Algebra I

von Jakob Neumann

Basierend auf der gleichnamigen Vorlesung von Harald Grobner

Wintersemester 2025/26

Das Skriptum wurde außerhalb der Vorlesung selbstständig zusammengestellt und um zusätzliche Erklärungen, Klarstellungen sowie ergänzendes Material aus eigenem Interesse erweitert. Etwaige Fehler oder Fehlinterpretationen gehen vollständig auf mich zurück.

Inhaltsverzeichnis

1 Ringe und Arithmetik

1 Die Arithmetik der ganzen Zahlen

Definition 1.1. Seien $a, b \in \mathbb{Z}$ ganze Zahlen. Dann ist a ein *Teiler* von b, falls eine ganze Zahl $k \in \mathbb{Z}$ existiert, sodass $ak = b$. Wir schreiben außerdem $a \mid b$, in Worten, „a teilt b“.

Proposition 1.1. Die Teilerrelation $\mid$ ist auf den ganzen Zahlen eine Quasiordnung.

Beweis. Seien $a, b, c \in \mathbb{Z}$ ganze Zahlen. Offenbar gilt, dass $a \mid a$, also ist die Teilerrelation reflexiv. Falls $a \mid b$ und $b \mid c$, dann gibt es $k_1, k_2 \in \mathbb{Z}$ mit $ak_1 = b$ und $bk_2 = c$. Es folgt, dass $c = bk_2 = (ak_1)\, k_2 = a\,(k_1\, k_2)$, i.e. $a \mid c$. Somit ist die Teilerrelation reflexiv und transitiv, damit eine Quasiordnung. □

Es sei angemerkt, dass die Teilerrelation auf den natürlichen Zahlen sogar eine Halbordnung ist, was bei den ganzen Zahlen nicht der Fall ist. Sind a und b ganze Zahlen mit $a \mid b$ und $b \mid a$ folgt nämlich nicht unbedingt, dass $a = b$. Allerdings gilt schon, dass $|a| = |b|$. Wir halten dies fest:

Lemma 1.1. Seien $a, b \in \mathbb{Z}$. Dann gilt:

(1) Die einzige ganze Zahl, die von 0 geteilt wird, ist 0 selbst.

(2) Ist a ein Teiler von b, dann gilt $|a| \leq |b|$.

(3) Falls $a \mid b$ und $b \mid a$, so folgt $|a| = |b|$.

(4) Falls $a \mid 1$, folgt dass $|a| = 1$.

Beweis. (1) Diese Aussage folgt sofort.

(2) Falls $a \mid b$, existiert $k \in \mathbb{Z}$ mit $ak = b$, sodass $|a|\,|k| = |ak| = |b|$, also $|a| \leq |b|$.

(3) Wir wenden (2) an, um einerseits $|a| \leq |b|$ zu erhalten und andererseits $|b| \leq |a|$. Daraus folgt nun, dass $|a| = |b|$.

(4) Da offenbar $1 \mid a$ gilt, folgt aus (3), dass auch $|a| = 1$ gelten muss. □

Lemma 1.2. Sei $a \in \mathbb{Z}$ ein Teiler von $b_1, \ldots, b_n \in \mathbb{Z}, n \in \mathbb{N}$ und seien $c_1, \ldots, c_n \in \mathbb{Z}$ beliebige ganze Zahlen. Dann gilt $a \mid \sum_{i=1}^{n} c_i\, b_i$.

Beweis. Da a ein Teiler von b_i für $i = 1, \ldots, n$ ist gilt $b_i = ak_i$ für $k_i \in \mathbb{Z}$. Daraus folgt, dass

$$\sum_{i=1}^{n} c_i\, b_i = \sum_{i=1}^{n} c_i\,(a\, k_i) = a \sum_{i=1}^{n} c_i\, k_i,$$

wobei $\sum_{i=1}^{n} c_i\, k_i \in \mathbb{Z}$. Also ist a ein Teiler von $\sum_{i=1}^{n} c_i\, b_i$. □

Definition 1.2. Eine ganze Zahl $p > 1$ heißt *Primzahl*, falls aus $p = ab$ mit $a, b \in \mathbb{N}$ notwendigerweise $a = 1$ oder $a = p$ folgt. Wir bezeichnen die Menge aller Primzahlen mit $\mathbb{P}$.

Satz 1.1. Sei $n > 1$ eine beliebige ganze Zahl. Dann existieren endlich viele Primzahlen $p_1, \ldots, p_k$, sodass $n = \prod_{i=1}^{k} p_i$.

Beweis. Wir zeigen den Satz mittels Induktion. Für $n=2$ folgt die Aussage sofort. Nehmen wir also an, dass es für alle $1<k\leq n\in\mathbb{N}$ eine Primfaktorenzerlegung gibt. Falls $n+1$ eine Primzahl ist, ist nichts mehr zu zeigen. Ansonsten existieren $a,b\in\mathbb{N}$ mit $n+1=ab$ und $a,b<n+1$ nach Lemma 1.1 (2), wobei insbesondere a und b Primfaktorzerlegungen besitzen. Aber dann ist auch $n+1$, als Produkt von a und b, das Produkt von endlich vielen Primzahlen. □

Unsere nächste Aussage werden wir auf zwei Arten beweisen. Zunächst der klassische Beweis nach Euklid[1.1]:

Satz 1.2. (Euklid) Es gibt unendlich viele Primzahlen.

Beweis. Sei für einen Widerspruch angenommen, dass es nur endlich viele Primzahlen $p_1,\dots,p_k$ gibt. Nach Satz 1.1 hat $m:=\prod_{i=1}^{k}p_i+1$ eine Primfaktorzerlegung. Insbesondere existiert also eine Primzahl p mit $p\,|\,m$. Da p mit einer der Primzahlen $p_1,\dots,p_n$ übereinstimmt, gilt $p\,|\,\prod_{i=1}^{k}p_i$. Nach Lemma 1.2 gilt daher auch $p\,|\,1$. Dann muss aber $p=1$ sein, ein Widerspruch. □

Unmittelbar folgt der Satz allerdings auch aus folgender interessanter Tatsache:

Satz 1.3. Die Reihe

$$\sum_{p\in\mathbb{P}}\frac{1}{p}$$

divergiert bestimmt gegen ∞.

Um die Divergenz zu zeigen, führen wir zunächst folgende Darstellung ein.

Definition 1.3. Die *Riemannsche*[1.2] *ζ-Funktion* ist definiert als die Funktion $\zeta\colon(1,\infty)\to\mathbb{R}$, die jedem $s>1$ die Summe der konvergenten Reihe

$$\zeta(s):=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

zuweist.

Es folgt beispielsweise aus dem Verdichtungskriterium von Cauchy[1.3], dass ζ für alle $s>1$ wohldefiniert ist. Eine wichtige Darstellung dieser Funktion ist Leonhard Euler[1.4] zu verdanken.

Proposition 1.2. Für jedes $s>1$ gilt die Ungleichung

$$\zeta(s)\leq\prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}.$$

Beweis. Für jedes $p\in\mathbb{P}$ gilt, dass

$$\frac{1}{1-p^{-s}}=\sum_{k=0}^{\infty}\left(\frac{1}{p^s}\right)^k=1+\frac{1}{p^s}+\frac{1}{(p^2)^s}+\frac{1}{(p^3)^s}+\cdots.$$

1.1. Euklid (ca. 350 v. Chr. – 270 v. Chr.), griechischer Mathematiker

1.2. Georg Friedrich Bernhard Riemann (1826 – 1866), deutscher Mathematiker

1.3. Augustin-Louis Cauchy (1789 – 1857), französischer Mathematiker und Physiker

1.4. Leonhard Euler (1707 – 1783), Schweizer Mathematiker, Physiker, Astronom, Geograph, Logiker und Ingenieur

Das gegebene Produkt lässt sich also erweitern zu

$$\prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}} = \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\cdots\right)\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\left(1+\frac{1}{5^s}+\cdots\right)\cdots,$$

wobei wir durch Ausmultiplizieren Summanden der Form

$$\frac{1}{(p_1^{k_1}\,p_2^{k_2}\cdots p_m^{k_m})^s} \quad \text{für } p_1,\ldots,p_m\in\mathbb{P} \text{ und } k_1,\ldots,k_m\in\mathbb{N}$$

erhalten. Nach Satz 1.1 hat jede natürliche Zahl $n\in\mathbb{N}$ eine Primfaktorzerlegung, also ist mindestens[1.5] ein Summand der Form $\frac{1}{n^s}$. Daraus folgt unmittelbar die gewünschte Ungleichung. □

Kommen wir also zum Beweis von Satz 1.3:

Beweis. Wegen Proposition 1.2, haben wir für festes $s>1$ die Abschätzung $\zeta(s)\leq\prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}$. Logarithmieren wir beide Seiten, erhalten wir

$$\log(\zeta(s))\leq\log\left(\prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}\right)=\sum_{p\in\mathbb{P}}\log\left(\frac{1}{1-p^{-s}}\right)=\sum_{p\in\mathbb{P}}-\log(1-p^{-s}).$$

Wir verwenden die Taylorreihendarstellung von $\log(1-p^{-s})$ und sehen, dass

$$\log(\zeta(s))\leq\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{1}{kp^{ks}},$$

wobei

$$\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}\leq\sum_{k=1}^{\infty}\left(\frac{1}{p^s}\right)^k=\frac{p^{-s}}{1-p^{-s}}<2p^{-s},$$

sodass

$$\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}<\sum_{p\in\mathbb{P}}\frac{2}{p^s}\leq\sum_{k=1}^{\infty}\frac{2}{k^s}<\infty.$$

Das erlaubt uns $\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}$ umzuordnen, i.e.

$$\log(\zeta(s))\leq\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}=\sum_{p\in\mathbb{P}}\frac{1}{p^s}+\sum_{p\in\mathbb{P}}\sum_{k=2}^{\infty}\frac{1}{kp^{ks}}.$$

Da $\lim_{s\to1^+}\sum_{n=1}^{\infty}\frac{1}{n^s}=\sum_{n=1}^{\infty}\frac{1}{n}=\infty$, folgt $\lim_{s\to1^+}\log(\zeta(s))=\infty$. Also insbesondere

$$\lim_{s\to1^+}\left(\sum_{p\in\mathbb{P}}\frac{1}{p^s}+\sum_{p\in\mathbb{P}}\sum_{k=2}^{\infty}\frac{1}{kp^{ks}}\right)=\infty.$$

Weil aber

$$0\leq\sum_{p\in\mathbb{P}}\sum_{k=2}^{\infty}\frac{1}{kp^{ks}}\leq\sum_{n=2}^{\infty}\sum_{k=2}^{\infty}\frac{1}{n^k}=\sum_{n=2}^{\infty}\frac{1}{n\,(n-1)}=1$$

1.5. Tatsächlich ist sogar *genau ein* Summand in dieser Form, bei Proposition 1.2 gilt also sogar Gleichheit. Um das zu zeigen, benötigen wir allerdings erst die Eindeutigkeit von Primfaktorzerlegungen. Das Produkt $\prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}$ wird dann *Euler'sche Produktdarstellung* von $\zeta(s)$ genannt.

für alle $s>1$, ist nur

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \lim_{s\to 1^+} \sum_{p\in\mathbb{P}} \frac{1}{p^s} = \infty$$

möglich. □

Als nächstes Ziel wollen wir die Eindeutigkeit der Primfaktorzerlegung beweisen. Dazu sind die folgenden Resultate notwendig.

Satz 1.4. (Division mit Rest) Sei $a\in\mathbb{Z}$ und $b>0$ eine positive ganze Zahl. Dann gibt es eindeutig bestimmte $q,r\in\mathbb{Z}$ mit $a=bq+r$ und $0\le r<b$.

Beweis. Existenz: Wir setzen $q:=\lfloor \frac{a}{b} \rfloor$ (die größte ganze Zahl, die kleiner oder gleich $\frac{a}{b}$ ist) und $r:=a-bq$. Aus $q\le\frac{a}{b}<q+1$ erhalten wir $bq\le a<bq+b$, also $0\le r<b$.

Eindeutigkeit: Wenn $a=bq+r=bq'+r'$ mit $0\le r,r'<b$ ist, dann gilt $0\le|bq-bq'|=|r'-r|<b$. Die Zahl $|r'-r|$ ist also durch b teilbar; da alle Vielfachen von b entweder kleiner oder gleich 0 sind oder größer oder gleich b sind, und $|r'-r|$ im halboffenen Interval $[0,b)$ liegt, muss $r'-r=0$, also $r'=r$ gelten, somit auch $q=q'$. □

Wie bekannt, nennen wir q in Satz 1.4 den *Quotienten* und r den *Rest* der Division. Einige andere wichtige Begriffe ergeben sich:

Definition 1.4. (1) Seien $a,b\in\mathbb{Z}$ ganze Zahlen, von denen mindestens eine ungleich Null ist. Dann definieren wir den *größten gemeinsamen Teiler*, als die größte ganze Zahl $d\in\mathbb{Z}$, die sowohl Teiler von a, als auch von b ist. Wir schreiben $\mathrm{ggT}(a,b)=d$.

(2) Gilt $\mathrm{ggT}(a,b)=1$, heißen a und b *teilerfremd* oder *relativ prim*.

Da jedenfalls die Einheit ein Teiler von a und b ist, ist die Menge der Teiler von a und b nichtleer, sodass der ggT schon wohldefiniert ist. Zur Bestimmung des ggT verwenden wir den auf Euklid zurückgehenden *Euklidischen Algorithmus*.

Lemma 1.3. Seien $a,b\in\mathbb{Z}$ und $q,r\in\mathbb{Z}$, sodass $a=bq+r$. Dann gilt $\mathrm{ggT}(a,b)=\mathrm{ggT}(b,r)$.

Beweis. Sei $d:=\mathrm{ggT}(a,b)$. Per Definition teilt d sowohl a als auch b, folglich auch jede ganzzahlige Linearkombination der beiden (Lemma 1.2). Insbesondere teilt d also $a-bq=r$. Somit ist d ein gemeinsamer Teiler von b und r.

Sei nun c ein beliebiger gemeinsamer Teiler von b und r. Dann teilt c auch die Linearkombination $a=bq+r$, also ist c ein gemeinsamer Teiler von a und b, i.e. $c\le d$. □

Satz 1.5. (Euklidischer Algorithmus) Seien $a,b\in\mathbb{N}$ mit $0\le b\le a$ und nicht beide null. Wir definieren rekursiv eine Folge von Resten $(r_i)_{i\in\mathbb{N}_0}$ durch wiederholte Division mit Rest:

$$r_0:=a,\quad r_1:=b,\quad r_{i-1}=q_i r_i+r_{i+1}\quad \text{mit } 0\le r_{i+1}<r_i \text{ für } i\ge 1 \text{ solange } r_i\neq 0.$$

Dann existiert ein Index $n\in\mathbb{N}$, sodass $r_n\neq 0$ und $r_{n+1}=0$ mit $\mathrm{ggT}(a,b)=r_n$.

Beweis. Zuerst bemerken wir, dass die Folge der Reste $(r_i)_{i\in\mathbb{N}_0}$ terminiert, da $r_1>r_2>r_3>\cdots\ge 0$ eine streng monoton fallende Folge natürlicher Zahlen (oder null) bedingt. Nach dem Wohlordnungsprinzip muss eine solche Folge endlich sein, sodass jedenfalls ein minimaler Index $n+1\in\mathbb{N}$ existiert mit $r_{n+1}=0$.

Durch wiederholte Anwendung von Lemma 1.3 auf die Kette der Divisionen erhalten wir eine Kette von Gleichheiten:

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_0, r_1) = \mathrm{ggT}(r_1, r_2) = \cdots = \mathrm{ggT}(r_{n-1}, r_n).$$

Die letzte Gleichung im Algorithmus lautet aber $r_{n-1} = q_n r_n + r_{n+1}$ mit $r_{n+1} = 0$, also

$$\mathrm{ggT}(r_{n-1}, r_n) = \mathrm{ggT}(r_n, r_{n+1}) = \mathrm{ggT}(r_n, 0) = r_n,$$

sodass *a fortiori* $\mathrm{ggT}(a,b) = r_n$ gelten muss. □

Eine wichtige Konsequenz von Satz 1.5 ist das Lemma von Bézout[1.6], welches wir als Korollar festhalten.

Folgerung 1.1. (Lemma von Bézout) Für alle $a, b \in \mathbb{Z}$, nicht beide null, existieren $x, y \in \mathbb{Z}$, sodass gilt:

$$ax + by = \mathrm{ggT}(a,b).$$

Beweis. Wir zeigen durch „Rückwärts"-Induktion, dass sich jeder Rest r_i im Euklidischen Algorithmus (Satz 1.5) als ganzzahlige Linearkombination von a und b darstellen lässt.

Offenbar gilt $r_0 = 1 \cdot a + 0 \cdot b$ und $r_1 = 0 \cdot a + 1 \cdot b$. Für den Induktionsschritt nehmen wir an, dass $x_{i-1}, y_{i-1}, x_i, y_i \in \mathbb{Z}$ mit $r_{i-1} = a x_{i-1} + b y_{i-1}$ und $r_i = a x_i + b y_i$ existieren. Aus der Gleichung $r_{i+1} = r_{i-1} - q_i r_i$ folgt somit, dass

$$r_{i+1} = (a x_{i-1} + b y_{i-1}) - q_i (a x_i + b y_i) = a (x_{i-1} - q_i x_i) + b (y_{i-1} - q_i y_i).$$

Setzen wir $x_{i+1} := x_{i-1} - q_i x_i$ und $y_{i+1} := y_{i-1} - q_i y_i$ so ist auch r_{i+1} eine Linearkombination von a und b. Dieser Prozess kann fortgesetzt werden, bis wir schließlich den Rest $r_n = \mathrm{ggT}(a,b)$ erreichen, der sich ebenfalls in der Form $r_n = a x_n + b y_n$ für $x_n, y_n \in \mathbb{Z}$ darstellen lässt, was die Behauptung beweist. □

Beispiel 1.1. Wir berechnen $\mathrm{ggT}(1071, 462)$ mittels des Euklidischen Algorithmus:

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \text{ mit } q_1 = 2, r_2 = 147, \\ 462 &= 3 \cdot 147 + 21 \text{ mit } q_2 = 3, r_3 = 21, \\ 147 &= 7 \cdot 21 + 0 \text{ mit } q_3 = 7, r_4 = 0. \end{aligned}$$

Also $\mathrm{ggT}(1071, 462) = 21$. Zur Darstellung des ggT als Linearkombination, lösen wir die Gleichungen rückwärts auf:

$$\begin{aligned} 21 &= 462 - 3 \cdot 147, \\ 147 &= 1071 - 2 \cdot 462, \end{aligned}$$

also

$$21 = 462 - 3 \cdot (1071 - 2 \cdot 462) = 7 \cdot 462 - 3 \cdot 1071.$$

Folgerung 1.2. Seien $a, b \in \mathbb{Z}$. Gilt $\mathrm{ggT}(a,b) \mid d$ für ein $d \in \mathbb{N}$, so existieren $x, y \in \mathbb{Z}$ mit

$$ax + by = d.$$

1.6. Étienne Bézout (1730 – 1783), französischer Mathematiker

Beweis. Falls $\mathrm{ggT}(a,b) \mid d$, existiert $k \in \mathbb{N}$ mit $\mathrm{ggT}(a,b)\, k = d$. Nach Folgerung 1.1 gilt $ax + by = \mathrm{ggT}(a,b)$ für $x, y \in \mathbb{Z}$ und Multiplikation mit k liefert nun

$$axk + byk = (ax + by)\, k = \mathrm{ggT}(a,b)\, k = d,$$

also ist d eine Linearkombination von a und b. □

Lemma 1.4. (Fundamentallemma) Seien $a, b, c \in \mathbb{Z}$. Falls $\mathrm{ggT}(a,b) = 1$ und $a \mid bc$, so folgt $a \mid c$.

Beweis. Sei vorausgesetzt, dass $\mathrm{ggT}(a,b) = 1$ gilt. Aus Folgerung 1.1 folgt daher die Existenz ganzer Zahlen $x, y \in \mathbb{Z}$, sodass $ax + by = 1$. Multiplizieren wir die Gleichung mit c, erhalten wir

$$axc + byc = c.$$

Betrachten wir nun die beiden Summanden der linken Seite. Der erste Summand, axc, ist offenbar durch a teilbar. Für den zweiten Summanden, byc, gilt nach Voraussetzung, dass a das Produkt bc teilt und folglich ist dieser Term ebenfalls durch a teilbar.

Da beide Summanden auf der linken Seite der Gleichung Vielfache von a sind, muss auch ihre Summe, welche c ist, ein Vielfaches von a sein. Es gilt also $a \mid c$, was zu beweisen war. □

Proposition 1.3. Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und p eine Primzahl. Teilt p das Produkt $\prod_{i=1}^{n} a_i$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p \mid a_i$.

Beweis. Wir gehen mittels Induktion nach n vor; offenbar stimmt die Aussage für $n = 1$. Sei die Aussage also für ein $n \in \mathbb{N}$ wahr und angenommen, dass $p \mid \prod_{i=1}^{n+1} a_i$ für ganze Zahlen $a_1, \ldots, a_{n+1}$. Falls $p \mid a_{n+1}$, so ist nichts mehr zu zeigen. Falls jedoch $p \nmid a_{n+1}$, so muss jedenfalls $\mathrm{ggT}(p, a_{n+1}) = 1$ folgen, da p eine Primzahl ist und somit folgt aus Lemma 1.4, dass $p \mid \prod_{i=1}^{n} a_i$. Aus der Induktionsannahme folgt somit, dass ein $i \in \{1, \ldots, n\}$ mit $p \mid a_i$ existiert, was zu beweisen war. □

Wir verfügen nun über alle Werkzeuge, um die Eindeutigkeit der Primfaktorzerlegung aus Satz 1.1 zu beweisen.

Satz 1.6. (Fundamentalsatz der Arithmetik) Es sei $a \in \mathbb{Z}$, ungleich null. Dann existiert zu jeder Primzahl $p \in \mathbb{P}$ genau eine ganze Zahl $\nu_p(a) \geq 0$, sodass

$$a = \mathrm{sgn}(a) \prod_{p \in \mathbb{P}} p^{\nu_p(a)}.$$

Beweis. Sei zunächst $a \geq 1$. Wir wissen bereits, dass es zu jeder Primzahl p ein $\nu_p(a) \in \mathbb{N}_0$ gibt, sodass $a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$. Für $a > 1$ folgt diese Tatsache nämlich aus Satz 1.1 und für $a = 1$ ist es ausreichend, einfach $\nu_p(a) = 0$ für alle Primzahlen p zu setzen. Es ist also nur noch die Eindeutigkeit dieser Zerlegung zu zeigen.

Seien für $a \geq 1$ zwei verschiedene Zerlegungen

$$a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)} = \prod_{p \in \mathbb{P}} p^{\mu_p(a)},$$

mit $\nu_p(a), \mu_p(a) \in \mathbb{N}_0$, gegeben. Dann gilt $\nu_{p_0}(a) \neq \mu_{p_0}(a)$ für ein $p_0 \in \mathbb{P}$. O. B. d. A. sei $\mu_{p_0}(a) < \nu_{p_0}(a)$. Dann ist

$$p_0^{\nu_{p_0}(a) - \mu_{p_0}(a)} \cdot \prod_{p \in \mathbb{P} \setminus \{p_0\}} p^{\nu_p(a)} = \prod_{p \in \mathbb{P} \setminus \{p_0\}} p^{\mu_p(a)}.$$

Ist das Produkt auf der rechten Seite leer, erhalten wir sofort einen Widerspruch; ist das Produkt nicht leer, dann existiert nach Proposition 1.3 eine Primzahl $p_1 \in \mathbb{P}$, die in $\prod_{p\in\mathbb{P}\setminus\{p_0\}} p^{\mu_p(a)}$ vorkommt, sodass $p_0 \mid p_1$. Das ist erneut ein Widerspruch, da jedenfalls $p_0 \neq p_1$ gelten muss. Es muss also $\nu_p(a) = \mu_p(a)$ für alle $p \in \mathbb{P}$ gelten.

Der Übergang zu $a \leq -1$ folgt nun unmittelbar. □

2 Grundbegriffe

In diesem Kapitel werden wir einige wesentliche Definitionen geben, die vor allem durch die Frage motiviert sind, in welcher Weise, sich die Eigenschaften der ganzen Zahlen, insbesondere die Existenz und Eindeutigkeit von Primfaktorzerlegungen, verallgemeinern lassen. Konkret formuliert suchen wir nach einer „Struktur“ R mit gewissen Operationen $+$ und $\cdot$, die wie in $\mathbb{Z}$ miteinander verträglich sind und aus denen sich jene Aussagen herleiten lassen, die wir verwendet haben, um den Fundamentalsatz der Arithmetik zu beweisen.

Wir fangen an mit der Definition einer *Gruppe*:

Definition 2.1. Es sei G eine Menge und $\circ\colon G \times G \to G$ eine Abbildung. Das Paar $(G, \circ)$ heißt *Gruppe*, falls gilt:

(1) $x \circ (y \circ z) = (x \circ y) \circ z$ für alle $x, y, z \in G$. (*Assoziativität von „$\circ$“*)

(2) Es gibt ein Element $e \in G$, sodass $e \circ x = x \circ e = e$ für alle $x \in G$. (*Neutrales Element*)

(3) Zu jedem $x \in G$ existiert ein $y \in G$, sodass $x \circ y = e = y \circ x$. (*Inverses*)

Gilt ferner

(4) $x \circ y = y \circ x$ für alle $x, y \in G$,

so heißt G *abelsch*[2.1] (seltener: *kommutativ*).

Notierung 2.1. Falls im Kontext klar ist, mit welcher Gruppenoperation G ausgestattet ist, schreibt man statt $(G, \circ)$ oft nur G und bezeichnet schon G alleine als Gruppe. Ist die Gruppenoperation von G eine Addition „$+$“, so schreiben wir für das neutrale Element normalerweise 0 und nennen G eine *additive Gruppe*. Ähnlich bezeichnen wir G als *multiplikative Gruppe*, wenn die Gruppenoperation ein Produkt „$\cdot$“ darstellen soll und bezeichnen das neutrale Element als *Einselement* bzw. 1. Ebenso verwenden wir im Fall von zwei Gruppen G, H oft die Schreibweise e_G bzw. e_H für das neutrale Element von G bzw. H; manchmal erlauben wir uns, diesen Index auch zu vernachlässigen, wenn es im Kontext klar ist.

An dieser Stelle sei bemerkt, dass die Definition eines inversen Elements aktuell noch lückenhaft ist, da nicht unmittelbar klar ist, ob e wirklich eindeutig bestimmt ist! Glücklicherweise ist das aber der Fall:

Folgerung 2.1. Sei $(G, \circ)$ eine Gruppe. Dann gelten:

(1) Das neutrale Element e von G ist eindeutig bestimmt.

(2) Zu jedem $x \in G$ ist das inverse Element $x^{-1} \in G$ eindeutig bestimmt.

(3) Für das neutrale Element gilt $e^{-1} = e$.

(4) Ist $x \in G$, so folgt $(x^{-1})^{-1} = x$.

(5) Sind $x, y \in G$, so ist $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

2.1. Niels Henrik Abel (1802 – 1829), norwegischer Mathematiker

(6) Jedes beliebig geklammerte Produkt $x_1 \circ x_2 \circ \cdots \circ x_n$ für $n \in \mathbb{N}, x_1, \ldots, x_n \in G$ lässt sich in „linksnormierter“ Weise schreiben, i.e. $(\cdots((x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_n)$. Mit anderen Worten: Klammern dürfen beliebig gesetzt werden und sogar weggelassen werden.

Beweis. (1) Sei $e' \in G$ ein weiteres neutrales Element. Dann folgt $e' = e \circ e' = e$.

(2) Sei $x \in G$. Gilt $x \circ y = e = y \circ x$ und $x \circ y' = e = y' \circ x$ für $y, y' \in G$, so folgt

$$y = e \circ y = (y' \circ x) \circ y = y' \circ (x \circ y) = y' \circ e = y'.$$

(3) Es gilt $e = e \circ e$. Daraus folgt mit (2), dass $e^{-1} = e$.

(4) Es gilt $x \circ x^{-1} = e$. Nach (2) folgt $(x^{-1})^{-1} = x$.

(5) Wir sehen

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e.$$

Nach (2) folgt also, dass $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

(6) Wir führen eine Induktion nach n. Für $n = 3$ stimmt die Behauptung mit Punkt (1) aus der Definition einer Gruppe überein. Sei $n \geq 4$. Dann gilt mittels der Induktionsvoraussetzung, dass

$$\begin{aligned}(\cdots(x_1 \circ \cdots \circ x_j) \circ (x_{j+1} \circ \cdots \circ x_n)\cdots) &= (\cdots(x_1 \circ \cdots \circ x_j) \circ (x_{j+1} \circ \cdots \circ x_{n-1}) \circ x_n) \\ &= ((\cdots(x_1 \circ \cdots \circ x_j) \circ (x_{j+1} \circ \cdots \circ x_{n-1})) \circ x_n) \\ &= (\cdots((x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_n),\end{aligned}$$

was zu zeigen war. □

Es folgen nun einige Beispiele von Gruppen.

Beispiel 2.1. (1) Die ganzen Zahlen $\mathbb{Z}$ bilden eine (abelsche) Gruppe unter der Addition „+“, aber keine Gruppe unter der Multiplikation „·“. Beispielsweise hat 0 kein multiplikativ inverses Element.

(2) Ein Vektorraum V über dem Körper[2.2] K bildet definitionsgemäß unter der Vektoraddition eine abelsche Gruppe.

(3) Die *allgemeine lineare Gruppe* $\mathrm{GL}(n, K)$ der $n \times n$ Matrizen A über dem Körper K mit $\det A \neq 0$ ist (wie der Name andeutet) eine Gruppe mit der Matrixmultiplikation. Ebenso bekannt sind die *spezielle lineare Gruppe* $\mathrm{SL}(n, K)$ mit $\det A = 1$, die *orthogonale Gruppe* $\mathrm{O}(n)$ über $\mathbb{R}$, die *unitäre Gruppe* $\mathrm{U}(n)$ über $\mathbb{C}$ und deren speziellen Analoge $\mathrm{SO}(n)$ und $\mathrm{SU}(n)$ mit $\det A = 1$. Im Allgemeinen handelt es sich bei diesen Gruppen um nicht-abelsche Gruppen.

(4) Es sei M eine beliebige Menge. Die Menge der bijektiven Selbstabbildungen von M bilden unter der Zusammensetzung von Funktionen eine Gruppe $S(M)$, die *symmetrische Gruppe von* M. Ist $M = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreiben wir statt $S(M)$ auch S_n und bezeichnen diese Gruppe als *n-te symmetrische Gruppe*.

(5) Wir definieren für $m \in \mathbb{N}$ die *Restklassen modulo m*, wobei zwei Zahlen $r, s \in \mathbb{Z}$ genau dann in derselben Restklasse liegen, wenn die Division durch m, nach Satz 1.4, den gleichen Rest ergibt, i.e. $m \mid r - s$[2.3]. Die Einteilung der ganzen Zahlen in Restklassen modulo m, geschrieben $\mathbb{Z}/m\mathbb{Z}$ ist eine Einteilung in disjunkte Teilmengen. Jede Restklasse modulo m lässt sich beschreiben durch $r + m\mathbb{Z}$, wobei r irgendeine Zahl der Restklasse ist. Eine derartige Zahl r heißt ein *Repräsentant* der Restklasse. Die Addition in $\mathbb{Z}$ induziert in $\mathbb{Z}/m\mathbb{Z}$ eine Verknüpfungsvorschrift, nämlich

$$(r + m\mathbb{Z}) + (s + m\mathbb{Z}) = (r + s) + m\mathbb{Z}.$$

2.2. Wir werden bald die formale Definition eines Körpers einführen, setzen in diesem Beispiel allerdings voraus, dass der Begriff aus der Linearen Algebra bekannt ist.

2.3. Weitere Schreibweisen: $r \equiv s \pmod m$, $\bar{r} = \bar{s}$, $[r]_m = [s]_m$ und viele andere.

Diese Vorschrift ist offenbar wohldefiniert, sodass es sich bei $\mathbb{Z}/m\mathbb{Z}$ zusammen mit der Restklassenaddition sogar um eine abelsche Gruppe handelt.

Notierung 2.2. Es sei $(G, \circ)$ eine Gruppe. Für ein Element $x \in G$ und eine ganze Zahl $n \in \mathbb{Z}$ setzen wir:

$$x^n := \begin{cases} \overbrace{x \circ x \circ \cdots \circ x}^{n\text{-fach}} & \text{für } n \geq 2, \\ x \quad \text{für } n = 1, \\ e \quad \text{für } n = 0, \\ (x^{-n})^{-1} \quad \text{für } n \leq -1. \end{cases}$$

Beachte

$$x^{-m} = (x^m)^{-1} = (x \circ \cdots \circ x)^{-1} = (x^{-1})^m \quad \text{für } m \geq 1,$$
$$x^k \circ x^l = x^{k+l} \quad \text{und} \quad (x^k)^l = x^{k \cdot l} \quad \text{für } k, l \in \mathbb{Z}.$$

Zwei wichtige Definitionen:

Definition 2.2. Sei $(G, \circ)$ eine Gruppe. Falls ein $x \in G$ existiert, sodass für jedes $y \in G$ auch ein $n \in \mathbb{Z}$ mit $x^n = y$ existiert, dann heißt G *zyklisch* und x ein *Erzeuger* von G. Wir schreiben $G = \langle x \rangle$.

Definition 2.3. Eine Teilmenge H einer Gruppe $G = (G, \circ)$, sodass auch $(H, \circ)$ eine Gruppe ist, heißt *Untergruppe* von G. Wir schreiben $H \leq G$.

Man sieht z.B. sofort, dass $(\mathbb{Z}, +)$ eine zyklische Gruppe mit Erzeugern ± 1 ist. Tatsächlich lassen sich aus der Kommutativität der Addition in $\mathbb{Z}$ einige wichtige Tatsachen folgern:

Proposition 2.1. Sei $(G, \circ)$ eine zyklische Gruppe. Dann gilt:

(1) G ist abelsch.

(2) Ist $H \leq G$ eine Untergruppe von G, so ist auch H zyklisch.

Beweis. (1) Sei $G = \langle x \rangle$ für ein $x \in G$. Falls $y, z \in G$, so existieren $n_1, n_2 \in \mathbb{Z}$ mit $x^{n_1} = y, x^{n_2} = z$. Aus der Bemerkung in Notation 2.2 folgt nun, dass

$$y \circ z = x^{n_1} \circ x^{n_2} = x^{n_1 + n_2} = x^{n_2 + n_1} = x^{n_2} \circ x^{n_1} = z \circ y.$$

(2) Wir nehmen weiterhin an, dass $G = \langle x \rangle$ für ein $x \in G$. Falls $H = \{e\}$, so ist nichts mehr zu zeigen. Andererseits, sei $e \neq h \in H$ jenes Element dessen Exponent $n \in \mathbb{N}$ in der Darstellung $x^n = h$ minimal ist. Wir wollen zeigen, dass $H = \langle h \rangle$. Offensichtlich gilt $H \supseteq \langle h \rangle$, da H eine Untergruppe von G ist. Falls hingegen $y \in H \leq G$ ist, so gibt es ein $m \in \mathbb{Z}$ mit $x^m = y$. Nach Satz 1.4 gibt es außerdem $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r < n$. Daraus folgt

$$y = x^m = x^{qn+r} = x^{qn} \circ x^r.$$

Wäre $r \neq 0$, so würde $x^r = x^{-qn} \circ y \in H$ folgen, ein Widerspruch zur Minimalität von n. Also gilt $r = 0$ und insbesondere $y = x^{qn} = (x^n)^q = h^q$, nach der Bemerkung in Notation 2.2. Demnach $H \subseteq \langle h \rangle$, was zu zeigen war. □

Insbesondere folgt daraus, dass jede Untergruppe H der additiven Gruppe von $\mathbb{Z}$ zyklisch ist, also von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Diese Erkenntnis merken wir uns:

Folgerung 2.2. Alle Untergruppen von $(\mathbb{Z},+)$ sind von der Form $m\,\mathbb{Z}$ für ein $m\in\mathbb{N}$.

Insbesondere gibt uns Folgerung 2.2 einen weiteren Hinweis für unsere Suche nach einer Verallgemeinerung der ganzen Zahlen. Zentral in Proposition 2.1 ist nämlich die Division mit Rest in $\mathbb{Z}$ (Satz 1.4), die fast automatisch impliziert, dass die Untergruppen von $\mathbb{Z}$ eine bestimmte Form haben. Unsere Struktur R erfüllt also folgende Implikationskette:

> Existiert eine „Division mit Rest“ in R,
>
> so sind die echten R-„Unterräume“ von R maximal eindimensional,
>
> und es existiert foglich eine Zerlegung aller Elemente von R in „atomare“ Einheiten.

Das führt uns zur Definition eines *Rings*.

Definition 2.4. Es sei R eine additive abelsche Gruppe zusammen mit einer Multiplikation „$\cdot$“ von $R\times R\to R$, sodass für alle $r,s,t\in R$ gilt:

(1) $r\cdot(s\cdot t)=(r\cdot s)\cdot t$. (*Assoziativität von „$\cdot$“*)

(2) $r\cdot(s+t)=(r\cdot s)+(r\cdot t)$ und $(r+s)\cdot t=(r\cdot t)+(s\cdot t)$. (*Distributivität*)

Dann heißt das Tripel $(R,+,\cdot)$ ein *Ring*. Gilt ferner

(3) Es existiert ein Element $1\in R$, sodass $1\cdot r=r=r\cdot 1$ für alle $r\in R$,

nennt man R einen *Ring mit Eins*. Ein Ring $(R,+,\cdot)$ heißt *kommutativ* falls

(4) $r\cdot s=s\cdot r$ für alle $r,s\in R$. (*Kommutativität von „$\cdot$“*)

Notierung 2.3. Wie bei Gruppen lassen wir die Operationen „$+$“ und „$\cdot$“ manchmal weg und bezeichnen bereits R als Ring, wenn klar ist, welche Addition/Multiplikation gemeint ist. Außerdem vereinbaren wir die übliche „Punkt-vor-Strich“-Rechnung, i.e. $(r\cdot s)+(r\cdot t)=r\cdot s+r\cdot t$. Wollen wir deutlich machen, dass wir vom Nullelement in R reden, schreiben wir manchmal 0_R; die meiste Zeit werden wir aber schlicht 0 schreiben und meinen damit das neutrale Element in $(R,+)$.

Analog zur Untergruppe definieren wir:

Definition 2.5. Eine Teilmenge S eines Rings $R=(R,+,\cdot)$, sodass auch $(S,+,\cdot)$ ein Ring ist, heißt *Unterring* oder *Teilring* von R und wir schreiben $S\leq R$. Hat R zusätzlich ein Einselement $1\in R$, so verlangen wir, dass auch $1\in S$.

Folgerung 2.3. Sei $(R,+,\cdot)$ ein Ring. Dann gilt:

(1) Es gilt $r\cdot 0=0=0\cdot r$ für alle $r\in R$.

(2) Es gilt $r\cdot(-s)=-(r\cdot s)=(-r)\cdot s$ für alle $r,s\in R$.

(3) Ist $(R,+,\cdot)$ sogar ein Ring mit Eins, so ist das Einselement $1\in R$ eindeutig bestimmt.

Beweis. (1) Aus $r\cdot 0=r\cdot(0+0)=r\cdot 0+r\cdot 0$ folgt sofort $r\cdot 0=0$ und ebenso für $0\cdot r=0$.

(2) Für die linke Gleichung ist $r\cdot s+r\cdot(-s)=0$ zu zeigen. In der Tat,

$$r\cdot s+r\cdot(-s)=r\cdot(s+(-s))=r\cdot 0=0,$$

wegen (1). Ebenso für $(-r)\cdot s$.

(3) Sei $1'\in R$ ein Element mit $1'\cdot r=r$ für alle R. Dann folgt insbesondere, dass $1'=1'\cdot 1=1$. □

Definition 2.6. Sei $(R, +, \cdot)$ ein Ring.

(1) Ein Element $0 \neq r \in R$ heißt *Linksnullteiler*, wenn $0 \neq s \in R$ existiert mit $r \cdot s = 0$. Analog definieren wir *Rechtsnullteiler*.

(2) Ist r Links- oder Rechtsnullteiler, nennen wir r *Nullteiler*.

(3) Besitzt R keine Nullteiler, nennen wir R *nullteilerfrei*.

(4) Ist R ein nullteilerfreier kommutativer Ring mit Einselement $1 \neq 0$, heißt R *Integritätsring* oder *Integritätsbereich*.

Beispiel 2.2. (1) Die ganzen Zahlen $\mathbb{Z}$ bilden einen Integritätsbereich; die geraden Zahlen $2\,\mathbb{Z}$ bilden einen kommutativen Ring ohne Eins.

(2) Offenbar sind $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ alle Beispiele von Integritätsbereichen.

(3) Die komplexen $n \times n$-Matrizen bilden einen Ring mit Eins, der für $n \geq 2$ nicht kommutativ ist. Allgemein können wir für einen beliebigen Ring R den Matrizenring $M(n, R)$ aller $n \times n$-Matrizen mit Einträgen aus R konstruieren. Auch dieser ist in der Regel für $n \geq 2$ nicht kommutativ und ist ein Ring mit Eins, sofern auch R ein Einselement enthält.

(4) Die Restklassen modulo m für $m \in \mathbb{N}$ bilden einen kommutativen Ring mit Eins zusammen mit der Multiplikation

$$(r + m\,\mathbb{Z}) \cdot (s + m\,\mathbb{Z}) = (r \cdot s) + m\,\mathbb{Z}.$$

Manchmal schreiben wir statt $\mathbb{Z}/m\,\mathbb{Z}$ auch $\mathbb{Z}_m$. Offenbar hat $\mathbb{Z}/m\,\mathbb{Z}$ genau dann Nullteiler, wenn m keine Primzahl ist.

Definition 2.7. Es sei $(R, +, \cdot)$ ein Ring mit Einselement. Sei $r \in R$. Falls ein $s \in R$ existiert, sodass $r \cdot s = 1$, so heißt s ein *(multiplikatives) Rechtsinverses* von r. Falls $s \cdot r = 1$, dann heißt s ein *(multiplikatives) Linksinverses* von R. Besitzt $r \in R$ ein Links- und ein Rechtsinverses, dann stimmen diese überein und heißen schlicht das *multiplikative Inverse* $s = r^{-1}$ von r. Solch ein r nennen wir dann *Einheit* in R. Die Menge aller Einheiten bezeichnen wir mit R^*.

Lemma 2.1. Sei R ein Ring. Dann ist $(R^*, \cdot)$ eine Gruppe.

Beweis. Seien $a, b \in R^*$ beliebig. Dann gilt offenbar auch $a^{-1}, b^{-1} \in R^*$, sodass

$$(ab)\,(b^{-1}a^{-1}) = a\,(bb^{-1})\,a^{-1} = aa^{-1} = 1.$$

Das heißt $ab \in R^*$. Es folgt, dass R^* mit der Multiplikation eine Gruppe ist. □

Beispiel 2.3. (1) In $(\mathbb{Z}, +, \cdot)$ gilt offenbar $\mathbb{Z}^* = \{-1, 1\}$. Leicht lässt sich überprüfen, dass $\mathbb{Z}^*$, wie in Lemma 2.1 bewiesen, eine Gruppe mit der Multiplikation ist.

(2) Sei $m \geq 1$ eine ganze Zahl. Was sind die Einheiten in $\mathbb{Z}/m\,\mathbb{Z}$? Ist $a \in \mathbb{Z}/m\,\mathbb{Z}$ eine Einheit, so existiert $a^{-1} \in \mathbb{Z}/m\,\mathbb{Z}$ mit $aa^{-1} = 1$, was äquivalent zu $m \mid aa^{-1} - 1$ ist. (Siehe Beispiel 2.1 (5)). Also gibt es $x \in \mathbb{Z}$, sodass $mx = aa^{-1} - 1$ oder $aa^{-1} - mx = 1$. Nach Korollar 1.1 folgt also, dass $\mathrm{ggT}(a, m) = 1$. Tatsächlich gilt auch die Umkehrung: Aus $\mathrm{ggT}(a, m) = 1$ folgt $ax + my = 1$ für x, $y \in \mathbb{Z}$, also $ax = 1$ in $\mathbb{Z}/m\,\mathbb{Z}$.

(3) Die Euler'sche φ-Funktion weist jeder ganzen Zahl $m \geq 1$ die Anzahl der Einheiten in $\mathbb{Z}/m\,\mathbb{Z}$ zu, also

$$\varphi(m) := |(\mathbb{Z}/m\,\mathbb{Z})^*|.$$

Ist $p \in \mathbb{P}$ und $k \in \mathbb{N}$, so gilt $\varphi(p^k) = p^k - p^{k-1}$. Nach (2) sind die Einheiten in $\mathbb{Z}/p^k\mathbb{Z}$ nämlich jene ganzen Zahlen, die zu p^k teilerfremd sind. Aber nur die p^{k-1} Zahlen $p, 2p, \ldots, p^{k-1}p$ sind zu p *nicht* teilerfremd, was $\varphi(p^k) = p^k - p^{k-1}$ teilerfremde Zahlen übrig lässt.

Die Definition einer Einheit motiviert die Definition weiterer algebraischer Strukturen:

Definition 2.8. Ein Ring mit Eins, in dem alle von 0 verschiedenen Elemente Einheiten sind, heißt *Schiefkörper* oder *Divisionsring*. Ein kommutativer Divisionsring heißt *Körper*.

Beispiel 2.4. (1) Offenbar sind $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ alle Körper.

(2) Ein fundamentales Beispiel für einen Schiefkörper liefern die *Quaternionen* $\mathbb{H}$. Die Bezeichnung geht auf Hamilton[2.4] zurück, der diese zuerst beschrieben hat. Dazu betrachten wir $\{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$ als Basis des vierdimensionalen reellen Vektorraumes $\mathbb{R}^4$ mit der gewohnten komponentenweisen Addition und Skalarmultiplikation.

Wir versehen diesen Raum nun mit einer zusätzlichen bilinearen Abbildung $\mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}^4$, welche durch folgende Multiplikationstabelle für die Basiselemente gegeben ist:

	1	i	j	k
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

Man bezeichnet das dadurch entstehende Produkt als das *quaternionische Produkt*. Für die Elemente aus $\mathbb{R}^4$, die mit diesen Operationen versehen sind, schreiben wir dann $\mathbb{H}$. Insbesondere gilt für die Basiselemente die wichtige Relation

$$\mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1.$$

Wie aus der linearen Algebra bekannt ist, lässt sich das quaternionische Produkt in eindeutiger Weise zu einer linearen Abbildung auf $\mathbb{H}$ fortsetzen. Es lässt sich zeigen, dass $\mathbb{H}$ ein Schiefkörper ist, wobei wir sofort aus der Multiplikationstabelle entnehmen, dass die Quaternionenmultiplikation nicht kommutativ ist.

(3) Aus Beispiel 2.3 (2) entnehmen wir sofort, dass $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper ist, wenn m eine Primzahl ist. Wir schreiben dann statt $\mathbb{Z}/p\mathbb{Z}$ auch $\mathbb{F}_p$ (engl.: „*field*“) für $p \in \mathbb{P}$.

Lemma 2.2. Jeder Körper K ist ein Integritätsbereich.

Beweis. Sei $r \in K$ nicht das Nullelement. Dann existiert ein multiplikatives Inverses $r^{-1} \in K$, sodass aus Multiplikation der Gleichung $r \cdot s = 0$, $s \in K$, mit r^{-1} von links auch $s = 0$ folgt. Offenbar gilt auch $1 \neq 0$, sodass K tatsächlich ein Integritätsbereich ist. □

Proposition 2.2. Sei R ein endlicher Integritätsring. Dann ist R sogar ein Körper.

Beweis. Sei für $0 \neq r \in R$ die Abbildung $\varphi_r : R \to R$ durch $\varphi_r(s) = rs$ für alle $s \in R$ definiert. Gilt $\varphi_r(s_1) = \varphi_r(s_2)$ für $s_1, s_2 \in R$, so folgt $rs_1 = rs_2$. Das heißt $r(s_1 - s_2) = rs_1 - rs_2 = 0$; da R ein Integritätsbereich ist, folgt $s_1 - s_2 = 0$ bzw. $s_1 = s_2$. Also ist φ_r injektiv und da R endlich ist, sogar surjektiv, das heißt bijektiv. Dann existiert aber $s \in R$, sodass $\varphi_r(s) = 1$, i.e. $rs = 1$; also ist r eine Einheit. Da r beliebig gewählt worden ist, folgt, dass R ein Körper ist. □

2.4. William Rowan Hamilton (1805 – 1865), irischer Mathematiker und Physiker

Abschließend noch folgende Erkenntnis vom Zahlentheoretiker John Wilson[2.5]:

Lemma 2.3. (Wilson) Sei $p \in \mathbb{P}$ eine Primzahl. Dann gilt

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p).$$

Beweis. Da p eine Primzahl ist, ist $\mathbb{F}_p$ ein Körper. Wir zeigen zunächst, dass die einzigen selbstinversen Elemente in diesem Körper ± 1 sind. Gilt nämlich $u^2 \equiv 1 \,(\mathrm{mod}\, p)$, erhalten wir

$$(u+1)\,(u-1) \equiv u^2 - 1 \equiv 0 \,(\mathrm{mod}\, p).$$

Weil $\mathbb{F}_p$ ein Integritätsbereich ist (Lemma 2.2), folgt also $u \equiv \pm 1 \,(\mathrm{mod}\, p)$.

Betrachten wir nun das Produkt

$$(p-1)! = (p-1)\,(p-2)\cdots(2)\,(1).$$

Aus dem vorherigen Absatz folgt, dass in dieser Liste für beliebiges $n \in \{2, \ldots, p-2\}$ auch sein multiplikatives Inverses $n^{-1} \neq n$ vorkommt. Weil multiplikative Inverse eindeutig sind, vereinfacht sich das Produkt also zu

$$(p-2)\,(p-3)\cdots(3)\,(2) \equiv 1 \,(\mathrm{mod}\, p),$$

d.h.

$$(p-1)! \equiv (p-1)\,(1) \equiv -1 \,(\mathrm{mod}\, p),$$

wie gewünscht. □

3 Noethersche, faktorielle und euklidische Ringe

Definition 3.1. (1) Es sei R ein Ring und $I \subseteq R$ eine Untergruppe von $(R, +)$. Dann nennen wir I *Linksideal* von R, wenn

$$r \cdot x \in I \text{ für alle } r \in R \text{ und } x \in I.$$

Analog heißt I *Rechtsideal* von R, wenn

$$x \cdot r \in I \text{ für alle } r \in R \text{ und } x \in I.$$

Ist I sowohl Links- als auch Rechtsideal, dann heißt I ein (zweiseitiges) *Ideal*. Wir schreiben dann $I \trianglelefteq R$.

