Algebraische Strukturen

Daniele Agostini

6. Februar 2024

Kapitel 1

Gruppen

1.1 Definition von Gruppe

Definition 1.1.1 (Gruppe)**.** Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung

$$\bullet\colon G \times G \to G \qquad (a, b) \mapsto a \bullet b$$

mit drei Eigenschaften:

- *Assoziativität*: Für alle $a, b, c \in G$ gilt: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$.
- *Neutrales Element*: Es gibt ein Element $e \in G$ so, dass $a \bullet e = e \bullet a = a$ für alle $a \in G$.
- *Inverses Element*: Für alle $a \in G$ gibt es ein Element $a^{-1} \in G$ so, dass $a \bullet a^{-1} = a^{-1} \bullet a = e$, wobei e ein neutrales Element von G ist.

Wir schreiben manchmal eine Gruppe als $(G, \bullet)$, um zu zeigen, dass wir die Menge G zusammen mit der Verknüpfung $\bullet$ als Gruppe betrachten. Manchmal schreiben wir einfach G wenn keine Verwechslung möglich ist.

In der Definition steht das *ein* neutrales element und *ein* inverses Element existieren, also prinzipiell können wir zwei haben. Sie sind tatsächlich eindeutig bestimmt:

Proposition 1.1.2. *Sei $(G, \bullet)$ eine Gruppe.*

1. *Seien e, e' zwei neutrale Elementen von G. Dann $e = e'$.*
2. *Sei $a \in G$ und seien $a^{-1}, (a^{-1})'$ zwei Inverse von a. Dann $a^{-1} = (a^{-1})'$.*

Beweis. 1. Da e ein neutrales Element von G ist, wissen wir dass $e' = e \bullet e'$, aber da e' auch ein neutrales Element von G ist, wissen wir dass $e \bullet e' = e$. Es folgt dass $e = e'$.

2. Da $(a^{-1})'$ eine Inversen von a ist, wissen wir dass $e = a \bullet (a^{-1})'$. Wir koennen beide Seiten mit a^{-1} verknupfen:

$$a^{-1} = a^{-1} \bullet e = a^{-1} \bullet (a \bullet (a^{-1})') = (a^{-1} \bullet a) \bullet (a^{-1})' = e \bullet (a^{-1})' = (a^{-1})'$$

□

Jetzt können wir "*das* neutrale Element" und "*das* inverse Element" sagen.

1.1.1 Viele Beispiele

Beispiel 1.1.3 (Ganze Zahlen)**.** Das grundlegende Beispiel einer Gruppe ist die Menge $\mathbb{Z}$ von ganzen Zahlen. Die Verknüpfung hier ist die Summe von Zahlen

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad (a, b) \mapsto a + b.$$

Wir überprüfen die drei Eigenschaften:

- Die Summe ist assoziativ: Für alle $a, b, c \in \mathbb{Z}$ gilt, dass $a + (b + c) = (a + b) + c$.
- Die Null ist das neutrale Element: Für alle $a \in \mathbb{Z}$ gilt, dass $a + 0 = 0 + a = a$.
- Das inverse Element einer ganzen Zahl a ist $-a$: $a + (-a) = (-a) + a$.

Beispiel 1.1.4 (Rationale Zahlen ohne Null)**.** Eine andere bekannte Gruppe ist die Menge $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ mit der Verknüpfung Multiplikation:

$$\cdot\colon \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^* \qquad (a, b) \mapsto a \cdot b$$

Diese Verknüpfung ist wohldefiniert, weil, wenn $a, b \in \mathbb{Q}$ beide nicht Null sind, dann ist $a \cdot b$ nicht Null auch. Wir überprüfen die drei Eigenschaften:

- Die Multiplikation ist assoziativ: Für alle $a, b, c \in \mathbb{Q}^*$ gilt, dass $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Die Eins ist das neutrale Element: Für alle $a \in \mathbb{Q}^*$ gilt, dass $a \cdot 1 = 1 \cdot a = a$.
- Das inverse Element von $a \in \mathbb{Q}^*$ ist $a^{-1} = \frac{1}{a}$.

Man kann auf diese Weise zeigen, dass $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ und $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ mit der üblichen Multiplikation zwei Gruppen sind.

Beispiel 1.1.5 (Vektorräume)**.** Ein Beispiel aus der linearen Algebra sind Vektorräume. Jeder Vektorraum V ist eine Gruppe mit der Summe:

$$+\colon V \times V \to V \qquad (u, v) \mapsto u + v$$

Zum Beispiel $\mathbb{R}^2, \mathbb{R}^3, \mathbb{Q}^{2023}$ mit der komponentenweisen Addition sind alle Gruppen. Und die Menge $\mathbb{C}[x]$ von allen komplexen Polynome ist eine Gruppe mit der üblichen Addition von Polynomen.

Beispiel 1.1.6 (Invertierbare Matrizen)**.** Noch ein Beispiel aus der linearen Algebra sind invertierbare Matrizen. Eine reelle $n \times n$ Matrix A heißt invertierbar, wenn eine andere $n \times n$ reelle Matrix A^{-1} existiert, so dass

$$A \cdot A^{-1} = A^{-1} \cdot A = \mathrm{Id}_n \,.$$

Hierbei bezeichnet $A \cdot A^{-1}$ die übliche Matrixmultiplikation und Id_n ist die Einheitsmatrix:

$$\mathrm{Id}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{pmatrix}$$

Sei $GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid A \text{ invertierbar }\}$. Wir wollen zeigen, dass $GL_n(\mathbb{R})$ eine Gruppe mit der üblichen Matrizenmultiplikation ist:

$$\cdot\colon GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \qquad (A, B) \mapsto A \cdot B$$

Diese Verknüpfung ist wohldefiniert: Seien A und B in $GL_n(\mathbb{R})$ zwei invertierbare Matrizen mit Inversen A^{-1} und B^{-1}. Dann ist AB ebenfalls invertierbar, mit dem Inversen $B^{-1}A^{-1}$:

$$B^{-1}A^{-1} \cdot (AB) = B^{-1} \cdot (A^{-1}A) \cdot B = B^{-1} \cdot \mathrm{Id}_n \cdot B = B^{-1} \cdot (\mathrm{Id}_n \cdot B) = B^{-1} \cdot B = \mathrm{Id}_n$$

Wir können auch mit der Determinante argumentieren: Eine reelle Matrix $A \in \mathbb{R}^{n\times n}$ ist invertierbar genau dann, wenn $\det(A) \neq 0$. Wenn A und B beide in $GL_n(\mathbb{R})$ invertierbar sind, dann ist $\det(A)\det(B) \neq 0$, so dass $\det(AB) = \det(A)\det(B) \neq 0$. Das zeigt erneut, dass AB invertierbar ist. Jetzt müssen wir zeigen, dass die Matrixmultiplikation alle drei Eigenschaften erfüllt:

- Die Matrixmultiplikation ist assoziativ: Für alle $A, B, C \in GL_2(\mathbb{R})$ gilt, dass $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.
- Die Einheitsmatrix ist das neutrale Element: Für alle $A \in GL_n(\mathbb{R})$ gilt, dass $A \cdot \mathrm{Id}_n = \mathrm{Id}_n \cdot A = A$.
- Die Matrixinverse ist das Inverse.

Beispiel 1.1.7 (Natürliche Zahlen)**.** Wir sollten auch etwas sehen, das keine Gruppe ist. Betrachten wir die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, \dots\}$ mit der üblichen Summe. Wir überprüfen die drei Eigenschaften einer Gruppe:

- Die Summe ist assoziativ.
- Die Null ist das neutrale Element.
- Das Inverse existiert nicht immer: Für $a \in \mathbb{N}$, $a \neq 0$ und für alle $b \in \mathbb{N}$ haben wir, dass $a + b \neq 0$. Ein Grund ist zum Beispiel, dass aus $a > 0$ und $b \geq 0$ folgt, dass $a + b > 0$. Oder wir können auch mit $\mathbb{Z}$ argumentieren: Ein Inverses von a in $\mathbb{N}$ wäre auch ein Inverses von a in $\mathbb{Z}$. Ein Inverses von a in $\mathbb{Z}$ ist $-a$, und wir wissen, dass es ein einziges Inverses gibt. Also, wenn a ein Inverses in $\mathbb{N}$ haben müsste, dann müsste es $-a$ sein. Aber $-a \notin \mathbb{N}$, wenn $a > 0$.

Bemerkung 1.1.8. Ob eine Menge G eine Gruppe ist oder nicht, hängt nicht nur von der Menge ab, sondern auch von der Verknüpfung. Zum Beispiel, wenn wir sagen, dass "die natürlichen Zahlen keine Gruppe sind", meinen wir eigentlich, dass "die natürlichen Zahlen mit der üblichen Summe keine Gruppe sind". Mit einer anderen Verknüpfung können die natürlichen Zahlen tatsächlich eine Gruppe sein. Zum Beispiel, wir definieren eine Verknüpfung $\oplus$ als die übliche Summe von zwei natürlichen Zahlen in dezimaler Zifferndarstellung, aber ohne Übertrag:

$$489 \oplus 59 = 438, \qquad 489 \oplus 621 = 0.$$

Man sollte also immer klar im Kopf haben, mit welcher Verknüpfung man arbeitet, auch wenn man dies nicht explizit angibt.

Bemerkung 1.1.9. Noch ein Beispiel von eine nicht-Gruppe. Betrachten wir die Menge von komplexe Polynome die nicht Null sind:

$$\mathbb{C}[X]^* = \{f(x) \in \mathbb{C}[X] \mid f(x) \neq 0\}$$

Als Verknüpfung nehmen wir die übliche Multiplikation von Polynome:

$$\cdot : \mathbb{C}[X]^* \times \mathbb{C}[X]^* \to \mathbb{C}[X]^* \qquad (f(x), g(x)) \mapsto f(x) \cdot g(x)$$

Das ist wohldefiniert weil, wenn $f(x), g(x)$ nicht Null sind, denn ist $f(x) \cdot g(x)$ nicht null auch. Wir uberprüfen die drei Eigenschaften:

- Die Multiplikation ist assoziativ.
- Die Eins ist das neutrale Element.
- Das inverse Element existiert nicht immer: betrachten wir zum Beispiel das Polynom $f(x) = x$. Wir zeigen jetzt dass x kein inverses Element hat. Wenn $g(x)$ ein inverses ist, denn $g(x) \cdot x = 1$ und insbesondere $\deg(1) = \deg(g(x)x)$, aber $\deg(g(x)) \geq 0$ für alle $g(x)$ und dann
$$0 = \deg(1) = \deg(g(x)x) = \deg(g(x)) + \deg(x) \geq 0 + 1 = 1$$
Das ist ein Widerspruch. Also, x hat kein inverses in $\mathbb{C}[X]^*$.

Definition 1.1.10 (Kommmutative oder abelsche Gruppe)**.** Eine Gruppe $(G, \bullet)$ heißt kommutativ oder abelsch wenn

$$a \bullet b = b \bullet a \quad \text{für alle} a, b \in G$$

Beispiel 1.1.11. Die Gruppen $(\mathbb{Z}, +), (\mathbb{Q}^*, \cdot)$ oder $(V, +)$, wo V ein Vektorraum ist, sind alle kommutativ. Die Gruppe $(GL_n(\mathbb{R}), \cdot)$ ist nicht Kommutativ wenn $n \geq 2$. Zum Beispiel

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Beispiel 1.1.12 (Restklassen modulo n)**.** Sei $n \in \mathbb{Z}$. Wir definieren die *Kongruenz modulo n* zwischen $a, b \in \mathbb{Z}$ wie folgt:

$$a \equiv b \mod n \qquad \text{genau dann, wenn} \qquad n|(a-b) \text{ in } \mathbb{Z}$$

Wir zeigen dass die Kongruenz modulo n eine Äquivalenzrelation auf $\mathbb{Z}$ ist: wir müssen die drei Eigenschaften einer Äquivalenzrelation uberpr̈ufen.

- Reflexivität: $a \equiv a \mod n$ weil n immer $a - a = 0$ teilt.
- Symmetrie: wenn $a \equiv b \mod n$, denn $b \equiv a \mod n$ auch. Aber das ist einfach, weil $n|(a-b)$ gilt genau dann, wenn $n|(b-a)$ gilt.
- Transitivität: wenn $a \equiv b \mod n$ und $b \equiv c \mod n$, denn $a \equiv c$ auch. Aber das ist einfach, weil $a - c = (a - b) + (b - c)$ so dass, wenn n beide $(a - b)$ und $(b - c)$ teilt, dann n teilt $(a - c)$ auch.

Das zeigt dass die Kongruenz eine Äquivalenzrelation ist. Wir schreiben $\mathbb{Z}/n\mathbb{Z}$ für die Menge von Äquivalenzklassen dieser Relation. Die heißen *Restklassen modulo n*:

$$\mathbb{Z}/n\mathbb{Z} = \{[a] \,|\, a \in \mathbb{Z}\} \qquad [a] = [b] \text{ in } \mathbb{Z}/n\mathbb{Z} \iff a \equiv b \mod n \text{ in } \mathbb{Z}$$

Wir definieren eine Summe auf $\mathbb{Z}/n\mathbb{Z}$ wie folgt:

$$+ \colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad ([a],[b]) \mapsto [a+b]$$

Das ist wohldefiniert: seien $a, b, a'b' \in \mathbb{Z}$ so dass $[a] = [a']$ und $[b] = [b']$ in $\mathbb{Z}/n\mathbb{Z}$. Wir müssen zeigen dass $[a+b] = [a'+b']$ in $\mathbb{Z}/n\mathbb{Z}$. Anders gesagt, wir mussen zeigen dass, wenn $a \equiv a'$ mod n und $b \equiv b'$ mod n gelten, dann gilt $a + b \equiv a' + b'$ mod n auch. Aber das ist einfach, weil

$$a + b - a' - b' = (a - a') + (b - b')$$

und, wenn n beide $a - a'$ und $b - b'$ teilt, dann teilt n $(a - a') + (b - b')$ auch.

