{-1}(\{e_H\}) = \{e_G\}$. Das heißt aber $x = y$, und f muss injektiv sein. ◯

Definition 1.3.4 Kern

Ist $f : G \longrightarrow H$ ein Homomorphismus zwischen zwei Gruppen, so heißt die Untergruppe $f^{-1}(\{e_H\}) \subseteq G$ der *Kern* von f.

Wir haben also gerade gezeigt: $f \in \mathrm{Hom}(G, H)$ ist genau dann injektiv, wenn $\mathrm{Kern}\,(f) = \{e_G\}$.

Wegen dieses Sachverhaltes und wegen des damit eng verknüpften Homomorphiesatzes führt man den Kern überhaupt ein.

Beispiel 1.3.5 Kerne

a) Der Kern des trivialen Homomorphismus (siehe 1.3.2a)) von G nach H ist G, sein Bild ist $\{e_H\}$.

b) Im Beispiel 1.3.2b) ist das Bild des Homomorphismus

$$\mathbb{Z} \longrightarrow H, \quad x \mapsto h^x,$$

die von h erzeugte Gruppe $\langle h \rangle$, und der Kern ist entweder $\{0\}$, nämlich wenn h nicht endliche Ordnung hat, oder er ist die Untergruppe von $\mathbb{Z}$, die von der Ordnung von h erzeugt wird.

c) Die Exponentialabbildung $\mathbb{R} \ni x \mapsto e^x \in \mathbb{R}_{>0}$ ist surjektiv, ihr Kern besteht nur aus der 0, also ist sie auch injektiv. Sie ist ein bijektiver Homomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}_{>0}, \cdot)$.

Definition 1.3.6 Endo-, Auto-, Isomorphismus

Wie für Magmen haben wir die folgenden Begrifflichkeiten:

a) Für eine Gruppe G heißt ein Homomorphismus von G nach G auch ein *Endomorphismus.* Die Menge aller Endomorphismen wird mit $\mathrm{End}(G)$ notiert.

b) Ein bijektiver Homomorphismus zwischen zwei Gruppen G und H heißt ein *Isomorphismus* zwischen G und H.

c) Einen bijektiven Endomorphismus der Gruppe G nennt man *Automorphismus* von G. Die Menge aller Automorphismen wird mit $\mathrm{Aut}(G)$ notiert.

Schreibweise: Wenn es (mindestens) einen Isomorphismus zwischen G und H gibt, so nennt man sie *isomorph*, und schreibt dafür $G \cong H$. Isomorph zu sein ist eine Äquivalenzrelation auf jeder Menge von Gruppen.

Beispiel 1.3.7 Wir haben gerade gesehen, dass die Exponentialabbildung ein Isomorphismus ist. Ein zweites Beispiel gewinnen wir wie folgt.

Es sei $G = \{1, -1\}$ mit Multiplikation und $H = \mathbb{Z}/2\mathbb{Z}$. Dann ist die Abbildung

$$f : G \longrightarrow H, \quad f(1) = [0], \ f(-1) = [1],$$

ein Gruppenisomorphismus.

Bemerkung 1.3.8 Invertieren eines Isomorphismus

Wie in 1.1.7 gesehen, ist die Inverse zu einem Magmenisomorphismus wieder ein Magmenisomorphismus.

Insbesondere ist für jede Gruppe G die Menge $\mathrm{Aut}(G)$ eine Gruppe bezüglich der Komposition von Abbildungen als Verknüpfung.

Beispiel 1.3.9 Konjugation, Zentrum

Es sei G eine Gruppe. Für festes $g \in G$ ist die Abbildung

$$\kappa_g : G \to G, \ \kappa_g(x) := gxg^{-1}$$

ein Automorphismus von G. Sie heißt die *Konjugation mit* g.

Zwei Gruppenmitglieder $x, y \in G$ heißen *zueinander konjugiert*, wenn es ein $g \in G$ gibt mit $y = gxg^{-1}$.

Die Abbildung $\kappa : G \to \mathrm{Aut}(G), g \mapsto \kappa_g$, ist ein Homomorphismus. Ihr Kern heißt das *Zentrum* $Z(G)$ von G, es gilt also

$$Z(G) = \{g \in G \mid \forall x \in G : \ gx = xg\}.$$

Das Bild $\kappa(G) =: \mathrm{Inn}(G)$ wird die Untergruppe der *inneren Automorphismen* in $\mathrm{Aut}(G)$ genannt.

Bemerkung 1.3.10 Normalteiler

Es sei K der Kern des Homomorphismus $f : G \longrightarrow H$. Dann gilt für alle $g \in G$ und alle $k \in K$, dass auch $g * k * g^{-1} \in K$:

$$f(g * k * g^{-1}) = f(g) \bullet f(k) \bullet f(g)^{-1} = f(g) \bullet e_H \bullet f(g)^{-1} = e_H.$$

Dieser Eigenschaft von K gibt man einen Namen und nennt K einen *Normalteiler* oder auch eine *normale Untergruppe*.

Ein Normalteiler von G ist also eine Untergruppe $N \subseteq G$, sodass für alle $n \in N$ und $g \in G$ die Bedingung $gng^{-1} \in N$ erfüllt ist. Anders gesagt: N ist invariant unter allen inneren Automorphismen.

Wenn eine Untergruppe U von G ein Normalteiler ist, dann wird das oft mit der Notation $U \lhd G$ ausgedrückt.

In abelschen Gruppen sind alle Untergruppen normal.

Als Übung kann man zum Beispiel zeigen, dass eine Untergruppe von Index 2 immer normal ist.

1.4 Faktorgruppen

Definition 1.4.1 Nebenklassen

a) Es sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann heißen $g, h \in G$ *kongruent modulo* U, wenn

$$g^{-1}h \in U.$$

Das ist eine Äquivalenzrelation auf G, und die Äquivalenzklassen sind von der Gestalt $gU = \{gu \mid u \in U\}$. Sie heißen die *Linksnebenklassen* nach U. Die Menge dieser Nebenklassen heißt der *Faktorraum* G/U.

Die Abbildung $\pi_U : G \to G/U,\ g \mapsto gU$ heißt die *kanonische Projektion.*

b) Analog gibt es auch Rechtsnebenklassen Ug, die ebenfalls eine disjunkte Zerlegung von G liefern.

c) Bemerkung: Es gilt $Ug = gU$ für alle $g \in G$ genau dann, wenn U ein Normalteiler (1.3.10) von G ist.

Definition 1.4.2 Faktorgruppe

Es sei $N \lhd G$ ein Normalteiler in der Gruppe G. Dann wird auf G/N (sprich: G modulo N) durch

$$(gN) \cdot (hN) := ghN$$

eine Verknüpfung definiert. Diese ist wegen

$$ghN = ghNN = g(hNh^{-1})hN = gNhN$$

tatsächlich wohldefiniert.

Sie ist assoziativ, da die Multiplikation in G dies ist, $N = e_G N$ ist das neutrale Element, und zu gN ist $g^{-1}N$ invers. Also ist G/N eine Gruppe, die *Faktorgruppe von G modulo N.* Sie ist gerade so gemacht, dass die kanonische Projektion π_N ein Gruppenhomomorphismus ist. Der Kern ist N, und das zeigt auch, dass für eine Untergruppe, die kein Normalteiler ist, die Konstruktion so nicht funktioniert: Ein Kern ist ja immer ein Normalteiler.

Umgekehrt haben wir jetzt gesehen, dass jeder Normalteiler auch als Kern eines Gruppenhomomorphismus realisiert werden kann.

Wenn $N \lhd G$ ein Normalteiler ist und $\Psi : G/N \to H$ ein Gruppenhomomorphismus, dann ist auch $\Phi := \Psi \circ \pi_N$ ein Gruppenhomomorphismus. Diesen Spieß möchte man jetzt umdrehen.

Hilfssatz 1.4.3 Ein Homomorphiesatz

Es seien G, H zwei Gruppen und $N \lhd G$ ein Normalteiler.

a) Die Abbildung

$$L : \mathrm{Hom}(G/N, H) \to \mathrm{Hom}(G, H),\ \Psi \mapsto \Psi \circ \pi_N$$

ist injektiv und besitzt als Bild die Menge aller $\Phi \in \mathrm{Hom}(G, H)$ *mit der Eigenschaft*

$$N \subseteq \mathrm{Kern}(\Phi).$$

b) Ist $\Phi : G \to H$ *ein Homomorphismus mit* $\mathrm{Kern}(\Phi) = \mathrm{N}$*, dann ist*

$$\widetilde{\Phi} : G/N \ni gN \mapsto \Phi(g) \in \mathrm{Bild}(\Phi)$$

ein Isomorphismus zwischen G/N *und* $\mathrm{Bild}\,(\Phi)$.

Beweis. a) Es ist klar, dass die Abbildung injektiv ist. Ist umgekehrt Φ ein Homomorphismus von G nach H, dessen Kern N enthält, so wird durch

$$\Psi : G/N \to H,\ gN \mapsto \Phi(g),$$

eine Abbildung festgelegt. Diese ist offensichtlich ein Homomorphismus und erfüllt $\Phi = \Psi \circ \pi_N$.

Das zeigt die behauptete Bjektivität.

b) Wie in a) ist klar, dass die Abbildung $\widetilde{\Phi}$ wohldefiniert ist. Außerdem erfüllt sie $\Phi = \widetilde{\Phi} \circ \pi_N$. Ihr Bild ist gerade $\mathrm{Bild}\,(\Phi)$, und ihr Kern ist gerade $\{N\} = \{e_{G/N}\}$, also ist $\widetilde{\Phi}$ injektiv und damit ein bijektiver Homomorphismus. ◯

Folgerung 1.4.4 Erster Isomorphiesatz

Es seien G *eine Gruppe,* $H \leq G$ *eine Untergruppe und* $N \lhd G$ *ein Normalteiler. Dann ist auch* $HN = \{hn \mid h \in H,\ n \in N\}$ *eine Untergruppe von* G *und es gibt einen Isomorphismus*

$$H/(N \cap H) \cong (HN)/N.$$

Beweis. Die Einschränkung der kanonischen Projektion von G auf G/N nach H liefert einen Gruppenhomomorphismus von H nach G/N, dessen Bild offensichtlich gerade $(HN)/N$ ist. Der Kern aber ist $H \cap N$, und deshalb liefert 1.4.3 die Behauptung. ◯

Bemerkung 1.4.5 Endomorphismen von $\mathbb{Z}/n\mathbb{Z}$

a) Als eine Anwendung des Homomorphiesatzes wollen wir hier die Endomorphismen der Gruppe $H = \mathbb{Z}/n\mathbb{Z}$ studieren. Laut Homomorphiesatz entsprechen die genau den Homomorphismen von $\mathbb{Z}$ nach H, in deren Kern $n\mathbb{Z}$ enthalten ist. Sei also

$$\Phi : \mathbb{Z} \to H$$

ein Homomorphismus. Er ist durch $h := \Phi(1)$ gegeben, da $\forall k \in \mathbb{Z} : \Phi(k) = kh$. Jedes h aus H legt einen Homomorphismus fest.

Für jedes h gilt aber $nh = e_H$ (das ist der Satz von Lagrange), also liegt n und damit $n\mathbb{Z}$ im Kern eines jeden Homomorphismus von $\mathbb{Z}$ nach H.

Wir erhalten also für jedes $h \in H$ einen Endomorphismus von H, der den Erzeuger $1 + n\mathbb{Z}$ auf h abbildet. Das sind alle Endomorphismen.

b) Eine zweite Anwendung des Homomorphiesatzes ist folgendes:

Es seien $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ und $\Phi : G \to H$ ein Gruppenhomomorphismus.

Dann ist $\Phi(G) = \langle \Phi(g) \rangle$ isomorph zu $G/\text{Kern}(\Phi)$, und damit ist die Ordnung von $\Phi(g)$ gleich $\#G/\#\text{Kern}(\Phi)$, also ist die Ordnung von $\Phi(g)$ ein Teiler von n.

Definition 1.4.6 Einfachheit

Eine Gruppe G heißt *einfach*, wenn sie nichttrivial ist und keine Normalteiler außer G und $\{e_G\}$ besitzt.

Eine nichttriviale Gruppe ist also genau dann einfach, wenn jeder nichtkonstante Homomorphismus, der auf ihr definiert ist, injektiv ist.

Beispiele für einfache Gruppen sind Gruppen von Primzahlordnung. Später werden wir noch mehr einfache Gruppen sehen.

Alles andere als einfach sind die freien Gruppen. Ihnen wenden wir uns jetzt zu.

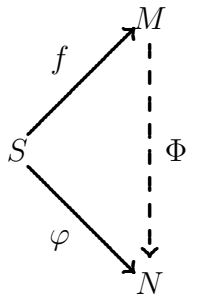
Definition 1.4.7 freie Gruppen

a) Es sei S eine Menge. Eine *freie Gruppe* über S ist eine Gruppe F mit einer Abbildung $f : S \to F$, sodass für jede Gruppe G und jede Abbildung $\varphi : S \to G$ genau ein Gruppenhomomorphismus $\Phi : F \to G$ existiert, für den

$$\forall s \in S : \varphi(s) = \Phi(f(s))$$

gilt.

b) Analog definiert man das *freie Monoid* M über der Menge S als ein Monoid M mit einer Abbildung $f : S \to M$, sodass für jede Abbildung von S in ein Monoid N genau ein Monoidhomomorphismus von M nach N existiert, der das folgende Diagramm kommutativ macht:



In beiden Fällen ist das definierte Objekt bis auf einen eindeutigen Isomorphismus durch die definierende Eigenschaft festgelegt, denn wenn z.B. sowohl M als auch N freie Monoide über S sind mit Abbildungen f und φ, dann gibt es sowohl von M nach N einen eindeutig bestimmten Homomorphismus Φ mit $\varphi = \Phi \circ f$ als auch von N nach M einen eindeutig bestimmten Homomorphismus Ψ mit $f = \Psi \circ \varphi$.

Damit bekommen wir die Endomorphismen $\Phi \circ \Psi$ und $\Psi \circ \Phi$, die jeweils

$$\Phi \circ \Psi \circ \varphi = \varphi \quad \text{und} \quad \Psi \circ \Phi \circ f = f$$

erfüllen und daher wegen der Eindeutigkeit jeweils die Identität sind.

Das freie Objekt ist also jeweils (bis auf Isomorphismus) eindeutig. Wir wollen jetzt sicherstellen, dass es existiert.

Hilfssatz 1.4.8 Die Existenz

Es sei S eine Menge. Dann existieren das freie Monoid und die freie Gruppe über S.

Beweis.

1. Die Existenz des freien Monoids ist einfach einzusehen, wir benutzen dazu die Menge M der endlichen Folgen in S :

$$M := \{(s_1, s_2, \ldots, s_n) \mid n \in \mathbb{N}_0, s_i \in S\}.$$

Als Verknüpfung auf M verwenden wir die Aneinanderhängung:

$$(s_1, s_2, \ldots, s_n) \circ (t_1, t_2, \ldots, t_m) := (s_1, s_2, \ldots, s_n, t_1, \ldots, t_m).$$

Es ist klar, dass dies assoziativ ist, und dass das „leere Wort“ neutrales Element für M ist.

M wird von den „einelementigen Folgen“ (s), $s \in S$, erzeugt, und wir benutzen $f : S \to M, s \mapsto (s)$ in der Definition des freien Monoids.

Ist nun $\varphi : S \to N$ eine Abbildung in ein Monoid, so liefert

$$\Phi((s_1, s_2, \ldots, s_n)) := \varphi(s_1) \cdot \ldots \cdot \varphi(s_n)$$

einen Monoidhomomorphismus, denn rechter Hand ist die Multiplikation ja auch assoziativ, und das leere Wort wird (definitionsgemäß) auf das neutrale Element in N abgebildet. Für Φ kann man leicht nachrechnen (wie in der Vorlesung geschehen), dass es tut was es soll.

2. Nun wollen wir eine freie Gruppe über S haben. Dazu nehmen wir eine zu S disjunkte Teilmenge $\widetilde{S}$, die zu S gleichmächtig ist, und eine feste Bijektion $\tilde{} : S \to \widetilde{S}$. Die inverse Abbildung nennen wir auch $\tilde{}$, es gilt also $\tilde{\tilde{s}} = s$.

(Wir fassen am Besten $\tilde{}$ als Abbildung von $S \cup \widetilde{S}$ in sich selbst auf.)

Es sei M das freie Monoid über $S \cup \widetilde{S}$. Wir fassen $S \cup \widetilde{S}$ als Teilmenge von M auf.

Für eine Abbildung $\varphi : S \to G$ (mit einer Gruppe G) sei Φ der eindeutig bestimmte Monoidhomomorphismus von M nach G, der für $s \in S$ die Bedingungen

$$\Phi(s) = \varphi(s), \quad \text{und} \quad \Phi(\tilde{s}) = \varphi(s)^{-1}$$

erfüllt.

Wir definieren auf M eine Relation:

$$m \sim n :\iff \forall G, \forall \varphi : S \to G : \Phi(m) = \Phi(n).$$

Dies ist eine Äquivalenzrelation: Reflexivität und Symmetrie sind klar, und die Transitivität eigentlich auch; wenn nämlich für alle φ gilt, dass $\Phi(m) = \Phi(n)$ und $\Phi(n) = \Phi(k)$, dann gilt auch für alle φ, dass $\Phi(m) = \Phi(k)$.

Wir definieren auf der Menge F aller Äquivalenzklassen eine Verknüpfung durch

$$[m] \circ [n] := [m \circ n].$$

Dies ist wohldefiniert, denn wenn für alle φ die Bedingung $\Phi(m) = \Phi(\hat{m})$ und $\Phi(n) = \Phi(\hat{n})$ erfüllt ist, dann gilt auch für alle φ die Gleichung

$$\Phi(m \circ n) = \Phi(m)\Phi(n) = \Phi(\hat{m})\Phi(\hat{n}) = \Phi(\hat{m} \circ \hat{n}).$$

Die Assoziativität folgt ähnlich, und die Äquivalenzklasse des leeren Wortes ist ein neutrales Element. Daher ist F ein Monoid.

Für ein Wort $m = (x_1, x_2, \ldots, x_k) \in M$ sei

$$\tilde{m} := (\tilde{x}_k, \ldots, \tilde{x}_2, \tilde{x}_1).$$

Dann ist klar, dass für jede Abbildung von S in eine Gruppe G folgt, dass

$$\Phi(\tilde{m}) = \Phi(m)^{-1}.$$

Daher ist die Äquivalenzklasse von $\tilde{m}$ im Monoid F zu der von m invers, und F ist eine Gruppe.

Nach Konstruktion hat diese die gewünschte Eigenschaft, die wir von der freien Gruppe über S erwarten. ◯

Bemerkung 1.4.9 Erzeuger und Relationen

Jede Gruppe G lässt sich als Faktorgruppe einer freien Gruppe schreiben, notfalls nehme man die freie Gruppe F über der Menge G und setze die Identität auf G zu einem Gruppenhomomorphismus von F nach G fort.

Allgemeiner kann man die freie Gruppe F über irgendeinem Erzeugendensystem S von G nehmen und die Identität auf diesem Erzeugendensystem zu einem Gruppenhomomorphismus $\pi : F \to G$ fortsetzen.

Eine Teilmenge $R \subset \mathrm{Kern}(\pi)$, für die der kleinste Normalteiler von F, der R enthält, gerade der Kern ist, ist dann ein System von Relationen zwischen den Erzeugern von G.

Ein Homomorphismus von G in eine andere Gruppe H lässt sich nach dem Homomorphiesatz 1.4.3 also auch verstehen als ein Homomorphismus von F nach H, der auf R trivial ist. Bisweilen ist das eine gute Antwort auf die Frage nach $\mathrm{Hom}(G, H)$.

Beispiel 1.4.10 $\mathbf{S}_3$

Die symmetrische Gruppe S_3 wird erzeugt von der Transposition $\tau = \tau_{1,2}$ und der Permutation ζ, die durch $1 \mapsto 2 \mapsto 3 \mapsto 1$ gegeben ist. Hierbei gilt $\tau^2 = \zeta^3 = 1$ und $\tau\zeta\tau^{-1} = \zeta^2$.

Es sei F die freie Gruppe in zwei Erzeugern x, y und $\pi : F \to S_3$ der Homomorphismus, der durch $\pi(x) = \tau,\ \pi(y) = \zeta$ festgelegt wird.

Dann ist π surjektiv, und wir wollen den Kern von π berechnen.

Im Kern liegen die Elemente $x^2,\ y^3,\ x^{-1}yxy^{-2}$. Es sei $N \subset F$ ein Normalteiler, der diese Elemente enthält. Dann wird F/N von den Restklassen $\xi = xN$ und $\eta = yN$ erzeugt. Wegen $\eta\xi = \xi\eta^2$ sind alle Elemente von F/N von der Gestalt $\xi^a\eta^b$, und hierbei zählt nur die Restklasse von a modulo 2 und die von b modulo 3. Also hat F/N höchstens 6 Elemente. Da aber S_3 eine Faktorgruppe von F/N ist, muss es auch mindestens 6 Elemente enthalten, und wir sehen, dass $N = \mathrm{Kern}(\pi)$ gilt.

Das heißt: Die Relationen $\tau^2 = \zeta^3 = 1$ und $\tau\zeta\tau^{-1} = \zeta^2$ erzwingen alle Rechenregeln in S_3.

1.5 Gruppenoperationen

Die Gruppentheorie dient dem Zweck, verschiedene Beispiele von Gruppen, die man ohnehin kennt und benutzt, unter einem einheitlichen Gesichtspunkt zu betrachten, indem eben die Gruppenaxiome als gemeinsames Wesensmerkmal der Beispiele herausdestilliert werden.

Wir haben bisher zwei Typen von Gruppen kennengelernt: Gruppen von Zahlen mit Addition oder Multiplikation als Verknüpfung und damit Verwandte (die Gruppen $\mathbb{Z}/n\mathbb{Z}$) stellen den einen Typ dar, die symmetrischen Gruppen den anderen. Der zweite Typ von Gruppen ist also dazu da, etwas mit Elementen einer Menge anzufangen. Dieser Aspekt soll hier etwas vertieft werden.

Definition 1.5.1 Gruppenoperation

Es seien $(G, *)$ eine Gruppe und M eine Menge. Dann ist eine *Operation von G auf M* definiert als eine Abbildung

$$\bullet : G \times M \longrightarrow M,$$

sodass die folgenden Bedingungen erfüllt sind:

a) $\forall m \in M : e_G \bullet m = m$,

b) $\forall m \in M, g_1, g_2 \in G : g_1 \bullet (g_2 \bullet m) = (g_1 * g_2) \bullet m$.

Eine Menge M mit einer festen Operation einer Gruppe G heißt amüsanter Weise auch eine *G-Menge.*

Wenn $G \subseteq \mathrm{Sym}(M)$ eine Untergruppe der symmetrischen Gruppe von M ist, dann wird solch eine Abbildung $\bullet$ zum Beispiel durch

$$g \bullet m := g(m)$$

gegeben. Dies ist die Urmutter aller Operationen, wie wir gleich sehen werden.

Hilfssatz 1.5.2 Operationen und symmetrische Gruppe

Es seien G eine Gruppe und M eine Menge.

a) Für jeden Homomorphismus $\Phi : G \longrightarrow \mathrm{Sym}(M)$ wird durch

$$g \bullet m := \Phi(g)(m)$$

eine Operation von G auf M festgelegt.

b) Für jede Operation $\bullet$ von G auf M gibt es einen Homomorphismus Φ, sodass $\bullet$ wie in Teil a) konstruiert werden kann.

Beweis. a) Dass hierbei aus einem Homomorphismus eine Operation gewonnen wird, ist klar.

b) Sei umgekehrt eine beliebige Operation $\bullet$ gegeben. Wir zeigen, wie man aus ihr den passenden Homomorphismus konstruiert. Für jedes $g \in G$ sei $\Phi_g : M \longrightarrow M$ die Abbildung, die durch

$$\forall m \in M : \ \Phi_g(m) := g \bullet m$$

gegeben wird. Die Abbildung Φ_g ist eine Bijektion, da die Abbildung $\Phi_{g^{-1}}$ zu ihr invers ist:

$$\begin{aligned} \forall m \in M : \quad & (\Phi_g \circ \Phi_{g^{-1}})(m) = g \bullet (g^{-1} \bullet m) \\ & = (g * g^{-1}) \bullet (m) = e_G \bullet m \\ & = m \\ & = (g^{-1} * g) \bullet (m) \\ & = (\Phi_{g^{-1}} \circ \Phi_g)(m). \end{aligned}$$

Also ist $g \mapsto \Phi_g$ eine Abbildung von G nach $\mathrm{Sym}(M)$, und diese ist ein Gruppenhomomorphismus wegen der zweiten Bedingung an die Operation. ◯

Beispiel 1.5.3 für Operationen

a) Im Fall $G = M$ wird eine wichtige Operation durch die Gruppenverknüpfung selbst festgelegt: $\bullet = *$. Man sieht leicht, dass der zugehörige Homomorphismus Φ von G in die symmetrische Gruppe $\mathrm{Sym}(G)$ injektiv ist, denn

$$\Phi(g)(e_G) = g * e_G = g,$$

also kann man g aus $\Phi(g)$ ablesen.

Das Bild von Φ ist also eine zu G isomorphe Untergruppe von $\mathrm{Sym}(G)$, und damit ist jede Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe. Diese Aussage nennt man oft den *Satz von Cayley*[3], den wir hiermit bewiesen haben. Er ist der Situation aus 1.1.6c) nachempfunden, oder eher umgekehrt.

b) Eine andere Art, wie G auf sich selbst operieren kann, ist die Operation durch Konjugation:

$$\forall g, m \in G : g \bullet m := gmg^{-1}.$$

c) Eine Untergruppe $G \subseteq \mathrm{Sym}(M)$ operiert auf der Potenzmenge von M durch

$$\forall \sigma \in G, \ A \subseteq M : \sigma \bullet A := \sigma(A).$$

[3] Arthur Cayley, 1821-1895

Auf ähnlichem Wege „induziert“ jede Gruppenoperation einer Gruppe auf einer Menge M eine Operation derselben Gruppe auf der Potenzmenge von M und auf anderen Derivaten von M, etwa den Abbildungen von M in eine andere Menge N. Nachrechnen:

$$G \times \mathrm{Abb}(M,N) \to \mathrm{Abb}(M,N), \quad (g,f) \mapsto [m \mapsto f(g^{-1} \bullet m)],$$

ist eine Operation.

Hilfssatz 1.5.4 Wieder einmal eine Äquivalenzrelation

Es sei G eine Gruppe, die auf der Menge M operiert. Dann wird auf M durch die Vorschrift

$$m_1 \sim m_2 : \Longleftrightarrow \exists g \in G : m_1 = g \bullet m_2$$

eine Äquivalenzrelation definiert.

Beweis. Die Relation ist reflexiv, da

$$\forall m \in M : m = e_G \bullet m, \text{ also } m \sim m.$$

Sie ist symmetrisch, da für alle $m_1, m_2 \in M$ gilt:

$$\begin{aligned} m_1 \sim m_2 &\Rightarrow \exists g \in G : g \bullet m_1 = m_2 \\ &\Rightarrow \exists g \in G : g^{-1} \bullet (g \bullet m_1) = g^{-1} \bullet m_2 \\ &\Rightarrow \exists g \in G : m_1 = g^{-1} \bullet m_2 \Rightarrow m_2 \sim m_1. \end{aligned}$$

Sie ist transitiv, da aus $m_1 \sim m_2$ und $m_2 \sim m_3$ die Existenz von $g_1, g_2 \in G$ mit

$$m_1 = g_1 \bullet m_2, \quad m_2 = g_2 \bullet m_3, \text{ also } m_1 = (g_1 * g_2) \bullet m_3$$

folgt und damit $m_1 \sim m_3$. ◯

Definition 1.5.5 Bahnen, Transitivität, Stabilisatoren

Es sei G eine Gruppe, die auf einer Menge M operiert.

Die Äquivalenzklassen aus der eben beschriebenen Äquivalenzrelation werden hier *Bahnen* oder auch *Orbiten* (von M unter der Operation von G) genannt. Die *Bahn von m* wird als

$$G \bullet m = \{g \bullet m \mid g \in G\}$$

notiert.

Die Operation heißt *transitiv*, wenn es genau eine Bahn gibt, wenn also ein m_0 existiert, sodass es für jedes $m \in M$ ein $g \in G$ gibt mit der Eigenschaft

$$m = g \bullet m_0.$$

Der *Stabilisator eines Elements* $m \in M$ unter einer gegebenen Operation der Gruppe G ist definiert als

$$\mathrm{Stab}_G(m) := \{g \in G \mid g \bullet m = m\}.$$

Ein *Fixpunkt von* G auf M ist ein Element, dessen Stabilisator ganz G ist. Die Menge aller Fixpunkte wird mit M^G notiert:

$$M^G := \{m \in M \mid \forall g \in G : g \bullet m = m\}.$$

Satz 1.5.6 Bahnbilanzformel

Es sei G eine Gruppe, die auf der endlichen Menge M operiert. Weiter sei $R \subseteq M$ ein Vertretersystem der Bahnen, d.h. aus jeder Bahn liegt genau ein Element in R. Dann gilt:

$$\#M = \sum_{r \in R} (G : \mathrm{Stab}_G(r)).$$

Beweis. Da M die disjunkte Vereinigung der Bahnen ist, gilt

$$\#M = \sum_{r \in R} \#(G \bullet r).$$

Es langt also, für jede einzelne Bahn $G \bullet r$ zu zeigen, dass

$$\#(G \bullet r) = (G : \mathrm{Stab}_G(r)).$$

Dazu betrachten wir die Abbildung

$$\eta : G \to G \bullet r, g \mapsto g \bullet r.$$

Sie ist surjektiv nach Definition der Bahn. Für zwei Elemente $g, h \in G$ gilt $\eta(g) = \eta(h)$ genau dann, wenn

$$\begin{aligned} g \bullet r = h \bullet r \quad &\iff r = g^{-1}h \bullet r \iff h^{-1}g \in \mathrm{Stab}_G(r) \\ &\iff g\mathrm{Stab}_G(r) = h\mathrm{Stab}_G(r). \end{aligned}$$

Das zeigt ganz analog zu den Überlegungen aus dem Beweis des Homomorphiesatzes, dass η eine wohldefinierte und injektive Abbildung

$$\widetilde{\eta} : G/\mathrm{Stab}_G(r) \to G \bullet r, \quad g\mathrm{Stab}_G(r) \mapsto g \bullet r,$$

liefert, die wegen der Surjektivität von η auch selbst surjektiv ist. Die Existenz solch einer Bijektion impliziert natürlich die gewünschte Übereinstimmung der Kardinalitäten. ◯

Wir werden die Bahnbilanzformel später noch zum Beweis von Strukturaussagen für endliche Gruppen benutzen.

Beispiel 1.5.7 Binomialkoeffizienten

a) Eine andere bekannte Anwendung der Bahnbilanzformel ist ein Beweis dafür, dass es für natürliche Zahlen $d \leq k$ in $\{1, \ldots, k\}$ genau $\binom{k}{d}$ Teilmengen mit d Elementen gibt. Denn die symmetrische Gruppe S_k operiert transitiv auf den d-elementigen Teilmengen, und der Stabilisator von $\{1, \ldots, d\}$ ist isomorph zu $S_d \times S_{k-d}$, hat also $d! \cdot (k-d)!$ Elemente, und damit Index $\binom{k}{d}$ in S_k.

b) Außerdem sieht man zum Beispiel, dass eine Operation einer Gruppe G von Primzahlordnung p auf einer Menge, deren Kardinalität nicht durch p teilbar ist, immer einen Fixpunkt haben muss. Denn sonst hätte jeder Punkt der Menge einen trivialen Stabilisator (G hat ja nur die Untergruppen G und $\{e_G\}$) und damit wäre die Kardinalität der Menge ein Vielfaches von p.