(2) Es sei R ein Ring mit Eins. Ein Ideal $I \trianglelefteq R$ heißt *endlich erzeugt*, wenn $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in R$ existieren, sodass $I = \{\sum_{i=1}^{n} a_i r_i \mid r_i \in R\}$; wir schreiben dann $I = (a_1, \ldots, a_n)$ und nennen $a_1, \ldots, a_n$ die Erzeuger von I. Falls $n = 1$, nennen wir $I = (a)$ das *von a erzeugte Hauptideal* in R.

(3) Ein kommutativer Ring mit Eins R heißt *noethersch*[3.1], wenn jedes Ideal von R endlich erzeugt ist. Ist R ein Integritätsbereich und jedes Ideal von R sogar ein Hauptideal, so heißt R ein *Hauptidealring*[3.2] (HIR).

2.5. John Wilson (1741 – 1793), britischer Mathematiker und Jurist

3.1. Emmy Noether (1882 – 1935), deutsche Mathematikerin

3.2. Englisch: *principal ideal domain* (PID).

Beispiel 3.1. (1) Jeder Ring R enthält die beiden (Haupt)ideale $\{0\}$ und R.

(2) Für jedes $m \in \mathbb{N}$ ist $m\,\mathbb{Z}$ ein Ideal von $m\,\mathbb{Z}$, wie leicht überprüft werden kann.

(3) Sei K ein Körper und R der Matrizenring über K aus Beispiel 2.2. Definieren wir

$$I := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in K \right\} \text{ und } J := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in K \right\},$$

so ist I ein Linksideal von R (aber kein Rechtsideal von R) und J ein Rechtsideal von R (aber kein Linksideal von R), denn

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in J \text{ aber } \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I \cup J.$$

Lemma 3.1. Es sei R ein Ring und $I, J \trianglelefteq R$ Ideale. Dann sind auch $I \cap J$, $I + J$ und $I \cdot J = \{\sum_{i=1}^{n} r_i\, s_i \mid n \in \mathbb{N}, r_i \in I, s_i \in J\}$ Ideale von R.

Beweis. Wir zeigen exemplarisch die erste Aussage; der Beweis, dass $I + J$ und $I \cdot J$ Ideale sind, verläuft dann ähnlich.

Sei dazu $x \in I \cap J$ und $r \in R$ beliebig. Dann folgt $rx \in I$, da I ein Ideal ist und ebenso $rx \in J$, also $rx \in I \cap J$. Da I und J beide additive Untergruppen von R sind, ist auch $I \cap J$ eine additive Untergruppe von R. Es folgt, dass $I \cap J$ ein Ideal von R ist. □

Beispiel 3.2. Sei $R = \mathbb{Z}$ und $a, b \in \mathbb{Z}$ ganze Zahlen. Betrachten wir die Hauptideale (a) und (b). Dann gilt:

- $(a) + (b) = (a, b) = (\mathrm{ggT}(a, b))$: Offenbar gilt $(a) + (b) = (a, b)$, wir müssen also nur $(a, b) = (\mathrm{ggT}(a, b))$ zeigen. Sei $d = ar_1 + br_2$ für $r_1, r_2 \in \mathbb{Z}$ beliebig. Da $\mathrm{ggT}(a, b)$ sowohl a als auch b teilt, gilt insbesondere $d \in (\mathrm{ggT}(a, b))$. Die Umkehrung folgt wiederum aus Folgerung 1.2.

- $(a) \cap (b) = (\mathrm{kgV}(a, b))$: Falls $d \in (a) \cap (b)$, existieren $r_1, r_2 \in \mathbb{Z}$ mit $d = ar_1$ und $d = br_2$, sodass d alle Primfaktoren von a und b enthält, also $\mathrm{kgV}(a, b) \mid d$. Es folgt $d \in (\mathrm{kgV}(a, b))$. Umgekehrt, ist $d \in (\mathrm{kgV}(a, b))$, so gilt erneut $\mathrm{kgV}(a, b) \mid d$, d.h. d enthält alle Primfaktoren von $\mathrm{kgV}(a, b)$, insbesondere jene von a und jene von b, sodass $d \in (a)$ und $d \in (b)$.

- $(a) \cdot (b) = (ab)$: Sei $d = \sum_{i=1}^{n} (ar_i)\,(bs_i)$ für $r_i, s_i \in \mathbb{Z}$, $1 \leq i \leq n$ beliebig. Dann gilt $d = \sum_{i=1}^{n} (ar_i)\,(bs_i) = (ab)\,(\sum_{i=1}^{n} r_i\, s_i)$, also $d \in (ab)$. Die Umkehrung ist offensichtlich.

Lemma 3.2. Sei R ein kommutativer Ring mit Eins. Dann ist R genau dann ein Körper, wenn R nur zwei Ideale enthält.

Beweis. Sei zunächst vorausgesetzt, dass R ein Körper ist. Dann sind die einzigen Ideale von R das Nullideal $\{0\}$ und R selbst. In der Tat, falls $I \neq \{0\}$ ein Ideal ist, so enthält es $0 \neq x \in I \subseteq R$. Da R ein Körper ist, existiert $x^{-1} \in R$ mit $1 = xx^{-1} \in I$. Daraus folgt aber, dass $I = R$ gelten muss.

Umgekehrt, sei R ein kommutativer Ring mit Eins mit genau zwei Idealen. Diese müssen $\{0\}$ und R sein. Falls $0 \neq r \in R$, so muss offenbar $(r) \neq \{0\}$ sein, also $(r) = R$. Aber dann gilt insbesondere, dass $1 \in R$, d.h. es existiert $r^{-1} \in R$, sodass $1 = rr^{-1} \in (r)$. Es folgt, dass r eine Einheit ist und R ein Körper. □

Wir untersuchen nun eine bestimmte Konstruktion, um aus einem beliebigen Ring R einen weiteren Ring R zu „schöpfen“. Es stellt sich dann die Frage, welche Eigenschaften diesem Ring von R vererbt werden.

Beispiel 3.3. Es sei R ein Ring. Mit $R[X]$ bezeichnen wir die Menge aller R-wertigen Folgen $(a_0, a_1, \dots)$ mit $a_i \in R$, sodass $a_i = 0$ für alle bis auf endlich viele $i \in \mathbb{N}_0$. Dann ist $R[X]$ ein Ring vermöge der Operationen

$$\begin{aligned}(a_0, a_1, \dots) + (b_0, b_1, \dots) &:= (a_0 + b_0, a_1 + b_1, \dots),\\ (a_0, a_1, \dots) \cdot (b_0, b_1, \dots) &:= (c_0, c_1, \dots) \text{ mit } c_k = \sum_{i=0}^{k} a_{k-i}\, b_i \text{ für } k \geq 0.\end{aligned}$$

Offenbar identifiziert die injektive Einbettungsabbildung $\iota_R : R \to R[X], \iota_R(r) := (r, 0, 0, \dots)$ den Ring R mit einem Teilring $\iota_R(R) \leq R[X]$ von $R[X]$.

Ist R ein Ring mit Einselement 1, dann ist $(1, 0, 0, \dots)$ ein Einselement in $R[X]$, sodass wir

$$X := (0, 1, 0, \dots)$$

definieren können. Dann gilt offenbar $X^n = (0, \dots, 0, 1, 0, \dots)$ für alle $n \in \mathbb{N}_0$. Setzen wir für $a \in R$ $aX^n = \iota_R(a)\, X^n$ und $X^n a = X^n \iota_R(a)$, dann gilt $aX^n = X^n a$, sodass wir jedes Element $f \in R[X]$ in der Form

$$f = \sum_{i=0}^{n} a_i X^i \text{ für ein } n \in \mathbb{N}_0$$

darstellen können.

Ist $f \neq 0$, so setzen wir voraus, dass n maximal mit der Eigenschaft $a_n \neq 0$ gewählt worden ist. Die Koeffizienten $a_0, \dots, a_n \in R$ sind dann eindeutig bestimmt und wir nennen n den *Grad von* f. Wir schreiben $\deg(f) := n$, wobei wir insbesondere $\deg(0) = -\infty$ setzen.

Den Ring $R[X]$ nennen wir dann *Polynomring über R mit Variablen X* und seine Elemente *Polynome in X* (mit Koeffizienten in R). Die Elemente der Menge $\iota_R(R)$ nennen wir außerdem *konstante Polynome*.

Der Polynomring $R[X_1, \dots, X_n]$ in n Variablen $X_1, \dots, X_n$ ist dann rekursiv definiert durch

$$R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n]$$

für $n \geq 2$. Sei beispielsweise

$$f(X, Y) = a_{00} + a_{10} X + a_{01} Y + a_{20} X^2 + a_{11} XY + a_{02} Y^2.$$

Dann lässt sich f als $f(X, Y) = \left(\underbrace{a_{00} + a_{10} X + a_{20} X^2}_{\in R[X]}\right) + \left(\underbrace{a_{11} X + a_{01}}_{\in R[X]}\right) Y + \left(\underbrace{a_{02}}_{\in R[X]}\right) Y^2$ schreiben.

Folgende Eigenschaften werden von R an $R[X]$ weitergegeben.

Proposition 3.1. Sei R ein Ring. Dann gilt:

(1) Ist R kommutativ, so ist auch $R[X]$ kommutativ.

(2) Ist R nullteilerfrei, so ist auch $R[X]$ nullteilerfrei.

(3) Ist R ein Integritätsbereich, so ist auch $R[X]$ ein Integritätsbereich.

Beweis. (1) Sei R kommutativ. Eine Rechnung zeigt, dass

$$\begin{aligned}(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) &= \left(\sum_{i=0}^{0} a_{0-i}\, b_0, \sum_{i=0}^{1} a_{1-i}\, b_0, \dots\right) = \left(\sum_{i=0}^{0} b_{0-i}\, a_0, \sum_{i=0}^{1} b_{1-i}\, a_0, \dots\right)\\ &= (b_0, b_1, \dots) \cdot (a_0, a_1, \dots)\end{aligned}$$

für alle $(a_0, a_1, \dots)$ und $(b_0, b_1, \dots) \in R[X]$, sodass auch $R[X]$ kommutativ ist.

(2) Sei R nullteilerfrei und $(a_0, a_1, \dots), (b_0, b_1, \dots) \in R[X]$ nicht das Nullelement. Dann existieren minimale Indizes $k_1, k_2 \in \mathbb{N}_0$, sodass $a_{k_1} \neq 0$ und $b_{k_2} \neq 0$. Sei $k := k_1 + k_2$; das k-te Glied des Produktes dieser Folgen ist dann durch $\sum_{i=0}^{k} a_{k-i}\, b_i$ gegeben. Ist $i = 0, \dots, k_2 - 1$, dann ist offenbar $b_i = 0$. Falls $i = k_2 + 1, \dots, k_1 + k_2$, dann

$$k - i \leq k - (k_2 + 1) = (k_1 + k_2) - 1 = k_1 - 1,$$

sodass $a_{k-i} = 0$ für diese i. Also verbleibt nur der Summand $a_{k_1} b_{k_2}$, der nach Annahme jedenfalls nicht Null ist. Daraus folgt nun unmittelbar, dass $(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) \neq 0$, i.e. $R[X]$ ist nullteilerfrei.

(3) Sei R nun ein Integritätsbereich. Die Kommutativität und Nullteilerfreiheit von $R[X]$ folgt aus (1) und (2). Offenbar ist auch $(1, 0, \dots) \neq (0, 0, \dots)$, also ist auch $R[X]$ ein Integritätsbereich. □

Beispiel 3.4. Der Polynomring $\mathbb{Z}[X]$ ist kein Hauptidealring, da das Ideal $(2, X)$ kein Hauptideal ist. Wäre nämlich $(2, X) = (f)$ für ein $f \in \mathbb{Z}[X]$, so würde $2 \in (f)$ und $X \in (f)$ folgen. Das ist nur möglich, falls $f = \pm 1$. Aber dann folgt $(2, X) = (f) = \mathbb{Z}[X]$, was offenbar nicht der Fall ist.

Nun zu einem bekannten Ergebnis aus der kommutativen Algebra. Er stammt von [3.3].

Satz 3.1. (Hilbert'scher Basissatz) Sei R ein noetherscher Ring. Dann ist auch $R[X_1, \dots, X_n]$ noethersch.

Beweis. Zeigen wir den Satz für $n = 1$, so ergibt sich induktiv, dass der Satz für alle $n \in \mathbb{N}$ hält.

Betrachten wir für R noethersch also den Polynomring in einer Variablen $R[X]$. Sei indirekt angenommen, dass $R[X]$ nicht noethersch ist. Dann existiert ein Ideal $I \subseteq R[X]$, das nicht endlich erzeugt ist. Wir konstruieren nun rekursiv eine Folge von Polynomen $(f_k)_{k \in \mathbb{N}}$ in I:

(1) Sei f_1 ein von Null verschiedenes Polynom in I mit minimalem Grad.

(2) Für $k \geq 1$, sei $I_k := (f_1, \dots, f_k)$ das von $f_1, \dots, f_k$ erzeugte Ideal. Da I nicht endlich erzeugt ist, ist I_k eine echte Teilmenge von I. Wir können also f_{k+1} als ein Polynom minimalen Grades in $I \setminus I_k$ wählen.

So ergibt sich eine Folge von Polynomen mit $\deg(f_1) \leq \deg(f_2) \leq \deg(f_3) \leq \cdots$. Sei $d_k := \deg(f_k)$ und sei $a_k \in R$ der Leitkoeffizient von f_k für jedes $k \geq 1$. Betrachten wir das von diesen Leitkoeffizienten in R erzeugte Ideal $J := (a_1, a_2, a_3, \dots) \subseteq R$. Da R noethersch ist, ist J endlich erzeugt. Es gibt also ein $m \in \mathbb{N}$ mit $J = (a_1, \dots, a_m)$[3.4]. Insbesondere liegt der Leitkoeffizient a_{m+1} in J, sodass Elemente $r_1, \dots, r_m \in R$ mit $a_{m+1} = \sum_{i=1}^{m} r_i\, a_i$ existieren.

Wir setzen nun

$$h := \sum_{i=1}^{m} r_i\, X^{d_{m+1} - d_i}\, f_i.$$

Da $d_i \leq d_{m+1}$ für $i \leq m$ gilt, sind die Exponenten $d_{m+1} - d_i$ nicht negativ, also ist h wohldefiniert. Weiterhin gilt $h \in I_m = (f_1, \dots, f_m)$ mit $\deg(h) = d_{m+1}$ und Leitkoeffizient $\sum_{i=1}^{m} r_i\, a_i = a_{m+1}$. Betrachten wir nun das Polynom $g := f_{m+1} - h$. Dann folgt aus $f_{m+1} \in I, h \in I_m \subseteq I$, dass $g = f_{m+1} - h \in I$ und $g \notin I_m$, da sonst $f_{m+1} = g + h \in I_m$; also $g \in I \setminus I_m$. Aber nach Definition ist $\deg(g) < \deg(f_{m+1})$. Wir haben also ein Polynom $g \in I \setminus I_m$ gefunden, dessen Grad echt kleiner als der Grad von f_{m+1} ist, im Widerspruch zur Wahl von f_{m+1} als Polynom minimalen Grades in $I \setminus I_m$. □

3.3. David Hilbert (1862 – 1943), deutscher Mathematiker, Physiker und Philosoph

3.4. Wir werden in Proposition 3.2 sehen, warum die Erzeuger von J auch unter den a_k sein müssen.

Aus Satz 3.1 lässt sich ein interessantes (Gegen)beispiel gewinnen.

Beispiel 3.5. Wir betrachten den Polynomring $\mathbb{Q}[X_1, X_2] = \mathbb{Q}[X, Y]$ in zwei Variablen über den rationalen Zahlen. Nach Lemma 3.2 ist $\mathbb{Q}$ ein Hauptidealring und daher noethersch, also ist nach Satz 3.1 auch $\mathbb{Q}[X, Y]$ noethersch. Sei $I := (X, Y)$ die Menge aller Polynome in $\mathbb{Q}[X, Y]$ ohne konstante Koeffizienten; dann ist I kein Hauptideal. In der Tat, wäre $I = (f)$ für ein $f \in \mathbb{Q}[X, Y]$, so würde $f \mid X$ und $f \mid Y$ folgen, i.e. $f = \pm 1$. Also $I = (f) = \mathbb{Q}[X, Y]$, was offenbar ein Widerspruch ist. Der Ring $\mathbb{Q}[X, Y]$ ist also ein noetherscher Ring, der kein Hauptidealring ist.

Diese Überlegungen dienen als erster Schritt in unserer Konkretisierung/Präzisierung von Kästchen 2.2: Ideale scheinen eine gute Verallgemeinerung des Begriffes eines „R-Unterraums“ zu sein. Wir fahren auf diese Art und Weise fort.

Definition 3.2. Sei R ein kommutativer Ring mit Eins mit $a, b \in R$. Wir sagen, dass a ein *Teiler* von b ist, falls ein Element $r \in R$ existiert, sodass $ar = b$. Wir schreiben dann $a \mid b$, in Worten „a teilt b“.

Definition 3.3. Sei R ein kommutativer Ring mit Eins mit $a, b \in R$. Wir sagen, dass a und b *zueinander assoziiert sind*, falls eine Einheit $\varepsilon \in R^*$ existiert, sodass $a = \varepsilon b$. Wir schreiben dann $a \sim b$.

Die Ähnlichkeit zu den analogen Definitionen in $\mathbb{Z}$ ist kaum zu übersehen. Entsprechend übertragen sich Teile des folgenden Lemmas fast wortgleich aus Lemma 1.1.

Lemma 3.3. Sei R ein kommutativer Ring mit Eins. Dann gilt:

(1) Die Relation „$\sim$“ ist auf R eine Äquivalenzrelation.

(2) Ist R sogar ein Integritätsbereich, so gilt $a \mid b$ und $b \mid a$ genau dann, wenn $a \sim b$.

(3) Falls $b \mid a$ für $a, b \in R$, so folgt $bc \mid ac$ für alle $c \in R$.

(4) Sei $a \in R$ ein Teiler von $b_1, \ldots, b_n \in R, n \in \mathbb{N}$ und seien $c_1, \ldots, c_n \in R$ beliebig. Dann folgt, dass $a \mid \sum_{i=1}^{n} c_i b_i$.

Beweis. (1) Die Reflexivität folgt aus $a = 1 \cdot a$. Die Symmetrie folgt aus

$$a \sim b \quad \Leftrightarrow \quad a = \varepsilon \cdot b \quad \Leftrightarrow \quad \varepsilon^{-1} \cdot a = b \quad \Leftrightarrow \quad b \sim a$$

für eine Einheit $\varepsilon \in R^*$. Für die Transitivität sei angemerkt, dass falls $a \sim b$ und $b \sim c$, Einheiten $\varepsilon_1, \varepsilon_2 \in R^*$ existieren, sodass $a = \varepsilon_1 \cdot b$ und $b = \varepsilon_2 \cdot c$, also

$$a = \varepsilon_1 \cdot b = \varepsilon_1 \cdot (\varepsilon_2 \cdot c) = (\varepsilon_1 \cdot \varepsilon_2) \cdot c$$

für die Einheit $\varepsilon_1 \cdot \varepsilon_2 \in R^*$ (nach Lemma 2.1).

(2) Sei zunächst vorausgesetzt, dass $a \mid b$ und $b \mid a$. Dann ist $a\varepsilon_1 = b$ und $b\varepsilon_2 = a$ für $\varepsilon_1, \varepsilon_2 \in R$. Also

$$b = a\varepsilon_1 = (b\varepsilon_2)\,\varepsilon_1 = b\,(\varepsilon_2\,\varepsilon_1).$$

Da R ein Integritätsbereich ist, folgt $\varepsilon_2 \varepsilon_1 = 1$, also insbesondere $\varepsilon_1, \varepsilon_2 \in R^*$. Aber das heißt $a \sim b$. Die Umkehrung folgt unmittelbar.

(3) & (4) Der Beweis verläuft wie in $\mathbb{Z}$ (siehe Lemma 1.1). □

Definition 3.4. Sei R ein kommutativer Ring mit Eins. Ein Element $p \in R \setminus R^*$ ungleich Null heißt *irreduzibel*, wenn aus $p = a \cdot b$ stets folgt, dass a oder b eine Einheit ist. Ferner heißt p *prim*, wenn für alle $a, b \in R$ aus $p \mid ab$ auch $p \mid a$ oder $p \mid b$ folgt.

Beispiel 3.6. (1) In $\mathbb{Z}$ sind die irreduziblen Elemente von der Form $\pm p$ für eine Primzahl $p \in \mathbb{P}$.

(2) Wegen $0 = 0 \cdot 0$ ist $0 \in R$ für einen beliebigen kommutativen Ring mit Eins nicht irreduzibel.

(3) Sind $p, p' \in R$ mit $p \sim p'$ und ist p sogar irreduzibel, so ist auch p' irreduzibel. Es gilt nämlich $p = \varepsilon \cdot p'$ für eine Einheit ε. Ist also $p' = a \cdot b$ für $a, b \in R$, so auch $p = \varepsilon \cdot p' = \varepsilon ab$, i.e. εa oder b ist eine Einheit. Da $\varepsilon \in R^*$, muss also insbesondere a oder b eine Einheit sein.

(4) Sind $p, p' \in R$ mit $p \sim p'$ und ist p sogar prim, so ist auch p' prim. Gilt $p' \mid ab$, dann folgt aus Lemma 3.3, dass $p = \varepsilon \cdot p' \mid \varepsilon ab$, sodass $p \mid \varepsilon a$ oder $p \mid b$. Also folgt $p' \mid p \mid \varepsilon a$ oder $p' \mid p \mid b$, i.e. $p' \mid a$ oder $p' \mid b$.

Lemma 3.4. Sei R ein Integritätsbereich. Ist $p \in R$ prim, dann auch irreduzibel.

Beweis. Sei vorausgesetzt, dass $p \in R$ Primelement ist mit $p = a \cdot b$ für fixierte $a, b \in R$. Dann ist p per Definition keine Einheit und nicht Null; wir müssen also nur zeigen, dass a oder b eine Einheit ist. Da p prim ist, teilt p entweder a oder b. Nehmen wir beispielsweise an, dass $p \mid a$. Dann gilt $a = pr$ für $r \in R$, sodass $p = ab = (pr)\, b = p\,(rb)$. Aber R ist ein Integritätsbereich, also muss schon folgen, dass $rb = 1$, i.e., dass b Einheit ist. □

Beispiel 3.7. (1) Die Voraussetzung in Lemma 3.4, dass R ein Integritätsbereich ist, ist wesentlich. In $\mathbb{Z}/6\,\mathbb{Z}$ ist leicht zu überprüfen, dass die Elemente $2, 3, 4$ prim sind, aber

$$2 = 2 \cdot 4, \quad 4 = 2 \cdot 2, \quad 3 = 3 \cdot 3$$

gilt, also keines davon irreduzibel ist.

(2) Die Umkehrung von Lemma 3.4 gilt im Allgemeinen nicht. Sei $R := \mathbb{Q} + \mathbb{R}[X]$ der Ring der reellen Polynome mit rationalen konstanten Koeffizienten. Dann ist das Polynom X in R irreduzibel, aber nicht prim: Aus $X \mid (\sqrt{2}\, X)^2$ folgt nicht, dass $X \mid \sqrt{2}\, X$ in R, da $\sqrt{2} \notin R$.

Die Definition von primen und irreduziblen Elementen motiviert die folgende Definition.

Definition 3.5. Sei R ein Integritätsbereich. Dann heißt R ein *Ring mit Faktorzerlegung*, falls für alle $r \in R$, sodass $r \neq 0$ und r keine Einheit ist, irreduzible Elemente $p_1, \ldots, p_n \in R$ existieren mit

$$r = \prod_{i=1}^{n} p_i.$$

Sind diese Faktoren sogar eindeutig, im Sinne, dass falls eine weitere Zerlegung $p'_1, \ldots, p'_m \in R$ mit

$$p = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} p'_i,$$

erstens $m = n$ gelten muss und zweitens eine Bijektion $\varphi \colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ existiert, sodass $p_i \sim p'_{\varphi(i)}$ für alle $i \in \{1, \ldots, n\}$, so nennen wir R *faktoriell*[3.5].

3.5. Englisch: *unique factorization domain* (UFD)

Aus Satz 1.1 folgt, dass $\mathbb{Z}$ ein Ring mit Faktorzerlegung ist und aus Satz 1.6 folgt, dass $\mathbb{Z}$ sogar faktoriell ist. Diese Begriffe erlauben es uns, Kasten 2.2 etwas zu präzisieren:

> Existiert eine „Division mit Rest“ im *Ring* R,
>
> so ist R ein *Hauptidealring*,
>
> und deswegen sogar *faktoriell*.

Natürlich ist die obige Implikationskette zurzeit eine Aussage, die wir noch nicht bewiesen haben. Widmen wir uns zunächst einer etwas allgemeineren Frage: Ist R ein Hauptidealring, so sind seine Ideal in gewissem Sinne „eindimensional“. Anstatt (bis auf Weiteres) der Frage nachzugehen, ob R dann auch faktoriell ist, nehmen wir an, dass R ein noetherscher Integritätsbereich ist, i.e. wir haben nicht unbedingt „eindimensionale“, sondern „endlichdimensionale“ Ideale. Folgt dann, dass R ein Ring mit Faktorzerlegung ist? Sogar, dass er faktoriell ist? Die Antwort auf die erste Frage ist ja und die Antwort auf die zweite Frage ist nein, wie wir später sehen werden.

Satz 3.2. Sei R ein noetherscher Integritätsbereich. Dann ist R ein Ring mit Faktorzerlegung.

Für den Beweis brauchen wir zuerst einige Hilfsresultate.

Lemma 3.5. Sei R ein Integritätsbereich. Dann gilt für alle $a, b \in R$:

(1) $(b) \subseteq (a)$ genau dann, wenn $a \mid b$.

(2) $(a) = (b)$ genau dann, wenn $a \sim b$.

(3) a ist genau dann irreduzibel, wenn (a) maximal unter den echten Hauptidealen von R bezüglich der Mengeninklusion ist.

Beweis. (1) Falls $(b) \subseteq (a)$, so folgt $b \in (b) \subseteq (a)$, also $b = ar$ für $r \in R$. Das heißt aber $a \mid b$.

(2) Das folgt aus (1) und Lemma 3.3 (2).

(3) Sei zuerst angenommen, dass a irreduzibel ist. Sei $(a) \subseteq (b) \neq R$ für $b \in R$. Dann ist b keine Einheit. Wegen (1) haben wir $b \mid a$, also $a = br$ für $r \in R$. Aber a ist irreduzibel, also muss r Einheit sein, d.h. $a \sim b$. Aus (2) folgt $(a) = (b)$.

Umgekehrt sei (a) nun unter den echten Hauptidealen von R bezüglich $\subseteq$ maximal gewählt. Dann ist a jedenfalls keine Einheit. Sei $a = br$ für $b, r \in B$ und o. B. d. A. vorausgesetzt, dass r keine Einheit ist; wir müssen zeigen, dass b Einheit ist. Es gilt $(a) \subseteq (r)$ nach (1) und nach Voraussetzung $(a) = (r)$. Aus (2) folgt, dass $a \sim r$, i.e. b ist Einheit. □

Proposition 3.2. Sei R ein kommutativer Ring mit Eins. Dann sind äquivalent:

(1) R ist noethersch.

(2) Jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq \cdots$ von Idealen in R wird stationär, d.h., es existiert ein Index $N \in \mathbb{N}$, sodass $I_n = I_N$ für alle $n \geq N$.

(3) Jede nichtleere Menge $\mathcal{I}$ von Idealen in R besitzt ein maximales Element bezüglich der Mengeninklusion.

Beweis. (1) $\Rightarrow$ (2) Sei $I_1 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Kette von Idealen in R. Wir betrachten die Vereinigung $I := \bigcup_{n=1}^{\infty} I_n$; dann ist I ein Ideal. Offenbar ist I nicht leer, da $0 \in I_1 \subseteq I$. Falls $a, b \in I$, so gibt es Indizes $k_1, k_2 \in \mathbb{N}$ mit $a \in I_{k_1}, b \in I_{k_2}$. Setzen wir $k := \max\{k_1, k_2\}$, dann folgt $a, b \in I_k$ und insbesondere $a - b \in I_k \subseteq I$. Ist wiederum $a \in I$ und $r \in R$, dann existiert $k \in \mathbb{N}$ mit $a \in I_k$ und damit auch $ra \in I_k \subseteq I$. Also ist I ein Ideal.

Da R noethersch ist, ist I endlich erzeugt. Sei $I = (a_1, \dots, a_k)$ für $a_1, \dots, a_k \in I$. Für jedes $j \in \{1, \dots, k\}$ gibt es einen Index $n_j \in \mathbb{N}$, sodass $a_j \in I_{n_j}$. Sei $N := \max\{n_1, \dots, n_k\}$. Wegen $I_{n_j} \subseteq I_N$ für alle $j \in \{1, \dots, n\}$, gilt $a_1, \dots, a_k \in I_N$ und deshalb $I = (a_1, \dots, a_k) \subseteq I_N$. Andererseits folgt per Konstruktion von I, dass $I_N \subseteq I$, also $I = I_N$.

Für jedes $n \geq N$ folgt nun $I_N \subseteq I_n \subseteq I$ und da $I_N = I$ muss $I_n = I_N$ gelten, d.h. die Kette $I_1 \subseteq I_2 \subseteq \cdots$ wird ab dem Index N stationär.

(2) $\Rightarrow$ (3) Sei $\mathcal{I}$ eine nichtleere Menge von Idealen in R. Sei indirekt angenommen, dass $\mathcal{I}$ kein maximales Element hat. Weil $\mathcal{I}$ nichtleer ist, können wir ein Ideal $I_1 \in \mathcal{I}$ wählen; dann ist I_1 nicht maximal, sodass ein Ideal $I_2 \in \mathcal{I}$ mit $I_1 \subsetneq I_2$ existiert. Ebenso ist I_2 nicht maximal in $\mathcal{I}$, also muss es $I_3 \in \mathcal{I}$ geben mit $I_1 \subsetneq I_2 \subsetneq I_3$ und wir können diesen Prozess fortsetzen, um eine unendliche aufsteigende Kette $I_1 \subsetneq I_2 \subsetneq \cdots$ von Idealen in R zu finden, die nicht stationär wird, im Widerspruch zur Annahme.

(3) $\Rightarrow$ (1) Sei I ein beliebiges Ideal in R; wir wollen zeigen, dass I endlich erzeugt ist. Sei

$$\mathcal{I} := \{J \trianglelefteq R \mid J \subseteq I \text{ und } J \text{ ist endlich erzeugt}\}.$$

Dann ist die Familie $\mathcal{I}$ jedenfalls nicht leer, da $(0) \in \mathcal{I}$. Nach Voraussetzung besitzt $\mathcal{I}$ also ein maximales Element J_0. Per Definition ist J_0 endlich erzeugt mit $J_0 \subseteq I$. Sei zum Widerspruch angenommen, dass $J_0 \subsetneq I$. Dann existiert $a \in I$ mit $a \notin J_0$. Betrachten wir das Ideal $J_1 := J_0 + (a)$; da J_0 endlich erzeugt ist mit $J_0 = (a_1, \dots, a_k)$ für $a_1, \dots, a_k \in R$ ist auch $J_1 = (a_1, \dots, a_k, a)$ endlich erzeugt. Dann ist $J_0 \subsetneq J_1$. Aber offenbar gilt dann $J_1 \trianglelefteq R$, $J_1 \subseteq I$ und J_1 ist endlich erzeugt, i.e. $J_1 \in \mathcal{I}$, im Widerspruch zur Annahme, dass J_0 maximal in $\mathcal{I}$ gewählt worden ist. Es muss also $J_0 = I$ gelten. □

Bedingung (2) in Proposition 3.2 wird *aufsteigende Kettenbedingung* (engl.: *ascending chain condition*) genannt und ist auch außerhalb der Algebra, insbesondere der Mengentheorie, geläufig. Kommen wir nun zum Beweis von Satz 3.2.

Beweis. Sei

$$\mathcal{I} := \{(a) \mid a \neq 0, a \notin R^*, a \text{ hat keine Zerlegung in irreduzible Elemente}\}.$$

Wir zeigen, dass $\mathcal{I}$ die leere Menge ist. Wäre das nicht der Fall, so würde nach Proposition 3.2 ein maximales Element $(a) \in \mathcal{I}$ für ein $a \in R$ existieren. Da a offenbar nicht irreduzibel ist, existieren Elemente $u, v \in R \setminus R^*$ mit $a = uv$. Aus Lemma 3.5 (1) und (2) folgt, dass $(a) \subsetneq (u)$ sowie $(a) \subsetneq (v)$, sodass wegen der Maximalität von (a) in $\mathcal{I}$ nur die Möglichkeit $(u), (v) \notin \mathcal{I}$ verbleibt. Insbesondere müssen u und v eine Zerlegung in irreduzible Elemente haben; dann hat aber auch das Produkt $a = uv$ eine Zerlegung in irreduzible Elemente; ein Widerspruch. Es gilt also tatsächlich $\mathcal{I} = \emptyset$. □

Damit haben wir erfolgreich bewiesen, dass jeder noethersche Ring ein Ring mit Faktorzerlegung ist. Gilt auch die Umkehrung? Für die Antwort begeben wir uns ins Unendliche.

Beispiel 3.8. (1) Sei R ein Ring. Wir definieren den *Polynomring* $R[X_1, X_2, \dots]$ *in abzählbar unendlich vielen Variablen* als

$$R[X_1, X_2, \dots] := \bigcup_{n=1}^{\infty} R[X_1, \dots, X_n]$$

mit der gewohnten Addition und Multiplikation aus Beispiel 3.3. Jedes Polynom $f \in R[X_1, X_2, ...]$ ist offenbar Element eines Polynomrings $R[X_1, \dots, X_n]$ in nur n Variablen. Sei R nun ein noetherscher Integritätsbereich. Dann ist $R[X_1, \dots, X_n]$ nach Proposition 3.1 (3) und Satz 3.1 auch ein noetherscher Integritätsbereich und f hat damit nach Satz 3.2 eine Zerlegung in irreduzible Polynome in $R[X_1, \dots, X_n]$. Somit ist $R[X_1, X_2, \dots]$ ein Ring mit Faktorzerlegung, der nicht noethersch ist. In der Tat, die unendlich aufsteigende Kette von Idealen

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots$$

wird nicht stationär, im Widerspruch zu Proposition 3.2 (2).

(2) Wie wichtig ist die Vorausssetzung, dass R in Satz 3.2 noethersch ist? Betrachten wir dazu folgende Konstruktion.[3.6] Sei S die Menge aller Folgen in $\mathbb{N}_0$. Wir betrachten die formalen Monome

$$X^a := X_1^{a_1} X_2^{a_2} \cdots, \quad a = (a_1, a_2, \dots) \in S,$$

wobei auch unendlich viele der a_i von Null verschieden sein dürfen. Definieren wir R als den $\mathbb{C}$-Vektorraum mit diesen Monomen als Basis und versehen R mit der Multiplikation $X^a X^b := X^{a+b}$, so ist R ein Integritätsbereich. Die irreduziblen Monome in R sind dann (bis auf Multiplikation mit Einheiten) genau die $X_i, i \geq 1$. Zusammen mit der Beobachtung, dass die Faktoren eines Monoms auch Monome sein müssen, folgt, dass $X_1 X_2 X_3 \cdots = X^{(1,1,1,\dots)}$ keine endliche Faktorisierung in irreduzible Elemente hat. Insbesondere ist R ein Ring ohne Faktorzerlegung.

(3) Ein weiteres Gegenbeispiel im Sinne von (2): Sei $R := \{f \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\}$ zusammen mit der üblichen Addition und Multiplikation von Polynomen ein Ring. Da R ein Unterring von $\mathbb{Q}[X]$ ist, ist R ein Integritätsbereich. Sei zunächst festgestellt, dass 2 keine Einheit in R ist. Ferner existiert kein irreduzibles lineares Polynom mit konstantem Term Null. In der Tat, ist $f \in R$ mit $\deg(f) = 1$ und $f(0) = 0$, so können wir $f = aX$ für ein $a \in \mathbb{Q}$ schreiben und es folgt

$$aX = 2 \cdot \left(\frac{a}{2} X\right) = 2 \cdot \left(2 \cdot \frac{a}{4} X\right) = \cdots = 2^k \left(\frac{a}{2^k} X\right) \quad \text{für } k \in \mathbb{N}_0.$$

Insbesondere erhalten wir eine unendliche „Faktorisierungskette“

$$X = 2 \cdot \left(\frac{1}{2} X\right), \quad \frac{1}{2} X = 2 \cdot \left(\frac{1}{4} X\right), \quad \dots, \quad \frac{1}{2^k} X = 2 \cdot \left(\frac{1}{2^{k+1}} X\right)$$

für $k \in \mathbb{N}_0$. Also ist R kein Ring mit Faktorzerlegung. Offenbar ist R auch nicht noethersch (Satz 3.2), was wir konkret durch die aufsteigende Kette von Hauptidealen $(X) \subsetneq \left(\frac{1}{2} X\right) \subsetneq \left(\frac{1}{4} X\right) \subsetneq \cdots$ sehen können. Zuletzt sei noch bemerkt, dass obwohl R kein Ring mit Faktorzerlegung ist, irreduzible Elemente trotzdem existieren (beispielsweise 2); vgl. auch das vorherige Beispiel.

Satz 3.3. Sei R ein Ring mit Faktorzerlegung. Dann ist R genau dann faktoriell, wenn jedes irreduzible Element von R auch prim ist.

Beweis. ($\Rightarrow$) Sei R faktoriell. Wir müssen zeigen, dass jedes irreduzible Element auch prim ist. Sei also $p \in R$ irreduzibel. Angenommen, p teilt das Produkt ab für $a, b \in R$; dann existiert $c \in R$ mit $pc = ab$. Sind a oder b Null oder eine Einheit, so ist $p \mid a$ oder $p \mid b$ unmittelbar erfüllt. Andererseits, da R faktoriell ist, gibt es eindeutig bestimmte irreduzible Elemente $p_1, \dots, p_n \in R$ und $p_{n+1}, \dots, p_m \in R$ mit

$$a = \prod_{i=1}^{n} p_i \quad \text{und} \quad b = \prod_{j=n+1}^{m} p_j,$$

d.h. $pc = \prod_{i=1}^{m} p_i$. Da p selbst irreduzibel ist, folgt aus der Eindeutigkeit dieser Zerlegung, dass $p \sim p_i$ für ein $i \in \{1,...,m\}$. Gilt $i \in \{1,...,n\}$, so folgt insbesondere, dass $p \mid a$ und gilt $i \in \{n+1,...,m\}$, muss jedenfalls $p \mid b$ folgen. Somit ist p prim.

($\Leftarrow$) Sei R nun ein Ring mit Faktorzerlegung, in dem jedes irreduzible Element prim ist. Sei $r \in R$ mit

$$r = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} p_i'$$

3.6. Vielen Dank an Noah Maxwell Arbesfeld (Universität Wien) für dieses Beispiel.

für irreduzible Elemente $p_1, \dots, p_n \in R$ und $p'_1, \dots, p'_n \in R$; wir wollen zeigen, dass diese Zerlegung eindeutig ist, im Sinne von Definition 3.5.

Wir führen Induktion nach m durch. Der Fall $m = 1$ folgt unmittelbar. Sei vorausgesetzt, dass die Behauptung für Zerlegungen der Länge $m-1$ bereits bewiesen ist. Aus $\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} p'_i$ folgt, dass $p_1 \mid \prod_{i=1}^{m} p'_i$. Da p_1 irreduzibel ist, ist es nach Annahme prim und daher existiert $j \in \{1, \dots, m\}$, sodass $p_1 \mid p'_j$; nehmen wir o. B. d. A. an, dass $p_1 \mid p'_1$. Dann gibt es $q \in R$ mit $p_1 q = p'_1$. Da p'_1 irreduzibel ist und p_1 keine Einheit ist, folgt, dass $q \in R^*$, i.e. $p_1 \sim p'_1$. Wir können ohne Einschränkung annehmen, dass $q = 1$, also bekommen wir $\prod_{i=2}^{n} p_i = \prod_{i=2}^{m} p'_i$. Nach Induktionsvoraussetzung gilt also $n-1 = m-1$ und es existiert eine Bijektion $\varphi' : \{1, \dots, n-1\} \to \{1, \dots, m-1\}$ mit $p_i \sim p'_{\varphi(i)}$ für $i = 1, \dots, n-1$. Insbesondere gilt $n = m$. Definieren wir außerdem

$$\varphi : \{1, \dots, n\} \to \{1, \dots, m\}, \quad \varphi(k) := \begin{cases} m, \text{ falls } k = n, \\ \varphi'(k), \text{ sonst} \end{cases}$$

so folgt die Behauptung. □

Ein Integritätsbereich ist also genau dann faktoriell, wenn die Begriffe „prim“ und „faktoriell“ zusammenfallen. Wir sind nun bereit die erste Implikation aus Kästchen 2.2 zu beweisen.

Satz 3.4. Jeder Hauptidealring R ist faktoriell.

Beweis. Da R ein Hauptidealring ist, ist R noethersch und somit ein Ring mit Faktorzerlegung, nach Satz 3.2. Wir müssen noch zeigen, dass jedes irreduzible Element $p \in R$ auch prim ist. Seien also $a, b \in R$ mit $p \mid ab$ und o. B. d. A. $p \nmid a$; wir müssen zeigen, dass $p \mid b$. Wegen $p \nmid a$ gilt $a \notin (p)$, also insbesondere $(p) \subsetneq (a) + (p)$. Da R ein Hauptidealring ist, muss $(a) + (p)$ ein Hauptideal sein. Wegen Lemma 3.5 ist (p) unter den echten Hauptidealen aber maximal, sodass $(a) + (p) = R$ gelten muss. Also gibt es $u, v \in R$ mit $au + pv = 1$, woraus folgt $b = abu + bpv$. Aus $p \mid ab$ folgt also $p \mid b$, d.h. p ist prim. □

Uns fehlt noch eine Präzisierung der „Division mit Rest“. Das wollen wir mit folgender Definition erreichen.

Definition 3.6. Es sei R ein Integritätsbereich. Dann heißt R *euklidisch*, wenn es eine Abbildung $\omega : R \setminus \{0\} \to \mathbb{N}_0$ gibt, sodass für alle $a, b \in R$, mit $b \neq 0$, Elemente $q, r \in R$ existieren mit $a = bq + r$ und $r = 0$ oder $\omega(r) < \omega(b)$.

Beispiel 3.9. (1) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, wenn wir $\omega : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$, $\omega(n) := |n|$ setzen.

(2) Jeder Körper K ist ein euklidischer Ring mit Bewertungsfunktion $\omega : K \setminus \{0\} \to \mathbb{N}_0$ indem wir beispielsweise $\omega(x) = 1$ für alle $x \in K$ setzen. Für $x \in K$ und $0 \neq y \in K$ gilt nämlich immer, dass $x = \left(\frac{x}{y}\right) \cdot y$.

Proposition 3.3. Sei R ein euklidischer Ring bezüglich der Abbildung $\omega : R \setminus \{0\} \to \mathbb{N}_0$. Dann ist R auch euklidisch bezüglich der Abbildung

$$\omega^* : R \setminus \{0\} \to \mathbb{N}_0, \quad \omega^*(r) := \min_{s \in (r) \setminus \{0\}} \omega(s)$$

und erfüllt die Ungleichung $\omega^*(r) \leq \omega^*(rs)$ für alle $r, s \in R \setminus \{0\}$.

Beweis. Seien $a, b \in R$ mit $b \neq 0$. Dann existiert $b_0 \in (b)$, sodass $\omega(b_0) = \omega^*(b)$. Sei $c \in R$ mit $b_0 = bc$. Da R euklidisch ist, gibt es $q_0, r \in R$ mit $a = b_0 q_0 + r$, wobei $r = 0$ oder $\omega(r) < \omega(b_0)$. Daraus folgt $a = (bc) q_0 + r = b(cq_0) + r$. Setzen wir $q := cq_0$, so folgt $a = bq + r$. Ist $r = 0$, so ist der Beweis, dass R bezüglich ω^* euklidisch ist, fertig. Ansonsten folgt $\omega^*(r) \leq \omega(r) < \omega(b_0) = \omega^*(b)$.

Um die Ungleichung zu zeigen seien $r, s \in R \setminus \{0\}$. Dann gilt $r \mid rs$, also $(rs) \subseteq (r)$ nach Lemma 3.5 (1), sodass

$$\omega^*(r) = \min_{s \in (r) \setminus \{0\}} \omega(s) \leq \min_{t \in (rs) \setminus \{0\}} \omega(t) = \omega^*(rs),$$

was wir zeigen wollten. □

Satz 3.5. Jeder euklidische Ring R ist ein Hauptidealring.

Beweis. Sei $I \trianglelefteq R$ ein Ideal in R, das nicht das Nullideal ist. Wir wählen $a \in I \setminus \{0\}$ so, dass $\omega(a) \in \mathbb{N}_0$ in I minimal ist. Ist $b \in I$ beliebig, so existieren $q, r \in R$ mit $b = aq + r$ und $r = 0$ bzw. $\omega(r) < \omega(a)$. Da $r = b - aq \in I$ und $\omega(a)$ in I minimal ist, folgt $r = 0$. Das heißt $b = aq$, i.e. $b \in (a)$. Es folgt, dass $I = (a)$ und damit ist I ein Hauptideal, was zu zeigen war. □

Der Polynomring $\mathbb{Z}[X]$ ist nach Beispiel 3.4 kein Hauptidealring und nach Satz 3.5 also kein euklidischer Ring. Zusammenfassend ergibt das:

Ist R ein *euklidischer Ring*,
so ist R ein *Hauptidealring*,
und deswegen sogar *faktoriell*.

Zum Abschluss führen wir noch einen wichtigen Begriffe ein.

Definition 3.7. Sei R ein Integritätsbereich und $A \subseteq R$ eine nichtleere Teilmenge von R. Wir sagen, dass $d \in R$ ein *gemeinsamer Teiler* von A ist, falls $d \mid a$ für alle $a \in A$. Ein gemeinsamer Teiler d von A wird *Maximalteiler* genannt, falls für jeden gemeinsamen Teiler c von A gilt, dass $c \mid d$.

Lemma 3.6. Sei R ein Integritätsbereich, $A \subseteq R$ eine nichtleere Teilmenge. Sei $d \in R$ ein Maximalteiler von A und $d' \in R$. Dann ist d' genau dann Maximalteiler, wenn $d \sim d'$.

Beweis. Nehmen wir zunächst an, dass $d \sim d'$. Dann gilt $d \mid d'$ und $d' \mid d$, also $d \sim d'$ nach Lemma 3.3 (2). Um die Umkehrung zu zeigen, nehmen wir an, dass $d \sim d'$. Dann folgt wieder aus Lemma 3.3 (2), dass $d \mid d'$ und $d' \mid d$. Ist $a \in A$ also beliebig, so folgt $d' \mid d \mid a$, da die Teilerrelation transitiv ist, i.e. d' ist ein gemeinsamer Teiler von A. Ist nun $e \in R$ ein weiterer gemeinsamer Teiler von A, so folgt jedenfalls $e \mid d \mid d'$, sodass d' tatsächlich Maximalteiler von A ist. □

Proposition 3.4. Sei R ein faktorieller Ring. Dann hat jede nichtleere Teilmenge $A \subseteq R$ von R einen Maximalteiler.

Beweis. Sei

$$D := \{x \in R \mid x \neq 0, x \mid a \text{ für alle } a \in A\}.$$

Dann ist D offenbar nicht leer. Sei $\ell \colon R \to \mathbb{N}_0$ jene Funktion, die jedem Element die Länge seiner (eindeutigen) Primfaktorisierung zuweist, wobei wir für Einheiten $u \in R$ vereinbaren, dass $\ell(u) = 0$. Jedenfalls gilt dann $\ell(x) \leq \ell(a)$ für alle $a \in A$ und $x \in D$. Somit ist $\ell(D) \subseteq \mathbb{N}_0$ eine von oben beschränkte Teilmenge und wir können $d \in D$ mit $\ell(d)$ maximal wählen. Wir zeigen, dass d ein Maximalteiler von A ist.

Per Definition ist d ein gemeinsamer Teiler von A. Ist $d' \in D$ beliebig, so müssen wir noch zeigen, dass $d' \mid d$. Sei $c \in R$ ein gemeinsamer Faktor von d und d' mit $\ell(c)$ maximal. Schreiben wir dann

$$d = cy, \quad d' = cy', \quad y, y' \in R,$$

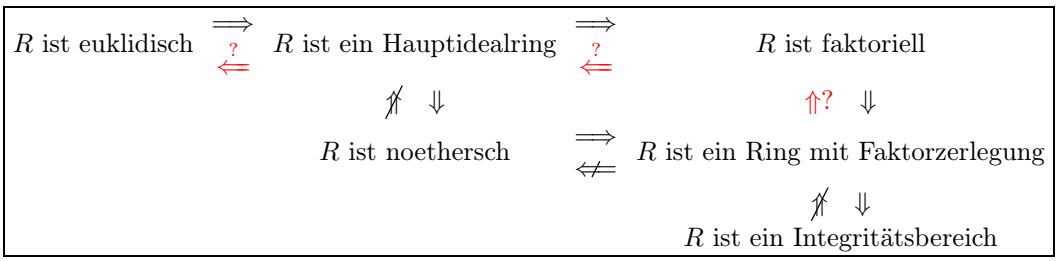
so wollen wir $y' \in R^*$ zeigen. Ist y' aber keine Einheit, so folgt, dass y' einen Primfaktor $p \mid y'$ hat. Da $\ell(cp) = \ell(c) + 1$ und c so gewählt war, dass $\ell(c)$ maximal unter allen gemeinsamen Faktoren von d und d' ist, folgt, $cp \nmid d$ und daher $p \nmid y$.

Sei $a \in A$ beliebig mit $a = dz = cyz$ für ein $z \in R$. Da $d' \mid a$, folgt $cp \mid a$ und daraus $cp \mid cyz$, sodass $p \mid yz$. Da p ein Primelement ist und $p \nmid y$, folgt $p \mid z$, d.h. $dp \mid a$. Insbesondere, weil a beliebig gewählt war, $dp \in D$. Aber das ist ein Widerspruch dazu, dass d maximale Länge $\ell(d)$ unter allen Elementen von D hat, da $\ell(dp) = \ell(d) + 1$. Somit muss y' Einheit sein und $d' \mid d$. □

Eine Bemerkung: In vielen Lehrbüchern ist die Bezeichnung „größter gemeinsamer Teiler“ anstatt der hier eingeführen Bezeichnung des „Maximalteilers“ gängig. Streng genommen sind diese Begriffe aber nicht (beliebig) austauschbar. In den ganzen Zahlen, ordnen wir die Menge der gemeinsamen Teiler anhand der natürlichen „$\leq$“-Ordnungsrelation. Für allgemeine Integritätsbereiche ist die Existenz einer solchen Relation aber nicht garantiert, also müssen wir auf die schwächere „$\mid$“-Quasiordnung zurückgreifen. Das führt dazu, dass Maximalteiler nur bis auf Assoziiertheit eindeutig sind: Die Maximalteiler von 15 und 20 in $\mathbb{Z}$ sind ± 5, deren größter gemeinsamer Teiler hingegen beschränkt sich nur auf $+5$.