Wir zeigen jetzt dass die Menge $\mathbb{Z}/n\mathbb{Z}$ mit dieser Summe eine Gruppe ist:

- Assoziativität: $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c]$ für alle $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$.
- Neutrales Element: $[a] + [0] = [a] = [0] + [a]$ für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$.
- Inverses Element: $[a] + [-a] = [0] = [-a] + [a]$ für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$.

Das zeigt, dass $(\mathbb{Z}/n\mathbb{Z}, +)$ eine Gruppe ist. Außerdem, ist es eine kommutative Gruppe, da $[a] + [b] = [a + b] = [b] + [a]$ für alle $[a], [b] \in \mathbb{Z}$.

Außerdem, $\mathbb{Z}/n\mathbb{Z}$ ist eine endliche Gruppe: erstmal sehen wir dass $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(-n)\mathbb{Z}$ so dass wir koennen annehmen dass $n \geq 0$ ist. Also, sei $n \in \mathbb{N}$, wir wollen zeigen dass $\mathbb{Z}/n\mathbb{Z}$ genau n Elemente hat:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

das bedeutet dass für jede $a \in \mathbb{Z}$ es gibt genau ein $r \in \{0, 1, \ldots, n-1\}$ so dass $[a] = [r]$ n $\mathbb{Z}/n\mathbb{Z}$. Das ist eine einfache Konsequenz von der übliche Division mit Rest: für jede $a \in \mathbb{Z}$ existieren genau ein $k \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots, n-1\}$ so dass

$$a = k \cdot n + r$$

Die Zahlen k und r heißen das Ganzzahlquotient und der Rest von der Division. Insbesonders, sehen wir dass $[a] = [r]$ in $\mathbb{Z}/n\mathbb{Z}$. Angenommen wir dass noch ein $r' \in \{0, 1, \ldots, n-1\}$ existiert, so dass $[a] = [r']$ in $\mathbb{Z}/n\mathbb{Z}$. Dann existiert $k' \in \mathbb{Z}$ so dass $a = \kappa' \cdot n + r'$. Aber, da das Quotient und der Rest von der Division eindeuting bestimmt sind, es muss sein dass $k = k'$ und $r = r'$.

1.1.2 Allgemeine Eigenschaften einer Gruppe

Wir zeigen jetzt manche nutzliche Eigenschaften einer Gruppe:

Proposition 1.1.13. *Sei $(G, \bullet)$ eine Gruppe und $a, b, x \in G$.*

1. *Wenn $a \bullet x = b$ dann $x = a^{-1} \bullet b$.*
   Wenn $x \bullet a = b$ dann $a = b \bullet a^{-1}$.

2. *Wenn $a \bullet x = b \bullet x$, dann $a = b$.*
Wenn $x \bullet a = x \bullet b$, dann $a = b$.

Beweis. 1. Wenn $a \bullet x = b$, dann können wir beide Seite mit a^{-1} von links Verknüpfen und wir bekommen

$$a^{-1} \bullet b = a^{-1} \bullet (a \bullet x) = (a \bullet a^{-1}) \bullet x = e \bullet x = x.$$

Etwas änliches funktioniert wenn $x \bullet a = b$.

2. Wenn $a \bullet x = b \bullet x$, dann können wir beide Seiten mit x^{-1} von rechts Verknüpfen und wir bekommen

$$\begin{aligned}(a \bullet x) \bullet x^{-1} = (b \bullet x) \bullet x^{-1} &\implies a \bullet (x \bullet x{-}1) = b \bullet (x \bullet x^{-1}) \\ &\implies a \bullet e = b \bullet e \implies a = b.\end{aligned}$$

Etwas änliches funktioniert wenn $x \bullet a = x \bullet b$.

□

Bemerkung 1.1.14. Die zweite Eigenschaft in der vorherigen Proposition heißt *Kürzbarkeit.*

Jetzt zeigen wir, wie sich die Inverse in Bezug auf die Verknüpfung verhält

Proposition 1.1.15. *Sei $(G, \bullet)$ eine Gruppe und $a, b \in G$.*

1. *Wenn $a \bullet b = e$ oder $b \bullet a = e$, denn $a = b^{-1}$.*
2. *$(a^{-1})^{-1} = a$.*
3. *$(a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$.*

Beweis. 1. Die Definition sagt dass a das Inverses von b ist, wenn beide Gleichungen $a \bullet b = b \bullet a = e$ gelten. Der Sinn von dieser Proposition ist dass eine Gleichung reicht. Also, angenommen dass $a \bullet b = e$, Proposition 1.1.13 zeigt dass $b = a^{-1} \bullet e = a^{-1}$. Die gleicht Proposition ergibt die Lösung wenn $b \bullet a = e$.

2. Sei $x = a^{-1}$. Wir wollen zeigen dass $x^{-1} = a$. Es reicht zu zeigen dass $a \bullet x = e$, aber $a \bullet x = a \bullet a^{-1} = e$.

3. Sei $x = a \bullet b$. Wir wollen zeigen dass $x^{-1} = b^{-1} \bullet a^{-1}$. Es reicht zu zeigen dass $x \bullet (b^{-1} \bullet a^{-1}) = e$, aber

$$\begin{aligned}x \bullet (b^{-1} \bullet a^{-1}) &= (a \bullet b) \bullet (b^{-1} \bullet a^{-1}) \\ &= a \bullet (b \bullet (b^{-1} \bullet a^{-1})) = a \bullet ((b \bullet b^{-1}) \bullet a^{-1}) \\ &= a \bullet (e \bullet a^{-1}) = a \bullet a^{-1} = e.\end{aligned}$$

□

Bemerkung 1.1.16. In der letzten Beweis haben wir mehrfach die Assoziativität benutzt. Es ist aber manchmal etwas aufwendig, alle Klammern explizit aufzuschreiben, also in der Zukunft schreiben wir in einer Gruppe $(G, \bullet)$ einfach $a \bullet b \bullet c$ statt $(a \bullet b) \bullet c$ oder $a \bullet (b \bullet c)$. Dank die Assoziativität, diese Ausdrücke sind gleich, damit keine Verwechslungsgefahr besteht wenn wir nur $a \bullet b \bullet c$ schreiben. Mit der gleichen Begründung können wir sie auch für mehrere Elemente schreiben so dass der Ausdruck

$$a_1 \bullet a_2 \bullet a_3 \bullet \cdots \bullet a_n$$

ein wohldefiniertes Element von G ist, wenn $a_i \in G$ beliebige Elemente von G sind.

Wir führen jetzt ein bisschen mehr Notation ein: sei $(G, \bullet)$ eine Gruppe und $g \in G$. Für $n \in \mathbb{N}$ definieren wir

$$g^0 = e, \quad g^n = g \bullet g \bullet \cdots \bullet g \ (n \text{ mal}), \quad g^{-n} = g^{-1} \bullet g^{-1} \bullet \cdots \bullet g^{-1} \ (n \text{ mal}), \text{ wenn } n > 0$$

so dass wir eigentlich g^n für alle $k \in \mathbb{Z}$ definiert haben.

Proposition 1.1.17. *Seien $(G, \bullet)$ eine Gruppe und $g \in \mathbb{Z}$ eine Elemente. Dann*

1. *$(g^n)^{-1} = (g^{-1})^n = g^{-n}$ für alle $n \in \mathbb{Z}$.*
2. *$(g^n)^m = g^{n \cdot m}$ für alle $n, m \in \mathbb{Z}$.*
3. *$g^{n+m} = g^n \bullet g^m$ für alle $n, m \in \mathbb{Z}$.*

Außerdem, wenn G kommutativ ist, und $a, b \in G$ dann

4. *$(a \bullet b)^n = a^n \bullet b^n$ für alle $n \in \mathbb{Z}$.*

Beweis. Eine gute Übung.

□

1.2 Untergruppen

Definition 1.2.1 (Untergruppe)**.** Sei $(G, \bullet)$ eine Gruppe. Eine Untergruppe von G ist eine Teilmenge $H \subseteq G$ mit drei Eigenschaften;

1. $e \in H$.
2. wenn $a, b \in H$ dann $a \bullet b \in H$.
3. wenn $a \in H$, dann $a^{-1} \in H$.

Wir schreiben manchmal $H \leq G$ um zu bezeichnen dass H eine Untergruppe von G ist.

Bemerkung 1.2.2. Sei $(G, \bullet)$ eine Gruppe und $H \leq G$ eine Untergruppe. Die Abbildung

$$\bullet \colon H \times H \to H, \qquad (a, b) \mapsto a \bullet b$$

wo $a \bullet b$ die Verknupfung von G ist, ist wohldefiniert, weil wenn $a, b \in H$ dann $a \bullet b$. Diese Abbildung ist eine Verknüpfung auf H, und H mit dieser Verknüpfung ist eine Gruppe: die Assoziativität $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ gilt für alle $a, b, c \in H$ weil sie für alle $a, b, c \in G$ gilt. Außerdem, das neutrales Element in H ist das neutrales element $e \in G$ und das inverses eines Element $a \in H$ ist das inverses $a^{-1} \in G$.

Bemerkung 1.2.3. Wir sollten hier ein wenig vorsichtig sein. Wenn wir sagen, dass eine Untergruppe von $(G, \bullet)$ eine Teilmenge ist, die auch eine Gruppe ist, haben wir immer die Verknupfung $\bullet$ von G im Kopf. Zum Beispiel, $\mathbb{Q}$ ist eine Gruppe mit der Summe und $\mathbb{Q}^*$ ist eine Gruppe mit der Multiplikation, aber $\mathbb{Q}^*$ ist keine Untergruppe von $\mathbb{Q}$ (warum?), obwohl sie eine Teilmenge von $\mathbb{Q}$ ist, die auch eine Gruppe ist.

Von nun an werden wir die Verknüpfung $\bullet$ nicht immer explizit schreiben, wenn keine Verwechslungsgefahr besteht

Beispiel 1.2.4. Sei $n \in \mathbb{Z}$ und $n\mathbb{Z} = \{n \cdot k \,|\, k \in \mathbb{Z}\}$ die Teilmenge von alle Elemente die teilbar durch n sind. Diese ist eine Untergruppe von $\mathbb{Z}$. Wir uberprüfen die drei Eigenschaften:

1. $0 \in \mathbb{Z}$, da $0 = n \cdot 0$.
2. Wenn $a = n \cdot k$ und $b = n \cdot h$ in $\mathbb{Z}$ sind, dann ist $a + b = n \cdot (h + k)$ in $n\mathbb{Z}$ auch.
3. Wenn $a = n \cdot k$ in $n\mathbb{Z}$ ist, dann ist $-a = n \cdot (-k)$ auch.

Zum Beispiel, die Menge $2\mathbb{Z}$ von alle gerade ganze Zahlen ist eine Untergruppe. Ist die Menge von alle ungerade Zahlen eine Untergruppe?

Beispiel 1.2.5. Seien $(G, \bullet)$ eine Gruppe und $g \in G$ ein Element. Wir betrachten die Menge $\langle g \rangle = \{g^n \,|\, n \in \mathbb{Z}\}$. Diese ist eine Untergruppe:

- $e = g^0 \in \langle g \rangle$.
- Wenn $g^n, g^m \in \langle g \rangle$ dann $g^n \bullet g^m = g^{n+m} \in \langle g \rangle$.
- Wenn $g^n \in \langle g \rangle$, dann $(g^n)^{-1} = g^{-n} \in \langle g \rangle$.

Die Untergruppe $\langle g \rangle$ heißt die Untergruppe erzeugt von g. Zum Beispiel, die Untergruppe $< n >$ erzeugt von n in $\mathbb{Z}$ ist genau $n\mathbb{Z}$.

Beispiel 1.2.6. Sei $\mathbb{K}$ ein Körper und $GL_n(\mathbb{K})$ die Gruppe von invertierbare Matrizen. Die Teilmenge $SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \,|\, \det(g) = 1\}$ ist eine Untergruppe von $GL_n(\mathbb{K})$. Wir uberprüfen die drei Eigenschaften:

1. $\det(\mathrm{Id}) = 1$.
2. Wenn $\det(A) = \det(B) = 1$ dann $\det(A \cdot B) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$.
3. Wenn $\det(A) = 1$, dann $\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$.

Die Gruppe $SL_n(\mathbb{K})$ heißt die spezielle lineare Gruppe.

Beispiel 1.2.7. Wir betrachten $\mathbb{C}^*$ mit der Multiplikation als Gruppe. Die Menge $S^1 = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$ ist eine Untergruppe. Wir ubeprüfen die drei Eigenschaften:

1. $1 \in S^1$.
2. wenn $a, b \in S^1$ dann $|ab| = |a| \cdot |b| = 1 \cdot 1 = 1$.
3. wenn $a \in S^1$, dann $|a^{-1}| = |a|^{-1} = 1^{-1} = 1$.