Beispiel 1.5.8 Zykelzerlegung

Es sei n eine natürliche Zahl und $\sigma \in S_n$ eine Permutation der Menge $M = \{1, \ldots, n\}$.

Dann operiert die von σ erzeugte Untergruppe $H \subseteq S_n$ auf M, und wir können M in Bahnen $B_1, \ldots, B_r$ zerlegen. Da H zyklisch ist, lassen sich die Bahnen so anordnen, dass σ darauf durch „Verschiebung“ wirkt:

$$\#B_i = k, \quad B_i = \{x_1, x_2, \ldots, x_k\}, \ \sigma(x_i) = \begin{cases} x_{i+1} & , 1 \leq i \leq k-1, \\ x_1 & , i = k. \end{cases}$$

Für $k \geq 2$ ist ein *k-Zykel* eine Permutation, die genau eine Bahn von Länge k hat und sonst nur Bahnen der Länge 1.

Man notiert einen solchen Zykel dann (wenn die nichttriviale Bahn aus den Elementen $x_1, \ldots, x_k$ in der eben nahegelegten Reihenfolge besteht) als

$$\sigma = (x_1 \ x_2 \ \ldots \ x_k).$$

Die Identität nennen wir den 1-Zykel.

Die Zykelzerlegung von M unter H zeigt, dass sich σ als Produkt von paarweise kommutierenden Zykeln schreiben lässt. Dabei braucht man soviele Faktoren, wie es Bahnen der Länge > 1 gibt. Zwei Elemente aus der S_n sind genau dann zueinander konjugiert, wenn die Typen ihrer Zykelzerlegungen (also die Kardinalitäten ihrer Bahnen) übereinstimmen.

Da jeder k-Zykel sich als Produkt von $k-1$ Transpositionen schreiben lässt, sehen wir wieder wie in 1.1.4, dass S_n von den Transpositionen erzeugt wird. (NB: Als Gruppenerzeugnis stimmt das auch für $n = 1$.)

Definition 1.5.9 Signum / Alternierende Gruppe

Auf der symmetrischen Gruppe S_n gibt es die *Signum*sabbildung

$$\text{sign} : S_n \to \{\pm 1\},\ \sigma \mapsto \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Man rechnet leicht nach, dass das ein Gruppenhomomorphismus ist, der für $n \geq 2$ sogar surjektiv ist. Wenn σ ein Produkt von d Transpositionen ist, dann gilt $\text{sign}(\sigma) = (-1)^d$.

Der Kern davon heißt die *alternierende Gruppe* A_n. Für $n \geq 2$ ist das eine Untergruppe vom Index 2 in S_n.

Bemerkung 1.5.10 Erzeuger von A_n

Induktiv sieht man, dass A_n von 3-Zykeln erzeugt wird:

Für $n = 1$ oder 2 ist das klar, denn A_1 und A_2 bestehen beide nur aus der Identität. Auch für $n = 3$ ist das klar, denn

$$A_3 = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

wird vom 3-Zykel $(1\ 2\ 3)$ erzeugt.

Schließlich lässt eine Permutation $\sigma \in A_{n+1}$ entweder die Zahl $n + 1$ fest und kann daher wie ein Element von S_n behandelt werden, oder sie tut das nicht. Dann sei $r \leq n$ eine von $\sigma(n+1)$ verschiedene Zahl. Das definiert einen Dreizykel

$$\zeta = (\sigma(n + 1)\ n + 1\ r) \in A_{n+1}.$$

Es folgt, dass $\zeta \circ \sigma$ das Element $n + 1$ fixiert und daher nach Induktionsvoraussetzung ein Produkt von 3-Zykeln ist. Das gilt dann auch für

$$\sigma = \zeta \circ \zeta \circ (\zeta \circ \sigma).$$

1.6 Aufbau des Zahlensystems I

Wir wollen nun noch kurz dokumentieren, wie die Konstruktion der ganzen Zahlen aus den natürlichen im Kontext der allgemeinen Strukturtheorie zu sehen ist. Fangen wir also mit diesen an.

Bemerkung 1.6.1 Natürliche Zahlen

Die natürlichen Zahlen $\mathbb{N} := \{1, 2, 3, \dots\}$ werden als bekannt vorausgesetzt[4], und natürlich auch, wie man sie addiert und multipliziert.

[4]Laut Leopold Kronecker (1823-1891) wurden sie vom lieben Gott gemacht, der Rest ist Menschenwerk.

Addition und Multiplikation sind kommutativ und assoziativ, und sie erfüllen das Distributivgesetz.

Weiter gibt es eine Anordnung:

$$\forall m, n \in \mathbb{N} : [m > n :\iff \exists k \in \mathbb{N} : k + n = m].$$

Beachten Sie, dass 0 hier keine natürliche Zahl ist – das ist für die elementare Zahlentheorie der richtige Standpunkt. In Mitteleuropa war ja bis in die frühe Neuzeit die Null überhaupt nicht als Zahl akzeptiert.

Es gilt für natürliche Zahlen m, n, s, t :

$$[m < n \text{ und } s < t] \Rightarrow [m \cdot s < n \cdot t \text{ und } m + s < n + t].$$

Außerdem wissen wir schon, dass für $a, b, c \in \mathbb{N}$ gilt:

$$[a + b = c + b \Rightarrow a = c] \text{ und } [a \cdot b = c \cdot b \Rightarrow a = c].$$

Ärgerlicher Weise lässt sich nicht jede Subtraktion in $\mathbb{N}$ durchführen, oder – was dasselbe ist – nicht jede Gleichung der Form

$$a + x = b$$

mit $a, b \in \mathbb{N}$ durch ein $x \in \mathbb{N}$ lösen.

Dazu müssen wir $\mathbb{N}$ größer machen.

Bemerkung 1.6.2 Endlich annulliert

Zunächst nehmen wir künstlich ein Element 0 zu $\mathbb{N}$ dazu und definieren die Anordnung, Addition und Multiplikation auf $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ so, dass die alten Regeln für $\mathbb{N}$ erhalten bleiben und

$$\forall n \in \mathbb{N}_0 : 0 \leq n, 0 + n = n + 0 = n, 0 \cdot n = n \cdot 0 = 0.$$

Dann gelten Kommutativität, Assoziativität und das Distributivgesetz immer noch für Addition und Multiplikation.

Wir hätten auch direkt zur Konstruktion von $\mathbb{Z}$ schreiten und die 0 erst nachher darin entdecken können, aber so wird die Konstruktion etwas „natürlicher“. Ein allgemeines Verfahren hilft uns nun, aus $\mathbb{N}$ eine Gruppe zu gewinnen.

Konstruktion 1.6.3 Die Grothendieck[5]-Konstruktion

Es sei $(M, *)$ ein kommutatives Monoid mit Kürzungsregel, das heißt:

$$\forall a, b, c \in M : a * b = c * b \Rightarrow a = c.$$

[5]Alexander Grothendieck, geb. 1928

Dann gibt es eine Gruppe $(G, *)$, die $(M, *)$ als Untermonoid enthält und die folgende Eigenschaft hat:

Für jede Gruppe H und jeden Monoidhomomorphismus $\varphi : M \to H$ gibt es eine eindeutige Fortsetzung von φ nach G.

Beweis. Der Beweis besteht in der Konstruktion der passenden Gruppe.

Dazu betrachten wir auf der Menge $P := M \times M$ die folgende Äquivalenzrelation:

$$(m, s) \equiv (n, t) \iff m * t = n * s.$$

Dass dies eine Äquivalenzrelation ist, rechnet man leicht nach, braucht aber dazu die Kürzungsregel.

Für die Äquivalenzklasse von (m, s) schreiben wir intuitiver Weise $m - s$ (Minuend minus Subtrahend).

Es sei $G := P/\equiv$ die Menge aller Äquivalenzklassen. Wir wollen darauf eine Gruppenstruktur festlegen. Wir versuchen es mit dem aus der Schule bekannten Ansatz

$$(m - s) + (n - t) := (m * n) - (s * t).$$

Da hier mit den Vertretern der Klassen hantiert wird, müssen wir noch die Wohldefiniertheit nachweisen, also dass die Klasse auf der rechten Seite bei anderer Wahl der Vertreter links sich nicht ändert.

Seien also $(m, s) \equiv (m', s')$ und $(n, t) \equiv (n', t')$. Dann gilt

$$m * s' = m' * s \quad \text{und} \quad n * t' = n' * t.$$

Es folgt

$$m * s' * n * t' = m' * s * n' * t,$$

und damit, weil $*$ kommutativ ist,

$$(m * n, s * t) \equiv (m' * n', s' * t'),$$

wie gewünscht.

Diese Verknüpfung ist assoziativ (klar) und es gibt ein neutrales Element, nämlich (e_M, e_M). Außerdem ist zu $m - s$ die Klasse $s - m$ invers, denn

$$(m - s) + (s - m) = (m * s) - (s * m) = e_m - e_m.$$

Nun betrachten wir den Monoid-Homomorphismus

$$\Phi : M \to G, \quad m \mapsto m - e_m.$$

Dieser ist injektiv und verwirklicht daher unseren Wunsch, M als Untermonoid einer Gruppe zu erhalten.

Wenn $\varphi : M \to H$ ein Monoidhomomorphismus von M in eine beliebige Gruppe ist, so wird durch

$$(m - s) \mapsto \varphi(m)\varphi(s)^{-1}$$

eine Abbildung auf G definiert, die wegen der Kürzungsregel wohldefiniert ist und sich leicht als Gruppenhomomorphismus entpuppt. Da G von M erzeugt wird, ist diese Fortsetzung eindeutig. ◯

Folgerung 1.6.4 Ganze Zahlen

Es gibt einen kleinsten Ring $\mathbb{Z}$, der die natürlichen Zahlen enthält.

Beweis. Da $(\mathbb{N}_0, +)$ ein kommutatives Monoid mit Kürzungsregel ist, existiert eine (additiv geschriebene) Gruppe mit den eben bewiesenen Eigenschaften. Wir nennen sie hier $\mathbb{Z}$. Sie ist bis auf Isomorphismus eindeutig bestimmt und all ihre Elemente sind von der Gestalt $m - n,\ m, n \in \mathbb{N}_0$.

Auf $\mathbb{Z}$ definieren wir eine Multiplikation durch

$$(m - n)(k - l) := mk + nl - ml - nk.$$

Man überprüft leicht, dass dies wohldefiniert ist und alle Eigenschaften der Multiplikation von $\mathbb{N}$ erbt: Assoziativität, Kommutativität, Distributivgesetz, Nullteilerfreiheit. ◯

Allerdings lernen wir erst im nächsten Kapitel, was ein Ring ist, von daher vertiefen wir das jetzt nicht näher.

Wir halten noch folgendes fest:

Bemerkung 1.6.5 Mangelnde Kürzungseigenschaft

Wenn $(M, +)$ eine kommutative Halbgruppe ist, dann gibt es eine Gruppe G und einen Magmenhomomorphismus $\Phi : M \to G$, sodass für jeden Magmenhomomorphismus Ψ von M in eine beliebige Gruppe H genau ein Gruppenhomomorphismus $\tilde{\Psi} : G \to H$ existiert mit

$$\Psi = \tilde{\Psi} \circ \Phi.$$

Denn:

Im Gegensatz zu 1.6.3 fehlt uns hier die Kürzungsregel. Also können wir uns nicht sicher sein, dass wir wie eben eine Äquivalenzrelation auf $M \times M$ bekommen.

Wir entschärfen die Bedingung unserer Relation zu

$$(m, s) \equiv (n, t) \iff \exists r \in M :\ r + m + t = r + n + s.$$

Das ist tatsächlich wieder eine Äquivalenzrelation, und der Rest geht durch wie gehabt, wenn wir die Inklusion von vorhin durch die Abbildung

$$\Phi(m) := [(m + m, m)]$$

ersetzen. Insbesondere trägt dies der Tatsache Rechnung, dass wir kein neutrales Element vorausgesetzt haben.

Allerdings kann es uns jetzt passieren, dass G trivial ist, obwohl das für M nicht gilt.

Beispiel: $M = (\mathbb{Z}, \cdot)$.

Kapitel 2

Ringe und Moduln

In diesem Kapitel soll nur sehr kurz erläutert werden, was ein Ring ist. Wichtige Einsichten struktureller Art heben wir für später auf.

2.1 Ringe

Definition 2.1.1 Ringe

Ein *Ring* ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, sodass $(R,+)$ eine abelsche Gruppe ist (das Neutralelement heiße 0), und weiterhin $\cdot$ assoziativ ist, ein neutrales Element besitzt (das 1 heiße) und die Distributivgesetze erfüllt sind:

$$\forall a,b,c,d \in R : (a+b)\cdot c = ac + bc \quad \text{und} \quad a\cdot(c+d) = ac + ad.$$

Hierbei benutzen wir die Konvention „Punkt vor Strich“.

Ein Ring heißt *kommutativ*, wenn seine Multiplikation kommutativ ist.

Es gibt auch Quellen, in denen Ringe ohne 1 studiert werden. Wir werden uns den Luxus eines Einselements immer zubilligen, auch wenn die andere Sichtweise durchaus gerechtfertigt ist.

Beispiel 2.1.2 ein paar Ringe

a) Die ganzen Zahlen $\mathbb{Z}$ sind (mit der üblichen Addition und Multiplikation) ein Ring. Genauso auch $\mathbb{Q}$ und $\mathbb{R}$.

b) Für eine abelsche Gruppe $(A,+)$ ist $\mathrm{End}(A)$ ein Ring, wenn wir Addition und Multiplikation wie folgt festlegen:

$$\forall \varphi,\psi \in \mathrm{End}(A) : (\varphi+\psi)(a) := \varphi(a)+\psi(a), \quad (\varphi\cdot\psi)(a) := \varphi(\psi(a)).$$

Damit die Addition überhaupt wieder einen Endomorphismus ausspuckt, muss man die Kommutativität von A voraussetzen.

Zum Beispiel ist $\mathbb{Z} = \mathrm{End}_{\mathrm{Gruppen}}(\mathbb{Z})$, denn ein Endomorphismus ist eindeutig durch das Bild der 1 bestimmt, und das kann beliebig vorgegeben werden.

c) Die Menge der Endomorphismen von $\mathbb{Z}/n\mathbb{Z}$ hatten wir nach dem Homomorphiesatz auch mit $\mathbb{Z}/n\mathbb{Z}$ identifiziert, indem wir Φ auf $\Phi(1)$ abgebildet haben. Die Multiplikation, die durch die Komposition auf der Menge der Endomorphismen gegeben ist, wird dabei zu der Vorschrift, die zwei Restklassen $a + n\mathbb{Z}$ und $b + n\mathbb{Z}$ die Klasse von ab zuordnet. Wir müssen hier nicht mehr nachrechnen, dass das wohldefiniert ist!

d) Der Endomorphismenring eines Vektorraums ist auch immer ein Ring, und meistens kein kommutativer. Sonst wäre ja die Quantenmechanik falsch...

Definition 2.1.3 Ringhomomorphismus

Es seien R, S zwei Ringe. Ein *Homomorphismus* zwischen R und S ist eine Abbildung $\Phi : R \to S$, die sowohl für die Addition als auch für die Multiplikation ein Magmenhomomorphismus ist und außerdem noch

$$\Phi(1_R) = 1_S$$

erfüllt.

Als *Kern eines Homomorphismus* zwischen Ringen bezeichnen wir das Urbild der 0. Es ist eine Untergruppe von R, die unter Multiplikation mit beliebigen Elementen aus R abgeschlossen ist.

Beispiel 2.1.4 Cayley die dritte

Zum Beispiel die Abbildung $\{0\} \to \mathbb{Z}, \Phi(0) = 0$, ist zwar magmatisch, aber sie bildet das Einselement von $\{0\}$ nicht auf das von $\mathbb{Z}$ ab, ist also kein Ringhomomorphismus.

Hingegen ist für $n \in \mathbb{N}$ die kanonische Projektion (siehe 1.4.1)

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = \mathrm{End}(\mathbb{Z}/n\mathbb{Z})$$

ein Ringhomomorphismus.

Weiter erhalten wir für jeden Ring R einen Ringhomomorphismus

$$\lambda : R \to \mathrm{End}_{\mathrm{Gruppen}}((R, +)), \quad r \mapsto \lambda_r = [x \mapsto rx].$$

Er ist injektiv, weil R ein Einselement hat, und man aus der Abbildung λ_r die Zahl $r = \lambda_r(1)$ zurückerhält.

Man vergleiche dies wieder mit 1.5.3, wo ähnliches für Gruppen passierte.

Definition 2.1.5 Einheitengruppe

Die *Einheiten* eines Ringes R sind die Elemente $r \in R$, für die ein $\tilde{r} \in R$ existiert mit

$$r\tilde{r} = \tilde{r}r = 1_R.$$

Zum Beispiel ist 1_R selbst eine Einheit. Das Element $\tilde{r}$ ist aufgrund dieser Beziehung eindeutig durch r festgelegt und wir schreiben in Zukunft r^{-1} dafür.

Die Einheiten in R bilden bezüglich der Multiplikation eine Gruppe, die wir mit $R^\times$ notieren.

Als **Beispiel** betrachten wir den Ring $\mathbb{Z}/N\mathbb{Z}$ für $N \in \mathbb{N}$. Hier ist die Klasse $a+N\mathbb{Z}$ genau dann eine Einheit, wenn ein $b \in \mathbb{Z}$ existiert mit $ab+N\mathbb{Z} = 1+N\mathbb{Z}$. Also:

$$a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times \iff \exists b, l \in \mathbb{Z} : ab + Nl = 1.$$

Wenn $d \in \mathbb{N}$ ein gemeinsamer Teiler von a und N ist, muss er dann auch 1 teilen, also gilt (mit ggT für den größten gemeinsamen Teiler):

$$a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times \Rightarrow \mathrm{ggT}(a, N) = 1.$$

Wenn umgekehrt der ggT von a und N 1 ist, dann betrachten wir die Gruppe

$$\{ab + Nl \mid b, l \in \mathbb{Z}\} \leq \mathbb{Z}.$$

Wegen 1.2.5 ist diese Gruppe von der Gestalt $g\mathbb{Z}$ für ein $g \in \mathbb{N}$, und dieses g muss ein gemeinsamer Teiler von a und N sein, also 1. Andererseits ist daher 1 von der Gestalt $ab + Nl$, also $a + N\mathbb{Z}$ eine Einheit in $\mathbb{Z}/N\mathbb{Z}$.

Wir halten fest:

$$a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times \iff \mathrm{ggT}(a, N) = 1.$$

Bemerkung 2.1.6 Homomorphismus und Einheiten

Es sei $\Phi : R \to S$ ein Ringhomomorphismus.

Dann gilt $\Phi(R^\times) \subseteq S^\times$, denn aus $r\tilde{r} = \tilde{r}r = 1_R$ wird die Gleichung

$$\Phi(r)\Phi(\tilde{r}) = \Phi(\tilde{r})\Phi(r) = \Phi(1_R) = 1_S.$$

An der letzten Stelle wird die Zusatzbedingung an Ringhomomorphismen wirksam.

Insbesondere vermittelt Φ also einen Gruppenhomomorphismus von $R^\times$ nach $S^\times$.

Genauso wie Untergrupen gibt es auch Teilringe, und es ist eigentlich relativ naheliegend, wie dieser Begriff zu definieren ist.

Definition 2.1.7 Teilringe

Es sei R ein Ring.

Ein *Teilring* von R ist eine Teilmenge $T \subseteq R$, die bezüglich der Addition eine Untergruppe und bezüglich der Multiplikation ein Untermonoid von R ist. Die Eins von R soll also auch darin liegen.

Definition 2.1.8 Nullteiler, Körper

Es sei R ein Ring.

a) Ein Element $a \in R$ heißt ein *Nullteiler*, wenn es ein $b \in R, b \neq 0$, gibt, für das $ab = 0$ oder $ba = 0$ gilt.

R heißt *nullteilerfrei*, wenn 0 der einzige Nullteiler in R ist. Das erzwingt unter anderem $R \neq \{0\}$, denn im Nullring ist 0 kein Nullteiler. Außerdem kann man bei Nullteilerfreiheit aus einer Gleichung wie $xy = xz$ immer folgern, dass $x = 0$ oder $y = z$ gilt, man erhält also eine Kürzungsregel.

b) R heißt ein *Integritätsbereich*, wenn R kommutativ und nullteilerfrei ist. Da R also wie gesagt nicht nur aus der Null besteht, gilt insbesondere $0_R \neq 1_R$.

c) R heißt ein *Körper*, wenn R kommutativ ist, $0 \neq 1$ gilt und jedes von Null verschiedene Element eine Einheit ist: $R^\times = R \setminus \{0\}$.

Ein Körper ist insbesondere ein Integritätsbereich, und das gilt dann auch für jeden Teilring.

Das Beispiel in der Definition 2.1.5 zeigt, dass $\mathbb{Z}/N\mathbb{Z}$ genau dann ein Körper ist, wenn es sich bei N um eine Primzahl handelt. Denn genau dann sind alle Zahlen $1, 2, \ldots, N-1$ zu N teilerfremd.

Beispiel 2.1.9 Es gibt Ringe mit Nullteilern

Der Ring $\mathbb{Z}/4\mathbb{Z}$ enthält den Nullteiler $2 + 4\mathbb{Z}$, ist also nicht nullteilerfrei.

Auch der Ring der stetigen Funktionen auf dem Intervall $[0, 1]$ ist nicht nullteilerfrei, denn es gibt darin Funktionen f, g, die nicht 0 sind, und von denen die eine auf $[0, \frac{1}{2}]$ verschwindet, die andere auf $[\frac{1}{2}, 1]$. Ihr Produkt ist also 0.

$\mathbb{Q}$ und $\mathbb{R}$ hingegen sind nullteilerfrei, sogar Körper.

Hilfssatz 2.1.10 Charakteristik

Es sei R ein Ring. Dann gibt es genau einen Ringhomomorphismus von $\mathbb{Z}$ nach R.

Es sei $n \in \mathbb{N}_0$ der nichtnegative Erzeuger des Kerns. Dann heißt n die Charakteristik *von R, in Zeichen* $\mathrm{char}(R)$.

Die Charakteristik eines nullteilerfreien Rings R ist entweder 0 oder eine Primzahl[1].

Beweis. Der Homomorphismus muss 1 auf 1_R abbilden und ist dadurch eindeutig festgelegt, denn 1 erzeugt die additive Gruppe von $\mathbb{Z}$. Man rechnet leicht nach, dass der entsprechende Gruppenhomomorphismus

$$\Phi : \mathbb{Z} \to R,\ k \mapsto k \cdot 1_R$$

tatsächlich ein Ringhomomorphismus ist. Zum Beispiel gilt für $k, l \geq 0$:

$$\begin{aligned} \Phi(k) &= \textstyle\sum_{i=1}^{k} 1_R, \\ \Phi(l) &= \textstyle\sum_{j=1}^{l} 1_R, \\ \Phi(kl) &= \textstyle\sum_{h=1}^{kl} 1_R \cdot 1_R \overset{(*)}{=} (\sum_{i=1}^{k} 1_R) \cdot (\sum_{j=1}^{l} 1_R) = \Phi(k)\Phi(l). \end{aligned}$$

Bei $(*)$ nutzen wir das Distributivgesetz aus.

Nun sei R ein Ring mit Charakteristik $n > 1$. Wenn n eine Zerlegung $n = ab$ in zwei natürliche Zahlen $1 < a, b < n$ hat, dann gilt $\Phi(a), \Phi(b) \neq 0$.

Andererseits gilt

$$\Phi(a) \cdot \Phi(b) = \Phi(n) = 0,$$

und daher ist R unter der gemachten Voraussetzung nicht nullteilerfrei.

Der Vollständigkeit halber sei noch angemerkt, dass der einzige Ring mit Charakteristik 1 der Ring ist, bei dem $1 = 0$ gilt, was erzwingt, dass 0 das einzige Element ist. ◯

Definition 2.1.11 Ideale

Es sei R ein Ring.

a) Ein *Ideal* in R ist eine Teilmenge $I \subseteq R$, die bezüglich der Addition eine Untergruppe ist und die folgende Eigenschaft hat:

$$\forall x \in I,\ r \in R : \quad xr \in I \text{ und } rx \in I.$$

Wie vorhin gesehen sind Kerne von Ringhomomorphismen immer Ideale.

Dass die Umkehrung auch gilt liegt an der folgenden Konstruktion.

b) Es sei $I \subseteq R$ ein Ideal. Da die Addition kommutativ ist, ist dann R/I eine kommutative Gruppe bezüglich der Addition

$$(r + I) + (\tilde{r} + I) = (r + \tilde{r}) + I.$$

[1] Eine Primzahl ist eine natürliche Zahl $p > 1$, die sich nicht als Produkt von zwei kleineren Zahlen schreiben lässt.

Wie man leicht nachrechnet, definiert auch die Vorschrift

$$(r + I) \cdot (\tilde{r} + I) := (r \cdot \tilde{r}) + I$$

eine assoziative Verknüpfung mit neutralem Element $1 + I$. Für diese beiden Verknüpfungen auf R/I gelten dann auch die Distributivgesetze, also wird R/I auf diese Weise zu einem Ring: Der *Faktorring von R modulo I*.

Das verallgemeinert die Ringeigenschaft von $\mathbb{Z}/n\mathbb{Z}$ aus 2.1.2.

Die kanonische Projektion $\pi : R \to R/I$ ist sogar ein surjektiver Ringhomomorphismus.

Bemerkung 2.1.12 Homomorphiesatz

Für Ringhomomorphismen gilt nun ähnlich wie in der Situation von Gruppen ein Homomorphiesatz. Wir halten insbesondere die folgende Aussage fest:

Wenn $\Phi : R \to S$ ein Ringhomomorphismus ist und $I \subseteq \text{Kern}(\Phi)$ ein Ideal in R, dann *faktorisiert* Φ über die kanonische Projektion von R nach R/I, das heißt: Es gibt einen Ringhomomorphismus $\tilde{\Phi} : R/I \to S$, sodass $\Phi = \tilde{\Phi} \circ \pi$.

$\tilde{\Phi}$ ist hierdurch eindeutig festgelegt, es gilt nämlich wegen der definierenden Gleichheit: $\forall r \in R : \tilde{\Phi}(r + I) = \Phi(r)$.

Wir halten an dieser Stelle ein interessantes Ergebnis fest, das wir in 3.1.19 noch mit etwas mehr Leben füllen werden.

Satz 2.1.13 Chinesischer Restsatz

Es seien $M, N \in \mathbb{N}$ natürliche Zahlen, die außer 1 keinen gemeinsamen Teiler haben. Dann gibt es einen Isomorphismus

$$\mathbb{Z}/(MN\mathbb{Z}) \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}Z.$$

Hierbei wird rechter Hand komponentenweise addiert und multipliziert.

Beweis. Wir verwenden den einzig möglichen Ringhomomorphismus

$$\Psi : \mathbb{Z} \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, \quad k \mapsto (k + M\mathbb{Z},\ k + N\mathbb{Z}).$$

Da M und N keinen gemeinsamen Teiler außer 1 haben, gilt nach 1.2.8c), dass 1 sich mit geeigneten $x, y \in \mathbb{Z}$ schreiben lässt als

$$1 = xM + yN.$$

Daher ist $1 \equiv yN \pmod{M\mathbb{Z}}$ und $1 \equiv xM \pmod{N\mathbb{Z}}$. Für alle $a, b \in \mathbb{Z}$ gilt daher

$$\Psi(yNa + xMb) = (a + M\mathbb{Z}, b + N\mathbb{Z}),$$

und folglich ist Ψ surjektiv.

Der Kern von Ψ muss nach dem Homomorphiesatz eine Untergruppe von Index MN in $\mathbb{Z}$ sein, aber hier gibt es nur die Untergruppe $MN\mathbb{Z}$. Wieder der Homomorphiesatz liefert die Behauptung. ◯

In der Situation des Satzes gibt es also für gegebene Zahlen $a, b \in \mathbb{Z}$ immer ein $x \in \mathbb{Z}$, sodass M ein Teiler von $x-a$ und N ein Teiler von $x-b$ ist. Auch dies wird oft der chinesische Restsatz genannt.

Außerdem sehen wir am Beweis, dass $M\mathbb{Z} \cap N\mathbb{Z}$, was ja der Kern von Ψ ist, gleich $MN\mathbb{Z}$ ist andererseits liegen in dem Durchschnitt alle gemeinsamen Vielfachen von M und N. Das zeigt, dass MN das kleinste gemeinsame Vielfache von M und N ist, wenn diese teilerfremd sind.

Zu unserem Satz haben wir noch ein algebraisches Pendant:

Bemerkung 2.1.14 Algebraische Version

Es seien R ein kommutativer Ring und I, J zwei Ideale in R, sodass $I + J = R$ gilt. Dann gibt es einen Isomorphismus

$$\Phi : R/(I \cap J) \to R/I \times R/J,$$

wobei rechter Hand ein Ring steht, indem wir komponentenweise addieren und multiplizieren.

Beweis. Der Ansatz geht über die naheliegende Abbildung

$$\hat{\Psi} : R \to R/I \times R/J,\ r \mapsto (r + I, r + J).$$

Diese Abbildung ist surjektiv, denn es gibt $i_0 \in I,\ j_0 \in J$ mit $1 = i_0 + j_0$, und damit gilt für alle $a, b \in R$:

$$a + I = (i_0 + j_0)a + I = j_0 a + I = (j_0 a + i_0 b) + I, \quad b + J = \ldots = (j_0 a + i_0 b) + J,$$

also $(a + I, b + J) = \hat{\Psi}(j_0 a + i_0 b)$.

Der Kern ist gerade $I \cap J$, und dann liefert der Homomorphiesatz was wir brauchen. ◯

2.2 Moduln

Definition 2.2.1 R-Modul

Es sei R ein Ring. Ein *R-Modul* (oder auch *Modul über R*) ist eine abelsche Gruppe M (mit zumeist additiv geschriebener Verknüpfung) zusammen mit einer Abbildung

$$\cdot : R \times M \to M,$$

für die die folgenden Bedingungen erfüllt sind:

$$\begin{aligned} \forall r,s \in R, \forall m \in M: \quad (r+s)\cdot m &= r\cdot m + s\cdot m \\ \forall r \in R, \forall m,n \in M: \quad r\cdot(m+n) &= r\cdot m + r\cdot n \\ \forall r,s \in R, \forall m \in M: \quad (rs)\cdot m &= r\cdot(s\cdot m) \\ \forall m \in M: \quad 1\cdot m &= m. \end{aligned}$$

Das sind dieselben Bedingungen, wie man sie von Vektorräumen her kennt, aber jetzt ist der Skalarbereich ein Ring. Wieder gilt $0_R \cdot m = 0_M$ für alle $m \in M$, aber im allgemeinen kann man aus $m \neq 0_M, r\cdot m = 0_M$ nicht mehr folgern, dass $r = 0_R$ gilt.

Etwas präziser sollten wir unsere Moduln lieber Linksmoduln nennen, für einen Rechtsmodul würde man $(rs)m = s(rm)$ fordern (und am besten die Skalare rechts hinschreiben...).