4 Quotientenringe und Homomorphismen

Wir beschäftigen uns nun mit den Umkehrungen und einigen weiteren Implikationen von Kästchen 3.5. Wir wissen aus Beispiel 3.5, dass es noethersche Ringe gibt, die keine Hauptidealringe sind. In Beispiel 3.8 (1) haben wir einen Ring mit Faktorzerlegung gesehen, der nicht noethersch ist, in Beispiel 3.8 (2) einen Integritätsbereich, der kein Ring mit Faktorzerlegung ist. Wir beschäftigen uns also mit folgenden Fragen:



Wir werden auch weitere Gegenbeispiele für jene Implikationen sehen, die nur in eine Richtung gelten. Folgende Proposition wird sich jedenfalls als nützlich erweisen.

Proposition 4.1. Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent:

(1) R ist ein Körper.

(2) $R[X]$ ist euklidisch mit $\omega = \deg$, wobei der Quotient und der Rest sogar eindeutig bestimmt sind.

(3) $R[X]$ ist ein Hauptidealring.

Aktuell können wir Proposition 4.1 noch nicht vollständig beweisen. Zum Beweis benötigen wir u. a. folgendes Hilfsresultat.

Lemma 4.1. Sei R ein Integritätsbereich und $f, g \in R[X]$. Dann gilt:

(1) $\deg(f \cdot g) = \deg(f) + \deg(g)$.

(2) $R[X]^*$ ist die Menge der invertierbaren konstanten Polynome.

Beweis. (1) Das folgt sofort aus der Definition der Polynommultiplikation.

(2) Falls $f \cdot g = 1$ für $f, g \in R[X]$ mit $f, g \neq 0$, so gilt nach (1), dass

$$\deg(f) + \deg(g) = \deg(f \cdot g) = \deg(1) = 0.$$

Das kann nur der Fall sein, falls $\deg(f) = \deg(g) = 0$. Dann sind aber f und g konstante Polynome, die insbesondere in R invertierbar sein müssen. □

Definition 4.1. Sei R ein kommutativer Ring mit Eins und $I \lhd R$ ein echtes Ideal von R.

(1) I heißt *Primideal*, falls für alle $r, s \in R$ aus $rs \in I$ auch $r \in I$ oder $s \in I$ folgt. Wir nennen die Menge aller Primideale von R das *Spektrum von* R und schreiben

$$\operatorname{Spec} R := \{I \lhd R \mid I \text{ Primideal}\}.$$

(2) I heißt *maximales Ideal*, falls I in der Menge aller echten Ideale bezüglich $\subseteq$ maximal ist; i.e. falls für alle Ideale $J \lhd R$ aus $I \subseteq J$ auch $I = J$ folgt. Wir nennen die Menge aller maximalen Ideale von R das *maximale Spektrum von* R und schreiben

$$\operatorname{MSpec} R := \{I \lhd R \mid I \text{ maximales Ideal}\}.$$

Beispiel 4.1. (1) Sei $R = \mathbb{Z}$. Ist $p \in \mathbb{P}$ eine Primzahl, dann ist $p\mathbb{Z}$ ein Primideal. Außerdem ist auch das von Null erzeugte Hauptideal (0) ein Primideal. Allgemein gilt, dass R genau dann ein Integritätsbereich ist, wenn $(0) \in \operatorname{Spec} R$.

(2) Sei wieder $R = \mathbb{Z}$. Ist $p \in \mathbb{P}$ eine Primzahl, dann ist $p\mathbb{Z}$ auch ein maximales Ideal, aber $(0) \notin \operatorname{MSpec} R$. Allgemein gilt, dass $(0) \in \operatorname{MSpec} R$ genau dann, wenn R ein Körper ist.

(3) Aus Lemma 3.5 (3) folgt, dass in einem Integritätsbereich R ein Element $a \in R$ genau dann irreduzibel ist, wenn (a) in der Menge der echten *Hauptideale* von R maximal ist. Ist R also ein Hauptidealring, dann ist $a \in R$ genau dann irreduzibel, wenn (a) ein maximales Ideal ist.

Lemma 4.2. Sei R ein Integritätsbereich. Dann ist $0 \neq a \in R$ genau dann ein Primelement, wenn $(a) \in \operatorname{Spec} R \setminus \{(0)\}$.

Beweis. Sei $a \in R$ prim und $bc \in (a)$ für $b, c \in R$. Dann ist a ein Teiler von bc und daher $a \mid b$ oder $a \mid c$, woraus $b \in (a)$ oder $c \in (a)$ folgt. Also $(a) \in \operatorname{Spec} R \setminus \{(0)\}$. Umgekehrt sei $(a) \neq (0)$ ein Primideal; dann folgt $a \neq 0$ und $a \notin R^*$. Aus $a \mid bc$ folgt $bc \in (a)$, sodass $b \in (a)$ oder $c \in (a)$, d.h. $a \mid b$ oder $a \mid c$.□

Ist R insbesondere ein Hauptidealring, so ist $p \in R$ genau dann prim, wenn p irreduzibel ist, sodass in Hauptidealringen gilt $\operatorname{Spec} R = \operatorname{MSpec} R \cup \{(0)\}$. Das halten wir auch fest:

Proposition 4.2. Sei R ein Hauptidealring. Dann gilt $\operatorname{Spec} R = \operatorname{MSpec} R \cup \{(0)\}$.

Bis jetzt kennen wir nur eine Methode, um aus einem Ring R einen weiteren Ring zu schaffen. Wir lernen jetzt eine weitere kennen.

Definition 4.2. Sei R ein kommutativer Ring mit Eins und $I \trianglelefteq R$ ein Ideal. Dann ist

$$R/I := \{r + I \mid r \in R\}$$

mit den Operationen

$$(a+I)+(b+I) := (a+b)+I,$$
$$(a+I)\cdot(b+I) := (a\cdot b)+I$$

ein kommutativer Ring mit Einselement $1+I$. Wir nennen R/I den *Restklassenring von R modulo I*[4.1].

Wir haben Quotientenringe bereits unter dem Deckmantel der Restklassenringe in den ganzen Zahlen kennengelernt. In der Tat, setzen wir $R=\mathbb{Z}$ und $I=m\,\mathbb{Z}$ für $m\in\mathbb{Z}$, so gilt $R/I=\mathbb{Z}/m\,\mathbb{Z}$. Setzen wir beispielsweise $m=0$, so erhalten wir $\mathbb{Z}/0\,\mathbb{Z}=\mathbb{Z}$ und setzen wir $m=1$, gilt $\mathbb{Z}/1\,\mathbb{Z}=\{0\}$. Intuitiv forcieren wir in R/I, dass alle Elemente in I dem Nullelement entsprechen (in den obigen Beispielen setzen wir einerseits nur die Null auf Null bzw. ganz $\mathbb{Z}$ auf Null). Man vergleiche Restklassenringe auch mit Quotientenvektorräumen aus der linearen Algebra.

Beispiel 4.2. Sei R ein kommutativer Ring mit Eins und $R[X]$ der Polynomring. Sei $I:=(X)$ das von X erzeugte Hauptideal. Dann ist $R[X]/(X)=\{f+(X)\mid f\in R[X]\}$, wobei wir

$$f=\sum_{i=0}^{n} a_i\,X^i = a_0 + X\left(\sum_{i=1}^{n} a_i\,X^{i-1}\right)$$

schreiben können. Also $f+I=a_0+I$, i.e. $R[X]/(X)$ ist die Menge der konstanten Polynome. Wir können R also mit $R[X]/(X)$ identifizieren.

Proposition 4.3. Sei R ein kommutativer Ring mit Eins und $I\trianglelefteq R$ ein Ideal.

(1) $I\in\operatorname{Spec} R$ genau dann, wenn R/I ein Integritätsbereich ist.

(2) $I\in\operatorname{MSpec} R$ genau dann, wenn R/I ein Körper ist.

Beweis. (1) Wir müssen zeigen, dass R/I nicht der Nullring und nullteilerfrei ist. Dazu bemerken wir:

$$\begin{aligned} R/I \text{ nullteilerfrei, nicht Nullring} &\Leftrightarrow I\trianglelefteq R \text{ und aus } (r+I)\cdot(s+I)=I \text{ folgt } r+I=I \text{ oder } s+I=I\\ &\Leftrightarrow I\trianglelefteq R \text{ und aus } rs+I=I \text{ folgt } r+I=I \text{ oder } s+I=I\\ &\Leftrightarrow I\trianglelefteq R \text{ und aus } rs\in I \text{ folgt } r\in I \text{ oder } s\in I\\ &\Leftrightarrow I\in\operatorname{Spec} R. \end{aligned}$$

(2) Sei $I\trianglelefteq R$ ein maximales Ideal. Nach Definition ist $I\neq R$, also ist R/I nicht der Nullring. Sei also $a+I\in R/I$ mit $a\notin I$ beliebig. Dann folgt $I\subsetneq(a)+I=R$, da I maximal ist, sodass ein $b\in R$ und $s\in I$ existiert mit $ab+s=1$. Dann folgt aber $ab-1=s\in I$, i.e. $(ab-1)+I=I$ oder

$$(a+I)\cdot(b+I)=ab+I=1+I,$$

d.h. $a+I$ hat multiplikatives Inverses $b+I$.

Sei umgekehrt R/I ein Körper. Sei $J\trianglelefteq R$ ein Ideal mit $I\subsetneq J$. Dann ist $J=R$. In der Tat, sei $a\in J\setminus I$. Dann existiert $b\in R$ mit $ab+I=(a+I)\cdot(b+I)=1+I$, i.e. $ab-1\in I\subsetneq J$. Da $a\in J$ folgt insbesondere $ab\in J$ und damit $1\in J$, d.h. $J=R$. □

4.1. Andere Sprechweisen für R/I: Quotientenring, Faktorring.

Beispiel 4.3. Setzen wir in Beispiel 4.2 $R = \mathbb{Z}$, so sehen wir insbesondere, dass $I = (X)$ ein Primideal in $\mathbb{Z}[X]$ ist (da die ganzen Zahlen ein Integritätsbereich sind), aber kein maximales Ideal (da die ganzen Zahlen kein Körper sind).

Satz 4.1. Jeder kommutative Ring R mit Eins hat ein maximales Ideal.

Beweis. Siehe [Con18]. □

Beispiel 4.4. (1) Ist R ein kommutativer Ring mit Eins und $I \lhd R$ ein maximales Ideal von R, dann ist R/I nach Proposition 4.3 ein Körper und *a fortiori* ein Integritätsbereich, d.h. I ist ein Primideal. Es gilt also $\operatorname{MSpec} R \subseteq \operatorname{Spec} R$.

(2) In $\mathbb{Z}$ ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn m eine Primzahl ist, i.e. die maximalen Ideale von $\mathbb{Z}$ sind jene der Form $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$. Die Primideale sind nach Proposition 4.2 dann von der Form $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$ und das Nullideal.

(3) Beschränken wir uns in Beispiel 3.3 nicht nur auf Folgen von $\mathbb{N}_0$ nach R mit endlichem Träger, sondern lassen auch unendlich viele Folgenglieder, die nicht Null sind, zu, so erhalten wir (vermöge derselben Operationen) den Ring $R[[X]]$ der *formalen Potenzreihen*. Offenbar gilt $R[X] \subseteq R[[X]]$. Gibt es auch einen Ring, der „dazwischen“ liegt?

Sei K ein beliebiger Körper mit rationaler Norm, d.h. es gibt eine Funktion $|\cdot| : K \to \mathbb{Q}$, welche die Eigenschaften einer Norm erfüllt. Sei

$$\mathcal{C}_K := \{(a_n)_{n\in\mathbb{N}} \mid \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 : \exists N \in \mathbb{N} : \forall n, m \geq N : |a_n - a_m| < \varepsilon\}$$

die Menge der Cauchyfolgen bezüglich $|\cdot|$. Wir definieren

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}},$$
$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n \cdot b_n)_{n\in\mathbb{N}}$$

für Cauchyfolgen $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$. Aus der Analysis wissen wir, dass diese Operationen wohldefiniert sind. Tatsächlich ist $(\mathcal{C}_K, +, \cdot)$ sogar ein kommutativer Ring mit Eins, wie leicht überprüft werden kann. Ferner ist die Menge der Nullfolgen

$$N_K := \{(a_n)_{n\in\mathbb{N}} \in \mathcal{C}_K \mid \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 : \exists N \in \mathbb{N} : \forall n \geq N : |a_n| < \varepsilon\}$$

ein maximales Ideal in $\mathcal{C}_K$. Damit ist $\hat{K} := \mathcal{C}_K / N_K$ ein Körper und, wie gezeigt werden kann (siehe beispielsweise [Kal15], Kapitel 4.1), sogar vollständig. Wir erhalten außerdem eine injektive Abbildung $\hat{\imath} : K \to \hat{K}$, die jedem $a \in K$ das Element

$$\hat{\imath}(a) := (a, a, a, \dots) + N_K$$

zuweist. Setzen wir insbesondere $K := \mathbb{Q}$, so erhalten wir als Vervollständigung von $\mathbb{Q}$ die reellen Zahlen $\hat{\mathbb{Q}} = \mathbb{R}$.

Ganz allgemein kann man mit einem ähnlichen Verfahren aus einem beliebigen normierten Vektorraum V dessen Vervollständigung $\bar{V}$ konstruieren; diese ist dann ein Banach[4.2]raum, in den V isometrisch und dicht eingebettet ist.

Dieses Beispiel entspringt einem allgemeineren Konzept und führt uns zu folgender Definition.

4.2. Stefan Banach (1892 – 1945), polnischer Mathematiker

Definition 4.3. Sei A eine nichtleere Indexmenge und $(R_a)_{a\in A}$ eine Familie von Ringen. Dann ist

$$\prod_{a\in A} R_a := \{(r_a)_{a\in A} \mid \forall a \in A\colon r_a \in R_a\}$$

ein Ring vermöge der komponentenweisen Operationen

$$(r_a)_{a\in A} + (s_a)_{a\in A} := (r_a + s_a)_{a\in A},$$
$$(r_a)_{a\in A} \cdot (s_a)_{a\in A} := (r_a \cdot s_a)_{a\in A}.$$

Wir nennen $\prod_{a\in A} R_a$ den *Produktring* der R_a und sagen, dass $\prod_{a\in A} R_a$ *äußeres Produkt der* R_a ist.

Kehren wir nun zurück zum noch ausstehenden Beweis von Proposition 4.1:

Beweis. (1) $\Rightarrow$ (2) Seien $f, g \in R[X]$ mit $g \neq 0$ beliebig. Wir müssen zeigen, dass Polynome q, $r \in R[X]$ existieren, sodass $f = gq + r$ und $\deg(r) < \deg(g)$. Ist $\deg(f) < \deg(g)$, so können wir einfach $q = 0$ und $r = f$ setzen. Seien nun $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$ wobei $m = \deg(g) \leq \deg(f) = n$. Wir führen jetzt Induktion nach n: Ist $n = 0$, dann folgt die Aussage unmittelbar aus Beispiel 3.9 (2). Gilt die Aussage für $n-1$, so setzen wir zunächst $s := f - \frac{a_n}{b_m} \cdot g \cdot X^{n-m}$. Dann ist $s \in R[X]$ und $\deg(s) < \deg(f)$; also gibt es nach Induktionsvoraussetzung $q_0, r \in R[X]$, sodass $s = q_0 g + r$ und $\deg(r) < \deg(g)$. Daraus folgt aber, dass $f = \left(q_0 + \frac{a_n}{b_m} X^{n-m}\right) g + r$. Somit können wir $q := q_0 + \frac{a_n}{b_m} X^{n-m}$ setzen und die Behauptung folgt.

Zur Eindeutigkeit: Seien $q_1, q_2, r_1, r_2 \in R[X]$, sodass $f = q_1 g + r_1 = q_2 g + r_2$ mit $\deg(r_1), \deg(r_2) < \deg(g)$. Dann ist $(q_1 - q_2)\, g = r_2 - r_1$. Da im Fall $q_2 - q_1 \neq 0$ folgen würde, dass

$$\deg((q_1 - q_2)\, g) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g),$$

gäbe es einen Widerspruch zu $\deg(r_2 - r_1) < \deg(g)$. Also ist $q_1 = q_2$ und $r_1 = r_2$.

(2) $\Rightarrow$ (3) Das folgt unmittelbar aus Satz 3.5.

(3) $\Rightarrow$ (1) Sei $R[X]$ ein Hauptidealring. Wegen Beispiel 4.2 können wir $R[X]/(X)$ mit R selbst identifizieren. Da R nach Annahme ein Integritätsbereich ist, ist nach Proposition 4.3 $R[X]/(X)$ also auch ein Integritätsbereich, d.h. (X) ist ein Primideal in $R[X]$. Aber $R[X]$ ist ein Hauptidealring, daher $(X) \neq (0)$ nach Proposition 4.2 auch ein maximales Ideal. Wieder aus Proposition 4.3 folgt, dass $R[X]/(X)$ ein Körper ist, insbesondere also R, was wir zeigen wollten. □

Um mehr über die Umkehrung „HIR $\Rightarrow$ euklidisch“ in Kästchen 4 zu erfahren, werden uns Polynomringe alleine also nicht weiterhelfen. Womöglich ist ein Zusammenspiel von Polynomringen und den uns nun zur Verfügung stehenden Quotientenringe ausreichend, um diese Frage zu klären.

Lemma 4.3. (Korrespondenzsatz für Ideale) Sei R ein kommutativer Ring mit Eins und $I \trianglelefteq R$ ein Ideal. Dann entsprechen die Ideale $\bar{J} \trianglelefteq R/I$ von R/I bijektiv den Idealen $J \trianglelefteq R$ von R, die I enthalten. Formal existiert also eine Bijektion

$$\Phi\colon \mathcal{J} := \{J \trianglelefteq R \mid I \subseteq J\} \to \bar{\mathcal{J}} := \{\bar{J} \trianglelefteq R/I\}.$$

Beweis. Es sei $\pi\colon R \to R/I, \pi(r) := r + I$ die *natürliche Projektion*. Offenbar gilt

$$\pi(r+s) = \pi(r) + \pi(s), \quad \pi(r \cdot s) = \pi(r) \cdot \pi(s), \quad \pi(1) = 1 + I$$

und ferner ist π surjektiv.

Sei $J \in \mathcal{J}$; dann ist $\pi(J) \in \bar{\mathcal{J}}$. In der Tat, seien $a+I, b+I \in \pi(J)$ und $r+I \in R/I$ beliebig. Dann existieren $a_0, b_0 \in J$ mit $\pi(a_0) = a_0 + I, \pi(b_0) = b + I$, und da π surjektiv ist auch $r_0 \in R$ mit $\pi(r_0) = r + I$, sodass einerseits

$$(a+I) - (b+I) = \pi(a_0) - \pi(b_0) = \pi(a_0 - b_0) \in \pi(J),$$

da $a_0 - b_0 \in J$, und andererseits

$$(r+I) \cdot (a+I) = \pi(r_0) \cdot \pi(a_0) = \pi(r_0\, a_0) \in \pi(J)$$

wegen $r_0\, a_0 \in J$ folgt. Also folgt $\pi(J) \in \bar{\mathcal{J}}$.

Somit ist die Abbildung $\Phi\colon \mathcal{J} \to \bar{\mathcal{J}}, \Phi(J) := \pi(J)$ wohldefiniert. Wir zeigen, dass Φ bijektiv ist. Um die Surjektivität zu zeigen, beweisen wir zunächst, dass $\pi^{-1}(\bar{J}) \in \mathcal{J}$ für alle $\bar{J} \in \bar{\mathcal{J}}$. Sind a, $b \in \pi^{-1}(\bar{J})$, so folgt

$$\pi(a-b) = \underbrace{\pi(a)}_{\in \bar{J}} - \underbrace{\pi(b)}_{\in \bar{J}} \in \bar{J},$$

i.e. $a - b \in \pi^{-1}(\bar{J})$ und für beliebiges $r \in R$ gilt ähnlich

$$\pi(ra) = \underbrace{\pi(r)}_{\in R/I}\, \underbrace{\pi(a)}_{\in \bar{J}} \in \bar{J},$$

also auch $ra \in \pi^{-1}(\bar{J})$. Es folgt, dass $\pi^{-1}(\bar{J}) \in \mathcal{J}$. Ist also $\bar{J} \in \bar{\mathcal{J}}$ beliebig, so folgt aus der Surjektivität von π, dass $\Phi(\pi^{-1}(\bar{J})) = \pi(\pi^{-1}(\bar{J})) = \bar{J}$, wie gewünscht.

Zur Injektivität: Gilt $\Phi(J) = \Phi(J')$ für Ideale $J, J' \in \mathcal{J}$, so folgt

$$J = J + I = \pi(J) = \Phi(J) = \Phi(J') = \pi(J') = J' + I = J'$$

da $I \subseteq J, J'$. □

Als Anwendung davon haben wir folgendes hilfreiches Ergebnis.

Lemma 4.4. Sei R ein noetherscher Ring und $I \trianglelefteq R$ ein Ideal. Dann ist R/I noethersch.

Beweis. Sei $\bar{J}_1 \subseteq \bar{J}_2 \subseteq \cdots$ eine aufsteigende Kette $(\bar{J}_n)_{n\geq 1}$ von Idealen in R/I. Mit der Notation von Lemma 4.3, existiert eine Bijektion $\Phi\colon \mathcal{J} \to \bar{\mathcal{J}}$, sodass $(\Phi^{-1}(\bar{J}_n))_{n\geq 1}$ eine aufsteigende Kette von Idealen in R ist. Da R noethersch ist, wird $(\Phi^{-1}(\bar{J}_n))_{n\geq 1}$ nach Proposition 3.2 stationär und dementsprechend auch $(\Phi(\Phi^{-1}(\bar{J}_n)))_{n\geq 1} = (\bar{J}_n)_{n\geq 1}$, d.h. R/I ist noethersch. □

Unmittelbar folgern lässt sich aus diesem Lemma, aus Proposition 4.3 und Satz 3.2:

Folgerung 4.1. Ist R ein noetherscher Integritätsbereich und $I \in \operatorname{Spec} R$, dann ist R/I ein noetherscher Integritätsbereich und in Folge ein Ring mit Faktorzerlegung.

Definition 4.4. Seien R und S Ringe.

(1) Eine Abbildung $\phi\colon R \to S$ heißt *(Ring)-Homomorphismus*, wenn für alle $r, s \in R$ gilt, dass

$$\phi(r+s) = \phi(r) + \phi(s) \quad \text{und} \quad \phi(r \cdot s) = \phi(r) \cdot \phi(s).$$

Haben R und S zusätzlich Einselemente 1_R bzw. 1_S, verlangen wir auch, dass $\phi(1_R) = 1_S$ und nennen ϕ dann einen *Homomorphismus (von R nach S) mit Eins*.

(2) Ein injektiver Homomorphismus heißt *Monomorphismus* oder *(isomorphe) Einbettung* und wir schreiben $\phi\colon R \hookrightarrow S$.

(3) Ein surjektiver Homomorphismus heißt *Epimorphismus* und wir schreiben $\phi\colon R \twoheadrightarrow S$.

(4) Ein bijektiver Homomorphismus heißt *Isomorphismus*. Wir schreiben dann $\phi\colon R \xrightarrow{\sim} S$ und $R \cong S$. Man nennt R und S dann zueinander *isomorph*.

Beispiel 4.5. (1) Die Einbettungsabbildung $\iota_R : R \to R[X]$ aus Beispiel 3.3 ist ein injektiver Homomorphismus; hat R ein Einselement, dann ist ι_R auch ein Homomorphismus mit Eins. Ebenso ist $\hat{\iota} : K \to \hat{K}$ aus Beispiel 4.4 ein injektiver Homomorphismus mit Eins.

(2) In Beispiel 4.2 haben wir gezeigt, dass R und $R[X]/(X)$ miteinander identifizierbar sind (dieses Faktum haben wir dann in Proposition 4.1 verwendet). Formal gilt also $R \cong R[X]/(X)$.

(3) Die natürliche Projektion $\pi\colon R \to R/I$, die wir im Beweis von Lemma 4.3 verwendet haben ist ein Epimorphismus und wird dementsprechend auch *kanonischer Homomorphismus* bzw. *kanonischer Epimorphismus* genannt.

(4) Für alle Ringe R, S ist die Nullabbildung $r \mapsto 0_S$ ein Homomorphismus. Haben R und S allerdings Einselemente, so ist diese Abbildung nicht notwendigerweise (sofern das Null- und Einselement nicht zusammenfallen) ein Homomorphismus mit Eins.

(5) Die Identität auf einem Ring R ist immer ein Isomorphismus von R nach R.

Lemma 4.5. Seien R und S Ringe, $\phi\colon R \to S$ ein Homomorphismus. Dann gilt $\phi(0_R) = 0_S$ und $\phi(-r) = -\phi(r)$ für alle $r \in R$.

Beweis. Für beliebiges $r \in R$ haben wir

$$\phi(r) = \phi(0_R + r) = \phi(0_R) + \phi(r),$$

i.e. $\phi(0_R) = 0_S$ und demnach

$$0_S = \phi(0_R) = \phi(r + (-r)) = \phi(r) + \phi(-r),$$

also $\phi(-r) = -\phi(r)$. □

Im Gegensatz dazu folgt aus der Definition eines Ringhomomorphismus von R nach S *ohne* Eins nicht, dass das Einselement von R ins Einselement von S übergeht. Dementsprechend haben wir den zusätzlichen Homomorphismus von R nach S *mit* Eins eingeführt, wo dies garantiert ist.

Definition 4.5. Seien R und S Ringe, $\phi\colon R \to S$ ein Homomorphismus. Dann heißt die Menge

$$\ker \phi := \{r \in R \mid \phi(r) = 0_S\}$$

der *Kern von* ϕ. Ferner definieren wir das *Bild von* ϕ als

$$\operatorname{im} \phi := \{\phi(r) \mid r \in R\}.$$

Lemma 4.6. Seien R und S Ringe, $\phi\colon R \to S$ ein Homomorphismus. Dann gilt:

(1) $\ker \phi$ ist ein Ideal von R und $\operatorname{im} \phi$ ist ein Teilring von S.

(2) ϕ ist genau dann ein Monomorphismus, wenn $\ker \phi = \{0_R\}$.

Beweis. (1) Seien $r_1, r_2 \in \ker \phi$ und $r \in R$ beliebig. Dann gilt

$$\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0_S - 0_S = 0_S,$$

also $r_1 - r_2 \in \ker \phi$, sodass $\ker \phi$ eine additive Untergruppe von R ist. Ferner sehen wir $\phi(rr_1) = \phi(r)\,\phi(r_1) = \phi(r) \cdot 0_S = 0_S$, also ist $\ker \phi$ ein Linksideal. Ähnlich zeigt man, dass $\ker \phi$ auch ein Rechtsideal ist, i.e. $\ker \phi$ ist ein Ideal von R.

Die Behauptung, dass $\operatorname{im} \phi$ ein Teilring von S ist folgt unmittelbar aus der Definition von $\operatorname{im} \phi$.

(2) Ist ϕ ein Monomorphismus, so folgt unmittelbar aus Lemma 4.5, dass $\ker \phi$ trivial ist. Umgekehrt, falls $\ker \phi = \{0_R\}$, so folgt aus $\phi(r_1) = \phi(r_2)$ für $r_1, r_2 \in R$, dass $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0_S$, also $r_1 - r_2 \in \ker \phi$, d.h. $r_1 = r_2$. □

Satz 4.2. (Erster Isomorphiesatz für Ringe) Es sei $\phi: R \to S$ ein Ringhomomorphismus von R nach S. Dann induziert ϕ einen Isomorphismus

$$\phi^* : R/\ker \phi \xrightarrow{\sim} \operatorname{im} \phi, \quad \phi^*(r + \ker \phi) := \phi(r).$$

Insbesondere gilt $R/\ker \phi \cong \operatorname{im} \phi$.

Beweis. Sei $K := \ker \phi$. Wir zeigen schrittweise, dass ϕ^* ein wohldefinierter Isomorphismus von R nach S ist.

Wohldefiniertheit: Seien $r_1, r_2 \in R$ mit $r_1 + K = r_2 + K$. Dann gilt $r_1 - r_2 \in K$, also $\phi(r_1) - \phi(r_2) = \phi(r_1 - r_2) = 0$. Insbesondere muss $\phi(r_1) = \phi(r_2)$ gelten, d.h. $\phi^*(r_1 + K) = \phi^*(r_2 + K)$.

Homomorphieeigenschaft: Für alle $r, s \in R$ gilt

$$\begin{aligned}\phi^*((r+K)+(s+K)) &= \phi^*((r+s)+K) = \phi(r+s) = \phi(r) + \phi(s) \\ &= \phi^*(r+K) + \phi^*(s+K).\end{aligned}$$

Analog zeigt man, dass ϕ^* auch mit der Multiplikation verträglich ist.

Injektivität: Ist $0 = \phi^*(r + K) = \phi(r)$ für ein $r \in R$, so gilt offenbar $r \in K$. Daraus folgt, dass $\ker \phi^* = \{0 + K\}$ und somit ist ϕ^* nach Lemma 4.6 (2) injektiv.

Surjektivität: Das folgt unmittelbar aus der Definition von ϕ^*. □

Beispiel 4.6. (1) Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $\mathbb{Z}[X]/(p, X)$ ein Körper, da die Abbildung

$$\phi: \mathbb{Z}[X] \to \mathbb{F}_p, \quad \phi(f) := a_0 \,(\mathrm{mod}\, p) \quad \text{für } f = \sum_{i=0}^{n} a_i X^i,$$

Kern (p, X) hat mit Bild $\mathbb{F}_p$. Nach Satz 4.2 gilt also die Isomorphie $\mathbb{Z}[X]/(p, X) \cong \mathbb{F}_p$ und wir sehen insbesondere, dass (p, X) ein maximales Ideal in $\mathbb{F}_p$ ist.

(2) Offenbar können wir Beispiel 4.2 mit dem Ersten Isomorphiesatz für Ringe leicht formalisieren, indem wir die Abbildung $\phi: R[X] \to R$ betrachten, die jedem Polynom $f \in R[X]$ sein konstantes Glied zuweist.

5 Polynomringe

Definition 5.1. Sei S ein Ring und $R \leq S$ ein Unterring von S.

(1) Es sei $b \in S$ und $f \in R[X]$ beliebig mit $f = \sum_{i=0}^{n} a_i X^i$ für $a_0, \ldots, a_n \in R$. Wir definieren die Abbildung

$$\mathrm{ev}_b : R[X] \to S, \quad f \mapsto \mathrm{ev}_b(f) := \begin{cases} \sum_{i=0}^{n} a_i b^i, \text{ falls } f \neq 0, \\ 0, \text{ falls } f = 0, \end{cases}$$

genannt *Evaluationsabbildung bei* $b \in S$.

(2) Sei umgekehrt $f \in R[X]$ gegeben. Dann existiert eine natürliche Zuweisung $f \mapsto F$, wobei

$$F : S \to S, \quad b \mapsto f(b) := \mathrm{ev}_b(f).$$

Wir nennen dann $b \in S$ eine *Nullstelle* von f, falls $f(b) = 0$ gilt, i.e. $f \in \ker \mathrm{ev}_b$. Wir nennen diese Zuweisung

$$\mathrm{Polfkt} : R[X] \to \{\phi : S \to S \text{ Abbildung}\}.$$

Beispiel 5.1. Ist S ein kommutativer Ring mit Eins, so ist die Evaluationsabbildung offenbar ein Ringhomomorphismus. Bei nicht-kommutativen Ringen ist das nicht der Fall. Sei beispielsweise $R = S = M_2(\mathbb{Z})$ der Matrizenring aus Beispiel 2.2 (3). Setzen wir $f := X - A$ und $g := X + A$ für fixiertes $A \in M_2(\mathbb{Z})$, dann folgt $f \cdot g = X^2 - A^2$. Insbesondere sei $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ und $B := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Dann gilt

$$\mathrm{ev}_B(f \cdot g) = B^2 - A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^2 - \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ aber}$$
$$\mathrm{ev}_B(f) \cdot \mathrm{ev}_B(g) = \left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right) \cdot \left(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix},$$

also ist ev_B nicht multiplikativ.

In den reellen Zahlen verwenden wir die Begriffe „Polynom“ und „Polynomfunktion“ synonym. Formal ist Polfkt in $\mathbb{R}[X]$ also injektiv. Wann ist das allgemein der Fall, i.e. wann kann man ein Polynom mit seiner Polynomfunktion identifizieren? Seien dazu $f, g \in R[X]$ mit $\mathrm{Polfkt}(f) = \mathrm{Polfkt}(g)$. Dann gilt:

$$\begin{aligned} \mathrm{Polfkt}(f) = \mathrm{Polfkt}(g) &\Leftrightarrow f(b) = g(b) \text{ für alle } b \in S \\ &\Leftrightarrow \mathrm{ev}_b(f) = \mathrm{ev}_b(g) \text{ für alle } b \in S \\ &\Leftrightarrow \mathrm{ev}_b(f - g) = 0 \text{ für alle } b \in S \\ &\Leftrightarrow f - g \in \ker \mathrm{ev}_b \text{ für alle } b \in S \\ &\Leftrightarrow f - g \in \bigcap_{b \in S} \ker \mathrm{ev}_b. \end{aligned}$$

Also ist Polfkt genau dann injektiv, wenn $\bigcap_{b \in S} \ker \mathrm{ev}_b$ trivial ist. Bei reellen Polynomen ist das offenbar der Fall, aber das ist nicht immer so:

Beispiel 5.2. Betrachten wir die Polynome $f := X^5, g := X$ in $S := \mathbb{Z}/5\mathbb{Z}$. Dann gilt

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 2, \quad f(3) = 3, \quad f(4) = 4,$$

also $f = g$. Somit gilt $0 \neq X^5 - X \in \bigcap_{b \in S} \ker \mathrm{ev}_b$.

Proposition 5.1. Sei K ein Körper und $f \in K[X]$ ein Polynom mit $\deg(f) \geq 0$. Es gilt:

(1) $f \in K[X]^* \Leftrightarrow \deg(f) = 0$.

(2) Ist $\deg(f) = 1$, dann ist f irreduzibel in $K[X]$.

(3) Ist $\deg(f) \geq 1$ und hat f eine Nullstelle $\alpha \in K$, dann folgt $(X - \alpha) \mid f$. Insbesondere gilt für f reduzibel dann, dass $\deg(f) > 1$.

(4) Ist $\deg(f) = 2$ oder $\deg(f) = 3$, dann ist f genau dann irreduzibel, wenn f keine Nullstelle in K hat.

Beweis. (1) Siehe Lemma 4.1.

(2) Ist $\deg(f)=1$, dann gilt $f\in K[X]$, wobei $f\neq 0$ und $f\notin K[X]^*$ nach (1). Sei $g\in K[X]$ mit $g|f$; dann gibt es $q\in K[X]$ mit $f=gq$, sodass

$$1=\deg(f)=\deg(gq)=\deg(g)+\deg(q).$$

Dann muss aber mindestens eines der Polynome von Grad Null sein, i.e. Einheit.

(3) Sei $\deg(f)\geq 1$ und $f(\alpha)=0$. Sei $g:=X-\alpha$. Nach Proposition 4.1 ist $K[X]$ euklidisch bezüglich deg, sodass $q,r\in K[X]$ mit $f=gq+r$ existieren und $\deg(r)<\deg(g)=1$. Dann folgt

$$0=f(\alpha)=g(\alpha)\,q(\alpha)+r(\alpha),$$

also $r(\alpha)=0$. Daraus folgt $f=gq$, i.e. $g|f$. Ist $\deg(f)>1$, so ist $\deg(q)>0$, also f nicht irreduzibel.

(4) Sei $\deg(f)=2$ oder $\deg(f)=3$. Falls f eine Nullstelle $\alpha\in K$ hat, dann ist f nach (3) nicht irreduzibel. Umgekehrt, nehmen wir an, dass f nicht irreduzibel in $K[X]$ ist. Dann können wir $f=pq$ mit $p,q\in K[X]$ schreiben, wobei $p,q\neq 0$ und $p,q\notin K[X]^*$. Insbesondere ist $\deg(p)>0$ und $\deg(q)>0$, sodass aus

$$\deg(p)+\deg(q)=\deg(pq)=\deg(f)\in\{2,3\}$$

folgt, dass einer der beiden Grade genau Eins ist. Sei o. B. d. A. angenommen, dass $\deg(p)=1$, also $p=a_1X+a_0$ für $a_0,a_1\in K$ und $a_1\neq 0$. Dann gilt aber für $\alpha:=(-a_0)\,a_1^{-1}$, dass

$$f(\alpha)=p((-a_0)\,a_1^{-1})\,q((-a_0)\,a_1^{-1})=(a_1\,(-a_0)\,a_1^{-1}+a_0)\,q((-a_0)\,a_1^{-1})=0.$$

Also hat f eine Nullstelle bei $\alpha\in K$. □

Daraus ergibt sich ein wohlbekanntes Resultat:

Folgerung 5.1. Sei K ein Körper und $f\in K[X]$ nicht das konstante Nullpolynom. Dann hat f höchstens $\deg(f)$ Nullstellen.

Beweis. Man wende vollständige Induktion nach $\deg(f)$ an und verwende dann Proposition 5.1 (3). □

Die Annahme, dass K ein Körper ist, ist wesentlich, wie folgendes Beispiel zeigt.

Beispiel 5.3. (1) Das Polynom $2X$ hat in $\mathbb{Z}/4\mathbb{Z}$ die zwei Nullstellen 0 und 2, obwohl $\deg(2X)=1$.

(2) Das Polynom $f:=X^4+2X^2+1=(X^2+1)^2$ ist offenbar reduzibel in $\mathbb{R}[X]$, hat aber keine reellen Nullstellen. Das zeigt, dass die Annahme $\deg(f)=2,3$ in Proposition 5.1 (4) wichtig ist.

Folgerung 5.2. Sei K ein Körper und $f\in K[X]$ ein irreduzibles Polynom. Dann ist $K[X]/(f)$ ein Körper.

Beweis. Da f irreduzibel ist, ist (f) im Hauptidealring (wegen Proposition 4.1) $K[X]$ maximal und somit ist $K[X]/(f)$ nach Proposition 4.3 sogar ein Körper. □

Später hilfreich sein wird dieses Resultat, das umgangssprachlich auch als „*Freshman's Dream*“ bekannt ist:

Lemma 5.1. Sei $p\in\mathbb{P}$ eine Primzahl. Dann gilt in $\mathbb{F}_p[X,Y]$,

$$(X+Y)^p=X^p+Y^p.$$

Beweis. Da $\mathbb{F}_p[X,Y]$ ein kommutativer Ring ist gilt nach dem Binomischen Lehrsatz

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

Untersuchen wir den dort vorkommenden Binomialkoeffizienten $\binom{p}{k}$ für $0<k<p$. Per Definition haben wir $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, also $p! = \binom{p}{k}(p-k)!k!$; insbesondere teilt p die rechte Seite dieser letzten Gleichung. Da p eine Primzahl ist, gilt $p \mid \binom{p}{k}$ oder $p \mid (p-k)!$ oder $p \mid k!$ und offenbar ist wegen $0<k<p$ die einzige Möglichkeit $p \mid \binom{p}{k}$. Folglich fallen alle Summanden mit $0<k<p$ aus der obigen Summe weg und es verbleibt

$$(X+Y)^p = \binom{p}{0} X^{p-0} Y^0 + \binom{p}{p} X^{p-p} Y^p = X^p + Y^p.$$

□

Unmittelbar hat dieses Lemma den *Kleinen Satz von Fermat*[5.1] als Konsequenz.

Lemma 5.2. (Fermat) Sei $p \in \mathbb{P}$ eine Primzahl. Dann gilt $a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{Z}$.

Beweis. Es reicht die Behauptung für natürliches a zu zeigen, indem wir vollständige Induktion nach $a \in \mathbb{N}_0$ führen. Für $a = 0$ ist die Aussage offensichtlich wahr und setzen wir voraus, dass sie für $a \in \mathbb{N}_0$ stimmt, so folgt aus Lemma 5.1 sofort

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1,$$

was zu zeigen war. □

Kehren wir nun zum Studium von Polynomringen zurück. Unter anderem ergibt sich folgende wichtige Anwendung aus dem anfänglich etwas unscheinbar wirkenden Korollar 5.2:

Satz 5.1. Es gilt $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$.

Dazu zunächst Wiederholung eines bekannten Hilfssatzes.

Lemma 5.3. Sei $f \in \mathbb{R}[X]$ ein Polynom und $\xi = a + b\sqrt{-1}$ mit $a, b \in \mathbb{R}$ eine Nullstelle von f. Dann ist auch $\bar{\xi} = a - b\sqrt{-1}$ eine Nullstelle von f.

Beweis. Sei $f = \sum_{i=0}^{n} a_i X^i$ für $a_0, \ldots, a_n \in \mathbb{R}$ und $n = \deg(f)$. Ist $f(\xi) = 0$, so folgt

$$0 = \sum_{i=0}^{n} a_i \xi^i = f(\xi)$$

und daher

$$f(\bar{\xi}) = \sum_{i=0}^{n} a_i (\bar{\xi})^i = \sum_{i=0}^{n} a_i \bar{\xi^i} = \sum_{i=0}^{n} \overline{a_i \xi^i} = \overline{\sum_{i=0}^{n} a_i \xi^i} = 0,$$

wie gewünscht. □

Der Beweis ist nun eine einfache Anwendung von Satz 4.2.

5.1. Pierre de Fermat (1607 – 1665), französischer Mathematiker und Jurist

Beweis. Da X^2+1 keine reellen Nullstellen hat, ist das Polynom X^2+1 in $\mathbb{R}[X]$ nach Proposition 5.1 (4) irreduzibel, sodass

$$\mathbb{R}[X]/(X^2+1)$$

nach Folgerung 5.2 ein Körper ist. Nach Beispiel 5.1 ist

$$\phi\colon \mathbb{R}[X] \to \mathbb{C}, \quad \phi(f) := \mathrm{ev}_{\sqrt{-1}}(f) = f(\sqrt{-1})$$

ein Homomorphismus und sogar surjektiv. In der Tat, ist $z = a + b\sqrt{-1}$ mit $a, b \in \mathbb{R}$ eine komplexe Zahl, so gilt $\phi(a + bX) = a + b\sqrt{-1} = z$. Weiterhin ist $\ker \phi = \{f \in \mathbb{R}[X] \mid \phi(f) = f(\sqrt{-1}) = 0\}$, i.e. die Menge der reellen Polynome f mit Nullstelle $\sqrt{-1}$. Aus Lemma 5.3 ist für diese Polynome auch $-\sqrt{-1}$ eine Nullstelle, f hat also Teiler $X \pm \sqrt{-1}$ nach Proposition 5.1, i.e. $f \in (X^2+1)$. Daraus folgt $\ker \phi = (X^2+1)$, sodass aus dem Ersten Isomorphiesatz für Ringe (Satz 4.2) folgt, $\mathbb{R}[X]/(X^2+1) \cong \operatorname{im} \phi$ und da ϕ surjektiv ist, insbesondere

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C},$$

was zu zeigen war. □

Tatsächlich verhält sich (wenig überraschend) der Körper $\mathbb{R}[X]/(X^2+1)$ wie die bereits bekannten komplexen Zahlen und verfügt über deren gewohnten Eigenschaften. Es ist also nicht nur denkbar, die *Isomorphie* von $\mathbb{R}[X]/(X^2+1)$ und dem bereits bestehenden[5.2] Objekt $\mathbb{C}$ zu zeigen, sondern die komplexen Zahlen ausgehend von $\mathbb{R}[X]/(X^2+1)$ zu *definieren*.

Setzen wir dazu $I := (X^2+1)$ als das von X^2+1 erzeugte Hauptideal in $\mathbb{R}[X]$. Definieren wir dann

$$\sqrt{-1}_I := X + I,$$

so folgt

$$(\sqrt{-1}_I)^2 = (X+I)^2 = (X^2+I) = -1 + I,$$

wobei $-1+I$ genau das additive Inverse der Eins in $\mathbb{R}[X]/I = \mathbb{R}[X]/(X^2+1)$ ist. Die Zahl $\sqrt{-1}_I$ spielt also die Rolle der imaginären Einheit in diesem neuen Körper. Weitere Beobachtung zeigt außerdem, dass

$$\begin{aligned}\mathbb{R}[X]/I = \{f + I \mid f \in \mathbb{R}[X]\} &= \left\{\sum_{i=0}^{n} a_i X^i + I \mid a_0, \ldots, a_1 \in \mathbb{R}\right\} \\ &= \{a_0 + a_1 X + I \mid a_0, a_1 \in \mathbb{R}\},\end{aligned}$$

wobei die Addition und Multiplikation von Elementen $a_0 + a_1 X + I$ in $\mathbb{R}[X]/I$ jener in $\mathbb{C}$ entspricht. Das legt nahe, $\mathbb{C}$ als die Menge der Restklassen $a_0 + a_1 X + I$ zu definieren mit „reellem Teil“ a_0, „imaginärem Teil“ a_1 und „imaginärer Einheit“ $\sqrt{-1}_I = X + I$.[5.3]

Ebenfalls erhalten wir die Einbettung

$$\rho_{\mathbb{R}}\colon \mathbb{R} \underset{\iota_{\mathbb{R}}}{\hookrightarrow} \mathbb{R}[X] \underset{\pi}{\twoheadrightarrow} \mathbb{R}[X]/(X^2+1)$$

der reellen Zahlen in den komplexen Zahlen. Das Bild im $\rho_{\mathbb{R}} = \rho_{\mathbb{R}}(\mathbb{R})$ entspricht genau dem Unterkörper $\{a + 0\sqrt{-1} \mid a \in \mathbb{R}\}$. Die Bedeutung der komplexen Zahlen ergibt sich daraus, dass $\mathbb{C}$ nicht nur topologisch vollständig ist (bezüglich der gewohnten euklidischen Metrik), sondern auch das algebraische Pendant erfüllt, die sogenannte *algebraische Abgeschlossenheit*.

5.2. Platonisten mögen hier „bestehend“ lesen, Formalisten „eingeführt“ und Konstruktivisten „konstruiert“.

5.3. Alternativ ergibt sich aus dieser Darstellung ein expliziter Isomorphismus $a_0 + a_1 X \mapsto a_0 + a_1\sqrt{-1}$ in Satz 5.1.

Lemma 5.4. Es sei K ein Körper und $f \in K[X]$ ein Polynom. Dann sind äquivalent:

(1) f ist genau dann irreduzibel, wenn $\deg(f) = 1$.

(2) Ist f nicht konstant mit $n := \deg(f)$, dann gibt es eindeutig bestimmte $\alpha_0, \ldots, \alpha_n$ mit

$$f = \alpha_0 \prod_{i=1}^{n} (X - \alpha_i).$$

(3) Falls f nicht konstant ist, hat f eine Nullstelle in K.

Beweis. (1) $\Rightarrow$ (2) Sei $f \in K[X]$ nicht-konstant mit $f = \sum_{i=1}^{n} a_i X^i$. Da $K[X]$ ein Hauptidealring ist (Proposition 4.1) und daher faktoriell (Satz 3.4) gibt es eindeutig bestimmte irreduzible Polynome $p_1, \ldots, p_m \in K[X]$, sodass $f = \varepsilon \cdot \prod_{i=1}^{m} p_i$ für eine Einheit $\varepsilon \in K[X]^*$. Nach Annahme gilt $p_i = c_i X + b_i$ mit $c_i \neq 0$ für jedes $i \in \{1, \ldots, m\}$, sodass

$$f = \varepsilon \cdot \prod_{i=1}^{m} p_i = \varepsilon \cdot \prod_{i=1}^{m} (c_i X + b_i).$$

Aus Proposition 4.1 (1) folgt, dass $m = n$, also

$$f = \varepsilon \cdot \prod_{i=1}^{n} c_i^{-1} \cdot \prod_{i=1}^{n} (X + b_i c_i^{-1}).$$

Sei

$$\alpha_0 := \varepsilon \cdot \prod_{i=1}^{n} c_i^{-1} \quad \text{und} \quad a_i := -b_i c_i^{-1};$$

dann folgt $f = \alpha_0 \prod_{i=1}^{n} (X - \alpha_i)$.

(2) $\Rightarrow$ (3) Das folgt unmittelbar aus der Darstellung von f als Produkt von Linearfaktoren.

(3) $\Rightarrow$ (1) Sei $f \in K[X]$ irreduzibel. Dann ist f nicht das Nullpolynom und keine Einheit, daher $\deg(f) \geq 1$. Nach Annahme hat f also eine Nullstelle $\alpha \in K$; also folgt aus Proposition 5.1 (3), dass $X - \alpha$ das Polynom f teilt. Da f aber irreduzibel ist, muss schon $f \sim X - \alpha$ gelten, d.h. $\deg(f) = 1$. □

Definition 5.2. Ein Körper, der die äquivalenten Bedingungen aus Lemma 5.4 erfüllt, heißt *algebraisch abgeschlossen*.

Satz 5.2. (Fundamentalsatz der Algebra) $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis. Siehe [Kal15] für eine der unzähligen Beweismethoden. □

Satz 5.3. Es existiert kein endlicher algebraisch abgeschlossener Körper.

Beweis. Sei vorausgesetzt, dass K ein endlicher algebraisch abgeschlossener Körper mit Elementen $\alpha_1, \ldots, \alpha_n \in K$ ist. Da K insbesondere ein Integritätsbereich ist, gilt $n \geq 2$ mit $0 \neq 1$. Dann hat aber das nicht-konstante Polynom

$$1 + \prod_{i=1}^{n} (X - \alpha_i)$$

keine Nullstelle in K, im Widerspruch zu Lemma 5.4. □

6 Quadratische Zahlkörper und Ganzheitsringe

Wir kennen mittlerweile einige interessante und hilfreiche Konstruktionen von Ringen. Eine weitere Konstruktion, um Gegenbeispiele von Kästchen 3.5 zu finden, führen wir jetzt ein.