Die Menge $\mu_n = \{z \in \mathbb{C}^* \,|\, z^n = 1\}$ ist eine Untergruppe von S^1, sodass sie auch eine Untergruppe von $\mathbb{C}^*$ ist. Wir uberprüfen die drei Eigenschaften:

1. $1^n = 1$, so dass $1 \in \mu_n$.
2. wenn $a^n = 1$ und $b^n = 1$, dann $(ab)^n = a^n \cdot b^n = 1 \cdot 1 = 1$.

3. wenn $a^n = 1$, dann $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$.

Sei $\zeta_n = e^{\frac{2\pi i}{n}}$. Wir sehen dass $\langle\zeta\rangle = \left\{\zeta^k \mid k \in \mathbb{Z}\right\}$ und für alle $k \in \mathbb{Z}$ sehen wir dass $(\zeta^k)^n = (\zeta^n)^k = 1^k = 1$, also $\langle\zeta\rangle \subseteq \mu_n$. Außerdem wißen wir dass wenn $z^n = 1$, dann $z = \zeta^k$ für ein $k \in \mathbb{Z}$. Also, $\mu_n = \langle\zeta\rangle$.

Proposition 1.2.8. *Sei $(G, \bullet)$ eine Gruppe.*

1. *Seien $H_1, H_2 \subseteq G$ zwei Untergruppen, dann $H_1 \cap H_2$ ist auch eine Untergruppe.*

2. *Sei $(H_i \mid i \in I)$ eine Familie von Untergruppen von G, dann $\cap_{i\in I} H_i$ ist eine Untergruppe.*

Beweis. Da (1) ein Spezialfall von (2) ist, genügt es, (2) zu Zeigen. Sei $H = \cap_{i\in I} H_i$. Es ist einfach zu zeigen dass H eine Untergruppe ist: z.B. da jede H_i eine Untergruppe ist, wissen wir dass $e \in H_i$ für alle $i \in I$, so dass $e \in H$ auch. Eine ähnliche Argumentation zeigt, dass H durch die Verknüpfung und die Inversen geschlossen ist. □

Bemerkung 1.2.9. Die Vereinigung von Untergruppen ist im Allgemeinen keine Untergruppe. Z. B. $2\mathbb{Z}$ und $3\mathbb{Z}$ sind zwei Untergruppen von $\mathbb{Z}$ aber $2\mathbb{Z} \cup 3\mathbb{Z}$ ist keine Untergruppe: $2 \in 2\mathbb{Z}$ und $3 \in 3\mathbb{Z}$, aber $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Deswegen haben wir die folgende Definition:

Definition 1.2.10 (Erzeugte Untergruppe)**.** Sei $(G, \bullet)$ eine Gruppe und $S \subseteq G$ eine Menge. Die Untergruppe erzeigt von S ist

$$\langle S\rangle = \bigcap_{\substack{H\leq G,\\ S\subseteq H}} H$$

Bemerkung 1.2.11. Die Untergruppe $\langle S\rangle$ ist die kleinste Untergruppe die S enthalt. Dass bedeutet dass, wenn $H \leq G$ eine Untergruppe ist, so dass $S \subseteq H$, dann $\langle S\rangle \leq H$.

Beispiel 1.2.12. Sei G eine Gruppe und $g \in G$ ein Element. Die Untergruppe $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$ ist genau die Untergruppe erzeugt von G.

Beispiel 1.2.13. Sei G eine *kommutative* Gruppe, und seien $a, b \in G$ zwei Elementen. Wir sagen, dass

$$\langle a, b\rangle = \{a^n b^m \mid n, m \in \mathbb{Z}\}.$$

Wenn G eine Kommutative gruppe ist und $S \subseteq G$ eine Teilmenge ist, dann haben wir

$$\langle S\rangle = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in S, n_i \in \mathbb{Z}\}$$

Ist das noch wahr wenn G nicht kommutativ ist?

1.2.1 Nebenklassen

Definition 1.2.14 (Nebenklasse)**.** Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Sei auch $g \in G$ ein Element. Die Nebenklasse von g ist die Menge

$$gH = \{gh \mid h \in H\}$$

Bemerkung 1.2.15. Die Menge gH ist, genauer gesagt, die Linksnebenklasse von g. Die Rechtsnebenklasse von g ist die Menge

$$Hg = \{hg \,|\, h \in H\}$$

Wir werden normalerweise mit Linksnebenklassen arbeiten, und wir werden einfach "Nebenklassen" nutzen.

Lemma 1.2.16. *Seien G eine Gruppe, H eine Untergruppe und g_1H und g_2H zwei Nebenklassen. Die folgende Aussage sind Äquivalent:*

1. $g_2^{-1}g_1 \in H$.
2. $g_1 \in g_2H$.
3. $g_1H = g_2H$.

Beweis. (1) $\implies$ (2): Wenn $h \in H$ existiert so dass $g_2^{-1}g_1 = h$, dann können wir beide Seiten mit g_2 verknüpfen und wir bekommen $g_1 = g_2h \in g_2H$.

(2) $\implies$ (3): Wenn $g_1 \in g_2H$, dann existiert $h \in H$ so dass $g_1 = g_2h$. Wir zeigen dass $g_1H = g_2H$. Sei $h' \in H$: dann $g_1h' = g_2hh' \in g_2H$, da $hh' \in H$. Das zeigt dass $g_1H \subseteq g_2H$. Außerdem, $g_2h' = g_1h^{-1}h' \in g_1H$, da $h^{-1}h \in H$. Das zeigt dass $g_2H \subseteq g_1H$, so dass $g_1H = g_2H$.

(3) $\implies$ (1): $g_1 = g_1e \in g_1H$ so dass $g_1 \in g_2H$ auch, weil $g_1H = g_2H$. Dann existiert $h \in H$ so dass $g_1 = g_2h$, oder, anders ausgedrückt, $g_2^{-1}g_1 = h$. □

Proposition 1.2.17. *Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Zwei Nebenklassen g_1H, g_2H sind entweder gleich oder disjunkt: entweder $g_1H = g_2H$ oder $g_1H \cap g_2H = \emptyset$.*

Beweis. Wir müssen zeigen, dass wenn $g_1H \cap g_2H \neq \emptyset$, dann $g_1H = g_2H$. Sei $x \in g_1H \cap g_2H$. Dann existieren $h_1, h_2 \in H$ so dass $x = g_1h_1 = g_2h_2$ so dass $g_1 = g_2h_2h_1^{-1}$. Da $h_2h_1^{-1} \in H$, wissen wir dass $g_1 \in g_2H$, und dann $g_1H = g_2H$. □

Definition 1.2.18 (Kongruenz modulo H)**.** Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Wir definieren die relation von Kongruenz modulo H auf G als:

$$a \equiv b \mod H \quad \iff \quad b^{-1}a \in H$$

Lemma 1.2.19. *Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Die Kongruenz modulo H ist eine Äquivalenzrelation und die Äquivalenzklassen sind genau die Nebenklassen. Wir bezeichnen die Quotientmengen mit G/H.*

Beweis. Die Relation $a \equiv b \mod H$ ist definiert als $b^{-1}a \in H$ und wir haben schon gezeigt dass dies äquivalent ist zu $aH = bH$. Es ist jetzt einfach zu zeigen dass diese eine Äquivalenzrelation ist. Die Äquivalenzklasse von $a \in G$ ist die Menge von alle $b \in G$ so dass $a \equiv b \mod H$, oder, änders gedruckt die Menge von alle $b \in H$ so dass $aH = bH$. Wir haben schon gezeigt dass diese Menge genau die Nebenklasse aH ist. □

Bemerkung 1.2.20. Die Menge G/H ist definiert als die Menge von alle Äquivalenzklassen der Kongruenz modulo H. Das ist die Menge von alle Nebenklassen: $G/H = \{gH \,|,\ g \in G\}$. Wir werden auch die Notation $[g] \in G/H$ verwenden.

Definition 1.2.21 (Index einer Untergruppe)**.** Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Der Index $[G : H]$ von H in G ist die Anzahl von verschiedenen Nebenklassen von H in G, oder, anders ausgedrückt, die Kardinalität von G/H.

Der Index kann endlich oder unendlich sein. Wenn die Gruppe G endlich ist, dann ist der Index immer endlich und wir haben eine nutzliche Formel:

Satz 1.2.1 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe.*

$$|G/H| = \frac{|G|}{|H|}.$$

Beweis. Erstmals sei gH eine Nebenklassen von H. Die Abbildung

$$H \to gH, \quad h \mapsto gh$$

ist injektiv weil wenn $gh_1 = gh_2$ dann $h_1 = h_2$. Die Abbildung ist auch surjektiv wegen die Definition von gH. Die Abbildung ist deswegen bijektiv, so dass $|gH| = |H|$: alle Nebenklassen haben die selbe Kardinalität.

Sei $|G/H| = r$ so dass $G/H = \{g_1H, g_2H, \ldots, g_rH\}$ mit g_iH paarweise verschieden Nebenklassen. Die Gruppe G ist die disjunkte Vereinigung der Nebenklassen $G = \bigcup_{i=1}^{r} g_iH$, und wir haben schon gezeigt dass $|g_iH| = |H|$ für alle i, so dass

$$|G| = \sum_{i=1}^{r} |g_iH| = \sum_{i=1}^{r} |H| = r \cdot |H|.$$

□

Dieser Satz kann man kurz beweisen aber er hat viele Konsequenzen. Bevor wir manche von diese zeigen, führen wir ein bisschen mehr Notation ein.

Definition 1.2.22 (Ordnung einer Gruppe)**.** Die Ordnung einer Gruppe G ist die Mächtigkeit $|G|$.

Definition 1.2.23 (Ordnung eines Elementes)**.** Seien G eine Gruppe und $g \in G$ ein Element. Die Ordnung $\mathrm{ord}(g)$ von g ist das kleinstes $n \in \mathbb{N}, n > 0$ so dass

$$g^n = e$$

Wenn kein solches n existiert, sagen wir dass die Ordnung von G unendlich ist.

Bemerkung 1.2.24. Diese zwei Definitionen sind kompatibel: die Ordnung von $g \in G$ ist auch die Ordnung von der Untergruppe $\langle g \rangle \leq G$. Zuerst zeigen wir, dass wenn $g \in G$ Ordnung $n \in \mathbb{N}$ hat, dann $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$. Sei $h \in \mathbb{Z}$ dann können wir schreiben $h = k \cdot n + r$ wo $k \in \mathbb{Z}$ und $r \in \{0, \ldots, n-1\}$. Es folgt dass $g^h = h^{k \cdot n + r} = g^{k \cdot n} g^r = (g^n)^k \cdot g^r = e^k \cdot g^r = g^r$. Das zeigt dass $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, wir müssen auch zeigen dass diese Elementen paarweise disjunkt sind. Seien $0 \leq i < j \leq n-1$ so dass $g^j = g^i$, dann $g^{j-i} = e$ aber das ist ein Widerspruch, da $0 < j - i < n$ und n die Ordnung von g ist.

Wenn die Ordnung von g unendlich ist, dann ist es einfach zu zeigen dass die Menge $\langle g \rangle$ auch unendlich ist.

Korollar 1.2.25. *Sei G eine endliche Gruppe.*

1. *Die Ordnung von einer Untergruppe H teilt die Ordnung von G.*
2. *Die Ordnung von einem Element $g \in G$ teilt die Ordnung von G.*
3. *$g^{|G|} = e$ für alle $g \in G$.*

Beweis. 1. $|G| = |G/H| \cdot |H|$.

2. Die Ordnug $\mathrm{ord}(g)$ ist die Ordnung der Untergruppe $\langle g \rangle$.
3. Da $\mathrm{ord}(g)||G|$, existiert $h \in \mathbb{Z}$ so dass $|G| = h \cdot \mathrm{ord}(G)$. Dann $g^{|}G| = g^{h \cdot \mathrm{ord}(G)} = (g^{\mathrm{ord}(G)})^h = e^h = e$.

□

Korollar 1.2.26. *Sei G eine endliche Gruppe von Primzahlordnung. Dann ist G zyklisch.*

Beweis. Sei $g \in G, g \neq e$ (warum existiert so ein g?), dann $|\langle g \rangle|$ teilt $|G|$ und $|\langle g \rangle| > 1$. Da $|G|$ ein Primzahl ist, es muss sein dass $|\langle g \rangle| = |G|$. □

Beispiel 1.2.27 (Untergruppen von $\mathbb{Z}$)**.** Wir zeigen dass alle Untergruppe von $\mathbb{Z}$ sind zyklisch. Die Untergruppe $\{0\}$ ist sicher zyklisch. Sei denn $H \leq \mathbb{Z}$ eine Untergruppe, $H \neq \{0\}$. Wir wollen zeigen dass $H = n\mathbb{Z}$, wo $n = \min\{h \in H \mid h > 0\}$. Wir zeigen zuerst dass die Menge $\{h \in H \mid h > 0\}$ nicht leer ist: da $H \neq \{0\}$ existiert $h \in H, h \neq 0$. Wenn $h > 0$ erledigt, wenn $h < 0$, dann $-h \in H$ und $-h > 0$. Die Menge $\{h \in H \mid h > 0\}$ ist dann nicht leer und hat ein Minimum n. Sei jetzt $h \in H$: dank der Division mit Rest, existieren $k \in \mathbb{Z}$ und $0 \leq r \leq n-1$ so dass $h = k \cot n + r$. Dann $r = h - k \cdot n$ ist in H, weil $h, n \in H$ und die einzige Möglichkeit ist dass $r = 0$. Das zeigt dass $h = k \cdot n$, also $H = n\mathbb{Z}$.