Beispiel 2.2.2 Schon gesehen

a) Es seien R ein Ring und $I \subseteq R$ ein Ideal. Dann wird I mit der auf $R \times I$ eingeschränkten Multiplikation ein R-Modul.

b) Die Abbildungen von einer Menge M nach R sind ein R-Modul mit der naheliegenden Addition und Multiplikation

$$(f+g)(m) := f(m) + g(m), \quad (r\cdot f)(m) := r\cdot(f(m)).$$

Ein Untermodul darin ist zum Beispiel die Menge aller Abbildungen mit endlichem Träger, die also nur an endlich vielen Stellen einen von 0 verschiedenen Wert annehmen.

Wir schreiben dafür $\mathrm{Abb}(M,R)_0$.

c) Ist $R \subseteq S$ ein Teilring von S, so wird S selbst auch zu einem R-Modul. Zum Beispiel ist $\mathbb{Q}$ ein $\mathbb{Z}$-Modul...

Bemerkung 2.2.3 alternative Beschreibung

So wie eine Gruppenoperation von G auf M eigentlich nichts anderes ist als ein Homomorphismus von G nach Sym_M, kann man auch Moduln anders beschreiben.

In der Tat: Wenn M ein Modul über einem Ring R ist, dann wird durch

$$\rho : R \to \mathrm{End}_{\mathrm{Gruppen}}(M), \ \rho(r)(m) := r\cdot m,$$

ein Ringhomomorphismus von R in den Endomorphismenring der abelschen Gruppe M gegeben.

Ist umgekehrt $\rho : R \to \mathrm{End}(M)$ ein solcher Ringhomomorphismus, so wird durch

$$\mu : R \times M \to M, \quad (r,m) \mapsto \rho(r)(m) =: r\cdot m,$$

eine Modulstruktur auf M festgelegt.

Insbesondere sehen wir aus 2.1.10, dass jede abelsche Gruppe auf genau eine Art zu einem $\mathbb{Z}$-Modul gemacht werden kann.

Bemerkung 2.2.4 Untermoduln, Modulerzeugnis

a) Es seien M ein R-Modul und $U \subseteq M$ eine Teilmenge. Dann heißt U ein *Untermodul* von M, wenn U eine additive Untergruppe ist und unter der auf M gegebenen skalaren Multiplikation mit Elementen aus R invariant ist:

$$U \leq M \quad \text{und} \quad \forall r \in R, u \in U : ru \in U.$$

b) Der Durchschnitt aller Untermoduln, die eine gegebene Teilmenge T von M enthalten, ist wieder ein Untermodul, und heißt der von T erzeugte Untermodul. Man schreibt dafür

$$\langle T \rangle_{R-\text{Moduln}} = \{\sum_{i=1}^{d} r_i t_i \mid d \in \mathbb{N}_0, r_i \in R, t_i \in T\}.$$

c) Für kommutative Ringe R sind die Untermoduln von R genau die Ideale in R.

Bemerkung 2.2.5 Faktormoduln

Es ist naheliegend, wie der Begriff eines R-Modulhomomorphismus definiert werden muss: Sind M, N zwei R-moduln, so ist das eine Abbildung $\Phi : M \to N$, sodass für alle $m, m' \in M$ und für alle $r \in R$ gilt:

$$\Phi(m + m') = \Phi(m) + \Phi(m') \quad \text{und} \quad \Phi(rm) = r\Phi(m).$$

Wie in der Linearen Algebra für Vektorräume kann man auch hier Faktormoduln nach Untermoduln einführen. Es gilt derselbe Homomorphiesatz wie in der Linearen Algebra und wie wir ihn prinzipiell auch schon für Gruppen und Ringe gesehen haben.

Das meiste aus der Linearen Algebra sollte man allerdings nicht unbesehen in die Welt der Moduln übernehmen. Insbesondere gibt es für die meisten Moduln keine Basis – wie wir noch systematischer untersuchen werden.

2.3 Monoidringe, Algebren

Hier wollen wir ein weitverbreitetes Verfahren studieren, wie man mit gewissen Daten neue Ringe konstruieren kann. Wir verallgemeinern dabei (und wiederholen auch) die Konstruktion des Polynomrings.

Konstruktion 2.3.1 Monoidring

Es sei R ein kommutativer Ring und $(M, \diamond)$ ein Monoid. Weiter sei $A := \mathrm{Abb}(M, R)_0$ die Menge aller Abbildungen von M nach R, die nur bei endlich vielen Stellen einen Wert $\neq 0$ annehmen. Wie vorhin gesehen (2.2.2 b)), ist diese Menge ein R-Modul.

Wir definieren auf A eine Multiplikation, indem wir für zwei Abbildungen $f, g \in A$ ein Produkt $f * g$ definieren durch Angabe der Funktionswerte:

$$\forall x \in M : \ (f * g)(x) := \sum_{y,z \in M : y \diamond z = x} f(y) \cdot g(z).$$

Es ist klar, dass diese Summe in Wirklichkeit endlich ist und auch nur für endlich viele x einen von Null verschiedenen Wert ergeben kann.

Man rechnet leicht nach, dass A mit argumentweiser Addition und dem hier eingeführten Produkt (auch *Faltung* genannt) ein Ring wird. Er heißt der *Monoidring* zu M über R und wird mit $R[M]$ notiert. Sein Einselement ist die Abbildung, die beim neutralen Element von M den Wert 1 annimmt und sonst verschwindet.

Für $m \in M$ sei $\delta_m \in A$ die Abbildung, die bei m den Wert 1 und sonst den Wert 0 hat.

Jedes $f \in A$ lässt sich schreiben als

$$f = \sum_{m \in M} f(m) \delta_m,$$

und diese Schreibweise ist die einzige Möglichkeit, f als R-Linearkombination der Funktionen δ_m zu schreiben.

Das Produkt von f und g ist dann

$$(\sum_{m \in M} f(m)\delta_m) * (\sum_{n \in M} g(n)\delta_n) = \sum_{m,n \in M} f(m) \cdot g(n) \delta_{m \diamond n}.$$

Speziell finden wir

$$\delta_m * \delta_n = \delta_{m \diamond n}.$$

Insbesondere können wir die Monoidverknüpfung auf M aus dem Monoidring rekonstruieren.

Beispiel 2.3.2 Polynomring, Gruppenring

Es sei R ein kommutativer Ring.

a) Der *Polynomring in einer Variablen* über R ist gerade der Monoidring zum Monoid $(\mathbb{N}_0, +)$. Anstelle von δ_n schreibt man hier allerdings X^n und nennt X

die Variable. Und die Multiplikation schreibt man mit einem Punkt anstelle eines Sternchen.

Wir schreiben also in Zukunft:

$$R[X] = \{\sum_{i=0}^{d} a_i X^i \mid d \in \mathbb{N}_0, a_i \in R\}.$$

Der *Grad* eines Polynoms $f = \sum a_i X^i \neq 0$ ist definiert als $\deg(f) = \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}$. Der Grad des Nullpolynoms wird auf $-\infty$ normiert.

Der Koeffizient $a_{\deg(f)}$ heißt der *Leitkoeffizient* von f.

b) Allgemeiner ist der Polynomring in endlich vielen Variablen $X_1, \ldots, X_k$ auch der Monoidring über dem Monoid $\mathbb{N}_0^k$.

c) Ist $(M, \diamond)$ eine Gruppe, so spricht man auch vom *Gruppenring* anstelle des Monoidrings. Dann ist M vermöge $m \mapsto \delta_m$ isomorph zu einer Untergruppe von $R[M]^\times$.

Faul veranlagte Leute schreiben statt $\sum_{m\in M} r_m \delta_m$ auch einfach $\sum_{m\in M} r_m m$.

Hilfssatz 2.3.3 Regeln für das Rechnen mit dem Grad

Es seien $f, g \in R[X]$ Polynome. Dann gelten die folgenden Regeln für die Grade:

- $\deg(f+g) \leq \max(\deg(f), \deg(g))$.
- $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.
- $\deg(f \cdot g) = \deg(f) + \deg(g)$, *falls R nullteilerfrei ist.*

Beweis. Es sei $m := \max(\deg(f), \deg(g))$. Dann lassen sich f und g schreiben als

$$f = \sum_{i=0}^{m} r_i X^i, \quad g = \sum_{i=0}^{m} s_i X^i,$$

und damit ist

$$f + g = \sum_{i=0}^{m} (r_i + s_i) X^i,$$

und man braucht keinen Summationsindex größer als m. Das zeigt die erste Ungleichung.

Nun seien $d = \deg(f)$, $e = \deg(g)$. Weiter schreiben wir

$$f = \sum_{i=0}^{d} r_i X^i, \quad g = \sum_{i=0}^{e} s_i X^i,$$

wobei r_d und s_e beide nicht Null sind. Dann ist

$$f \cdot g = \sum_{k=0}^{d+e} \left(\sum_{i=0}^{k} r_i s_{k-i} \right) X^k,$$

und das zeigt, dass $\deg(f \cdot g) \leq d + e$.

Der Koeffizient, der in fg vor X^{d+e} steht, ist $r_d s_e$. Im Falle der Nullteilerfreiheit von R ist dieses Produkt nicht 0. ◯

Hilfssatz 2.3.4 Polynomdivision

Es sei K ein Körper. Dann gelten:

a) Der Polynomring $K[X]$ ist nullteilerfrei.

b) Sind $f, g \in K[X]$ zwei Polynome und $g \neq 0$, so gibt es Polynome $h, r \in K[X]$, sodass $f = gh + r$ gilt und $\deg(r) < \deg(g)$.

Beweis.

a) Die Nullteilerfreiheit von $K[X]$ folgt aus der Additivität des Grads bei der Multiplikation zweier Polynome.

b) Wenn der Grad von f kleiner ist als der von g, so setzen wir $h = 0$ und $r = f$.

Ansonsten argumentieren wir per Induktion über den Grad von f. Ist dieser nämlich mindestens so groß wie der von g, so bilden wir für geeignete Konstanten $c \in K^\times$ und $d \in \mathbb{N}_0$ das Polynom

$$\tilde{f} = f - cX^d g,$$

sodass dessen Grad kleiner ist als der von f. Induktiv gibt es $\tilde{h}$ und $\tilde{r}$, sodass $\tilde{f} - \tilde{h}g = \tilde{r}$, aber dann ist auch

$$f - (\tilde{h} + cX^d)g = \tilde{r} =: r.$$

Das beendet den Beweis. ◯

Bemerkung 2.3.5 Division mit Rest

In der Situation von gerade eben sagt man auch wie in der Schule, dass f bei Division durch g den Rest r lässt. Wir werden das später im zahlentheoretischen Kontext noch einmal beleuchten.

Definition 2.3.6 Algebren

Es sei R ein Ring. Eine *R-Algebra* ist ein Ring A zusammen mit einem Ringhomomorphismus $\sigma : R \to A$, sodass für alle $r \in R, a \in A$ die Gleichheit

$$\sigma(r) \cdot a = a \cdot \sigma(r)$$

gilt. Man sagt dann auch, dass $\sigma(r)$ mit a *kommutiert*.

Die Abbildung σ wird der *Strukturmorphismus* von A genannt.

Die Vorschrift $(r, a) \mapsto \sigma(r) \cdot a$ macht dann aus A einen R-Modul, und die Multiplikation in A ist R-bilinear.

Insbesondere gilt auch für alle $r, s \in R$:

$$\sigma(r)\sigma(s) = \sigma(s)\sigma(r).$$

Das heißt, dass die so genannten *Kommutatoren* $rs - sr$, $r, s \in R$, von σ annulliert werden. Das von ihnen erzeugte Ideal ist also im Kern von σ, und der Faktorring nach dem Kern muss daher kommutativ sein.

Demnach ist es für viele Zwecke angebracht, Algebren nur über kommutativen Ringen zu betrachten.

Beispiel 2.3.7 Zentrum...

a) Es sei A ein beliebiger Ring. Mit

$$Z(A) := \{r \in A \mid \forall a \in A : ra = ar\}$$

bezeichnet man das *Zentrum* von A. $Z(A)$ ist ein Teilring von A, und es ist der größte Teilring R, für den A durch die Inklusion von R nach A zu einer R-Algebra gemacht wird.

b) Für jeden kommutativen Ring R und jedes Monoid M ist $R[M]$ eine R-Algebra vermöge

$$\sigma : R \to R[M], \quad r \mapsto r\delta_e,$$

wobei $e \in M$ das neutrale Element ist.

c) Für jeden kommutativen Ring R und jede natürliche Zahl n erhält die Menge $R^{n\times n}$ der $n \times n$-Matrizen eine Struktur als R-Algebra, indem man Addition und Multiplikation so einführt wie in der Linearen Algebra.

Definition 2.3.8 R-Algebren-Homomorphismen

Es sei R ein (gerne kommutativer) Ring.

Ein *Homomorphismus zwischen zwei R-Algebren* A und B (mit Strukturmorphismen σ, τ) ist ein Ringhomomorphismus $\Phi : A \to B$, der die Strukturmorphismen respektiert, d.h.

$$\Phi \circ \sigma = \tau.$$

Er ist also gleichzeitig ein Ringhomomorphismus und ein R-Modulhomomorphismus.

Wir schreiben für die Menge aller dieser Homomorphismen

$$\mathrm{Hom}_{R-\mathrm{Alg}}(A, B).$$

Analog gibt es die Gruppe aller R-Algebren-Automorphismen

$$\mathrm{Aut}_{R-\mathrm{Alg}}(A) =: \mathrm{Aut}(A|R),$$

die *Automorphismen von A über R*.

Vorsicht: Häufig wird hierfür auch $\mathrm{Aut}(A/R)$ geschrieben. Das verkneife ich mir, da der schräge Strich zu gerne mit der Bildung des Faktormoduls verwechselt wird.

Beispiel 2.3.9 Zweierlei Realitäten

a) Es gibt genau zwei $\mathbb{R}$-Algebrenautomorphismen von $\mathbb{C}$, nämlich die Identität und die komplexe Konjugation.

b) Der einzige Endomorphismus von $\mathbb{R}$ als $\mathbb{Q}$-Algebra ist die Identität.

Denn: Sei σ so ein Automorphismus. Er ist die Identität auf $\mathbb{Q}$, da er die 1 festlässt und $\mathbb{Q}$-linear ist. Weiterhin bildet er positive Elemente auf positive Elemente ab, denn das sind genau die Elemente, aus denen in $\mathbb{R}$ eine Quadratwurzel gezogen werden kann, und das muss der Automorphismus respektieren. Das impliziert, dass der Automorphismus (der ja insbesondere additiv ist) die Anordnung auf $\mathbb{R}$ erhält:

$$\forall x, y \in \mathbb{R} : x < y \Rightarrow \sigma(x) < \sigma(y).$$

Nun seien $\alpha \in \mathbb{R}$ eine Zahl und

$$r_1 < r_2 < r_3 < \cdots < \alpha < \cdots < s_3 < s_2 < s_1$$

zwei rationale Folgen $(r_i), (s_i)$, die von unten beziehungsweise oben gegen α konvergieren.

Dann folgt

$$\forall i : r_i = \sigma(r_i) < \sigma(\alpha) < \sigma(s_i) = s_i,$$

und da α eindeutig durch diese Folgen charakterisiert ist (archimedisches Axiom!), folgt $\alpha = \sigma(\alpha)$.

c) Trotzdem gibt es überabzählbar viele Automorphismen von $\mathbb{C}$, aber bis auf besagte zwei aus Punkt a) machen die mit $\mathbb{R}$ nichts, was man sich vorstellen kann oder auch nur will.

Beispiel 2.3.10 Ein wichtiger Algebrenhomomorphismus

Es sei R ein kommutativer Ring und A eine R-Algebra. Für ein Polynom $f = \sum r_i X^i \in R[X]$ und festes $a \in A$ definieren wir

$$f(a) := \sum \sigma(r_i) a^i.$$

Dabei ist $a^0 = 1$ und rekursiv $a^{i+1} = a \cdot a^i$.

Dann ist die Abbildung

$$E_a : R[X] \longrightarrow A, \quad f \mapsto E_a(f) := f(a),$$

die *Einsetzabbildung bei* a. (Man nennt diese auch die Auswertungsabbildung.) E_a ist ein R-Algebrenhomomorphismus. Es gilt $E_a(1) = 1$, da $a^0 = 1$ gesetzt wurde. Weiter gilt für Polynome $f = \sum_{i=0}^m r_i X^i$, $g = \sum_{i=0}^m s_i X^i$:

$$\begin{aligned} E_a(f+g) &= \textstyle\sum_{i=0}^m (r_i + s_i) a^i = \sum_{i=0}^m r_i a^i + \sum_{i=0}^m s_i a^i \\ &= E_a(f) + E_a(g). \\ E_a(f \cdot g) &= \textstyle\sum_{k=0}^{2m} \sum_{i=0}^k (r_i \cdot s_{k-i}) a^k = \sum_{i=0}^m r_i a^i \cdot \sum_{i=0}^m s_i a^i \\ &= E_a(f) \cdot E_a(g). \end{aligned}$$

Dabei haben wir in der Notation (wie allseits üblich) den Strukturmorphismus σ unterdrückt und benutzen, dass die Elemente aus R mit allen Elementen aus A kommutieren: man braucht $a^i s_{k-i} = s_{k-i} a^i$ beim Umsortieren.

Das Bild von E_a wird meistens mit $R[a]$ bezeichnet. Es ist

$$R[a] = \{\sum_{i=0}^d r_i a^i \mid d \in \mathbb{N},\ r_0, \ldots, r_d \in R\}.$$

Dies ist ein kommutativer Teilring von A, und zwar die kleinste Unteralgebra (klar, wie das zu definieren ist, oder?), die a enthält.

Analog schreibt man $R[a_1, \ldots, a_n]$ für die kleinste Unteralgebra von A, die $a_1, \ldots, a_n$ enthält. Vorsicht: Dies ist meistens (mangels Kommutativität) kein Bild eines Polynomrings (in mehreren Variablen) mehr.

Beispiel 2.3.11 Nullstellen eines Polynoms

Es seien K ein Körper und $f \in K[X]$ en Polynom vom Grad $d > 0$.

Ein Element $a \in K$ heißt eine *Nullstelle* von f, wenn $f(a) = 0$.

2.3.4 liefert uns ein Polynom $h \in K[X]$, sodass der Grad von $f - (X - a)h$ kleiner ist als der von $X - a$, also kleiner als 1. Damit ist $f - h(X - a)$ konstant, und weil a eine Nullstelle von f und von $X - a$ ist, ist diese Konstante 0. Also gilt $f = (X - a)h$.

Rekursiv sieht man daran, dass f höchstens d Nullstellen in K haben kann.

Hilfssatz 2.3.12 Eine universelle Abbildungseigenschaft

Es seien R ein kommutativer Ring, $(M, \diamond)$ ein Monoid, A eine R-Algebra und $\varphi : (M, \diamond) \to (A, \cdot)$ ein Monoidmorphismus.

Dann gibt es genau einen R-Algebren-Homomorphismus $\Phi : R[M] \to A$, der die Bedingung

$$\forall m \in M : \ \Phi(\delta_m) = \varphi(m)$$

erfüllt.

Beweis. Natürlich muss hier gelten, dass für ein Element $f = \sum_{m \in M} f(m) \cdot \delta_m$ die Abbildung Φ durch die Setzung

$$\Phi(f) = \sum_{m \in M} f(m)\varphi(m)$$

gegeben ist. Man rechnet leicht nach, dass dies ein R-Algebrenhomomorphismus ist. ◯

Folgerung 2.3.13 Polynomringe & Co.

Es sei $\mathbb{Z}[X]$ der Polynomring über $\mathbb{Z}$ in einer Variablen. Jeder Ring A wird auf genau eine Art zu einer $\mathbb{Z}$-Algebra, durch den eindeutig bestimmten Ringhomomorphismus von $\mathbb{Z}$ nach A. Die $\mathbb{Z}$-Algebren-Homomorphismen von $\mathbb{Z}[X]$ nach A werden also durch Vorgabe eines beliebigen Elements $a \in A$ als Bild von X festgesetzt.

Wenn hingegen $\mathbb{Z}[X, Y]$ ein Polynomring in zwei Variablen ist, dann haben wir eine Bijektion

$$\mathrm{Hom}(\mathbb{Z}[X, Y], A) \ni \Phi \mapsto (\Phi(X), \Phi(Y)) \in \{(a, b) \in A^2 \mid ab = ba\}.$$

Ist schließlich $Q = \mathbb{Z}[X, Y]/I$ für das von $I = XY - 1$ erzeugte Ideal, so sagt uns der Homomorphiesatz mit dem, was wir gerade über den Polynomring gelernt haben, dass

$$\begin{aligned} \mathrm{Hom}(Q, A) \ni \Phi \mapsto (\Phi(X + I), \Phi(Y + I)) \ &\in \{(a, b) \in A^2 \mid ab = ba = 1\} \\ &= \{(a, a^{-1}) \mid a \in A^\times\} \end{aligned}$$

eine Bijektion ist. Die Homomorphismen von Q nach A entsprechen bijektiv den Einheiten von A.

Bemerkung 2.3.14 Potenzreihen

a) Für jede natürliche Zahl n gibt es nur endlich viele Möglichkeiten, sie als Summe zweier natürlicher Zahlen zu schreiben.

Daher ist für zwei Abbildungen $f, g : \mathbb{N}_0 \to R$ (R ein kommutativer Ring) die Vorschrift

$$(f * g)(n) := \sum_{k,l \in \mathbb{N}_0,\ k+l=n} f(k)g(l)$$

nicht mit Konvergenzproblemen behaftet und liefert eine neue Abbildung von $\mathbb{N}_0$ nach R.

Auf diese Weise wird aus der Menge aller Abbildung von $\mathbb{N}_0$ nach R ein Ring, der Ring der *formalen Potenzreihen*.

b) Wenn allgemeiner $(M, \diamond)$ ein Monoid ist, in dem es für jedes $x \in M$ nur endliche viele $y, z \in M$ mit $y \diamond z = x$ gibt, dann wird durch die Formel aus 2.3.1 eine Ringstruktur auf $\mathrm{Abb}(M, R)$ definiert.

2.4 Aufbau des Zahlensystems II

In diesem Abschnitt wird dokumentiert, wie man aus dem Ring der ganzen Zahlen den Körper der rationalen Zahlen gewinnt. Zentral hierfür ist, dass $\mathbb{Z}$ ein Integritätsbereich ist (siehe 2.1.8), und dann kann man auch allgemeiner ansetzen:

Satz 2.4.1 Der Quotientenkörper

Es sei R ein Integritätsbereich. Dann gibt es einen Körper Q, der R als Teilring enthält und folgende Eigenschaft hat:

Ist K irgendein Körper und $\Phi : R \to K$ ein injektiver Ringhomomorphismus, so lässt sich Φ zu einem Ringhomomorphismus $\tilde{\Phi} : Q \to K$ fortsetzen.

Beweis.

Um eine Beweisidee zu entwickeln, nehmen wir erst einmal an, wir wüssten schon, dass R in einem Körper F enthalten ist.

Dann sind alle Elemente $x \in R \setminus \{0\}$ in F invertierbar. Man rechnet leicht nach, dass

$$Q := \{\frac{z}{n} \mid z, n \in R,\ n \neq 0\}$$

selbst ein Teilkörper von F ist. Ist $\Phi : R \to K$ wie in der Aussage des Satzes, dann können wir auf Q die Abbildung $\tilde{\Phi}$ definieren durch

$$\tilde{\Phi}(z/n) = \Phi(z)/\Phi(n).$$

Dies ist wohldefiniert, insbesondere auch, da $\Phi(n) \neq 0$ gilt für $n \neq 0$: Φ ist ja injektiv.

Wir müssen also „nur“ zeigen, dass es einen Körper gibt, der R als Teilring enthält, und wissen dann, wie Q zu konstruieren ist. Am besten nehmen wir uns aber direkt vor, Q zu konstruieren. Die Konstruktion ist eine Variante von der in 1.6.3: Wir definieren auf Paaren von Ringelementen eine Äquivalenzrelation und anschließend auf den Äquivalenzklassen die naheliegenden Verknüpfungen.

Dazu betrachten wir auf $M := R \times (R \setminus \{0\})$ die Relation

$$(z, n) \sim (\tilde{z}, \tilde{n}) \iff \tilde{n}z = n\tilde{z}.$$

Da R nullteilerfrei ist, ist dies eine Äquivalenzrelation. Die Äquivalenzklasse von (z, n) bezeichnen wir mit $\frac{z}{n}$ und setzen

$$Q := \{\frac{z}{n} \mid (z, n) \in M\}.$$

Man rechnet nach, dass dies ein Ring ist, wenn man

$$\frac{z}{n} + \frac{y}{m} := \frac{zm + yn}{mn} \quad \text{und} \quad \frac{z}{n} \cdot \frac{y}{m} := \frac{zy}{mn}$$

setzt. Dabei braucht man immer wieder die Nullteilerfreiheit und die Kommutativität von R.

Das Nullelement von Q ist $\frac{0}{1} = \frac{0}{n}$, das Einselement ist $\frac{1}{1} = \frac{n}{n}$ (für alle $n \neq 0$), und im Fall $z \neq 0$ ist zu $\frac{z}{n}$ der Bruch $\frac{n}{z}$ invers (bezüglich der Multiplikation). Damit ist Q ein Körper.

Streng genommen enthält er R nicht, aber die Abbildung

$$\iota : R \to Q, \quad \iota(r) = \frac{r}{1},$$

ist ein injektiver Ringhomomorphismus, und wir identifizieren R mit $\iota(R)$.

Dann ist alles gezeigt. ◯

Bemerkung 2.4.2 Rationale Zahlen, rationale Funktionen

a) Für $R = \mathbb{Z}$ liefert diese Konstruktion gerade den Körper $\mathbb{Q}$ der rationalen Zahlen.

b) Angewandt auf den Polynomring $k[X]$ in einer Variablen über dem Körper k liefert er den Körper der *rationalen Funktionen*

$$k(X) := \{\frac{f}{g} \mid f, g \in k[X], g \neq 0\}.$$

Diese „Funktionen“ sind nicht mehr auf ganz k definiert, sie haben Definitionslücken, die hier *Polstellen* genannt werden – ein Begriff, der auch in der Funktionentheorie und der algebraischen Geometrie eine Rolle spielt.

c) Eine ähnliche Konstruktion kann man auch für kommutative Ringe R durchführen, die nicht unbedingt nullteilerfrei sind. Wenn $S \subseteq R$ ein *multiplikatives System* ist, d.h. $1 \in S$ und $\forall s,t \in S : st \in S$, dann erhält man auf $R \times S$ eine Äquivalenzrelation durch

$$(z,n) \sim (\tilde{z},\tilde{n}) \iff \exists u \in S : u(\tilde{n}z - n\tilde{z}) = 0.$$

Dieses zusätzliche u fängt die mangelnde Nullteilerfreiheit beim Nachweis der Transitivität auf.

Ansonsten rechnet man mit den Äquivalenzklassen genauso wie oben und erhält einen Ring, der üblicherweise mit $S^{-1}R$ notiert wird.

Dieser Prozess der *Lokalisierung* ist in der Algebraischen Geometrie und in der Algebraischen Zahlentheorie von großer Bedeutung.

Für nullteilerfreie Ringe ist eben $S = R \setminus \{0\}$ multiplikativ, und damit ordnet sich unser Spezialfall in diese allgemeinere Situation ein.

Kapitel 3

Teilbarkeit und Primzahlen

In diesem Kapitel übernimmt die Zahlentheorie das Kommando und belebt ein Stück weit die algebraischen Konzepte. Die Konzepte, die hier im Lauf der Zeit eingeführt werden, haben wir allerdings teilweise schon kennengelernt.

3.1 Teilbarkeit

Definition 3.1.1 Teiler, ggT, kgV, Teilerfremdheit

Es sei n eine natürliche Zahl. Dann heißt $d \in \mathbb{N}$ ein *Teiler* von n, falls ein $t \in \mathbb{N}$ existiert mit $d \cdot t = n$. Wie schreiben dann $d \mid n$.

In diesem Fall heißt n ein *Vielfaches* von d.

Die Menge aller Teiler von n ist endlich, denn alle Teiler von n sind $\leq n$.

Für zwei Zahlen n, m ist daher auch die Menge aller gemeinsamen Teiler endlich. Das größte Element dieser Menge heißt der *größte gemeinsame Teiler* von n und m. Er wird als $\mathrm{ggT}(m, n)$ notiert, oder manchmal auch einfach als (m, n). Analog kann man den ggT einer nichtleeren Menge von natürlichen Zahlen definieren.

In der Menge aller gemeinsamen Vielfachen von m und n liegt $m \cdot n$. Also gibt es auch ein kleinstes Element dieser Teilmenge von $\mathbb{N}$. Es heißt das *kleinste gemeinsame Vielfache* von m und n und wird mit $\mathrm{kgV}(m, n)$ notiert. Analog kann man das kgV einer endlichen Menge von natürlichen Zahlen definieren.

Zwei natürliche Zahlen m, n heißen *teilerfremd,* wenn der einzige gemeinsame Teiler in den natürlichen Zahlen 1 ist.

Der Begriff des Teilers lässt sich praktisch ungeändert auf kommutative Ringe übertragen, siehe 3.1.8

Um den Begriff des ggT zu übertragen, müssen wir ihn mangels Ordnungsrelation erst von einer anderen Warte aus verstehen, tun das aber bis Definition 3.1.11.

Hilfssatz 3.1.2 Berechnung des ggT

Es seien $a, b \in \mathbb{N}$ *gegeben. Dann gibt es* $c, d \in \mathbb{Z}$, *sodass*

$$ac + bd = \mathrm{ggT}(a, b).$$

Beweis. Wir kennen das schon aus 1.2.8c), beweisen es aber noch einmal etwas anders:

Es sei $a \leq b \in \mathbb{N}$. Man sieht schnell, dass der ggT von a und b dasselbe ist wie der ggT von a und $b - a$, denn jeder gemeinsame Teiler von a, b ist auch einer von $a, b - a$ und umgekehrt.

Da im Fall $a = b$ oder $a = 1$ offensichtlich $c = 1, d = 0$ eine gute Wahl ist, lässt sich also schön eine vollständige Induktion nach $\max(a, b)$ machen.

Im Fall $1 < a < b$ ist nämlich das Maximum von $\{a, b - a\}$ kleiner als das von $\{a, b\}$, und es existieren $\tilde{c}, \tilde{d} \in \mathbb{Z}$, sodass

$$\tilde{c}a + \tilde{d}(b - a) = \mathrm{ggT}(a, b - a) = \mathrm{ggT}(a, b).$$

Also tun $c := \tilde{c} - \tilde{d}$ und $d := \tilde{d}$ was wir von ihnen wollen. ◯

Folgerung 3.1.3 Teiler des ggT

Für natürliche Zahlen a, b *sind die Teiler von* $\mathrm{ggT}(a, b)$ *genau die gemeinsamen Teiler von* a *und* b.

Die bisher unklare Richtung wird nun geklärt, denn ein gemeinsamer Teiler von a und b teilt natürlich auch alle Zahlen der Form $ca + db$, $c, d \in \mathbb{Z}$.

Insbesondere ist der ggT von a und b **der** gemeinsame Teiler, der ein Vielfaches aller gemeinsamen Teiler ist, also das kleinste gemeinsame Vielfache aller Teiler. Da gibt es nur eines – das ist das schöne an den natürlichen Zahlen.