Sei $d \in \mathbb{Z}$ mit $d \neq 0$ und $d \neq 1$ eine quadratfreie ganze Zahl (d.h., aus $n \mid d$ und $n = m^2$ für ein $m \in \mathbb{Z}$ folgt, dass $n = 1$). Wir setzen[6.1]

$$p_d := \begin{cases} X^2 - d, \text{ falls } d \equiv 2, 3 \pmod 4, \\ X^2 - X + \frac{1-d}{4}, \text{ falls } d \equiv 1 \pmod 4 \end{cases}$$

sowie

$$\omega_d := \begin{cases} \sqrt{d}, \text{ falls } d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, \text{ falls } d \equiv 1 \pmod 4 \end{cases}, \quad \omega_d^* := \begin{cases} -\sqrt{d}, \text{ falls } d \equiv 2, 3 \pmod 4, \\ \frac{1-\sqrt{d}}{2}, \text{ falls } d \equiv 1 \pmod 4. \end{cases}$$

Dann ist p_d ein ganzzahliges Polynom, also Element von $\mathbb{Z}[X]$, somit von $\mathbb{Q}[X]$ und als Polynom in $\mathbb{Q}[X]$ sogar irreduzibel. In der Tat zerfällt $p_d = (X - \omega_d)(X - \omega_d^*)$ in Linearfaktoren über $\mathbb{C}$, wobei aber $\sqrt{d} \notin \mathbb{Q}$, da wir d quadratfrei gewählt haben, sodass per Definition $\omega_d, \omega_d^* \notin \mathbb{Q}$. Es folgt, dass p_d keine rationalen Nullstellen hat, nach Proposition 5.1 (4) also irreduzibel in $\mathbb{Q}[X]$ ist. Aus Folgerung 5.2 folgt, dass $\mathbb{Q}[X]/(p_d)$ ein Körper ist.

Definition 6.1. Wir nennen den Körper

$$\mathbb{Q}(\sqrt{d}) := \mathbb{Q}[X]/(p_d),$$

für $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, *quadratischen Zahlkörper*.

Die Elemente dieses Körpers können ähnlich wie in $\mathbb{C}$ dargestellt werden:

Lemma 6.1. Es gilt

$$\mathbb{Q}(\sqrt{d}) \cong \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Beweis. Sei, ähnlich wie im Beweis von Satz 5.1

$$\phi \colon \mathbb{Q}[X] \to \mathbb{C}, \quad \phi(f) := f(\omega_d)$$

die Evaluationsabbildung. Ist $f \in \mathbb{Q}[X]$ ein beliebiges Polynom, so folgt aus Proposition 4.1, dass $f = qp_d + r$ für $q, r \in \mathbb{Q}[X]$ und $\deg(r) < \deg(p_d) = 2$. Wir können also $r = a + bX$ für $a, b \in \mathbb{Q}[X]$ schreiben, sodass

$$f(\omega_d) = a + b\omega_d.$$

Liegt f im Kern von ϕ, so gilt $a + b\omega_d = 0$; insbesondere folgt aus $\omega_d \notin \mathbb{Q}$, dass $a = b = 0$. Daraus folgt $r = 0$ und $f = qp_d$, i.e. $\ker \phi = (p_d)$.

Aus der obigen Bemerkung wissen wir $\operatorname{im} \phi = \{a + b\omega_d \mid a, b \in \mathbb{Q}\}$. Wir zeigen, dass $\operatorname{im} \phi = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Ist $d \equiv 2, 3 \pmod 4$, so gilt per Definition $\omega_d = \sqrt{d}$; sei also $d \equiv 1 \pmod 4$ und daher $\omega_d = \frac{1+\sqrt{d}}{2}$. Sei $a + b\omega_d \in \operatorname{im} \phi$ für $a, b \in \mathbb{Q}$ beliebig. Einsetzen liefert dann

$$a + b\omega_d = a + \frac{b + b\sqrt{d}}{2} = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{d} \in \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

6.1. Der Grund, warum wir p_d und ω_d so wählen, wird in Proposition 6.3 aufgeklärt.

Sei umgekehrt $p+q\sqrt{d}$ mit $p,q\in\mathbb{Q}$. Schreiben wir $\sqrt{d}=2\omega_d-1$, so folgt

$$p+q\sqrt{d}=p+q\,(2\omega_d-1)=(p-q)+2\,q\omega_d\in\operatorname{im}\phi.$$

Die Behauptung folgt also aus Satz 4.2. □

Auf diese Weise ist es dann natürlich $\mathbb{Q}(\sqrt{d})$ als zweidimensionalen Vektorraum über $\mathbb{Q}$ (vermöge der gewohnten Vektoraddition und Skalarmultiplikation) mit Basis $\{1,\sqrt{d}\}$ bzw. $\{1,\omega_d\}$ bzw. $\{1,\omega_d^*\}$ aufzufassen. Wir sagen dann, dass $\mathbb{Q}(\sqrt{d}):\mathbb{Q}$ eine Körpererweiterung vom Grad

$$[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))=2$$

ist. (Mehr dazu im Kapitel über Körper.)

Lemma 6.2. $\mathbb{Q}(\sqrt{d})$ ist ein zweidimensionaler $\mathbb{Q}$-Vektorraum mit Basen $\{1,\sqrt{d}\}$, $\{1,\omega_d\}$ und $\{1,\omega_d^*\}$.

Beweis. Identifizieren wir, Lemma 6.1 folgend, $\mathbb{Q}(\sqrt{d})$ als Teilkörper von $\mathbb{C}$, so folgt unmittelbar, dass $\mathbb{Q}(\sqrt{d})$ ein Vektorraum über $\mathbb{Q}$ ist. Weisen wir nun nach, dass die behaupteten Mengen auch Basen dieses Vektorraums sind.

Offenbar ist $\{1,\sqrt{d}\}$ ein Erzeugendensystem. Sei $a+b\sqrt{d}=0$ mit $a,b\in\mathbb{Q}$. Gilt $b\neq 0$, so folgt, dass $\sqrt{d}=-\frac{a}{b}\in\mathbb{Q}$, ein Widerspruch zur Irrationalität von $\sqrt{d}$. Demnach muss $a=b=0$ gelten. Somit ist $\{1,\sqrt{d}\}$ eine Basis von $\mathbb{Q}(\sqrt{d})$ und $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{d})=2$.

Es verbleibt noch zu zeigen, dass auch $\{1,\omega_d\}$ eine Basis ist; der Nachweis für $\{1,\omega_d^*\}$ ist ähnlich. Im Fall $d\equiv 2,3\pmod 4$, gilt $\omega_d=\sqrt{d}$, sodass wir annehmen können, dass $d\equiv 1\pmod 4$. Ist aber

$$0=a+b\omega_d=a+b\left(\frac{1+\sqrt{d}}{2}\right)=\left(a+\frac{b}{2}\right)+\frac{b}{2}\sqrt{d}$$

für $a,b\in\mathbb{Q}$, so folgt aus der linearen Unabhängigkeit von $\{1,\sqrt{d}\}$, dass $a=b=0$, also ist auch $\{1,\omega_d\}$ eine Basis von $\mathbb{Q}(\sqrt{d})$. □

Proposition 6.1. Sei $\mathcal{O}_d:=\mathbb{Z}[X]/(p_d)$ ein kommutativer Ring mit Eins. Dann ist

$$\phi_d:\mathcal{O}_d\to\mathbb{Q}(\sqrt{d}),\quad \phi_d(f+p_d\mathbb{Z}[X]):=f+p_d\mathbb{Q}[X]$$

eine isomorphe Einbettung von Ringen.

Noch können wir diese Proposition nicht beweisen; sie hat aber interessante Konsequenzen, die weitere Hinweise zu den Umkehrungen in Kästchen 4 liefern werden, wie folgendes Ergebnis zeigt.

Folgerung 6.1. Das Hauptideal (p_d) ist in $\mathbb{Z}[X]$ prim.

Beweis. Sei ϕ die Abbildung aus Proposition 6.1. Da $\mathbb{Q}(\sqrt{d})$ als Körper nullteilerfrei ist, ist insbesondere $\operatorname{im}\phi\leq\mathbb{Q}(\sqrt{d})$ nullteilerfrei. Aber $\operatorname{im}\phi\cong\mathcal{O}_d$, also ist $\mathcal{O}_d=\mathbb{Z}[X]/(p_d)$ nullteilerfrei und daher ein Integritätsbereich. Aus Proposition 4.3 folgt, dass (p_d) ein Primideal in $\mathbb{Z}[X]$ ist. □

Definition 6.2. Sei R ein faktorieller Ring und $f\in R[X]$ mit $n:=\deg(f)$ und

$$f=\sum_{i=0}^{n}a_i\,X^i,\quad a_0,\ldots,a_n\in R,$$

nicht das Nullpolynom. Dann heißt f *primitiv*, wenn ein (und damit jeder) Maximalteiler von $\{a_0, \dots, a_n\}$ eine Einheit in R ist.

Beispiel 6.1. Sei $f := \sum_{i=0}^{n} a_i X^i$ in $R[X]$, R faktoriell.

(1) f ist offenbar primitiv, so $a_n \sim 1$. Falls sogar $a_n = 1$ gilt, nennen wir f *normiert* bzw. *monisch*.

(2) Ist f irreduzibel und $\deg(f) \geq 1$, dann ist f primitiv, da jedes nicht primitive Polynom durch Rausfaktorisieren des nichttrivialen Maximalteilers der Koeffizienten offenbar reduzibel ist.

Das folgende Lemma wurde von Gauß[6.2] in seinen *Disquisitiones Arithmeticae* (1801) präsentiert.

Lemma 6.3. (Lemma von Gauß) Sei R ein faktorieller Ring und seien $f, g \in R[X]$ primitive Polynome. Dann ist das Produkt $f \cdot g$ auch primitiv.

Beweis. Wir schreiben für $n := \deg(f), m := \deg(g)$, die Ausdrücke $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i$ an. Nehmen wir indirekt an, dass $f \cdot g$ nicht primitiv ist. Dann existiert ein irreduzibles Element $p \in R$, sodass $p \mid \sum_{i=0}^{k} a_i\, b_{k-i}$ für alle $k \in \mathbb{N}_0$. Da f und g primitiv sind, existieren minimale $i_0 \in \{0, \dots, n\}$ und $j_0 \in \{0, \dots, m\}$, sodass einerseits $p \nmid a_{i_0}$ und $p \nmid b_{j_0}$. Sei $k_0 := i_0 + j_0$ und betrachten wir den k_0-ten Koeffizienten $\sum_{\ell=0}^{k_0} a_\ell\, b_{k_0-\ell}$; nach Annahme ist p Teiler davon. Für $\ell < i_0$ folgt aus der Minimalität von i_0, dass $p \mid a_\ell$, also $p \mid \sum_{\ell=0}^{i_0-1} a_\ell\, b_{k_0-\ell}$ und daher

$$p \mid \sum_{\ell=i_0}^{k_0} a_\ell\, b_{k_0-\ell}.$$

Andererseits folgt für $\ell > i_0$, dass $k_0 - \ell < k_0 - i_0 = j_0$, also $p \mid b_{k_0-\ell}$, sodass auch

$$p \mid \sum_{\ell=i_0+1}^{k_0} a_\ell\, b_{k_0-\ell}.$$

Insgesamt ergibt sich daraus $p \mid a_{i_0} b_{k_0-i_0} = a_{i_0} b_{j_0}$. Da R faktoriell ist, ist p nach Satz 3.3 auch prim, sodass $p \mid a_{i_0}$ oder $p \mid b_{j_0}$; das ist ein Widerspruch. Es folgt, dass $f \cdot g$ primitiv sein muss. □

Ein alternativer, eleganterer Beweis[6.3]:

Beweis. Sei $\gamma \in R$ ein gemeinsamer Teiler der Koeffizienten von $f \cdot g$. Angenommen, $\gamma \notin R^*$. Sei $p \in R$ ein irreduzibler Faktor von γ. Da R faktoriell ist, ist p ein Primelement, also $R' := R/(p)$ ein Integritätsbereich. Insbesondere ist nach Proposition 3.1 $R'[X]$ ein Integritätsbereich.

Sei $\pi : R \to R', \pi(r) := r + (p)$, die kanonische Projektion. Definieren wir weiters

$$\phi : R[X] \to R'[X], \quad \phi\left(\sum_{i=0}^{n} a_i X^i\right) := \sum_{i=0}^{n} \pi(a_i)\, X^i$$

für ein Polynom mit Koeffizienten $a_i \in R, 0 \leq i \leq n$. Da jeder Koeffizient von $fg \in R[X]$ nach Annahme durch p teilbar ist, folgt $\phi(f)\,\phi(g) = \phi(fg) = 0 \in R'[X]$. Da $R'[X]$ ein Integritätsbereich ist, folgt $\phi(f) = 0$ oder $\phi(g) = 0$, ein Widerspruch dazu, dass f und g primitiv sind. Also ist $\gamma \in R^*$ und folglich ist $f \cdot g$ primitiv. □

6.2. Carl Friedrich Gauß (1777 – 1855), deutscher Mathematiker, Statistiker, Astronom, Geodät, Elektrotechniker und Physiker

6.3. Vielen Dank an Jianghua Lu (The University of Hong Kong) für diesen Beweis.

Ist $f := \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ nicht Null, dann ist $\frac{1}{d} \cdot f$ mit $d := \mathrm{ggT}(a_0, \ldots, a_n)$ ein primitives Polynom in $\mathbb{Z}[X]$. Somit können wir aus beliebigen Polynomen $g := \sum_{i=0}^{m} \frac{b_i}{c_i} X^i \in \mathbb{Q}[X]$, $g \neq 0$ primitive ganzzahlige Polynome erhalten, indem wir g zuerst mit dem Produkt $\prod_{i=0}^{m} c_i$ multiplizieren, um $g' := (\prod_{i=0}^{m} c_i) \cdot g \in \mathbb{Z}[X]$ zu erhalten und dann auf primitive Gestalt bringen.

Lemma 6.4. Ein primitives Polynom $f \in \mathbb{Z}[X]$ ist in $\mathbb{Z}[X]$ genau dann irreduzibel, wenn es in $\mathbb{Q}[X]$ irreduzibel ist.

Beweis. ($\Leftarrow$) Nehmen wir an, dass f in $\mathbb{Q}[X]$ irreduzibel ist und sei $f = g \cdot h$ für $g, h \in \mathbb{Z}[X]$; wir wollen zeigen, dass g oder h in $\mathbb{Z}[X]$ Einheit ist. Da $f \in \mathbb{Q}[X]$ irreduzibel ist, folgt, dass g oder h in $\mathbb{Q}[X]$ Einheit ist. Nehmen wir o. B. d. A. an, dass $g \in \mathbb{Q}[X]^* = \mathbb{Q}^*$. Dann folgt $g \in \mathbb{Q}^* \cap \mathbb{Z}[X] = \mathbb{Z} \setminus \{0\}$. Schreiben wir für $n := \deg(f)$ das Polynom f als $f = \sum_{i=0}^{n} a_i X^i$ für $a_0, \ldots, a_n \in \mathbb{Z}$, so folgt $g \mid a_i$ für alle $i \in \{1, \ldots, n\}$. Nach Annahme ist f primitiv, also folgt, dass g Einheit in $\mathbb{Z}[X]$ ist.

($\Leftarrow$) Sei vorausgesetzt, dass $f \in \mathbb{Z}[X]$ irreduzibel ist und sei $f = g \cdot h$ für $g, h \in \mathbb{Q}[X]$; wir wollen jetzt zeigen, dass g oder h in $\mathbb{Q}[X]$ Einheit ist. Nach unserer obigen Bemerkung existieren $p, q \in \mathbb{Q}$, sodass $p \cdot g$ und $q \cdot h$ in $\mathbb{Z}[X]$ primitiv sind. Nach Lemma 6.3 ist dann auch $(p \cdot g) \cdot (q \cdot h) = (pq) \cdot (gh) = pqf$ in $\mathbb{Z}[X]$ primitiv. Da f selbst primitiv ist, folgt zunächst, dass $pq \in \mathbb{Z}$ und nun aus der Primitivität von pqf sogar $pq = \pm 1$, i.e. $\pm f = (pg) \cdot (qh)$, sodass aus der Irreduzibilität von f in $\mathbb{Z}[X]$ folgt, dass pg oder qh Einheit in $\mathbb{Z}[X]$ ist. Insbesondere ist dann g oder h aber Einheit in $\mathbb{Q}[X]$, was wir zeigen wollten. □

Beispiel 6.2. Die Bedingung, dass f in Lemma 6.4 primitiv ist, ist wesentlich. Beispielsweise ist $f = 2X + 2$ in $\mathbb{Z}[X]$ nicht irreduzibel, da $f = 2(X + 1)$, aber 2 ist in den rationalen Zahlen eine Einheit, d.h. f ist in $\mathbb{Q}[X]$ irreduzibel.

Eine nützliche Umformulierung von Lemma 6.4:

Folgerung 6.2. Sei $f \in \mathbb{Z}[X]$ ein primitives Polynom. Zerfällt f in ein Produkt $f = gh$ mit g, $h \in \mathbb{Q}[X]$, so existieren primitive Polynome $g', h' \in \mathbb{Z}[X]$, sodass $g \sim g'$ und $h \sim h'$ in $\mathbb{Q}[X]$ und $f = g'h'$. Insbesondere unterscheiden sich die Faktoren in $\mathbb{Q}[X]$ von denen in $\mathbb{Z}[X]$ nur durch Konstanten in $\mathbb{Q}$.

In der Praxis am hilfreichsten ist allerdings die Originalfassung von Gauß selbst:

Folgerung 6.3. Sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom das Produkt $f = gh$ zweier normierter Polynome $g, h \in \mathbb{Q}[X]$. Dann folgt $g, h \in \mathbb{Z}[X]$.

Beweis. Nach Folgerung 6.2 existieren $g', h' \in \mathbb{Z}[X]$ primitiv sowie $\varepsilon_1, \varepsilon_2 \in \mathbb{Q}^*$ mit $g = \varepsilon_1 g'$ und $h = \varepsilon_2 h'$. Da g monisch ist, folgt $\varepsilon_1 = \frac{1}{k_1}$ für ein $k_1 \in \mathbb{N}$ und ebenso $\varepsilon_2 = \frac{1}{k_2}$ für $k_2 \in \mathbb{N}$. Dann ist aber $g'h' = k_1 k_2 gh = k_1 k_2 f$ primitiv, daher $k_1 k_2 = 1$ und insbesondere $k_1 = k_2 = 1$, sodass $g, h \in \mathbb{Z}[X]$.□

Folgerung 6.4. Es seien $f, g \in \mathbb{Z}[X]$ und f irreduzibel. Ist $\zeta \in \mathbb{C}$ eine gemeinsame Nullstelle von f und g, sodass $f(\zeta) = g(\zeta) = 0$, dann gilt $f \mid g$ in $\mathbb{Z}[X]$.

Beweis. Sei $q \in \mathbb{Z}[X]$ ein primitives Polynom mit minimalem Grad $\deg(q) \geq 0$, sodass $q(\zeta) = 0$ (diese Menge ist offenbar nicht leer).

Nach Proposition 4.1 existieren $h, r \in \mathbb{Q}[X]$ mit $g = hq + r$ und $\deg(r) < \deg(q)$. Aus $q(\zeta) = 0$ und $g(\zeta) = 0$ folgt insbesondere, dass $r(\zeta) = 0$, also $r = 0$ aufgrund der Minimalität von $\deg(q)$. Analog existiert $h' \in \mathbb{Q}[X]$ mit $f = h'q$. Nach Lemma 6.4 ist f in $\mathbb{Q}[X]$ irreduzibel, also $h' = c$ für ein $c \in \mathbb{Q}^*$. Da f und q primitiv sind, folgt $c = \pm 1$, also $g = \pm h \cdot f$.

Sei nun $a \in \mathbb{Q}^*$ so gewählt, dass $a\,h \in \mathbb{Z}[X]$ primitiv ist. Dann ist nach Lemma 6.3 auch $a\,g = a\,(\pm h \cdot f) = \pm(a\,h) \cdot f$ primitiv. Da g ganzzahlige Koeffizienten hat, gilt also $\frac{1}{a} \in \mathbb{Z}$. Daraus folgt $h \in \mathbb{Z}[X]$ und somit $f \mid g$. □

Nun der Beweis von Proposition 6.1:

Beweis. Sei angenommen, dass $f + p_d\,\mathbb{Q}[X] = g + p_d\,\mathbb{Q}[X]$ für $f, g \in \mathbb{Z}[X]$; wir wollen zeigen, dass $f + p_d\,\mathbb{Z}[X] = g + p_d\,\mathbb{Z}[X]$. Dann gilt $f - g \in p_d\,\mathbb{Q}[X]$, sodass $p_d \mid f - g$ in $\mathbb{Q}[X]$. Es existiert also $q \in \mathbb{Q}[X]$ mit $f - g = p_d\,q$. Andererseits sehen wir, dass

$$(f - g)(\omega_d) = p_d(\omega_d)\; q(\omega_d) = 0.$$

Da p_d in $\mathbb{Z}[X]$ irreduzibel ist folgt aus Folgerung 6.4, dass $p_d \mid f - g$ in $\mathbb{Z}[X]$. Das heißt aber genau, dass $f + p_d\,\mathbb{Z}[X] = g + p_d\,\mathbb{Z}[X]$. □

Insbesondere folgt, dass $\mathcal{O}_d$ noethersch ist und damit ein Ring mit Faktorzerlegung! Außerdem:

Proposition 6.2. Es gilt

$$\mathcal{O}_d \cong \{a + b\omega_d \mid a, b \in \mathbb{Z}\}$$

vermittels dem Isomorphismus

$$\psi\colon \mathcal{O}_d \to \{a + b\omega_d \mid a, b \in \mathbb{Z}\}, \quad \psi(f + p_d\,\mathbb{Z}[X]) := f(\omega_d).$$

Beweis. Zur Wohldefiniertheit von ψ: Gilt $f + p_d\,\mathbb{Z}[X] = f' + p_d\,\mathbb{Z}[X]$, so folgt $f - f' \in p_d\,\mathbb{Z}[X]$, d.h. $f = f' + p_d\,q$ mit $q \in \mathbb{Z}[X]$. Daraus folgt

$$f(\omega_d) = f'(\omega_d) + p_d(\omega_d) \cdot q(\omega_d) = f'(\omega_d).$$

Zur Homomorphieeigenschaft von ψ: Seien $f + p_d\,\mathbb{Z}[X]$, $g + p_d\,\mathbb{Z}[X]$ beliebige Elemente aus $\mathcal{O}_d$. Dann gilt

$$\psi(f + g + p_d\,\mathbb{Z}[X]) = (f + g)(\omega_d) = f(\omega_d) + g(\omega_d) = \psi(f + p_d\,\mathbb{Z}[X]) + \psi(g + p_d\,\mathbb{Z}[X])$$

und ähnlich

$$\psi(f \cdot g + p_d\,\mathbb{Z}[X]) = (f \cdot g)(\omega_d) = f(\omega_d) \cdot g(\omega_d) = \psi(f + p_d\,\mathbb{Z}[X]) \cdot \psi(g + p_d\,\mathbb{Z}[X]).$$

Außerdem gilt $\psi(1 + p_d\,\mathbb{Z}[X]) = 1$, sodass ψ tatsächlich die Homomorphieeigenschaft erfüllt und damit ein Homomorphismus mit Einselement ist.

Zur Bijektivität von ψ: Für beliebiges $a + b\omega_d \in \{a + b\omega_d \mid a, b \in \mathbb{Z}\}$ sehen wir, dass $\psi(a + bX + p_d\,\mathbb{Z}[X]) = a + b\omega_d$, also ist ψ surjektiv. Gilt andererseits $f(\omega_d) = 0$ für $f \in \mathbb{Z}[X]$, so folgt aus Korollar 6.4, dass $p_d \mid f$ in $\mathbb{Z}[X]$, i.e. $f \in p_d\,\mathbb{Z}[X]$. Der Kern von ψ ist also trivial, daher ist ψ injektiv. □

Definition 6.3. Der Ring $\mathcal{O}_d$ heißt *Ring der ganzen Zahlen in* $\mathbb{Q}(\sqrt{d})$. Ist $\{\alpha, \beta\} \subseteq \mathcal{O}_d$ eine Teilmenge von $\mathcal{O}_d$, so nennen wir $\{\alpha, \beta\}$ *Ganzheitsbasis* von $\mathcal{O}_d$, falls

$$\mathcal{O}_d \cong \{\alpha x + \beta y \mid x, y \in \mathbb{Z}\}$$

und schreiben dann $\mathcal{O}_d = \mathbb{Z}\,\alpha \oplus \mathbb{Z}\,\beta$[6.4].

6.4. Formal haben wir „$\oplus$“ in diesem Kontext nicht definiert. Wir meinen hier aber, dass einerseits $\mathcal{O}_d = \mathbb{Z}\,\alpha + \mathbb{Z}\,\beta$ gilt und andererseits $\mathbb{Z}\,\alpha \cap \mathbb{Z}\,\beta = \{0\}$, d.h. die jeweiligen $x, y \in \mathbb{Z}$ sind eindeutig bestimmt (cf. direkte Summen von Vektorräumen).

Insbesondere gilt nach Proposition 6.2, dass $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\,\omega_d$ und ähnlich $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\,\omega_d^*$. Im Allgemeinen ist aber $\mathcal{O}_d \neq \mathbb{Z} \oplus \mathbb{Z}\,\sqrt{d}$, da wir für $d \equiv 1 \pmod 4$ beispielsweise

$$\frac{1+\sqrt{d}}{2} \in \mathcal{O}_d, \quad \text{aber} \quad \frac{1+\sqrt{d}}{2} \notin \{a + b\,\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

erhalten. In diesem Fall gilt lediglich die Inklusion $\mathbb{Z} \oplus \mathbb{Z}\,\sqrt{d} \subseteq \mathcal{O}_d$. Ist $\{\alpha, \beta\}$ eine Ganzheitsbasis von $\mathcal{O}_d$ und $g \in \mathbb{Z}$, dann ist offenbar auch $\{\beta, \alpha + g\beta\}$ eine Ganzheitsbasis von $\mathcal{O}_d$.

Definition 6.4. (1) Wir nennen die Abbildung

$$*\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), \quad \alpha = a + b\omega_d \mapsto \alpha^* := a + b\omega_d^*$$

die *Konjugationsabbildung*.

(2) Die Abbildung definiert durch

$$N_d\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), \quad \alpha \mapsto N_d(\alpha) := \alpha \cdot \alpha^*$$

wird die *d-Norm in* $\mathbb{Q}(\sqrt{d})$ genannt. Analog definieren wir die *Spur* von α als

$$\mathrm{Tr}_d\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), \quad \mathrm{Tr}_d(\alpha) := \alpha + \alpha^*.$$

Beide Abbildungen erfüllen folgende elementaren Eigenschaften, die nicht weiter überraschend sind.

Lemma 6.5. Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Dann gilt:

(1) $(\alpha + \beta)^* = \alpha^* + \beta^*$.

(2) $(\alpha \cdot \beta)^* = \alpha^* \cdot \beta^*$.

(3) $(\alpha^*)^* = \alpha$.

(4) $\alpha^* = \alpha$ genau dann, wenn $\alpha \in \mathbb{Q}$.

(5) $\alpha + \alpha^* \in \mathbb{Q}$ und $\alpha \cdot \alpha^* \in \mathbb{Q}$ mit $\alpha \in \mathcal{O}_d$ genau dann, wenn $\alpha + \alpha^* \in \mathbb{Z}, \alpha \cdot \alpha^* \in \mathbb{Z}$.

Beweis. (1) Sei $\alpha = a + b\omega_d$ und $\beta = p + q\omega_d$ mit $a, b, p, q \in \mathbb{Q}$. Unmittelbar aus der Definition folgt

$$(\alpha + \beta)^* = ((a+p) + (b+q)\,\omega_d)^* = (a+p) + (b+q)\,\omega_d^* = (a + b\omega_d^*) + (p + q\omega_d^*) = \alpha^* + \beta^*.$$

(2) Es gilt zunächst

$$\alpha\beta = (a + b\omega_d)\,(p + q\omega_d) = ap + (aq + bp)\,\omega_d + bq\omega_d^2.$$

Sei $S := \omega_d + \omega_d^*$ und $P := \omega_d\,\omega_d^*$, sodass $S, P \in \mathbb{Q}$ und $\omega_d^2 = S\omega_d - P$. Dann erhalten wir

$$\alpha\beta = ap + (aq + bp)\,\omega_d + bq\,(S\omega_d - P) = (ap - bpP) + (aq + bp + bqS)\,\omega_d.$$

Daraus folgt einerseits

$$(\alpha\beta)^* = (ap - bpP) + (aq + bp + bqS)\,\omega_d^*$$

und andererseits, dass

$$\begin{aligned}\alpha^*\,\beta^* &= (a+b\omega_d^*)\,(p+q\omega_d^*) = ap+(aq+bp)\,\omega_d + bq\,(S\omega_d^*-P)\\ &= (ap-bpP)+(aq+bp+bqS)\,\omega_d^*,\end{aligned}$$

d.h. es gilt Gleichheit.

(3) Man überprüft leicht, dass $(\omega_d^*)^* = \omega_d$. Daraus folgt sofort

$$(\alpha^*)^* = (a+b\omega_d^*)^* = (a+b\,(\omega_d^*)^*) = a+b\omega_d = \alpha.$$

(4) Es gilt $\alpha^* = \alpha \Leftrightarrow a+b\omega_d^* = a+b\omega_d \Leftrightarrow b\,(\omega_d^*-\omega_d) = 0$. Weil $\omega_d \neq \omega_d^*$, kann nur $b=0$ sein, also $\alpha \in \mathbb{Q}$.

(5) Sei $\alpha \in \mathcal{O}_d$. Dann existieren $a, b \in \mathbb{Z}$ mit $\alpha = a+b\omega_d$ und

$$\alpha+\alpha^* = 2a+b\,(\omega_d+\omega_d^*), \quad \alpha\cdot\alpha^* = a^2+ab\,(\omega_d+\omega_d^*)+b^2\,(\omega_d\cdot\omega_d^*).$$

Ist $d \equiv 2,3 \pmod 4$, dann ist $\omega_d = \sqrt{d}$ und daher $\omega_d+\omega_d^* = 0$ bzw. $\omega_d\cdot\omega_d^* = -d$. Falls $d \equiv 1 \pmod 4$, ist $\omega_d = \frac{1+\sqrt{d}}{2}$, sodass $\omega_d+\omega_d^* = 1$ und $\omega_d\cdot\omega_d^* = \frac{1-d}{4} \in \mathbb{Z}$. In beiden Fällen sind $\alpha+\alpha^*, \alpha\cdot\alpha^*$ ganzzahlig.

Umgekehrt, sei $\alpha = a+b\sqrt{d}$ mit $a, b \in \mathbb{Q}$, sodass $2a = \alpha+\alpha^* \in \mathbb{Z}$ und $a^2-b^2d = \alpha\cdot\alpha^* \in \mathbb{Z}$. Dann gilt $a = \frac{u}{2}$, $u \in \mathbb{Z}$. Also $\frac{u^2}{4}-b^2d = a^2-b^2d = \alpha\cdot\alpha^* \in \mathbb{Z}$ bzw. $u^2-4b^2d \in 4\mathbb{Z}$. Da d quadratfrei ist, ist der Nenner von b (in gekürzter Form) ein Teiler von 2, sodass wir $b = \frac{v}{2}$, $v \in \mathbb{Z}$ schreiben können, also

$$u^2 \equiv dv^2 \pmod 4.$$

Jedenfalls gilt dann $u^2 \equiv 0 \pmod 4$ oder $u^2 \equiv 1 \pmod 4$ und ebenso $v^2 \equiv 0 \pmod 4$ oder $v^2 \equiv 1 \pmod 4$.

Falls $d \equiv 2,3 \pmod 4$, so ist $v^2 \equiv 0 \pmod 4$ die einzige Möglichkeit. Dann sind aber u und v gerade, daher auch $a = \frac{u}{2}, b = \frac{v}{2}$ ganze Zahlen. Falls $d \equiv 1 \pmod 4$, folgt $u^2 \equiv v^2 \pmod 4$ bzw. $u \equiv v \pmod 2$. Also

$$\alpha = \frac{u}{2}+\frac{v}{2}\sqrt{d} = \frac{u-v}{2}+v\left(\frac{1+\sqrt{d}}{2}\right) = \frac{u-v}{2}+v\omega_d,$$

wobei $\frac{u-v}{2}$ und v ganze Zahlen sind. Es folgt $\alpha \in \mathcal{O}_d$. □

Lemma 6.6. Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Dann gilt:

(1) $N_d(\alpha\beta) = N_d(\alpha)\,N_d(\beta)$.

(2) $N_d(\alpha) = 0$ genau dann, wenn $\alpha = 0$.

(3) $N_d(q) = q^2$ für alle $q \in \mathbb{Q}$.

(4) $N_d(\alpha), \mathrm{Tr}_d(\alpha) \in \mathbb{Q}$ und $N_d(k), \mathrm{Tr}_d(k) \in \mathbb{Z}$ für alle $k \in \mathcal{O}_d$.

(5) $N_d(\alpha) = \alpha\,\bar{\alpha} = |\alpha|^2$, falls $d < 0$.

Beweis. (1) Aus Lemma 6.5 (2) erhalten wir

$$N_d(\alpha\beta) = (\alpha\beta)\,(\alpha\beta)^* = (\alpha\alpha^*)\,(\beta\beta^*) = N_d(\alpha)\,N_d(\beta).$$

(2) Sei $N_d(\alpha) = \alpha\alpha^* = 0$. Da $\mathbb{Q}(\sqrt{d})$ per Definition ein Körper ist, gilt $\alpha = 0$ oder $\alpha^* = 0$. In beiden Fällen gilt also $\alpha = 0$. Die Rückrichtung folgt sofort.

(3) Sei $q \in \mathbb{Q}$. Unter Berücksichtigung von Lemma 6.5 (2) sehen wir, dass $N_d(q) = qq^* = q^2$.

(4) Das haben wir bereits in Lemma 6.5 (5) gezeigt.

(5) Sei $d<0$ und $\alpha = p + q\sqrt{d}$ für $p, q \in \mathbb{Q}$. Dann gilt

$$\alpha^* = p - q\sqrt{d} = p - q\left(\sqrt{-1}\cdot\sqrt{|d|}\right) = \overline{p + q\left(\sqrt{-1}\cdot\sqrt{|d|}\right)} = \overline{p + q\sqrt{d}} = \bar{\alpha},$$

sodass $N_d(\alpha) = \alpha\alpha^* = \alpha\,\bar{\alpha} = |\alpha|^2$. □

Als Konsequenz davon ergeben sich folgende hilfreiche Resultate.

Folgerung 6.5. Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Falls $\alpha \mid \beta$, so gilt $N_d(\alpha) \mid N_d(\beta)$.

Beweis. Das ist eine Anwendung von Lemma 6.6 (1). □

Die Umkehrung gilt nicht. Wir werden später sehen, dass $2 \pm \sqrt{-1}$ in $\mathcal{O}_{-1}$ irreduzibel sind, obwohl $N_{-1}(2+\sqrt{-1}) = N_{-1}(2-\sqrt{-1}) = 5$.

Lemma 6.7. Sei $\alpha \in \mathcal{O}_d$. Dann gilt $\alpha \in \mathcal{O}_d^*$ genau dann, wenn $N_d(\alpha) = \pm 1$.

Beweis. Ist $\alpha \in \mathcal{O}_d^*$, so existiert ein $\beta \in \mathcal{O}_d$ mit $\alpha \cdot \beta = 1$. Aus Lemma 6.6 folgt dann

$$\underbrace{N_d(\alpha)}_{\in\mathbb{Z}} \cdot \underbrace{N_d(\beta)}_{\in\mathbb{Z}} = N_d(\alpha\cdot\beta) = N_d(1) = 1,$$

also $N_d(\alpha) \in \mathbb{Z}^*$. Umgekehrt folgt $\pm 1 = N_d(\alpha) = \alpha \cdot \alpha^*$, sodass α multiplikatives Inverses $\pm\alpha^*$ in $\mathcal{O}_d$ hat, i.e. $\alpha \in \mathcal{O}_d^*$. □

Folgerung 6.6. Sei $\alpha \in \mathcal{O}_d$. Ist $N_d(\alpha)$ irreduzibel, dann ist auch α irreduzibel.

Beweis. Angenommen $N_d(\alpha)$ ist irreduzibel. Sei $\alpha = \beta\gamma$ für $\beta, \gamma \in \mathcal{O}_d$. Dann gilt $N_d(\alpha) = N_d(\beta)\,N_d(\gamma)$ nach Lemma 6.6 (1). Also $N_d(\beta) = \pm 1$ oder $N_d(\gamma) = \pm 1$, i.e. folgt aus Lemma 6.7, dass β oder γ Einheit ist. □

Die Umkehrung gilt nicht: Man zeigt leicht, dass 2 in $\mathcal{O}_{-5}$ irreduzibel ist, aber $N_{-5}(2) = 4$.

Beispiel 6.3. Berechnen wir die Einheiten in einigen der $\mathcal{O}_d$ für quadratfreies $d<0$.

(1) Falls $d \notin \{-1, -3\}$, so gilt $\mathcal{O}_d^* = \{\pm 1\}$. In der Tat, wir unterscheiden zwei Fälle. Sei zunächst $d \equiv 1 \pmod 4$ und schreiben wir $\alpha = \frac{a + b\sqrt{d}}{2}$ für $a, b \in \mathbb{Z}$ mit $a \equiv b \pmod 2$. Falls α Einheit ist, so gilt $1 = N_d(\alpha) = \frac{a^2 + |d|\,b^2}{4}$, d.h. wir suchen nach ganzzahligen Lösungen für $a^2 + |d|\,b^2 = 4$. Da d quadratfrei ist mit $d \equiv 1 \pmod 4$ und $d \neq -1$ und $d \neq -3$, folgt dass $d \leq -7$. Also

$$4 = a^2 + |d|\,b^2 \geq a^2 + 7b^2,$$

d.h. $b = 0$ und $a = \pm 2$. Es folgt $\alpha = \frac{a + b\sqrt{d}}{2} = \pm 1$. Nehmen wir jetzt an, dass $d \equiv 2, 3 \pmod 4$ mit $\alpha = a + b\sqrt{d}$ für $a, b \in \mathbb{Z}$. Ist α Einheit, so haben wir $1 = N_d(a + b\sqrt{d}) = a^2 + |d|\,b^2$ und wie zuvor bemerken wir, dass $d \leq -2$. Insbesondere folgt $1 = a^2 + 2b^2$ und daher $b = 0$ bzw. $a = \pm 1$.

(2) Es gilt $\mathcal{O}_{-1}^* = \{(\sqrt{-1})^k \mid 0 \leq k < 4\}$. Wir haben $-1 \equiv 3 \pmod 4$, d.h. jede Einheit in $\mathcal{O}_{-1}$ ist von der Form $a + b\sqrt{d}$ für bestimmte ganze Zahlen a, b. Insbesondere gilt $1 = N_{-1}(a + b\sqrt{d}) = a^2 + b^2$, eine Gleichung die nur die Lösungen $a = \pm 1, b = 0$ und $a = 0, b = \pm 1$ in den ganzen Zahlen hat. Aber diese vier Möglichkeiten sind genau $(\sqrt{-1})^k$ für $k = 0, 1, 2, 3$.

(3) Zuletzt zeigen wir, dass $\mathcal{O}_{-3}^* = \left\{ \left(\frac{1+\sqrt{-3}}{2} \right)^k \mid 0 \leq k < 6 \right\}$. Da $-3 \equiv 1 \pmod 4$, suchen wir nach Einheiten der Form $\frac{a+b\sqrt{d}}{2}$ für ganze Zahlen a, b mit $a \equiv b \pmod 2$ und $1 = N_{-3}\left(\frac{a+b\sqrt{d}}{2} \right) = \frac{a^2+3b^2}{4}$ bzw. $4 = a^2 + 3b^2$. Ganzzahlige Lösungen dieser Gleichung sind

$$a = b = 1, \quad a = b = -1, \quad a = 1, b = -1, \quad a = -1, b = 1, \quad a = 2, b = 0, \quad a = -2, b = 0.$$

Diese sechs Möglichkeiten sind genau die Werte $\left(\frac{1+\sqrt{-3}}{2} \right)^k$ für $k = 0, 1, 2, 3, 4, 5$.

(4) Für $d > 0$ verhalten sich die Einheiten in $\mathcal{O}_d$ allerdings anders… Mehr dazu später.

In den Beweisen der letzten Ergebnisse haben wir ein wenig Intuition gewonnen, um die Wahl von p_d und ω_d, wie angedeutet, zu begründen. Um das zu präzisieren, benötigen wir zunächst folgende Definition.

Definition 6.5. Sei S ein kommutativer Ring mit Einselement und $R \leq S$ ein Unterring von S. Dann heißt $s \in S$ *ganz über* R, wenn es die Nullstelle eines normierten Polynoms aus $R[X]$ ist. Die Menge der über R ganzen Elemente von S heißt der *ganze Abschluss von* R *in* S.

Proposition 6.3. $\mathcal{O}_d$ ist der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$.

Beweis. Sei $\alpha \in \mathcal{O}_d$ beliebig. Nach Lemma 6.6 (4) sind dann $\mathrm{Tr}_d(\alpha) = \alpha + \alpha^*$ und $N_d(\alpha) = \alpha \cdot \alpha^*$ ganze Zahlen, sodass

$$f := (X - \alpha)(X - \alpha^*) = X^2 - (\alpha + \alpha^*) X + \alpha\alpha^* \in \mathbb{Z}[X].$$

Da $f(\alpha) = 0$, ist α also ganz über $\mathbb{Z}$.

Umgekehrt, sei nun $\alpha \in \mathbb{Q}(\sqrt{d})$ ganz über $\mathbb{Z}$. Es existiert also ein normiertes Polynom $f \in \mathbb{Z}[X]$, sodass $f(\alpha) = 0$. Wir unterscheiden zwei Fälle: Ist $\alpha \in \mathbb{Q}$, so können wir $\alpha = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ teilerfremd, schreiben. Schreiben wir $f = \sum_{i=0}^n a_i X^i$ mit $a_n = 1$, so folgt

$$f(\alpha) = f\left(\frac{p}{q} \right) = \left(\frac{p}{q} \right)^n + a_{n-1} \left(\frac{p}{q} \right)^{n-1} + \cdots + a_0 = 0,$$

also $p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$, sodass $q (a_{n-1} p^{n-1} + \cdots + a_0 q^{n-1}) = -p^n$. Also $q \mid p^n$, sodass aus der Teilerfremdheit von p und q folgt, dass $q = 1$. Somit $\alpha \in \mathbb{Z} \subseteq \mathcal{O}_d$.

Falls $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, so bemerken wir zunächst, dass auch $f(\alpha^*) = (f(\alpha))^* = 0$. Weil $\alpha \notin \mathbb{Q}$, folgt $\alpha \neq \alpha^*$, sodass f durch $g := (X - \alpha)(X - \alpha^*) = X^2 - (\alpha + \alpha^*) X + \alpha\alpha^*$ teilbar ist. Es existiert also ein normiertes Polynom $h \in \mathbb{Q}[X]$, sodass $f = gh$; aus Folgerung 6.3 folgt dann, dass f insbesondere in $\mathbb{Z}[X]$ reduzibel ist mit $g, h \in \mathbb{Z}[X]$. Dann folgt aber insbesondere $\alpha + \alpha^*, \alpha\alpha^* \in \mathbb{Z}$, sodass $\alpha \in \mathcal{O}_d$ wegen Lemma 6.5 (5). □

Das klärt unter anderem die Bezeichnung „Ganzheitsbasis“. Es zeigt auch, wie wir bereits wissen, warum im Allgemeinen nicht $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ gilt: Ist $d \equiv 1 \pmod 4$, werden die Lösungen ω_d, ω_d^* des normierten ganzzahligen Polynoms p_d in $\mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ vernachlässigt.

Manchmal nennen wir den Ring der „ganzen“ Zahlen in $\mathbb{Q}(\sqrt{d})$ auch *Ganzheitsring*. Offenbar hat dieser viele interessante Eigenschaften, die wir nun weiter untersuchen werden. Insbesondere wollen wir dabei das Ziel, Gegenbeispiele für Kästchen 4 zu finden, nicht aus den Augen verlieren.

Proposition 6.4. Es sei $I \trianglelefteq \mathcal{O}_d$ ein Ideal mit $I \neq (0)$. Dann existiert eine Ganzheitsbasis $\{\alpha_1, \alpha_2\}$ von $\mathcal{O}_d$ sowie $d_1, d_2 \in \mathbb{N}$ mit $d_1 \mid d_2$, sodass

$$I = \mathbb{Z}(d_1 \alpha_1) \oplus \mathbb{Z}(d_2 \alpha_2).$$

Beweis. Für eine beliebige geordnete Ganzheitsbasis $\{\beta_1, \beta_2\}$ von $\mathcal{O}_d$, sei

$$\Gamma(\beta_1, \beta_2) := \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : m\beta_1 + k\beta_2 \in I\}.$$

Dann ist $\Gamma(\beta_1, \beta_2) \neq \{0\}$. In der Tat, sei $\alpha \in I, \alpha \neq 0$; dann ist $N_d(\alpha) = \alpha \cdot \alpha^* \in I \cap \mathbb{Z}$ (Lemma 6.6 (4)), sodass $\operatorname{sgn}(\alpha\alpha^*) \cdot \alpha\alpha^* \in I \cap \mathbb{N}$. Also gibt es ein $n \in I \cap \mathbb{N}$ und damit auch $n\beta_1 \in I$, woraus $n \in \Gamma(\beta_1, \beta_2)$ folgt. Weiters ist $\Gamma(\beta_1, \beta_2)$ offenbar eine additive Untergruppe von $\mathbb{Z}$, sodass aus Korollar 2.2 folgt, dass $\Gamma(\beta_1, \beta_2) = d(\beta_1, \beta_2)\,\mathbb{Z}$ für einen eindeutig bestimmten Erzeuger $d(\beta_1, \beta_2) \in \mathbb{N}$. Sei $\{\beta_1, \beta_2\}$ so gewählt, dass $d_1 := d(\beta_1, \beta_2)$ minimal ist.

Wir haben bereits gesehen, dass $\{\beta_2, \beta_1 + g\beta_2\}$ für alle $g \in \mathbb{Z}$ eine Ganzheitsbasis von $\mathcal{O}_d$ ist. Wir zeigen: Ist $v \in \mathbb{Z}$ so, dass $d_1\,\beta_1 + v\beta_2 \in I$, dann muss schon d_1 ein Teiler von v sein. Seien nämlich $q, r \in \mathbb{Z}$ so gewählt, dass $v = qd_1 + r$ für $0 \leq r < d_1$. Dann ist $d_1\,(\beta_1 + q\beta_2) + r\beta_2 \in I$, sodass $r \in \Gamma(\beta_2, \beta_1 + q\beta_2)$ und $d_1 \leq d(\beta_2, \beta_1 + q\beta_2)$. Also muss $r = 0$ gelten, d.h. $d_1 \mid v$.

Es sei nun $v_0 \in \mathbb{Z}$ so gewählt, dass $d_1\,\beta_1 + v_0\,\beta_2 \in I$ und nach eben $v_0 = d_1\,g$ für ein $g \in \mathbb{Z}$. Setze $\alpha_1 := \beta_1 + g\beta_2$ und $\alpha_2 := \beta_2$. Dann ist ist $\{\alpha_1, \alpha_2\}$ eine Ganzheitsbasis von $\mathcal{O}_d$. Sei wie vorhin $n \in I \cap \mathbb{N}$. Wie zuvor gilt $n\beta_2 \in I$, also ist $\beta_2^{-1} I \cap \mathbb{Z}$ eine nichttriviale Untergruppe von $\mathbb{Z}$. Es existiert also auch $d_2 \in \mathbb{N}$ mit $\beta_2^{-1} I \cap \mathbb{Z} = d_2\,\mathbb{Z}$ und $d_1\,\beta_2 \in I$. Sei nun $\alpha := m\alpha_1 + n\alpha_2 = m\beta_1 + (mg + n)\,\beta_2$ ein Element von I für fixierte $m, n \in \mathbb{Z}$. Dann ist $m \in \Gamma(\beta_1, \beta_2) = d_1\,\mathbb{Z}$, also $d_1 \mid m$. Aus $d_1\,\alpha_1 = d_1\,\beta_1 + v_0\,\beta_2 \in I$ folgt $m\alpha_1 \in I$, also $n\alpha_2 \in I$, sodass $n \in d_2\,\mathbb{Z}$ und daher $d_2 \mid n$. Zusammengefasst folgt also $\alpha \in \mathbb{Z}\,(d_1\,\alpha_1) \oplus \mathbb{Z}\,(d_2\,\alpha_2)$. Weil α beliebig gewählt war, folgern wir

$$I = \mathbb{Z}\,(d_1\,\alpha_1) \oplus \mathbb{Z}\,(d_2\,\alpha_2).$$

Um $d_1 \mid d_2$ zu zeigen, bemerken wir, dass $d_2\,\beta_2 \in I$ und daher $d_1\,\alpha_1 + d_2\,\beta_2 = d_1\,\beta_1 + (d_1\,g + d_2)\,\beta_2 \in I$. Aus dem letzten Absatz folgt somit $d_1 \mid d_1\,g + d_2$ und *a fortiori* $d_1 \mid d_2$. □

Folgerung 6.7. Es sei $I \trianglelefteq \mathcal{O}_d$ ein Ideal mit $I \neq (0)$. Dann ist $\mathcal{O}_d / I$ endlich.

Beweis. Nach Proposition 6.4 gibt es eine Ganzheitsbasis $\{\alpha_1, \alpha_2\}$ von $\mathcal{O}_d$ sowie $d_1, d_2 \in \mathbb{N}$ mit $I = \mathbb{Z}\,(d_1\,\alpha_1) \oplus \mathbb{Z}\,(d_2\,\alpha_2)$. Wir definieren die Abbildung

$$\phi\colon (\mathbb{Z}/d_1\,\mathbb{Z}) \times (\mathbb{Z}/d_2\,\mathbb{Z}) \to \mathcal{O}_d/I, \quad \phi(a, b) := a\alpha_1 + b\alpha_2 + I$$

und zeigen, dass ϕ eine Bijektion ist; klarerweise ist ϕ wohldefiniert. Sei $A := a\,\alpha_1 + b\alpha_2$ und $E := e\,\alpha_1 + f\alpha_2$ für $a, e \in \mathbb{Z}/d_1\,\mathbb{Z}$ und $b, f \in \mathbb{Z}/d_2\,\mathbb{Z}$. Falls $\phi(a, b) = \phi(e, f)$, so folgt $\phi(a, b) - \phi(e, f) \in I$. Also gilt

$$(a - e)\,\alpha_1 + (b - f)\,\alpha_2 = A - E = pd_1\,\alpha_1 + qd_2\,\alpha_2$$

für $p, q \in \mathbb{Z}$. Dann folgt aber $a - e \equiv 0 \pmod{d_1}$ und $b - f \equiv 0 \pmod{d_2}$, sodass ϕ injektiv ist. Die Surjektivität von ϕ folgt unmittelbar. Somit ist ϕ bijektiv; insbesondere hat $\mathcal{O}_d/I$ genau $d_1 \cdot d_2$ Elemente. □

Folgerung 6.8. Sei $I \triangleleft \mathcal{O}_d$ ein Primideal, $I \neq (0)$. Dann ist I maximal.