1.2.2 Normale Untergruppe und Faktorgruppen

Wir haben früher gesehen dass $\mathbb{Z}/n\mathbb{Z}$ mit der Verknüpfung $[a]+[b] = [a+b]$ eine Gruppe ist. Gilt dass für alle Menge G/H? Genauer gesagt, seien G eine Gruppe und $H \leq G$ eine Untergruppe. Wir köennen eine Vernküpfung auf G/H durch

$$G/H \times G/H \mapsto G/H, \qquad ([a],[b]) \mapsto [ab]$$

definieren und vielleicht ist mit dieser G/H eine Gruppe. Das Problem ist dass diese Vernküpfung nicht wohldefiniert ist! Seien $a', b' \in G$ so dass $[a'] = [a]$ und $[b'] = [b]$ in G/H. Wir müssen uberprüfen ob $[ab] = [a'b']$ in G/H. Anders ausgedruckt, wir wissen dass $a' \in aH, b' \in bH$ und wir müssen beweisen dass $a'b' \in abH$. Aber das ist nicht immer wahr, die Untergruppen mit dieser Eigenschaft sind spezielle Untergruppe:

Definition 1.2.28 (Normale Untergruppe)**.** Sei G eine Gruppe. Ein Normalteiler oder normale Untergruppe von G ist eine Untergruppe $H \leq G$ so dass

$$gHg^{-1} \subseteq H \qquad \text{für alle } g \in G.$$

Wenn H eine normale Untergruppe von G ist, schreiben wir $H \trianglelefteq G$.

Proposition 1.2.29. *Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Die folgende Aussage sind äquivalent:*

1. *H ist eine normale Untergruppe von G.*
2. *$gHg^{-1} = H$ für alle $g \in G$.*
3. *$gH = Hg$ für alle $g \in G$.*
4. *$aHbH = abH$ für alle $a, b \in G$.*
5. *Die Vernküpfung*
$$G/H \times G/H \to G/H \qquad ([a], [b]) \mapsto [ab]$$
ist wohldefiniert und macht G/H zu einer Gruppe.

Beweis. (1) $\implies$ (2): Wir müssen beweisen dass $H \subseteq gHg^{-1}$, die andere Inklusion folgt von der Definition von Normalteiler. Sei $h \in H$. Da H eine normale Untergruppe ist, wissen wir dass $g^{-1}Hg = g^{-1}H(g^{-1})^{-1} \subseteq H$, so dass $g^{-1}hg = h' \in H$. Und dann $h = gh'g^{-1} \in gHg^{-1}$.

(2) $\implies$ (3): Wir verknüpfen $gHg^{-1} = H$ von rechts mit g und wir bekommen $gH = Hg$.

(3) $\implies$ (4): Wir wissen dass $Hb = bH$ so dass $aHbH = abHH$. Wir müssen nur zeigen dass $HH = H$. Aber $HH \subseteq H$ weil H abgeschlossen für die Verknüpfung ist, und $H \subseteq HH$ weil $H = eH \subseteq HH$.

(4) $\implies$ (5): Seien $a', b' \in G$ so dass $[a'] = [a], [b'] = [b]$ in G/H. Dass bedeutet dass $a' = ah_1$ und $b' = bh_2$ für $h_1, h_2 \in H$. Wir müssen beweisen dass $[a'b'] = [ab]$ in G/H. Wir haben $a'b' = ah_1bh_2 = abh_3$, dank unsere Annhame und das bedeutet $[a'b'] = [ab] \in G/H$. Nun ist es eigentlich einfach zu beweisen, dass G/H eine Gruppe ist. Die Assoziativität folgt aus der Assoziativität von G, das neutrale Element ist $[e]$ und das Inverse von $[a]$ ist $[a^{-1}]$.

(5) $\implies$ (1): Seien $g \in G, h \in H$ und $g' = gh$. Die zwei Elemente g, g' sind gleich in G/H so dass $[g'g^{-1}] = [g'][g^{-1}] = [g][g^{-1}] = [gg^{-1}] = [e]$. Das bedeutet $ghg^{-1} = g'g^{-1} \in H$. Da dies für alle g in G und h in H gilt, folgt daraus, dass H normal ist. □

Definition 1.2.30 (Faktorgruppe)**.** Seien G eine Gruppe und $H \trianglelefteq G$ eine normale Untergruppe. Die Menge G/H mit Mit der oben genannten Verknüpfung heißt die Faktorgruppe von G nach H.

Beispiel 1.2.31. Jede Gruppe hat zwei normale Untergruppen G und $\{e\}$.

Beispiel 1.2.32. Sei G eine kommutative Gruppe und $H \leq G$ eine Untergruppe. Für alle $g \in G, h \in H$ gilt dass $ghg^{-1} = gg^{-1}h = eh = h$, so dass $gHg^{-1} = H$ auch. Das bedeutet dass jede Untergruppe einer kommutative Gruppe normal ist.

Beispiel 1.2.33. Sei $\mathbb{K}$ ein Körper. Wir betrachten die Gruppe $GL_2(\mathbb{K})$ und die Untergruppe

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{K} \right\}$$

Man kann uberprüfen dass H eine Untergruppe ist durch die Identität

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 1 & 0 \end{pmatrix} \text{ für alle } a, b \in \mathbb{K}$$

Diese Untergruppe ist aber nicht normal:

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^{-1} = \begin{pmatrix}0 & 1\\ 1 & x\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$$

und die letzte Matrix ist nicht in H wenn $x \neq 0$.

1.3 Homomorphismen

Definition 1.3.1. Seien G und H zwei Gruppen. Eine Abbildung $\phi\colon G \to H$ ist ein Homomorphismus von Gruppen wenn

$$\phi(ab) = \phi(a)\cdot\phi(b) \qquad \text{für alle } a, b \in G$$

Bemerkung 1.3.2. In der Definition $a \cdot b$ bezeichnet die Verknüpfung in G und $\phi(a)\cdot\phi(b)$ bezeichnet die Verknüpfung in H.

Proposition 1.3.3. *Sei $\phi\colon G \to H$ ein Homomorphismus von Gruppen.*

1. *$\phi(e_G) = e_H$ wo e_G und e_H die neutrale Elementen von G und H sind.*
2. *$\phi(a^{-1}) = \phi(a)^{-1}$ für alle $a \in G$.*
3. *Sei $K \leq G$ eine Untergruppe, dann ist $\phi(K) \leq H$ eine Untergruppe.*
4. *Sei $L \leq H$ eine Untergruppe, dann ist $\phi^{-1}(L)$ eine Untergruppe. Außerdem, wenn $L \trianglelefteq K$ eine normale Untergruppe ist, dann ist $\phi^{-1}(L) \trianglelefteq$ eine normale Untergruppe von G*

Beweis.

1. Da $e_G = e_G \cdot e_G$, folgt dass $\phi(e_G)\cdot\phi(e_G) = \phi(e_G)$, und dann $\phi(e_G) = e_H$.
2. Wir haben $\phi(a)\cdot\phi(a^{-1}) = \phi(a\cdot a^{-1}) = \phi(e_G) = e_H$ und das bedeutet dass $\phi(a^{-1}) = \phi(a)^{-1}$.
3. Wir haben $e_G \in K$ so dass $\phi(e_G) = e_H \in \phi(K)$. Sind $k_1, k_2 \in K$, so $\phi(k_1)\phi(k_2) = \phi(k_1k_2) \in \phi(K)$ und $\phi(k_1)^{-1} = \phi(k_1^{-1}) \in \phi(K)$.
4. Die Menge $\phi^{-1}(L)$ ist definiert als $\phi^{-1}(L) = \{x \in G \mid \phi(x) \in L\}$. Wir haben $e_G \in \phi^{-1}(L)$ weil $\phi(e_G) = e_H \in L$. Wenn $a, b \in \phi^{-1}(L)$, dann $\phi(ab) = \phi(a)\phi(b) \in L$ und $\phi(a^{-1}) = \phi(a)^{-1} \in L$, so dass $ab, a^{-1} \in \phi^{-1}(L)$. Angenommen wir dass L eine normale Untergruppe von H ist. Sei $x \in \phi^{-1}(L)$ und $g \in G$, dann $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} \in \phi(g)L\phi(g)^{-1} = L$, so dass $gxg^{-1} \in L$.

□

Definition 1.3.4 (Kern)**.** Der Kern eines Homomorphismus $\phi\colon G \to H$ ist definiert als

$$\ker\phi\colon = \phi^{-1}(\{e_H\}) = \{a \in G \mid \phi(a) = e_H\}$$

Bemerkung 1.3.5. Sei $\phi\colon G \to H$ ein Homomorphismus von Gruppen. Der Kern $\ker\phi$ ist eine normale Untergruppe von G und das Bild $\operatorname{im}\phi$ ist eine Untergruppe von H.

Lemma 1.3.6. *Ein Homomorphismus von Gruppen $\phi\colon G \to H$ ist injektiv genau wann, denn $\ker\phi = \{e_G\}$.*

Beweis. Wir wissen dass $\phi(e_G) = e_H$ für jedes Homomorphismus ϕ, so dass, wenn ϕ injektiv ist, e_G ist das einzige Element, das auf e_h abgebildet wird, und das bedeutet $\ker\phi = \{e_G\}$.

Andererseits, wenn $\ker\phi = \{e_G\}$, seien $a, b \in G$ so dass $\phi(a) = \phi(b)$. Dann $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e_H$ so dass, dank unsere Annehme, $ab^{-1} = e_G$, und $a = b$. □

Beispiel 1.3.7. Sei $n \in \mathbb{Z}$. Wir definieren eine Abbildung $\phi_n \colon \mathbb{Z} \to \mathbb{Z}$ als $\phi_n(k) = n \cdot k$. Diese ist ein Homomorphismus von Gruppen. Das Bild $n\mathbb{Z} \subseteq \mathbb{Z}$ ist eine Untergruppe.

Beispiel 1.3.8. Seien G eine Gruppe und $g \in G$ ein Element. Wir definieren eine Abbildung

$$\phi \colon \mathbb{Z} \to G, \qquad \phi(n) = g^n$$

Da $g^{n+m} = g^n \cdot g^m$, ist diese Abbildung ein Homomorphismus von Gruppen. Das Bild $\langle g \rangle$ ist die Untergruppe von G erzeugt von g. Der Kern von ϕ ist genau die Untergruppe erzeugt von $\mathrm{ord}(g)$.

Beispiel 1.3.9. Sei $\mathbb{K}$ ein Körper. Die Abbildung

$$\det \colon GL_n(\mathbb{K}) \to \mathbb{K}^*, \qquad A \mapsto \det(A)$$

ist ein Homomorphismus, da $\det(AB) = \det(A)\det(B)$. Der Kern ist $SL_n(\mathbb{K})$. Das zeigt dass $SL_n(\mathbb{K})$ eine normale Untergruppe von G ist.

Proposition 1.3.10.
1. *Die Identität* $\mathrm{id}_G \colon G \to G$ *ist ein Homomorphismus für jede Gruppe* G.
2. *Seien* $\phi \colon G \to H$ *und* $\psi \colon H \to K$ *zwei Homomorphismen von Gruppen. Dann ist* $\psi \circ \phi \colon G \to K$ *auch ein Homomorphismus.*
3. *Sei* $\phi \colon G \to H$ *ein Homomorphismus von Gruppen das auch invertierbar ist. Dann ist die inverse Abbildung* $\phi^{-1} \colon H \to G$ *auch ein Homomorphismus.*

Beweis.
1. Einfach.
2. Seien $a, b \in G$, dann $(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a)) \cdot \psi(\phi(b)) = (\psi \circ \phi)(a) \cdot (\psi \circ \phi)(b)$.
3. Seien $x, y \in H$. Wir müssen beweisen dass $\phi^{-1}(xy) = \phi^{-1}(x) \cdot \phi^{-1}(y)$, und da ϕ bijektiv ist, das ist äquivalent zu $\phi(\phi^{-1}(xy)) = \phi(\phi^{-1}(x)\phi^{-1}(y))$. Wir sehen dass $\phi(\phi^{-1}(xy)) = xy$ und $\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy$.

□

Definition 1.3.11 (Isomorphismus)**.** Ein Isomorphismus zwischen zwei Gruppen G, H ist ein invertierbare Homomorphismus $\phi \colon G \to H$. Zwei Gruppen heißen isomorph, wenn zwischen ihnen ein Isomorphismus existiert. Wir schreiben $G \cong H$.

Definition 1.3.12 (Automorphismus)**.** Ein Isomorphismus $\phi \colon G \to G$ heißt Automorphismus.

Beispiel 1.3.13. Sei G eine Gruppe, die Menge $S(G) = \{f \colon G \to G \mid f \text{ invertierbar }\}$ ist eine Gruppe mit der übliche Komposition von Abbildungen. Die Menge $\mathrm{Aut}(G) = \{\phi \colon G \to G \mid \phi\text{isomorphismus}\}$ ist eine Untergruppe von $S(G)$.