Bemerkung 3.1.4 Euklidischer[1] Algorithmus

Es seien wieder a, b natürliche Zahlen, $a < b$. Ein algorithmisches Verfahren zur Umsetzung der eben gewonnen Einsicht (also: Konstruktion von c, d) geht so:

Setze $a_0 := b, a_1 := a$. Wähle $k_1 \in \mathbb{N}$, sodass

$$0 \leq a_2 := a_0 - k_1 a_1 < a_1.$$

Dadurch wird a_2 festgelegt. Eine Wahl von k_1 wie angegeben geht natürlich, denn nur endlich viele Zahlen $k \cdot a_1$ sind kleiner als a_0, und wir setzen

$$k_1 := \max\{k \in \mathbb{N}_0 \mid ka_1 \leq a_0\}.$$

[1] Euklid, ca. 300 v. Chr.; im Prinzip wird das Vorgehen hier im siebten Buch der Elemente, §1 u. 2, beschrieben. Sehr wahrscheinlich hat Euklid das von pythagoräischen Quellen abgeschrieben.

Dann gilt

$$k_1 a_1 \leq a_0 < (k_1 + 1)a_1,$$

und wir haben, was wir wollen.

Fall 1: $a_2 = 0$: Hier ist a_1 ein Teiler von a_0, also ist a der ggT von a und b und wir sind fertig.

Fall 2: $a_2 \neq 0$: Wähle eine natürliche Zahl k_2, sodass

$$0 \leq a_3 := a_1 - k_2 a_2 < a_2.$$

Mache sukzessive so weiter. Wenn a_i nicht 0 ist, so wähle $k_i \in \mathbb{N}$ derart, dass

$$0 \leq a_{i+1} := a_{i-1} - k_i a_i < a_i.$$

Irgendwann wird das so definierte a_{i+1} Null sein, und dann brechen wir den Vorgang ab.

Mit dem Argument vom Anfang des Beweises von 3.1.2 gilt hier:

$$\mathrm{ggT}(a_i, a_{i-1}) = \mathrm{ggT}(a_{i+1}, a_i).$$

Wenn dann am Ende $a_{i+1} = 0$ gilt, so ist a_i ein Teiler von a_{i-1} und damit ist

$$a_i = \mathrm{ggT}(a_i, a_{i-1}) = \mathrm{ggT}(a, b).$$

Durch „Zurückrechnen“ sieht man, wie a_i sich als ganzzahlige Linearkombination von a und b schreiben lässt.

Anstatt das jetzt allgemein zurückzuverfolgen, machen wir das in einem Beispiel.

Beispiel 3.1.5 Zwei Zahlen wohnen, ach, auf meinem Blatt

Wir wollen den ggT der natürlichen Zahlen 117 und 265 finden und als ganzzahlige Linearkombination der beiden schreiben.

$$\begin{array}{lll}
a_0 = 265, & a_1 & = 117 \\
k_1 = 2, & a_2 = 265 - 2 \cdot 117 = 265 - 234 & = 31 \\
k_2 = 3, & a_3 = 117 - 3 \cdot 31 = 117 - 93 & = 24 \\
k_3 = 1, & a_4 = 31 - 24 & = 7 \\
k_4 = 3, & a_5 = 24 - 3 \cdot 7 & = 3 \\
k_5 = 2, & a_6 = 7 - 2 \cdot 3 & = 1 \\
k_6 = 3, & a_7 = 3 - 3 \cdot 1 & = 0 \quad - \quad \text{Bingo.}
\end{array}$$

Der ggT ist also $a_6 = 1$, und die Zahlen waren demnach teilerfremd. Weiter gilt

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) \\ &= 7 \cdot 7 - 2 \cdot 24 = 7 \cdot (31 - 24) - 2 \cdot 24 \\ &= 7 \cdot 31 - 9 \cdot (117 - 3 \cdot 31) = 34 \cdot (265 - 2 \cdot 117) - 9 \cdot 117 \\ &= 34 \cdot 265 - 77 \cdot 117, \end{aligned}$$

und wir können tatsächlich ganz stumpfsinnig den ggT als Linearkombination von 265 und 117 schreiben. Wir haben also konkrete Wahlen für die Zahlen c, d aus Hilfssatz 3.1.2 gefunden.

Hilfssatz 3.1.6 Ein paar Folgerungen

Es seien $a, b \in \mathbb{N}$ gegeben.

a) Für $g = \mathrm{ggT}(a, b)$ sind die Zahlen $\frac{a}{g}$ und $\frac{b}{g}$ teilerfremd.

b) Wenn a, b teilerfremd sind und $c \in \mathbb{N}$ eine Zahl ist, sodass $a \mid bc$ gilt, dann teilt a schon c.

c) Es gilt $\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) = a \cdot b$.

Beweis. a) Wir können g nach 3.1.2 schreiben als

$$g = ax + by, \quad x, y \in \mathbb{Z}.$$

Daher ist

$$1 = \frac{a}{g} \cdot x + \frac{b}{g} \cdot y,$$

und jeder gemeinsame natürliche Teiler von $\frac{a}{g}$ und $\frac{b}{g}$ teilt auch 1, muss also selbst 1 sein.

b) Es sei $bc = ad,\ d \in \mathbb{N}$.

Jetzt ist ja 1 der ggT von a und b, wir können also 1 schreiben als

$$1 = ax + by, \quad x, y \in \mathbb{Z}.$$

Multiplikation mit c liefert

$$c = acx + bcy = a(cx + dy), \quad \text{also} \quad a \mid c.$$

Ach so: $(cx + dy)$ ist eine natürliche Zahl, denn sie ist ganz und a und c sind positiv, also ist auch $(cx + dy)$ positiv.

c) Das ist eine nette Übung zum b)-Teil. Am besten fängt man mit teilerfremden a, b an... ◯

Folgerung 3.1.7 Gekürzte Brüche

Jede rationale Zahl q lässt sich auf genau eine Art als

$$q = \frac{z}{n}, \quad z \in \mathbb{Z},\ n \in \mathbb{N},$$

schreiben, wobei entweder $z = 0,\ n = 1$ gilt oder $|z|$ und n teilerfremd sind.

NB: Nachher brauchen wir diese Fallunterscheidung nicht mehr, weil wir für alle Paare ganzer Zahlen einen ggT definieren werden.

Beweis. Wenn $q = 0$ ist, so ist $q = \frac{0}{1}$. Das ist der eine Fall.

Sei also $q \neq 0$. Dann ist $q = \frac{w}{m}$ für geeignete $w \in \mathbb{Z}, m \in \mathbb{N}$. Wenn g der größte gemeinsame Teiler von $|w|$ und m ist, dann gilt für $z = w/g,\ n = m/g$, dass

$$q = \frac{z}{n},$$

und $|z|$ und n sind nach dem letzten Hilfssatz teilerfremd.

Ist $q = \frac{s}{k}$ eine weitere Darstellung von q als Bruch teilerfremder Zahlen $s \in \mathbb{Z},\ k \in \mathbb{N}$, so gilt

$$\frac{s}{k} = \frac{z}{n}, \quad \text{also} \quad |z| \cdot k = |s| \cdot n.$$

Da $|z|, n$ und $|s|, k$ jeweils teilerfremd sind, folgt aus dem letzten Hilfssatz, dass $|z|$ ein Teiler von $|s|$ ist und umgekehrt. Daher sind sie gleich. Genauso auch k und n. Die Vorzeichen von z und s sind durch das Vorzeichen von q festgelegt, also sind auch z und s gleich. ◯

Nun wollen wir den Begriff der Teilbarkeit auf ein etwas abstrakteres Niveau heben. Zunächst sollte man von den natürlichen zu den ganzen Zahlen übergehen. Aber wieso nicht gleich zu kommutativen Ringen?

Definition 3.1.8 Nochmals die Teilbarkeit

Es sei R ein kommutativer Ring. Dann heißt $a \in R$ ein *Teiler* von $b \in R$, falls ein $c \in R$ existiert, sodass $b = c \cdot a$.

Für natürliche Zahlen ergibt das den alten Begriff, wenn wir $\mathbb{Z}$ als $\mathbb{N}$ enthaltenden Ring verwenden.

Für beliebiges R ist der zweite Faktor c jetzt nicht mehr eindeutig. In der Welt der natürlichen Zahlen war das so, und es bleibt so, wenn wir voraussetzen, dass R nullteilerfrei ist und $a \neq 0$ gilt. Denn dann folgt aus $ac_1 = ac_2$, dass $a(c_1 - c_2) = 0$, also $c_1 = c_2$.

Nullteilerfreiheit ist für Teilbarkeitseigenschaften in Ringen also oft eine gute Voraussetzung.

Definition 3.1.9 Assoziiertheit

Es sei R ein kommutativer Ring. Zwei Elemente $a, b \in R$ heißen *assoziiert*, falls eine Einheit (siehe 2.1.5) $e \in R^\times$ existiert, sodass $b = a \cdot e$.

Für $R = \mathbb{Z}$ heißt das einfach, dass die zwei Zahlen bis aufs Vorzeichen übereinstimmen.

Assoziiert zu sein ist eine Äquivalenzrelation auf R. Die Äquivalenzklasse von a heißt seine *Assoziiertenklasse* und ist genau $a \cdot R^\times$. Das ist die Bahn von a unter der naheliegenden Operation von $R^\times$ auf R.

Man sagt auch, die Assoziiertenklasse von a teile die von b, wenn a ein Teiler von b ist. Es ist klar, dass diese Begriffsbildung nicht von der Wahl der Repräsentanten der Assoziiertenklassen abhängt, denn zwei solche Repräsentanten unterscheiden sich ja nur um eine Einheit.

Bemerkung 3.1.10 Eine Ordnungsrelation

Wenn R kommutativ und nullteilerfrei ist, dann wird durch die Teilbarkeit eine Ordnungsrelation auf der Menge der Assoziiertenklassen festgelegt:

$$aR^\times \preceq bR^\times \iff a \mid b.$$

Transitivität ist klar, dazu braucht man auch weder die Nullteilerfreiheit noch die Bildung der Assoziiertenklassen, das geht schon elementweise.

Interessanter ist es zu zeigen, dass zwei Assoziiertenklassen $a \cdot R^\times$ und $b \cdot R^\times$ übereinstimmen, wenn sie sich gegenseitig teilen. Das ist klar, wenn eine der beiden Klassen nur aus der Null besteht. Ansonsten geht es so: a und b teilen sich gegenseitig, es gibt also $c, d \in R$, sodass

$$a = bc \text{ und } b = ad.$$

Daraus folgt $a = acd$, und da R nullteilerfrei ist, folgt aus $a(1 - cd) = 0$, dass $1 - cd = 0$. Daher ist $cd = 1$, und auch $dc = 1$, da R kommutativ ist. Es sind also c und d Einheiten in R und folglich a und b assoziiert.

Definition 3.1.11 Noch einmal der ggT

Es seien R ein kommutativer und nullteilerfreier Ring und $a, b \in R$.

a) Das Element $g \in R$ heißt ein *größter gemeinsamer Teiler* von a und b, wenn g ein gemeinsamer Teiler ist und jeder gemeinsame Teiler von a und b auch g teilt.

   NB: Das Adjektiv „größter“ bezieht sich also auf die Ordnungsrelation aus 3.1.10.

Wenn man von **dem** ggT sprechen will, so muss man damit eigentlich die Assoziiertenklasse (eines beliebigen ggT) meinen. Im Falle $R = \mathbb{Z}$ gibt es in einer Assoziiertenklasse $\{a, -a\}$ immer die naheliegende Wahl, als Vertreter das nichtnegative Element zu wählen.

Wegen 3.1.3 fallen dann für natürliche Zahlen die beiden Definitionen des ggT zusammen.

b) a und b heißen *teilerfremd*, wenn die einzigen gemeinsamen Teiler die Einheiten in R sind.

Beispiel 3.1.12 Ein paar ggT

Es sei R ein kommutativer und nullteilerfreier Ring.

a) Der ggT von $a \in R$ und einer Einheit $e \in R^\times$ ist immer die Assoziiertenklasse von 1, also $R^\times$. Klar, denn nur Einheiten teilen Einheiten.

b) Der ggT von $a \in R$ und 0 ist immer $a \cdot R^\times$. Klar, denn alles teilt 0.

c) In $R = \mathbb{Z}[X]$ ist der ggT von X und 2 gleich 1. Es gibt kein nichtkonstantes Polynom, das 2 teilen würde, also muss der ggT eine Konstante sein, und die einzigen Teiler von 2 (in $\mathbb{Z}$), die auch X teilen, sind ± 1.

Hilfssatz 3.1.13 Die Idealisierung

Es sei R ein nullteilerfreier kommutativer Ring. Weiter seien $a, b \in R$.

a) Ist d ein gemeinsamer Teiler von a und b, so teilt d auch jede Linearkombination $ax + by$, $x, y \in R$.

b) Wenn es ein $g \in R$ gibt, sodass

$$\{ax + by \mid x, y \in R\} = Rg := \{rg \mid r \in R\}$$

gilt, dann ist g ein ggT *von a und b.*

Beweis. a) Das ist klar. Aus $a = rd, b = sd$, $r, s \in R$ folgt

$$ax + by = (rx + sy)d.$$

b) Es ist g ein Teiler von a und b, da beide zur linker Hand definierten Menge gehören. Zum Beispiel ist $a = a \cdot 1 + b \cdot 0$.

Andererseits gehört g selber auch zu dieser Menge, und in a) hatten wir gesehen, dass jeder gemeinsame Teiler von a und b daher auch g teilt. Definitionsgemäß ist also g ein ggT von a und b. ◯

Definition 3.1.14 Wieder ein Ideal

a) Es sei R ein kommutativer Ring, $a, b \in R$. Die Menge $\{ax + by \mid x, y \in R\}$ ins Feld geführt, die gerade eben im Zuge der Teilbarkeit eine Rolle spielte, ist dann ein Ideal in R (siehe 2.1.11).

Tatsächlich kommt der Name „Ideal“ daher, dass Ideale als „Idealisierung“ des Begriffs des ggT zum ersten Male das Licht der Welt erblickten.[2]

Die abstrakte Definition der Ideale, wie sie natürlich auch hier im Text zunächst gegeben wurde, ist erst nachträglich zu Bedeutung gekommen.

b) Ein Ideal $I \subseteq R$ heißt ein *Hauptideal*, falls ein $g \in I$ existiert, sodass $I = Rg$ gilt.

Falls der Ring klar ist, werden wir oft $(g) := Rg$ schreiben.

Ein Element g mit $I = (g)$ heißt dann ein *Erzeuger* von I.

Nicht jedes Ideal ist ein Hauptideal, was auch mit daran liegt, dass nicht in jedem Ring ein ggT für beliebige Elemente existiert.

Zum Beispiel ist das von 2 und X erzeugte Ideal im Polynomring $\mathbb{Z}[X]$ kein Hauptideal, da es sonst vom ggT 1 der Erzeuger erzeugt sein müsste, aber 1 liegt gar nicht in dem betrachteten Ideal.

c) Ein nullteilerfreier kommutativer Ring R, in dem jedes Ideal ein Hauptideal ist, heißt sinnvoller Weise ein *Hauptidealring*.

Nach 3.1.13 haben in einem Hauptidealring zwei Elemente stets einen ggT.

Hilfssatz 3.1.15 Assoziiertenklassen und Ideale

Es sei R ein Hauptidealring. Dann gelten:

a) Zwei Elemente $g, h \in R$ sind genau dann Erzeuger desselben Hauptideals $Rg = Rh$, wenn sie assoziiert sind.

b) In jeder nichtleeren Teilmenge $S \subseteq R$ gibt es ein Element m, das bezüglich Teilbarkeit minimal ist[3]*.*

Beweis. a) ist klar, denn beide Bedingungen sind in nullteilerfreien Ringen dazu äquivalent, dass g und h sich gegenseitig teilen.

b) ist etwas trickreicher. Wir schließen durch einen Widerspruchsbeweis und nehmen dazu an, die Aussage sei falsch.

[2] Nämlich bei Ernst Eduard Kummer, 1810-1893

[3] Das soll heißen, dass alle $s \in S$, die m teilen, zu m assoziiert sind, ist also eigentlich eine Bedingung an die Assoziiertenklassen $sR^\times$, $s \in S$.

Es sei $s_1 \in S$ irgendein Element. Nach Annahme ist es nicht minimal, das heißt, es gibt einen Teiler $s_2 \in S$ von s_1, der nicht zu s_1 assoziiert ist. Sukzessive so fortfahrend wählen wir Elemente $s_i \in S$, sodass jeweils s_{i+1} ein Teiler von s_i ist, aber nicht umgekehrt.

Dann erhalten wir – wegen der Teilbarkeitsbedingung – eine echt aufsteigende Kette von Idealen

$$Rs_1 \subset Rs_2 \subset Rs_3 \subset \ldots$$

Die Vereinigung $I = \cup_{i\in\mathbb{N}} Rs_i$ dieser Ideale ist auch ein Ideal von R, denn:

- $0 \in I$
- $\forall a, b \in I : \exists i \in \mathbb{N} : a, b \in Rs_i$, und daher gilt auch $a + b \in Rs_i \subseteq I$.
- $\forall a \in I, r \in R : \exists i \in \mathbb{N} : a \in Rs_i$ und daher gilt $ra \in Rs_i \subseteq I$.

Da R ein Hauptidealring ist, gibt es ein $a \in I$ mit $I = Ra$. Dieses a liegt aber schon in einem der Rs_i, und es folgt

$$Ra \subseteq Rs_i \subseteq Ra, \quad \text{also} \quad Ra = Rs_i.$$

Es folgt für alle $k \geq i$:

$$Rs_i \subseteq Rs_k \subseteq Ra = Rs_i,$$

also $Rs_k = Rs_i$. Daher ist die Kette – entgegen der Konstruktion – nicht echt aufsteigend. Dies liefert den gewünschten Widerspruch. ◯

Wir beschreiben jetzt eine wichtige Klasse von Hauptidealringen.

Definition 3.1.16 Euklidischer Ring

Es sei R ein nullteilerfreier kommutativer Ring. Weiter sei $\gamma : R \to \mathbb{N}_0$ eine Abbildung.

Dann heißt R *euklidisch bezüglich* γ, falls $[\gamma(r) = 0 \iff r = 0]$ und vor allem folgendes gilt: für alle $a, b \in R, b \neq 0$, gibt es $c \in R$, sodass

$$\gamma(a - bc) < \gamma(b).$$

Bemerkung 3.1.17 Euklid und die Hauptideale

Jeder euklidische Ring (R, γ) ist ein Hauptidealring. Ist nämlich $I \subseteq R$ ein Ideal, so ist entweder $I = \{0\} = R \cdot 0$ – ein Hauptideal – oder es gibt ein $g \in I$, sodass

$$\gamma(g) = \min\{\gamma(x) \mid x \in I, x \neq 0\}.$$

Es ist klar, dass dieses g jedes $a \in I$ teilen muss, denn g ist nicht 0, also existiert ein $c \in R$ mit $\gamma(a - cg) < \gamma(g)$, was nach Wahl von g ja $\gamma(a - cg) = 0$ erzwingt, denn $a - cg \in I$.

Es folgt nach 3.1.13, dass in einem euklidischen Ring je zwei Elemente immer einen ggT haben. Dieser lässt sich wie in 3.1.4 berechnen, wenn man dort die k_i so wählt, dass $\gamma(a_{i-1} - k_i a_i) < \gamma(a_i)$ gilt, was geradezu nach Definition der euklidischen Ringe möglich ist.

Es ist übrigens im Allgemeinen sehr schwer zu entscheiden, ob ein gegebener Hauptidealring durch Wahl einer Abbildung γ von R nach $\mathbb{N}_0$ zu einem euklidischen Ring gemacht werden kann. Wenn man so ein γ sieht, dann ist alles gut. Aber wenn man keines sieht, könnte es dennoch eines geben. Das zu widerlegen ist schwer, denn die Abbildung γ unterliegt keinen weitreichenden strukturellen Einschränkungen, sodass ein Ansatz sich gar nicht aufdrängt.

Beispiel 3.1.18 Einige euklidische Ringe

a) $\mathbb{Z}$ ist bezüglich $\gamma(z) = |z|$ euklidisch. Das haben wir im Prinzip gerade beim euklidischen Algorithmus ausgeschlachtet.

b) Ist K ein Körper, so ist der Polynomring $K[X]$ euklidisch, wenn wir

$$\gamma(0) = 0, \quad \text{und sonst} \quad \gamma(f) = \operatorname{grad}(f) + 1$$

setzen. Das liegt an an den Regeln der Polynomdivision aus 2.3.4.

Noch kohärenter wird das, wenn wir alternativ $\gamma(f) = 2^{\operatorname{grad}(f)}$ setzen. Dabei ist insbesondere der Grad des Nullpolynoms gleich $-\infty$, und $2^{-\infty} = 0$.

c) Der Ring der ganzen Gaußschen[4] Zahlen $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist euklidisch bezüglich der Abbildung

$$\gamma(a + b\mathrm{i}) := a^2 + b^2 = |a + b\mathrm{i}|^2.$$

Denn: Für $a + b\mathrm{i},\ c + d\mathrm{i} \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$ betrachten wir

$$\frac{a + b\mathrm{i}}{c + d\mathrm{i}} = \frac{ac + bd + (bc - ad)\mathrm{i}}{c^2 + d^2} =: x + y\mathrm{i} \in \mathbb{C}.$$

Wähle nun $m, n \in \mathbb{Z}$ mit $|m - x|, |n - y| \leq \frac{1}{2}$.

Dann gilt

$$a + b\mathrm{i} - (c + d\mathrm{i})(m + n\mathrm{i}) = ((x - m) + (y - n)\mathrm{i})(c + d\mathrm{i}),$$

und die Multiplikativität des Betrages zeigt dann

$$\gamma(a + b\mathrm{i} - (c + d\mathrm{i})(m + n\mathrm{i})) \leq \frac{1}{2}\gamma(c + d\mathrm{i}).$$

[4]Carl Friedrich Gauß, 1777-1855

d) Der Ring $R := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ ist kein Hauptidealring, also bezüglich keiner Abbildung γ euklidisch.

Es ist nämlich die Menge

$$I := \{2x + (1 + \sqrt{5})y \mid x, y \in \mathbb{Z}\}$$

ein Ideal in R, aber kein Hauptideal.

Ideal ist es, da es eine Untergruppe ist und für $2x + (1 + \sqrt{5})y \in I$ sowie $a + b\sqrt{5} \in R$ gilt

$$\begin{aligned}&(a + b\sqrt{5}) \cdot (2x + (1 + \sqrt{5})y) = \\ &(2ax + (1 + \sqrt{5})ay) + (2b(2y - x) + (1 + \sqrt{5})b(2x + y)).\end{aligned}$$

Das ist eine Summe von zwei Elementen in I, also selbst auch in I.

Wenn I ein Hauptideal wäre, so gäbe es ein $g \in I$ mit $I = Rg$. Dann wäre also g ein Teiler von 2 im Ring R. Welche gibt es da?

Aus $(a+b\sqrt{5})(c+d\sqrt{5}) = 2$ folgt $ad+bc = 0$, denn $\sqrt{5}$ ist nicht rational. Also folgt $\frac{a}{b} = -\frac{c}{d}$. Wenn nun g ein gemeinsamer Teiler von a und b in $\mathbb{Z}$ wäre, so würde es auch $ac + 5bd = 2$ teilen. Es ist also $\mathrm{ggT}(a, b) = 1$ oder 2. Wäre der ggT 2, dann wäre 2 auch ein Teiler von $a + b\sqrt{5}$ in R, und damit wären die beiden assoziiert. Analog wären 2 und $c+d\sqrt{5}$ assoziiert, wenn c, d nicht teilerfremd wären.

Wären hingegen a, b und c, d jeweils teilerfremd, so folgte aus $\frac{a}{b} = -\frac{c}{d}$, dass

$$(a, b) = \pm(c, -d).$$

Eingesetzt in die Zerlegung von 2 impliziert das

$$a^2 - 5b^2 = \pm 2.$$

Diese Gleichung ist in $\mathbb{Z}$ nicht lösbar, denn eine Zahl der Gestalt

$$\pm 2 - a^2$$

ist niemals durch 5 teilbar, wie eine Fallunterscheidung nach dem Rest der Division von a durch 5 zeigt.

Die einzigen Teiler von 2 in R sind also Einheiten und zu 2 assoziierte Elemente. Insbesondere gilt dies für unseren hypothetischen Erzeuger g von I, und das würde zeigen, dass $I = R$ oder $I = 2R$ gilt.

Der ersten Fall kann nicht auftreten, denn $1 \notin I$. Der zweite Fall kann nicht auftreten, denn $1 + \sqrt{5} \in I$, aber $\notin 2R$.

Daher ist I kein Hauptideal und mithin R nicht euklidisch.

Bemerkung 3.1.19 Chinesischer Restsatz

a) Es seien R ein Hauptidealring und r, s in R zwei teilerfremde Elemente, also so beschaffen, dass $1 = rx + sy$ für geeignete $x, y \in R$.

Dann erfüllen die Ideale $I = Rr$ und $J = Rs$ die Voraussetzung des Chinesischen Restsatzes 2.1.14, und wir finden

$$R/(Rr \cap Rs) \cong R/(Rr)timesR/(Rs).$$

Unsere Konstruktion des Isomorphismus zeigt insbesondere, dass es für alle $a, b \in \mathbb{R}$ ein $x \in R$ gibt, für das simultan

$$x \equiv a \pmod{Rr} \quad \text{und} \quad x \equiv b \pmod{Rs}$$

gilt. Es ist diese Art von Aussage, die klassischer Weise chinesischer Restsatz genannt wird.

Sie lässt sich natürlich für endlich viele (paarweise teilerfremde) Elemente verallgemeinern.

b) Zum Beispiel sagt er für $R = K[X]$, K ein Körper, dass sich für je n paarweise verschiedene Elemente $x_1, \ldots, x_n \in K$ und jede Vorgabe von Elementen $a_1, \ldots, a_n \in K$ ein Polynom f finden lässt mit

$$f(x_i) = a_i,\ 1 \leq i \leq n.$$

Dieses ist eine Lösung der simultanen Kongruenzbedingung

$$f \equiv a_i \pmod{(X - x_i)},\ 1 \leq i \leq n,$$

die es nach unserem Satz geben muss.

Man kann hier auch noch feinere Bedingungen vorgeben (Nullstellenordnungen oder allgemeiner Werte von Ableitungen...).

Bemerkung 3.1.20 Einheiten in $\mathbb{Z}/N\mathbb{Z}$

Es sei $N \in \mathbb{N}$ gegeben.

Aus 2.1.5 wissen wir, dass $a + \mathbb{Z}N$ genau dann in $R = \mathbb{Z}/N\mathbb{Z}$ invertierbar ist, wenn a und N teilerfremd sind.

Wir setzen

$$\varphi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times| = |\{a \in \mathbb{N} \mid a \leq N,\ \mathrm{ggT}(a, N) = 1\}|.$$

Das ist die *Eulersche*[5] *φ-Funktion.*

Nach dem Chinesischen Restsatz gilt für teilerfremde M, N :

$$\varphi(MN) = \varphi(M) \cdot \varphi(N).$$

[5]Leonhard Euler, 1707-1783

3.2 Primzahlen

Definition 3.2.1 Primzahl

Eine *Primzahl* ist eine natürliche Zahl $p > 1$, die sich nicht als Produkt zweier kleinerer natürlicher Zahlen schreiben lässt.

Die Menge der Primzahlen notieren wir mit $\mathbb{P}$.

$$\begin{aligned}\mathbb{P} &= \{n \in \mathbb{N} \mid n > 1 \text{ und } \forall d, t < n : d \cdot t \neq n\} \\ &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots\}.\end{aligned}$$

Es ist eine der vornehmsten Aufgaben der Zahlentheorie, mehr zu den Pünktchen hier zu sagen.

Hilfssatz 3.2.2 Alternative Charakterisierung

Eine natürliche Zahl $n > 1$ ist genau dann eine Primzahl, wenn für jedes Paar $(a, b) \in \mathbb{N}^2$ von natürlichen Zahlen gilt:

$$n \text{ teilt } ab \Rightarrow n \text{ teilt } a \text{ oder } n \text{ teilt } b.$$

Beweis. Es sei zunächst n eine Primzahl, die ab teilt.

Ist n kein Teiler von a, so sind a und n teilerfremd, denn der ggT ist ja ein gemeinsamer Teiler, aber nicht $\pm n$.

3.1.6b) sagt uns daher, dass in diesem Fall n ein Teiler von b ist, und genau das wollten wir wissen.

Umgekehrt erfülle n die Bedingung aus dem Hilfssatz. Wir müssen zeigen, dass es eine Primzahl ist. Sei also $a \in \mathbb{N}$ ein Teiler von n. Dann gibt es ein $b \in \mathbb{N}$ mit $n = ab$.

Dann ist aber nach Voraussetzung n ein Teiler von a oder von b, und damit sind nicht beide Faktoren kleiner als n – das mussten wir zeigen. ◯

Bemerkung 3.2.3 Klarheiten

Für jede natürliche Zahl n ist die Menge der Teiler

$$\{d \in \mathbb{N} : d \mid n\} \subseteq \{1, 2, 3, \dots, n\}$$

endlich, hat also ein kleinstes Element – klar: die Eins. Für $n \geq 2$ hat auch die Menge $\mathcal{D}$ der von Eins verschiedenen Teiler ein kleinstes Element p. Dieses ist zwangsläufig eine Primzahl, denn aus $p = ab$ mit $a, b < p$ folgt $a, b \in \mathcal{D}$, also $p \neq \min(\mathcal{D})$.

Also wird jede natürliche Zahl $n \geq 2$ von einer Primzahl p geteilt.

Im Fall $p \neq n$ wird auch n/p von einer Primzahl geteilt, und induktiv sieht man, dass n ein Produkt von Primzahlen ist.

Die 1 ist nach einer sinnvollen Konvention ein leeres Produkt:

$$1 = \prod_{p \in \emptyset \subset \mathbb{P}} p.$$

Satz 3.2.4 Fundamentalsatz der Arithmetik

Jede natürliche Zahl n lässt sich als Produkt von Primzahlen schreiben. Diese Darstellung ist eindeutig, wenn die Primfaktoren der Größe nach sortiert werden.

Beweis. Nur die Eindeutigkeit ist noch nicht klar.

Es sei n eine natürliche Zahl, und es seien

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_t$$

zwei Zerlegungen von n als Produkt von Primzahlen, wobei

$$p_1 \leq p_2 \leq \ldots \leq p_s, \quad q_1 \leq q_2 \leq \ldots \leq q_t.$$

Wir müssen zeigen, dass $s = t$ und $p_i = q_i,\ 1 \leq i \leq s,$ gilt.

Das machen wir durch vollständige Induktion nach $\min\{s, t\}$. Ist dieses 0, so ist $n = 1,$ und hier ist die Eindeutigkeit klar. Ist das Minimum 1, so ist n eine Primzahl, und die Behauptung ist auch klar.

Ansonsten ist p_1 ein Teiler von $q_1 \cdot \ldots \cdot q_t,$ und da p_1 prim ist ist es nach 3.2.2 ein Teiler eines der Faktoren, also eines q_j. Da q_j eine Primzahl ist, folgt $p_1 = q_j,$ und wegen der Nullteilerfreiheit von $\mathbb{Z}$ können wir diesen Faktor kürzen. Wir erhalten eine Gleichheit von Produkten von Primzahlen, mit weniger Faktoren, und aus der (unausgesprochenen) Induktionsannahme folgt die gewünschte Identität. ◯

Folgerung 3.2.5 Die p-adische Bewertung

Es sei $p \in \mathbb{P}$ eine Primzahl. Dann gibt es für jede ganze Zahl $k \neq 0$ eine eindeutig bestimmte Zahl $\mathrm{v}_p(k) \in \mathbb{N}_0$, sodass $p^{\mathrm{v}_p(k)}$ ein Teiler von k ist, aber $p^{\mathrm{v}_p(k)+1}$ nicht.