Beweis. Nach Proposition 4.3 ist $\mathcal{O}_d/I$ ein Integritätsbereich, der nach Folgerung 6.7 endlich ist und nach Proposition 2.2 somit ein Körper, sodass aus Proposition 4.3 folgt, dass I maximal ist.□

Diese Erkenntnisse führen uns zum ersten zentralen Satz unserer Untersuchungen.

Satz 6.1. Der Ring $\mathcal{O}_d$ ist genau dann ein Hauptidealring, wenn er faktoriell ist.

Beweis. Falls $\mathcal{O}_d$ ein Hauptidealring ist, dann ist er nach Satz 3.4 auch faktoriell. Sei $\mathcal{O}_d$ also nun faktoriell und $I \lhd \mathcal{O}_d$ ein echtes Ideal, das nicht das Nullideal ist (sonst ist I offensichtlich ein Hauptideal). Also können wir $\alpha \in \mathcal{O}_d \setminus \mathcal{O}_d^*$ nicht Null wählen.

Nehmen wir zunächst an, dass I ein Primideal ist. Weil $\mathcal{O}_d$ nach Proposition 6.1 ein Ring mit Faktorzerlegung ist, existieren irreduzible Elemente $p_1, \dots, p_n \in \mathcal{O}_d$, sodass $\alpha = \prod_{i=1}^n p_i$. Weil I prim ist, muss es ein $i \in \{1, \dots, n\}$ geben, sodass $p_i \in I$; dann ist auch $(p_i) \subseteq I$. Nach Annahme ist $\mathcal{O}_d$ faktoriell, also ist p_i auch ein Primelement von $\mathcal{O}_d$ (Satz 3.3) und damit (p_i) auch ein Primideal von $\mathcal{O}_d$. Aber (p_i) ist nach Folgerung 6.8 sogar maximal, sodass $(p_i) = I$ folgen muss.

Es sei nun $I \neq (0)$ ein beliebiges Ideal von $\mathcal{O}_d$. Dann existieren nach Proposition 6.4 Elemente α, $\beta \in I$, sodass $I = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$. Da $\mathcal{O}_d$ faktoriell ist, existiert nach Lemma 3.6 ein Maximalteiler $g \in \mathcal{O}_d$ von $\{\alpha, \beta\}$. Setzen wir also $J := g^{-1} I$, so folgt $J \trianglelefteq \mathcal{O}_d$. In der Tat, aus $g \mid \alpha$ und $g \mid \beta$ folgt zunächst $J \subseteq \mathcal{O}_d$. Sind $x, y \in J, \alpha \in \mathcal{O}_d$, so folgt $gx, gy \in I$, daher $g(x-y) = gx - gy \in I$ und $x - y \in J$; ähnlich gilt $g\alpha x \in I$ und damit $x\alpha \in J$. Wenn wir zeigen können, dass $J = \mathcal{O}_d$, so folgt automatisch $(g) = g\mathcal{O}_d = I$. In der Tat, falls $J \neq \mathcal{O}_d$, so existiert nach Proposition 3.2 (3) ein maximales Ideal $K \lhd \mathcal{O}_d$ mit $J \subseteq K$. Insbesondere ist K aber ein Primideal, daher $K = (\xi)$ für ein $\xi \in \mathcal{O}_d$. Da $g^{-1}\alpha, g^{-1}\beta \in J$, ist $g^{-1}\alpha, g^{-1}\beta \in (\xi)$, also $\xi \mid g^{-1}\alpha$ sowie $\xi \mid g^{-1}\beta$. Daraus folgt $g\xi \mid \alpha$ und $g\xi \mid \beta$ und weil g ein Maximalteiler von $\{\alpha, \beta\}$ war, folgt $g\xi \mid g$. Dann folgt aber, dass ξ Einheit ist, ein Widerspruch dazu, dass K maximal ist. Also muss schon $J = \mathcal{O}_d$ gelten. □

Der Ring der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$ wird also auf jeden Fall keine Gegenbeispiele für faktorielle Ringe, die keine Hauptidealringe sind, liefern. Für die Vervollständigung von Kästchen 4 brauchen wir also noch mehr Informationen. Naturgemäß stellen sich folgende Fragen: Für welche $d \in \mathbb{Z}$ ist $\mathcal{O}_d$ faktoriell (und dementsprechend ein Hauptidealring)? Für welche sogar euklidisch? Um diese Fragen zu beantworten, schränken wir uns zunächst auf $d < 0$ ein. Behandeln wir zunächst euklidische Ringe.

Lemma 6.8. Es sei $d < 0$ eine quadratfreie ganze Zahl und

$$d \notin \{-1, -2, -3, -7, -11\}.$$

Dann sind 2 und 3 irreduzibel in $\mathcal{O}_d$.

Beweis. Sei $p \in \{2, 3\}$. Offenbar gilt $p \neq 0$ und $p \notin \mathcal{O}_d^*$. Sei angenommen, dass $p = \alpha\beta$ für α, $\beta \in \mathcal{O}_d \setminus \mathcal{O}_d^*$. Dann ist

$$p^2 = N_d(p) = N_d(\alpha)\, N_d(\beta)$$

und da $\alpha, \beta \notin \mathcal{O}_d^*$ gilt auch $N_d(\alpha), N_d(\beta) \neq 1$. Daraus folgt $N_d(\alpha) = N_d(\beta) = p$. Sei $\alpha = a + b\omega_d$ für $a, b \in \mathbb{Z}$, sodass

$$p = N_d(\alpha) = \begin{cases} a^2 + |d|\, b^2, & d \equiv 2, 3 \pmod 4, \\ \left(a + \frac{b}{2}\right)^2 + \frac{|d|}{4} b^2, & d \equiv 1 \pmod 4. \end{cases}$$

Weil $d \notin \{-1, -2, -3, -7, -11\}$, haben wir im ersten Fall $|d| \geq 5$ und im zweiten Fall $\frac{|d|}{4} \geq \frac{15}{4} \geq 3$, sodass $b^2 = 0$ folgt. Dann gilt aber $p = a^2$; ein Widerspruch. □

Proposition 6.5. Es sei $d < 0$ eine quadratfreie ganze Zahl und

$$d \notin \{-1, -2, -3, -7, -11\}.$$

Dann ist $\mathcal{O}_d$ nicht euklidisch.

Beweis. Nehmen wir an, dass $\mathcal{O}_d$ bezüglich einer Abbildung $\omega\colon \mathcal{O}_d \setminus \{0\} \to \mathbb{N}_0$ euklidisch ist. Nach Beispiel 6.3 gilt $\mathcal{O}_d^* = \{-1, 1\}$; wählen wir also $\alpha_0 \in \mathcal{O}_d \setminus \{0, \pm 1\}$ so, dass $\omega(\alpha_0) \in \mathbb{N}_0$ minimal ist. Seien $q, r \in \mathcal{O}_d$ außerdem so, dass $2 = q\alpha_0 + r$ mit $r = 0$ oder $\omega(r) < \omega(\alpha_0)$. Insbesondere muss dann aber $r = 0$ oder $r = \pm 1$ sein, wobei $r = 1$ ausgeschlossen ist. Falls $r = 0$, dann $\alpha_0 \mid 2$; da aber $\alpha_0 \notin \mathcal{O}_d^*$ und 2 nach Lemma 6.8 irreduzibel ist, folgt $\alpha_0 = \pm 2$. Falls wiederum $r = -1$, so gilt $\alpha_0 \mid 3$ und aus einem ähnlichen Argument folgt dann $\alpha_0 = \pm 3$. Zusammengefasst haben wir also $\alpha_0 \in \{\pm 2, \pm 3\}$. Seien $q', r' \in \mathcal{O}_d$ nun so, dass $\omega_d = q'\alpha_0 + r'$ und $r' = 0$ oder $\omega(r') < \omega(\alpha_0)$. Erneut haben wir $r' = 0$ oder $r' = \pm 1$; wir zeigen, dass beide Möglichkeiten zu einem Widerspruch führen. Ist $r' = 0$, so haben wir $\alpha_0 \mid \omega_d$ in $\mathcal{O}_d$, was zum Widerspruch $\alpha_0^{-1}\omega_d \in \mathcal{O}_d$ führt, da $\alpha_0 \in \{\pm 2, \pm 3\}$. Ist $r' = \pm 1$, so erhalten wir den ähnlichen Widerspruch $\alpha_0^{-1}(\mp 1 + \omega_d) \in \mathcal{O}_d$. □

Auch die Umkehrung gilt! Um das zu zeigen, treffen wir noch folgende Vorbereitung.

Lemma 6.9. Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Dann ist $\mathcal{O}_d$ genau dann bezüglich $|N_d|$ euklidisch, wenn für alle $\alpha \in \mathbb{Q}(\sqrt{d})$ ein $\beta \in \mathcal{O}_d$ existiert, sodass $|N_d(\alpha - \beta)| < 1$.

Beweis. Nehmen wir zunächst an, dass $\mathcal{O}_d$ bezüglich $|N_d|$ euklidisch ist. Sei $\alpha \in \mathbb{Q}(\sqrt{d})$ beliebig mit $\alpha = a + b\omega_d$ für $a, b \in \mathbb{Q}$. Dann existiert ein $m \in \mathbb{N}$ mit $m\alpha \in \mathcal{O}_d$ und nach Voraussetzung somit auch $q, r \in \mathcal{O}_d$ mit $m\alpha = mq + r$ und $r = 0$ bzw. $|N_d(r)| < |N_d(m)|$. In beiden Fällen folgt

$$|N_d(m)|\,|N_d(\alpha - q)| = |N_d(m\alpha - mq)| = |N_d(r)| < |N_d(m)|,$$

sodass $|N_d(\alpha - q)| < 1$, wie gewünscht.

Sei nun vorausgesetzt, dass für alle $\alpha \in \mathbb{Q}(\sqrt{d})$ ein $\beta \in \mathcal{O}_d$ mit $|N_d(\alpha - \beta)| < 1$ existiert. Seien $\gamma, \delta \in \mathcal{O}_d$ mit $\delta \neq 0$ beliebig. Dann ist $\gamma\delta^{-1} \in \mathbb{Q}(\sqrt{d})$, sodass nach Voraussetzung ein $\beta \in \mathcal{O}_d$ mit $|N_d(\gamma\delta^{-1} - \beta)| < 1$. Setzen wir $r := \gamma - \beta\delta \in \mathcal{O}_d$, folgt $\gamma = \beta\delta + r$ und $|N_d(r)| < |N_d(\delta)|$. □

Erinnern wir uns an die Definition eines euklidischen Ringes, so wissen wir, dass wir eine Art „Division mit Rest“ zur Verfügung haben. Lemma 6.9 sagt also im Prinzip, dass wir bei Division von α durch $\beta \neq 0$ ein Element erhalten (den Quotienten), das maximalen Abstand 1 zu α hat.

Proposition 6.6. Ist $d \in \{-1, -2, -3, -7, -11\}$, dann ist $\mathcal{O}_d$ euklidisch bezüglich $\omega = N_d = |N_d|$.

Beweis. Betrachten wir den Ausdruck $N_d(\alpha) = |N_d(\alpha)| = |\alpha|^2$ für beliebiges $\alpha \in \mathbb{Q}(\sqrt{d})$.

Sei zuerst $d \in \{-1, -2\}$. Dann gilt $d \not\equiv 1 \pmod 4$ und es gibt $r, s \in \mathbb{Q}$ mit $\alpha = r + s\sqrt{d}$. Seien x, $y \in \mathbb{Z}$ so gewählt, dass $|x - r| \leq \frac{1}{2}, |y - s| \leq \frac{1}{2}$ und sei $\beta := x + y\sqrt{d} \in \mathcal{O}_d$. Dann ist

$$|\alpha - \beta|^2 = (x - r)^2 + |d|\,(y - s)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} < 1.$$

Die Behauptung folgt also aus Lemma 6.9.

Sei nun $d \in \{-3, -7, -11\}$. Dann ist $d \equiv 1 \pmod 4$. Sei wieder $\alpha \in \mathbb{Q}(\sqrt{d})$ beliebig mit $\alpha = r + s\sqrt{d}$. Sei $y \in \mathbb{Z}$ so gewählt, dass $|2s - y| \leq \frac{1}{2}$ und $x \in \mathbb{Z}$ so gewählt, dass $\left|r - x - \frac{y}{2}\right| \leq \frac{1}{2}$. Setzen wir $\beta := x + y\omega_d$, dann ist

$$|\alpha - \beta|^2 = \left(r - x - \frac{y}{2}\right)^2 + \left(s - \frac{y}{2}\right)^2 |d| \leq \frac{1}{4} + \frac{|d|}{16} \leq \frac{15}{16} < 1$$

und somit folgt die Behauptung wieder aus Lemma 6.9. □

Folgerung 6.9. Sei $d < 0$ eine quadratfreie ganze Zahl. Dann ist $\mathcal{O}_d$ genau dann euklidisch bezüglich $\omega = |N_d|$, wenn $d \in \{-1, -2, -3, -7, -11\}$.

Für $d=-1$ nennen wir den folglich euklidischen Ring $\mathcal{O}_d=\mathcal{O}_{-1}$ den *Ring der Gauß'schen Zahlen* und schreiben $\mathbb{Z}[\sqrt{-1}]$. Für $d=-3$ nennen wir $\mathcal{O}_d=\mathcal{O}_{-3}$ den *Ring der Eisenstein-Zahlen* und schreiben $\mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right]$. Die Einheiten in diesen Ringen haben wir bereits in Beispiel 6.3 bestimmt. Als kleinen Exkurs wollen wir die Primelemente in $\mathbb{Z}[\sqrt{-1}]$ bestimmen.

Lemma 6.10. Das Polynom X^2+1 ist in $\mathbb{F}_p[X]$ genau dann irreduzibel, wenn $p\equiv 3 \pmod 4$ für eine Primzahl p.

Beweis. ($\Rightarrow$) Setzen wir zuerst voraus, dass $p\equiv 3 \pmod 4$. Dann gilt $p=4k+3$ für ein $k\in\mathbb{N}$. Nach Proposition 5.1 ist X^2+1 genau dann irreduzibel, wenn keine Nullstelle in $\mathbb{F}_p$ existiert; nehmen wir für einen Widerspruch an, dass dies der Fall ist. Also gilt $\alpha^2\equiv -1 \pmod p$ für ein $\alpha\in\mathbb{F}_p$ und insbesondere $\alpha^4\equiv 1 \pmod p$. Nach Lemma 5.2,

$$1\equiv \alpha^{p-1}\equiv \alpha^{4k+2}\equiv \alpha^2\,\alpha^{4k}\equiv \alpha^2\equiv -1 \pmod p,$$

i.e. $0\equiv 2 \pmod p$. Da offensichtlich $p\neq 2$, ist das ein Widerspruch.

($\Leftarrow$) Wir zeigen, dass falls $p\not\equiv 3 \pmod 4$ ist, X^2+1 eine Nullstelle in $\mathbb{F}_p$ hat. Falls $p=2$, hat X^2+1 die Nullstelle $\alpha=1$, also können wir annehmen, dass $p\equiv 1 \pmod 4$, d.h. $p=4k+1$ für ein $k\in\mathbb{N}$. Aus dem Satz von Wilson (Lemma 2.3) folgt

$$\begin{aligned}
-1 &\equiv (p-1)\,(p-2)\cdots(2)\,(1)\\
&\equiv \left(\frac{p+(p-2)}{2}\right)\left(\frac{p+(p-4)}{2}\right)\cdots\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)\cdots\left(\frac{p-(p-4)}{2}\right)\left(\frac{p-(p-2)}{2}\right)\\
&\equiv \left(-\frac{p-(p-2)}{2}\right)\left(-\frac{p-(p-4)}{2}\right)\cdots\left(-\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right)\cdots\left(\frac{p-(p-4)}{2}\right)\left(\frac{p-(p-2)}{2}\right)\\
&\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2(-1)^{\frac{p-1}{2}} \pmod p.
\end{aligned}$$

Weil $(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1$, folgt insbesondere $-1\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p$, d.h. X^2+1 hat die Nullstelle $\alpha=\left(\frac{p-1}{2}\right)!$ in $\mathbb{F}_p$. □

Lemma 6.11. Sei $\pi\in\mathcal{O}_d$ ein Primelement. Dann gilt $|N_d(\pi)|=p$ oder $|N_d(\pi)|=p^2$ für eine Primzahl $p\in\mathbb{P}$.

Beweis. Sei $n:=|N_d(\pi)|=\prod_{i=1}^k p_i$ für Primzahlen $p_1,\dots,p_k\in\mathbb{P}$. Da $N_d(\pi)=\pi\pi^*$, folgt $\pi\mid n$. Weil π ein Primelement ist, existiert also ein $i\in\{1,\dots,k\}$ sodass $\pi\mid p_i$ in $\mathcal{O}_d$. Wegen Folgerung 6.5 gilt dann aber auch $N_d(\pi)\mid N_d(p_i)$, d.h. $n\mid p_i^2$ in $\mathbb{Z}$. Daraus folgt $n\in\{1,p_i,p_i^2\}$ und da π prim ist, kann nur $n\in\{p_i,p_i^2\}$ der Fall sein. □

Satz 6.2. Die Primelemente im Ring der Gauß'schen Zahlen sind (bis auf Assoziiertheit) gegeben durch jene Elemente π, die eine der folgenden Eigenschaften erfüllen:

(1) $\pi=1+\sqrt{-1}$,

(2) $N_{-1}(\pi)=p$ für eine Primzahl $p\equiv 1 \pmod 4$.

(3) $\pi=p$ für eine Primzahl $p\equiv 3 \pmod 4$.

Beweis. Sei π ein Primelement von $\mathbb{Z}[\sqrt{-1}]$. Nach Lemma 6.11 existiert eine Primzahl $p\in\mathbb{P}$ mit $N_{-1}(\pi)=p$ oder $N_{-1}(\pi)=p^2$. Wir unterscheiden drei wesentliche Fälle.

Falls $p=2$ und $N_{-1}(\pi)=p=2$, so folgt aus $2=N_{-1}(\pi)=\pi\pi^*$, dass $\pi\,|\,2$. Mittels der Faktorisierung

$$2=(1+\sqrt{-1})\,(1-\sqrt{-1})=(-\sqrt{-1})\,(1+\sqrt{-1})^2$$

und dem Faktum, dass π prim ist, folgt $\pi\,|\,1+\sqrt{-1}$. Aber $N_{-1}(1+\sqrt{-1})=2$, d.h. $1+\sqrt{-1}$ ist irreduzibel und daher $\pi\sim 1+\sqrt{-1}$. Falls wiederum $p=2$ und $N_{-1}(\pi)=p^2=4$, so muss $\pi\sim 2$ gelten, ein Widerspruch dazu, dass π prim und daher irreduzibel ist.

Falls $p\equiv 1\,(\mathrm{mod}\,4)$, hat X^2+1 nach Lemma 6.10 eine Nullstelle $u\in\mathbb{Z}$ modulo p, sodass $u^2+1\equiv 0\,(\mathrm{mod}\,p)$. Also

$$p\,|\,u^2+1=(u+\sqrt{-1})\,(u-\sqrt{-1}).$$

Da p keinen der beiden Faktoren auf der rechten Seite teilt, ist p kein Primelement von $\mathbb{Z}[\sqrt{-1}]$. Wäre $N_{-1}(\pi)=p^2$, so gilt $\pi\,|\,p^2$, insbesondere also $\pi\,|\,p$, da π prim ist. Da außerdem $N_{-1}(\pi)=N_{-1}(p)$, folgt $\pi\sim p$, im Widerspruch dazu, dass π prim, p aber nicht ist. Folglich $N_{-1}(\pi)=p$.

Falls $p\equiv 3\,(\mathrm{mod}\,4)$ und $N_{-1}(\pi)=p$, so setzen wir zunächst $\pi=a+b\sqrt{-1}$ für $a,b\in\mathbb{Z}$ an. Also $p=N_{-1}(\pi)=a^2+b^2$, was $p\equiv 3\,(\mathrm{mod}\,4)$ widerspricht. Es folgt $N_{-1}(\pi)=N_{-1}(p)=p^2$ und da $\pi\,|\,p$ muss sogar $\pi\sim p$ gelten. □

Wir folgern also, dass für quadratfreies $d<0$ der Ring $\mathcal{O}_d$ genau dann euklidisch ist (und zwar bezüglich $\omega=|N_d|$), wenn $d\in\{-1,-2,-3,-7,-11\}$. Wir nennen $\mathcal{O}_d$ dann *norm-euklidisch*. Nach Satz 3.5 und Satz 3.4 sind diese Ringe auch Hauptidealringe, dementsprechend faktoriell. Es stellt sich nun die Frage, ob diese Liste auch vollständig ist oder die Möglichkeit besteht, weitere Beispiele für faktorielle Ringe (äquivalent Hauptidealringe) zu finden, die allerdings nicht euklidisch sind.

Proposition 6.7. Es sei $d<0$ eine quadratfreie ganze Zahl und $d\equiv 2,3\,(\mathrm{mod}\,4)$. Dann ist $\mathcal{O}_d$ genau dann faktoriell, wenn $d\in\{-1,-2\}$.

Beweis. Wie eben festgestellt, falls $d\in\{-1,-2\}$, ist $\mathcal{O}_d$ euklidisch und damit auch faktoriell. Sei also umgekehrt $d\notin\{-1,-2\}$ eine negative quadratfreie ganze Zahl. Insbesondere muss dann $d\notin\{-1,-2,-3,-7,-11\}$ sein, sodass aus Lemma 6.8 folgt, dass 2 irreduzibel in $\mathcal{O}_d$ ist. Nehmen wir für einen Widerspruch an, dass $\mathcal{O}_d$ faktoriell ist. Dann wäre 2 nach Satz 3.3 ein Primelement von $\mathcal{O}_d$. Da $d\equiv 2,3\,(\mathrm{mod}\,4)$ ist aber 2 ein Teiler von

$$d\,(1-d)=\sqrt{d}\cdot\sqrt{d}\cdot(1-\sqrt{d})\,(1+\sqrt{d}),$$

also $2\,|\,\sqrt{d}$ oder $2\,|\,1\pm\sqrt{d}$. Das führt zum Widerspruch $\frac{1}{2}\sqrt{d}\in\mathcal{O}_d$ bzw. $\frac{1\pm\sqrt{d}}{2}\in\mathcal{O}_d$. Somit ist $\mathcal{O}_d$ nicht faktoriell. □

Das beantwortet unsere Frage also im Fall von $d\equiv 2,3\,(\mathrm{mod}\,4)$. Was ist, wenn $d\equiv 1\,(\mathrm{mod}\,4)$? Diese Frage ist nicht ganz so leicht zu beantworten. Zunächst verallgemeinern wir das recht intuitive Lemma 6.9.

Definition 6.6. Sei $\alpha\in\mathbb{Q}(\sqrt{d})$. Wir nennen α ein *inopportunes Element*, wenn $\alpha\notin\mathcal{O}_d$ und wenn für alle $\gamma,\delta\in\mathcal{O}_d$ mit $\alpha\gamma-\delta\neq 0$ folgt, dass $|N_d(\alpha\gamma-\delta)|\geq 1$.

Lemma 6.12. Sei $\alpha\in\mathbb{Q}(\sqrt{d})$ inopportun. Dann gilt:

(1) $|N_d(\alpha)|\geq 1$.

(2) $\alpha\notin\mathbb{Q}$.

(3) Ist $\beta\in\mathcal{O}_d$, dann ist $\alpha+\beta$ inopportun.

(4) Ist $\beta\in\mathcal{O}_d$ so, dass $\alpha\beta\notin\mathcal{O}_d$, dann ist $\alpha\beta$ inopportun.

Beweis. (1) Offenbar ist $\alpha \neq 0$. Per Definition gilt also $|N_d(\alpha)| = |N_d(\alpha \cdot 1 - 0)| \geq 1$.

(2) Wäre $\alpha \in \mathbb{Q}$, so wäre $0 < \alpha - \lfloor \alpha \rfloor < 1$ und daher $|N_d(\alpha - \lfloor \alpha \rfloor)| = (\alpha - \lfloor \alpha \rfloor)^2 < 1$, sodass α nicht inopportun sein kann.

(3) Sei $\beta \in \mathcal{O}_d$. Offenbar ist $\alpha + \beta$ nicht in $\mathcal{O}_d$. Sind $\gamma, \delta \in \mathcal{O}_d$ mit $(\alpha + \beta)\,\gamma - \delta \neq 0$, so folgt insbesondere $\alpha\gamma - (\delta - \beta\gamma) = (\alpha + \beta)\,\gamma - \delta \neq 0$ und damit

$$|N_d((\alpha + \beta)\,\gamma - \delta)| = |N_d(\alpha\gamma - (\delta - \beta\gamma))| \geq 1,$$

da α inopportun ist und $\gamma, \delta - \beta\gamma \in \mathcal{O}_d$.

(4) Sei $\beta \in \mathcal{O}_d$ so, dass $\alpha\beta \notin \mathcal{O}_d$. Seien $\gamma, \delta \in \mathcal{O}_d$ mit $\alpha\beta\gamma - \delta \neq 0$. Dann folgt aus $\beta\gamma \in \mathcal{O}_d$, dass

$$|N_d(\alpha\beta\gamma - \delta)| = |N_d(\alpha\,(\beta\gamma) - \delta)| \geq 1;$$

also ist $\alpha\beta$ inopportun. □

Die Bezeichnung „inopportun“ ergibt auch Sinn, denn inopportune Elemente bezeichnen jene Elemente, deren Existenz wir in Lemma 6.9 ausschließen wollen. Folgendes Lemma ist also nicht weiter überraschend.

Lemma 6.13. Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei. Existiert kein inopportunes Element $\alpha \in \mathbb{Q}(\sqrt{d})$, dann ist $\mathcal{O}_d$ ein faktorieller Ring.

Beweis. Wir nehmen an, dass es keine inopportunen Elemente in $\mathbb{Q}(\sqrt{d})$ gibt und weiters, dass $\mathcal{O}_d$ nicht faktoriell ist. Nach Satz 3.3 existiert also ein irreduzibles Element $\pi \in \mathcal{O}_d$, das nicht prim ist, i.e. es gibt außerdem $\xi, \eta \in \mathcal{O}_d$, sodass $\pi \mid \xi\eta$, aber $\pi \nmid \xi$ und $\pi \nmid \eta$. Nehmen wir zusätzlich an, dass $|N_d(\xi\eta)| \in \mathbb{N}_0$ minimal ist. Wir definieren nun

$$\alpha := \begin{cases} \xi\pi^{-1}, \text{ falls } |N_d(\xi)| \geq |N_d(\pi)|, \\ \xi^{-1}\,\pi, \text{ falls } |N_d(\xi)| < |N_d(\pi)|. \end{cases}$$

Dann ist $\alpha \in \mathbb{Q}(\sqrt{d})$. Da $\pi \nmid \xi$, ist $\xi\pi^{-1} \notin \mathcal{O}_d$ und wäre $\xi^{-1}\,\pi \in \mathcal{O}_d$, i.e. $\xi \mid \pi$, so würde $\xi \sim \pi$ folgen. In der Tat, da $\pi \mid \xi\eta$, aber $\pi \nmid \eta$, muss $\xi \notin \mathcal{O}_d^*$ gelten, sodass $\xi \sim \pi$ wegen der Irreduzibilität von π. Also existiert eine Einheit $\varepsilon \in \mathcal{O}_d^*$ mit $\xi = \varepsilon\pi$, im Widerspruch zu $\pi \nmid \xi$. Zusammengefasst gilt ergo $\alpha \notin \mathcal{O}_d$. Nach Voraussetzung muss es also $\gamma, \delta \in \mathcal{O}_d$ geben, sodass $0 < |N_d(\alpha\gamma - \delta)| < 1$. Wir erhalten

$$\begin{aligned} \alpha = \xi\pi^{-1} \Longrightarrow \quad & 0 < |N_d(\xi\gamma\pi^{-1} - \delta)| < 1 \Longrightarrow \quad 0 < |N_d(\xi\gamma - \delta\pi)| < |N_d(\pi)| \leq |N_d(\xi)|, \\ \alpha = \xi^{-1}\,\pi \Longrightarrow \quad & 0 < |N_d(\xi^{-1}\,\pi\gamma - \delta)| < 1 \Longrightarrow \quad 0 < |N_d(\pi\gamma - \delta\xi)| < |N_d(\xi)| \leq |N_d(\pi)|. \end{aligned}$$

In beiden Fällen können wir also $\varphi, \psi \in \mathcal{O}_d$ so wählen, dass $\nu := \xi\varphi - \pi\psi$ die Abschätzung

$$0 < |N_d(\nu)| < \min\{|N_d(\xi)|, |N_d(\pi)|\}$$

erfüllt. Da $|N_d(\nu)| < |N_d(\pi)|$, folgt $\pi \nmid \nu$ und nach Annahme gilt auch $\pi \nmid \eta$ sowie $\pi \mid \nu\eta$. Das ist ein Widerspruch zur Minimalität von $|N_d(\xi\eta)|$, da

$$|N_d(\nu\eta)| = |N_d(\nu)|\,|N_d(\eta)| < |N_d(\xi)|\,|N_d(\eta)| = |N_d(\xi\eta)|.$$

Also muss $\mathcal{O}_d$ schon faktoriell sein. □

In der Praxis ist es schwierig nur mit Hilfe der Definition von inopportunen Elementen nachzuweisen, dass $\mathcal{O}_d$ tatsächlich faktoriell ist, bedingt durch deren „komplizierte“ Form. Allerdings haben wir dazu eine Lösung:

Lemma 6.14. Es sei $d \in \mathbb{Z} \setminus \{0,1\}$ quadratfrei. Ist $\alpha \in \mathbb{Q}(\sqrt{d})$ inopportun, dann existiert ein inopportunes Element $\alpha' \in \mathbb{Q}(\sqrt{d})$ der Form

$$\alpha' = \frac{n - \omega_d}{p}$$

für eine Primzahl p und $n \in \mathbb{N}_0$ mit $0 \leq n < p$.

Beweis. Sei $\alpha \in \mathbb{Q}(\sqrt{d})$ inopportun mit $\alpha = \frac{a + b\omega_d}{c}$ für $a, b \in \mathbb{Z}$ und $c \in \mathbb{N}$ in gekürzter Form. Sei $p \in \mathbb{P}$ ein Primteiler von c und $\alpha_1 := \frac{c}{p}\alpha = \frac{a + b\omega_d}{p}$. Da α vollständig gekürzt ist, folgt aus Lemma 6.12 (4), dass α_1 inopportun ist. Falls $b \mid p$, würde $\frac{b}{p} \in \mathbb{Z}$ folgen und daher wäre die rationale Zahl $\frac{a}{p} = \alpha_1 - \frac{b}{p}\omega_d$ nach Lemma 6.12 (3) inopportun, im Widerspruch zu Lemma 6.12 (2). Daher $\operatorname{ggT}(b, p) = 1$. Nach dem Lemma von Bézout (Lemma 1.1) existieren also $x, y \in \mathbb{Z}$ so, dass $bx - py = -1$. Weil aus $\alpha_1 x \in \mathcal{O}_d$ folgt, dass $p \mid bx$ und daher insbesondere der Widerspruch $p \mid -1$, haben wir $\alpha_1 x \notin \mathcal{O}_d$. Sei

$$\alpha_2 := \alpha_1 x - y\omega_d = \frac{ax + (bx - py)\,\omega_d}{p} = \frac{ax - \omega_d}{p}.$$

Weil α_1 inopportun ist und $\alpha_1 x \notin \mathcal{O}_d$, ist $\alpha_1 x$ inopportun und in weiterer Folge auch $\alpha_2 = \alpha_1 x - y\omega_d$. Nach dem Divisionsalgorithmus existieren $n \in \mathbb{N}_0$ und $z \in \mathbb{Z}$ so, dass $ax = pz + n$. Dann ist $z = \frac{ax - n}{p}$ und

$$\alpha_2 - z = \frac{ax - \omega_d}{p} - \frac{ax - n}{p} = \frac{n - \omega_d}{p}$$

inopportun, wobei $p \in \mathbb{P}$ und $0 \leq n < p$. □

Um zu zeigen, dass $\mathcal{O}_d$ faktoriell ist, reicht es also aus, zu zeigen, dass kein inopportunes Element der Form $\frac{n - \omega_d}{p}$ für eine Primzahl p und eine natürliche Zahl $0 \leq n < p$ existiert. Wir haben bis jetzt noch nicht verwendet, dass $d < 0$ und $d \equiv 1 \pmod 4$. In diesem Fall ist $d = 1 - 4m$ für ein $m \in \mathbb{N}$ und $\omega_d = \frac{1 + \sqrt{d}}{2}$. Für $d = -3, -7, -11$ wissen wir bereits, dass $\mathcal{O}_d$ euklidisch ist, wir können also $m \geq 4$ annehmen. Das führt uns zu folgendem Satz.

Satz 6.3. Sei $d = 1 - 4m$ für $m \in \mathbb{N}, m \geq 4$ und d quadratfrei. Dann ist $\mathcal{O}_d$ genau dann faktoriell, wenn

$$p_d(n) = n^2 - n + m$$

für alle $n \in \{0, \ldots, m-1\}$ eine Primzahl ist.

Beweis. ($\Leftarrow$) Wir führen einen Beweis durch Widerspruch. Nehmen wir an, dass $\mathcal{O}_d$ nicht faktoriell ist. Dann existiert ein inopportunes Element $\alpha \in \mathbb{Q}(\sqrt{d})$ nach Lemma 6.13, das o. B. d. A. von der Form $\alpha = \frac{n - \omega_d}{p}$ für $p \in \mathbb{P}$ und $0 \leq n < p$ ist (Lemma 6.14).

Wir zeigen nun, dass $p \leq m - 1$. Da α inopportun ist, ist

$$n^2 - n + m = N_d(n - \omega_d) \geq N_d(p) = p^2.$$

Da $n < p$ erhalten wir $p^2 \leq n\,(n-1) + m < p\,(p-1) + m = p^2 - p + m$, also tatsächlich $p \leq m - 1$.

Sei nun $0 \leq n < p \leq m - 1$. Dann ist $N_d(n - \omega_d) = n^2 - n + m$ nach Annahme eine Primzahl, sodass zusammen mit dem Faktum $p \in \mathbb{P}$ folgt, dass entweder $p = N_d(n - \omega_d)$ oder $\operatorname{ggT}(p, N_d(n - \omega_d)) = 1$ für jene n. Wäre $p = N_d(n - \omega_d)$ für ein $0 \leq n < p$, dann wäre auch

$$0 < N_d\left(\frac{n - \omega_d}{p}\right) = \frac{N_d(n - \omega_d)}{N_d(p)} = \frac{p}{p^2} < 1,$$

ein Widerspruch zur Inopportunität von α. Somit haben wir $\mathrm{ggT}(p, N_d(n-\omega_d)) = 1$ für alle $0 \leq n < p$. Es existieren also $x, y \in \mathbb{Z}$ mit $N_d(n-\omega_d)\, x - p\, y = 1$ nach Lemma 1.1, sodass wir aus $N_d(n-\omega_d) = (n-\omega_d)\,(n-\omega_d)^*$ die Abschätzung

$$\frac{n-\omega_d}{p}\,(n-\omega_d)^*\, x - y = \frac{1}{p} < 1$$

erhalten. Da $(n-\omega_d)^*\, x$ und y ganzzahlig sind, liefert das ebenfalls den Widerspruch $0 < N_d\Big(\frac{n-\omega_d}{p}\,(n-\omega_d^*)\, x - y\Big) < 1$ zur Inopportunität von α.

($\Rightarrow$) Sei $\mathcal{O}_d$ faktoriell. Wir zeigen zunächst, dass $n-\omega_d$ in $\mathcal{O}_d$ für alle $n \in \{0, \ldots, m-1\}$ irreduzibel ist. Da $\frac{1}{k}\,(n-\omega_d) \notin \mathcal{O}_d$ für $k \in \mathbb{Z} \setminus \{\pm 1\}$, teilt kein $k \in \mathbb{Z} \setminus \{\pm 1\}$ die Zahl $n-\omega_d$. Sei nun $n-\omega_d = \alpha\beta$ für $\alpha, \beta \in \mathcal{O}_d \setminus (\mathbb{Z} \setminus \{\pm 1\})$ mit $\alpha = a + b\omega_d$ und $\beta = e + f\omega_d$, wobei $b \neq 0$, $f \neq 0$; wir führen das zu einem Widerspruch. Dann ist aber

$$N_d(\alpha) = \left(a + \frac{b}{2}\right)^2 + \left(m - \frac{1}{4}\right) b^2 \geq m - \frac{1}{4}$$

und weil $N_d(\alpha) \in \mathbb{Z}$ insbesondere $N_d(\alpha) \geq m$; ein ähnliches Argument zeigt, dass $N_d(\beta) \geq m$ und daraus folgt

$$m^2 \leq N_d(\alpha)\, N_d(\beta) = N_d(\alpha\beta) = N_d(n-\omega_d) = n^2 - n + m < m^2 - m + m = m^2,$$

ein Widerspruch. Somit ist $n-\omega_d$ irreduzibel. Wäre $p_d(n) = n^2 - n + m$ also nicht prim für ein $n \in \{0, \ldots, m-1\}$, so gäbe es Zerlegungen

$$\prod_{i=1}^{k} p_i = n^2 - n + m = N_d(n-\omega_d) = (n-\omega_d)\,(n-\omega_d^*)$$

für Primzahlen $p_1, \ldots, p_k$ und $k \geq 2$, im Widerspruch dazu, dass $\mathcal{O}_d$ faktoriell ist. □

Da $p_d(0) = p_d(1) = m$, reicht es, die Bedingungen von Satz 6.3 für alle Primzahlen $1 \leq n \leq m-2$ zu prüfen. Manuelle Berechnungen zeigen dann, dass in den Fällen

$$d = -19, \quad d = -43, \quad d = -67, \quad d = -163$$

der Ring $\mathcal{O}_d$ sogar faktoriell ist. Gibt es noch mehr Beispiele?

Satz 6.4. Sei $d < 0$ eine quadratfreie Zahl. Dann ist $\mathcal{O}_d$ genau dann faktoriell, falls

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Beweis. Siehe [Cox89], Satz 7.30. □

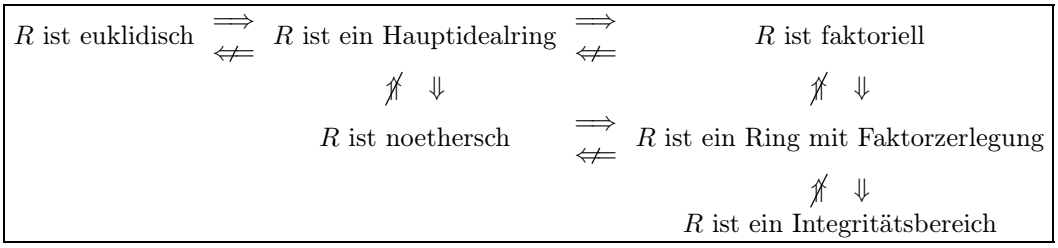
Damit haben wir für $d < 0$ vollständig geklärt, wann $\mathcal{O}_d$ (norm-)euklidisch/Hauptidealring/faktoriell/noethersch/Ring mit Faktorzerlegung ist. Außerdem haben wir Gegenbeispiele für faktorielle Ringe, die nicht euklidisch sind (siehe Kästchen 4) gewonnen.

7 Lokalisierungen und Quotientenkörper

Proposition 7.1. $\mathbb{Z}[X]$ ist faktoriell.

Beweis. Sei $f \in \mathbb{Z}[X]$ beliebig, nicht Null, mit $f = \sum_{i=0}^{n} a_i x^i$ für $a_0,\dots,a_n \in \mathbb{Z}$. Sei $a := \mathrm{ggT}(a_0,\dots,a_n)$, betrachtet als konstantes Polynom. Dann können wir $f = a\,g$ für primitives $g \in \mathbb{Z}[X]$ schreiben und außerdem $a = \prod_{j=1}^{k} p_j$ für Primzahlen $p_1,\dots,p_k \in \mathbb{P}$. In $\mathbb{Q}[X]$ können wir auch $g = \prod_{j=1}^{\ell} q_j$ in irreduzible Polynome $q_1,\dots,q_\ell \in \mathbb{Q}[X]$ zerlegen. Da g primitiv ist, folgt aus dem Lemma von Gauß (Korollar 6.2), dass wir für jedes q_j, $j = 1,\dots,\ell$, ein primitives Polynom $q_j' \in \mathbb{Z}[X]$ mit $q_j \sim q_j'$ finden, sodass $g = \prod_{j=1}^{\ell} q_j'$. Damit ist $f = (\prod_{j=1}^{k} p_j)\,(\prod_{j=1}^{\ell} q_j')$ eine eindeutig bestimmte Zerlegung von f in irreduzible Elemente aus $\mathbb{Z}[X]$. □

Das bringt unsere Übersicht auf folgende Form:



Allerdings sind wir noch nicht fertig: Der Beweis von Proposition 7.1 erweckt stark den Anschein, dass sich eine weitere (strukturelle) Verallgemeinerung verbirgt. Um dem auf den Grund zu gehen, wollen wir unser Augenmerk auf Ideale in Ringen (insbesondere Primideale) lenken. Zwei Beobachtungen dazu:

(1) Im Beweis von Proposition 7.1 sowie einigen anderen Aussagen zu $\mathbb{Z}[X]$, haben wir die Eigenschaften von $\mathbb{Q}[X]$ verwendet und gewissermaßen einen „Übergang“ von $\mathbb{Z}$ nach $\mathbb{Q}$ gemacht.

(2) Ist (0) ein maximales Ideal eines Ringes R, so ist R auch ein Körper. Insbesondere ist R Beispiel eines *lokalen Ringes* (siehe Definition 7.1). Der gesuchte Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ könnte also genau jenem Übergang von einem Ring in seine „Lokalisierung“ entsprechen (cf. andere Konstruktionen mit Ringen, wie $R \rightsquigarrow R[X]$ bzw. $R \rightsquigarrow R/I$).

Lemma 7.1. Sei R ein kommutativer Ring mit Eins. Dann sind die folgenden Bedingungen äquivalent:

(1) R hat genau ein maximales Ideal I.

(2) $R \setminus R^*$ ist ein Ideal von R.

(3) R hat genau ein maximales Ideal I mit $1 + I \subseteq R^*$.

Beweis. (1) ⇒ (2) Setzen wir voraus, dass R genau ein maximales Ideal I hat. Wir zeigen, dass $I = R \setminus R^*$. Da I maximal ist, ist I ein echtes Ideal, ergo $I \subseteq R \setminus R^*$. Nehmen wir nun für einen Widerspruch an, dass $I \subsetneq R \setminus R^*$, i.e. es existiert $a \in R \setminus R^*$ mit $a \notin I$. Dann folgt $I \subsetneq I + (a) = R$ wegen der Maximalität von I. Also können wir $1 = r + ab$ für $r \in I$ und $b \in R$ schreiben. Es folgt, dass $ab = 1 - r \notin I$ und da a per Annahme keine Einheit ist, ist auch $1 - r$ keine Einheit. Sei $\mathcal{I} := \{J \trianglelefteq R \mid (1-r) \subseteq J\}$. Aus dem Lemma von Zorn folgt, dass $\mathcal{I}$ ein maximales Element J hat; insbesondere ist J ein maximales Ideal mit $(1-r) \subseteq J$, sodass $I \neq J$. Da wir I aber als einziges maximales Ideal von R vorausgesetzt haben, ist das ein Widerspruch. Es folgt $I = R \setminus R^*$.

(2) ⇒ (3) Sei $I := R \setminus R^*$; dann ist I nach Annahme ein maximales Ideal. Ist $r \in I$ beliebig, so folgt $1 + r \notin I$, da I ein echtes Ideal ist. Insbesondere gilt $1 + r \notin R \setminus R^*$. Folglich ist $1 + r$ eine Einheit von R und $1 + I \subseteq R^*$.

(3) ⇒ (1) Sei $I \neq J$ ein anderes maximales Ideal von R. Dann gilt $I \subseteq I + J$, also $I + J = R$ nach der Maximalität von I. Das heißt es gibt $r_I \in I, r_J \in J$ sodass $r_I + r_J = 1 \in R$. Insbesondere folgt $r_J = 1 - r_I \in 1 + I \subseteq R^*$, d.h. $J = R$, ein Widerspruch. Es folgt, dass I das eindeutige maximale Ideal von R ist. □

Definition 7.1. Sei R ein kommutativer Ring mit Eins. Erfüllt R eine (und damit alle) Bedingung aus Lemma 7.1, so nennen wir R einen *lokalen Ring*.

Beispiel 7.1. Erinnern wir uns zurück an den Ring der formalen Potenzreihen aus Beispiel 4.4. Ist $R = K$ ein Körper, so ist der Ring $K[[X]]$ der formalen Potenzreihen über K ein lokaler Ring.

Sei $f := \sum_{i=0}^{\infty} a_i X^i$ eine Potenzreihe mit Koeffizienten $a_i \in K, i \geq 0$. Wir wollen zeigen, dass falls $f \notin (X)$ gilt, f Einheit ist. Dann folgt, dass (X) die Menge der Nicht-Einheiten in $K[[X]]$ ist, der Ring also lokal ist. In der Tat können wir das multiplikative Inverse von f explizit angeben, indem wir

$$b_0 := a_0^{-1}, \quad b_i := -a_0^{-1} \left(\sum_{j=0}^{i-1} b_j a_{i-j} \right)$$

für $i \in \mathbb{N}$ setzen, wobei $a_0 \neq 0$, da $f \notin (X)$. Setzen wir $g := \sum_{i=0}^{\infty} b_i X^i$, so gilt $fg = 1$. In der Tat, ist $i > 0$, haben wir $a_0 b_i = -\sum_{j=0}^{i-1} b_j a_{i-j}$, d.h. $\sum_{j=0}^{i} a_{i-j} b_j = 0$, was genau dem i-ten Koeffizienten des Produkts fg entspricht. Da $a_0 b_0 = 1$, ist f also tatsächlich Einheit.

Definition 7.2. Sei R ein kommutativer Ring mit Eins. Wir nennen eine Teilmenge $S \subseteq R$ *multiplikativ*, falls $1 \in S$ und aus $r, s \in S$ auch $rs \in S$ folgt.

Lemma 7.2. Sei R ein kommutativer Ring mit Eins und $I \trianglelefteq R$ ein Ideal von R. Dann ist I genau dann ein Primideal, wenn sein Komplement $S := R \setminus I$ eine multiplikative Teilmenge von R ist.

Beweis. Nehmen wir zunächst an, dass S multiplikativ ist. Da per Definition dann $1 \in S$, folgt dass I ein echtes Ideal ist. Seien $a, b \in R$ mit $ab \in I$ und $a \notin I$; wir wollen zeigen, dass $b \in I$. In der Tat, aus $b \notin I$ folgt $a, b \in S$ und damit $ab \in S$ wegen der Multiplikativität von S, ein Widerspruch zu $ab \in I$. Also $b \in I$, i.e. I ist ein Primideal.

Umgekehrt, sei I ein Primideal und seien $a, b \in S$. Angenommen, $ab \in I$. Da I prim ist, folgt $a \in I$ oder $b \in I$; beide Fälle liefern einen Widerspruch zu $a, b \in S$ und somit muss $ab \notin I$ gelten, i.e. $ab \in S$. Da I ein Primideal ist, folgt $1 \notin I$, d.h. $1 \in S$ und S ist multiplikativ. □

Beispiel 7.2. (1) Sei $R = \mathbb{Z}$ und $S = \{2^k \mid k \in \mathbb{N}_0\} = \{1, 2, 4, \dots\}$. Dann ist S eine multiplikative Teilmenge von R.

(2) Sei $R = \mathbb{Z}$ und $S = \{1\}$. Dann ist S offenbar multiplikativ, aber $R \setminus S = \mathbb{Z} \setminus \{1\}$ ist kein Ideal. Da $R \setminus S$ kein Ideal ist, steht das nicht im Widerspruch zur Aussage von Lemma 7.2.

Die vorhin angedeutete Lokalisierung wollen wir nun formal aufschreiben.

Definition 7.3. Sei R ein kommutativer Ring mit Eins nicht der Nullring. Sei außerdem $S \subseteq R$ eine multiplikative Teilmenge von R. Wir definieren die Relation „$\approx$“ auf $R \times S$ durch

$$(a, s) \approx (b, t) \quad :\Leftrightarrow \quad \exists u \in S : u(at - bs) = 0.$$

Lemma 7.3. Sei R ein kommutativer Ring mit Eins, $S \subseteq R$ eine multiplikative Teilmenge. Dann ist „$\approx$“ eine Äquivalenzrelation auf $R \times S$.

Beweis. Offenbar ist „$\approx$“ reflexiv und symmetrisch. Es verbleibt noch die Transitivität zu zeigen. Seien $(a, s), (b, t), (c, r) \in R \times S$ mit $(a, s) \approx (b, t)$ und $(b, t) \approx (c, r)$. Dann existieren $u, v \in S$ mit

$$u(at - bs) = 0, \quad v(br - ct) = 0.$$

Daraus folgt $urv(at-bs)=0$ und $vsu(br-ct)=0$ und somit $atruv=bsruv=ctsuv$, d.h. $uvt(ar-cs)=0$. Da S multiplikativ ist, ist auch $uvt\in S$ und es folgt $(a,s)\approx(c,r)$, wie gewünscht. □

Ist $(a,s)\in R\times S$, so schreiben wir suggestiv $\frac{a}{s}$ für die von (a,s) induzierte Äquivalenzklasse bezüglich „$\approx$“. Es gilt nämlich:

Definition 7.4. Die Menge

$$S^{-1}R:=\left\{\frac{a}{s}\mid(a,s)\in R\times S\right\}$$

mit den Operationen

$$\frac{a}{s}+\frac{b}{t}:=\frac{at+bs}{st},\quad \frac{a}{s}\cdot\frac{b}{t}:=\frac{a\cdot b}{s\cdot t}$$

definiert einen kommutativen Ring mit Eins, genannt „*Ring der Brüche von R bezüglich S*“.

Es ist klar, welche Elemente von $S^{-1}R$ das Nullelement bzw. das Einselement darstellen. Wir schließen ab jetzt aus, dass $0\in S$, um den Spezialfall zu vermeiden, dass $S^{-1}R$ der Nullring ist. Außerdem erhalten wir wieder einen Homormophismus $\varphi_S: R\to S^{-1}R$, der jedes Element $r\in R$ an den Bruch $\varphi_S(r):=\frac{r}{1}$ schickt. Es gilt $\ker\varphi_S=\{r\in R\mid\exists s\in S: sr=0\}$; insbesondere ist φ_S also eine isomorphe Einbettung, sofern R auch nullteilerfrei ist.