Bemerkung 1.3.14. Die Relation $G \cong H$ ist eine Äquivalenzrelation: sie ist reflexiv weil $\mathrm{id}_G \colon G \to G$ ein Isomorphismus für jede Gruppe G ist. Sie ist symmetrisch weil, wenn $\phi \colon G \to H$ ein Isomorphismus von Gruppen ist, dann ist $\phi^{-1} \colon H \to G$ ein Isomorphismus auch. Endlich sie ist transitiv weil, wenn $\phi \colon G \to H$ und $\psi \colon H \to K$ zwei Gruppenisomorphismen sind, dann ist $\psi \circ \phi \colon G \to K$ ein Gruppenisomorphismus: die Komposition von Homomorphismen ist ein Homomorphismus und die Komposition von invertierbare Abbildungen ist eine invertierbare Abbildung.

1.3.1 Die Isomorphiesätze

Homomorphismen und Quotientengruppe sind sehr eng verbundet.

Lemma 1.3.15. *Seien G eine Gruppe und $N \trianglelefteq G$ eine normale Untergruppe. Die Projektion $\pi \colon G \to G/N$ ist ein surjektiv Gruppenhomomorphismus und $\ker \pi = N$.*

Beweis. Die Projektion ist ein Homomorphismus von Gruppen weil $\pi(xy) = [xy] = [x] \cdot [y] = \pi(x) \cdot \pi(y)$. Es ist klar, dass die Projektion surjektiv ist, und

$$\ker \pi = \{x \in G \mid \pi(x) = [e]\} = \{x \in G \mid [x] = [e]\} = N$$

□

Damit ist es einfach, die universelle Eigenschaft der Faktrogruppe zu beweisen

Satz 1.3.1 (Universelle Eigenschaft der Faktrogruppe)**.** *Seien G eine Gruppe und $N \trianglelefteq G$ eine normale Untergruppe. Sei $\phi \colon G \to H$ ein Gruppenhomomorphismus. Es gibt ein Gruppenhomomorphismus $\overline{\phi} \colon G/N \to H$ so dass*

$$\phi = \overline{\phi} \circ \pi,$$

genau dann, wenn $N \leq \ker \phi$. Außerdem ist $\overline{\phi}$, wenn es existiert, eindeutig

Beweis. Nehmen wir zunächst an, dass $\overline{\phi}$ existiert. Dann gilt für alle $x \in N$:

$$\phi(x) = \overline{\phi}(\pi(x)) = \overline{\phi}([e]) = e.$$

Das bedeutet dass $N \leq \ker \phi$. Umgekhert, nehmen wir an dass $N \leq \ker N$. Wir definieren die Abbildung

$$\overline{\phi} \colon G/N \to H, \qquad \overline{\phi}([x]) = \phi(x)$$

Wir müssen uberprüfen ob diese wohldefiniert ist: seien $x, y \in G$ so dass $[x] = [y]$ in G/N. Denn $x = yg$ mit $g \in N$, und

$$\phi(x) = \phi(yg) = \phi(y)\phi(g) = \phi(y)e = \phi(y)$$

Wir zeigen dass $\overline{\phi}$ ein Homomorphismus ist: seien $x, y \in G$, dann

$$\overline{\phi}([x] \cdot [y]) = \overline{\phi}([xy]) = \phi(xy) = \phi(x)\phi(y) = \overline{\phi}(x) \cdot \overline{\phi}(y)$$

Endlich, wenn $\overline{\phi}$ so dass $\phi = \overline{\phi} \circ \pi$ existiert, es muss sein dass $\phi(x) = \overline{\phi}([x])$ so dass $\overline{\phi}$ eindeutig ist. □

Satz 1.3.2 (Homomorphiesatz)**.** *Sei $\phi\colon G \to H$ ein Gruppenhomomorphismus. Dann die Abbildung*

$$\overline{\phi}\colon G/\ker\phi \longrightarrow \operatorname{im}\phi, \quad [x] \mapsto \phi(x)$$

ist ein Isomorphismus von Gruppen.

Beweis. Die universelle Eigenschaft der Faktorgruppe zeigt dass $\overline{\phi}$ ein wohldefiniert Gruppenhomomorphismus ist. Es ist auch surjektiv weil alle Elementen in $\operatorname{im}\phi$ die Form $\phi(x)$ für $x \in G$ haben. Wir müssen noch beweisen dass ϕ injektiv ist. Das ist äquivalent zu $\ker\overline{\phi} = \{[e]\}$ und

$$\ker\overline{\phi} = \{[x] \in G/\ker\phi \,|\, \phi(x) = e\} = \{[x] \in G/\ker\phi \,|\, x \in \ker\phi\} = \{[e]\}.$$

□

Beispiel 1.3.16. Sei $G = \langle g\rangle$ eine zyklische Gruppe. Wir wollen zeigen dass $G \cong \mathbb{Z}$ oder $G \cong \mathbb{Z}/n\mathbb{Z}$ für $n > 0$. Da G zyklisch ist, ist das Homomorphismus

$$\phi\colon \mathbb{Z} \to G, \qquad h \mapsto g^h$$

surjektiv. Wenn $\operatorname{ord}(g) = \infty$ dann ist ϕ injektiv und $G \cong \mathbb{Z}$. Wenn $\operatorname{ord}(g) = n$ dann $\ker\phi = n\mathbb{Z}$ und der erster Isomorphiesatz gibt $G \cong \mathbb{Z}/n\mathbb{Z}$.

Wir betrachten jetzt die Untergruppen von einer Faktorgruppe G/N. Sei G eine Gruppe, $N \trianglelefteq G$ eine normale Untergruppe und $\pi\colon G \to G/N$ die Projektion. Sei $H \leq G$ eine Untergruppe so dass $N \leq H$: wir betrachten das Gruppenhomomorphismus

$$\pi_{|H}\colon H \to G/N$$

Der Kern ist $\ker\pi_{|H} = N$ und das Bild ist $\pi(H) = \{[x] \,|\, x \in H\}$ so dass es gibt ein Isomorphismus

$$H/N \xrightarrow{\sim} \pi(H)$$

Auf diese Weise können wir H/N als eine Untergruppe von G/N betrachten.

Satz 1.3.3. *Seien G eine Gruppe und $N \trianglelefteq G$ eine normale Untergruppe. Jede Untergruppe von G/N hat die Form H/N für genau eine Untergruppe $H \leq G$ so dass $N \leq H$. Außerdem, H/N ist normal genau dann, wenn H normal ist.*

Beweis. Sei $\pi\colon G \to G/N$ die Projektion. Sei $L \leq G/N$ eine Untergruppe: die Untergruppe $H = \pi^{-1}(L)$ enthält N weil, $N = \pi^{-1}([e])$ und $[e] \in L$. Wir sehen dass $L = \pi(\pi^{-1}(L)) = \pi(H) = H/N$. Sei jetzt $H' \leq G$ eine Untergruppe so dass $N \leq H'$ und $H'/N = L$. Dann $H' \leq \pi^{-1}(L) = H$. Wir wollen zeigen dass $H \leq H'$: sei $x \in H'$, dann $\pi(x) \in L = H'/N$ so dass $x = x'n$ für $x' \in H', n \in N$. Es folgt dass $x = x'n \in H'$. Das zeigt dass $L = H/N$ für genau eine Untergruppe $H \leq G$ so dass $N \leq G$.

Außerdem, wenn $L \trianglelefteq G/N$ eine normale Untegruppe ist, wissen wir dass $H = \pi^{-1}(L)$ eine normale Untegruppe von G ist. Umgekhert, sei $H \trianglelefteq G$ eine normale Untergruppe so dass $N \leq H$. Dann H/N ist eine normale Untegruppe von G/N: für jede $g \in G, h \in H$ gilt $[g][h][g]^{-1} = [ghg^{-1}] \in H/N$, weil $ghg^{-1} \in H$. □

Beispiel 1.3.17. Sei $n > 0$. Die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ haben die Form $d\mathbb{Z}/n\mathbb{Z}$, mit $d \in \mathbb{Z}$ so dass $d|n$.

Frage 1.3.18. Sei $n > 0$. Wir betrachten die Projektion $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ und die zwei Untegruppen $H_1 = \{0\}$ und $H_2 = n\mathbb{Z}$. Dann haben wir zwei verschiedene Untegruppen von $\mathbb{Z}$ so dass $\pi(H_1) = \pi(H_2)$. Warum?

Satz 1.3.4. *Seien G eine Gruppe, $N \trianglelefteq G$ eine normale Untegruppe und $H \leq G$ eine beliebige Untergruppe. Die Teilmenge NH ist eine Untergruppe und die Abbildung*

$$H/H \cap N \longrightarrow HN/N, \quad [h] \mod H \cap N \mapsto [h] \mod N$$

ist ein Isomorphismus von Gruppen.

Beweis. Wir wissen (aus einer Aufgabe) dass NH eine Untegruppe ist genau denn, wann $HN = NH$. Da N eine normale Untergruppe ist, wissen wir dass $Nh = hN$ für alle $h \in H$, und denn $HN = \bigcup_h hN = \bigcup Nh = NH$. Wir haben $H \leq HN, N \trianglelefteq HN$ so dass die Komposition $H \to HN \to HN/N$ ein Gruppenhomomorphismus ist. Die Gruppenhomomorphismus

$$H \to HN/N, \qquad h \mapsto [h]$$

ist surjektiv, weil $[hn] = [h]$ in HN/N für alle $n \in H, n \in N$. Außerdem, der Kern ist genau $H \cap N$. Dann ist unsere Aussage eine Folge des Homomorphiesatzes. □

Satz 1.3.5. *Seien G eine Gruppe, $N \leq H \leq G$ zwei Untegruppen so dass $N \trianglelefteq G, H \trianglelefteq G$ normale Untegruppen von G sind. Dann die Abbildung*

$$(G/N)/(H/N) \longrightarrow G/H, \qquad [g] \mod H/N \mapsto [g] \mod H$$

ist ein Isomorphismus von Gruppen.

Beweis. Erstens bemerken wir, dass H/N eine normale Untegruppe von G/N ist, so dass $(G/N)/(H/N)$ eine Gruppe ist. Das Gruppenhomomorphismus $\pi\colon G \to G/H$ hat Kern $\ker \pi \geq N$, so dass es einen weiteren Homomorphismus ergibt

$$G/N \to G/H, \qquad [g] \mod N \mapsto [g] \mod H$$

Diese Homomorphismus ist surjektiv und der Kern ist

$$\{[g] \in G/N \mid [g] = [e] \text{ in } G/H\} = \{[h] \in G/N \mid h \in H\} = H/N.$$

Dann ist unsere Aussage eine Folge des Homomorphiesatzes. □

Beispiel 1.3.19. Seien $n, d > 0$ zwei ganze Zahlen so dass $d|n$. Dann $d\mathbb{Z}/n\mathbb{Z}$ ist eine Untegruppe von $\mathbb{Z}/n\mathbb{Z}$ und $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$. Das zeigt dass

$$|d\mathbb{Z}/n\mathbb{Z}| = \left|\frac{d}{n}\right|$$

1.4 Die symmetrische Gruppe

Wir hatten viel Theorie. Jetzt betrachten wir ein wichtiges Beispiel: die symmetrische Gruppe.

Beispiel 1.4.1. Sei X eine Menge. Die symmetrische Gruppe von X ist die Menge

$$S(X) = \{f \colon X \to X \mid f \text{ invertierbar } \}$$

Die symmetrische Gruppe $S(X)$ ist eine Gruppe mit der übliche Komposition von Abbildungen.

Bemerkung 1.4.2. Sei $F \colon X \to Y$ eine bijektive Abbildung zwischen zwei Mengen. Die Abbildung

$$\varphi \colon S(Y) \to S(X), \quad f \mapsto F \circ f \circ F^{-1}$$

ist ein Gruppenhomomorphismus, da

$$\varphi(f \circ g) = F \circ (f \circ g) \circ F^{-1} = F \circ f \circ F^{-1} \circ F \circ g \circ F^{-1} = \varphi(f) \circ \varphi(g)$$

Außerdem, ϕ ist invertierbar, da die inverse Abbildung

$$G \colon S(Y) \to S(X), \quad g \mapsto F^{-1} \circ g \circ F$$

ist. Das bedeutet, dass wenn zwei Mengen die gleiche Machtigkäit haben, dann sind die symmetrische Gruppen $S(X)$ und $S(Y)$ isomorph. Insbesonders, alle symmetrische Gruppen von endliche Mengen sind isomorph zu einer den Gruppen $S(\{1, 2, \ldots, n\})$.

Definition 1.4.3 (Endliche symmetrische Gruppe)**.** Die symmetrische Gruppe vom Grad n ist

$$S_n \coloneqq S(\{1, \ldots, n\})$$

Ein Element $\sigma \in S_n$ heißt auch eine Permutation von n Elementen.