Dann gilt insbesondere

$$k = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(k)}$$

Für $k = 0$ schreibt man formal $\mathrm{v}_p(0) = \infty$.

Es gelten für alle $k, l \in \mathbb{Z}$ die Regeln

$$\begin{aligned} \mathrm{v}_p(k+l) &\geq \min\{\mathrm{v}_p(k), \mathrm{v}_p(l)\}, \\ \mathrm{v}_p(k \cdot l) &= \mathrm{v}_p(k) + \mathrm{v}_p(l). \end{aligned}$$

Beweis. Die Zahl $\mathrm{v}_p(k)$ zählt, wie oft die Primzahl p als Faktor in der Zerlegung von $|k|$ als Produkt von Primzahlen, vorkommt, wie sie laut 3.2.4 existiert.

Zu begründen sind nur noch die Rechenregeln. Die erste ist wegen des Distributivgesetzes klar, die zweite folgt unmittelbar aus der Eindeutigkeit der Primfaktorzerlegung. ◯

Folgerung 3.2.6 v_p **und der ggT**

Es seien $a, b \in \mathbb{N}$. *Dann gelten:*

a) b teilt a genau dann, wenn

$$\forall p \in \mathbb{P} : \mathrm{v}_p(b) \leq \mathrm{v}_p(a).$$

b) Der ggT von a und b ist

$$g = \prod_{p \in \mathbb{P}} p^{e_p}, \quad \text{wobei} \quad e_p = \min\{\mathrm{v}_p(a), \mathrm{v}_p(b)\}.$$

c) Das kgV von a und b ist

$$k = \prod_{p \in \mathbb{P}} p^{f_p}, \quad \text{wobei} \quad f_p = \max\{\mathrm{v}_p(a), \mathrm{v}_p(b)\}.$$

Beweis. a) Wenn für alle p die Bedingung $\mathrm{v}_p(b) \leq \mathrm{v}_p(a)$ gilt, dann ist

$$a = b \cdot \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(a) - \mathrm{v}_p(b)},$$

und das Produkt ist eine natürliche Zahl.

Ist umgekehrt $a = bc$ mit $c \in \mathbb{N}$, so gilt für alle $p \in \mathbb{P}$

$$\mathrm{v}_p(a) = \mathrm{v}_p(b) + \mathrm{v}_p(c) \geq \mathrm{v}_p(b)$$

und es folgt die Behauptung.

b) und c) sind einfache Konsequenzen hieraus. ◯

Bemerkung 3.2.7 Fortsetzungsgeschichte

Die Abbildung $\mathrm{v}_p : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ heißt die *p-adische Bewertung* auf $\mathbb{Z}$. Sie wird durch

$$\mathrm{v}_p(\frac{z}{n}) := \mathrm{v}_p(z) - \mathrm{v}_p(n)$$

zu einer Abbildung von $\mathbb{Q}$ nach $\mathbb{Z} \cup \{\infty\}$ fortgesetzt und behält dabei die beiden Eigenschaften aus der letzten Folgerung bei.

Wir wollen die Eigenschaften dieser Bewertung nicht weiter ausschlachten, die Notation wird aber gelegentlich hilfreich sein.

Als nächstes übertragen wir den arithmetisch motivierten Primzahlbegriff in die Ringtheorie.

Definition 3.2.8 irreduzibel oder prim?

Es sei R ein kommutativer Ring.

Ein Element $m \in R$ heißt *irreduzibel*, wenn $m \notin R^\times$ und für alle $a, b \in R$ gilt:

$$m = ab \Rightarrow a \in R^\times \text{ oder } b \in R^\times.$$

Ein Element $p \in R$ heißt ein *Primelement*, wenn es keine Einheit in R ist und wenn für $a, b \in R$ gilt:

$$p \text{ teilt } ab \Rightarrow p \text{ teilt } a \text{ oder } p \text{ teilt } b.$$

Irreduzibilität eines Elementes $m \in R$ heißt also, dass seine Assoziiertenklasse $mR^\times$ in R unter den Klassen $\neq R^\times$ bezüglich der Ordnungsrelation der Teilbarkeit minimal ist: Jeder Teiler von m ist entweder eine Einheit oder zu m assoziiert. Die Rechnung unter d) in 3.1.18 zeigt unter anderem, dass 2 in $\mathbb{Z}[\sqrt{5}]$ irreduzibel ist.

Für die Primzahlen gilt jetzt: Sie sind – laut Vergleich der Definitionen – gerade die positiven irreduziblen Elemente im Ring $\mathbb{Z}$, und laut 3.2.2 auch genau die positiven Primelemente in $\mathbb{Z}$.

Hilfssatz 3.2.9 Prim vs. irreduzibel

Es sei R ein nullteilerfreier kommutativer Ring.

a) Ein von 0 verschiedenes Primelement in R ist immer irreduzibel.

b) Wenn R ein Hauptidealring ist, dann ist ein irreduzibles Element in R immer auch prim.

Beweis. a) Es sei $0 \neq p \in R$ prim. Weiter seien $a, b \in R$ zwei Elemente mit $p = ab$.

Da p prim ist, muss es a oder b teilen. Es sei oBdA $a = cp$. Dann folgt

$$p = ab = cpb, \quad \text{also} \quad p(1 - bc) = 0,$$

und da R nullteilerfrei ist, folgt $1 - bc = 0$, also ist $bc = 1$, und b ist eine Einheit.

b) Nun seien R ein Hauptidealring und $m \in R$ irreduzibel. Weiter seien $a, b \in R$ Elemente, sodass m ein Teiler von ab ist: $ab = mt$, $t \in R$. Wenn m kein Teiler von a ist, dann sind a und m teilerfremd, denn die einzigen Teiler von m sind Einheiten und zu m assoziierte Elemente. Aber auch alle zu m assoziierten können a nicht teilen. Also ist 1 ein ggT von a und m, und nach 3.1.13 lässt 1 sich schreiben als

$$1 = ac + md, \quad c, d \in R \text{ geeignet.}$$

Multiplikation mit b macht daraus wieder – wie schon für $\mathbb{Z}$ gesehen –

$$b = abc + mbd = m(tc + bd),$$

also ist m ein Teiler von b.

Insgesamt zeigt das, dass m prim ist. ◯

Jetzt können wir den Fundamentalsatz der Arithmetik in die Welt der Hauptidealringe übertragen. Die in $\mathbb{N}$ geltende Eindeutigkeit muss einem Akt der Willkür weichen – wir müssen erst aus jeder Assoziiertenklassen von Primelementen einen Vertreter wählen.

Satz 3.2.10 Primzerlegung in Hauptidealringen

Es sei R ein Hauptidealring. Weiter sei $\mathbb{P}_R$ ein Vertretersystem der Assoziiertenklassen von Primelementen $\neq 0$.

Dann ist jedes $r \in R \setminus \{0\}$ assoziiert zu einem Produkt von endlich vielen Primelementen.

Sind weiter $s, t \in \mathbb{N}_0$ und $p_1, \ldots, p_s, q_1, \ldots q_t \in \mathbb{P}_R$ derart, dass Einheiten $\delta, \varepsilon \in R^\times$ existieren mit

$$r = \delta \cdot p_1 \cdot \ldots \cdot p_s = \varepsilon \cdot q_1 \cdot \ldots \cdot q_t,$$

so gelten $\varepsilon = \delta$, $s = t$ und – bis auf eine Vertauschung der Reihenfolge der Faktoren – es gilt $p_i = q_i$ für alle $1 \leq i \leq s$.

Beweis. Die Eindeutigkeit geht im Prinzip genauso wie im Fall $R = \mathbb{Z}$, und dazu sage ich jetzt nichts weiter.

Die Existenz der Zerlegung haben wir schon vorbereitet.

Wir nehmen an, die Aussage des Satzes sei falsch, und betrachten die Menge S aller Elemente $0 \neq r \in R$, die nicht zu einem Produkt von Elementen aus $\mathbb{P}_R$ assoziiert sind. Diese Menge ist dann nicht leer, und es gibt nach 3.1.15 ein minimales Element $m \in S$.

Natürlich ist m kein Primelement, da es sonst ja zu einem $p \in \mathbb{P}_R$ assoziiert wäre. Es sei $m = ab$ eine Zerlegung in zwei echte Faktoren, also beide nicht zu m assoziiert. Dann sind a und b im Sinne der Teilbarkeit kleiner als m und gehören demnach nicht zu S. Genau hier braucht man übrigens, dass m nicht 0 ist.

Es gibt also eine Zerlegung

$$a = e \cdot p_1 \cdot \ldots \cdot p_k, \quad b = f \cdot q_1 \cdot \ldots \cdot q_l$$

mit Primelementen $p_i, q_j \in \mathbb{P}_R$ und Einheiten e, f und es folgt

$$m = ef \cdot p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l$$

entgegen der Annahme. Damit ist diese zum Widerspruch geführt. ◯

Beispiel 3.2.11 Primelemente in $\mathbb{Z}[\mathrm{i}]$

Der Ring $\mathbb{Z}[\mathrm{i}]$ der ganzen Gaußschen Zahlen ist ein Hauptidealring, siehe 3.1.18. Es ist also interessant, eine Übersicht über die Primelemente hier zu bekommen. Hierzu benutzen wir die Normabbildung $N : \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$, $N(z) := |z|^2$ und die komplexe Konjugation:

$$\overline{x + y\mathrm{i}} = x - y\mathrm{i}.$$

Diese Abbildung ist insbesondere multiplikativ:

$$\overline{zw} = \overline{z} \cdot \overline{w}.$$

Wenn nun $\pi \in \mathbb{Z}[\mathrm{i}]$ ein Primelement $\neq 0$ ist, dann teilt es also $N(\pi) = \pi \cdot \overline{\pi}$, und dies ist eine natürliche Zahl. Da diese natürliche Zahl ein Produkt von Primfaktoren ist, muss π bereits einen dieser Primfaktoren teilen, da es ein Primelement ist. Die Primelemente in $\mathbb{Z}[\mathrm{i}]$ finden sich also gerade als Primteiler der natürlichen Primzahlen.

Es sei π ein Teiler der Primzahl p. Dann gilt

$$N(\pi) | N(p) = p^2,$$

und wir haben zwei Möglichkeiten: $N(\pi) = p$ oder $N(\pi) = p^2$.

NB: $N(\pi) = 1$ würde heißen, dass $\pi\overline{\pi} = 1$, und dann wäre ja π eine Einheit, was verboten ist.

Weiter sei nun $\pi = a + b\mathrm{i}$, $a, b \in \mathbb{Z}$. Dann ist $N(\pi) = a^2 + b^2$, und wir kommen letztlich zur Frage, wann eine Primzahl $p \in \mathbb{P}$ sich als Summe von zwei Quadraten schreiben lässt.

Fall 1: $p = 2$.

Hier gilt $2 = -\mathrm{i}(1+\mathrm{i})^2$, und der einzige Primteiler von 2 in $\mathbb{Z}[\mathrm{i}]$ ist die Assoziiertenklasse von $1+\mathrm{i}$. 2 ist assoziiert zum Quadrat eines Primelements.

Fall 2: p lässt nach Division durch 4 Rest 3.

Wäre hier p die Norm eines Primelements $a+b\mathrm{i}$, so folgte aus $p = a^2+b^2$, dass ohne Einschränkung a gerade und b ungerade ist (ansonsten wäre die Summe der Quadrate gerade), und $a = 2s, b = 2t+1$ liefert

$$a^2 + b^2 = 4(s^2 + t^2 + t) + 1.$$

Daher hat jeder Primteiler π von p die Norm p^2, und aus

$$p = z \cdot \pi$$

folgt $p^2 = N(p) = N(z) \cdot N(\pi) = N(z) \cdot p^2$, also $z\overline{z} = N(z) = 1$, und z ist eine Einheit. Das heißt, dass p selbst prim ist in $\mathbb{Z}[\mathrm{i}]$.

Fall 3: p lässt nach Division durch 4 Rest 1.

Hier sehen wir schnell Beispiele:

$$5 = 2^2 + 1^2,\ 13 = 3^2 + 2^2,\ 17 = 4^2 + 1^2,\ 29 = 5^2 + 2^2,$$

aber keine Gegenbeispiele. Wir werden in Kürze (siehe 3.2.12) zeigen, dass es eine Zahl $u \in \{0, \ldots, p-1\}$ gibt, sodass u^2+1 ein Vielfaches von p ist:

$$\exists u, k \in \{1, \ldots, p-1\} : u^2 + 1 = kp.$$

Ein Primteiler π von p in $\mathbb{Z}[\mathrm{i}]$ teilt daher auch $u+\mathrm{i}$ oder $u-\mathrm{i}$, und daher hat π als Norm einen Teiler von kp. Da aber nach den vorhergehenden Überlegungen die Norm von π ein Teiler von p^2 sein muss, ist die Norm ein gemeinsamer Teiler von kp und p^2, also p, denn 1 ist sie nicht und $k < p$.

In diesem Fall hat also p zwei nicht assoziierte Primteiler

$$a \pm \mathrm{i}b, a^2 + b^2 = p.$$

Hilfssatz 3.2.12 Nachtrag

Es sei p eine Primzahl die bei Division durch 4 Rest 1 lässt.

Dann gibt es eine Zahl $u \in \{1, \ldots, \frac{p-1}{2}\}$, sodass p ein Teiler von u^2+1 ist.

Beweis.

Wir müssen zeigen, dass es ein u gibt, für das die Restklasse von u^2+1 in $R=\mathbb{Z}/p\mathbb{Z}$ Null ist.

Wir betrachten dazu die Zahl $v=\frac{p-1}{2}!\in\mathbb{N}$. Nach Voraussetzung ist $\frac{p-1}{2}$ gerade, und daher $v=(-1)\cdot(-2)\cdot\ldots\cdot(-(p-1)/2)$.

Für $1\leq k\leq\frac{p-1}{2}$ gilt

$$\frac{p-1}{2}+k=p-(\frac{p-1}{2}-k+1),$$

also ist v modulo p dasselbe wie $\frac{p+1}{2}\cdot(\frac{p+1}{2}+1)\cdot\ldots\cdot(p-1)$. Daher folgt aus dem Rechnen im Restklassenring, dass v^2 und $(p-1)!$ denselben Rest bei Division durch p lassen.

Für jedes $a\in\{1,\ldots,p-1\}$ gibt es ein $b\in\{1,\ldots,p-1\}$, sodass ab bei Division durch p den Rest 1 lässt, denn a,p sind teilerfremd. Dieses b ist eindeutig bestimmt. Für $a=1$ ist $b=1$, für $a=p-1$ ist $b=p-1$, aber sonst gilt hier $a\neq b$. Denn: Aus $a=b$ folgt, dass p ein Teiler von a^2-1 ist, also schon $a-1$ oder $a+1$ teilt. Aber a liegt zwischen 1 und $p-1$.

Man kann also alle Faktoren in $(p-1)!$ außer 1 und $p-1$ so in Paaren gruppieren, dass das Produkt eines jeden Paares bei Division durch p Rest 1 lässt. Folglich lässt $(p-1)!$ denselben Rest wie $1\cdot(p-1)=p-1$, also Rest -1.

Nun weiß man also für v, dass v^2+1 durch p teilbar ist. Ersetze nun v durch ein $u=\pm v-kp,\ 0<u\leq\frac{p-1}{2}$. Dann haben wir die Behauptung. ◯

Folgerung 3.2.13 Summen zweier Quadrate

Eine natürliche Zahl n ist genau dann als Summe zweier Quadrate von ganzen Zahlen schreibbar, wenn für alle Primzahlen $p\in\mathbb{P}$, die bei Division durch 4 Rest 3 lassen, der Exponent $\mathrm{v}_p(n)$ in der Primfaktorzerlegung von n gerade ist.

Beweis. Die Zahl n ist genau dann Summe zweier Quadrate, wenn sie die Norm eines Elements $a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]\setminus\{0\}$ ist.

Nun schreibt man $a+b\mathrm{i}$ als Produkt von Primelementen in $\mathbb{Z}[\mathrm{i}]$ und überlegt sich mit 3.2.11, dass das Betragsquadrat eines Primfaktors entweder 2 oder eine Primzahl $p=4k+1$ oder das Quadrat einer Primzahl $p=4k+3$ ist. Das zeigt die Notwendigkeit der Bedingung.

Da die Faktoren, die es laut der Bedingung gibt, allesamt Normen in $\mathbb{Z}[\mathrm{i}]$ sind, ist diese wegen $|z\cdot w|^2=|z|^2\cdot|w|^2$ auch hinreichend. ◯

So ist 209 zwar kongruent zu 1 modulo 8, aber da $209=11\cdot19$ gilt, bleibt die Suche nach $a,b\in\mathbb{Z}$ mit $209=a^2+b^2$ vergebens.

Bemerkung 3.2.14 Restklassenkörper

a) Es sei R ein Hauptidealring. Für welche Ideale Rg ist der Restklassenring R/Rg ein Körper? Das ist genau dann der Fall, wenn g irreduzibel ist, denn genau dann ist jedes $a \notin Rg$ modulo g invertierbar.

b) Für eine Primzahl p bezeichnen wir mit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ den Körper mit p Elementen. Er hat $p-1$ Einheiten, wir können auch sagen:

$$\varphi(p) = p - 1.$$

Allgemein ist die Anzahl der teilerfremden Restklassen modulo p^n gegeben durch

$$\varphi(p^n) = (p-1)p^{n-1}.$$

Dabei ist φ Eulers φ-Funktion (siehe 3.1.20).

Die Rechenregel von dort lehrt uns dann noch allgemeiner, dass

$$\varphi(N) = \prod_{p|N} p^{\mathrm{v}_p(N)-1}(p-1) = N \cdot \prod_{p|N}(p-1)/p.$$

3.3 Zur Verteilung der Primzahlen

Hilfssatz 3.3.1 Noch einmal Euklid

Es gibt unendlich viele Primzahlen.

Beweis. Es sei $N \in \mathbb{N}$. Die Zahl

$$M := N! + 1$$

hat einen Primteiler, aber dieser kann nicht $\leq N$ sein, denn sonst müsste er mit $N!$ auch $1 = M - N!$ teilen. Also gibt es eine Primzahl $> N$. ◯

Hilfssatz 3.3.2 Lückenhaft

Es sei $k \in \mathbb{N}$. Dann gibt es eine natürliche Zahl M, sodass zwischen M und $M + k$ keine Primzahl liegt.

Beweis. Setze $M = (k+2)! + 2$. ◯

Nun könnte man fragen, wie sich bequem eine schöne Liste von Primzahlen erstellen lässt. Auch hier ist die Antwort schon über 2000 Jahre alt.

Bemerkung 3.3.3 Sieb des Eratosthenes[6]

Es sei $M \in \mathbb{N}$ eine natürliche Zahl. Betrachte

$$S_1 := \{n \in \mathbb{N} \mid 2 \leq n \leq M\}.$$

Die kleinste Zahl von S_1 ist $p_1 := 2$, eine Primzahl. Setze

$$S_2 := \{n \in S_1 \mid p_1 \text{ teilt nicht } n\}.$$

Das Minimum von S_2 ist $p_2 := 3$, eine Primzahl. Setze

$$S_3 := \{n \in S_2 \mid p_2 \text{ teilt nicht } n\}.$$

Das sind die Zahlen aus S_1, die keine Vielfachen von 2 oder 3 sind. Mache sukzessive so weiter: Setze $p_i = \min(S_i)$, solange dies nicht leer ist. Dann ist p_i eine Primzahl, sonst wäre es vorher schon als Vielfaches einer kleineren Zahl gestrichen worden. Setze weiter

$$S_{i+1} := \{n \in S_i \mid p_i \text{ teilt nicht } n\}.$$

Wenn schließlich S_{i+1} leer ist, dann gilt

$$\{p_1, p_2, \ldots, p_i\} = S_1 \cap \mathbb{P} = \{p \in \mathbb{P} \mid p \leq M\}.$$

Kleine Fußnote am Rande: Sobald $p_j > \sqrt{M}$ gilt, sind in S_j nur noch Primzahlen übrig, denn eine natürliche Zahl $n \geq 2$, die keine Primzahl ist, hat einen Teiler $\leq \sqrt{n}$. Man kann also hier schon mit dem Sieben aufhören. Dann ist

$$\{p_1, \ldots, p_j\} \cup S_j$$

die gesuchte Menge der Primzahlen $\leq M$.

Bemerkung 3.3.4 Ein Euler-Produkt

Leonhard Euler hat das folgende Argument für die Unendlichkeit der Menge der Primzahlen gegeben: Wenn es nur endlich viele Primzahlen $\{p_1, \ldots, p_k\}$ gäbe, $p_1 < p_2 < \ldots < p_k$, so betrachte die rationale Zahl

$$\begin{aligned} \prod_{i=1}^{k} \frac{1}{1-p_i^{-1}} &= \prod_{i=1}^{k} (\sum_{j_i=0}^{\infty} p_i^{-j_i}) \\ &= \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \cdots \sum_{j_k=0}^{\infty} p_1^{-j_1} \cdot p_2^{-j_2} \cdot \ldots \cdot p_k^{-j_k} \\ &= \sum_{n=1}^{\infty} \frac{1}{n}. \end{aligned}$$

[6] Eratosthenes, ca. 284-200 v.Chr.

Hier benutzen wir zunächst die geometrische Reihe und dann das Distributivgesetz in seiner Inkarnation als Cauchy[7]-Faltungsvorschrift für das (endliche) Produkt absolut konvergenter Reihen. Schließlich kommt wegen des Fundamentalsatzes der Arithmetik – wir haben ja alle Primzahlen ins Feld geführt! – die harmonische Reihe heraus, die bekanntlich divergiert. Ein Widerspruch!

Über Konvergenzfragen hat Euler sich übrigens nie sehr große Gedanken gemacht. Aber er hatte die entscheidende Einsicht, wie es geht, und mehr noch, wie sich die Dinge mit dieser Art von Argumentation quantitativ genauer fassen lassen. Wir wollen ihm noch etwas dabei zusehen.

Vorher sagen wir schon einmal, dass in der analytischen Zahlentheorie anstelle von ln immer log gesagt wird; so heißt hier der natürliche Logarithmus.

Außerdem lässt sich jede Zahl $n \in \mathbb{N}$ auf eindeutig bestimmte Art als Produkt einer Quadratzahl und einer quadratfreien Zahl schreiben, wobei quadratfrei heißt, dass es außer 1 keinen quadratischen Faktor gibt. Die 1 ist sowohl Quadratzahl als auch quadratfrei...

Die quadratfreien Zahlen sind also genau die Produkte von endlich vielen paarweise verschiedenen Primzahlen, ihre Liste fängt so an:

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, \ldots$$

Wenn $n = \prod_{p\in\mathbb{P}} p^{\mathrm{v}_p(n)}$ die Zerlegung von n als Produkt von Primzahlpotenzen ist, dann ist $f := \prod_{p\,:\,\mathrm{v}_p(n)\ \text{ungerade}} p$ der benötigte quadratfreie Faktor. In der natürlichen Zahl n/f kommt jeder Primfaktor mit einem geraden Exponenten vor, also ist diese Zahl ein Quadrat.

Hilfssatz 3.3.5 Noch eine Einsicht von Euler

Für jede reelle Zahl $x > 1$ gilt

$$\sum_{p\in\mathbb{P}, p\le x} \frac{1}{p} \geq \log(\log x) - \log 2.$$

Beweis. Wir betrachten zunächst

$$\log x = \int_1^x \frac{1}{t}\mathrm{d}t < \sum_{\mathbb{N}\ni n\le x} \frac{1}{n}$$

Andererseits ist (wenn wir $n = m^2 f$ mit quadratfreiem f als Faktor schreiben)

$$\sum_{n\le x} \frac{1}{n} \le \sum_{m\le\sqrt{x}} \frac{1}{m^2} \cdot \sum_{f\le x} \frac{1}{f} \le 2 \prod_{\mathbb{P}\ni p\le x} (1 + \frac{1}{p}) \le 2 \cdot \exp(\sum_{\mathbb{P}\ni p\le x} \frac{1}{p}),$$

[7] Augustin-Louis Cauchy, 1789-1857

denn $\exp(t) \geq 1 + t$ für reelles t.

Hier haben wir die Summe

$$\sum_{m \leq x} \frac{1}{m^2}$$

durch 2 abgeschätzt, was wegen

$$\frac{1}{m^2} < \frac{1}{m-1} - \frac{1}{m} \quad (m \geq 2)$$

und eines Teleskopsummenarguments legal ist.

Ziehen des Logarithmus aus der nun resultierende Ungleichung

$$\log x < 2 \exp(\sum_{p \leq x} \frac{1}{p})$$

liefert das gewünschte Ergebnis. ◯

Bemerkung 3.3.6 Die Verteilungsfunktion – der Primzahlsatz

Für eine reelle Zahl x sei

$$\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}.$$

Diese Funktion zählt also, wieviele Primzahlen unterhalb x es gibt.

Schon Euklid wusste also, dass $\lim_{x \to \infty} \pi(x) = \infty$.

Hätte man für die n-te Primzahl eine Abschätzung vom Typ

$$p_n \geq C \cdot n^{1/(1-\varepsilon)}, \quad n >> 0, C \text{ eine Konstante},$$

so würde dies die Konvergenz der Summe der Kehrwerte der Primzahlen nach sich ziehen. Also gibt es – wegen Eulers Lemma – solch eine Abschätzung nicht, und das zeigt, dass $\pi(x)$ zum Beispiel immer wieder größer sein muss als $x^{1-\delta}$ für jedes positive δ. Also sogar

$$\limsup_{x \to \infty} \pi(x) \frac{x^\delta}{x} = \infty.$$

Schon bei Lagrange, spätestens bei Gauß findet sich eine präzise Vermutung, wie schnell $\pi(x)$ ansteigt. Die Vermutung war

$$\lim_{x \to \infty} \pi(x) \cdot \frac{\log x}{x} = 1.$$

Das ist nach der Regel von L'Hospital[8] so äquivalent zur eigentlich von Gauß stammenden Formel

$$\lim_{x \to \infty} \pi(x) \cdot \frac{1}{\int_2^x (\log t)^{-1} \mathrm{d}t} = 1.$$

[8]Guillaume Francois Antoine L'Hospital, 1661-1704

Allerdings liefert der hier im Nenner stehende Integrallogarithmus ein besseres Konvergenzverhalten.

Dass Gauß den richtigen Riecher hatte wurde erst etwa 100 Jahre später bewiesen, und zwar mit Methoden der Funktionentheorie und unabhängig voneinander 1896 von Hadamard[9] und La Vallée-Poussin[10]. Sie benutzten beide die Riemannsche Zetafunktion, siehe 3.3.10d).

Noch einmal etwa 50 Jahre später gab es einen Beweis ohne Funktionentheorie, den sogenannten elementaren Beweis des Primzahlsatzes, der von Erdös[11] und Selberg[12] auch unabhängig erbracht wurde.

Eine kurze Abschweifung soll zeigen, was man mit solchen Aussagen wie dem Primzahlsatz anfangen kann.

Hilfssatz 3.3.7 Lückenlos

Es sei $\varepsilon > 0$ gegeben. Dann gibt es eine reelle Zahl x_0, sodass für alle $x \geq x_0$ im Intervall $[x, (1+\varepsilon)x]$ eine Primzahl existiert.

Beweis. Es bezeichne wie vorhin π die Primzahlzählfunktion. Für jedes $\delta > 0$ gilt nach dem Primzahlsatz für große x :

$$\frac{x}{\log x}(1-\delta) \leq \pi(x) \leq \frac{x}{\log x}(1+\delta).$$

Wir finden also für solche x insbesondere

$$\pi((1+\varepsilon)x) - \pi(x) \geq \frac{(1+\varepsilon)x}{\log((1+\varepsilon)x)}(1-\delta) - \frac{x}{\log x}(1+\delta).$$

Wenn wir

$$0 < \delta < \frac{\varepsilon}{2+\varepsilon}.$$

wählen, so geht die rechte Seite mit x gegen Unendlich, denn es gilt

$$\frac{(1+\varepsilon)x}{\log((1+\varepsilon)x)}(1-\delta) - \frac{x}{\log x}(1+\delta) = \left(\frac{(1+\varepsilon)(1-\delta)}{1+\frac{\log(1+\varepsilon)}{\log x}} - 1 - \delta\right) \cdot \frac{x}{\log x},$$

und der Ausdruck in Klammern geht für $x \to \infty$ gegen

$$\varepsilon - 2\delta - \varepsilon\delta > 0,$$

[9] Jaques Hadamard, 1865 - 1963
[10] Charles Jean Gustav Nicolas, Baron de La Vallée-Poussin, 1866-1962
[11] Paul Erdös, 1913 - 1996
[12] Atle Selberg, 1917 - 2007

wobei die Positivität aus der Einschränkung an δ resultiert.

Damit ist für großes x

$$\pi((1+\varepsilon)x) - \pi(x) > \frac{\varepsilon - 2\delta - \varepsilon\delta}{2} \frac{x}{\log x} \to_{x\to\infty} \infty,$$

und für große x liegt mindestens eine Primzahl zwischen x und $(1+\varepsilon)x$. ◯

Aus dem Hilfssatz ergibt sich zwanglos die

Folgerung 3.3.8 Ein Dichtheitssatz

Die Menge aller Brüche p/ℓ, wobei p und ℓ Primzahlen sind, ist dicht in $\mathbb{R}_{\geq 0}$.

Beweis. Wir zeigen, dass für positive reelle Zahlen $y < z$ stets mindestens ein Paar von Primzahlen p, ℓ existiert mit

$$y \leq \frac{p}{\ell} \leq z.$$

Denn dies ist gleichbedeutend mit

$$\ell y \leq p \leq \ell y(1 + \frac{z-y}{y}),$$

und nachdem man $\varepsilon := \frac{z-y}{y}$ gesetzt hat, sieht man aus dem letzten Hilfssatz, dass für hinreichend großes ℓ immer mindestens ein p mit der gewünschten Eigenschaft existiert. ◯

Definition 3.3.9 Arithmetische Funktionen

Eine *arithmetische Funktion* ist eine Abbildung $\alpha : \mathbb{N} \to \mathbb{C}$.

Die Menge $\mathcal{A} = \mathrm{Abb}(\mathbb{N}, \mathbb{C})$ aller arithmetischen Funktionen ist mit den üblichen Verknüpfungen ein komplexer Vektorraum.

Wir definieren eine weitere Verknüpfung – die *Faltung* – durch

$$* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}, (\alpha * \beta)(n) := \sum_{d|n} \alpha(d) \cdot \beta(n/d).$$

Das ist die Verknüpfung aus 2.3.14b), wobei wir $R = \mathbb{C}$ setzen und $(M, \diamond) = (\mathbb{N}, \cdot)$.

Wie dort in der allgemeinen Situation gesagt wird $(\mathcal{A}, +, *)$ ein kommutativer Ring. Das Einselement ist die Abbildung δ mit

$$\delta(n) := \begin{cases} 1, & \text{falls } n = 1, \\ 0, & \text{sonst.} \end{cases}$$

Eine arithmetische Funktion α heißt *strikt multiplikativ*, falls $\alpha(1) = 1$ gilt und $\forall m, n \in \mathbb{N} : \alpha(mn) = \alpha(m)\alpha(n)$.