Beispiel 7.3. (1) Warum lassen wir in der Definition von „$\approx$“ Multiplikation mit $u\in S$ zu? Sei zunächst „$\tilde{\approx}$“ auf $R\times S$ definiert durch

$$(a,s)\tilde{\approx}(b,t)\quad:\Leftrightarrow\quad at-bs=0.$$

Falls R ein Integritätsbereich ist und $0\notin S$, sind die Relationen „$\approx$“ und „$\tilde{\approx}$“ gleich. Ist R allerdings nicht nullteilerfrei, verletzen wir mit dieser vereinfachten Version die Transitivität.

Sei beispielsweise $R=\mathbb{Z}/6\mathbb{Z}$ und $S=\{1,2,4\}$. Dann gilt:

$$(3,1)\tilde{\approx}(0,2),\quad (0,2)\tilde{\approx}(0,1),\quad (3,1)\not\tilde{\approx}(0,1).$$

Andererseits haben wir

$$(3,1)\approx(0,2),\quad (0,2)\approx(0,1),\quad (3,1)\approx(0,1).$$

(2) Der Ring der Brüche aus Punkt (1) weist einige kuriose Eigenschaften auf. Zunächst ist der Homomorphismus $\varphi_S: R\to S^{-1}R$ nicht injektiv, da (wie wir auch oben gesehen haben) in $S^{-1}R$ $0=3$ gilt. Man kann zeigen, dass in diesem Fall $S^{-1}R\cong\mathbb{Z}/3\mathbb{Z}$.

(3) Es gilt $S^{-1}R=\{0\}$ genau dann, wenn $0\in S$. Gilt nämlich $\frac{0}{1}=\frac{1}{1}$ in $S^{-1}R$, so existiert $u\in S$ mit $u=u(1\cdot1-0\cdot1)=0$, d.h. $0\in S$. Die Umkehrung folgt unmittelbar.

(4) Die Zuordnung $S\mapsto S^{-1}R$ ist nicht injektiv. Sei $R=\mathbb{Z}$, sei $S=\{6^n\mid n\in\mathbb{N}_0\}$ und $T=\{2^n\cdot3^m\mid m,n\in\mathbb{N}_0\}$. Dann gilt offenbar $S\neq T$, aber $S^{-1}R=T^{-1}R$.

Definition 7.5. Es sei R ein kommutativer Ring mit Eins und nicht der Nullring. Sei $I\in\operatorname{Spec}R$; dann ist $R\setminus I$ nach Lemma 7.2 multiplikativ. Wir nennen

$$R_I:=S^{-1}R=(R\setminus I)^{-1}R$$

die *Lokalisierung von R bei I*.

Bevor wir uns Beispiele ansehen, untersuchen wir noch einige elementare Eigenschaften von Lokalisierungen.

Lemma 7.4. Sei R ein kommutativer Ring mit Eins und nicht der Nullring. Sei I ein Primideal. Dann ist $\frac{a}{s} \in (R_I)^*$ genau dann, wenn $a \notin I$.

Beweis. Falls $\frac{a}{s}$ eine Einheit von R_I ist, so existiert $\frac{b}{t} \in R_I$ mit

$$\frac{ab}{st} = \frac{a}{s} \cdot \frac{b}{t} = 1,$$

d.h. es existiert $u \in R \setminus I$ mit $u(ab - st) = 0$. Weil $R \setminus I$ multiplikativ ist, folgt $uab = ust \in R \setminus I$ und daher außerdem $a \notin I$, wie gewünscht. Ist umgekehrt $a \notin I$, so ist $a \in R \setminus I$ und daher $\frac{s}{a} \in R_I$ mit $\frac{a}{s} \cdot \frac{s}{a} = 1$. □

Eine weitere wichtige Folgerung:

Folgerung 7.1. Sei R ein kommutativer Ring mit Eins und nicht der Nullring. Sei I ein Primideal. Dann ist R_I ein lokaler Ring.

Beweis. Nach Lemma 7.4 ist $R_I \setminus R_I^* = \left\{\frac{a}{s} \mid a \in I\right\}$. Da I ein Ideal von R ist, ist $R_I \setminus R_I^*$ ein Ideal von R_I. Somit ist R_I nach Lemma 7.1 ein lokaler Ring. □

Beispiel 7.4. (1) Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\right\}$ per Definition und nach Lemma 7.4 gilt weiterhin $\mathbb{Z}_{(p)}^* = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid a, p \nmid b\right\}$. Da $\mathbb{Z}_{(p)}$ nach Korollar 7.1 ein lokaler Ring ist, hat $\mathbb{Z}_{(p)}$ nur ein maximales Ideal und dieses Ideal ist $\mathbb{Z}_{(p)}^*$.

(2) Wir wollen alle Unterringe von $\mathbb{Q}$, die $\mathbb{Z}$ enthalten, finden. Sei $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ ein derartiger Ring. Dann ist die Menge

$$S := \left\{b \in \mathbb{N} \mid \exists a \in \mathbb{Z} : \frac{a}{b} \in R,\ \mathrm{ggT}(a,b) = 1\right\}$$

nicht leer. Wir zeigen, dass S multiplikativ ist und $R = S^{-1}\mathbb{Z}$. Sei $b \in S$ beliebig und $\frac{a}{b} \in R$ mit $\mathrm{ggT}(a,b) = 1$; dann gibt es $x, y \in \mathbb{Z}$ mit $ax + by = 1$, insbesondere $\frac{a}{b}x + y = \frac{1}{b}$, sodass $\frac{1}{b} \in R$. Also ist $\frac{1}{b} \in R$ für alle $b \in S$. Daraus folgt unmittelbar, dass S multiplikativ ist und $R = S^{-1}\mathbb{Z}$.

Folgerung 7.2. Sei R ein Integritätsbereich. Dann ist die Lokalisierung von R bei (0) ein Körper.

Beweis. Wir haben $(R_{(0)})^* = \left\{\frac{a}{s} \mid a \notin (0)\right\} = R_{(0)} \setminus \{0\}$ nach Lemma 7.4. □

Diesem Körper geben wir auch einen speziellen Namen.

Definition 7.6. Sei R ein Integritätsbereich. Dann nennen wir $R_{(0)}$ den *Quotientenkörper* von R[7.1].

Beispiel 7.5. (1) Ist $R = \mathbb{Z}$, so ist der Quotientenkörper $\mathbb{Z}_{(0)}$ der gewohnte Körper der rationalen Zahlen, i.e. $\mathbb{Z}_{(0)} = \mathbb{Q}$.

7.1. Englisch: „*field of fractions*“.

(2) Es sei K ein Körper und $K[X]$ der zugehörige Polynomring. Dann schreiben wir $K(X)$ für den Quotientenkörper von $K[X]$. Analog schreiben wir $K(X_1,\dots,X_n)$ für den Quotientenkörper des Polynomrings von K in n Variablen, $K[X_1,\dots,X_n]$. Die Elemente dieses Körpers nennen wir *rationale Funktionen über K in den Variablen $X_1,\dots,X_n$*. Im Allgemeinen sind die Elemente von $K(X_1,\dots,X_n)$ aber nicht an allen Punkten definiert, intuitiv genau dann, wenn der Nenner der rationalen Funktion eine Nullstelle hat.

(3) Der Körper $\mathbb{C}(X)$ ist eine echte Körpererweiterung der komplexen Zahlen (d.h. ein Körper, der $\mathbb{C}$ enthält).

(4) Ist $d\in\mathbb{Z}\setminus\{0,1\}$ quadratfrei, so ist $\mathbb{Q}(\sqrt{d})$ der Quotientenkörper von $\mathcal{O}_d$. In der Tat, sind α, $\beta\in\mathcal{O}_d$, $\beta\neq 0$, so ist $\frac{\alpha}{\beta}=\frac{\alpha\beta^*}{N_d(\beta)}\in\mathbb{Q}(\sqrt{d})$ und umgekehrt, falls $\alpha\in\mathbb{Q}(\sqrt{d})$, so können wir $\alpha=\frac{a+b\omega_d}{c}$ für $a,b,c\in\mathbb{Z}$ mit $c\neq 0$ schreiben.

Kehren wir nun zu unserer ursprünglichen Motivation zurück, die Lokalisierung eines Rings einzuführen. Die Beweise der folgenden Behauptungen übertragen sich nahezu wortgleich aus den zuvor bewiesenen Lemma 6.4, Folgerung 6.2, Folgerung 6.3 und Proposition 7.1 indem wir „$\mathbb{Z}$“ durch „R“ und „$\mathbb{Q}$“ durch „K“ ersetzen.

Lemma 7.5. Sei R ein faktorieller Ring und $K:=R_{(0)}$ der Quotientenkörper von R. Ein primitives Polynom $f\in R[X]$ ist in $R[X]$ genau dann irreduzibel, wenn es in $K[X]$ irreduzibel ist.

Folgerung 7.3. Sei R ein faktorieller Ring und $K:=R_{(0)}$ der Quotientenkörper von R.

Sei $f\in R[X]$ ein primitives Polynom. Zerfällt f in ein Produkt $f=gh$ mit $g,h\in K[X]$, so existieren primitive Polynome $g',h'\in R[X]$, sodass $g\sim g'$ und $h\sim h'$ in $K[X]$ und $f=g'h'$. Insbesondere unterscheiden sich die Faktoren in $K[X]$ von denen in $R[X]$ nur durch Konstanten in K.

Folgerung 7.4. Sei R ein faktorieller Ring und $K:=R_{(0)}$ der Quotientenkörper von R.

Sei $f\in R[X]$ ein normiertes Polynom das Produkt $f=gh$ zweier normierter Polynome $g,h\in K[X]$. Dann folgt $g,h\in R[X]$.

Proposition 7.2. Sei R ein faktorieller Ring. Dann ist $R[X]$ faktoriell.

Folgerung 7.5. Sei R ein faktorieller Ring. Dann ist auch $R[X_1,\dots,X_n]$ faktoriell.

Ein durchaus nützliches Resultat, zurückgehend auf Theodor Schönemann[7.2], aber nach Gotthold Eisenstein[7.3] benannt:

Proposition 7.3. (Eisensteinkriterium) Sei R ein faktorieller Ring mit Quotientenkörper $K=R_{(0)}$. Ist $f\in R[X]$ ein primitives Polynom vom Grad $\deg(f)=n$ mit $f=\sum_{i=0}^{n}a_iX^i$ und existiert ein Primelement $p\in R$, sodass

- $p\,|\,a_i$ für $i=0,\dots,n-1$,
- $p\nmid a_n$,
- $p^2\nmid a_0$,

dann ist f irreduzibel in $R[X]$ und $K[X]$.

7.2. Theodor Schönemann (1812 – 1868), deutscher Mathematiker

7.3. Gotthold Eisenstein (1823 – 1852), deutscher Mathematiker

Beweis. Sei $p \in R$ ein Primelement, das die drei genannten Eigenschaften erfüllt. Da $p \mid a_0$, aber $p \nmid a_n$, folgt $n \geq 1$. Nach Lemma 7.5 ist es ausreichend die Irreduzibilität von f in $R[X]$ zu zeigen. Nehmen wir also indirekt an, dass $f = g \cdot h$ für $g, h \in R[X]$, wobei g und h nicht Einheiten sind. Dann folgt $\deg(g), \deg(h) > 0$. In der Tat, aus $\deg(g) = 0$ folgt, dass $g = b_0 \in R$. Dann ist aber b_0 ein Teiler aller Koeffizienten von f und, da f primitiv ist, somit Einheit; ein Widerspruch. Ähnlich zeigt man, dass $\deg(h) > 0$. Wir können also $g = \sum_{i=0}^{r} b_i X^i$ und $h = \sum_{i=0}^{s} c_i X^i$ für $r = \deg(g), s = \deg(h)$ und $b_0, \ldots, b_r, c_0, \ldots, c_s \in R$ schreiben. Da R ein Integritätsbereich ist, folgt $r + s = \deg(g \cdot h) = \deg(f) = n$ und damit $r, s \leq n - 1$. Weiters gilt $a_n = b_r c_s$ und $a_0 = b_0 c_0$; da $p \nmid a_n$, folgt $p \nmid b_r$ sowie $p \nmid c_s$ und aus $p^2 \nmid a_0$ folgt, dass p genau einen Faktor b_0 oder c_0 teilt. O. B. d. A. nehmen wir an, dass $p \mid b_0$ und $p \nmid c_0$. Sei nun $t \in \mathbb{N}_0$ mit der Eigenschaft, dass $p \mid b_i$ für $i = 0, \ldots, t$ maximal gewählt. Dann gilt $0 \leq t < r$. Betrachten wir den Koeffizienten

$$a_{t+1} = b_{t+1} c_0 + \sum_{i=1}^{t} b_i c_{t-i+1}$$

und bemerken, dass jeder Summand in der rechten Summe nach Definition von t durch p teilbar ist. Da aber $p \nmid b_{t+1} c_0$, folgt $p \nmid a_{t+1}$, sodass nur die Möglichkeit $t + 1 = n$ verbleibt. Daraus folgt aber $r = \deg(g) \geq t + 1 = n$ und das ist ein Widerspruch. □

Ein Polynom, für das ein solches p existiert, wird auch *Eisensteinpolynom bezüglich p genannt*.

Beispiel 7.6. (1) Betrachten wir das Polynom $f := X^3 + 6X^2 + 4X + 2 \in \mathbb{Z}[X]$. Wenden wir das Eisensteinkriterium mit $p = 2$ an, folgt die Irreduzibilität von f in $\mathbb{Z}[X]$ (und demnach auch $\mathbb{Q}[X]$).

(2) Die Umkehrung des Eisensteinkriteriums gilt nicht. Das ganzzahlige Polynom $X^2 + 4$ erfüllt die Voraussetzungen nicht, ist aber in $\mathbb{Q}[X]$ irreduzibel. Auch $X^2 - 4$ erfüllt das Kriterium nicht, ist aber in $\mathbb{Q}[X]$ in $X^2 - 4 = (X + 2)(X - 2)$ zerlegbar.

(3) Sei $n \geq 2$ eine natürliche Zahl und p eine Primzahl. Das Polynom $f := X^n - p \in \mathbb{Z}[X]$ ist nach dem Eisensteinkriterium (angewandt mit p) irreduzibel in $\mathbb{Q}[X]$. Dies zeigt insbesondere, dass $\sqrt[n]{p}$ irrational ist und dass es für jeden Grad $n \geq 1$ irreduzible Polynome in $\mathbb{Q}[X]$ gibt.

(4) Sei $f := X^2 + Y^2 + 1$ ein Polynom in $\mathbb{R}[X, Y]$. Da $\mathbb{R}[X, Y] \cong (\mathbb{R}[X])[Y]$ können wir f als Polynom in der Variablen Y mit Koeffizienten im Ring $R := \mathbb{R}[X]$ auffassen, d.h $f = Y^2 + (X^2 + 1) \in R[Y]$. Dann ist R ein faktorieller Ring und das Element $p := X^2 + 1$ ist in $\mathbb{R}[X]$ irreduzibel, somit ein Primelement. Aus dem Eisensteinkriterium folgt nun, dass f in $\mathbb{R}[X, Y]$ irreduzibel ist.

(5) Sei p eine Primzahl. Das *p-te Kreisteilungspolynom* (oder *p-tes zyklotomisches Polynom*) ist definiert als

$$\Phi_p := \sum_{i=0}^{p-1} X^i = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Dann gilt $\Phi_p = \frac{X^p - 1}{X - 1}$. Zwar können wir das Eisensteinkriterium nicht direkt auf Φ_p anwenden, aber betrachten wir die Substitution

$$g := \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{1}{X} \sum_{k=1}^{p} \binom{p}{k} X^k = \sum_{k=1}^{p} \binom{p}{k} X^{k-1},$$

so sehen wir, dass p alle Koeffizienten mit Ausnahme des Leitkoeffizienten teilt (siehe auch Lemma 5.1) und p^2 kein Teiler des konstanten Gliedes ist, d.h. g ist nach dem Eisensteinkriterium irreduzibel. Dementsprechend ist auch Φ_p irreduzibel. Mehr zu diesem Polynom in Beispiel 1.5 (4).

Schließen wir nun den Kreis und kommen zurück zum quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ und den Ringen ganzer Zahlen $\mathcal{O}_d$. Den Fall $d < 0$, quadratfrei, haben wir bereits untersucht; nehmen wir also nun an, dass $d \geq 2$. Wir wissen bereits, dass $\mathcal{O}_d$ *genau dann* ein Hauptidealring ist, wenn er faktoriell ist (Satz 6.1), genauso wie im Fall $d < 0$. Durchaus gibt es noch mehr Ähnlichkeiten, aber auch Unterschiede.

Beispiel 7.7. (1) Da X^2-2 und X^2-3 in $\mathbb{F}_5[X]$ irreduzibel sind, sind $2, 3, 2\pm\sqrt{10}$ in $\mathcal{O}_{10}$ irreduzibel. Dann folgt aber, dass -6 die zwei Zerlegungen

$$(2+\sqrt{10})\,(2-\sqrt{10}) = -6 = (-1)\,(2)\,(3)$$

hat, also ist $\mathcal{O}_{10}$ nicht faktoriell.

(2) Für $d \geq 2$ gibt es Beispiele von Ringen, die euklidisch sind, aber nicht norm-euklidisch, im Gegensatz zum Fall $d<0$. Beispielsweise kann man zeigen, dass $\mathcal{O}_{14}$ nicht bezüglich $\omega = |N_{14}|$ euklidisch ist, aber dafür bezüglich einer anderen Abbildung.

(3) Sei $\phi := \frac{1+\sqrt{5}}{2}$ der goldene Schnitt; dann gilt bekanntermaßen $\phi^2 - \phi - 1 = 0$, sodass ϕ eine Einheit von $\mathcal{O}_5$ ist. Da $\phi > 1$ und die Einheitengruppe unter der Multiplikation abgeschlossen ist, folgt, dass $\mathcal{O}_5$ unendlich viele Einheiten hat, erneut ein Unterschied zum Fall $d<0$, wo wir nur endlich viele Einheiten haben (siehe Beispiel 6.3).

Beispiel 7.7 (3) lässt sich sogar verallgemeinern. Ist $d \geq 2$ eine quadratfreie ganze Zahl, so ist die Einheitengruppe von $\mathcal{O}_d^*$ unendlich. Um das zu beweisen, benötigen wir einen Satz aus der Zahlentheorie, benannt nach Adolf Hurwitz[7.4]:

Satz 7.1. (Hurwitz) Sei $\alpha \in \mathbb{R}$ eine irrationale Zahl. Dann existieren unendlich viele $p, q \in \mathbb{Z}$ mit $\mathrm{ggT}(p,q) = 1$, sodass

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\,q^2}.$$

Beweis. Siehe Satz 193 in [HW60]. □

Lemma 7.6. Sei $d \geq 2$ eine quadratfreie ganze Zahl. Dann existiert ein kleinstes $\varepsilon_0 \in \mathcal{O}_d^*$ mit $\varepsilon_0 > 1$. Wir nennen ε_0 *Fundamentaleinheit*.

Proposition 7.4. Sei $d \geq 2$ eine quadratfreie ganze Zahl und ε_0 die zugehörige Fundamentaleinheit. Dann gilt:

$$\mathcal{O}_d^* = \{\kappa \cdot \varepsilon_0^n \mid \kappa = \pm 1, n \in \mathbb{Z}\}.$$

Beweis. Aus Lemma 2.1 folgern wir unmittelbar die erste Mengeninklusion. Sei nun umgekehrt $\varepsilon \in \mathcal{O}_d^*$. Wir unterscheiden vier Fälle.

- $\varepsilon = 1$: Offensichtlich.
- $\varepsilon > 1$: Dann gilt $\varepsilon_0 \leq \varepsilon$ und daher existiert ein $n \in \mathbb{N}$ mit $\varepsilon_0^n \leq \varepsilon < \varepsilon_0^{n+1}$, insbesondere $1 \leq \varepsilon\varepsilon_0^{-n} < \varepsilon_0$. Wegen $\varepsilon\varepsilon_0^{-n} < \varepsilon_0$ muss $\varepsilon\varepsilon_0^{-n} = 1$ folgen, d.h. $\varepsilon = \varepsilon_0^n$, wie gewünscht.
- $0 < \varepsilon < 1$: Dann ist $\varepsilon^{-1} > 1$ und aus dem obigen Fall folgt, dass ein $m \in \mathbb{Z}$ mit $\varepsilon^{-1} = \varepsilon_0^m$ existiert. Insbesondere gilt $\varepsilon = \varepsilon_0^{-m}$.
- $\varepsilon < 0$: Dann ist $-\varepsilon > 0$, also folgt aus den bereits gezeigten Fällen, dass $-\varepsilon = \varepsilon_0^m$ für ein $m \in \mathbb{Z}$ und damit $\varepsilon = -\varepsilon_0^m$.

Also hält auch die umgekehrte Mengeninklusion. □

Unmittelbar aus dieser Proposition folgt:

7.4. Adolf Hurwitz (1859 – 1919), deutscher Mathematiker

Folgerung 7.6. Für $d \geq 2$ eine quadratfreie ganze Zahl ist $\mathcal{O}_d^*$ ist abzählbar unendlich.

Damit haben wir einen wesentlichen Unterschied zwischen $\mathcal{O}_d$ für $d \geq 2$ und $\mathcal{O}_d$ für $d < 0$ gefunden, da die Einheitengruppe des letzteren Ringes nach Beispiel 6.3 jedenfalls endlich ist. Der Approximationssatz von Hurwitz ist in dieser Hinsicht jedoch noch tiefgreifender. Topologisch betrachtet liegt $\mathcal{O}_d$ für $d \geq 2$ dicht in den reellen Zahlen (als Obermenge der rationalen Zahlen), während $\mathcal{O}_d$ für $d < 0$ diskret in $\mathbb{C} = \mathbb{R}^2$ liegt. Um zu sehen, wie wichtig diese Eigenschaften sind, blicken wir auf den Beweis von Satz 1.4, die Division mit Rest, zurück: „Wir setzen $q := \left\lfloor \frac{a}{b} \right\rfloor$ (*die größte ganze Zahl, die kleiner oder gleich* $\frac{a}{b}$ *ist*)…“

Schließen wir nun unsere Diskussion der Ringe (der ganzen Zahlen) ab. Dazu geben wir einen Überblick zahlentheoretischer Ergebnisse, die die wichtigsten verbleibenden Fragen – nämlich jene, die wir im Fall $d < 0$ bereits untersucht haben – beantworten. Eine deutlich tiefgehendere Studie ist in [Lem04] zu finden.

Satz 7.2. (Chatland, Davenport, Inkeri) Es sei $d \geq 2$ eine quadratfreie ganze Zahl. Dann ist $\mathcal{O}_d$ genau dann norm-euklidisch, wenn

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Satz 7.3. (Narkiewicz) Es sei $d \geq 2$ eine quadratfreie ganze Zahl. Für alle, bis auf höchstens zwei Ausnahmen ist $\mathcal{O}_d$ genau dann faktoriell, wenn er euklidisch ist.

Es ist unbekannt, ob es unendlich viele quadratfreie ganze Zahlen $d \geq 2$ gibt, sodass $\mathcal{O}_d$ faktoriell ist. Jedenfalls wird es vermutet. Ebenso wird vermutet, dass es die zwei „ominösen“ Ausnahmen in Narkiewicz' Theorem nicht gibt. Der Grund dafür ist u. a. in der Theorie der automorphen Formen und ihrer L-Funktionen zu finden, siehe z. B. [Gro23].

2 Körper

Widmen wir uns nun der Körpertheorie ganz allgemein. Im letzten Abschnitt haben wir $\mathcal{O}_d$ als Unterring von $\mathbb{Q}(\sqrt{d})$ untersucht und kurz bemerkt, dass $\mathbb{Q}(\sqrt{d})$ eine „Körpererweiterung von $\mathbb{Q}$ vom Grad 2“ ist. Das suggeriert die Existenz von Körpererweiterungen höheren Grades. Die Formalisierung dieser Konzepte wird ein wesentlicher Bestandteil dieses Kapitels sein. In unserer Untersuchung von Ringen haben wir bereits zahlreiche andere Beispiele von Körpern gesehen: Die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$, insbesondere die auf Cauchy[0.1] zurückgehende Beschreibung als $\mathbb{R}[X]/(X^2+1)$ oder die zuletzt studierten Quotientenkörper.

1 Algebraische Körpererweiterungen

Definition 1.1. Es seien K, L Körper mit $K \subseteq L$.

(1) Wir nennen L *Körpererweiterung von* K oder *Erweiterungskörper von* K. Ferner nennen wir K dann *Teilkörper von* L. Ist außerdem M ein Körper mit $K \subseteq M \subseteq L$, so heißt M *Zwischenkörper*. Wir schreiben $L\colon K$, um die Körpererweiterung von L über K zu bezeichnen.

(2) Die Körpermultiplikation von Elementen aus K mit Elementen aus L macht L zu einem Vektorraum über K. Als solcher besitzt L eine bestimmte Dimension $\dim_K L$. Sie heißt *Grad von* L *über* K und wird mit $[L\colon K]$ bezeichnet. Eine Körpererweiterung $L\colon K$ von endlichem Körpergrad heißt *endlich*.

0.1. Augustin-Louis Cauchy (1789 – 1857), französischer Mathematiker und Physiker

Beispiel 1.1. (1) Die reellen Zahlen sind eine Körpererweiterung der rationalen Zahlen, $\mathbb{Q} \subseteq \mathbb{R}$.

(2) Für $d \in \mathbb{Z}$, quadratfrei, haben wir $\mathbb{Q}(\sqrt{d})$ als Körpererweiterung von $\mathbb{Q}$ kennengelernt. Insbesondere ist $\mathbb{Q}(\sqrt{d})$ Zwischenkörper $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

(3) Ist K ein Körper, so ist der Körper der rationalen Funktionen $K(X)$ über K eine Körpererweiterung von K. Offenbar ist im Gegensatz dazu $K[X]$ *keine* Körpererweiterung von K.

Lemma 1.1. Es seien $K \subseteq K' \subseteq K''$ drei Körper. Dann gilt

$$[K'' : K] = [K'' : K'] \cdot [K' : K].$$

Insbesondere ist $K'' : K$ genau dann endlich, wenn sowohl $K' : K$, als auch $K'' : K'$ endlich sind.

Beweis. Es sei U eine Basis von $K'' : K'$ und V eine Basis von $K' : K$. Wir zeigen, dass $W := \{uv \mid u \in U, v \in V\}$ eine Basis von $K'' : K$ ist. Aus der linearen Unabhängigkeit von U folgt dann, dass die Elemente in W paarweise verschieden sind und daraus die Behauptung.

Erzeugendensystem: Sei $u \in K''$ beliebig. Dann ist $u = \sum_{i=1}^{n} m_i u_i$ für ein $n \in \mathbb{N}, m_i \in K'$ und $u_i \in U$, da U Erzeugendensystem von K'' als K'-Vektorraum ist. Da aber K' ein K-Vektorraum ist, ist jedes m_i von der Form $m_i = \sum_{j=1}^{n_i} k_{ij} v_j$ für ein $n_i = n_i(m_i), k_{ij} \in K$ und $v_j \in V$. Daher ist

$$u = \sum_{i=1}^{n} m_i u_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n_i} k_{ij} v_j \right) u_i = \sum_{i=1}^{n} \sum_{j=1}^{n_i} k_{ij} (u_i v_j),$$

sodass W ein Erzeugendensystem von K'' über K ist.

Lineare Unabhängigkeit: Sei nun

$$\sum_{i=1}^{n} \sum_{j=1}^{\ell} k_{ij} (u_i v_j) = 0 \quad \text{für } \ell, n \in \mathbb{N}, k_{ij} \in K \text{ und } u_i v_j \in W.$$

Sei $m_i := \sum_{j=1}^{\ell} k_{ij} v_j \in K'$ für $i = 1, \ldots, n$. Dann folgt $\sum_{i=1}^{n} m_i u_i = 0$ und da U als Basis von K'' über K' linear unabhängig ist, muss $m_i = 0$ für alle i folgen. Insbesondere folgt daraus, dass $\sum_{j=1}^{\ell} k_{ij} v_j = 0$ und da V als Basis von K' über K auch linear unabhängig ist, folgt sogar $k_{ij} = 0$ für alle i und j. Damit ist die lineare Unabhängigkeit von W gezeigt. □

Eine interessante Konsequenz ist:

Folgerung 1.1. Es seien $K \subseteq K' \subseteq K''$ drei Körper. Dann folgt, dass $[K' : K]$ ein Teiler von $[K'' : K]$ ist. Insbesondere gilt: Wenn $[K'' : K]$ eine Primzahl ist, so gibt es zwischen K'' und K keinen echten Zwischenkörper.

Beweis. Die erste Aussage folgt unmittelbar aus Lemma 1.1. Ist $[K'' : K]$ eine Primzahl und gibt es einen Zwischenkörper $K \subseteq K' \subseteq K''$, so folgt aus demselben Lemma $[K' : K] = 1$ oder $[K'' : K'] = 1$. Insbesondere muss $K = K'$ oder $K' = K''$ gelten. □

Lemma 1.1 ist also ein hilfreiches Werkzeug, die Frage der Existenz von Teilkörpern in ein Teilbarkeitsproblem zu verwandeln.

Definition 1.2. Es sei L ein Körper und $\Theta \subseteq L$ eine Teilmenge.

(1) Der Durchschnitt aller Teilkörper (bzw. Unterringe) von L, welche Θ enthalten, ist ein Teilkörper (bzw. Unterring) von L und heißt der *von* Θ *erzeugte Teilkörper* (bzw. *Unterring*) *von* L.

(2) Ist $L:K$ eine Körpererweiterung eines Körpers K und $\Xi \subseteq L$ eine Teilmenge, so heißt der von $K \cup \Xi$ erzeugte Teilkörper (bzw. Unterring) von L der *von* Ξ *über* K *erzeugte Teilkörper* (bzw. *Unterring*) *von* L und wird mit $K(\Xi)$ (bzw. $K[\Xi]$) bezeichnet. Ist $\Xi = \{\alpha_1, \ldots, \alpha_n\}$ eine endliche Menge, so schreiben wir $K(\alpha_1, \ldots, \alpha_n)$ (bzw. $K[\alpha_1, \ldots, \alpha_n]$).

Die Notation aus Punkt (2) erinnert stark an jene der (Lokalisierung von) Polynomringen. Das ist auch gerechtfertigt:

Proposition 1.1. Sei $L:K$ eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt für den von K und $\alpha_1, \ldots, \alpha_n$ erzeugten Zwischenkörper

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, a_n)} \mid f, g \in K[X_1, \ldots, X_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Beweis. Sei S die rechte Seite. Ist $\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \in S$ für $f, g \in K[X_1, \ldots, X_n]$ und $g(\alpha_1, \ldots, \alpha_n) \neq 0$, so sind der Zähler und Nenner Elemente von $K(\alpha_1, \ldots, \alpha_n)$, da dieser als Körper unter Multiplikation und Addition abgeschlossen ist und damit auch das Ergebnis der Division dieser Elemente. Es folgt $S \subseteq K(\alpha_1, \ldots, \alpha_n)$. Umgekehrt folgt unmittelbar, dass S ein Teilkörper von L ist, der $K \cup \{\alpha_1, \ldots, \alpha_n\}$ enthält und damit per Definition $K(\alpha_1, \ldots, \alpha_n) \subseteq S$. □

Ein analoges Resultat werden wir in Kürze auch für $K[\alpha_1, \ldots, \alpha_n]$ sehen.

Definition 1.3. Es sei $K \subseteq L$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch über* K, falls $f \in K[X]$, $f \neq 0$, existiert mit $f(\alpha) = 0$. Falls kein solches Polynom existiert, nennen wir α *transzendent über* K. Die Erweiterung $L:K$ heißt *algebraisch*, wenn jedes Element von L algebraisch ist und sonst nennen wir $L:K$ *transzendent*.

Beispiel 1.2. (1) Sei $K = \mathbb{Q}$ und $\alpha = \sqrt{2}$. Dann ist $f := X^2 - 2 \in K[X]$ ein Polynom mit $\sqrt{2}$ als Nullstelle. Folglich ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$. Eine transzendente Körpererweiterung $L:K$ kann also sehr wohl algebraische Elemente enthalten, die nicht schon in K waren.

(2) Als Nullstelle von $X^2 + 1$ ist $\sqrt{-1}$ algebraisch über $\mathbb{Q}$ und daher insbesondere über $\mathbb{R}$.

(3) Charles Hermite[1.1] hat im Jahr 1873 bewiesen, dass e transzendent ist. Kurz danach hat Lindemann[1.2] im Jahr 1882 gezeigt, dass auch π transzendent ist.

(4) Ist $\alpha \in K$, dann ist α auch algebraisch über K, nämlich als Nullstelle des Polynoms $X - \alpha$.

(5) Ein algebraisches Element über $\mathbb{Q}$ heißt *algebraische Zahl*. Da es höchstens abzählbar unendlich viele rationale Polynome mit endlich vielen Nullstellen und deshalb nur höchstens abzählbar unendlich viele algebraische Zahlen gibt, folgt, dass überabzählbar unendlich viele transzendente reelle Zahlen existieren.

Die Bedeutung algebraischer Elemente sehen wir in folgendem Satz.

Satz 1.1. Es sei $L:K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann gilt:

(1) $K(\alpha) = K[\alpha]$.

(2) $K(\alpha) \cong K[X]/(\varphi)$ für ein irreduzibles, monisches Polynom $\varphi \in K[X]$ vom Grad $n \geq 1$.

(3) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ ist eine K-Basis von $K(\alpha)$ und es gilt $[K(\alpha):K] = n$.

Insbesondere ist das Polynom φ in (2) als irreduzibles, monisches Polynom mit $\varphi(\alpha) = 0$ eindeutig bestimmt. Ist $g \in K[X]$ mit $g(\alpha) = 0$, so folgt $\varphi \mid g$.

1.1. Charles Hermite (1822 – 1901), französischer Mathematiker

1.2. Carl Louis Ferdinand Lindemann (1852 – 1939), deutscher Mathematiker

Beweis. (1) Da $K \subseteq K[\alpha]$, können wir die Evaluationsabbildung $\mathrm{ev}_\alpha : K[X] \to K[\alpha]$ betrachten. Diese ist ein Ringhomomorphismus und sogar surjektiv. In der Tat, da offenbar $K \cup \{\alpha\} \subseteq \operatorname{im} \mathrm{ev}_\alpha$ folgt aus der Definition von $K[\alpha]$ als Durchschnitt aller Unterringe, die $K \cup \{\alpha\}$ enthalten, dass $K[\alpha] \subseteq \operatorname{im} \mathrm{ev}_\alpha$ und daher sogar $K[\alpha] = \operatorname{im} \mathrm{ev}_\alpha$.

Nach Lemma 4.6 (1) ist $\ker \mathrm{ev}_\alpha \trianglelefteq K[X]$ ein Ideal von $K[X]$. Nach Proposition 4.1 ist $K[X]$ aber ein Hauptidealring und somit existiert $f \in K[X]$ mit $\ker \mathrm{ev}_\alpha = (f)$. Dann gilt $f(\alpha) = 0$. Insbesondere folgt aus α algebraisch, dass $(f) \neq (0)$ und aus der Surjektivität von ev_α, dass $\ker \mathrm{ev}_\alpha \neq K[X]$. Somit ist (f) ein echtes Ideal von $K[X]$, also $f \neq 0$ und $f \notin K[X]^*$. Daraus folgt, dass $\deg(f) \geq 1$. Wir können also $f = \sum_{i=0}^{n} a_i X^i$ für $a_0, \ldots, a_n \in K$ mit $n = \deg(f)$ schreiben. Da $a_n \neq 0$, ist $\varphi := a_n^{-1} f$ wohldefiniert. Wir halten einige Eigenschaften von φ fest:

- φ ist monisch mit $\deg(\varphi) \geq 1$.
- Es gilt $\varphi \sim f$ und somit $(\varphi) = (f)$ nach Lemma 3.5 (2).
- $\varphi \in \ker \mathrm{ev}_\alpha$, also $\varphi(\alpha) = 0$.

Aus dem Isomorphiesatz für Ringe 4.2 folgt, dass

$$K[X]/(\varphi) = K[X]/\ker \mathrm{ev}_\alpha \cong \operatorname{im} \mathrm{ev}_\alpha = K[\alpha].$$

Da $K[\alpha] \subseteq L$, ist $K[\alpha]$ nullteilerfrei, sodass nach Proposition 4.3 (φ) ein Primideal in $K[X]$ ist, φ also ein Primelement in $K[X]$ (Lemma 4.2), daher irreduzibel (Lemma 3.4) und also ein maximales Ideal (Proposition 4.1 und Lemma 3.5 (3)), insbesondere $K[X]/(\varphi)$ also ein Körper (Proposition 4.3). Da $K(\alpha)$ nach Definition der *kleinste* Körper ist, der $K \cup \{\alpha\}$ enthält muss schon $K(\alpha) = K[\alpha]$ gelten.

(2) Aus Teil (1) wissen wir, dass $K(\alpha) \cong K[X]/(\varphi)$ für ein irreduzibles, monisches Polynom φ mit $\deg(\varphi) \geq 1$. Wir zeigen nun, dass es eindeutig bestimmt ist. Ist aber $g(\alpha) = 0$ für ein $g \in K[X]$, so folgt $\mathrm{ev}_\alpha(g) = 0$, also $g \in \ker \mathrm{ev}_\alpha$ und damit $g \in (\varphi)$, i.e. $\varphi \mid g$.

(3) Sei $\beta \in K(\alpha)$ beliebig. Nach (1) existiert $g \in K[X]$ mit $\mathrm{ev}_\alpha(g) = \beta$, d.h. $g(\alpha) = \beta$. Da $K[X]$ bezüglich deg euklidisch ist (Proposition 4.1), existieren $q, r \in K[X]$ mit $g = q\varphi + r$ und $\deg(r) < \deg(\varphi)$. Sei $r = \sum_{i=0}^{m} b_i X^i$ für $b_0, \ldots, b_m \in K$ und $m = \deg(r)$. Dann folgt

$$g(\alpha) = q(\alpha)\,\varphi(\alpha) + r(\alpha) = r(\alpha) = \sum_{i=0}^{m} b_i \alpha^i,$$

sodass $\{1, \alpha, \ldots, \alpha^{n-1}\}$ jedenfalls Erzeugendensystem von $K(\alpha)$ ist. Es verbleibt noch, die lineare Unabhängigkeit zu zeigen. Angenommen, dass $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$ für $\lambda_0, \ldots, \lambda_{n-1} \in K$. Sei $h := \sum_{i=0}^{n-1} \lambda_i X^i$. Dann gilt $h(\alpha) = \sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$ und $\deg(h) < n = \deg(\varphi)$. Nach (2) haben wir aber auch $\varphi \mid h$ und daher muss $h = 0$ sein. Insbesondere folgt, dass $\lambda_0 = \cdots = \lambda_{n-1} = 0$. □

Definition 1.4. Das eindeutig bestimmte irreduzible, monische Polynom $\varphi \in K[X]$ mit $\varphi(\alpha) = 0$ aus Satz 1.1 (2) heißt *Minimalpolynom von α über K*.

Beispiel 1.3. (1) Das Element $\alpha := \sqrt{2}$ ist, wie bereits festgestellt, über $\mathbb{Q}$ algebraisch und hat Minimalpolynom $X^2 - 2$. Aber α ist (trivialerweise) auch algebraisch über $\mathbb{R}$ mit Minimalpolynom $X - \sqrt{2}$. Der Körper, über den wir α betrachten, spielt also eine wesentliche Rolle.

(2) Betrachten wir den Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt{2})$ ist offenbar $X^2 - 3$, also $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ wegen Satz 1.1. Aus Satz 1.1 folgt außerdem, dass $\{1, \sqrt{3}\}$ eine Basis von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ über $\mathbb{Q}(\sqrt{2})$ ist. Die Gradregel liefert nun $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Eine Basis von $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$ ist gegeben durch $\{1, \sqrt{2}\}$; ist also $\alpha = \alpha_1 + \alpha_2\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ für $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{2})$, so folgt durch Substitution von $\alpha_1 = a_1 + b_1\sqrt{2}$ und $\alpha_2 = a_2 + b_2\sqrt{2}$, $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, dass

$$\alpha = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\sqrt{3} = a_1 + b_1\sqrt{2} + a_2\sqrt{3} + b_2\sqrt{6}.$$

Da $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ eine vier-elementige Menge ist, folgt dass dies bereits eine Basis von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ über den rationalen Zahlen ist.

Folgerung 1.2. Ist $L\colon K$ eine Körpererweiterung und sind $\alpha_1, \ldots, \alpha_n \in L$ algebraische Elemente, so ist $K(\alpha_1, \ldots, \alpha_n)$ eine endliche Erweiterung von K mit $K[\alpha_1, \ldots, \alpha_n] = K(\alpha_1, \ldots, \alpha_n)$.

Beispiel 1.4. Es sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist $\sqrt[n]{p}$ als Nullstelle des Polynoms $\varphi := X^n - p \in \mathbb{Q}[X]$ algebraisch über $\mathbb{Q}$ und folglich ist $\mathbb{Q}[\sqrt[n]{p}]$ eine endliche Körpererweiterung von $\mathbb{Q}$. Aus dem Kriterium von Eisenstein folgt, dass φ irreduzibel ist (cf. Beispiel 7.6) und ist als normiertes Polynom demnach schon das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$. Es folgt, dass $[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = \deg(\varphi) = n$. Insbesondere ist nach der Gradregel (Lemma 1.1) die Erweiterung $\mathbb{R}\colon\mathbb{Q}$ unendlich.

Auch die Umkehrung von Satz 1.1 gilt:

Proposition 1.2. Es sei $L\colon K$ eine endliche Körpererweiterung des Körpers K. Dann ist L algebraisch über K und $L = K(\alpha_1, \ldots, \alpha_n)$ für $\alpha_1, \ldots, \alpha_n \in L$.

Beweis. Sei $n := [L\colon K]$ eine positive ganze Zahl und sei $\alpha \in L$ beliebig. Dann sind die $n+1$ Elemente $1, \alpha, \ldots, \alpha^n$ linear abhängig über K, sodass es $\lambda_0, \ldots, \lambda_n \in K$ gibt, die nicht alle Null sind, mit $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$. Daraus folgt aber unmittelbar, dass α Nullstelle des Polynoms $g := \sum_{i=0}^{n} \lambda_i X^i \in K[X] \setminus \{0\}$ ist. Weil α beliebig gewählt worden ist, folgt, dass $L\colon K$ algebraisch ist. Sei nun $\alpha_1, \ldots, \alpha_n \in L$ eine Basis von L als Vektorraum über K; dann gilt $L = K(\alpha_1, \ldots, \alpha_n)$. In der Tat, per Definition gilt $K(\alpha_1, \ldots, \alpha_n) \subseteq L$ und ist $\alpha \in L$ beliebig, so ist wegen der Abgeschlossenheit von $K(\alpha_1, \ldots, \alpha_n)$ unter Addition und (Skalar-)Multiplikation auch die Linearkombination von $\alpha_1, \ldots, \alpha_n$, die α beschreibt, in $K(\alpha_1, \ldots, \alpha_n)$. □

Beispiel 1.5. (1) Die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})\colon\mathbb{Q}$ ist algebraisch.

(2) Da $\mathrm{e}^{\pi\sqrt{-1}/n}$ für $n \in \mathbb{N}$ eine Nullstelle des Polynoms $X^{2n} - 1$ ist, folgt, dass $\mathbb{Q}(\mathrm{e}^{\pi\sqrt{-1}/n})$ endlich ist und damit sogar algebraisch. Insbesondere sehen wir, dass

$$\cos\Big(\frac{\pi}{n}\Big) = \frac{1}{2}\,(\mathrm{e}^{\pi\sqrt{-1}/n} + \mathrm{e}^{-\pi\sqrt{-1}/n}) \in \mathbb{Q}(\mathrm{e}^{\pi\sqrt{-1}/n})$$

und also auch algebraisch über $\mathbb{Q}$ ist.

(3) Wir haben bereits gesehen, dass sowohl π, als auch e transzendent (über $\mathbb{Q}$) sind. Gilt das auch für $\pi + \mathrm{e}$ und $\pi \cdot \mathrm{e}$? Die Antwort ist unbekannt, aber wir können feststellen, dass *mindestens eine* dieser Zahlen transzendent über $\mathbb{Q}$ sein muss. Wären beide Zahlen $\pi + \mathrm{e}, \pi \cdot \mathrm{e}$ algebraisch über $\mathbb{Q}$, so wäre $\mathbb{Q}(\pi \cdot \mathrm{e}, \pi + \mathrm{e})$ eine endliche Körpererweiterung von $\mathbb{Q}$ und daher algebraisch. Insbesondere ist dann $(\pi - \mathrm{e})^2 = (\pi + \mathrm{e})^2 - 4\,(\pi \cdot \mathrm{e})$ algebraisch über $\mathbb{Q}$ und folglich auch $\pi - \mathrm{e}$. Daraus ergibt sich dann aber der Widerspruch, dass π algebraisch über $\mathbb{Q}$ ist.

(4) Sei $\zeta_p := \mathrm{e}^{2\pi\sqrt{-1}/p}$ für eine Primzahl $p \in \mathbb{P}$ die *p-te primitive Einheitswurzel*. Dann ist ζ_p Nullstelle des rationalen Polynoms $X^p - 1$ und damit algebraisch über $\mathbb{Q}$. Da $X^p - 1 = (X - 1) \cdot \Phi_p$ und $\zeta_p \neq 1$ für das zyklotomische Polynom Φ_p aus Beispiel 7.6 gilt, folgt, dass Φ_p sogar das Minimalpolynom von ζ_p über $\mathbb{Q}$ ist. Aus Satz 1.1 folgt also

$$\mathbb{Q}(\zeta_p) = \bigoplus_{k=0}^{p-2} \mathbb{Q}\,\zeta_p^k$$

(mit der Notation aus Definition 6.3) und ferner

$$\mathbb{Q}[X]\,/\,(\Phi_p) \cong \mathbb{Q}(\zeta_p)$$

mit $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$, was die Bezeichnung „*Kreisteilungskörper vom Grad* $p-1$“ rechtfertigt.

(5) Sei $d \in \mathbb{Z} \setminus \{0,1\}$ eine quadratfreie ganze Zahl. Dann ist ω_d algebraisch, $\mathbb{Q}(\omega_d)$ also eine algebraische Körpererweiterung von $\mathbb{Q}$ und $\mathbb{Q}[X]/(\varphi) \cong \mathbb{Q}(\omega_d)$ für das Minimalpolynom φ von ω_d. Doch wir haben gesehen (Diskussion vor Definition 6.1), dass p_d das Minimalpolynom von ω_d in $\mathbb{Q}$ ist, also erhalten wir die bekannte Beziehung $\mathbb{Q}[X]/(p_d) \cong \mathbb{Q}(\omega_d) = \mathbb{Q}(\sqrt{d})$[1.3].

Der Begriff der algebraischen Körpererweiterung ist „transitiv“:

Lemma 1.2. Seien $K \subseteq M \subseteq L$ Körpererweiterungen. Ist $\alpha \in L$ algebraisch über M und ist $M:K$ algebraisch, so ist auch α algebraisch über K. Insbesondere ist die Erweiterung $L:K$ genau dann algebraisch, wenn $L:M$ und $M:K$ algebraisch sind.

Beweis. Sei $\varphi = \sum_{i=0}^{n} a_i X^i$ das Minimalpolynom von α über M. Dann ist α über dem Teilkörper $K(a_0,\dots,a_n)$ von M algebraisch, sodass $[K(a_0,\dots,a_n,\alpha):K(a_0,\dots,a_n)] < \infty$ nach Satz 1.1. Nach Folgerung 1.2 ist auch $[K(a_0,\dots,a_n):K] < \infty$, wegen Lemma 1.1 also insbesondere $[K(a_0,\dots,a_n,\alpha):K] < \infty$. Wegen Proposition 1.2 ist $K(a_0,\dots,a_n,\alpha)$ algebraisch über K, insbesondere also α algebraisch über K. □

In Definition 5.2 haben wir die algebraische Abgeschlossenheit definiert. Wir wollen diesen Begriff nun weiter ausführen.

Definition 1.5. (1) Es sei $K:\mathbb{Q}$ eine endliche Körpererweiterung. Dann heißt K *(algebraischer)*[1.4] *Zahlkörper*.

(2) Es sei K ein Körper, $K':K$ eine algebraisch abgeschlossene Körpererweiterung und $\Xi := \{\alpha \in K' \mid \alpha \text{ alg. über } K\}$. Dann heißt $\bar{K} := K(\Xi)$ der *algebraische Abschluss von* K *in* K'.

Ist $K = \mathbb{Q}$ und $K' = \mathbb{C}$, so nennt man $\bar{\mathbb{Q}}$ schlicht den Körper der *algebraischen Zahlen* und $\alpha \in \mathbb{C}$ *algebraisch*, wenn es algebraisch über $\mathbb{Q}$ ist. Ansonsten nennt man α *transzendent*.

Die Bezeichnung „algebraischer Abschluss“ ist angebracht:

Lemma 1.3. Sei K ein Körper, $K':K$ eine algebraisch abgeschlossene Körpererweiterung. Dann gilt:

(1) Ist $\Xi := \{\alpha \in K' \mid \alpha \text{ alg. über } K\}$, so gilt $\bar{K} = \Xi$.

(2) $\bar{K}$ ist algebraisch über K.

(3) $\bar{K}$ ist algebraisch abgeschlossen.

Beweis. (1) Per Definition gilt $\Xi \subseteq \bar{K}$. Seien umgekehrt $\alpha, \beta \in \Xi$; wenn wir zeigen können, dass auch $\alpha+\beta, \alpha\cdot\beta, \alpha^{-1}$ in Ξ liegen, i.e. Ξ ein Körper ist, so folgt aus der Minimalität von $K(\Xi)$ unmittelbar, dass $K(\Xi) \subseteq \Xi$. In der Tat, $K(\alpha,\beta)$ ist nach Proposition 1.2 eine endliche Körpererweiterung, daher algebraisch und somit sind auch $\alpha+\beta, \alpha\cdot\beta$ und α^{-1} algebraisch über K.

(2) Das folgt unmittelbar aus (1).

(3) Sei $f \in \bar{K}[X]$ ein beliebiges nichtkonstantes Polynom. Da $\bar{K} \subseteq K'$, hat f eine Nullstelle $\alpha \in K'$ und α ist algebraisch über $\bar{K}$. Da $\bar{K}$ algebraisch über K ist, nach (2), folgt aus Lemma 1.2, dass α algebraisch über K ist, also $\alpha \in \Xi$. Aber wegen (1) gilt $\bar{K} = \Xi$, also hat f eine Nullstelle in $\bar{K}$. □

1.3. Für $d = -3$ erhalten wir sogar, da $2\zeta_3 + 1 = \sqrt{-3}$, dass $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$.