Wir darstellen eine Permutation $\sigma \in S_n$ als

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Beispiel 1.4.4. Zum Beispiel, die Permutation $\sigma \in S_4$ definiert als

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

ist die Abbildung $\sigma \colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ so dass $\sigma(1) = 1, \sigma(2) = 1, \sigma(3) = 3, \sigma(4) = 2$. Wir rechnen

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{id}$$

Eine andere Permutation in S_4 ist

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Die Komposition von σ und τ ist

$$\sigma\tau = \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Lemma 1.4.5. *Die symmetrische Gruppe S_n hat Ordnung $n!$.*

Beweis. Eine Permutation $\sigma \in S_n$ ist von $\sigma(1), \sigma(2), \ldots, \sigma(n)$ bestimmt. Wir haben n Möglichkeiten für $\sigma(1)$, $n-1$ Möglichkeiten für $\sigma(2)$ (alle Elementen ausser $\sigma(1)$), $n-2$ Möglichkeiten für $\sigma(3)$, und so weiter. □

Beispiel 1.4.6. Die symmetrische Gruppe S_1 hat nur ein Element, die Identität. Die symmetrische Gruppe S_2 hat 2 Elementen

$$S_2 = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

und ist zyklisch. Die symmetrische Gruppe S_3 hat 6 Elementen

$$S_3 = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Die Gruppe S_3 ist nicht kommutativ, da

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Es gibt eine andere und kompakter Darstellung von Permutationen durch zyklische Permutationen.

Definition 1.4.7 (Zyklische Permutationen)**.** Eine Permutation $\sigma \in S_n$ heißt zyklisch , oder ein Zyklus, wenn $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ existieren so dass

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \quad \ldots \quad , \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1$$

und $\sigma(b) = b$ für alle $b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$. Genauer gesagt, σ heißt k-Zyklus und wir schreiben

$$\sigma = (a_1 a_2 a_3 \ldots a_k)$$

Ein 2-Zyklus heißt auch Transposition. Zwei Zyklen $\sigma = (a_1 a_2 \ldots a_k), \tau = (b_1 b_2 \ldots b_h)$ heißen disjunkt wenn

$$\{a_1, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_h\} = \emptyset$$

Beispiel 1.4.8. Alle Permutationen in S_3 sind zyklisch

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13), \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132).$$

Die Permutationen in S_4 sind nicht alle zyklisch: zum Beispiel in S_4 haben wir die zwei Transpositionen

$$(12) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad (34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34)$$

und die Komposition

$$(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

ist nich zyklisch aber ein Produkt von disjunkte Zyklen. Die folgende Permutation in S_8 ist auch ein Produkt von disjunkte Zyklen:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 1 & 2 & 8 & 7 \end{pmatrix} = (135)(246)(78)$$

Proposition 1.4.9. *Alle Permutationen in S_n sind ein Produkt von disjunkte zyklische Permutationen.*

Beweis. Sei $i_1 \in \{1, 2, \ldots, n\}$ und sei k_1 die kleinste positive ganze Zahl so dass $\sigma^{k_1}(i_1) = i_1$. Wir definieren das k_1-Zyklus $(i_1\sigma(i_1)\sigma^2(i_1)\ldots\sigma^{k_1-1}(i_1))$. Wenn $\{1, 2, \ldots, n\} = \{i_1, \sigma(i_1), \ldots, \sigma^{k_1-1}(i_1)\}$, dann

$$\sigma = (i_1\, \sigma(i_1)\, \sigma^2(i_1)\, \ldots\, \sigma^{k_1-1}(i_1)).$$

Wenn nicht, existiert $i_2 \in \{1, 2, \ldots, n\} \setminus \{i_1, \sigma(i_1), \ldots, \sigma^{k_1-1}(i_1)\}$. Sei k_2 die kleinste positive ganze Zahl so dass $\sigma^{k_2}(i_2) = i_2$. Wir definieren das k_2-Zyklus $(i_2\, \sigma(i_2)\, \sigma^2(i_2)\, \ldots\, \sigma^{k_2-1}(i_2))$. Die zwei Zyklen sind disjunkt da, wenn $\sigma^r(i_1) = \sigma^s(i_2)$, dann $i_2 = \sigma^{r-s}(i_1)$, und das ist unmöglich, weil $i_2 \notin \{i_1, \sigma(i_1), \ldots, \sigma^{k_1-1}(i_1)\}$. Wenn $\{1, 2, \ldots, n\} = \{i_1, \sigma(i_1), \ldots, \sigma^{k_1-1}(i_1)\} \cup \{i_2, \sigma(i_2), \ldots, \sigma^{k_2-2}(i_2)\}$, dann

$$\sigma = (i_1\, \sigma(i_1)\, \sigma^2(i_1)\, \ldots\, \sigma^{k_1-1}(i_1))(i_2\, \sigma(i_2)\, \sigma^2(i_2)\, \ldots\, \sigma^{k_2-1}(i_2)).$$

Wenn nicht existiert i_3... und so weiter. □

Korollar 1.4.10. *Ein k-Zyklus ist ein Produkt von $k-1$ Transpositionen. Alle Permutationen in S_n sind ein Produkt von Transpositionen.*

Beweis. Es reicht zu zeigen dass jede Zyklus ein Produkt von Transpositionen ist. Sei $(a_1a_2\ldots a_k) \in S_n$ ein k-Zyklus. Dann

$$(a_1a_2\ldots a_k) = (a_1a_k)(a_1a_{k-1})\ldots(a_1a_4)(a_1a_3)(a_1a_2)$$

ist ein Produkt von $k-1$ Transpositionen. □

Man kann die Konjugation innerhalb von S_n leicht durch Zyklen ausdrücken:

Lemma 1.4.11. *Sei $(a_1a_2\ldots a_k) \in S_n$ ein k-Zyklus und sei $\sigma \in S_n$ eine Permutation. Dann*

$$\sigma(a_1a_2\ldots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\ldots\sigma(a_k))$$

Beweis. Sei $\tau = \sigma(a_1a_2\ldots a_k)\sigma^{-1}$. Dann $\tau(\sigma(a_1)) = \sigma(a_2), \tau(\sigma(a_2)) = \sigma(a_3), \ldots, \tau(\sigma(a_k)) = \sigma(a_1)$ und $\tau(\sigma(b)) = \sigma(b)$ für $b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$. □

Bemerkung 1.4.12. Sei $N \trianglelefteq S_n$ eine normale Untegruppe die eine Transposition $\tau = (hk)$ enthält. Dann N enthählt alle Transpositionen von S_n und da die Transpositionen die ganze symmetrische Gruppe erzeugen, es muss sein dass $N = S_n$.

1.4.1 Signum und Alternierende Gruppe

Definition 1.4.13 (Signum einer Permutation)**.** Das Signum einer Permutation $\sigma \in S_n$ ist

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

Satz 1.4.1. *1. Für jedes $\sigma \in S_n$, gilt $\operatorname{sgn}(\sigma) = (-1)^{|\operatorname{inv}(\sigma)|}$, wobei*

$$\operatorname{inv}(\sigma) = \{(i, j) \,|\, 1 \le i < j \le n, \quad \sigma(i) > \sigma(j)\}$$

die Menge von Inversionen von σ ist.

2. Das Signum ist ein Gruppenhomomorphismus

$$\operatorname{sgn}\colon S_n \to \{\pm 1\}.$$

3. Das Signum einer Transposition τ ist $\operatorname{sgn}(\tau) = -1$.

4. Dan Signum eines k-Zyklus σ ist $\operatorname{sgn}(\sigma) = (-1)^{k-1}$.

Beweis. 1. Wir haben

$$\begin{aligned}
\prod_{i<j}(\sigma(i)-\sigma(j)) &= \prod_{\substack{i<j\\ \sigma(i)<\sigma(j)}} (\sigma(i)-\sigma(j)) \cdot \prod_{\substack{i<j\\ \sigma(i)>\sigma(j)}} (\sigma(i)-\sigma(j)) \\
&= (-1)^{|\operatorname{inv}(\sigma)|} \prod_{\substack{i<j\\ \sigma(i)<\sigma(j)}} (\sigma(i)-\sigma(j)) \cdot \prod_{\substack{i<j\\ \sigma(i)>\sigma(j)}} (\sigma(j)-\sigma(i)) \\
&= (-1)^{|\operatorname{inv}(\sigma)|} \prod_{\substack{i<j\\ \sigma(i)<\sigma(j)}} (\sigma(i)-\sigma(j)) \cdot \prod_{\substack{j<i\\ \sigma(j)>\sigma(i)}} (\sigma(i)-\sigma(j)) \\
&= (-1)^{|\operatorname{inv}(\sigma)|} \prod_{\sigma(i)<\sigma(j)} (\sigma(i)-\sigma(j)) = (-1)^{|\operatorname{inv}(\sigma)|} \cdot \prod_{i<j}(i-j).
\end{aligned}$$

2. Seien σ, τ zwei Permutationen. Das Signum von $\sigma\tau$ ist

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

und

$$\begin{aligned}
\prod_{i<j} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} &= \prod_{\substack{i<j\\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\substack{i<j\\ \tau(i)>\tau(j)}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \\
&= \prod_{\substack{i<j\\ \tau(i)<\tau(j)}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\substack{j<i\\ \tau(j)>\tau(i)}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \\
&= \prod_{\tau(i)<\tau(j)} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} = \operatorname{sgn}(\sigma).
\end{aligned}$$

Das zeigt dass sgn ein Homomorphismus ist.

3. Sei $\tau = (hk) \in S_n$ eine Transposition, womit $h < k$. Die Inversionen von τ sind

$$\operatorname{inv}(\tau) = \{(h,k)\} \sqcup \{(h,j) \mid h < j < k\} \sqcup \{(i,k) \mid h < i < k\}$$

so dass $|\operatorname{inv}(\tau)| = 2(k-h-1)+1$ und $\operatorname{sgn}(\sigma) = (-1)^{2(k-h-1)+1} = -1$.

4. Ein k-Zyklus ist ein Produkt von $k-1$ Transpositionen, und sgn ist ein Homomorphismus. □

Definition 1.4.14 (Gerade und Ungerade Permutationen)**.** Eine Permutation $\sigma \in S_n$ heißt gerade wenn $\operatorname{sgn}(\sigma) = 1$ und ungerade wenn $\operatorname{sgn}(\sigma) = -1$.

Definition 1.4.15 (Alternierende Gruppe)**.** Die Menge A_n von alle gerade Permutationen in S_n heißt die Alternierende Gruppe vom Grad n.

Korollar 1.4.16. *Die Alternierende Gruppe A_n ist eine normale Untegruppe von S_n und $S_n/A_n \cong \{\pm 1\}$ wenn $n \geq 2$.*

Beweis. Die alternierende Gruppe ist der Kern vom Signum $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ und das Signum ist surjektiv wenn $n \geq 2$ weil es gibt eine Transposition. □

1.4.2 Satz von Cayley

Satz 1.4.2. *Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe*

Beweis. Wir zeigen dass G ist isomorph zu einer Untegruppe von der symmetrische Gruppe $S(G)$. Wenn $|G| = n$ dann $S(G) \cong S_{n!}$. Fur jede $g \in G$ definieren wir die Abbildung

$$T_g\colon G \to G, \qquad x \mapsto gx$$

Man hat $T_e = \mathrm{id}_G$ und $T_g \circ T_h = T_{gh}$ so dass T_g ist invertierbar mit inverse Abbildung $T_{g^{-1}}$. Das definiert eine Abbildung

$$T\colon G \to S(G), \qquad g \mapsto T_g$$

die ein Gruppenhomomorphismus ist. Wir m üssen nur zeigen dass T injektiv ist, aber

$$\ker T = \{g \in G \,|\, T_g = \mathrm{id}_G\} = \{g \in G \,|\, gx = x \text{ für alle } x \in G\} = \{e\}.$$

□

1.5 Direkte Produkten

Definition 1.5.1 (Direktes Produkt von Gruppen)**.** Seien G_1, G_2 zwei Gruppen. Die Menge $G_1 \times G_2$ mit der Verknupfüng

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

ist eine Gruppe die die direkte Produkte von G_1 und G_2 heißt.

Bemerkung 1.5.2. Eine änliche Definition gilt für das Produkt $G_1 \times G_2 \times \cdots \times G_s$ und eigentlich für das Produkt $\prod_{i \in I} G_i$ einer beliebige Familie von Gruppen.

Beispiel 1.5.3. Die Gruppe $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ heißt manchmal die Kleinsche Vierergruppe. Sie ist eine kommutative Gruppe mit 4 Elementen: $V = \{([0],[0]), ([1],[0]), ([0],[1]), ([1],[1])\}$. Wir sehen dass alle Elementen haben Ordnung 1 oder 2, so dass V nicht zyklisch ist. Insbesonders $V \ncong \mathbb{Z}/4\mathbb{Z}$.

Beispiel 1.5.4. Die Gruppe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} = \{([0],[0]),([0],[1]),([0],[2]),([1],[0]),([1],[1]),([1],[2])\}$ hat Ordnung 6 und ist zyklisch. Zum Beispiel, das Element $([1],[1])$ erzeugt die ganze Gruppe:

$$\begin{aligned} 1\cdot([1],[1]) &= ([1],[1]), & 2\cdot([1],[1]) &= ([0],[2]),\\ 3\cdot([1],[1]) &= ([1],[0]), & 4\cdot([1],[1]) &= ([0],[1]),\\ 5\cdot([1],[1]) &= ([1],[2]), & 6\cdot([1],[1]) &= ([0],[0]). \end{aligned}$$

Insbesonders $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\cong\mathbb{Z}/6\mathbb{Z}$.