Sie heißt *multiplikativ*, falls $\alpha(1) = 1$ gilt und

$$\forall m, n \in \mathbb{N} : \mathrm{ggT}(m, n) = 1 \Rightarrow \alpha(mn) = \alpha(m) \cdot \alpha(n).$$

Bemerkung 3.3.10 Einheiten und Dirichletreihen[13]

a) Die Einheiten in $\mathcal{A}$ sind genau die Folgen α mit $\alpha(1) \neq 0$. Der Beweis ist eine machbare Übungsaufgabe.

b) Die multiplikativen arithmetischen Funktionen bilden eine Untergruppe von $\mathcal{A}^\times$.

Insbesondere hat zum Beispiel die (sogar strikt) multiplikative arithmetische Funktion $\eta(n) = 1$ eine Inverse. Sie ist gegeben durch

$$\mu(n) = \begin{cases} 0, & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^k, & \text{falls } n = p_1 \cdot \ldots \cdot p_k,\ p_i \in \mathbb{P} \text{ paarweise verschieden.} \end{cases}$$

und heißt die Möbius[14]-Funktion. Diese ist übrigens nicht mehr strikt multiplikativ!

Speziell gilt für $\varphi, \psi \in \mathcal{A}$:

$$\varphi = \eta * \psi \iff \psi = \mu * \varphi.$$

Diese Formel heißt die Möbius-Inversionsformel. Machen Sie sich bewusst, was das konkret heißt!

c) Die Eulersche φ-Funktion ist multiplikativ (siehe 3.1.20), aber nicht strikt multiplikativ.

d) Für eine arithmetische Funktion $\varphi = (\varphi(n))_{n\in\mathbb{N}}$ bezeichnen wir mit

$$D(\varphi, s) := \sum_{n\in\mathbb{N}} \frac{\varphi(n)}{n^s}$$

die zugehörige *formale Dirichletreihe*. Falls diese für ein $\sigma \in \mathbb{R}$ konvergiert, so konvergiert sie auch für alle $s > \sigma$, und für alle $s > \sigma + 1$ konvergiert sie sogar absolut. In Wirklichkeit gilt das sogar für alle komplexen s mit $\mathrm{Re}(s) > \sigma + 1$.

Beispiel: Die *Riemannsche*[15] *Zetafunktion* $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$ konvergiert (überhaupt, und dann auch absolut) genau dann, wenn $\mathrm{Re}(s) > 1$.

[13] Johann Peter Gustav Lejeune Dirichlet, 1805-1859
[14] August Ferdinand Möbius, 1790-1868
[15] Bernhard Georg Friedrich Riemann, 1826-1866

e) Für zwei arithmetische Funktionen φ, ψ gilt formal

$$D(\varphi, s) \cdot D(\psi, s) = \sum_{m,n \in \mathbb{N}} \frac{\varphi(n) \cdot \psi(m)}{n^s m^s} = D(\varphi * \psi, s).$$

Diese Gleichheit gilt „wirklich“ für diejenigen Werte von s, wo die Dirichletreihen absolut konvergieren.

Zum Beispiel ist $1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n) n^{-s}$ für $\mathrm{Re}(s) > 1$.

f) Für eine multiplikative arithmetische Funktion φ und eine Primzahl p sei

$$\varphi_p(n) = \begin{cases} \varphi(n), & \text{falls } n = p^k,\ k \in \mathbb{N}_0, \\ 0, & \text{sonst.} \end{cases}$$

Das ist der *p-Anteil* von φ, und es gilt

$$\varphi = *_{p \in \mathbb{P}} \varphi_p.$$

Das liegt einfach am Fundamentalsatz der Arithmetik. Für jedes n sind nur endlich viele Primfaktoren beteiligt, und deshalb ist das scheinbar unendliche Faltungsprodukt rechter Hand in Wirklichkeit endlich.

e) impliziert dann – auf zunächst formaler Ebene –

$$D(\varphi, s) = \prod_{p \in \mathbb{P}} D(\varphi_p, s) = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{\varphi(p^k)}{p^{ks}}.$$

Diese stimmt im Fall der absoluten Konvergenz tatsächlich für die Funktion $D(\varphi)$. Statt $D(\varphi_p, s)$ ist es gebräuchlicher, $D_p(\varphi, s)$ zu schreiben. Diese Funktion heißt dann ein *Euler-Faktor* von $D(\varphi, s)$.

Bemerkung 3.3.11 Einige Aussagen zur Verteilung der Primzahlen

a) Neben dem Primzahlsatz an sich gibt es auch den Dirichletschen Primzahlsatz, der besagt, dass es für je zwei teilerfremde ganze Zahlen a, b (mit $a \neq 0$) unendlich viele Primzahlen der Gestalt $ak+b$, $k \in \mathbb{Z}$ gibt. Im Beweis benutzte er wesentlich Eigenschaften geeignet gewählter Dirichlet-Reihen, und das ist übrigens häufig eine Methode, um Aussagen zur Verteilung der Primzahlen zu beweisen.

Für $a \in \{1, 2, 3, 4, 6\}$ kann man Dirichlets Satz für alle relevanten Werte von b relativ elementar zeigen – im Wesentlichen muss man nur $b = \pm 1$ ansehen.

Für alle anderen Zahlen a gibt es mehr als 2 zu a teilerfremde Reste.

b) Es wird vermutet, dass es unendlich viele Primzahlen p gibt, für die auch $p+2$ eine Primzahl ist. Diese *Primzahlzwillingsvermutung* lässt sich auch quantifizieren, aber bisher nicht beweisen.

c) Es wird vermutet, dass sich jede gerade natürliche Zahl ≥ 4 als Summe zweier Primzahlen schreiben lässt. Dies ist die sogenannte Goldbach[16]-Vermutung.

d) Es ist mittlerweile bekannt, dass es für jedes $k \in \mathbb{N}$ natürliche Zahlen a, b gibt, sodass $b, a+b, 2a+b, \ldots, ka+b$ allesamt Primzahlen sind. Dieser Satz von Tao[17] und Green[18] war eine der Arbeiten, für die Tao im Jahre 2006 die Fields[19]-Medaille bekam.

Ein wichtiges Hilfsmittel im Umgang mit Primzahlen ist der folgende Hilfssatz.

Hilfssatz 3.3.12 Kleiner Satz von Fermat[20]

Es sei p eine Primzahl und $c \in \mathbb{Z}$. Dann ist p ein Teiler von $c^p - c$.

Beweis. Für $c = 0$ ist die Aussage wahr, und dann greift vollständige Induktion nach oben und unten:

Wenn die Aussage für c gilt, so auch für $c+1$, denn

$$\begin{aligned}(c+1)^p - (c+1) &= c^p + \sum_{i=1}^{p-1} \binom{p}{i} c^i + 1 - c - 1 \\ &= c^p - c + \sum_{i=1}^{p-1} \binom{p}{i} c^i\end{aligned}$$

und hier sind die Binomialkoeffizienten in der Summe alle durch p teilbar, also nach Annahme die ganze rechte Seite.

Genauso gilt sie auch für $c-1$ und damit für alle ganzen Zahlen. ◯

Bemerkung 3.3.13 Ein halber Euklid

Es sei p eine ungerade Primzahl, sodass sich eine ganze Zahl a findet, für die a^2+1 von p geteilt wird.

Dann ist die (multiplikative) Ordnung von $a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ gleich 4.

Nach dem Satz von Lagrange ist daher 4 ein Teiler von $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, also lässt p bei Division durch 4 Rest 1.

[16] Christian von Goldbach, 1690 - 1764
[17] Terence Tao, geb. 1975
[18] Ben Green, geb. 1977
[19] John Charles Fields, 1863-1932
[20] Pierre de Fermat, 1601-1665

Das können wir nutzen, um einzusehen, dass es unendlich viele Primzahlen gibt, die bei Division durch 4 Rest 1 lassen.

Denn für $N \geq 2$ ist jeder Primteiler p von $(N!)^2 + 1$ ungerade, $> N$ und lässt nach der vorangehenden Diskussion Rest 1 bei Division durch 4.

Genauso gibt es unendlich viele Primzahlen, die bei Division durch 4 Rest 3 lassen, denn $N! - 1$ tut dies für $N \geq 4$, und damit können nicht alle Primteiler Rest 1 lassen.

Es soll hier kurz angedeutet werden, wie analytische Hilfsmittel helfen, diese beiden Aussagen auf einmal zu sehen und noch zu verschärfen.

Bemerkung 3.3.14 Zwei Zetafunktionen[21]

Wir haben schon die Riemannsche Zetafunktion gesehen:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}, \ s > 1.$$

Für den Ring $R = \mathbb{Z}[\mathrm{i}]$ gibt es auch eine Zetafunktion, einen Spezialfall für die Klasse Dedekindscher Zetafunktionen, nämlich

$$\zeta_R := \sum_{r \neq 0}^{*} \frac{1}{N(r)^s} = \prod_{\pi \text{ prim}}^{*} \frac{1}{1 - N(\pi)^{-s}}, \ s > 1,$$

wobei die Summen und Produkte mit Sternchen bedeuten, dass über Assoziiertenklassen summiert (oder multipliziert) wird.

(Im Allgemeinen würde man hier Assoziertenklassen durch Ideale ersetzen, aber wir haben ja einen Hauptidealring...)

Als Vertreter der Assoziiertenklassen wählen wir hier die Elemente im ersten Quadranten mit Realteil > 0. Jedes Element aus $R \setminus \{0\}$ lässt sich durch Multiplikation mit einer Potenz von i in diese Menge schieben.

Die Produktformel bringt auch für R einfach den Fundamentalsatz der Arithmetik zum Ausdruck.

In 3.2.11 haben wir gelernt, wie die Primelemente in R mit den Primzahlen zusammenhängen. Wir können das Produkt für ζ_R auch schreiben als

$$\zeta_R(s) = \frac{1}{1 - 2^{-s}} \cdot \prod_{4|(p-1)} \left(\frac{1}{1 - p^{-s}}\right)^2 \cdot \prod_{4|(p-3)} \left(\frac{1}{1 - p^{-2s}}\right).$$

Das kommt daher, dass 2 genau einen Primteiler (von Norm 2) in R hat, die Primzahlen $p = 4k + 3$ in R prim bleiben, aber Norm p^2 bekommen, und die

[21] Dieser Punkt ist optional

Primzahlen $p = 4k+1$ in R in zwei nicht assoziierte Primfaktoren zerfallen, die beide Norm p haben.

Ein Argument von Dirichlet zeigt, dass sowohl $(s-1)\cdot\zeta(s)$ als auch $(s-1)\cdot\zeta_R(s)$ für $s \searrow 1$ gegen eine von Null verschiedene Zahl streben.

Genauer gilt für $s > 1$:

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} \geq \int_1^{\infty} \frac{1}{x^s} \mathrm{d}x = \frac{1}{s-1}.$$

Analog finden wir nach unten

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} \leq 1 + \int_1^{\infty} \frac{1}{x^s} \mathrm{d}x = 1 + \frac{1}{s-1},$$

also insgesamt

$$\lim_{s \searrow 1} (s-1)\zeta(s) = 1.$$

Etwas aufwendiger wird das für ζ_R, das wir erst einmal etwas konkreter als

$$\zeta_R(s) = \frac{1}{4} \sum_{(0,0) \neq (m,n) \in \mathbb{Z}^2} \frac{1}{(m^2+n^2)^s}$$

umschreiben. Das benutzen wir, um die Summanden abzuschätzen.

Wir schreiben die Zahlen m^2+n^2 der Größe nach sortiert auf, und zwar jede so oft, wie sie auftaucht:

$$0 < \gamma_1 \leq \gamma_2 \leq \gamma_3 \ldots$$

und erhalten

$$\zeta_R(s) = \sum_{k=1}^{\infty} \frac{1}{\gamma_k^s}.$$

Um jeden Punkt $(m,n) \in \mathbb{Z}^2$ denken wir uns nun ein achsenparalleles Quadrat mit Kantenlänge 1 und Mittelpunkt (m,n). Dieses liegt ganz im Kreis mit Mittelpunkt 0 und Radius r, sobald $r \geq \sqrt{m^2+n^2} + \frac{\sqrt{2}}{2}$.

Umgekehrt liegt der Kreis mit Mittelpunkt 0 und Radius r ganz in der Vereinigung dieser Quadrate für alle Punkte (m,n) mit $\sqrt{m^2+n^2} \leq r + \frac{\sqrt{2}}{2}$.

Es folgt

$$\pi \cdot (r - \frac{\sqrt{2}}{2})^2 \leq \#\{(m,n) \mid m^2+n^2 \leq r^2\} \leq \pi \cdot (r + \frac{\sqrt{2}}{2})^2.$$

Das zeigt, dass $\lim_{k\to\infty} k/\gamma_k = \pi$.

Dies wiederum impliziert erstens, dass $\zeta_R(s)$ für $s > 1$ konvergiert und zweitens, dass

$$\lim_{s \searrow 1}(s-1)\zeta_R(s) = \frac{\pi}{4}.$$

Nun schreiben wir $\mathbb{P}_i$, $i \in \{1, 3\}$ für die Menge aller Primzahlen, die bei Division durch 4 Rest i lassen, und erinnern wir uns an die Produktformel

$$\zeta_R(s) = \frac{1}{1-2^{-s}} \cdot \prod_{p \in \mathbb{P}_1} \frac{1}{(1-p^{-s})^2} \cdot \prod_{p \in \mathbb{P}_3} \frac{1}{1-p^{-2s}}.$$

Wäre nun $\mathbb{P}_1$ endlich, so wäre

$$\zeta_R(s) = \zeta(2s) \cdot \frac{1-2^{-2s}}{1-2^{-s}} \cdot \prod_{p \in \mathbb{P}_1} \frac{(1-p^{-2s})}{(1-p^{-s})^2}.$$

Dies konvergiert für $s = 1,$ und diese Konvergenz zeigt, dass

$$\lim_{s \searrow 1}(s-1)\zeta_R(s) = 0.$$

Ein Widerspruch.

Analog führt die Annahme, $\mathbb{P}_3$ sei endlich, zur Folgerung, dass

$$\lim_{s \searrow 1}(s-1)\zeta_R(s) = \infty,$$

was auch ein Widerspruch wäre.

Es müssen also sowohl $\mathbb{P}_1$ als auch $\mathbb{P}_3$ unendlich sein, und sogar vergleichbar viele Elemente $\leq x$ enthalten, damit nicht eine von beiden Klassen von Primzahlen das Konvergenzverhalten von $(s-1)\zeta_R(s)$ zu sehr dominiert.

Das ist eine Verschärfung der bloßen Aussage, beide Mengen seien unendlich.

3.4 Gleichungssysteme

Definition 3.4.1 Basen

Es sei A eine (additiv geschriebene) abelsche Gruppe. Dann heißt $B \subseteq A$ eine *($\mathbb{Z}$-)Basis* von A, wenn sich jedes $a \in A$ auf eindeutig bestimmte Art als

$$a = \sum_{b \in B} \lambda_b \cdot b, \ \lambda_b \in \mathbb{Z}, \text{ fast alle } \lambda_b = 0$$

schreiben lässt. Dabei heißt *fast alle* genauer: alle bis auf endlich viele.

Wir werden zumeist endliche Basen B betrachten, und dann kann man diesen Zusatz auch weglassen.

Wenn A eine Basis B hat, dann nennt man A auch eine *freie abelsche Gruppe über* B.

Ist dann G irgendeine abelsche Gruppe und $\varphi : B \to G$ eine Abbildung, so lässt sich diese Abbildung auf genau eine Art zu einem Gruppenhomomorphismus $\Phi : A \to G$ fortsetzen.

Bemerkung 3.4.2 Ohne jede Basis

a) Jede Basis einer freien abelschen Gruppe ist insbesondere über $\mathbb{Z}$ linear unabhängig, denn sonst könnte man die 0 auf zwei verschiedene Arten als Linearkombination schreiben.

b) Nicht jede abelsche Gruppe hat eine Basis. Zum Beispiel $\mathbb{Q}$ besitzt keine.

c) Die positiven rationalen Zahlen sind eine Gruppe bezüglich der Multiplikation. Als Gruppe wird sie von den Primzahlen erzeugt, die – wegen der Eindeutigkeit der Primfaktorzerlegung – eine Basis von $\mathbb{Q}_{>0}$ bilden.

d) Es ist nicht immer so, dass ein minimales Erzeugendensystem eine Basis sein muss, selbst wenn es eine solche gibt; auch eine maximale, linear unabhängige Teilmenge ist nicht immer eine Basis... es gibt keinen so einfachen Basisergänzungssatz wie in der Linearen Algebra.

   Die richtige Definition steht eben da oben, und das ist die Eigenschaft, mit der immer gearbeitet wird.

e) Eine Basis B von $\mathbb{Z}^n$ hat immer n Elemente, denn die Standardbasis und B sind dann beide auch $\mathbb{Q}$-Basen von $\mathbb{Q}^n$.

   Da jede abelsche Gruppe A mit einer endlichen Basis zu einem $\mathbb{Z}^r$ isomorph ist, ist die Anzahl der Elemente einer Basis eine Invariante von A. Sie heißt der *Rang* von A.

Hilfssatz 3.4.3 ... und dann doch!

Es seien $n \in \mathbb{N}_0$ und $A \subseteq \mathbb{Z}^n$ eine Untergruppe.

Dann hat A eine Basis aus höchstens n Elementen.

Beweis. Wir machen vollständige Induktion nach n.

Für $n = 0$ ist nichts zu zeigen (die leere Menge ist eine Basis von $\mathbb{Z}^0$), und für $n = 1$ ist die Aussage auch klar, denn entweder A ist $\{0\}$ oder nicht, und im zweiten Fall besteht A aus allen Vielfachen von $a_0 := \min\{x \in A \mid x > 0\}$. Also ist (wegen der Nullteilerfreiheit von $\mathbb{Z}$) $\{a_0\}$ eine Basis von A.

Nun sei die Behauptung wahr für n und A eine Untergruppe von $\mathbb{Z}^{n+1}$.

Weiter sei

$$\Phi : \mathbb{Z}^{n+1} \to \mathbb{Z},\ \Phi((z_1, \ldots, z_{n+1})^\top) = z_{n+1}.$$

Dann ist $\Phi(A)$ eine Untergruppe von $\mathbb{Z}$.

Fall 1: $\Phi(A) = \{0\}$. Dann ist A „in Wirklichkeit“ eine Untergruppe von $\mathbb{Z}^n \subset \mathbb{Z}^{n+1}$, und wir können die Induktionsannahme direkt für A benutzen.

Fall 2: $\Phi(A) \neq \{0\}$. Sei dann $x_0 > 0$ der positive Erzeuger von $\Phi(A)$.

Dann gibt es ein $b_0 \in A$, sodass $\Phi(b_0) = x_0$.

Nun sei $K := \text{Kern}(\Phi) = \{a \in A \mid \Phi(a) = 0\}$. Der Kern von Φ wird nun wieder mit $\mathbb{Z}^n$ identifiziert, und das zeigt, dass K eine Basis B aus höchstens n Elementen besitzt.

Dann gilt für $a \in A$:

$$a = \frac{\Phi(a)}{x_0} b_0 + (a - \frac{\Phi(a)}{x_0} b_0) = \frac{\Phi(a)}{x_0} b_0 + \sum_{b \in B} \lambda_b \cdot b$$

für geeignete ganze Zahlen $\lambda_b, b \in B$. Es ist klar, dass die Vorfaktoren hierbei eindeutig bestimmt sind (der Vorfaktor vor b_0 ergibt sich aus $\Phi(a) = \lambda_{b_0} \Phi(b_0)$, der Rest weil B linear unabhängig ist).

Also ist $B \cup \{b_0\}$ eine Basis von A und hat höchstens $n+1$ Elemente. ◯

Hilfssatz 3.4.4 Unimodulare Matrizen

Es sei $M \in \mathbb{Z}^{n \times n}$ gegeben. Dann sind äquivalent:

i) Die Spalten von M bilden eine Basis von $\mathbb{Z}^n$.

ii) Es gibt eine zu M inverse Matrix mit ganzzahligen Einträgen.

iii) $\det(M) = \pm 1$.

Matrizen, für die eine dieser Aussagen stimmt, heißen unimodulare Matrizen.

Beweis.

i) $\Rightarrow$ ii) Wenn die Spalten von M eine Basis von $\mathbb{Z}^n$ bilden, dann lassen sich die Standardbasisvektoren als ganzzahlige Linearkombinationen dieser Spalten schreiben, das heißt es gibt $v_1, \ldots, v_n \in \mathbb{Z}^n$ mit $Mv_i = e_i$. Die Matrix N mit Spalten $v_1, \ldots, v_n$ ist also zu M invers und ganzzahlig.

ii) $\Rightarrow$ iii) Aus $MN = E_n, M, N \in \mathbb{Z}^{n \times n}$, folgt

$$\det(M) \cdot \det(N) = \det(E_n) = 1,$$

also sind die ganzen Zahlen $\det(M)$ und $\det(N)$ Einheiten in $\mathbb{Z}$.

iii)$\Rightarrow$i)

Sei umgekehrt $\det(M) = \pm 1$. Das charakteristische Polynom

$$\mathrm{CP}_M(X) = \det(XE_n - M) = \sum_{i=0}^{n} a_i X^i$$

ist ein normiertes ganzzahliges Polynom mit konstantem Term $a_0 = \pm 1$ – das ist gerade die Bedingung an die Determinante von M.

Der Satz von Cayley-Hamilton[22] sagt dann, dass

$$\sum_{i=0}^{n} a_i M^i = 0,$$

und daraus folgt

$$M \cdot (\sum_{i=1}^{n} a_i M^{i-1}) = \sum_{i=1}^{n} a_i M^i = \pm E_n.$$

Die Matrix $\pm \sum_{i=1}^{n} a_i M^{i-1}$ ist also ganzzahlig und invers zu M, und damit sind insbesondere die Standardbasisvektoren von $\mathbb{Z}^n$ in der von den Spalten von M erzeugten Untergruppe von $\mathbb{Z}^n$. Diese Spalten erzeugen also $\mathbb{Z}^n$, und da sie linear unabhängig sind, bilden sie eine Basis. ◯

Definition 3.4.5 Nicht alles ist primitiv...

Es sei $v \in \mathbb{Z}^n$. Dann heißt der ggT der Einträge von v auch der *Inhalt* von v, kurz $\mathrm{Inh}(v)$.

Wenn der Inhalt von v 1 ist, dann heißt v auch ein *primitiver Vektor*.

Hilfssatz 3.4.6 Basisergänzung

Ein Vektor $v \in \mathbb{Z}^n$ ist genau dann ein Element einer Basis von $\mathbb{Z}^n$, wenn $\mathrm{Inh}(v) = 1$.

Beweis. Es sei $v \in B$, B eine Basis von $\mathbb{Z}^n$. Da dann $\mathrm{Inh}(v)$ ein Teiler der Determinante der unimodularen Matrix ist, deren Spalten die Elemente von B sind, ist $\mathrm{Inh}(v) = 1$.

Sei umgekehrt $\mathrm{Inh}(v) = 1$. Dann ist – wegen Euklid – 1 eine ganzzahlige Linearkombination der Einträge von v, also

$$\exists w \in \mathbb{Z}^n : w^\top \cdot v = 1.$$

[22] William Rowan Hamilton, 1805-1865

Analog zum Vorgehen im Beweis von 3.4.3 sei

$$K := \{u \in \mathbb{Z}^n \mid w^\top \cdot u = 0\}.$$

Dann findet sich wegen $x - (w^\top \cdot x) \cdot v \in K$

$$\mathbb{Z}^n = \mathbb{Z} \cdot v + K,$$

und $\mathbb{Z} \cdot v \cap K = \{0\}$, und die Hinzunahme von v zu einer Basis von K liefert eine Basis von $\mathbb{Z}^n$. ◯

Satz 3.4.7 Elementarteilersatz

Es seien F eine freie abelsche Gruppe vom Rang n und $U \subseteq F$ eine Untergruppe vom Rang r.

Dann gibt es eine Basis $\{b_1, \ldots, b_n\}$ von F und natürliche Zahlen $e_1 \mid e_2 \mid \cdots \mid e_r$, sodass

$$\{e_1 b_1,\ e_2 b_2, \ldots, e_r b_r\}$$

eine Basis von U ist.

NB: Dies ist ein ganz passabler Ersatz für den Basisergänzungsersatz.

Beweis. Ohne Einschränkung dürfen wir $F = \mathbb{Z}^n$ annehmen.

Wir machen wieder vollständige Induktion, dieses Mal aber nach r. Für $r = 0$ ist nichts zu zeigen.

Für $r = 1$ sei c ein Basisvektor von U und $e = \mathrm{Inh}(c)$. Dann ist $b_1 := c/e$ ein ganzzahliger Vektor vom Inhalt 1. Nach dem eben gesehenen lässt er sich also zu einer Basis von $\mathbb{Z}^n$ ergänzen. Das ist die Behauptung.

Es sei $r \geq 2$. Dann gibt es ein $c_1 \in U$ derart, dass $\mathrm{Inh}(c_1)$ unter den Inhalten von Elementen $\neq 0$ von U minimal ist. Sei e_1 der Inhalt von c_1. Insbesondere gibt es kein $u \in U$, dessen Inhalt ein echter Teiler von e_1 ist.

Wir wählen ein $w \in \mathbb{Z}^n$ mit $w^\top \cdot c_1 = e_1$. Das Element $b_1 := \frac{1}{e_1} c_1$ ist primitiv in $\mathbb{Z}^n$, und mit

$$K := \{u \in \mathbb{Z}^n \mid w^\top \cdot u = 0\}$$

gilt

$$U = U \cap \mathbb{Z}^n = U \cap (\mathbb{Z} \cdot b_1 + K) = \mathbb{Z} \cdot c_1 + (U \cap K).$$

Nach Induktionsvoraussetzung gibt es eine Basis $\{b_2, \ldots, b_n\}$ von K und Zahlen $e_2 \mid e_3 \mid \cdots \mid e_r$, sodass

$$c_2 := e_2 b_2, \ldots, c_r := e_r b_r$$

eine Basis von $K \cap U$ bilden.

Noch zu zeigen ist nun, dass e_1 ein Teiler von e_2 ist.

Sei dazu $v \in \mathbb{Z}^n$ mit $v^\top \cdot c_2 = e_2$ gegeben. Das geht, da b_2 ja primitiv ist und daher e_2 der Inhalt von $c_2 = e_2 b_2$ ist.

Dann ist aber e_1 ein Teiler von $v^\top \cdot c_1$, und wir ersetzen v durch

$$\tilde{v} := v - \frac{v^\top \cdot c_1}{e_1} w.$$

Dann gilt für w und $\tilde{v}$ sogar

$$w^\top c_1 = e_1, w^\top c_2 = 0, \quad \tilde{v}^\top c_1 = 0, \quad \tilde{v}^\top c_2 = e_2.$$

Nun sei $\mathrm{ggT}(e_1, e_2) = se_1 + te_2$ für geeignete $s, t \in \mathbb{Z}$. Dann folgt

$$\mathrm{Inh}(sc_1 + tc_2) \mid (w + \tilde{v})^\top (sc_1 + tc_2) = \mathrm{ggT}(e_1, e_2) \mid e_1.$$

Da aber e_1 unter den Inhalten der Elemente von U minimal gewählt war, folgt $\mathrm{Inh}(sc_1 + tc_2) = e_1$, und damit teilt e_1 auch e_2.

Damit ist der Satz gezeigt. ◯

Bemerkung 3.4.8 Elementarteiler

Die Zahlen $e_1, \ldots, e_r$ aus dem Satz sind eindeutig durch U festgelegt; das soll hier nicht allgemein vorgeführt werden. Sie heißen die *Elementarteiler* von U in F.

Für e_1 sieht man wegen $e_1 \mid e_i$, dass e_1 alle Vektoren $e_i b_i$, $1 \leq i \leq r$, teilt. Diese aber erzeugen U, und deshalb teilt e_1 alle Elemente von $U \subseteq F$. Aber keine Zahl, die größer ist als e_1 teilt $e_1 b_1$. Daher ist e_1 eindeutig bestimmt als der größte gemeinsame Teiler aller Elemente von U :

$$e_1 = \max\{d \in \mathbb{N} \mid d^{-1} U \subseteq F\}.$$

Im Fall $r = n$ kann man e_r durch die folgende Bedingung charakterisieren:

$$e_r = \min\{d \in \mathbb{N} \mid dF \subseteq U\}.$$

Der Elementarteilersatz hat auch folgende Formulierung:

Satz 3.4.9 Die Matrixversion

Es sei $M \in \mathbb{Z}^{n \times m}$ eine ganzzahlige Matrix. Dann gibt es unimodulare Matrizen $S \in \mathrm{GL}_n(\mathbb{Z})$, $T \in \mathrm{GL}_m(\mathbb{Z})$, sodass

$$S^{-1} M T = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \mathrm{diag}(e_1, \ldots, e_r), \; e_1 \mid e_2 \mid \cdots \mid e_r \neq 0.$$

Die Nullen hier stehen für Nullmatrizen der jeweils passenden Größe.

Beweis: Wir betrachten die Abbildung $\Phi : \mathbb{Z}^m \to \mathbb{Z}^n$, die durch Multiplikation mit M gegeben ist. Ihr Bild ist eine Untergruppe $U \subseteq \mathbb{Z}^n$, und hier gibt es also eine Basis $\{b_1, \ldots, b_n\} \subset \mathbb{Z}^n$ sowie die zugehörigen Elementarteiler $e_1 \mid e_2 \mid \cdots \mid e_r$, sodass $e_i b_i, 1 \leq i \leq r$, eine Basis von U ist. Wir schreiben diese Basisvektoren in dieser Reihenfolge in eine Matrix S, welche dann natürlich unimodular ist.

Wir wählen Elemente $v_i \in \mathbb{Z}^m$ mit $M \cdot v_i = e_i b_i, 1 \leq i \leq r$. Da die Bilder dieser Elemente eine Basis von U sind, gilt – analog wie wir das schon für Linearformen zweimal benutzt haben –

$$\mathbb{Z}^m = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r + \mathrm{Kern}(\Phi).$$

Weiter sind $v_1, \ldots, v_r$ linear unabhängig, und nur ihre triviale Linearkombination liegt im Kern von Φ. Wenn wir nun noch eine Basis $\{v_{r+1}, \ldots, v_m\}$ vom Kern von Φ wählen, dann ist $T = (v_1\ v_2\ \ldots\ v_m)$ unimodular und es gilt

$$MT = (e_1 b_1\ e_2 b_2\ \ldots e_r b_r\ 0\ 0 \ldots\ 0) = SE,$$

wobei E die Elementarteilermatrix auf der rechten Seite der Behauptung ist. ◯

Bemerkung 3.4.10 Lineare Gleichungssysteme

Der eben gelernte Satz hat für die Theorie der Linearen Gleichungssysteme über $\mathbb{Z}$ eine ähnliche Bedeutung wie die Gauß-Normalform im Fall von Körpern.

Will man $Mx = b$ lösen, so löst man stattdessen

$$S^{-1}MTy = S^{-1}b,$$

und rechnet diesen Lösungsraum zurück mithilfe T^{-1}. Dabei ist $S^{-1}MTy = S^{-1}b$ genau dann ganzzahlig lösbar, wenn für die Einträge von $S^{-1}b = (\beta_1, \ldots, \beta_n)^\top$ gilt, dass $\beta_i = 0$ für $i \geq r+1$ und $e_i \mid \beta_i$ für $1 \leq i \leq r$.

Für ganzzahlige Lineare Gleichungssysteme weiß man also ganz gut Bescheid, was die Lösungstheorie angeht.