1.4. Da seine Elemente nach Proposition 1.2 alle algebraisch sind.

Beispiel 1.6. (1) Es gilt $\mathbb{Q} \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$. Ersetzen wir in Beispiel 1.4 „$\mathbb{R}$“ durch „$\bar{\mathbb{Q}}$“, so sehen wir, dass $\bar{\mathbb{Q}} : \mathbb{Q}$ eine unendliche Körpererweiterung von $\mathbb{Q}$ ist. Die Umkehrung von Proposition 1.2 gilt also nicht: Es existieren algebraische Körpererweiterungen, die unendlich sind.

(2) Sind $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ algebraisch, dann ist $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ ein algebraischer Zahlkörper mit $\mathbb{Q} \subseteq K \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$. Es gilt unter Anwendung von Lemma 1.2, dass $\bar{K} = \bar{\mathbb{Q}}$. Da $K : \mathbb{Q}$ endlich ist, folgt, dass der algebraische Abschluss endlicher Körpererweiterungen nicht unbedingt endlich sein muss. (Offenbar ist diese Beispiel nicht das einfachste.)

(3) Mit Hilfe des Auswahlaxioms kann man zeigen, dass jeder Körper K einen algebraischen Abschluss besitzt, d.h. es existiert ein kleinster Körper $\bar{K}$, der K enthält und algebraisch abgeschlossen ist.

(4) Ist $K' : K$ algebraisch abgeschlossen, so können wir im Allgemeinen nicht folgern, dass K' algebraisch über K ist, sei beispielsweise $K' = \mathbb{C}$ und $K = \mathbb{Q}$.

Viele der Begriffe, die wir in diesem Abschnitt eingeführt haben, sind Verallgemeinerungen von Konzepten, die uns schon im Studium der quadratischen Zahlkörper begegnet sind. In Proposition 6.3 haben wir gezeigt, dass $\mathcal{O}_d$ der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ ist. Gibt es auch ein Analogon davon in allgemeinen Zahlkörpern? Dazu ein kurzer Überblick; eine tiefgehendere Untersuchung dieser Objekte ist vor allem Gegenstand der algebraischen Zahlentheorie.

Definition 1.6. Es sei K ein algebraischer Zahlkörper. Dann heißt

$$\mathcal{O}_K := \{\alpha \in K \mid \exists f \in \mathbb{Z}[X] : \text{monisch},\ f(\alpha) = 0\}$$

der *ganze Abschluss* (oder *Ganzabschluss*) *von* $\mathbb{Z}$ *in* K.

Man kann zeigen:

Satz 1.2. Sei K ein algebraischer Zahlkörper. Dann ist $\mathcal{O}_K$ ein noetherscher Ring und heißt *Ring der ganzen Zahlen von* K.

Zum Abschluss noch einige interessante Resultate über $\mathcal{O}_K$, die auch den nächsten Abschnitt motivieren.

Satz 1.3. (Weinberger) Unter der Annahme der Verallgemeinerten Riemann'schen Vermutung gilt: Enthält $\mathcal{O}_K$ unendlich viele Einheiten, dann ist $\mathcal{O}_K$ genau dann euklidisch, wenn es ein HIR ist.

Ebenso kann man zeigen, dass $\mathcal{O}_K^*$ nur für $K = \mathbb{Q}$ und $K = \mathbb{Q}(\sqrt{d})$ für $d < 0$, quadratfrei, endlich ist. Das bedeutet, dass die Beispiele für Hauptidealringe, die nicht euklidisch sind, unter *allen* $\mathcal{O}_K$ genau $\mathcal{O}_{-19}, \mathcal{O}_{-43}, \mathcal{O}_{-67}$ und $\mathcal{O}_{-163}$ sind. Allerdings ist das unter der Annahme der Riemann'schen Vermutung. Was weiß man ohne Annahme dieser?

Satz 1.4. (Dirichlet'scher Einheitensatz) Sei K ein algebraischer Zahlkörper. Dann gilt

$$\mathcal{O}_K^* \cong \{\alpha \in K \mid \exists k \in \mathbb{N} : \alpha^k = 1\} \times \mathbb{Z}^\nu$$

für ein $\nu \geq 0$.

Beweis. Ein zugänglicher Beweis ist in [Mar18] zu finden. □

Das bedeutet insbesondere, dass $\mathcal{O}_K^*$ genau dann unendlich ist, wenn der Exponent ν größer als Null ist. Das führt uns zu folgendem Ergebnis:

Satz 1.5. (Murty, Harper) Ist $\nu \geq 4$ und ist K eine Galoiserweiterung der rationalen Zahlen, so ist der Ring $\mathcal{O}_K$ genau dann euklidisch, wenn er ein Hauptidealring ist.

2 Galoistheorie

Abgesehen davon, dass wir nicht über die notwendigen Mittel verfügen, diese Sätze rigoros zu beweisen, bleiben noch zwei Fragen offen: Was ist eine Galoiserweiterung? Wie ist die Isomorphie im Dirichlet'schen Einheitensatz zu verstehen? Folgendes Lemma ebnet den Weg zur Klärung dieser Fragen.

Lemma 2.1. Es seien $L\colon K$ und $F\colon K$ Körpererweiterungen und $\sigma\colon F \to L$ ein Körperhomomorphismus. Dann ist σ genau dann K-linear, wenn $\sigma(k) = k$ für alle $k \in K$.

Beweis. Es sei σ zunächst K-linear. Dann ist $\sigma(k) = \sigma(k \cdot 1) = k \cdot \sigma(1) = k$ für beliebiges $k \in K$. Umgekehrt, falls $\sigma(k) = k$ für alle $k \in K$ gilt, so seien $k, k' \in K$ sowie $u, v \in F$ beliebig. Dann gilt

$$\sigma(ku + k'v) = \sigma(k)\,\sigma(u) + \sigma(k')\,\sigma(v) = k\sigma(u) + k'\sigma(v),$$

also ist σ auch K-linear. □

Definition 2.1. Es seien $L\colon K$ und $F\colon K$ Körpererweiterungen und $\sigma\colon F \to L$ ein Körperhomomorphismus, der die äquivalenten Bedingungen aus Lemma 2.1 erfüllt. Dann heißt σ ein *K-Homomorphismus von F nach L*. Ist $F = L$ und σ sogar ein Isomorphismus, so nennen wir σ einen *K-Automorphismus von L*.

Wir schreiben

$$\mathrm{Gal}(L/K) := \{\sigma\colon L \xrightarrow{\sim} L \mid K\text{-Automorphismus}\}$$

für die Menge aller K-Automorphismen von L und nennen diese Menge die *Galois-Gruppe*[2.1] der Körpererweiterung $L\colon K$.

Beispiel 2.1. (1) Wir berechnen die Galois-Gruppe von $\mathbb{C}\colon\mathbb{R}$. Sei $\sigma\colon\mathbb{C}\to\mathbb{C}$ ein beliebiger $\mathbb{R}$-Automorphismus der komplexen Zahlen. Dann gilt für eine komplexe Zahl $a + b\sqrt{-1}$, $a, b \in \mathbb{R}$,

$$\sigma(a + b\sqrt{-1}) = \sigma(a) + \sigma(b)\,\sigma(\sqrt{-1}) = a + b\sigma(\sqrt{-1}).$$

Da $\sigma(\sqrt{-1})^2 = -1$ erfüllen muss, haben wir die zwei Möglichkeiten $\sigma(\sqrt{-1}) = \sqrt{-1}$ und $\sigma(\sqrt{-1}) = -\sqrt{-1}$. Das heißt die Galois-Gruppe von $\mathbb{C}\colon\mathbb{R}$ hat zwei Elemente: Die Identitäts- und Konjugationsabbildungen.

(2) In Beispiel 1.3 haben wir die Basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ von $\mathbb{Q}(\sqrt{2}, \sqrt{3})\colon\mathbb{Q}$ bestimmt; was ist die Galois-Gruppe dieser Körpererweiterung? Sei $\sigma\colon\mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ein $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dann gilt für ein beliebiges Element $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ aus diesem Körper

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sigma(\sqrt{2}) + c\sigma(\sqrt{3}) + d\sigma(\sqrt{6}).$$

Die Einschränkung $\sigma(\sqrt{2})^2 = 2, \sigma(\sqrt{3})^2 = 3, \sigma(\sqrt{6})^2 = 6$ liefert uns nun vier Möglichkeiten, i.e.

$$\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{3}) = \pm\sqrt{3},$$

wobei $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\,\sigma(\sqrt{3})$ bereits durch die Wahl von $\sigma(\sqrt{2})$ und $\sigma(\sqrt{3})$ festgelegt ist.

2.1. Évariste Galois (1811 – 1832), französischer Mathematiker

(3) Wir zeigen, dass die Galoisgruppe von $\mathbb{R}:\mathbb{Q}$ trivial ist. Sei $\sigma:\mathbb{R}\to\mathbb{R}$ ein $\mathbb{Q}$-Automorphismus. Falls $x>0$, so gilt $\sigma(x)=\sigma((\sqrt{x})^2)=\sigma(\sqrt{x})^2>0$. Falls also $x,y\in\mathbb{R}$ mit $x<y$, so gilt $\sigma(y)-\sigma(x)=\sigma(y-x)>0$, d.h. $\sigma(x)<\sigma(y)$.

Sei nun $x\in\mathbb{R}$ beliebig; wir wollen zeigen, dass $\sigma(x)=x$. Offenbar gilt das, wenn $x\in\mathbb{Q}$; sei also $x\notin\mathbb{Q}$. Dann können wir eine Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ finden, sodass $x_n\to x$ und $x_n<x$ für alle $n\geq 1$. Ähnlich finden wir eine Folge $(y_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$, sodass $y_n\to x$ und $y_n>x$ für alle $n\geq 1$. Es folgt, dass $x_n<x<y_n$ für alle $n\geq 1$, insbesondere $x_n=\sigma(x_n)<\sigma(x)<\sigma(y_n)=y_n$, sodass aus der Eindeutigkeit von Grenzwerten folgt, $\sigma(x)=x$.

Lemma 2.2. Es sei $L:K$ eine Körpererweiterung. Dann ist $\mathrm{Gal}(L/K)$ eine Gruppe bezüglich der Zusammensetzung von Abbildungen. Insbesondere gilt $\mathrm{Gal}(L/K)\leq S(L)$.

Beweis. Seien $\sigma_1,\sigma_2:L\xrightarrow{\sim}L$ zwei K-Automorphismen. Wir müssen zeigen, dass $\sigma_1\circ\sigma_2\in\mathrm{Gal}(L/K)$ und $\sigma_1^{-1}\in\mathrm{Gal}(L/K)$. Seien $u_1,u_2\in L$; dann existieren $v_1,v_2\in L$ mit $\sigma_1(v_1)=u_1$ und $\sigma_1(v_2)=u_2$. Daraus folgt

$$\sigma_1^{-1}(u_1+u_2)=\sigma_1^{-1}(\sigma_1(v_1)+\sigma_1(v_2))=\sigma_1^{-1}(\sigma_1(v_1+v_2))=v_1+v_2=\sigma_1^{-1}(u_1)+\sigma_1^{-1}(u_2)$$

und ähnlich $\sigma_1^{-1}(u_1\cdot u_2)=\sigma_1^{-1}(u_1)\cdot\sigma_1^{-1}(u_2)$. Ferner gilt $\sigma_1^{-1}(k)=\sigma_1^{-1}(\sigma_1(k))=k$ für alle $k\in K$, also tatsächlich $\sigma_1^{-1}\in\mathrm{Gal}(L/K)$. Außerdem sehen wir

$$\begin{aligned}(\sigma_1\circ\sigma_2)(u_1+u_2)&=\sigma_1(\sigma_2(u_1+u_2))=\sigma_1(\sigma_2(u_1)+\sigma_2(u_2))\\&=\sigma_1(\sigma_2(u_1))+\sigma_1(\sigma_2(u_2))\\&=(\sigma_1\circ\sigma_2)(u_1)+(\sigma_1\circ\sigma_2)(u_2)\end{aligned}$$

und $(\sigma_1\circ\sigma_2)(k)=\sigma_1(\sigma_2(k))=\sigma_1(k)=k$. Ähnlich zeigt man, dass $\sigma_1\circ\sigma_2$ mit der Multiplikation veträglich ist. Da die Identitätsabbildung auf L offenbar ein K-Automorphismus ist, folgt, dass $\mathrm{Gal}(L/K)$ eine Untergruppe von $S(L)$, der Bijektionen auf L, ist (siehe auch Beispiel 2.1 (4)). □

Lemma 2.3. Es sei $K\subseteq M\subseteq L$ eine Körpererweiterung mit Zwischenkörper M und $H\leq\mathrm{Gal}(L/K)$ eine Untergruppe. Dann gilt:

(1) $L^H:=\{\ell\in L\mid\forall\sigma\in H:\sigma(\ell)=\ell\}$ ist ein Zwischenkörper von $K\subseteq L$, genannt der *Fixkörper von H in L*.

(2) $\mathrm{Gal}(L/M)$ ist eine Untergruppe von $\mathrm{Gal}(L/K)$.

Beweis. (1) Seien $\ell_1,\ell_2\in L^H$ und $\sigma\in H$ beliebig. Dann gilt

$$\sigma(\ell_1-\ell_2)=\sigma(\ell_1)-\sigma(\ell_2)=\ell_1-\ell_2,\quad\sigma(\ell_1\cdot\ell_2^{-1})=\sigma(\ell_1)\cdot\sigma(\ell_2^{-1})=\ell_1\cdot\ell_2^{-1}$$

also handelt es sich tatsächlich um einen Teilkörper von L. Da $\sigma(k)=k$ für alle $k\in K$ per Definition von H folgt insbesondere $K\subseteq L^H\subseteq L$.

(2) Nach Lemma 2.2 ist $\mathrm{Gal}(L/M)$ tatsächlich eine Gruppe. Wir müssen also nur zeigen, dass $\mathrm{Gal}(L/M)\subseteq\mathrm{Gal}(L/K)$. Aber ist $\sigma\in\mathrm{Gal}(L/M)$ und $k\in K$ beliebig, so folgt $k\in M$ und daher $\sigma(k)=k$, da σ ein M-Automorphismus ist. □

Definition 2.2. Es sei $L:K$ eine Körpererweiterung. Ist $K=L^{\mathrm{Gal}(L/K)}$, dann heißt $L:K$ eine *Galoiserweiterung* bzw. *galoissch*.

Beispiel 2.2. (1) Sei $L:K$ eine Körpererweiterung und $K_0:=L^{\mathrm{Gal}(L/K)}$. Dann ist $K\subseteq K_0$ und $L:K_0$ eine Galoiserweiterung mit $\mathrm{Gal}(L/K_0)=\mathrm{Gal}(L/K)$.

(2) Für $d \in \mathbb{Z} \setminus \{0,1\}$ ist $\mathbb{Q}(\sqrt{d}) : \mathbb{Q}$ eine Galoiserweiterung. In der Tat, offenbar fixiert jeder $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\sqrt{d})$ die rationalen Zahlen während die Konjugationsabbildung ein Automorphismus ist, der alle anderen Elemente „bewegt“. Insbesondere erhalten wir so unendlich viele Galoiserweiterungen von $\mathbb{Q}$.

(3) Aus Beispiel 2.1 (1) folgt, dass $\mathbb{C} : \mathbb{R}$ galoissch ist.

(4) Sei K ein unendlicher Körper sodass $1 + 1 + \cdots + 1 \neq 0$ (formal, $\operatorname{char}(K) = 0$). Dann ist $K(X) : K$ eine Galoiserweiterung; beispielsweise induziert die Substitution $X \mapsto X + 1$ einen K-Automorphismus von $K(X)$ mit Fixkörper K, da K per Annahme unendlich ist. Insbesondere folgt, dass $K(X_1, \ldots, X_n) : K$ eine Galoiserweiterung ist.

Die Signifikanz von Galoiserweiterungen ist auf folgendes Resultat, genannt der „*Hauptsatz der Galoistheorie*“ zurückzuführen:

Satz 2.1. (Hauptsatz der Galoistheorie) Es sei $L : K$ eine endliche Galoiserweiterung. Dann gibt es eine Bijektion zwischen der Menge der Zwischenkörper von $K \subseteq L$ und der Menge der Untergruppen von $\operatorname{Gal}(L/K)$, gegeben durch

$$\begin{aligned} \{M \mid K \subseteq M \subseteq L \text{ Zwischenkörper}\} &\to \{H \mid H \leq \operatorname{Gal}(L/K) \text{ Untergruppe}\} \\ M &\mapsto \operatorname{Gal}(L/M) \end{aligned}$$

mit inverser Abbildung

$$L^H \hookleftarrow H.$$

Beweis. Siehe [Mil22], Satz 3.17. □

Beispiel 2.3. Wir wollen alle Zwischenkörper von $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$ bestimmen. Das Minimalpolynom von $\sqrt[3]{2}$ über dem Körper $\mathbb{Q}(\zeta_3)$ ist

$$X^3 - 2 = \big(X - \sqrt[3]{2}\big)\big(X - \sqrt[3]{2}\,\zeta_3\big)\big(X - \sqrt[3]{2}\,\zeta_3^2\big),$$

daher $\big[\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}(\zeta_3)\big] = 3$ und

$$\big[\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}\big] = \big[\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}(\zeta_3)\big] \cdot [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 6.$$

Eine Basis von $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$ über $\mathbb{Q}(\zeta_3)$ ist $\big\{1, \sqrt[3]{2}, \sqrt[3]{4}\big\}$ nach Satz 1.1. Weiterhin wissen wir, dass $\{1, \zeta_3\}$ eine Basis von $\mathbb{Q}(\zeta_3)$ über $\mathbb{Q}$ ist. Ist also $\alpha = \alpha_1 + \alpha_2\sqrt[3]{2} + \alpha_3\sqrt[3]{4} \in \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$, so haben wir $\alpha_1 = a_1 + b_1\,\zeta_3, \alpha_2 = a_2 + b_2\,\zeta_3$ und $\alpha_3 = a_3 + b_3\,\zeta_3$ für rationale a_i, b_i, $1 \leq i \leq 3$, sodass

$$\begin{aligned} \alpha &= \alpha_1 + \alpha_2\sqrt[3]{2} + \alpha_3\sqrt[3]{4} \\ &= a_1 + b_1\,\zeta_3 + (a_2 + b_2\,\zeta_3)\sqrt[3]{2} + (a_3 + b_3\,\zeta_3)\sqrt[3]{4} \\ &= a_1 + b_1\,\zeta_3 + a_2\sqrt[3]{2} + b_2\,\zeta_3\sqrt[3]{2} + a_3\sqrt[3]{4} + b_3\,\zeta_3\sqrt[3]{4}, \end{aligned}$$

i.e. $\big\{1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \zeta_3\sqrt[3]{2}, \zeta_3\sqrt[3]{4}\big\}$ ist Erzeugendensystem von $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$ als Vektorraum über $\mathbb{Q}$ und sogar Basis.

Wir berechnen nun die Galoisgruppe von $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}$. Sei $\sigma : \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) \to \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$ ein beliebiger $\mathbb{Q}$-Automorphismus von $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$. Mit α wie vorher, erhalten wir dann

$$\begin{aligned} \sigma\big(a_1 + b_1\,\zeta_3 + a_2\sqrt[3]{2} + b_2\,\zeta_3\sqrt[3]{2} + a_3\sqrt[3]{4} + b_3\,\zeta_3\sqrt[3]{4}\big) = a_1 + b_1\,\sigma(\zeta_3) + a_2\,\sigma\big(\sqrt[3]{2}\big) + b_2\,\sigma\big(\zeta_3\sqrt[3]{2}\big) \\ + a_3\,\sigma\big(\sqrt[3]{4}\big) + b_3\,\sigma\big(\zeta_3\sqrt[3]{4}\big), \end{aligned}$$

wobei wir $\sigma(\zeta_3)^3 = 1, \sigma\big(\sqrt[3]{2}\big)^3 = 2$ fordern (und bemerken, dass $\sigma\big(\sqrt[3]{4}\big)$ und $\sigma\big(\zeta_3\sqrt[3]{2}\big)$ damit automatisch bestimmt sind). Das liefert die Möglichkeiten

$$\sigma(\zeta_3) = \zeta_3, \quad \sigma(\zeta_3) = \zeta_3^2, \quad \sigma\big(\sqrt[3]{2}\big) = \sqrt[3]{2}, \quad \sigma\big(\sqrt[3]{2}\big) = \zeta_3\sqrt[3]{2}, \quad \sigma\big(\sqrt[3]{2}\big) = \zeta_3^2\sqrt[3]{2}.$$

Die Galoisgruppe von $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}$ hat also die sechs Elemente

$$\begin{aligned}
\sigma_1(\zeta_3) &= \zeta_3, & \sigma_1\big(\sqrt[3]{2}\big) &= \sqrt[3]{2},\\
\sigma_2(\zeta_3) &= \zeta_3^2, & \sigma_2\big(\sqrt[3]{2}\big) &= \sqrt[3]{2},\\
\sigma_3(\zeta_3) &= \zeta_3, & \sigma_3\big(\sqrt[3]{2}\big) &= \zeta_3\sqrt[3]{2},\\
\sigma_4(\zeta_3) &= \zeta_3^2, & \sigma_4\big(\sqrt[3]{2}\big) &= \zeta_3\sqrt[3]{2},\\
\sigma_5(\zeta_3) &= \zeta_3, & \sigma_5\big(\sqrt[3]{2}\big) &= \zeta_3^2\sqrt[3]{2},\\
\sigma_6(\zeta_3) &= \zeta_3^2, & \sigma_6\big(\sqrt[3]{2}\big) &= \zeta_3^2\sqrt[3]{2}.
\end{aligned}$$

Nach dem Fundamentalsatz der Galoistheorie, entspricht jede Untergruppe dieser sechselementigen Gruppe einem Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$, wobei $K = \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)^H$ für eine Untergruppe $H \leq \mathrm{Gal}\big(\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)/\mathbb{Q}\big)$. Also müssen wir die Untergruppen von $\mathrm{Gal}\big(\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)/\mathbb{Q}\big)$ bestimmen. Hier machen wir zwei Vorgriffe in die Gruppentheorie: Nach dem Satz von Lagrange (Proposition 1.2) haben die Untergruppen von $\mathrm{Gal}\big(\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)/\mathbb{Q}\big)$ entweder 2 oder 3 Elemente und diese sind nach Korollar 1.4 alle zyklisch. Somit erhalten wir die Untergruppen

$$\{\sigma_1\}, \quad \{\sigma_1, \sigma_2\}, \quad \{\sigma_1, \sigma_3, \sigma_5\}, \quad \{\sigma_1, \sigma_4\}, \quad \{\sigma_1, \sigma_6\}, \quad \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}.$$

Diese entsprechen genau den Zwischenkörpern (der Reihenfolge nach)

$$\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big), \mathbb{Q}\big(\sqrt[3]{2}\big), \mathbb{Q}(\zeta_3), \mathbb{Q}\big(\zeta_3^2\sqrt[3]{2}\big), \mathbb{Q}\big(\zeta_3\sqrt[3]{2}\big), \mathbb{Q}.$$

Konsequenz des Hauptsatzes ist unter anderem folgender Satz:

Satz 2.2. Jede endliche Gruppe G kann mit der Galoisgruppe einer Körpererweiterung $L : K$ identifiziert werden.

Um ihn zu beweisen, werden wir uns erlauben einen Augenblick in die Gruppentheorie, die ausführlich im nächsten Kapitel behandelt wird, vorzugreifen. Es handelt sich um den bekannten *Satz von Cayley*[2.2].

Lemma 2.4. (Cayley) Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$. Dann existiert eine Menge M und eine Untergruppe $U \leq S(M)$ mit $G \cong U$[2.3].

Beweis. Sei $M := G$. Für $g \in G$ definieren wir die Abbildung $f_g : M \to M$ durch $f_g(x) := g \cdot x$ für alle $x \in M$. Dann gilt

$$f_g \circ f_h = f_{g \cdot h}, \quad f_e = \mathrm{id}_M, \quad f_g \circ f_{g^{-1}} = \mathrm{id}_M$$

und offenbar ist f_g bijektiv. Folglich erhalten wir einen Gruppenhomomorphismus

$$\phi : G \to S(M), \quad \phi(g) := f_g.$$

2.2. Arthur Cayley (1821 – 1895), englischer Mathematiker

2.3. Siehe Definition 1.7 für eine formale Definition der Isomorphie von Gruppen und Gruppenhomomorphismen.

Da aus $f_g = f_h$ für $g, h \in G$ unmittelbar $g = f_g(e) = f_h(e) = h$ folgt, ist ϕ injektiv. Es folgt, dass ϕ ein Isomorphismus zwischen G und $U := \operatorname{im}\phi \leq S(M)$ ist. □

Insbesondere ist jede endliche Gruppe Untergruppe einer symmetrischen Gruppe S_n, $n \in \mathbb{N}$.

Lemma 2.5. Sei $\sigma \in S_n$, F ein beliebiger unendlicher Körper und $L := F(X_1, \ldots, X_n)$ der Körper der rationalen Funktionen über F. Dann ist die Abbildung

$$\tilde{\sigma} : L \to L, \quad \frac{f}{g} \mapsto \tilde{\sigma}\left(\frac{f}{g}\right) := \frac{f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})}{g(X_{\sigma(1)}, \ldots, X_{\sigma(n)})}$$

ein F-Automorphismus von L, i.e. $\tilde{\sigma} \in \operatorname{Gal}(L/F)$.

Beweis. Sei $\alpha = (\alpha_1, \ldots, \alpha_n)$ ein beliebiger Multiindex und $X := (X_1, \ldots, X_n)$. Dann gilt

$$\tilde{\sigma}\left(\sum_\alpha c_\alpha X^\alpha\right) = \sum_\alpha c_\alpha \prod_{i=1}^n X_{\sigma(i)}^{\alpha_i}$$

für $c_\alpha \in F$. Sei nun $f = \sum_\alpha a_\alpha X^\alpha$ und $g = \sum_\alpha b_\alpha X^\alpha$ für $a_\alpha, b_\alpha \in F$, sodass

$$\begin{aligned}\tilde{\sigma}(f+g) &= \tilde{\sigma}\left(\sum_\alpha (a_\alpha + b_\alpha) X^\alpha\right) = \sum_\alpha (a_\alpha + b_\alpha) \prod_{i=1}^n X_{\sigma(i)}^{\alpha_i} \\ &= \sum_\alpha a_\alpha \prod_{i=1}^n X_{\sigma(i)}^{\alpha_i} + \sum_\alpha b_\alpha \prod_{i=1}^n X_{\sigma(i)}^{\alpha_i} \\ &= \tilde{\sigma}(f) + \tilde{\sigma}(g).\end{aligned}$$

Ähnlich zeigt man, dass $\tilde{\sigma}(f \cdot g) = \tilde{\sigma}(f) \cdot \tilde{\sigma}(g)$. Das heißt, $\tilde{\sigma}$ ist ein Homomorphismus auf $F[X_1, \ldots, X_n]$. Nun ist auch $\tilde{\sigma}_{-1}$ ein Homomorphismus auf diesem Ring, wenn man σ durch sein Inverses σ^{-1} ersetzt und es folgt, dass $\tilde{\sigma} \circ \tilde{\sigma}_{-1}$ die Identität auf $F[X_1, \ldots, X_n]$ ist. Als unmittelbare Konsequenz davon ist $\tilde{\sigma}$ ein Körperautomorphismus von L und da $\tilde{\sigma}$ die konstanten Polynome in L offenbar fixiert, gilt insbesondere $\tilde{\sigma} \in \operatorname{Gal}(L/F)$. □

Der Beweis von Satz 2.2 ist nun eine Anwendung dieser Hilfsresultate.

Beweis. Nach dem Satz von Cayley, können wir o. B. d. A. annehmen, dass $G \leq S_n$ für ein $n \in \mathbb{N}$. Betrachten wir die Abbildung

$$\Phi : S_n \to \operatorname{Gal}(L/F), \quad \Phi(\sigma) = \tilde{\sigma}$$

aus Lemma 2.5. Diese Zuweisung ist ein injektiver Gruppenhomomorphismus, denn gilt $\tilde{\sigma} = \tilde{\rho}$ für $\rho, \sigma \in S_n$, so folgt

$$X_{\sigma(i)} = \tilde{\sigma}(X_i) = \tilde{\rho}(X_i) = X_{\rho(i)}$$

für $i = 1, \ldots, n$, d.h. $\sigma = \rho$ und die Homomorphieeigenschaft von Φ folgt unmittelbar. Also können wir G mit $H := \Phi(G) \leq \operatorname{Gal}(L/F)$ identifizieren, d.h. $H \cong G$. Setzen wir nun $K := L^H$, so folgt, dass $L : K$ eine endliche Galoiserweiterung ist (siehe [Lan02], Satz 1.8 für einen Beweis) und $\operatorname{Gal}(L/K) = H \cong G$. Somit haben wir eine Galoiserweiterung $L : K$ mit Galoisgruppe G gefunden. □

Es herrscht also eine gewisse Dualität:

„*Jede endliche Gruppe ist Untergruppe einer symmetrischen Gruppe.*“

„*Jede endliche Gruppe ist Galoisgruppe einer Körpererweiterung.*“

3 Gruppen

Wir beginnen das Kapitel, indem wir Konstruktionen und Definitionen, die wir im Kontext der Ringtheorie bereits gesehen haben, auch für Gruppen einführen. Es wird sich herausstellen, dass diese bei Gruppen in gewisser Art und Weise „simpler“ sind.

1 Untergruppen und Quotientengruppen

Definition 1.1. Es sei G eine Gruppe, $g \in G$. Dann nennen wir die Zahl

$$\operatorname{ord}_G(g) := \operatorname{ord}(g) := |\langle g \rangle|$$

die Ordnung von g.

Lemma 1.1. Es sei G eine Gruppe, $g \in G$. Dann gilt:

(1) $\operatorname{ord}(g)$ ist die Anzahl der Elemente in der von g erzeugten zyklischen Untergruppe $\langle g \rangle$ von G.

(2)

$$\operatorname{ord}(g) = \begin{cases} \min\{n \in \mathbb{N} \mid g^n = e\}, \text{ wenn } g \text{ endlich ist,} \\ \aleph_0, \text{ wenn } \langle g \rangle \text{ unendlich ist.} \end{cases}$$

Beweis. Beide Aussagen sind unmittelbare Konsequenz der Definition von $\operatorname{ord}(g)$. □

Lemma 1.2. Sei G eine Gruppe und $g \in G$ mit $\ell := \operatorname{ord}(g)$. Gilt $g^k = e$ für ein $k \in \mathbb{N}$, so folgt $\ell \mid k$.

Beweis. Es existieren $q, r \in \mathbb{N}_0$ mit $k = \ell q + r$ und $r < \ell$. Dann gilt

$$e = g^k = g^{\ell q + r} = g^{\ell q} g^r = (g^\ell)^q g^r = e^q g^r = g^r$$

und da $\ell \in \mathbb{N}$ per Definition minimal mit $g^\ell = e$ ist, folgt $r = 0$, d.h. $\ell \mid k$. □

Ein Analogon zum direkten Produkt von Ringen:

Definition 1.2. Es sei A eine beliebige nichtleere Indexmenge und $(G_a)_{a \in A}$ eine Familie von Gruppen. Dann ist

$$\prod_{a \in A} G_a = \{(g_a)_{a \in A} \mid g_a \in G_a, a \in A\}$$

eine Gruppe vermöge der Operationen

$$(g_a)_{a \in A} \circ (h_a)_{a \in A} := (g_a \circ h_a)_{a \in A}.$$

Offenbar ist $\prod_{a \in A} G_a$ genau dann abelsch, wenn G_a für alle $a \in A$ abelsch ist. Wir nennen $\prod_{a \in A} G_a$ die *Produktgruppe* oder das *(äußere) direkte Produkt der* G_a.

Beispiel 1.1. Ist $(H_a)_{a \in A}$ eine weitere Familie von Gruppen mit $H_a \leq G_a$ für alle $a \in A$, so folgt $\prod_{a \in A} H_a \leq \prod_{a \in A} G_a$. Die Umkehrung gilt wiederum nicht: Betrachten wir die Untergruppe

$$H := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b \equiv 0 \pmod 2\}$$

von $(\mathbb{Z} \times \mathbb{Z}, +)$. Angenommen $H_1 \times H_2 = H$ für $H_1, H_2 \leq \mathbb{Z}$. Da $(a, a) \in H$ für beliebiges $a \in \mathbb{Z}$, folgt dann insbesondere $H_1 = H_2 = \mathbb{Z}$, aber $(1, 0) \notin H$, also kann $H_1 \times H_2 = H$ nicht sein.

Auch Gruppen können „Ideale“ haben. Zunächst einige Vorbereitungen.

Definition 1.3. Sei G eine Gruppe und $H \leq G$ eine Untergruppe von G. Für jedes Element $g \in G$ nennen wir

$$gH := \{gh \mid h \in H\}$$

die *Linksnebenklasse von g nach H* (oder auch modulo H). Analog definieren wir die Rechtsnebenklasse $Hg := \{hg \mid g \in G\}$.

Proposition 1.1. Seien G eine Gruppe und $H \leq G$ sowie $g_1, g_2 \in G$. Dann bilden die Links- und Rechtsnebenklassen nach H eine Partition von G mit $g_1 H = g_2 H$ (bzw. $Hg_1 = Hg_2$) genau dann, wenn $g_1^{-1} g_2 \in H$ (bzw. $g_1 g_2^{-1} \in H$).

Beweis. Wir zeigen die Aussage für Linksnebenklassen; der Beweis für Rechtsnebenklassen verläuft analog. Die Nebenklassen $g_1 H$ und $g_2 H$ haben genau dann nichtleeren Schnitt, wenn wir $h_1, h_2 \in H$ mit $g_1 h_1 = g_2 h_2$ finden können. Ist $h \in H$ dann beliebig, so folgt

$$g_2 h = g_2 h_2 h_2^{-1} h = g_1 h_1 h_2^{-1} h \in g_1 H,$$

d.h. $g_2 H \subseteq g_1 H$ und ähnlich $g_1 H \subseteq g_2 H$, also $g_1 H = g_2 H$. Da $g \in gH$ für alle $g \in G$ sind die Nebenklassen nichtleer und deren Vereinigung ist ganz G, sodass tatsächlich eine Partition von G vorliegt. Mit der Beobachtung, dass $g_1 H = g_2 H$ genau dann, wenn $g_1^{-1} g_2 \in H$, folgt die Behauptung. □

Ist G nicht abelsch, so müssen Links- und Rechtsnebenklassen nicht übereinstimmen. Man findet aber für endliche wie unendliche Gruppen zumindest eine Bijektion.

Lemma 1.3. Sei G eine Gruppe und $H \leq G$. Dann gibt es eine Bijektion zwischen der Menge der Links- und Rechtsnebenklassen von G modulo H.

Beweis. Sei

$$\phi \colon \{gH \mid g \in G\} \to \{Hg \mid g \in G\}, \quad \phi(gH) := Hg^{-1}.$$

Diese Abbildung ist wohldefiniert. In der Tat, sind $g_1, g_2 \in G$ mit $g_1 H = g_2 H$, so gibt es $h_1, h_2 \in H$ mit $g_1 h_1 = g_2 h_2$, also $g_1 = g_2 h_2 h_1^{-1}$. Ist also $h g_1^{-1} \in H g_1^{-1}$ für ein $h \in H$, so folgt

$$h g_1^{-1} = h\,(g_2 h_2 h_1^{-1})^{-1} = h h_1 h_2^{-1} g_2^{-1} \in H g_2^{-1},$$

also $H g_1^{-1} \subseteq H g_2^{-1}$, sodass $\phi(g_1 H) = \phi(g_2 H)$. Ebenso ist ϕ injektiv. Gilt nämlich $\phi(g_1 H) = \phi(g_2 H)$, erneut für unbestimmte $g_1, g_2 \in H$, so folgt $g_1 H = g_2 H$ und ähnlich zeigt man, dass ϕ auch surjektiv ist. □

Das motiviert die folgende Definition.

Definition 1.4. Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann nennt man die Kardinalität der Menge aller Linksnebenklassen (oder, äquivalent, aller Rechtsnebenklassen) den *Index von H in G*. Man schreibt dafür dann $[G \colon H]$.

Proposition 1.2. (Lagrange) Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gibt es eine Bijektion $\varphi \colon H \times \{gH \mid g \in G\} \to G$, i.e.

$$|G| = |H| \cdot [G \colon H].$$

Wenn G endlich ist, gilt insbesondere $[G \colon H] = \frac{|G|}{|H|}$.

Beweis. Wir wählen für jede Linksnebenklasse gH, $g \in G$, ein fixiertes Element $r \in G$ aus und bezeichnen die Menge dieser Vertreter mit R, d.h. $\{gH \mid g \in G\} = \{rH \mid r \in R\}$ und $rH \neq r'H$ für alle verschiedenen $r, r' \in R$.

Sei nun

$$\varphi: H \times \{gH \mid g \in G\} \to G, \quad \varphi(h, gH) := r \circ h,$$

wobei r der zugehörige Vertreter der Nebenklasse gH ist. Diese Abbildung ist dann offenbar wohldefiniert. Gilt $\varphi(h_1, r_1) = \varphi(h_2, r_2)$ so folgt durch Umformung, dass $r_2^{-1} \circ r_1 \in H$, also $r_1 H = r_2 H$ bzw. $r_1 = r_2$ und $h_1 = h_2$, per Konstruktion unseres Vertretersystems. Wählen wir einen fixen Repräsentanten $r \in R$, so gilt auch $\varphi(r^{-1} g, rH) = r \circ (r^{-1} g) = g$ für beliebiges $g \in G$. □

Im endlichen Fall ist das obige Resultat auch als *Satz von Lagrange*[1.1] bekannt.

Ähnlich zur Gradregel bei Körpererweiterungen haben wir für Gruppenindizes den sogenannten *Indexsatz*. Er ist unmittelbare Konsequenz von Proposition 1.2.

Folgerung 1.1. (Indexsatz) Es seien $G \subseteq G' \subseteq G''$ drei endliche Gruppen. Dann gilt

$$[G'' : G] = [G'' : G'] \cdot [G' : G].$$

Beweis. Wir haben einerseits $[G'' : G'] = \frac{|G''|}{|G'|}$ und andererseits $[G' : G] = \frac{|G'|}{|G|}$, also

$$[G'' : G] = \frac{|G''|}{|G|} = \frac{|G''|}{|G'|} \cdot \frac{|G'|}{|G|} = [G'' : G'] \cdot \frac{|G'|}{|G|}.$$

□

Der Indexsatz lässt sich auch auf unendliche Gruppen verallgemeinern.

Definition 1.5. Sei G eine Gruppe. Eine Untergruppe $N \leq G$ heißt *normal* oder *Normalteiler von* G, falls

$$gNg^{-1} = N$$

für alle $g \in G$ gilt. Wir schreiben dann $N \trianglelefteq G$.

Beispiel 1.2. (1) Ist G abelsch, so ist offenbar jede Untergruppe $H \leq G$ Normalteiler von G.[1.2] Die Umkehrung gilt nicht. Betrachten wir beispielsweise die Quaternionen $\mathbb{H}$ aus Beispiel 2.4.[1.3] Insbesondere definieren wir die Quaternionengruppe Q_8 indem wir das Quaternionenprodukt als Operation auf der Menge

$$\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$$

auffassen. Die Untergruppen bestimmen wir durch Fallunterscheidung. Sei $U \leq Q_8$ eine beliebige Untergruppe; nehmen wir an, dass $U \neq \{1\}$ oder $U \neq \{\pm 1\}$. Dann ist eines von i, j und k in U. O. B. d. A. sei $\mathrm{i} \in U$; die anderen beiden Fälle sind ähnlich. Also ist auch $-1 = \mathrm{i}^2 \in U$, sodass entweder $U = Q_8$, falls j oder k Element von U ist und sonst $U = \{\pm 1, \pm \mathrm{i}\} = \langle \mathrm{i} \rangle$. Das liefert die (echten) Untergruppen

$$\langle 1 \rangle, \quad \langle -1 \rangle, \quad \langle \mathrm{i} \rangle, \quad \langle \mathrm{j} \rangle, \quad \langle \mathrm{k} \rangle$$

1.1. Joseph-Louis Lagrange (1736 – 1813), italienischer Mathematiker, Physiker und Astronom

1.2. Eine Gruppe G deren Untergruppen alle Normalteiler von G sind werden *dedekindsche Gruppen* genannt.

1.3. Dementsprechend bezeichnen wir nicht-abelsche dedekindsche Gruppen auch als *hamiltonsche Gruppen*. Sie können (bis auf Isomorphie) vollständig angegeben werden.

von Q_8. Insbesondere bemerken wir, dass diese Untergruppen von Q_8 zyklisch sind und daher abelsch, Q_8 hingegen nicht. Ferner sind sie sogar Normalteiler von Q_8, wie man leicht überprüfen kann.

(2) Sei S_3 die symmetrische Gruppe auf drei Elementen. Dann ist $H := \langle (12) \rangle$ eine abelsche Untergruppe von S_3, aber nicht normal, da $(123)\,(12)\,(123)^{-1} = (23) \notin H$.

Nun zum gruppentheoretischen Pendant von Quotientenringen und Homomorphismen.

Definition 1.6. Sei G eine Gruppe, $N \trianglelefteq G$. Dann ist

$$G/N := \{gN \mid g \in G\},$$

die Menge der Linksnebenklassen modulo N, mit der Operation

$$(gN) \circ (hN) := (g \circ h)\, N$$

eine Gruppe, genannt die *Quotientengruppe von G modulo N*[1.4].

Definition 1.7. Seien G, H Gruppen.

(1) Eine Abbildung $\phi\colon G \to H$ heißt (Gruppen)-Homomorphismus, wenn für alle $g, h \in G$ gilt, dass

$$\phi(g \circ h) = \phi(g) \circ \phi(h).$$

(2) Ein injektiver Homomorphismus heißt *Monomorphismus* oder *(isomorphe) Einbettung* und wir schreiben $\phi\colon G \hookrightarrow H$.

(3) Ein surjektiver Homomorphismus heißt *Epimorphismus* und wir schreiben $\phi\colon G \twoheadrightarrow H$.

(4) Ein bijektiver Homomorphismus heißt *Isomorphismus*. Wir schreiben dann $\phi\colon G \xrightarrow{\sim} H$ und $G \cong H$. Man nennt G und H dann zueinander *isomorph*.

Beispiel 1.3. (1) Die Abbildung $\phi\colon G \to S(M), \phi(g) := f_g$ im Beweis des Satzes von Cayley ist ein Monomorphismus.

(2) Ist G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler, so ist die *natürliche Projektion von G auf den Quotienten G/N* ein Epimorphismus (cf. Beispiel 4.5).

(3) Seien G_1, G_2 Gruppen. Dann ist

$$G_1 \times G_2 \to G_2 \times G_1, \quad (g_1, g_2) \mapsto (g_2, g_1)$$

ein Gruppenisomorphismus von G_1 nach G_2.

(4) Sei G eine Gruppe und $g \in G$. Dann ist

$$G \to G, \quad x \mapsto g x g^{-1}$$

ein Gruppenisomorphismus von G nach G. Wir nennen diese Abbildung die *Konjugation von g*.

(5) Die Nullabbildung ist (trivialerweise) immer ein Gruppenhomomorphismus.

Ganz analog im Fall zum Ringen beweist man:

1.4. Auch: *Faktorgruppe*, *Restklassengruppe*.

Lemma 1.4. Seien G und H Gruppen, $\phi\colon G \to H$ ein Homomorphismus. Dann gilt $\phi(e_G) = e_H$ und $\phi(g^{-1}) = \phi(g)^{-1}$ für alle $g \in G$.

Und:

Definition 1.8. Seien G und H Gruppen, $\phi\colon R \to S$ ein Homomorphismus. Dann heißt die Menge

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}$$

der *Kern von* ϕ. Ferner definieren wir das *Bild von* ϕ als

$$\operatorname{im} \phi := \{\phi(g) \mid g \in G\}.$$

Lemma 1.5. Seien G und H Gruppen, $\phi\colon G \to H$ ein Homomorphismus. Dann gilt:

(1) $\ker \phi$ ist ein Normalteiler von G und $\operatorname{im} \phi$ ist eine Untergruppe von H.

(2) ϕ ist genau dann ein Monomorphismus, wenn $\ker \phi = \{e_G\}$.

Genauso zentral wie bei Ringen ist der erste Isomorphiesatz für Gruppen. Zur Illustration kopieren wir seinen Beweis fast wortwörtlich:

Satz 1.1. (Erster Isomorphiesatz für Gruppen) Es sei $\phi\colon G \to H$ ein Gruppenhomomorphismus von G nach H. Dann induziert ϕ einen Isomorphismus

$$\phi^* : G/\ker \phi \xrightarrow{\sim} \operatorname{im} \phi, \quad \phi^*(g \ker \phi) := \phi(g).$$

Insbesondere gilt $G/\ker \phi \cong \operatorname{im} \phi$.

Beweis. Sei $K := \ker \phi$. Wir zeigen schrittweise, dass ϕ^* ein wohldefinierter Isomorphismus von G nach H ist.

Wohldefiniertheit: Seien $g_1, g_2 \in G$ mit $g_1 K = g_2 K$. Dann gilt $g_1 g_2^{-1} \in K$, also $\phi(g_1)\,\phi(g_2)^{-1} = \phi(g_1 g_2^{-1}) = e$. Insbesondere muss $\phi(g_1) = \phi(g_2)$ gelten, d.h. $\phi^*(g_1 K) = \phi^*(g_2 K)$.

Homomorphieeigenschaft: Für alle $g, h \in G$ gilt

$$\begin{aligned}\phi^*((gK) \circ (hK)) = \phi^*((g \circ h)\, K) = \phi(g \circ h) = \phi(g) \circ \phi(h)\\ = \phi^*(gK) \circ \phi^*(hK).\end{aligned}$$

Injektivität: Ist $e = \phi^*(gK) = \phi(g)$ für ein $g \in G$, so gilt offenbar $g \in K$. Daraus folgt, dass

$$\ker \phi^* = \{eK\}$$

und somit ist ϕ^* nach Lemma 1.5 (2) injektiv.

Surjektivität: Das folgt unmittelbar aus der Definition von ϕ^*. □

Der Begriff von Kern/Bild im Kontext der Gruppen hat ebenso eine Verbindung zu Normalteilern. Folgende Eigenschaften sind auch ganz allgemein nützlich:

Lemma 1.6. Sei G eine Gruppe mit neutralem Element $e \in G$ und $N \leq G$ eine Untergruppe. Dann sind die folgenden Aussagen äquivalent:

(1) Es gibt eine Gruppe H und einen Homomorphismus $\varphi\colon G \to H$ mit $N = \ker \varphi$.

(2) N ist Normalteiler von G.

(3) $gNg^{-1} \subseteq N$ für alle $g \in G$.

(4) $gN = Ng$ für alle $g \in G$.

(5) Links- und Rechtskongruenz modulo N definieren dieselbe Äquivalenzrelation.

(6) $gN \subseteq Ng$ für alle $g \in G$.

Beweis. Die Implikationskette $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6)$ folgt unmittelbar aus den Definitionen, wir müssen also nur zeigen, dass falls $gN \subseteq Ng$ für alle $g \in G$ gilt, N der Kern eines Homomorphismus von G nach H ist. Ist N Normalteiler, so folgt direkt, dass N der Kern der natürlichen Projektion auf den Quotienten G/N ist. Da $gN \subseteq Ng$ für alle $g \in G$, gilt insbesondere $gNg^{-1} \subseteq Ngg^{-1} = N$. Andererseits gilt auch $g^{-1}N \subseteq Ng^{-1}$, somit $N = gg^{-1}N \subseteq gNg^{-1}$, also $gNg^{-1} = N$ und N ist normal. □

Damit haben wir alle wesentlichen Definitionen aus der Ringtheorie in die Sprache der Gruppen übersetzt. Kommen wir nun zum ersten neuen Ergebnis.

Lemma 1.7. Sei G eine Gruppe und $H \leq G$ eine Untergruppe mit $[G:H] = 2$. Dann ist H ein Normalteiler von G.

Beweis. Sei $g \in G$ beliebig. Falls $g \in H$, folgt $gH = H = Hg$. Falls $g \notin H$, dann folgt aus $[G:H] = 2$, dass $gH = G \setminus H$ und ähnlich sieht man $Hg = G \setminus H$. Insbesondere also $gH = G \setminus H = Hg$. Da g beliebig gewählt war, folgt also $H \trianglelefteq G$. □

Proposition 1.3. Sei $n \in \mathbb{N}$ beliebig. Dann existiert eine bis auf Isomorphie eindeutig bestimmte zyklische Gruppe der Ordnung n, nämlich $(\mathbb{Z}/n\mathbb{Z}, +)$. Weiterhin ist jede unendliche zyklische Gruppe zu $(\mathbb{Z}, +)$ isomorph.

Beweis. Es sei $G := \{g^n \mid n \in \mathbb{Z}\}$ eine beliebige zyklische Gruppe. Dann ist

$$\phi : (\mathbb{Z}, +) \to (G, \circ), \quad m \mapsto g^m$$

ein surjektiver Gruppenhomomorphismus mit $\ker \phi \leq \mathbb{Z}$. Also existiert ein eindeutiges $d \in \mathbb{N}_0$ mit $\ker \phi = d\mathbb{Z}$ (Folgerung 2.2). Aus dem Ersten Isomorphiesatz folgt nun

$$\mathbb{Z}/d\mathbb{Z} \cong G.$$

Ist insbesondere $d = 0$, so folgt $\ker \phi = \{0\}$, d.h. ϕ ist injektiv und sogar ein Isomorphismus. □

Folgerung 1.2. Sei G eine endliche zyklische Gruppe mit $|G| = m$. Dann existiert zu jedem Teiler k von m genau eine Untergruppe $H \leq G$ mit $|H| = k$.

Beweis. Es gilt $G \cong \mathbb{Z}/m\mathbb{Z}$ nach Proposition 1.3. Sei $k \mid m$ ein Teiler von m. Dann existiert ein eindeutig bestimmtes $\ell \in \mathbb{N}$ mit $k \cdot \ell = m$. Nun ist $H = \{0, \ell, 2\ell, \ldots, (k-1)\ell\}$ die gewünschte Untergruppe von $\mathbb{Z}/m\mathbb{Z}$.

Um die Eindeutigkeit zu zeigen, sei $U \leq \mathbb{Z}/m\mathbb{Z}$ eine Untergruppe mit $|U| = k$. Dann ist $U = \langle a \rangle$ für ein $a \in \mathbb{Z}/m\mathbb{Z}$ und wegen $k = \operatorname{ord}(a) = \frac{m}{\operatorname{ggT}(a,m)}$, gilt $\operatorname{ggT}(a, m) = m/k = \ell$. Daher $\langle a \rangle = \langle \ell \rangle = H$, wie gewünscht. □

Unser nächstes Ziel ist es, folgende Frage zu beantworten: Hält die Umkehrung des Satzes von Lagrange? Formal: Sei G eine endliche Gruppe und k ein Teiler von $|G|$. Existiert eine Untergruppe $H \leq G$ der Ordnung k? Die Antwort ist *nein*, wie wir im nächsten Beispiel sehen werden. Welche Zusatzbedingungen müssen wir also fordern? In diesem Sinne führen wir nun einige wesentliche Begrifflichkeiten und Ergebnisse ein.