Wir können tatsachlich bestimmen wenn das direktes Produkt $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ zyklisch ist. Zuerst erinnern wir uns an

Lemma 1.5.5. *Seien G eine Gruppe und $g\in G$ ein Element mit endlicher Ordnung* $\operatorname{ord}(g)$. *Dann*

$$g^m = e \iff \operatorname{ord}(g)|m$$

Beweis. Die Menge $\{m\in\mathbb{Z}\,|\,g^m=e\}$ ist der Kern des Homomorphismus $\phi\colon\mathbb{Z}\to G,\ \phi(m)=g^m$. Dieser ist eine Untergruppe von $\mathbb{Z}$ und $\ker\phi\neq\{0\}$, da g endliche Ordnung hat. Denn wissen wir dass die Untegruppe $\ker\phi$ zyklisch ist, und dass es durch das kleinste positive Element erzeugt wird, das genau $\operatorname{ord}(g)$ ist. □

Dann haben wir

Lemma 1.5.6. *Seien G_1,G_2 zwei Gruppen und $g_1\in G_1, g_2\in G_2$ zwei Elementen mit endliche Ordnung. Dann hat $(g_1,g_2)\in G_1\times G_2$ endliche Ordnung*

$$\operatorname{ord}(g_1,g_2) = kgV(\operatorname{ord}(g_1),\operatorname{ord}(g_2))$$

womit kgV der kleinste gemeinsame Vielfaches ist.

Beweis. Sei $m = kgV(\operatorname{ord}(g_1),\operatorname{ord}(g_2))$. Wir zeigen dass $m|\operatorname{ord}(g_1,g_2)$ und dass $\operatorname{ord}(g_1,g_2)|m$.

Da m der kleinste gemensaime Vielfaches ist, $\operatorname{ord}(g_1)|m$ und $\operatorname{ord}(g_2)|m$. Dann zeigt das vorherige Lemma, dass

$$(g_1,g_2)^m = (g_1^m, g_2^m) = (e,e)$$

Das vorherige Lemma ergibt dass $\operatorname{ord}(g_1,g_2)|m$.

Andererseits

$$(e,e) = (g_1,g_2)^{\operatorname{ord}(g_1,g_2)} = (g_1^{\operatorname{ord}(g_1,g_2)}, g_2^{\operatorname{ord}(g_1,g_2)})$$

und das vorherige Lemma zeigt dass $\operatorname{ord}(g_1)|\operatorname{ord}(g_1,g_2)$ und $\operatorname{ord}(g_2)|\operatorname{ord}(g_1,g_2)$ und das ergibt dass $m|\operatorname{ord}(g_1,g_2)$. □

Korollar 1.5.7. *Die Gruppe $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ ist zyklisch genau denn wann n,m teilerfremd sind.*

Beweis. Die Gruppe $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ ist zyklisch genau denn wann ein element $([a],[b])$ in der Gruppe existiert, so dass $\operatorname{ord}([a],[b]) = m\cdot n$. Das vorherige Lemma ergibt dass $\operatorname{ord}([a],[b]) = kgV(\operatorname{ord}[a],\operatorname{ord}[b])$ und wir wissen dass $\operatorname{ord}[a]|m$ und $\operatorname{ord}[b]|n$, da $[a]\in\mathbb{Z}/n\mathbb{Z}$ und $[b]\in\mathbb{Z}/m\mathbb{Z}$. Dann

$$kgV(\operatorname{ord}[a],\operatorname{ord}[g]) = \frac{\operatorname{ord}([a])\cdot\operatorname{ord}([b])}{ggT(\operatorname{ord}[a],\operatorname{ord}[b])} = m\cdot n$$

genau denn wann $\operatorname{ord}[a]=m, \operatorname{ord}[b]=n$ und $ggT(m,n)=1$. □

Beispiel 1.5.8. Die Gruppe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ist zyklisch, so dass $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$.

Proposition 1.5.9 (Universelle Eigenschaft des direktes Produkt)**.** *Seien G_1, G_2 zwei Gruppen.*

1. *Die Projektionen $\mathrm{pr}_i \colon G_1 \times G_2 \to G_i$ für $i = 1, 2$ sind Gruppenhomomorphismen.*
2. *Sei H eine Gruppe und $\phi_i \colon H \to G_i, i = 1, 2$ Gruppenhomomorphismen. Dann ist die Abbildung*
$$\phi_1 \times \phi_2 \colon H \to G_1 \times G_2, \quad h \mapsto (\phi_1(h), \phi_2(h))$$
ein Gruppenhomomorphismus.

Beweis. Dies ist eine unkomplizierte Prüfung. □

Kapitel 2

Ringe

2.1 Ringe

Definition 2.1.1 (Ringe)**.** Ein Ring (mit 1) ist eine Menge R mit zwei Verknüpfungen, Summe und Multiplikation:

$$+\colon R \times R \to R, \qquad R, \qquad \cdot R \times R \to R$$

mit folgende Eigenschaften:

- $(R, +)$ ist eine abelsche Gruppe, mit neutrales Element 0.
- Es gibt eine multiplikative Neutrales $1 \in R$ so dass

$$1 \cdot x = x \cdot 1 = x \quad \text{for all } x \in R.$$

- Die Multiplikation is assoziativ:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad \text{for all } x, y, z \in R$$

- Es gelten die Distributivgesetze:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x \qquad \text{für alle } x, y, z \in R$$

Definition 2.1.2 (Kommutative Ringe)**.** Ein Ring R heißt kommutativ wenn die Multiplikation kommutativ ist.

Beispiel 2.1.3 (Ganze Zahlen)**.** Die ganze Zahlen $\mathbb{Z}$ mit der übliche Summe und übliche Multiplikation bilden einen Ring.

Beispiel 2.1.4 (Zahlen modulo n)**.** Wir definieren eine Multiplikation auf der abelsche Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ wie folgt:

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad ([a], [b]) \mapsto [a] \cdot [b] = [a \cdot b]$$

Diese Verknüpfung ist wohldefiniert: wenn $[a'] = [a]$ und $[b'] = [b]$, dann $a' = a + k \cdot n, b' = b + h \cdot n$ für $h, k \in \mathbb{Z}$. Wir rechnen

$$[a' \cdot b'] = [(a + k \cdot n) \cdot (b + h \cdot n)] = [ab + n \cdot (khn + kb + ha)] = [a \cdot b] \qquad \text{in } \mathbb{Z}/n\mathbb{Z}.$$

Wir sehen dass [1] ein neutrale Element für die Multiplikation ist. Die Multiplikation ist auch assoziativ da die Multiplikation auf $\mathbb{Z}$ assoziativ ist. Die Distributivität gilt, weil sie auf $\mathbb{Z}$ gilt. Endlich, die Multiplikation ist kommutativ, da die Multiplikation auf $\mathbb{Z}$ kommutativ ist. Das zeigt dass $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring ist.

Beispiel 2.1.5 (Körper)**.** Jede Körper ist ein kommutativer Ring. Zum Beispiel $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Beispiel 2.1.6 (Polynomring)**.** Der Polynomring $K[x]$ auf einem Körper K ist ein kommutativer Ring mit der übliche Summe und der übliche Multiplikation von Polynome.

Lemma 2.1.7 (Rechenregeln)**.** *Seien R ein Ring und $x, y, z \in R$. Dann gilt:*

1. $-(-x) = x$.
2. $-(x + y) = -x + (-y) = -x - y$.
3. $x + y = z \iff x = z - y$.
4. $x \cdot 0 = 0 \cdot x = 0$.
5. $(-x) \cdot y = x \cdot (-y) = -xy$.
6. $(-x) \cdot (-y) = xy$
7. $x \cdot (y - z) = xy - xz$.
8. $(-1) \cdot x = -x$.

Beweis. Die Eigenschaften $(1) - (2) - (3)$ sind Eigenschaften der abelsche Gruppe $(R, +)$.
Für die Nummer (4), berechnen wir:

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$$

so dass $0 \cdot x = 0$. Eine änliche Begrundung zeigt dass $x \cdot 0 = 0$. Für die Nummer (5), berechnen wir:

$$xy + (-x) \cdot y = (x - x) \cdot y = 0 \cdot y = 0$$

so dass $(-x) \cdot y = -xy$. Eine änliche Begrundung zeigt dass $x \cdot (-y) = -xy$. Für die Nummer (6), benutzen wir (5) und wir berechnen:

$$(-x)(-y) = -((-x) \cdot y) = -(-xy) = xy.$$

Für die Nummer (7), berechnen wir:

$$x(y - z) = xy + x(-z) = xy - xz$$

Für die Nummer (8), berechnen wir:

$$0 = 0 \cdot x = (-1 + 1) \cdot x = (-1) \cdot x + 1 \cdot x = (-1) \cdot x + x$$

so dass $(-1) \cdot x = -x$. □

Definition 2.1.8 (Einheit)**.** Sei R ein Ring. Eine Einheit ist ein Element $a \in R$ so dass $b \in R$ existiert, mit $ab = 1$. Die Menge $R^* = \{a \in R \,|\, a \text{ Einheit } \}$ ist eine Gruppe mit der Multiplikation, die Einheitsgruppe.

Definition 2.1.9 (Körper)**.** Ein kommutativer Ring R ist ein Körper falls jede $a \in R, a \neq 0$ eine Einheit ist: $R^* = R \setminus \{0\}$.

Definition 2.1.10 (Nullteiler)**.** Sei R ein Ring. Ein Nullteiler ist ein Element $a \in R, ane0$ so dass $b \in R, b \neq 0$ existiert mit $ab = 0$.

Definition 2.1.11 (Integritätsbereich)**.** Ein kommutativer Ring R ist ein Integritätsbereich, falls R keine Nullteiler besitzt.

Bemerkung 2.1.12. Ein kommutativer Ring R ist ein Integritätsbereich genau dann wenn die folgende Aussage gilt:

$$ab = 0 \implies a = 0 \text{ oder } b = 0.$$

Definition 2.1.13 (Nilpotentes Element)**.** Sei R ein Ring. Ein Element $a \in R$ heißt nilpotent wenn $a \neq 0$ und $n \in \mathbb{N}, n > 0$ existiert so dass

$$a^n = 0.$$

Definition 2.1.14 (Reduzierter Ring)**.** Ein kommutativer Ring R ist reduziert, falls R keine nilpotente Elementen hat.

Lemma 2.1.15. *Ein Körper ist ein Integritätsbereich und ein Integritätsbereich ist reduziert.*

Beweis. Sei R ein Körper und seien $a, b \in R$ so dass $ab = 0$. Wenn $a \neq 0$, dann ist a invertierbar und dann

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot ab = 1 \cdot b = b.$$

Das zeigt dass R ein Integritätsbereich.

Sei nun R ein Integritätsbereich und sei $a \in R$ so dass $a^n = 0$ für $n \in \mathbb{N}, n > 0$. Wir zeigen induktiv dass $a = 0$. Wenn $n = 1$ das ist klar. Wenn $n > 1$, dann $0 = a^n = a \cdot a^{n-1}$, und, da R ein Integritätsbereich ist, folgt dass $a = 0$ oder $a^{n-1} = 0$. Wenn $a = 0$, alles gut. Wenn $a^{n-1} = 0$, alles noch gut dank der Induktion. □

Beispiel 2.1.16. Der Ring $\mathbb{Z}/2\mathbb{Z}$ ist ein Körper: das einzige Element, das nicht Null ist, ist $[1]$. Der Ring $\mathbb{Z}/3\mathbb{Z}$ ist auch ein Körper: die Elementen die nicht null sind, sind $[1]$ und $[2]$, und $[2]^2 = [4] = [1]$ in $\mathbb{Z}/3\mathbb{Z}$. Der Ring $\mathbb{Z}/4\mathbb{Z}$ ist aber kein Körper, weil er nicht reduziert ist: $[2]^2 = [4] = [0]$ in $\mathbb{Z}/4\mathbb{Z}$ aber $[2] \neq [0]$. Wie geht es weiter?

Proposition 2.1.17. *Sei R ein endlicher Integritätsbereich. Dann ist R ein Körper.*

Beweis. Sei $a \in R, a \neq 0$. Wir wollen zeigen dass a invertierbar ist. Wir betrachten die Abbildung

$$\phi_a \colon R \to R, \qquad x \mapsto a \cdot x$$

Diese Abbildung ist ein Gruppenhomomorphismus: $\phi_a(x+y) = a(x+y) = ax+ay = \phi_a(x)+\phi_a(y)$. Diese Abbildung ist auch injektiv, da $x \in \ker \phi_a$ genau dann wenn $ax = 0$, aber, da R ein Integritätsbereich ist, es folgt dass $x = 0$. Da R endlich ist, die Abbildung ϕ_a ist auch surjektiv und es gibt einen $x \in R$ so dass $\phi_a(x) = 1$, und das bedeutet $ax = 1$, also a ist invertierbar. □

Korollar 2.1.18. *Sei $n \in \mathbb{Z}, n > 0$.*

- *$\mathbb{Z}/n\mathbb{Z}$ ist ein Körper $\iff$ $\mathbb{Z}/n\mathbb{Z}$ ist ein Integritätsbereich $\iff$ n ist ein Primzahl.*
- *$\mathbb{Z}/n\mathbb{Z}$ ist reduziert $\iff$ n ist quadratfrei.*

Beweis. • Da $\mathbb{Z}/n\mathbb{Z}$ ein endlicher Ring ist, er ist ein Körper genau dann, wenn er ein Integritätsbereich ist.