Beispiel 3.4.11 Mal eines mit Zahlen

Was sind die Elementarteiler der Matrix

$$M := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}?$$

Klar, der Rang ist 2 und das Bild der Multiplikation mit M wird von den ersten beiden Spalten erzeugt. Die erste hat Inhalt 1 und taugt von daher als erster Basisvektor b_1, und $e_1 = 1$. Nun muss der zweite Erzeuger so abgeändert werden, wie es Satz 3.4.7 verlangt, das heißt, wir müssen erst eine Spalte $w \in \mathbb{Z}^3$ finden

mit $w^\top \cdot b_1 = 1$. Hier können wir zum Beispiel den ersten Standardbasisvektor benutzen. Wir müssen dann die zweite Spalte s_2 von M so um ein Vielfaches von $c_1 := b_1$ abändern, dass der neu erhaltene Vektor mit $w^\top$ Produkt 0 hat. Konkret:

$$c_2 := s_2 - (w^\top \cdot s_2) \cdot c_1 = (0 \ -3 \ -6)^\top.$$

Dann setzen wir

$$b_2 := \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix}$$

und erhalten $e_2 = 3$. Wir ergänzen b_1, b_2 durch $b_3 := (0\ 0\ 1)^\top$ zu einer Basis von $\mathbb{Z}^3$. Andererseits ist $c_1 = M \cdot (1\ 0\ 0)^\top$ und $c_2 = M \cdot (-2\ 1\ 0)^\top$, und der Kern der Multiplikation mit M wird von $(1\ -2\ 1)^\top$ erzeugt, womit wir die drei Spalten der anderen unimodularen Matrix erhalten. Wir sehen:

$$M \cdot \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & -1 & 0 \\ 7 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Als Folgerung aus dem Elementarteilersatz ergibt sich die folgende Aussage:

Folgerung 3.4.12 Struktursatz für endlich erzeugte abelsche Gruppen

Jede endlich erzeugte abelsche Gruppe ist ein direktes Produkt von zyklischen Gruppen.

Beweis. Es seien A eine endlich erzeugte abelsche Gruppe und S ein endliches Erzeugendensystem von A. Die Anzahl der Erzeuger sei n.

Dann gibt es einen surjektiven Homomorphismus von $\mathbb{Z}^n$ nach A, der die Standardbasis von $\mathbb{Z}^n$ auf S schickt. Es sei U der Kern dieses Homomorphismus. Dann ist A isomorph zu $\mathbb{Z}^n/U$, und wir müssen nur noch zeigen, dass diese Faktorgruppe direktes Produkt von zyklischen ist. Dazu seien $e_1, \ldots, e_r$ die Elementarteiler von U in $\mathbb{Z}^n$ und $b_1, \ldots, b_n$ eine Basis von $\mathbb{Z}^n$ wie im Elementarteilersatz. Es folgt

$$\mathbb{Z}^n/U \cong \mathbb{Z}^n/D\mathbb{Z}^n, \quad D = \mathrm{diag}(e_1, e_2, \ldots, e_r, 0, \ldots 0).$$

Per Induktion nach n macht man sich dann klar, dass

$$\mathbb{Z}^n/U \cong \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_r\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}. \qquad \bigcirc$$

Folgerung 3.4.13 Einheitengruppen von Körpern

Es sei K ein Körper und $G \subset K^\times$ eine endliche Untergruppe seiner Einheitengruppe.

Dann ist G zyklisch. ◯

Beweis. Es sei $\Pi : \mathbb{Z}^r \to G$ ein surjektiver Gruppenhomomorphismus. So etwas gibt es, da G endlich und kommutativ ist.

Es sei c die Kardinalität von G

Weiter sei U der Kern von Π. Dann hat U in $\mathbb{Z}^r$ Index c und wegen 3.4.7 Rang r. Wir bezeichnen wie gehabt die Elementarteiler mit $e_1 \mid e_2 \mid \cdots \mid e_r$ und sehen in 3.4.7, dass

$$c = e_1 \cdot \ldots \cdot e_r.$$

Für jedes $v \in \mathbb{Z}^r$ gilt $e_r v \in U$. Daher gilt für jedes $\zeta \in G$ auch $\zeta^{e_r} = 1$, und ganz G besteht aus Nullstellen von $X^{e_r} - 1$. Es folgt $e_r \geq c$, und da e_r auch ein Teiler von c ist, müssen die beiden Zahlen gleich sein. Insbesondere sind alle anderen Elementarteiler 1, und es folgt mit dem Beweis von 3.4.7, dass

$$G \cong \mathbb{Z}^r/U \cong \mathbb{Z}/e_r\mathbb{Z}.$$

Das ist eine zyklische Gruppe. ◯

Bemerkung 3.4.14 Nichtlinear?

Wir wissen nun, wie man lineare Gleichungssysteme über $\mathbb{Z}$ recht übersichtlich lösen kann.

Nun seien allgemeiner $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ Polynome. Dann ist man interessiert an der Menge der ganzzahligen Lösungen des Gleichungssystems

$$P_i(x_1, \ldots, x_n) = 0,\ 1 \leq i \leq m.$$

Solch ein System ganzzahliger Polynomgleichung heißt eine *Diophantische*[23] *Gleichung*. Im Allgemeinen ist es sehr schwer, sinnvolle Aussagen über die Struktur des Lösungsraums eines solchen Gleichungssystems zu machen.

Man ist an verschiedenen Fragen interessiert:

- Gibt es überhaupt eine Lösung?
- Gibt es unendlich viele ganzzahlige Lösungen?
- Wie viele ganzzahlige Lösungen (x_i) mit $\max\{|x_i| \mid 1 \leq i \leq n\} \leq N$ gibt es?

[23] Diophantos von Alexandria, ca. 250

- Lässt sich die letzte Frage wenigstens asymptotisch in den Griff bekommen?

Natürlich kann es keine ganzzahlige Lösung geben, wenn es nicht einmal eine reelle gibt. Das lässt sich bisweilen mit Methoden der Analysis ausschließen. Zum Beispiel hat die Gleichung

$$x^2 + y^2 = -5$$

keine Lösung in $\mathbb{Z}^2$.

Aber nicht immer, wenn es eine reelle Lösung gibt, muss es eine ganzzahlige geben. Man denke etwa an die Gleichung $x^2 + y^2 = 3$. Deren Unlösbarkeit in $\mathbb{Z}$ sieht man durch Ausprobieren, denn x, y müssten betragsmäßig $\leq \sqrt{3}$ sein.

Es gibt neben dem Körper der reellen Zahlen noch eine Reihe weiterer Körper, die *p-adischen Zahlen* (wobei p die Primzahlen durchläuft), die oftmals auch benutzt werden können, um die Existenz einer rationalen Lösung von Polynomgleichungen auszuschließen. Sie fassen in gewisser Weise Regelmäßigkeiten des Rechnens in Restklassenringen $\mathbb{Z}/(p^n)$ zusammen, wobei p eine feste Primzahl ist und n alle natürlichen Zahlen durchläuft.

Bemerkung 3.4.15 Schinzels Hypothese

Ein prominentes Beispiel für die Verquickung von Diophantischen Problemen und Fragen nach der Verteilung der Primzahlen ist *Schinzels*[24] *Hypothese*. Sie sagt folgendes aus:

Sind $P_1, \ldots, P_m \in \mathbb{Z}[X]$ (nichtkonstante) irreduzible Polynome in einer Variablen mit positiven Leitkoeffizienten, sodass keine Primzahl p alle Werte

$$P_1(k) \cdot \ldots \cdot P_m(k), \ k \in \mathbb{Z}$$

teilt, dann gibt es unendliche viele $k \in \mathbb{Z}$, sodass alle Werte

$$P_1(k), \ldots, P_m(k)$$

Primzahlen sind.

Im allgemeinen ist hier nichts affirmatives bekannt, was den hypothetischen Charakter dieser Aussage unterstreicht.

Zum Beispiel die Primzahlzwillingsvermutung ($P_1 = X, P_2 = X + 2$) ist ein Spezialfall hiervon. Oder auch (für $m = 1$) die bisher unbewiesene Vermutung, es gebe unendlich viele Primzahlen der Form $k^2 + 1$.

Der populärste Fall, in dem man weiß, dass Schinzels Hypothese zutrifft, ist der eines Polynoms der Gestalt $aX + b$ für teilerfremde natürliche Zahlen a, b. Dann ist Schinzels Hypothese gerade die Aussage, die laut Dirichlets Primzahlsatz zutrifft: es gibt unendlich viele Primzahlen, die bei Division durch a Rest b lassen.

Es gibt auch eine genau quantifizierte Version von Schinzels Vermutung.

[24] Andrzej Schinzel, geb. 1937

Beispiel 3.4.16 Pythagoräische[25] Tripel

Eine diophantische Gleichgun, bei der man sehr gut Bescheid weiß, soll hier diskutiert werde: Die Gleichung $x^2 + y^2 = z^2$.

Ein *pythagoräisches Tripel* ist ein von (0,0,0) verschiedenes Tripel $(a, b, c) \in \mathbb{Z}^3$ mit

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

Da die Vorzeichen von a, b, c keine Rolle spielen, können wir auch nach $a, b, c \in \mathbb{N}_0$ suchen. Da mit (a, b, c) auch $(a/g, b/g, c/g)$ ein pythagoräisches Tripel ist, wenn $g = \mathrm{ggT}(a, b, c)$ gilt, dürfen wir a, b, c als teilerfremd voraussetzen, sogar als paarweise teilerfremd, denn ein gemeinsamer Primteiler von zwei beteiligten Zahlen müsste auch die dritte teilen.

Wenn a, b beide ungerade sind, dann lässt $a^2 + b^2$ bei Division durch 4 Rest 2. Das geht also nicht, denn ein gerades Quadrat ist immer durch 4 teilbar. Wir dürfen annehmen, dass a ungerade und b gerade ist.

Die pythagoräischen Tripel entsprechen via

$$(a, b, c) \mapsto (a/c, b/c)$$

den rationalen Punkten auf dem Einheitskreis. Diese lassen sich – ausgehend vom Punkt $(1, 0)$ als (der zweite der) Schnittpunkte von Geraden der Gestalt

$$y = m(x - 1),\ m \in \mathbb{Q},$$

mit dem Kreis schreiben. Wenn man $m = \frac{z}{n}$ mit teilerfremden z, n schreibt und alles ausrechnet, was zu rechnen ist, kommt man auf die folgende Gestalt von pythagoräischen Tripeln:

Entweder zn ist gerade, dann ist

$$a = z^2 - n^2, b = 2zn, c = z^2 + n^2.$$

Oder zn ist ungerade, dann ist die teilerfremde Lösung (a, b, c) gegeben durch

$$a = (z^2 - n^2)/2, b = zn, c = (z^2 + n^2)/2.$$

Aber nun ist a gerade und b ungerade, also haben die beiden nur die Rollen getauscht.

Jedes primitive pythagoräische Tripel mit ungeradem a ist von der ersten Gestalt, wobei $n < z$ teilerfremde natürliche Zahlen sind, eine davon gerade, die andere ungerade.

Beispiele: (3,4,5), (5,12,13), (7,24,25) sind pythagoräische Tripel.

[25] Pythagoras von Samos, ca. 580 -500 v.Chr.

Viel interessanter als der Fall der Quadriken ist der der kubischen Polynome. Hier landet man schnell bei den elliptischen Kurven, die ein Treffpunkt von Algebraischer Geometrie, Zahlentheorie, Funktionentheorie und auch Kryptographie sind.

3.5 Sylowsätze

Definition 3.5.1 **p-Gruppe, Sylow[26]gruppen**

a) Es sei p eine Primzahl. Eine endliche Gruppe G heißt eine *p-Gruppe*, wenn ihre Kardinalität eine Potenz von p ist.

b) Es seien G eine endliche Gruppe und p eine Primzahl. Dann heißt eine Untergruppe U von G eine *p-Sylowgruppe*, wenn ihre Kardinalität gleich der maximalen Potenz von p ist, die die Ordnung von G teilt. Vermeintlich präziser (weil formellastig):

$$\#G = \#U \cdot f, \quad \#U = p^e, \ p \not| f.$$

Eine p-Sylowgruppe ist also wegen des Satzes von Lagrange zwangsläufig maximal unter den p-Untergruppen einer gegebenen Gruppe G. Da liegt doch die Frage nahe, ob die Umkehr hiervon auch gilt, was hieße, dass jede p-Untergruppe in einer p-Sylowgruppe enthalten sein müsste. Hierzu müssen wir zunächst einmal sehen, dass es Sylowgruppen überhaupt gibt.

Satz 3.5.2 Erster Sylowsatz

Es seien G eine endliche Gruppe und p eine Primzahl. Dann existiert in G mindestens eine p-Sylowgruppe.

Beweis. Wir schreiben $\#G = p^e \cdot f, \ p \not| f,$ und betrachten die Menge M aller Teilmengen von G mit Kardinalität p^e. Wir müssen zeigen, dass mindestens ein Element von M eine Gruppe ist. Dazu betrachten wir die folgende Operation von G auf M:

$$\forall g \in G, A \in M : g \bullet A := \{ga \mid a \in A\}.$$

Der Stabilisator von $A \in M$ hat höchstens p^e Elemente. Hat er nicht p^e Elemente, so ist sein Index ein Vielfaches von p. Wenn wir nun zeigen können, dass die Kardinalität von M kein Vielfaches von p ist, dann sagt die Bahnbilanzformel, dass es mindestens ein $A \in M$ geben muss, dessen Stabilisator p^e Elemente hat, also eine p-Sylowgruppe ist.

[26]Peter Ludwig Mejdell Sylow, 1832-1918

Aber

$$\#M = \binom{p^e \cdot f}{p^e} = \frac{p^e f \cdot (p^e f - 1) \cdot (p^e f - 2) \cdot \ldots \cdot (p^e f - p^e + 1)}{p^e \cdot (p^e - 1) \cdot (p^e - 2) \cdot \ldots \cdot (p^e - p^e + 1)},$$

und die Zahlen $p^e f - k$ und $p^e - k$ haben für $0 \leq k \leq p^e - 1$ denselben p-Anteil (nämlich den von k), sodass nach Kürzen keine p-Potenz mehr übrigbleibt. ◯

Satz 3.5.3 Zweiter Sylowsatz

Es seien G eine endliche Gruppe und p eine Primzahl. Weiter sei $\#G = p^e \cdot f$ die Zerlegung von $\#G$ in eine p-Potenz und eine Zahl f, die kein Vielfaches von p ist.

Dann gelten die folgenden Aussagen:

a) Jede p-Untergruppe H von G ist in einer p-Sylowgruppe von G enthalten.

b) Je zwei p-Sylowgruppen von G sind zueinander konjugiert.

c) Die Anzahl der p-Sylowgruppen ist ein Teiler von f.

d) Die Anzahl der p-Sylowgruppen von G lässt bei Division durch p Rest 1.

Beweis. Es sei S die Menge aller p-Sylowgruppen in G. G operiert durch Konjugation auf S:

$$\forall g \in G, P \in S : g \bullet P := \{gxg^{-1} \mid x \in P\}.$$

Weiter sei $P \in S$ eine beliebige p-Sylowgruppe. Der Stabilisator von P enthält P, also ist die Kardinalität der G-Bahn von P $(= (G : \mathrm{Stab}_G(P)))$ ein Teiler von f und damit zu p teilerfremd.

a) Da alle Untergruppen von H in H eine p-Potenz als Index haben, erzwingt die Bahnbilanzformel für die Aktion von H auf $G \bullet P$, dass wenigstens ein $\tilde{P} \in G \bullet P$ von H stabilisiert wird:

$$\exists g \in G : \forall h \in H : hgPg^{-1}h^{-1} = gPg^{-1} =: \tilde{P}.$$

Im Gruppenerzeugnis $U = \tilde{P}H$ von $\tilde{P}$ und H ist also $\tilde{P}$ ein Normalteiler.

Da nach dem Homomorphiesatz $\tilde{P}H/\tilde{P} \cong H/(H \cap \tilde{P})$ gilt, ist $\tilde{P}H/\tilde{P}$ eine p-Gruppe. Andererseits ist ihre Kardinalität ein Teiler von $\#G/\#\tilde{P} = f$, also teilerfremd zu p. Daher ist $\#[H/(H \cap \tilde{P})] = 1$, also $H \subseteq \tilde{P}$.

Das zeigt, dass H in einer p-Sylowgruppe enthalten ist.

b) Falls H in Teil a) schon eine Sylowgruppe ist, zeigt das Argument gerade, dass ein g existiert mit $H \subseteq gPg^{-1}$. Da H und gPg^{-1} dieselbe endliche Kardinalität p^e haben folgt Gleichheit.

c) Wegen b) ist S eine Bahn unter G, also (nach der Bahnbilanzformel) $\#S = (G : \mathrm{Stab}_G(P))$, und das teilt f, da P in seinem eigenen Stabilisator liegt.

d) Das Argument aus a) zeigt, dass P die einzige p-Sylowgruppe ist, in deren Stabilisator sie liegt. Zerlegt man nun S in seine Bahnen unter P, so heißt das: Es gibt genau einen Fixpunkt (nämlich P selbst), und alle anderen Bahnlängen sind durch p teilbar – das sagt die Bahnbilanzformel. ◯

Bemerkung 3.5.4 Eine Anwendung

Wir illustrieren eine mögliche Anwendung dieses Satzes. Es seien $p < q$ zwei verschiedene Primzahlen und G eine Gruppe der Ordnung $p \cdot q$. Sie besitzt genau eine q-Sylowgruppe Q, denn 1 ist der einzige Teiler von p, der bei Division durch q Rest 1 lässt. Diese q-Sylowgruppe Q ist also ein Normalteiler von G. Es sei P eine p-Sylowgruppe (davon gibt es vielleicht mehrere). P ist isomorph zu G/Q, und wir können P als Nebenklassenvertreter von Q in G wählen:

$$G = \{xy \mid x \in P, y \in Q\}.$$

Q und P sind beide zyklisch, da sie von Primzahlordnung sind. Es sei ξ ein Erzeuger von P und η ein Erzeuger von Q. Dann ist

$$G = \{\xi^a \eta^b \mid 0 \leq a \leq p-1,\ 0 \leq b \leq q-1\}.$$

Damit haben wir Q und P mit $\mathbb{Z}/q\mathbb{Z}$ bzw. $\mathbb{Z}/p\mathbb{Z}$ identifiziert.

Wenn wir uns jetzt noch merken, wie P durch Konjugation auf Q operiert, dann können wir G aus diesen Bausteinen rekonstruieren. Die Operation aber können wir für die Erzeuger schreiben als

$$\xi\eta\xi^{-1} = \eta^c,$$

es folgt allgemein

$$\xi^a \eta^b \xi^{-a} = \eta^{bc^a},$$

und damit können wir beliebige Produkte in G auf Produkte in P und Q zurückführen.

Dies ist ein Spezialfall des *semidirekten Produkts* zweier Gruppen.

Insbesondere erzwingt die Wohldefiniertheit der Aktion auf P, dass die Zahl c die Eigenschaft $c^p \equiv 1 \pmod{q}$ hat. Wenn also q modulo p nicht 1 ist, dann verbietet uns Lagrange (als Fermat verkleidet) die Möglichkeit einer nichttrivialen Operation, und ξ vertauscht mit η. In diesem Fall ist G also abelsch. Das trifft für jede Gruppe der Ordnung

$$15,\ 33,\ 35,\ 65,\ 77\ldots$$

zu.

Auf jeden Fall ist es so, dass eine Gruppe der Ordnung pq immer einen abelschen Normalteiler hat, sodass der Quotient auch abelsch ist. Dieses Phänomen wird vom Begriff der Auflösbarkeit verallgemeinert.

Bemerkung 3.5.5 S_5

Welche Untergruppen $G \subseteq S_5$ operieren transitiv auf $\{1,2,3,4,5\}$?

Wenn G so eine Untergruppe ist, dann ist ihr Ordnung wegen der Bahnbilanzformel ein Vielfaches von 5. Sie enthält also eine 5-Sylowgruppe von S_5, die natürlich Ordnung 5 hat und damit zyklisch ist. In S_5 gibt es 6 solcher 5-Sylowgruppen, und bis auf Konjugation darf ich mir wünschen, dass die vom 5-Zykel

$$\zeta := (1\ 2\ 3\ 4\ 5)$$

erzeugte Gruppe $F = \langle\zeta\rangle$ in G liegt.

Der Normalisator N dieser Gruppe (die größte Untergruppe von G, in der F normal ist, also der Stabilisator unter der Konjugationsoperation) hat 20 Elemente, denn sein Index in S_5 ist die Anzahl der 5-Sylowgruppen.

Der Zykel $\tau = (2\ 3\ 5\ 4)$ erfüllt $\tau^{-1}\zeta\tau = \zeta^3$, er liegt also in N, und weil seine Ordnung 4 ist, wird N von ζ und τ erzeugt. Da zwei Elemente der Ordnung 5 konjugiert sind, ist der Zentralisator von ζ laut Bahnbilanzformel eine Untergruppe vom Index 24 in S_5, ihre Ordnung ist also 5, und daher ist der Zentralisator von ζ gleich S.

Welche Kardinalität kann G haben? Zunächst einmal alle Vielfachen von 5, die Teiler von 120 sind:

$$5,\ 10,\ 15,\ 20,\ 30,\ 40,\ 60,\ 120.$$

Eine Untergruppe, die F enthält, enthält entweder nur eine oder alle 6 5-Sylowgruppen, wie uns Sylows zweiter Satz verrät.

Im ersten Fall ist es eine Untergruppe von N, die F enthält, und das sind genau die Gruppen F, $\langle\zeta,\tau^2\rangle$ und N.

Die anderen Gruppen enthalten alle 5-Sylowgruppen, also alle Elemente der Ordnung 5. Da sich jeder Dreizykel als Produkt von 5-Zykeln schreiben lässt, liegt damit A_5 in G, und dieses muss A_5 oder S_5 sein.

Wir sehen also, dass von den laut Lagrange möglichen Kardinalitäten genau 5 (nämlich 5,10,20,60,120) als Kardinalitäten von solchen Gruppen vorkommen, und bis auf Konjugation (also Umbenennung der Zahlen 1,2,3,4,5) kennen wir diese Gruppen. Untergruppen mit 15, 30 oder 40 Elementen gibt es nicht.

Eng mit diesem Beispiel verknüpft ist das Folgende.

Beispiel 3.5.6 A_5 **ist einfach**

Wir wollen uns überlegen, dass die alternierende Gruppe A_5 keinen Normalteiler außer A_5 und $\{\mathrm{Id}\}$ besitzt. Dazu sehen wir uns die Sylowgruppen in A_5 an. Die Gruppenordnung von A_5 ist $60 = 2^2 \cdot 3 \cdot 5$.

Die 3- und 5-Sylowgruppen sind also jeweils zyklisch, und der zweite Sylowsatz zeigt, dass es davon 10 bzw. 6 gibt (da es insbesondere mehr als eine gibt).

Die Anzahl der 2-Sylowgruppen ist 5, eine davon ist die Gruppe

$$V_4 = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4), (1\ 4)(2\ 3), \mathrm{Id}\}.$$

Sie heißt die Kleinsche Vierergruppe und ist ein abelscher Normalteiler von S_4 mit Quotientengruppe S_3.

A_5 wird von den Dreizykeln erzeugt (siehe 1.5.10). Da (zum Beispiel)

$$(1\ 2\ 3\ 4\ 5) \circ (1\ 3\ 2\ 5\ 4) = (1\ 4\ 2)$$

gilt, wird A_5 auch von den Fünfzykeln erzeugt.

Nun sei $N \lhd A_5$ ein Normalteiler mit mehr als einem Element.

Wenn die Ordnung von N durch $p \in \{3, 5\}$ teilbar ist, dann enthält N eine p-Sylowgruppe von A_5 und damit, da N normal ist, alle p-Sylowgruppen, also alle p-Zykel und damit ist $N = A_5$.

Andererseits ist die Ordnung von N keine Zweierpotenz; das Zentrum von A_5 ist nämlich trivial, und damit besteht N nicht nur aus zwei Elementen, und N kann auch keine 2-Sylowgruppe sein, da die alle zueinander konjugiert sind.

Es folgt $N = A_5$ wie behauptet.

Kapitel 4

Endliche Körper

4.1 Quadratische Reste

Bemerkung 4.1.1 Die Quadrategruppe

Es sei F ein endlicher Körper mit q Elementen und Charakteristik $p > 2$. Dann heißt ein Element $a \in F^\times$ ein *Quadrat* in F, wenn ein $b \in F$ existiert mit $b^2 = a$.

Die Menge der Quadrate ist also das Bild der Abbildung

$$Q : F^\times \to F^\times,\ b \mapsto b^2.$$

Diese Abbildung ist ein Gruppenhomomorphismus. Der Kern von Q besteht aus allen Elementen, deren Quadrat 1 ist, also aus ± 1. Da die Charakteristik nicht 2 ist, sind das 2 verschiedene Elemente. Jedes Element im Bild hat also laut Homomorphiesatz genau zwei Urbilder und $Q(F^\times) \cong F^\times/\{\pm 1\}$ hat genau $\frac{q-1}{2}$ Elemente.

Definition 4.1.2 Legendre[1]-Symbol

Es sei $p \geq 3$ eine Primzahl. Für $a \in \mathbb{Z}$ sei

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{falls } p \mid a, \\ 1, & \text{falls } \exists x \in \mathbb{Z} \setminus p\mathbb{Z} : a \equiv x^2 \pmod{p}, \\ -1, & \text{sonst.} \end{cases}$$

Das ist das klassische Legendre-Symbol.

Als Variante hiervon sei F ein endlicher Körper ungerader Charakteristik. Dann ist

$$\left(\frac{\cdot}{F}\right) : F \to \{-1, 0, 1\}$$

[1] Adrien-Marie Legendre, 1752 - 1833

definiert durch die Bedingung

$$\left(\frac{a}{F}\right) = \begin{cases} 0, & \text{falls } a = 0, \\ 1, & \text{falls } a \in Q(F^\times), \\ -1, & \text{sonst.} \end{cases}$$

Das heißt speziell für $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) = \left(\frac{a + p\mathbb{Z}}{\mathbb{F}_p}\right).$$

Hier werden die Zahlen 0 und ± 1 entweder als ganze Zahlen oder als Elemente des endlichen Körpers aufgefasst. Weil dieser ungerade Charakteristik hat, sind das auch in F drei verschiedene Elemente.

Hilfssatz 4.1.3 Von Euler

a) Es sei F ein endlicher Körper mit ungerader Charakteristik und q Elementen. Dann gilt für $a \in F$:

$$\left(\frac{a}{F}\right) = a^{\frac{q-1}{2}}.$$

b) Analog gilt für eine ungerade Primzahl p und $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

c) Die Abbildung $\left(\frac{\cdot}{F}\right) : F^\times \to \{\pm 1\}$ ist ein Gruppenhomomorphismus.

d) Die Abbildung $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{0, \pm 1\}$ ist strikt multiplikativ.

Beweis. Es ist klar, wie b) aus a) folgt.

Um a) zu zeigen, sehen wir erst ein, dass genau für $a = 0$ auch $a^{\frac{q-1}{2}} = 0$ gilt, also nur der Fall $a \neq 0$ interessant ist.

Wegen des kleinen Satzes von Lagrange ist hier $a^{\frac{q-1}{2}}$ eine Quadratwurzel von 1, also 1 oder -1. Wenn $a = b^2$ ein Quadrat ist, dann folgt $a^{\frac{q-1}{2}} = b^{q-1} = 1$, was die Hälfte der Aussage ist.

Wenn a kein Quadrat ist, wählen wir einen Erzeuger ζ der zyklische Gruppe (siehe 3.4.13) $F^\times$ und schreiben

$$a = \zeta^d$$

mit minimalem $d \in \mathbb{N}$. Dieser Exponent d ist ungerade (sonst wäre a ein Quadrat). Wäre nun $a^{\frac{q-1}{2}} = 1$, so wäre

$$\zeta^{d\frac{q-1}{2}} = 1 = \zeta^{q-1}.$$

Da der ggT von $d\frac{q-1}{2}$ und $q-1$ gerade $\frac{q-1}{2}$ ist, wäre damit auch $\zeta^{\frac{q-1}{2}} = 1$, was der Tatsache widerspricht, dass ζ Ordnung $q-1$ hat.

c) und d) sind unmittelbare Konsequenzen hieraus, wobei klar sein dürfte, was in d) mit strikt multiplikativ gemeint ist. ◯

Folgerung 4.1.4 Vorauseilende Ergänzung

Der erste Ergänzungssatz zum quadratischen Reziprozitätsgesetz ist gerade der folgende Spezialfall von Eulers Formel

$$\forall 2 \neq p \in \mathbb{P} : \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod 4, \\ -1, & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Definition 4.1.5 Halbheiten

a) Es sei F ein endlicher Körper. Ein *Halbsystem* in F ist eine Teilmenge $H \subseteq F^\times$, sodass

$$H \cap (-H) = \emptyset \text{ und } F^\times = H \cup (-H).$$

Zum Beispiel bilden die Restklassen von $1, 2, \ldots, \frac{p-1}{2}$ ein Halbsystem in $\mathbb{F}_p$, $p > 2$ prim.

b) Es sei H ein Halbsystem in F und $a \in F^\times$. Dann heißt

$$f(a, H) := |\{h \in H \mid ah \notin H\}|$$

die *Fehlstandszahl von a bezüglich H*.

Zum Beispiel sind für beliebiges H die Fehlstandszahlen

$$f(1, H) = 0, \ f(-1, H) = \frac{|F| - 1}{2}.$$

Etwas substanzieller ist das folgende Beispiel: Mit dem Halbsystem aus a) gilt für $a = 2 + p\mathbb{Z}$

$$f(a, H) = |\{x \in H | 2x \notin H\}| = \begin{cases} \frac{p-1}{4}, & \text{falls } p \equiv 1 \pmod 4, \\ \frac{p+1}{4}, & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Hilfssatz 4.1.6 Von Gauß

Es seien F ein endlicher Körper mit Charakteristik $p > 2$, $H \subset F^\times$ ein Halbsystem in F und $a \in F^\times$.

Dann gilt

$$\left(\frac{a}{F}\right) = (-1)^{f(a,H)}.$$

Beweis. Für $h \in H$ sei $\sigma(h) \in \{\pm 1\}$ das Vorzeichen, für das $\sigma(h) \cdot ah \in H$ gilt. Es ist also $\sigma(h) = 1$, wenn $ah \in H$ liegt, und sonst ist es -1. Es gibt also $f(a, H)$ Werte für $h \in H$ mit $\sigma(h) = -1$.

Daher haben wir wegen Euler

$$\left(\frac{a}{F}\right) \prod_{h\in H} h = a^{\frac{q-1}{2}} \prod_{h\in H} h = \prod_{h\in H} ah = \prod_{h\in H} \sigma(h)h = (-1)^{f(a,H)} \prod_{h\in H} h.$$

Das zeigt die Behauptung. ◯

Bemerkung 4.1.7 Zweite Ergänzung

Das Beispielmaterial aus 4.1.5 b) zeigt, dass für eine Primzahl $p \geq 3$ gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Denn genau für die p aus der ersten Zeile ist $f(2, H)$ gerade.

Beispiel: 2 ist quadratischer Rest modulo 7, denn 7 teilt $3^2 - 2 = 7$. Es ist kein quadratischer Rest modulo 5. Modulo 17 hingegen schon, denn 17 teilt $6^2 - 2 = 34$.

Frage: Kann man diese Folgerung benutzen, um zu zeigen, dass es unendlich viele Primzahlen gibt, die bei Division durch 8 Rest 1 oder -1 lassen?

Satz 4.1.8 Das quadratische Reziprozitätsgesetz

Es seien $p \neq \ell$ zwei ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{\ell}\right) \cdot \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}}.$$

Beweis.