Beispiel 1.4. (1) Sei $n \geq 2$. Aus der linearen Algebra kennen wir die Abbildung

$$\operatorname{sgn} : S_n \to \{\pm 1\}, \quad \operatorname{sgn}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j},$$

die wir u. a. für die Definition der Determinante (nach Leibniz) benötigen. Dort haben wir gesehen, dass sgn sogar ein (surjektiver) Gruppenhomomorphismus ist. Den Kern dieser Abbildung nennen wir die *alternierende Gruppe*; geschrieben

$$A_n := \ker \operatorname{sgn}.$$

Da dann $A_n \lhd S_n$, folgt aus dem Ersten Isomorphiesatz und dem Satz von Lagrange, dass

$$2 = |S_n / A_n| = \frac{|S_n|}{|A_n|} = \frac{n!}{|A_n|},$$

also $|A_n| = n!/2$. Im Fall $n = 4$ ist $|A_4| = 12$ und obwohl $6 \mid 12$, existiert keine Untergruppe $H \leq A_4$ mit $|H| = 6$.

(2) Wir kennen den Satz von Lagrange, Proposition 1.2, eigentlich schon. Wir haben in Satz 2.2 gesehen, dass jede endliche Gruppe G zu einer Galoisgruppe $\operatorname{Gal}(L/K)$, $L : K$ Körpererweiterung, isomorph ist, wobei $|G| = [L : K]$. Weiters sagt der Hauptsatz der Galoistheorie eben, dass jede Untergruppe $H \leq G \cong \operatorname{Gal}(L/K)$ zu einem Zwischenkörper $K \subseteq M \subseteq L$ bijektiv korrespondiert, nämlich $M \cong L^H$. Dann gilt $|H| = [L : L^H]$ und $[G : H] = \frac{|G|}{|H|} = \frac{[L:K]}{[L:L^H]} = [L^H : K]$ nach der Gradregel. Zusammengefasst:

$$\overbrace{[L:K]}^{|G|} = \overbrace{[L:L^H]}^{H} \cdot \overbrace{[L^H:K]}^{[G:H]}.$$

Folgerung 1.3. Es sei G eine endliche Gruppe und $g \in G$. Dann ist $\operatorname{ord}(g)$ ein Teiler von $|G|$ und $g^{|G|} = e$.

Beweis. Die erste Behauptung folgt unmittelbar aus dem Satz von Lagrange; insbesondere ist $\frac{|G|}{\operatorname{ord}(g)}$ eine ganze Zahl. Die zweite Behauptung folgt wiederum aus der Beobachtung

$$g^{|G|} = g^{\operatorname{ord}(g) \cdot \frac{|G|}{\operatorname{ord}(g)}} = \left(g^{\operatorname{ord}(g)}\right)^{\frac{|G|}{\operatorname{ord}(g)}} = e^{\frac{|G|}{\operatorname{ord}(g)}} = e.$$

□

Man bemerke hier auch die Ähnlichkeit zum Kleinen Fermat'schen Satz, Lemma 5.2.

Folgerung 1.4. Sei G eine Gruppe mit $|G| = p$, $p \in \mathbb{P}$. Dann ist G zyklisch und $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$.

Beweis. Es sei $g \in G$ nicht das neutrale Element. Dann gilt $\operatorname{ord}(g) \geq 2$ und $\operatorname{ord}(g) \mid |G| = p$ nach Folgerung 1.3, also notwendigerweise $\operatorname{ord}(g) = p$, da p eine Primzahl ist. □

Auch diese Aussage kennen wir im Prinzip schon, nämlich Korollar 1.1.

2 Endliche Gruppen

Definition 2.1. Sei $(G, \circ)$ eine Gruppe und S eine nichtleere Menge. Eine *Aktion von G auf S* ist eine Abbildung

$$* : G \times S \to S, \quad (g, x) \mapsto g * x,$$

die folgende Bedingungen erfüllt:

(1) $e * x = x$ für alle $x \in S$.

(2) $g * (h * x) = (g \circ h) * x$ für alle $g, h \in G$ und $x \in S$.

Wir sagen, dass G auf S *operiert*.

Beispiel 2.1. (1) Sei $H \leq G$ eine Untergruppe und $S = G$. Dann ist

$$H \times G \to G, \quad (h, g) \mapsto h \circ g$$

eine Aktion von H auf G. Sie wird auch *Linkstranslation von H auf G* genannt.

(2) Sei $H \leq G$ wieder eine Untergruppe und $S = G$. Die Konjugationsabbildung

$$(h, g) \mapsto h * g := hgh^{-1},$$

genannt die *Konjugation von H auf G*, ist eine Aktion von H auf G.

(3) Sei $G = \mathrm{Gal}(L/K)$ und $S = L$ eine Galoiserweiterung des Körpers K. Man überprüft, dass

$$G \times L \to L, \quad (\sigma, \ell) \mapsto \sigma * \ell := \sigma(\ell)$$

eine Gruppenaktion von G auf K definiert.

(4) Sei V ein Vektorraum über einem Körper K. Dann definiert die Multiplikation von Vektoren aus V mit Skalaren aus K^* „$\cdot$“ die Gruppenaktion

$$K^* \times V \to V, \quad (k, v) \mapsto k \cdot v$$

von K^* auf V. Setzt man für alle $v \in V$ noch $0 \cdot v = v$, so kann diese auf ganz K ausgedehnt werden. Fordern wir zusätzlich, dass die Distributivgesetze $(k_1 + k_2) \cdot v = k_1 \cdot v + k_2 \cdot v$ und $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$ für $k, k_1, k_2 \in K$ und $v, v_1, v_2 \in V$ gelten, erhalten wir die übliche Struktur in Vektorräumen.

(5) Die Matrix-Vektor-Multiplikation

$$\mathrm{GL}(n, K) \times K^n \to K^n, \quad (A, v) \mapsto Av$$

definiert eine Aktion von $\mathrm{GL}(n, K)$ auf K^n.

Lemma 2.1. Sei G eine Gruppe und S eine Menge auf der G per „$*$“ operiert. Dann gilt:

(1) Die Relation

$$x \sim x' \quad :\Leftrightarrow \quad \exists g \in G \colon g * x = x'$$

ist eine Äquivalenzrelation auf S.

(2) Die Menge $G_x := \{g \in G \mid g * x = x\}$ ist eine Untergruppe von G für alle $x \in S$.

Beweis. (1) Reflexivität: Es gilt $e * x = x$ für alle $x \in S$, d.h. $x \sim x$.

Symmetrie: Nehmen wir an, dass $x \sim y$ für $x, y \in S$, also existiert $g \in G$ mit $g * x = y$ und daher

$$g^{-1} * y = g^{-1} * (g * x) = (g^{-1} \circ g) * x = e * x = x.$$

Transitivität: Sei $x \sim y$ und $y \sim z$ für $x, y, z \in S$. Dann gibt es $g_1, g_2 \in G$, sodass $g_1 * x = y$ und $g_2 * y = z$. Es folgt, dass $(g_2 \circ g_1) * x = g_2 * (g_1 * x) = g_2 * y = z$.

(2) Sei $x \in S$ beliebig. Sind $g_1, g_2 \in G_x$, so folgt

$$(g_1 \circ g_2) * x = g_1 * (g_2 * x) = g_1 * x = x,$$

d.h. $g_1 \circ g_2 \in G_x$. Da

$$g_1^{-1} * x = g_1^{-1} * (g_1 * x) = (g_1^{-1} \circ g_1) * x = x$$

und offenbar $e \in G_x$, folgt $G_x \leq G$. □

Wir nennen die von einer Aktion „$*$“ auf S induzierten Äquivalenzklassen die *Orbits von G in S*. Der Orbit von $x \in S$ wird auch mit $[x]_{G,*}$ oder $[x]$ oder Gx (sofern G und „$*$“ vom Kontext her klar sind) bezeichnet. Die Untergruppe G_x nennen wir auch den *Stabilisator von x in G*, alternativ die *Isotropiegruppe von x in G*.

Definition 2.2. Betrachten wir Beispiel 2.1 (2).

(1) Der Orbit von $g \in G$ bezüglich der Konjugation mit Elementen aus H heißt *H-Konjugationsklasse von g*. Es gilt $[g] = \{hgh^{-1} \mid h \in H\}$.

(2) Die Isotropiegruppe $H_g = \{h \in H \mid hgh^{-1} = g\}$ von einem $g \in G$ heißt *Zentralisator von g in H* und wird mit $C_H(g)$ bezeichnet. Im Fall $G = H$ wird der Durchschnitt

$$Z(G) := \bigcap_{g \in G} C_G(g)$$

das *Zentrum von G* genannt.

(3) Sei $S = \{K \leq G\}$ und

$$H \times S, \quad (h, K) \mapsto hKh^{-1}$$

eine Aktion von H auf S. Dann heißt die Isotropiegruppe von $K \in S$ in H bezüglich dieser Aktion der *Normalisator von K in H* und wird mit $N_H(K)$ bezeichnet.

Beispiel 2.2. (1) Sei $H = G$. Offenbar handelt es sich bei $Z(G)$ um jene Untergruppe von G, die aus den Elementen von G besteht, die man mit allen $g \in G$ vertauschen kann, i.e.

$$Z(G) = \{z \in G \mid \forall g \in G \colon zg = gz\}.$$

(2) Es gilt $N_G(K) \leq G$. Ferner gilt $K \trianglelefteq G$ genau dann, wenn $N_G(K) = G$. Außerdem gilt $K \trianglelefteq N_G(K)$, aber *nicht* unbedingt $N_G(K) \trianglelefteq G$. Sei beispielsweise $G = \mathrm{GL}(2, \mathbb{R})$ und $K \leq G$ die Menge der Diagonalmatrizen in dieser Gruppe. Dann ist der Normalisator von K in G die Menge der Matrizen, bei denen in jeder Zeile bzw. Spalte genau ein Eintrag ungleich Null ist. Insbesondere haben wir

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \in N_G(K), \quad \text{aber} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \notin N_G(K),$$

d.h. $N_G(K) \not\trianglelefteq G$.

Lemma 2.2. (Bahnformel) Sei G eine Gruppe, die per „$*$“ auf der Menge S operiert. Dann ist

$$|[x]_{G,*}| = [G \colon G_x].$$

Beweis. Betrachten wir die Abbildung

$$G/G_x \to [x]_{G,*}, \quad gG_x \mapsto g * x.$$

Diese ist wohldefiniert; denn gilt $g_1 G_x = g_2 G_x$ für $g_1, g_2 \in G$, so folgt:

$$\begin{aligned} g_1 g_2^{-1} \in G_x &\Leftrightarrow (g_1^{-1} g_2) * x = x \Leftrightarrow g_1^{-1} * (g_2 * x) = x \\ &\Leftrightarrow g_1 * (g_1^{-1} * (g_2 * x)) = g_1 * x \\ &\Leftrightarrow g_2 * x = g_1 * x. \end{aligned}$$

Da auch die Bijektivität sofort aus dieser Implikationskette ersichtlich ist, folgern wir

$$|[x]_{G,*}| = |G / G_x| = [G : G_x],$$

wie gewünscht. □

Im Englischen ist die Bahnformel als *Orbit-stabilizer theorem* bekannt.

Lemma 2.3. Es sei G eine endliche Gruppe mit $|G| = p^n$ für $p \in \mathbb{P}$, $n \in \mathbb{N}_0$. Ferner operiere G auf einer endlichen Menge S mit der Aktion „$*$“. Sei $S_0 := \{x \in S \mid \forall g \in G : g * x = x\}$. Dann ist

$$|S| \equiv |S_0| \pmod{p}.$$

Beweis. Per Definition von S_0 gilt $|[x]_{G,*}| = 1$ genau dann, wenn $x \in S_0$. Nach Lemma 2.1 gibt es eine Partition

$$S = S_0 \cup [x_1]_{G,*} \cup \cdots \cup [x_m]_{G,*}$$

für $x_1, \ldots, x_m \in S$ und $m \in \mathbb{N}$ wobei $|[x_i]_{G,*}| > 1$ und folglich $|G_{x_i}| < |G| = p^n$ für jene $1 \leq i \leq m$. Aus Lemma 2.2 sowie dem Satz von Lagrange folgt nun

$$\begin{aligned} |S| &= |S_0| + |[x_1]_{G,*}| + \cdots + |[x_m]_{G,*}| = |S_0| + [G : G_{x_1}] + \cdots + [G : G_{x_m}] \\ &= |S_0| + \frac{|G|}{|G_{x_1}|} + \cdots + \frac{|G|}{|G_{x_m}|} \\ &= |S_0| + \frac{p^n}{|G_{x_1}|} + \cdots + \frac{p^n}{|G_{x_m}|}, \end{aligned}$$

d.h. $|S| \equiv |S_0| \pmod{p}$. □

Mit diesem Lemma können wir nun den *Satz von Cauchy* beweisen:

Proposition 2.1. (Cauchy) Sei G eine endliche Gruppe mit $|G| = m$ und $p \mid m$ ein Primteiler von m. Dann existiert ein $g \in G$ mit $\operatorname{ord}(g) = p$. Insbesondere existiert eine Untergruppe $H \leq G$ mit $|H| = p$.

Beweis. Sei $S := \{(g_1, \ldots, g_p) \mid \prod_{i=1}^{p} g_i = e\}$. Da für eine beliebige Wahl von $g_1, \ldots, g_{p-1}$ das Element $g_p = \prod_{i=1}^{p-1} g_{p-i}^{-1}$ fixiert ist, folgt $|S| = m^{p-1}$, also $|S| \equiv 0 \pmod{p}$. Wir definieren die Aktion

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} \times S \to S, \quad (k, (g_1, \ldots, g_p)) &\mapsto k * (g_1, \ldots, g_p) \\ &:= (g_{k+1}, g_{k+2}, \ldots, g_p, g_1, g_2, \ldots, g_k). \end{aligned}$$

Diese Abbildung ist wohldefiniert, da $g \circ h = e$ automatisch $h \circ g = e$ impliziert und eine Aktion, da

$$\begin{aligned} 0 * (g_1, \ldots, g_p) &= (g_1, \ldots, g_p), \\ (k + k') * (g_1, \ldots, g_p) &= (g_{k+k'+1}, \ldots, g_p, g_1, \ldots, g_{k+k'}) = k * (g_{k'+1}, \ldots, g_p, g_1, \ldots, g_{k'}) \\ &= k * (k' * (g_1, \ldots, g_p)). \end{aligned}$$

Betrachten wir nun $S_0 = \{x \in S \mid \forall k \in \mathbb{Z}/p\mathbb{Z} : k * x = x\}$ aus Lemma 2.3. Dann gilt offenbar $(g_1, \ldots, g_p) \in S$ genau dann, wenn $g_1 = \cdots = g_p$. Da das p-Tupel $(e, \ldots, e)$ in S_0 liegt, folgt $|S_0| > 0$; ferner folgt aus $0 = |S| \equiv |S_0| \pmod{p}$ (eben Lemma 2.3) somit $|S_0| \geq 2$. Das heißt, es existiert $e \neq g \in G$ mit $(g, \ldots, g) \in S_0$, i.e. $g^p = \prod_{i=1}^{p} g_i = e$ und damit $\operatorname{ord}(g) = p$ (nach Lemma 1.2). □

Beispiel 2.3. (1) Sei G eine endliche Gruppe mit gerader Gruppenordnung. Dann hat G eine Involution nach dem Satz von Cauchy, d.h., ein Element $g \neq e$ mit $g^2 = e$.

(2) Aus dem Satz von Lagrange und dem Satz von Cauchy folgt: Eine endliche Gruppe G hat genau dann ungerade Ordnung, wenn e die eindeutige Lösung von $g^2 = e$ ist.

(3) Einen noch schnelleren Beweis von Folgerung 1.4 erhalten wir auch durch den Satz von Cauchy. Sei G eine endliche Gruppe mit $|G| = p$, $p \in \mathbb{P}$. Dann existiert $g \in G$ mit $\operatorname{ord}(g) = p = |G|$, also $G = \langle p \rangle$.

Der Satz von Cauchy ist ein Spezialfall des *Ersten Sylowsatzes*[2.1]:

Satz 2.1. (Erster Sylowsatz) Sei G eine endliche Gruppe mit $|G| = p^n \cdot k$ mit $p \in \mathbb{P}, n \geq 1$ und $\operatorname{ggT}(p, k) = 1$. Dann existieren Untergruppen

$$H_i \leq G \quad \text{mit} \quad |H_i| = p^i$$

für $i = 0, \ldots, n$.

Beweis. Wir führen vollständige Induktion nach n. Der Fall $n = 0$ ist offensichtlich.

Sei die Aussage nun für alle Gruppen G mit $|G| = p^{n-1} \cdot k$ und $\operatorname{ggT}(p, k) = 1$ gezeigt. Nehmen wir zunächst an, dass $k = 1$. Sei $S := G$ und $*$ die Konjugation von G auf sich selbst, d.h.

$$G \times G \to G, \quad (g, h) \mapsto hgh^{-1}.$$

Da $k = 1$, sind alle Voraussetzungen von Lemma 2.3 erfüllt und es gilt ferner $S_0 = \{g \in G \mid \forall h \in G : h * g = g\} = Z(G)$, also $|G| \equiv |Z(G)| \pmod{p}$. Da $Z(G) \leq G$ folgt aus dem Satz von Lagrange, dass $|Z(G)| \mid |G|$, insgesamt erhalten wir somit $p \mid |Z(G)|$ und $|Z(G)| \mid |G| = p^n$, i.e. $|Z(G)| = p^\ell$ für $1 \leq \ell \leq n$. Nach dem Satz von Cauchy existiert also $z \in Z(G)$ mit $\operatorname{ord}(z) = p$ und $\langle z \rangle \trianglelefteq G$; insbesondere ist $G/\langle z \rangle$ eine Gruppe. Aus dem Satz von Lagrange folgt nun, dass

$$|G/\langle z \rangle| = \frac{|G|}{|\langle z \rangle|} = \frac{p^n}{p} = p^{n-1},$$

also können wir die Induktionsvoraussetzung auf $G/\langle z \rangle$ anwenden, d.h. es existieren $H_i' \leq G/\langle z \rangle$ mit $H_i' = p^i$ für $i = 0, \ldots, n-1$. Betrachten wir die natürliche Projektion $\pi : G \twoheadrightarrow G/\langle z \rangle$. Dann ist $H_{i+1} := \pi^{-1}(H_i')$ eine Untergruppe von G mit $|H_{i+1}| = p^{i+1}$ für $i = 0, \ldots, n-1$, wie gewünscht.

Nehmen wir nun an, dass $k \neq 1$. Nach dem gerade Gezeigten reicht es, zu beweisen, dass $H \leq G$ mit $|H| = p^n$ existiert. Sei $p \mid |Z(G)|$ ein Primteiler; dann existiert wieder $z \in Z(G)$ mit $\operatorname{ord}(z) = p$ und wir können die Induktionsvoraussetzung erneut auf $G/\langle z \rangle$ anwenden, um $H_i = \pi^{-1}(H_i')$ für Untergruppen $H_i' \leq G/\langle z \rangle$ mit $|H_i'| = p^i$ für $i = 0, \ldots, n-1$ zu erhalten.

Es sei also $p \nmid |Z(G)|$. Nach Lemma 2.1 existiert ein $r \in \mathbb{N}_0$ bzw. eine Partition

$$G = Z(G) \cup \underbrace{[g_1]_{G,*} \cup \cdots \cup [g_r]_{G,*}}_{\text{Orbits mit } |[g]_{G,*}| > 1}$$

2.1. Peter Ludwig Mejdell Sylow (1832 – 1918), norwegischer Mathematiker

für $g_1, \dots, g_r \in G$ (mit $*$ der Konjugation auf G). Es folgt

$$p^n k = |G| = |Z(G)| + \sum_{j=1}^{r} |[g_j]_{G,*}|,$$

wobei $r \geq 1$, da $p \nmid |Z(G)|$ per Annahme. Also existiert ein $j \in \{1, \dots, r\}$ mit $|[g_j]_{G,*}| > 1$ und $p \nmid [g_j]_{G,*}$. Ferner gilt

$$|[g_j]_{G,*}| = [G : G_{g_j}] = \frac{|G|}{|G_{g_j}|} = \frac{p^n k}{|G_{g_j}|},$$

aber $p \nmid [g_j]_{G,*}$ impliziert $|G_{g_j}| = p^n k'$ mit $k' | k$. Insbesondere folgt aus $|[g_j]_{G,*}|$, dass $1 \leq k' < k$. Falls $k' = 1$, so ist $H = G_{g_j} \leq G$ die gewünschte Untergruppe von G und falls $k' > 1$, so können wir das obige Argument mit k' statt k wiederholen und nach endlich vielen Schritten eine Untergruppe $H \leq G$ von G mit $|H| = p^n$ erhalten. □

Fassen wir zusammen: Ist G eine beliebige endliche Gruppe mit $|G| = \prod_{p \in \mathbb{P}} p^{\nu_p}$ für Exponenten $\nu_p \in \mathbb{N}_0$, so existiert zu jeder Primzahlpotenz p^j mit $0 \leq j \leq \nu_p$ eine Untergruppe $H \leq G$ mit $|H| = p^j$. Die Untergruppe von Kardinalität p^{ν_p} nennen wir die *p-Sylowgruppe* von G. In Anbetracht von Beispiel 1.4, wo wir die alternierende Gruppe A_4 betrachtet haben, ist der Erste Sylowsatz diesbezüglich das „bestmögliche“ Resultat.

Man kann den Ersten Sylowsatz auch galoistheoretisch interpretieren. Sei $L : K$ eine endliche Galoiserweiterung. Zusammen mit dem Hauptsatz der Galoistheorie, sagt der Erste Sylowsatz dann, dass es zu jeder Primfaktorpotenz p^i, die $[L : K] = |\mathrm{Gal}(L/K)|$ teilt, einen Zwischenkörper M_i, $K \subseteq M_i \subseteq L$, gibt mit $[L : M_i] = p^i$. Dieser Ansatz leitet auch zum Versuch eines alternativen Beweises von Satz 2.1: Wir konstruieren eine endliche Galoiserweiterung $L : K$, finden einen Zwischenkörper M_i mit $[L : M_i] = p^i$ und verwenden dann Satz 2.2.

Nun ein kurzer Exkurs in die Theorie der abelschen Gruppen. Wir wissen, dass eine Gruppe G genau dann abelsch ist, wenn $G = Z(G) = \{g \in G \mid \forall h \in G : gh = hg\}$.

Definition 2.3. Sei G eine Gruppe. Sei $X := \{ghg^{-1}h^{-1} \mid g, h \in G\}$ die Menge der *Kommutatoren*. Wir nennen die Gruppe

$$[G; G] := \langle X \rangle$$

die *Kommutatorgruppe*, wobei wir mit $\langle X \rangle$ die von X erzeugte Untergruppe $\langle X \rangle \subseteq G$ bezeichnen, d.h. der Durchschnitt aller Untergruppen von G, die X enthalten.

Lemma 2.4. Sei G eine Gruppe. Dann gilt:

(1) G ist genau dann abelsch, wenn $[G; G] = \{e\}$.

(2) Die Kommutatorgruppe $[G; G]$ ist normal in G.

(3) $G/[G; G]$, die sogenannte *Abelisierung* von G, ist abelsch.

(4) Sei $G^{(1)} := [G; G]$ und $G^{(i+1)} := [G^{(i)}; G^{(i)}]$ für $i \geq 1$. Dann erhalten wir eine absteigende Kette

$$\cdots \trianglelefteq G^{(3)} \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G.$$

Beweis. (1) Ist G abelsch, so gilt für alle Kommutatoren $ghg^{-1}h^{-1} = e$, $g, h \in G$, also insbesondere $[G; G] = \{e\}$. Umgekehrt, falls $[G; G] = \{e\}$, so folgt für beliebige $g, h \in G$, dass $ghg^{-1}h^{-1} = e$, also $gh = hg$.

(2) Ist $g \in G$ und $c \in [G; G]$, so folgt $gcg^{-1}c^{-1} \in [G; G]$, also insbesondere $gcg^{-1} = (gcg^{-1}c^{-1})\, c \in [G; G]$ wegen der Abgeschlossenheit.

(3) Seien $g, h \in G$. Dann folgt $(gh)^{-1} hg = h^{-1} g^{-1} hg \in [G;G]$, also gilt für die Restklassen $gh\,[G;G] = hg\,[G;G]$ nach Proposition 1.1.

(4) Aus (2) folgt direkt $G^{(i+1)} \trianglelefteq G^{(i)}$ für alle $i \geq 1$. □

Ergibt die Kette aus Lemma 2.4 (4) nach endlich vielen Schritten schließlich $\{e\}$, d.h. es existiert ein $n \in \mathbb{N}$ mit $\{e\} = G^{(n)}$, so nennt man G *auflösbar*. Abelsche Gruppen sind also die „am schnellsten" auflösbaren Gruppen ($\{e\} = G^{(1)}$).

Lemma 2.5. Seien G und H Gruppen und $\phi: G \to H$ ein Homomorphismus. Dann gilt:

(1) $\phi([G;G]) = [\phi(G)\,;\phi(G)] \leq [H;H]$.

(2) Ist G auflösbar, so ist auch jede Untergruppe $G' \leq G$ von G auflösbar.

(3) Sind G und H auflösbar, so ist auch das direkte Produkt $G \times H$ auflösbar.

(4) Ist $N \trianglelefteq G$ und G auflösbar, so ist auch G/N auflösbar.

Beweis. (1) Seien $g_1, g_2 \in G$ beliebig. Dann folgt aus der Gleichung

$$\phi(g_1\, g_2\, g_1^{-1}\, g_2^{-1}) = \phi(g_1)\, \phi(g_2)\, \phi(g_1)^{-1}\, \phi(g_2)^{-1} \in [\phi(G); \phi(G)]$$

unmittelbar, dass $\phi([G;G]) = [\phi(G)\,;\phi(G)] \leq [H;H]$.

(2) Sei $G' \leq G$ eine beliebige Untergruppe von G. Da G auflösbar ist, existiert $n \geq 1$ mit $G^{(n)} = \{e\}$. Betrachten wir den Einbettungshomomorphismus $\phi: G' \to G$, $\phi(g) = g$, so gilt

$$G'^{(n)} \cong \phi(G)^{(n)} = \phi(G^{(n)}) = \phi(\{e\}) = \{e\},$$

wobei mit vollständiger Induktion nach n und (1) leicht zu zeigen ist, dass $\phi(G)^{(n)} = \phi(G^{(n)})$.

(3) Seien $g_1, g_2 \in G$ und $h_1, h_2 \in H$. Dann gilt

$$(g_1, h_1)\,(g_2, h_2)\,(g_1, h_1)^{-1}\,(g_2, h_2)^{-1} = (g_1\, g_2\, g_1^{-1}\, g_2^{-1}, h_1\, h_2\, h_1^{-1}\, h_2^{-1}),$$

d.h. $[G \times H; G \times H] = [G;G] \times [H;H]$. Zusammen mit vollständiger Induktion folgt daraus, dass $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$ für $n \geq 1$. Da G auflösbar ist, existiert $m_1 \geq 1$, sodass $G^{(m_1)} = \{e_G\}$ und ähnlich existiert $m_2 \geq 1$, sodass $H^{(m_2)} = \{e_H\}$. Für $m \geq \max\{m_1, m_2\}$ folgt also, dass

$$(G \times H)^{(m)} = G^{(m)} \times H^{(m)} = \{(e_G, e_H)\},$$

wie gewünscht.

(4) Für die kanonische Projektion $\pi: G \to G/N$ gilt $\pi(G^{(n)}) = (G/N)^{(n)}$. Ist also $G^{(m)} = \{e\}$ für ein $m \geq 1$, so folgt $(G/N)^{(m)} = \pi(G^{(m)}) = \{N\}$. Also ist G/N auflösbar. □

Beispiel 2.4. (1) S_2 ist abelsch, daher $S_2^{(1)} = \{e\}$ und ergo ist S_2 auflösbar. Wir erhalten die Kette $\{e\} \trianglelefteq S_2$. S_3 ist nicht abelsch, aber $S_3^{(1)} = A_3$ ist abelsch und wir bekommen die Kette $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$. Ebenso kann man zeigen, dass S_4 auflösbar ist.

(2) Andererseits ist S_5 nicht auflösbar, denn $S_5^{(1)} = A_5$ und $S_5^{(2)} = A_5^{(1)} = [A_5; A_5] = A_5$, d.h. $S_5^{(i)} = A_5 \neq \{e\}$ für alle $i \geq 1$. Tatsächlich gilt allgemein: Für $n \geq 5$ ist S_n nicht auflösbar. In der Tat, ist $\sigma \in S_5$, so setzen wir diese Permutation zu $\sigma' \in S_n$ wie folgt fort:

$$\sigma'(j) = \begin{cases} \sigma(j) \text{ für } 1 \leq j \leq 5, \\ j \text{ für } 6 \leq j \leq n. \end{cases}$$

Die resultiere Abbildung $S_5 \to S_n$ ist eine isomorphe Einbettung von Gruppen. Insbesondere enthält S_n für $n \geq 5$ eine Untergruppe, die zu S_5 isomorph ist und damit nach dem Eben erkannten nicht auflösbar sein kann. Damit ist S_n für $n \geq 5$ aber selbst nicht auflösbar.

Wir wollen mehr Beispiele für auflösbare Gruppen finden.

Definition 2.4. Sei G eine Gruppe. Gilt für jedes Element $g \in G$, dass $\operatorname{ord}(g) = p^j$ für ein $p \in \mathbb{P}$ und $j \in \mathbb{N}_0$, so nennen wir G eine *p-Gruppe*.

Lemma 2.6. Es sei G eine endliche Gruppe. Dann ist G genau dann eine p-Gruppe, wenn $|G| = p^n$ für $p \in \mathbb{P}$ und $n \geq 0$.

Beweis. Eine Richtung folgt aus dem Satz von Lagrange, die andere aus dem Satz von Cauchy. □

Beispiel 2.5. Nicht alle p-Gruppen müssen endlich sein. Die Gruppe

$$\bigoplus_{n \in \mathbb{N}} \mathbb{Z}/p\mathbb{Z} = \{(a_1, a_2, \dots) \mid a_i \in \mathbb{Z}/p\mathbb{Z}, a_i = 0 \text{ für alle bis auf endlich viele } i\}$$

ist beispielsweise eine unendliche p-Gruppe.

Lemma 2.7. Sei G eine nicht-triviale endliche p-Gruppe. Dann gilt $Z(G) \neq \{e\}$.

Beweis. Es gilt $S_0 = \{g \in G \mid \forall h \in G : hgh^{-1} = g\} = Z(G)$. Da G eine endliche p-Gruppe ist folgt aus Lemma 2.3, dass $|G| \equiv |Z(G)| \pmod p$. Da $|G| = p^n$ mit $n \geq 1$ folgt also $|Z(G)| \equiv 0 \pmod p$. Weil $e \in Z(G)$, folgt $|Z(G)| \geq 1$ und daher $|Z(G)| \geq p$, was zu zeigen war. □

Lemma 2.8. Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler, sodass N und die Quotientengruppe G/N auflösbar sind. Dann ist auch G auflösbar.

Beweis. Sei $\pi : G \to G/N$ die natürliche Projektion. Dann gilt nach Lemma 2.5 $\pi(G^{(i)}) = (G/N)^{(i)}$ für alle $i \geq 0$. Da G/N auflösbar ist, existiert $r \in \mathbb{N}_0$ mit $(G/N)^{(r)} = \{N\}$. Also $\pi(G^{(r)}) = \{N\}$ und damit $G^{(r)} \leq N$. Da auch N auflösbar ist, existiert $s \in \mathbb{N}_0$ mit $N^{(s)} = \{e\}$. Aus $G^{(r)} \leq N$ folgt nun induktiv $G^{(r+s)} = (G^{(r)})^{(s)} \leq N^{(s)} = \{e\}$. □

Proposition 2.2. Sei G eine endliche p-Gruppe mit $|G| = p^n$, $p \in \mathbb{P}$ prim, $n \geq 1$. Dann existiert zu jeder Primzahlpotenz $p^i, 0 \leq i \leq n$, eine normale Untergruppe $H_i \trianglelefteq G$ der Ordnung $|H_i| = p^i$.

Beweis. Wir führen den Beweis mittels vollständiger Induktion nach n. Für $n = 1$ wählen wir $H_0 = \{e\}$ und $H_1 = G$. Sei nun $n > 1$ und die Aussage für alle p-Gruppen der Ordnung p^{n-1} gezeigt. Weil G eine nicht-triviale p-Gruppe ist folgt aus Lemma 2.7 $Z(G) \neq \{e\}$. Nach dem Satz von Cauchy existiert daher ein $z \in Z(G)$ mit $\operatorname{ord}(z) = p$. Sei $Z := \langle z \rangle$; dann gilt $Z \leq Z(G)$, also insbesondere $Z \trianglelefteq G$ und $|Z| = p$. Es folgt $|G/Z| = \frac{|G|}{|Z|} = \frac{p^n}{p} = p^{n-1}$. Nach Induktionsvoraussetzung besitzt G/Z für jedes $0 \leq i \leq n-1$ einen Normalteiler $\overline{H_i} \trianglelefteq G/Z$ der Ordnung $|\overline{H_i}| = p^i$. Sei nun $\pi : G \to G/Z$ die natürliche Projektion und setze $H_{i+1} := \pi^{-1}(\overline{H_i})$. Dann gilt $H_{i+1} \trianglelefteq G$ und ferner

$$|H_{i+1}| = |Z|\,|\overline{H_i}| = p \cdot p^i = p^{i+1}.$$

Zusammen mit $H_0 := \{e\}$ erhalten wir somit für jedes $0 \leq i \leq n$ einen Normalteiler $H_i \trianglelefteq G$ mit $|H_i| = p^i$. □

Folgerung 2.1. Jede endliche p-Gruppe ist auflösbar.

Beweis. Sei G eine endliche p-Gruppe mit $|G| = p^n$ für $p \in \mathbb{P}, n \geq 0$. Wir führen den Beweis mittels vollständiger Induktion nach n. Für $n = 0$ ist $G = \{e\}$ und somit auflösbar. Sei nun $n \geq 1$ und die Aussage für alle p-Gruppen der Ordnung p^{n-1} gezeigt. Nach Proposition 2.2 existiert ein Normalteiler $N \trianglelefteq G$ mit $|N| = p^{n-1}$. Nach Induktionsvoraussetzung ist N auflösbar und es gilt $|G/N| = \frac{|G|}{|N|} = p$, also ist G/N eine Gruppe von Primordnung, damit zyklisch, insbesondere abelsch und somit auflösbar. Nach Lemma 2.8 ist folglich auch G auflösbar. □

Der Name „Erster Sylowsatz“ deutet auf die Existenz eines zweiten Sylowsatzes hin. In der Tat, es gibt sogar einen dritten. Der Vollständigkeit halber erwähnen wir diese, werden aber nicht weiter Gebrauch davon machen. Für den Beweis des dritten Sylowsatzes verweisen wir auf [Lan02], Seite 35.

Satz 2.2. (Zweiter Sylowsatz) Sei G eine endliche Gruppe, $H \leq G$ eine Untergruppe mit $|H| = p^j, j \geq 0$, $p \in \mathbb{P}$ eine Primzahl und P eine p-Sylow-Untergruppe von G. Dann ist H zu einer Untergruppe von P konjugiert, i.e. es gibt ein $g \in G$ mit $gHg^{-1} \leq P$.

Beweis. Sei $S := G/P = \{gP \mid g \in G\}$ die (nicht-leere) Menge der Linksnebenklassen von P in G, auf der H vermöge der Linkstranslation „$*$“ operiert, i.e. $h * (gP) = (hg)P$. Wir betrachten die Menge $S_0 = \{gP \in S \mid \forall h \in H : h * (gP) = gP\}$ aus Lemma 2.3 und erhalten, dass $|S_0| \equiv |S| \pmod{p}$. Aber es ist $|S| = |G/P| = [G:P]$ und $p \nmid [G:P]$. Daher $|S_0| \neq 0$ und es gibt $gP \in S_0$. Für dieses Element gilt nun

$$\begin{aligned} gP \in S_0 &\Leftrightarrow \forall h \in H : (hg)P = gP \\ &\Leftrightarrow \forall h \in H : (g^{-1}hg)P = P \\ &\Leftrightarrow \forall h \in H : g^{-1}hg \in P \\ &\Leftrightarrow g^{-1}Hg \subseteq P, \end{aligned}$$

i.e. $g^{-1}Hg \leq P$. □

Insbesondere sind je zwei p-Sylow-Untergruppen einer gegeben Gruppe G zueinander konjugiert. Folglich ist eine p-Sylow-Untergruppe genau dann normal in G, wenn sie die eindeutige p-Sylowgruppe von G ist.

Satz 2.3. (Dritter Sylowsatz) Sei G eine endliche Gruppe und $p \in \mathbb{P}$ eine Primzahl. Dann ist die Anzahl der p-Sylow-Untergruppen ein Teiler von $|G|$ und von der Form $1 + kp$ mit $k \in \mathbb{N}_0$.

4 Moduln

Kommen wir nochmal zurück zum Ersten Sylowsatz: Gibt es eine Verbesserung seiner Aussage für abelsche Gruppen? Um diese Frage zu beantworten, nehmen wir einen Umweg über Vektorräume, nun im Gewand der Gruppenaktionen.

1 Struktursatz

Sei K ein Körper, V ein K-Vektorraum, betrachtet als die abelsche Gruppe $(V, +)$ zusammen mit der Gruppenaktion „$\cdot$“ aus Beispiel 2.1.

Definition 1.1. (1) Sei $R = (R, +_R, \cdot_R)$ ein kommutativer Ring mit Eins $1_R \neq 0_R$ und $(M, +_M)$ eine abelsche Gruppe zusammen mit einer Abbildung

$$R \times M \to M, \quad (r, m) \mapsto r \cdot m,$$

die erfüllt:

(1) $1_R \cdot m = m$ für alle $m \in M$.

(2) $(a \cdot_R b) \cdot m = a \cdot (b \cdot m)$ für alle $a, b \in R$ und $m \in M$.

(3) $(a +_R b) \cdot m = a \cdot m +_M b \cdot m$ und $a \cdot (m +_M n) = a \cdot m +_M a \cdot n$ für alle $a, b \in R$ und $m, n \in M$.

Dann heißt $(M, \cdot)$ ein R-Modul oder ein Modul über R.

(2) Sei $(M, \cdot)$ ein R-Modul. Eine Untergruppe $N \leq M$ heißt R-Untermodul, sofern $r \cdot n \in N$ für alle $r \in R$ und $n \in N$.

Beispiel 1.1. (1) Ist R ein Körper, so sind die R-Moduln genau die R-Vektorräume.

(2) Der Produktring $M = R \times \cdots \times R = R^n$ mit $n \geq 1$ ist ein R-Modul mit „$\cdot$“ gegeben durch komponentenweise Multiplikation in R. Konkret, $r \cdot (a_1, \ldots, a_n) = (r \cdot a_1, \ldots, r \cdot a_n)$. Wir nennen dann R einen *freien R-Modul vom Rang n*. Freie Module sind also jene, die, analog zu Vektorräumen, über eine Art Basis verfügen.

(3) Die Ideale $I \trianglelefteq R$ eines kommutativen Rings R mit $1_R \neq 0_R$ sind genau die R-Untermoduln von R.

(4) Sei $(M, \cdot)$ ein R-Modul und N ein R-Untermodul. Da $N \leq M$ und M abelsch ist, ist $N \trianglelefteq M$ und die Quotientengruppe M/N ist wohldefiniert. Insbesondere ist M/N ein R-Modul vermöge

$$\cdot : R \times M/N \to M/N, (r, m+N) \mapsto r \cdot (m+N) := r \cdot m + N.$$

Wir nennen M/N dementsprechend einen *Quotientenmodul*.

(5) Jede abelsche Gruppe kann als $\mathbb{Z}$-Modul betrachtet werden mit der Skalarmultiplikation

$$\mathbb{Z} \times G \to G, (m, g) \mapsto m \cdot g := g^m.$$

Diese Sichtweise wird uns später zum Klassifikationssatz der endlich erzeugten abelschen Gruppen führen.

Definition 1.2. Es seien $M = (M, \cdot_M)$ und $N = (N, \cdot_N)$ R-Moduln. Ein Gruppenhomomorphismus $f : (M, +_M) \to (N, +_N)$ heißt R-Modul-Homomorphismus (oder Homomorphismus der R-Moduln M und N), wenn $f(r \cdot_M m) = r \cdot_N f(m)$ für alle $r \in R$ und $m \in M$.

Wie im Fall von Gruppen und Ringen sind dann $\ker f := \{m \in M \mid f(m) = 0\}$ und $\operatorname{im} f := \{m \in N \mid \exists m \in M : f(m) = n\}$, der Kern bzw. das Bild von f, R-Untermoduln von M bzw. N. Ebenso nennen wir einen injektiven Homomorphismus einen Monomorphismus bzw. Einbettung und einen surjektiven Homomorphismus einen Epimorphismus. Im bijektiven Fall sprechen wir wie gewohnt von einem Isomorphismus und schreiben $M \cong N$.

Es gilt (mit demselben Beweis wie in der linearen Algebra) der Erste Isomorphiesatz für R-Moduln.

Satz 1.1. (Erster Isomorphiesatz für R-Moduln) Seien M und N Moduln über dem Ring R und $f : M \to N$ ein R-Modul-Homomorphismus. Dann ist

$$\tilde{f} : M/\ker f \to \operatorname{im} f, \quad \tilde{f}(m + \ker f) := f(m)$$

ein wohldefinierter R-Modul-Isomorphismus.

Ist M ein R-Modul, $X \subseteq M$ eine nichtleere Teilmenge von M, so ist der Durchschnitt aller R-Moduln, die X enthalten, ein R-Untermodul von M, der X enthält. Wir schreiben dann $\langle X \rangle$ und nennen ihn den *von X erzeugten R-Untermodul von M*. Gibt es eine endliche Teilmenge $X \subseteq M$ mit $\langle X \rangle = M$, so nennen wir M *endlich erzeugt*.

Der wichtigste Satz über Moduln:

Satz 1.2. (Struktursatz für endlich erzeugte Moduln über Hauptidealringen) Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann:

(1) Es existieren $d_1, \dots, d_s \in R \setminus \{0\}$, nicht Einheiten, mit $d_1 \mid d_2 \mid \cdots \mid d_s$ und $p \in \mathbb{N}_0$ mit

$$M \cong \bigoplus_{i=1}^{s} R/(d_i) \oplus R^p.$$

(2) Sind $c_1, \dots, c_t \in R \setminus \{0\}$ ebenfalls nicht Einheiten mit $c_1 \mid c_2 \mid \cdots \mid c_t$ und $q \in \mathbb{N}_0$ sodass

$$M \cong \bigoplus_{i=1}^{t} R/(d_i) \oplus R^q,$$

dann gilt $s = t$, $p = q$ und $c_j \sim d_j$ für $1 \leq j \leq s = t$.

Beweis. Siehe [Lu26]. □

2 Anwendungen des Struktursatzes

Mit folgendem Satz können wir eine alternative Darstellung gewinnen. Er findet seinen Ursprung in der Zahlentheorie. Formuliert wurde er bereits ca. 300 – 500 n. Chr. in den sogenannten 孫子算經 (*Sūnzǐ Suànjīng*).

Satz 2.1. (Chinesischer Restsatz) Sei R ein Hauptidealring und seien $q_1, \dots, q_k \in R$ paarweise teilerfremd, d.h. $\mathrm{ggT}(q_i, q_j) = 1$ für alle $i \neq j$. Dann ist die Abbildung

$$R/(q_1\, q_2 \cdots q_k) \to (R/(q_1)) \times (R/(q_2)) \times \cdots \times (R/(q_k)),$$

definiert durch $r + (q_1\, q_2 \cdots q_k) \mapsto (r + (q_1), r + (q_2), \dots, r + (q_k))$ ein Ringisomorphismus.

Beweis. Man überprüft sofort, dass die gegebene Abbildung tatsächlich ein Ringisomorphismus ist. □

Zusammen mit dem Struktursatz führt uns das zur Klassifikation der endlich erzeugten abelschen Gruppen:

Satz 2.2. (Hauptsatz für endlich erzeugte abelsche Gruppen) Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $k \geq 0, t \geq 0$ und eindeutig bestimmte (bis auf Umordnung) Primzahlpotenzen $n_1, \dots, n_t \geq 1$ (nicht notwendigerweise verschieden), sodass

$$G \cong \mathbb{Z}^k \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{n_t}\mathbb{Z}.$$

Folgerung 2.1. Es sei G eine endliche abelsche Gruppe, $|G| = m$ und $k \mid m$ mit $k \geq 1$. Dann existiert eine Untergruppe $H \leq G$ mit $|H| = k$.

Beweis. Schreibe $G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{n_t}\mathbb{Z}$ wie im Hauptsatz für endlich erzeugte abelsche Gruppen. Dann gilt offenbar $m = \prod_{i=1}^{t} p_i^{n_i}$ und daher existieren $k_i \in \mathbb{N}_0, k_i \leq n_i$, mit $k = \prod_{i=1}^{t} p_i^{k_i}$. Nach Korollar 1.2 können wir Untergruppen $H_i \leq \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ mit $|H_i| = p_i^{k_i}$ finden. Setze nun $H := H_1 \times \cdots \times H_t$. Dann ist $|H| = |H_1| \cdots |H_t| = p_1^{k_1} \cdots p_t^{k_t} = k$. Also existiert eine Untergruppe von G mit k Elementen. □

Satz 2.3. Es sei G eine endliche Gruppe. Dann ist G genau dann zyklisch, wenn zu jedem positiven Teiler $d \geq 1$ von $|G|$ genau eine Untergruppe $H \leq G$ mit $|H| = d$ existiert.

Bevor wir diesen Satz beweisen, zeigen wir noch folgendes Lemma.

Lemma 2.1. Sei φ die Euler'sche φ-Funktion und $n \in \mathbb{N}$. Dann gilt $\sum_{d|n} \varphi(d) = n$.

Beweis. Betrachten wir die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$. Sei $d \mid n$ ein Teiler von n. Dann existiert eine zyklische Untergruppe von $\mathbb{Z}/n\mathbb{Z}$, die isomorph zu $\mathbb{Z}/d\mathbb{Z}$ ist. Weil für $a \in \mathbb{Z}/d\mathbb{Z}$ gilt $\operatorname{ord}(a) = \frac{d}{\operatorname{ggT}(a,d)}$ folgt insbesondere, dass $\mathbb{Z}/d\mathbb{Z}$ genau $\varphi(d)$ Erzeuger hat. Es folgt

$$n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d|n} |\{a \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ord}(a) = d\}| = \sum_{d|n} \varphi(d),$$

wie gewünscht. □

Nun zum Beweis des Satzes:

Beweis. Eine Richtung ist genau Folgerung 1.2. Um die andere Richtung zu zeigen, sei $n = |G|$ und setze $a_d := |\{g \in G \mid \operatorname{ord}(g) = d\}|$ für alle Teiler $d \mid n$. Dann folgt $\sum_{d|n} a_d = n$. Sei $g \in G$ beliebig mit Ordnung $d = \operatorname{ord}(g)$. Nach Annahme existiert eine eindeutige Untergruppe H_d mit $\langle g \rangle = H_d$. Es gibt nun zwei Fälle. Falls H_d zyklisch ist, folgt $a_d = \varphi(d)$. Falls H_d nicht zyklisch ist, folgt sofort $a_d = 0$. Insgesamt ergibt sich $a_d \leq \varphi(d)$ für alle $d \mid n$, also

$$n = \sum_{d|n} a_d \leq \sum_{d|n} \varphi(d) = n.$$

Es muss also Gleichheit für alle Teiler $d \mid n$ gelten. Insbesondere liefert das für $d = n$, dass $a_n = \varphi(n) > 0$. Das liefert die Existenz eines $g \in G$ mit $\operatorname{ord}(g) = n$, i.e. $\operatorname{ord}(g) = n = |G|$. Folglich gilt $G = \langle g \rangle$, i.e., G ist zyklisch. □

Folgerung 2.2. Es seien G, H endliche zyklische Gruppen. Dann ist $G \times H$ genau dann zyklisch, wenn $\operatorname{ggT}(|G|, |H|) = 1$.

Beweis. Angenommen $|G| = m$ und $|H| = n$ seien teilerfremd. Da G und H zyklisch sind, folgt $G \cong \mathbb{Z}/m\mathbb{Z}$ und $H \cong \mathbb{Z}/n\mathbb{Z}$. Folglich ist $G \times H \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ nach dem Chinesischen Restsatz (da $\operatorname{ggT}(m,n) = 1$) zyklisch.

Umgekehrt, sei $G \times H \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ zyklisch. Dann existiert zu jedem Teiler von $m \cdot n$ genau eine Untergruppe der entsprechenden Ordnung. Aber angenommen $\ell \mid m$ und $\ell \mid n$ für $\ell > 1$, sodass $m/\ell \in \mathbb{N}$ und $n/\ell \in \mathbb{N}$. Dann wären $\left(\frac{m}{\ell}\right)\mathbb{Z}/m\mathbb{Z} \times \{0\}$ und $\{0\} \times \left(\frac{n}{\ell}\right)\mathbb{Z}/n\mathbb{Z}$ verschiedene Untergruppen von G derselben Ordnung; ein Widerspruch. Es folgt $\operatorname{ggT}(m,n) = 1$. □

Literaturverzeichnis

[Con18] Keith Conrad. Zorn's lemma and some applications. https://www.acsu.buffalo.edu/~achirvas/Math461_Fall2018/conrad_zorn.pdf, 2018.

[Cox89] David A. Cox. *Primes of the Form $x^2 + n\,y^2$*. John Wiley & Sons, Hoboken, NJ, 1. edition, 1989.

[Gro23] Harald Grobner. *Smooth-automorphic Forms and Smooth-automorphic Representations*. World Scientific, Singapur, 1. edition, 2023.

[HW60] Godfrey H. Hardy und Edward M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, 4. edition, 1960.

[Kal15] Michael Kaltenbäck. *Fundament Analysis*. Heldermann, Lemgo, 1. edition, 2015.

[Lan02] Serge Lang. *Algebra*. Springer, New York City, NY, 3. edition, 2002.

[Lem04] Franz Lemmermeyer. The euclidean algorithm in algebraic number fields. http://www.fen.bilkent.edu.tr/~franz/publ/survey.pdf, 2004.

[Lu26] Jianghua Lu. *Algebra II*. 3. edition, 2026.

[Mar18] Daniel A. Marcus. *Number Fields*. Springer Nature, Cham, 2. edition, 2018.

[Mil22] James S. Milne. *Fields and Galois Theory*. 5. edition, 2022.