Wir arbeiten mit dem Halbsystem $H = \{1, 2, 3, \ldots, \frac{p-1}{2}\}$ modulo p. Mit $f := f(\ell, H)$ gilt dann $\left(\frac{\ell}{p}\right) = (-1)^f$. Dabei ist

$$f = |\{x \in \{1, \ldots, \frac{p-1}{2}\} \subseteq \mathbb{Z} \mid \exists y \in \mathbb{Z} : -\frac{p}{2} < \ell x - py < 0\}|.$$

Beh.: Für solch ein y gilt immer $1 \leq y \leq \frac{\ell-1}{2}$.
Denn: $0 < y$ ist klar, und andererseits gilt

$$py < \ell x + \frac{p}{2} < \frac{p}{2}(\ell + 1);$$

Division durch p ergibt $y < \frac{\ell+1}{2}$, und weil ℓ ungerade ist, muss $y \leq \frac{\ell-1}{2}$ gelten.
Wir können also symmetrischer schreiben

$$f = |\{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} : -\frac{p}{2} < \ell x - py < 0\}|.$$

Analog gilt

$$\left(\frac{p}{\ell}\right) = (-1)^{f'},$$

wobei

$$f' = |\{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} : 0 < \ell x - py < \frac{\ell}{2}\}|.$$

Dann wissen wir wegen Gauß:

$$\left(\frac{\ell}{p}\right) \cdot \left(\frac{p}{\ell}\right) = (-1)^{f+f'}.$$

Nun ist aber

$$f + f' = |S|,$$

für die Menge

$$S := \{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} \text{ mit } -\frac{p}{2} < \ell x - py < \frac{\ell}{2}\}.$$

Zu zeigen bleibt noch, dass $F + F'$ dieselbe Parität hat wie $\frac{p-1}{2} \cdot \frac{\ell-1}{2}$.
Um das einzusehen, benutzen wir die Abbildung

$$\sigma : S \to S, \quad \sigma(x, y) = (\frac{p+1}{2} - x, \frac{\ell+1}{2} - y).$$

Das ist die Einschränkung der Punktspiegelung am Punkt $(\frac{p+1}{4}, \frac{\ell+1}{4})$ auf die Menge S. Daher gilt $\sigma^2 = \mathrm{Id}_S$, und $|S|$ hat dieselbe Parität, wie die Anzahl der Fixpunkte von σ – alle anderen Punkte lassen sich in disjunkten Zweiergrüppchen $\{P, \sigma(P)\}$ gruppieren.

Der einzig mögliche Fixpunkt ist aber $(\frac{p+1}{4}, \frac{\ell+1}{4})$, und der liegt genau dann in S, wenn sowohl p als auch ℓ modulo 4 zu 3 kongruent sind.

Daher ist $|S|$ ungerade genau dann, wenn $p \equiv \ell \equiv 3 \pmod 4$, und das zeigt die Behauptung. ◯

Bemerkung 4.1.9 Tratsch

a) Die Einsichten aus 4.1.4 und 4.1.7 heißen die beiden Ergänzungen zum quadratischen Reziprozitätsgesetz.

b) Schon Legendre hatte das Reziprozitätsgesetz gesehen, aber mit Hilfsmitteln bewiesen, die zu seiner Zeit noch nicht zur Verfügung standen, insbesondere benutzte er den Dirichletschen Primzahlsatz. Erst Gauß fertigte gleich einige Beweise an, die schon zum Entstehungszeitpunkt streng gültig waren.

c) Ausgehend vom quadratischen Reziprozitätsgesetz wurden noch andere Reziprozitätsgesetze entwickelt. Zum Einen konnte man statt des Ringes $\mathbb{Z}$ natürlich erst einmal andere Ringe verwenden. Für $\mathbb{F}_p[X]$ zum Beispiel war das Aufgabe 9.4 im Sommersemester 2008.

Zum Anderen kann man – wenn der Ring schon größer ist – vielleicht auch kubische Potenzreste untersuchen, zum Beispiel in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, oder biquadratische Potenzreste, z.B. in $\mathbb{Z}[\mathrm{i}]$.

Es entstand eine ganze Industrie, die Reziprozitätsgesetze fabrizierte, bis hin zum krönenden Abschluss: dem Artinschen Reziprozitätsgesetz in der abelschen Klassenkörpertheorie.

In gewisser Weise erhält unser letzter Satz erst von solch einem höheren Standpunkt aus eine Existenzberechtigung.

Erst einmal nehmen wir den Satz als eine Möglichkeit, zusammen mit den multiplikativen Eigenschaften und den Ergänzungssätzen Legendre-Symbole zu berechnen.

Meistens benutzen wir ihn in der Form

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right) \cdot (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}.$$

Beispiel 4.1.10 Zahlenbeispiele

$$\left(\frac{111}{41}\right) = \left(\frac{3}{41}\right)\cdot\left(\frac{37}{41}\right) = \left(\frac{41}{3}\right)\cdot\left(\frac{41}{37}\right) = \left(\frac{2}{3}\right)\cdot\left(\frac{4}{37}\right) = -1.$$

$$\left(\frac{113}{41}\right) = \left(\frac{31}{41}\right) = \left(\frac{10}{31}\right) = \left(\frac{2}{31}\right)\cdot\left(\frac{5}{31}\right) = (-1)^{\frac{31^2-1}{8}}\cdot\left(\frac{31}{5}\right) = 1.$$

Tatsächlich ist $20^2 - 113 = 7 \cdot 41$.

Für eine ungerade Primzahl $p \neq 5$ ist 5 modulo p ein Quadrat genau dann, wenn p modulo 5 ein Quadrat ist, also genau dann, wenn $p \equiv 1$ oder -1 modulo 5 gilt, also $p \in \{11, 19, 29, 31, 41, 59, 61, \dots\}$.

Für eine ungerade Primzahl $p \neq 3$ ist 3 modulo p ein Quadrat genau dann, wenn p modulo 3 ein Quadrat und außerdem 1 modulo 4 ist, oder wenn p modulo 3 kein Quadrat aber dafür selbst kongruent 3 modulo 4 ist, wenn es also ± 1 modulo 12 ist, also $p \in \{11, 13, 23, 37, 47, 59, 61, \dots\}$.

4.2 Restklassenkörper

Definition 4.2.1 Restklassenkörper

Es seien R ein kommutativer Ring und $M \subset R$ ein Ideal, sodass R/M ein Körper ist. Dann heißt R/M ein *Restklassenkörper* von R.

Definition/Bemerkung 4.2.2 Maximale Ideale

a) Es sei R ein kommutativer Ring. Ein Ideal $M \subset R$ heißt ein *maximales Ideal*, wenn $M \neq R$ gilt und außerdem kein Ideal existiert, das echt zwischen M und R liegt.

Das ist also ein maximales Element in der Menge aller von R verschiedenen Ideale.

b) Nun sei $I \subset R$ ein beliebiges Ideal. Dann gilt: I ist maximales Ideal genau dann, wenn R/I ein Körper ist.

Denn: Wenn I in R ein maximales Ideal ist, dann ist R/I nicht der Nullring (da $I \neq R$ gilt), und jedes von Null verschiedene Element in R/I ist invertierbar, da für $a \in R \setminus I$ gilt, dass das von I und a erzeugte Ideal gleich R ist (es ist ja größer als I), was heißt, dass es $x \in R$ und $i \in I$ gibt, sodass $1 = xa + i$, also

$$1 + I = (x + I)(a + I).$$

Wenn hingegen R/I ein Körper ist, dann ist $I \neq R$ und für jedes Ideal J zwischen I und R gilt:

$$J/I = \{I\} \quad \text{oder} \quad J/I = R/I,$$

da es im Körper R/I keine anderen Ideale gibt. Im ersten Fall folgt $J = I$, im zweiten Fall $J = R$.

Bemerkung 4.2.3 Konstruktion einiger Körper

a) Es sei F ein Körper. Dann wissen wir schon, dass der Polynomring $F[X]$ ein Hauptidealring ist. Er ist also nullteilerfrei und jedes Ideal wird von einem Polynom erzeugt, das bis auf Normierung eindeutig ist.

Nun sei $I = mF[X]$ von einem irreduziblen Polynom m vom Grad d erzeugt. Dann sagt 3.2.14, dass der Faktorring $F[X]/mF[X]$ ein Körper ist.

Die Restklasse von X in $F[X]/(m)$ ist dann eine Nullstelle von m. Wir können also gezielt einen Körper konstruieren, in dem ein gegebenes Polynom eine Nullstelle hat.

Dieser Gedanke wird in der Algebra weiterverfolgt.

b) Der Grad von m heiße jetzt d. In $K = F[X]/(m)$ wird jedes Element von einem Polynom repräsentiert, dessen Grad kleiner ist als d. Zwei solche Polynome sind modulo m unterschiedlich. Also ist K ein d-dimensionaler F-Vektorraum. Auch das kann man im Sinne der Algebra ausnutzen.

Bemerkung 4.2.4 Einige endliche Körper

a) Wenn in der gerade gemachten Bemerkung F endlich ist und q Elemente hat, dann folgt $|K| = q^d$, und wir erhalten einen neuen endlichen Körper, wenn $d > 1$.

b) Wer Matrizen liebt kann sich auch ein Modell im Ring der $d \times d$-Matrizen $F^{d\times d}$ verschaffen, indem er den kleinsten Teilring betrachtet, der F und die Begleitmatrix zu m enthält.

c) Zur Verdeutlichung wird hier ausgehend von $\mathbb{F}_2$ ein Körper mit 4 Elementen konstruiert. Dazu benutzen wir das irreduzible Polynom $m = X^2+X+1 \in \mathbb{F}_2[X]$. Die Restklassen modulo m werden durch $0, 1, X, X + 1$ vertreten.

Sei α die Restklasse von X. Dann haben wir die folgenden Verknüpfungstafeln in $\mathbb{F}_2[X]/(m)$:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

,

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Insbesondere ist das natürlich etwas ganz anderes als $\mathbb{Z}/4\mathbb{Z}$. Die Einheitengruppe ist zyklisch und wird von α erzeugt.

Nun wollen wir umgekehrt sehen, dass wir alle endlichen Körper als Restklassenkörper von $\mathbb{F}_p[X]$ erhalten, wenn p die Primzahlen durchläuft.

4.3 Endliche Körper

Hilfssatz 4.3.1 Primkörper, Einheitengruppe

Es sei F ein endlicher Körper. Dann gelten:

a) Die Charakteristik von F ist eine Primzahl p, und $\mathbb{Z}/p\mathbb{Z}$ ist ein Teilring von F.

b) Die Kardinalität von F ist eine Potenz von p.

c) Die Einheitengruppe von F ist zyklisch.

d) F ist ein Restklassenkörper des Polynomrings $\mathbb{F}_p[X]$.

Beweis. a) Das ist in 2.1.10 enthalten.

b) klar: F ist ja nun ein endlich dimensionaler $\mathbb{F}_p$-Vektorraum.

c) Das ist ein Fall für 3.4.13.

d) Es sei $\zeta \in F^\times$ ein Erzeuger. Die Abbildung

$$\Psi : \mathbb{F}_p[X] \to F, \Psi(f) := f(\zeta)$$

ist ein Homomorphismus von $\mathbb{F}_p$-Algebren. Weiterhin ist für alle $e \in \mathbb{Z}$ das Element $\zeta^e = \Psi(X^e)$ im Bild von Ψ. Da $\Psi(0) = 0$ gilt und ζ die Gruppe der von 0 verschiedenen Elemente erzeugt, ist Ψ surjektiv, und wir finden die Behauptung als Konsequenz des Homomorphiesatzes. ◯

Definition 4.3.2 Primitives Element, Minimalpolynom

Ein Element $\zeta \in F^\times$, das die Einheitengruppe erzeugt, heißt auch ein *primitives Element* von F. Die Anzahl der primitiven Elemente von F ist $\varphi(q-1)$, wobei q wieder die Kardinalität von F ist und φ die Eulersche Phi-Funktion.

Der normierte Erzeuger m des Kerns von Ψ im Beweis heißt das *Minimalpolynom* von ζ (über $\mathbb{F}_p$).

Es ist offensichtlich irreduzibel, denn $\mathbb{F}_p[X]/(m)$ ist ein Körper (und dann siehe 3.2.14).

Bevor wir gezielter nach irreduziblen Polynomen suchen, sammeln wir noch zwei Sachverhalte am Wegesrand mit ein.

Bemerkung 4.3.3 Artin[2]s Vermutung

a) Es ist nun klar, woher in 3.2.12 die Bedingung kommt, dass $p \equiv 1 \pmod 4$. Denn genau in diesem Fall hat ein Erzeuger ζ von $\mathbb{F}_p^\times$ eine durch 4 teilbare Ordnung, und da die Ordnung von -1 genau 2 ist (p ist ja ungerade), muss es eine Potenz von ζ^2 sein, also selbst ein Quadrat.

b) Eine noch immer unbewiesene Vermutung von Emil Artin sagt, dass es für jede ganze Zahl $a \neq -1$, die keine ganze Quadratwurzel in $\mathbb{Z}$ hat, unendlich viele Primzahlen p gibt, sodass $a + p\mathbb{Z}$ ein primitives Element in $\mathbb{F}_p$ ist.

[2]Emil Artin, 1898 - 1962

Dies ist für keine einzige Zahl a bewiesen. Schon der Fall $a = 2$ ist nicht klar.

Zum Beispiel für $p = 3$ ist $a = 2$ primitiv, die Potenzen sind $2^1 = 2$ und $2^2 = 4$.

Auch modulo 5 und 11 ist 2 primitiv.

Modulo $p = 7$ sind die Potenzen von 2 gerade $2, 4$ und $8 = 1$, d.h. 2 erzeugt nur eine Untergruppe vom Index 2 in $\mathbb{F}_7^\times$. Ein Erzeuger von $\mathbb{F}_7^\times$ ist zum Beispiel (die Restklasse von) 5.

Modulo 17 ist die Ordnung von 2 gleich 8, also ist 2 hier nicht primitiv und (letztes Beispiel) modulo 31 ist die Ordnung von 2 gleich 5, also erzeugt 2 modulo 31 nur eine Gruppe vom Index 6 in $\mathbb{F}_{31}^\times$.

Ein Resultat von Heath-Brown[3] sagt unter anderem, dass für höchstens zwei Primzahlen als Werte für a die Artin-Vermutung falsch ist. Solche Ergebnisse sehen immer bizarr aus, nicht wahr?

Hilfssatz 4.3.4 Zyklizität die zweite

a) Es sei $p \geq 3$ eine Primzahl und $m \in \mathbb{N}$ natürlich. Dann ist die Einheitengruppe von $R := \mathbb{Z}/p^m\mathbb{Z}$ zyklisch.

b) Für $p = 2$ und $m \in \mathbb{N}$ ist $(\mathbb{Z}/2^m\mathbb{Z})^\times$ genau dann zyklisch, wenn $m = 1$ oder 2. Für $m \geq 3$ ist die Einheitengruppe isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Beweis. Der Begriff Ordnung ist in diesem Beweis immer bezüglich der Multiplikation gemeint, nicht additiv.

a) Wir zeigen zunächst, dass in $R^\times$ ein Element ζ der Ordnung $p - 1$ liegt. Dies gilt, denn es gibt eine ganze Zahl a, die modulo p Ordnung $p-1$ hat, und damit ist die Ordnung modulo p^m ein Vielfaches $l(p-1)$ von $p-1$, und a^l hat Ordnung $p - 1$ in $R^\times$.

Nun sei ρ die Restklasse von $1+p$ in $R^\times$. Es ist klar, dass die Ordnung ein Teiler von p^{m-1} ist, denn ρ liegt im Kern des surjektiven Gruppenhomomorphismus von $R^\times$ nach $\mathbb{F}_p^\times$, der $x + p^m\mathbb{Z}$ nach $x + p\mathbb{Z}$ schickt.

Wir behaupten, dass ρ die Ordnung p^{m-1} hat.

Für $m = 1$ bzw. 2 sieht man sofort, dass die Ordnung von ρ tatsächlich 1 bzw. p ist.

Nun sei $m \geq 3$ und die Behauptung für alle kleineren Werte von m gezeigt. Wir müssen zeigen, dass die Ordnung von $(1+p)$ modulo p^m nicht schon p^{m-2} teilt.

Aber $1 + p$ hat modulo p^{m-1} Ordnung p^{m-2}, und das heißt unter Ausnutzung der Induktionsvoraussetzung für $m - 2$ insbesondere auch, dass

$$(1 + p)^{p^{m-3}} = 1 + kp^{m-2} \text{ für ein } k \notin p\mathbb{Z}.$$

[3] David Rodney „Roger“ Heath-Brown, geb. 1952

Dann ist aber

$$(1+p)^{p^{m-2}} = ((1+p)^{p^{m-3}})^p = 1 + kp^{m-1} + rp^m,$$

wobei der Rest rp^m alle übrigen Summanden aus der binomischen Formel aufsammelt.

Das zeigt die behauptete Ordnung von ρ.

Da $R^\times$ abelsch ist und ζ und ρ jeweils eine zyklische Untergruppe der Ordnung $p-1$ bzw. p^{m-1} erzeugen und diese Ordnungen teilerfremd sind, liegt in $R^\times$ eine Untergruppe, die zu

$$\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$

isomorph ist. Diese Gruppe hat $(p-1)\cdot p^{m-1}$ Elemente, ist also gleich $R^\times$. Nach dem Chinesischen Restsatz ist sie zyklisch, und wir sind fertig.

b) verbleibt als Übung. ◯

Bemerkung 4.3.5 Kreisteilungspolynom

a) Wir behalten die Notation von Hilfssatz 4.3.1 bei.

Wegen des Satzes von Lagrange ist ein Erzeuger ζ von $F^\times$ eine Nullstelle des Polynoms $X^{q-1}-1$. Dies ist auch ein ganzzahliges Polynom, und als solches wollen wir es erst einmal – und dann auch gleich allgemeiner – untersuchen.

b) Es sei also $N \in \mathbb{N}$ beliebig. Die komplexen Nullstellen von $Z_N = X^N - 1$ sind die Zahlen der Gestalt

$$c_k := \cos(\frac{2\pi k}{N}) + \mathrm{i}\sin(\frac{2\pi k}{N}), \quad 1 \le k \le N.$$

Für $g = \mathrm{ggT}(k,N)$ ist hierbei c_k schon eine Nullstelle von $Z_{N/g}$, was (siehe Partialsummen der geometrischen Reihe) ein Teiler von Z_N ist.

Die Idee ist nun, Z_N zu modifizieren zu

$$\Phi_N := \prod_{1\le k\le N}^{*} (X - c_k),$$

wobei das Produkt (mit Sternchen) nur noch über die zu N teilerfremden k läuft.

Φ_N heißt das *N-te Kreisteilungspolynom*, sein Grad ist $\varphi(N)$.

c) Man kann nun offensichtlich Φ_N auch rekursiv so gewinnen:

$$\begin{aligned} \Phi_1 &= X - 1 \\ \Phi_N &= (X^N - 1) : (\textstyle\prod_{d|N, d<N} \Phi_d) \end{aligned}$$

Es ist klar, dass das dieselben komplexen Polynome gibt. Andererseits sieht man hier rekursiv auch, dass die Φ_N sogar normierte ganzzahlige Polynome sind, deren konstanter Term gleich -1 ist für $N = 1,$ und sonst gleich 1.

Die Polynomdivision geht ganzzahlig auf, da der Leitkoeffizient des Nenners 1 ist.

d) Beispiel: Für $p \in \mathbb{P}$ gilt $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$.

Weiter haben wir zum Beispiel $\Phi_4 = X^2 + 1, \Phi_6 = X^2 - X + 1$ und so weiter.

e) Ohne Beweis halten wir fest, dass Φ_N über $\mathbb{Q}$ irreduzibel ist.

Hilfssatz 4.3.6 Nullstellen des Kreisteilungspolynoms

Es sei K ein Körper, dessen Charakteristik kein Teiler von $N \in \mathbb{N}$ ist.

Dann sind äquivalent:

i) In $K^\times$ liegt ein Element der Ordnung N.

ii) In K gibt es eine Nullstelle des Kreisteilungspolynoms Φ_N.

Beweis.

i) $\Rightarrow$ ii) Es sei $\zeta \in K^\times$ ein Element der Ordnung N. Dann hat $X^N - 1$ die N paarweise verschiedenen Nullstellen $1, \zeta, \zeta^2, \ldots, \zeta^{N-1},$ und diese verteilen sich brav auf die Faktoren von

$$X^N - 1 = \prod_{d|N} \Phi_d,$$

also bekommt auch Φ_N eine Nullstelle ab.

ii) $\Rightarrow$ i) Nun sei $\zeta \in K$ eine Nullstelle von Φ_N. Das ist keine mehrfache Nullstelle von $X^N - 1,$ denn aus $(X - \zeta)^2 \mid (X^N - 1)$ folgt

$$(X - \zeta) \mid \frac{X^N - 1}{X - \zeta} = X^{N-1} + \zeta X^{N-2} + \zeta^2 X^{N-3} + \cdots + \zeta^{N-2} X + \zeta^{N-1}.$$

Also wäre ζ eine Nullstelle des rechten Ausdrucks, der bei Einsetzen von ζ aber gerade $N\zeta^{N-1}$ liefert. Da ζ nicht 0 ist, folgt $N\zeta^{N-1} \neq 0,$ da die Charakteristik von K kein Teiler von N ist.

Da für jeden echten Teiler d von N das Produkt $\Phi_N \cdot (X^d - 1)$ ein Teiler von $X^N - 1$ ist, haben die zwei Faktoren keine gemeinsame Nullstelle, und deshalb ist die Ordnung von ζ größer als d. Sie muss also N sein. ◯

Folgerung 4.3.7 Spezialfall von Dirichlets Primzahlsatz

Es sei $N \in \mathbb{N}$ beliebig.

Dann gibt es unendlich viele Primzahlen $p \equiv 1 \pmod{N}$.

Beweis. Ohne Einschränkung sei $N > 1$.

Für $e \in \mathbb{N}$ sei $M = (N + e)!$

Das N-te Kreisteilungspolynom Φ_N ist normiert, ganzzahlig, nichtkonstant und hat konstanten Term 1. Daher ist für großes e die natürliche Zahl

$$L := \Phi_N(M)$$

zu M teilerfremd (nämlich kongruent zu 1 modulo M) und größer als M.

Es sei p ein Primteiler von L. Dann ist N kein Vielfaches von p, und die Restklasse von M modulo p ist eine Nullstelle von Φ_N in $\mathbb{F}_p$. Nach dem letzten Hilfssatz hat diese Restklasse Ordnung N in $\mathbb{F}_p^\times$. Wegen des Satzes von Lagrange ist also $p - 1$ ein Vielfaches von N, was nichts anderes heißt als

$$p \equiv 1 \pmod{N}.$$

Außerdem ist p größer als M, und da dies für alle großen e geht, folgt die Behauptung. ◯

In 4.3.1 haben wir gesehen, dass die Kardinalität eines endlichen Körpers immer Potenz einer Primzahl ist. Nun gehen wir den umgekehrten Weg und zeigen:

Hilfssatz 4.3.8 Alle endlichen Körper

Es sei p eine Primzahl und $e \in \mathbb{N}$. Dann gibt es einen Körper mit p^e Elementen und je zwei solche Körper sind zueinander isomorph.

Beweis. Es sei $q = p^e$ und $N = q - 1$. Dann zerlegen wir das Kreisteilungspolynom Φ_N in $\mathbb{F}_p[X]$ in irreduzible Faktoren und wählen einen davon. Er heiße m und habe Grad d.

Dann ist $F := \mathbb{F}_p[X]/(m\mathbb{F}_p[X])$ ein Körper, der p^d Elemente enthält. Außerdem liegt in F eine primitive N-te Einheitswurzel, und es muss $q \leq p^d$ gelten.

Für die Restklasse ξ von X in F gilt $\xi^{q-1} = 1$, also $\xi^q = \xi$. Da F von $\mathbb{F}_p$ und ξ als Körper erzeugt wird, folgt aus den binomischen Formeln, und weil in F die Gleichung $p = 0$ gilt, dass alle Elemente $a \in F$ die Gleichung

$$a^q = a$$

erfüllen.

Demnach besteht F aus höchstens q Elementen (Nullstellen eines Polynoms vom Grad q in einem Körper!), was insgesamt $|F| = q$ zeigt.

Wenn $\widetilde{F}$ ein weiterer Körper mit q Elementen ist, dann findet sich in ihm auch eine Nullstelle von Φ_N, denn die Einheitengruppe ist zyklisch und besteht aus N Elementen. Es folgt dann, dass Φ_N über $\widetilde{F}$ in Linearfaktoren zerfällt, also auch unser alter Faktor m eine Nullstelle in $\widetilde{F}$ besitzt. Das Argument aus 4.3.1 d) zeigt dann, dass $\widetilde{F}$ zu F isomorph ist. ◯

Bemerkung 4.3.9 Noch mehr Galois[4]felder

Der eindeutig bestimmte Körper mit $q = p^e$ Elementen wird oft als $\mathbb{F}_q$ notiert, von Informatikern auch gerne als $GF(q)$.

Wenn $\zeta \in \mathbb{F}_q$ ein Element ist und m sein Minimalpolynom über $\mathbb{F}_p$, dann zerfällt m über $\mathbb{F}_q$ in paarweise verschiedene Linearfaktoren, denn m teilt $X^q - X$, und dies zerfällt auch.

Die Nullstellen von m sind genau $\zeta, \zeta^p, \zeta^{p^2} \ldots, \zeta^{p^{d-1}}$, wenn d der Grad von m ist.

Der Automorphismus Frob von $\mathbb{F}_q$, der durch $\mathrm{Frob}(x) := x^p$ gegeben ist, heißt der *Frobenius*[5]*automorphismus* von $\mathbb{F}_q$. Jeder Automorphismus ist eine Potenz von diesem. Ist $f \in \mathbb{F}_p[X]$ ein Polynom und $a \in \mathbb{F}_q$ eine Nullstelle von f, so ist auch $a^p = \mathrm{Frob}(a)$ eine Nullstelle von f. (Das ist ein Pendant zur Tatsache, dass mit jeder komplexen Nullstelle eines reellen Polynoms auch die komplex konjugierte Zahl eine Nullstelle ist.) Es gilt sogar, dass ein irreduzibles normiertes Polynom $f \in \mathbb{F}_p[X]$ vom Grad d immer von der Gestalt

$$(X - \alpha) \cdot (X - \alpha^p) \cdot \ldots \cdot (X - \alpha^{p^{d-1}})$$

ist, wobei α irgendeine Nullstelle von f in $\mathbb{F}_{p^d}$ bezeichnet. Dass die entsprechenden Potenzen von α auch Nullstellen sind, wurde gerade gesagt, weiter ist $\alpha^{p^d} = \alpha$, da $\alpha \in \mathbb{F}_{p^d}$ gilt, und die aufgeschriebenen Potenzen sind paarweise verschieden, denn aus $\alpha^{p^a} = \alpha^{p^b}, 0 \leq a < b \leq d-1$, folgt

$$(\alpha^{p^a})^{p^{b-a}} = \alpha^{p^a},$$

also $\alpha^{p^a} \in \mathbb{F}_{p^{b-a}}$, aber das Minimalpolynom von α^{p^a} ist ja f und hat Grad d, was einen Widerspruch liefert.

Jeder Teilkörper von $\mathbb{F}_q$ ist ein „Fixkörper“ einer Potenz von Frob, und auf diese Art entsprechen die Teilkörper bijektiv den Untergruppen der Automorphismengruppe von $\mathbb{F}_q$. Das ist ein Spezialfall des Hauptsatzes der Galoistheorie, den man in der Algebra kennen lernt.

Insbesondere liegt $\mathbb{F}_{p^e}$ genau dann in $\mathbb{F}_{p^d}$, wenn e ein Teiler von d ist.

Bemerkung 4.3.10 Noch ein Primzahlsatz

Es sei p eine Primzahl. Für jedes $d \in \mathbb{N}$ gibt es nur endlich viele normierte irreduzible Polynome vom Grad d in $\mathbb{F}_p[X]$.

Wie viele?

Es sei N_d ihre Anzahl.

[4]Evariste Galois, 1811-1832

[5]Georg Ferdinand Frobenius, 1849 - 1917

Für $d = 1$ gilt $N_1 = p$, denn die Polynome sind $X - a,\ a \in \mathbb{F}_p$.

Für $d = 2$ gilt $N_2 = \frac{p^2-p}{2}$, denn hier sind die gesuchten Polynome gerade die Minimalpolynome der Elemente $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, also von der Gestalt $(X-a)(X-a^p)$.

Analog ist $N_3 = \frac{p^3-p}{3}$.

Hingegen findet sich $N_4 = \frac{p^4-p^2}{4}$, denn hier liefern nur die Minimalpolynome von $a \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$ etwas, und je vier solcher Elemente teilen sich das Minimalpolynom.

Für allgemeines d hat ein Element in $\mathbb{F}_{p^d}$ ein Minimalpolynom über $\mathbb{F}_p$, dessen Grad t ein Teiler von d ist, denn es liegt dann in $\mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^d}$. Je t dieser Elemente haben dasselbe Minimalpolynom. Und jedes irreduzible Polynom vom Grad $t \mid d$ in $\mathbb{F}_p[X]$ hat t Nullstellen in $\mathbb{F}_{p^d}$.

Das zeigt

$$p^d = \sum_{t|d} t \cdot N_t,$$

und mit der Möbius-Inversionsformel folgt

$$N_d = \frac{1}{d} \sum_{t|d} \mu(t) p^{d/t},$$

wobei μ die Möbiussche μ-Funktion aus 3.3.10b) ist.

Index

Symbolverzeichnis

$\langle\cdot\rangle$	1.1.3, 1.2.7	Erzeugnis
$\leq$	1.2.3	Untergruppe
δ_m	2.3.1	Kronecker-(Dirac-)Delta, Basiselement im Monoidring
$\mathbb{F}_q$	4.3.9	endlicher Körper
φ	3.1.20	Eulersche φ-Funktion
Φ_n	4.3.5	Kreisteilungspolynom
$(G : H)$	1.2.12	Gruppenindex
G/U	1.4.1	Faktormenge
π_U	1.4.1	kanonische Projektion
$R^\times$	2.1.5	Einheitengruppe des Rings R
$R[a]$	2.3.10	Algebrenerzeugnis
$R[M]$	2.3.1	Monoidring
$R[X]$	2.3.2	Polynomring
S_d	1.1.4	symmetrische Gruppe
$\mathrm{Abb}(D, D)$	1.1.2	Abbildungen von D nach D
$\mathrm{Abb}(M, R)_0$	2.2.2	Abbildungen von M nach R mit endlichem Träger
$\mathrm{Aut}(\cdot)$	1.1.5, 1.3.6	Automorphismengruppe
$\mathrm{Aut}(A\|R)$	2.3.8	R-Algebren-Automorphismen
$\mathrm{char}(R)$	2.1.10	Charakteristik von R
$\deg(f)$	2.3.2	Grad des Polynoms f
$\mathrm{End}(\cdot)$	1.1.5, 1.3.6	Endomorphismen
$\mathrm{Hom}(\cdot, \cdot)$	1.1.5, 1.3.1	Homomorphismen
sign	1.5.9	Signum
$\mathrm{Stab}_G(m)$	1.5.5	Stabilisator von m unter G
$\mathrm{Sym}(\cdot)$	1.1.4	symmetrische Gruppe
$\tau_{y,z}$	1.1.4	Transposition
$\mathbb{Z}/n\mathbb{Z}$	1.2.2, 2.1.2	Restklassengruppe oder -ring

Stichworte