Sei nun $n = p$ ein Primzahl, wir wollen zeigen dass $\mathbb{Z}/p\mathbb{Z}$ ein Integritätsbereich ist. Seien $[a][b]$ mit $[a] \cdot [b] = [ab] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$, so dass $p|ab$ in $\mathbb{Z}$. Wir wollen zeigen dass $[a] = [0]$ oder $[b] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$. Wir schreiben ab als Produkt von Primzahlen $a = p_1^{e_1} \dots p_r^{e_r}, b = q_1^{f_1} \dots q_s^{f_s}$, und dann $ab = p_1^{e_1} \dots q_s^{f_s}$. Die Primfaktoren von ab sind $p_1, \dots, q_s$, aber p ist auch ein Primfaktor, da $p|ab$, so dass $p = p_i$ für eine i oder $p = q_j$ für eine j. Wenn $p = p_i$, dann $p|a$ und $[a] = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Wenn $p = q_j$ dann $p|b$ und $[b] = 0$ in $\mathbb{Z}/p\mathbb{Z}$.

Andererseits, nehmen wir an dass n kein Primzahl ist, so dass $n = ab$, mit $0 < a < n, 0 < b < n$. Dann $[a] \neq [0], [b] \neq [0]$ in $\mathbb{Z}/n\mathbb{Z}$ aber $[a] \cdot [b] = [ab] = [n] = [0]$, so dass $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich ist.

- Sei n quadratfrei, so dass $n = p_1 \dots p_r$ mit paarweise verschiedene Primzahlen p_i. Wir zeigen dass $\mathbb{Z}/n\mathbb{Z}$ reduziert ist: sei $[a]$ in $\mathbb{Z}/n\mathbb{Z}$ und $k \in \mathbb{N}, k > 0$ so dass $[a]^k = 0$ so dass $n|a^k$. Wir schreiben $a = q_1^{e_1} \dots q_s^{e_s}$ als Produkt von paarweise verschiedene Primzahlen. Dann $a^k = q_1^{k \cdot e_1} \dots q_s^{k \cdot e_s}$ so dass die Primfaktoren von a^k genau die Primfaktoren von a sind. Da $n|a^k$, wissen wir dass $p_i|a^k$ so dass jede p_i ein Primfaktor von a^k, und denn auch ein Primfaktor von a, ist. Bis zur Neunummerierung können wir schreiben $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} q_{r+1}^{e_{r+1}} \dots q_s^{e_s}$, so dass $n|a$ und $[a] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$.

  Andererseits, sei n nicht quadratfrei so dass die Primfaktorzerlegung von n ist: $n = p_1^{e_1} \cdot p_r^{e_r}$ mit $e_i \geq 1$ und $e_1 \geq 2$. Denn $[a] = [p_1 p_2^{e_2} \dots p_r^{e_2}] \neq [0]$ in $\mathbb{Z}/n\mathbb{Z}$, aber $[a]^{e_1} = [0]$. Das zeigt dass R nicht reduziert ist.

□

Beispiel 2.1.19. Das ergibt viele Beispiele: $\mathbb{Z}/5\mathbb{Z}$ Körper, $\mathbb{Z}/6\mathbb{Z}$ kein Integritätsbereich aber reduziert, $\mathbb{Z}/7\mathbb{Z}$ Körper, $\mathbb{Z}/8\mathbb{Z}$ nicht reduziert, $\mathbb{Z}/9\mathbb{Z}$ nicht reduziert, ...

Beispiel 2.1.20 (Der Polynomring)**.** Sei R ein kommutativer Ring. Der Polynomring $R[x]$ ist definiert als die Menge von formale endliche Summen

$$R[x] = \left\{ \sum_{n=0}^{d} a_n \cdot x^n \,|\, a_n \in R, \quad n \in \mathbb{N} \right\}$$

Der Grad von einem Polynom $f(x) = a_0 + a_1 \cdot x + \dots + a_d \cdot x^d \in R[x]$ mit $a_d \neq 0$ ist

$$\deg(f) = d = \max\{n \,|\, a_n \neq 0\}$$

Wir definieren auch $\deg(0) = -\infty$. Der Leitkoeffizient von $f \neq 0$ ist

$$LC(f) = a_d = a_{\deg f}.$$

Der Polynomring ist ein Ring mit der Summe und der Multiplikation von Polynome:

$$f(x)+g(x)=(\sum_{n=0}^{d}a_nx^n)+(\sum_{m=0}^{e}b_mx^m)=\sum_{k=0}^{\max\{d,e\}}(a_k+b_k)x^k$$
$$f(x)\cdot g(x)=(\sum_{n=0}^{d}a_nx^n)\cdot(\sum_{m=0}^{e}b_mx^m)=\sum_{k=0}^{d+e}\left(\sum_{n+m=k}a_nb_m\right)x^k$$

Man hat $\deg(f+g)\leq\max\{\deg(f),\deg(g)\}$ und $\deg(f\cdot g)\leq\deg(f)+\deg(g)$. Genauer gesagt, wenn $f\neq 0, g\neq 0$, mit $\deg(f)=d, \deg(g)=e$, dann $f(x)=a_0+\cdots+a_dx^d$ und $g(x)=b_0+\cdots+b_ex^e$, mit $a_d\neq 0, b_e\neq 0$. Dann

$$f(x)\cdot g(x)=a_0\cdot b_0+\cdots+a_d\cdot b_ex^{d+e}$$

so dass $\deg(f\cdot g)=d+e=\deg(f)+\deg(g)$ genau dann wenn $a_d\cdot b_e\neq 0$, oder $LC(f)\cdot LC(g)\neq 0$. Insbesondere, wenn R ein Integritätsbereich ist, $a_db_e\neq 0$, so dass $f\cdot g\neq 0$ und $\deg(f\cdot g)=d+e$. Wir schreiben dies als Lemma.

Lemma 2.1.21. *Sei R ein Integritätsbereich, dann $R[x]$ ist auch ein Integritätsbereich, und $\deg(f\cdot g)=\deg(f)+\deg(g)$ für alle $f,g\in R[x]$.*

Beweis. Wir haben schon gezeigt dass $R[x]$ ein Integritätsbereich ist, und dass $\deg(f\cdot g)=\deg(f)+\deg(g)$ für alle $f,g\in R[x]$ und $f\neq 0, g\neq 0$. Wenn $f=0$ oder $g=0$ dann $\deg(f\cdot g)=-\infty$ und $\deg(f)+\deg(g)=-\infty$. □

2.2 Ideale und Unterringe

Definition 2.2.1 (Unterring)**.** Sei R ein kommutativer Ring. Eine Teilmenge $S\subseteq R$ ist ein Unterring wenn die folgende Bedigungen gelten:

1. $S\subseteq(R,+)$ ist eine Untergruppe.
2. $ab\in S$ für alle $a,b\in S$.
3. $1\in S$.

Die Menge S mit den Einschrankungen von der Summe und der Multiplikation von R ist selbst ein Ring.

Beispiel 2.2.2. Der Ring $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$. Der einziger Unterring von $\mathbb{Z}$ ist $\mathbb{Z}$ selbst, weil jede Untergruppe $S\subseteq\mathbb{Z}$ die 1 enthält ist muss $\mathbb{Z}$ sein. Eine anliche Begrundung zeigt dass der einziger Unterring von $\mathbb{Z}/n\mathbb{Z}$ der ganze Ring ist. Wenn R ein Ring ist, dann ist R ein Unterring von $R[x]$.

Definition 2.2.3. Sei R ein kommutativer Ring. Ein Teilmenge $I\subseteq R$ ist ein ideal wenn die folgende Bedigungen gelten:

1. $I\subseteq(R,+)$ ist eine Untergruppe.
2. $ai\in I$ für alle $a\in R, i\in I$.

Ein Ideal heißt echt, wenn $I \subsetneq R$.

Beispiel 2.2.4. Die Untergruppe $n\mathbb{Z} \subseteq \mathbb{Z}$ ist ein Ideal für jede $n \in \mathbb{Z}$. Wenn R ein Ring ist, die Menge $xR[x] = \{x \cdot f(x) \,|\, f(x) \in R[x]\}$ ist ein Ideal von $R[x]$. Ein Ring R hat immer zwei Ideale: R selbst und $\{0\}$.

Bemerkung 2.2.5. Ein Ideal I ist echt genau dann wenn $1 \notin I$: wenn $1 \in I$ dann $a \cdot 1 = a \in I$ für alle $a \in R$.

Proposition 2.2.6. *Sei R ein Ring und seien I_1, I_2 zwei Ideale von R.*

1. *Die Summe $I_1 + I_2 = \{i_1 + i_2 \,|\, i_1 \in I_1, i_2 \in I_2\}$ ist ein Ideal von R.*
2. *Die Durchschnitt $I_1 \cap I_2$ ist ein Ideal von R.*

Änliche Aussagen gelten für die Summe und für die Durchschnitt von unendliche viele Ideale.

Beweis. Man überpruft leicht die Eigenschaften in der Definition. □

Definition 2.2.7 (Erzeugte Ideale)**.** Seien R ein kommutativer Ring und $A \subseteq R$ eine Teilmenge. Das Ideal erzeugt von A ist

$$(A) \coloneqq \bigcap_{\substack{I \subseteq R \text{ Ideal} \\ A \subseteq I}} I$$

Das Ideal (A) ist das kleinstes Ideal, das A enthält.

Proposition 2.2.8. *Seien R ein kommutativer Ring und $A \subseteq R$ eine Teilmenge. Das Ideal erzeugt von A ist*

$$(A) = \left\{ \sum_{i=1}^{n} r_i a_i \,|\, r_i \in R, a_i \in A, n \in \mathbb{N} \right\}$$

Beweis. Das ideal (A) enthält $a_1, \ldots, a_n$ für alle $a_i \in A$,und da (A) ein Ideal ist, wissen wir dass $r_1 a_1, \ldots, r_n a_n \in (A)$ für alle $r_i \in R$, und dann $\sum_{i=1}^{n} r_i a_i \in (A)$. Das zeigt dass $(A) \supseteq \{\sum_{i=1}^{n} r_i a_i \,|\, r_i \in R, a_i \in A, n \in \mathbb{N}\}$. Um die andere Inklusion zu beweisen, es reicht zu zeigen dass die Menge $\{\sum_{i=1}^{n} r_i a_i \,|\, r_i \in R, a_i \in A, n \in \mathbb{N}\}$ ein Ideal ist. Das ist eine leichte Uberprüfung von den Eigenschaften in der Definition von Ideal. □

Definition 2.2.9 (Hauptideal)**.** Sei R ein kommutativer Ring. Ein Ideal $I \subseteq R$ ist ein Hauptideal wenn $a \in I$ existiert sodass $I = (a)$.

Beispiel 2.2.10. Das Ideal $n\mathbb{Z} = (n)$ in $\mathbb{Z}$ ist ein Hauptideal. Das Ideal $xR[x] = (x)$ in $R[x]$ ist ein Hauptideal. Das Ideal $I = (2, x) \subseteq \mathbb{Z}[x]$ ist nicht ein Hauptideal (Hausaufgabe).

Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Da $(R, +)$ eine abelsche Gruppe ist, die Untegruppe I ist normal und die Faktorgruppe R/I ist eine Gruppe, aber sie ist auch ein Ring:

Proposition 2.2.11. *Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Die Faktorgruppe R/I mit der Multiplikation*

$$R/I \times R/I \longrightarrow R/I, \qquad ([a], [b]) \mapsto [ab]$$

ist ein kommutativer Ring.

Beweis. Wir zeigen dass die Multiplikation wohldefiniert ist: seien $a, b, a', b' \in R$ so dass $[a] = [a']$ und $[b] = [b']$ in R/I. Wir wollen zeigen dass $[ab] = [a'b']$ in R/I. Da die Klassen von a, a' und b, b' gleich sind, wissen wir dass $a = a' + i, b = b' + j$ mit $i, j \in I$. Dann $ab = (a' + i)(b' + j) = a'b' + a'j + b'i + ij$ und $aj + bi + ij \in I$ weil I ein Ideal ist. Denn $[ab] = [a'b']$ in R/I. Jetzt dass dass die Multiplikation wohldefiniert ist, kann Man leicht überprüfen dass R/I ein Ring ist. □

Definition 2.2.12 (Faktorring)**.** Der Ring R/I heißt Faktorring.

Beispiel 2.2.13. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau der Faktorring von dem Ideal $n\mathbb{Z} \subseteq \mathbb{Z}$.

Definition 2.2.14 (Maximales Ideal)**.** Sei R ein kommutativer Ring. Ein echtes Ideal $\mathfrak{m} \subsetneq R$ ist maximal wenn kein echtes Ideal $I \subsetneq R$ existiert mit $\mathfrak{m} \subsetneq I$.

Definition 2.2.15 (Primideal)**.** Sei R ein kommutativer Ring. Ein echtes Ideal $\mathfrak{p} \subseteq R$ ist prim wenn die folgende Aussage für alle $a, b \in R$ gilt:

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}.$$

Definition 2.2.16 (Radikales Ideal)**.** Sei R ein kommutativer Ring. Ein echtes Ideal $I \subseteq R$ ist radikal wenn die folgende Aussage für alle $a \in R, n \in \mathbb{N}$ gilt:

$$a^n \in I \implies a \in I$$

Proposition 2.2.17. *Seien R ein kommutativer Ring und $I \subseteq R$ ein echtes Ideal.*

1. *I ist maximal genau dann, wenn R/I ein Körper ist.*
2. *I is prim genau dann, wenn R/I ein Integritätsbereich ist.*
3. *I ist radikal genau dann, wenn R/I reduziert ist.*

Beweis. 1. Nehmen wir an dass I maximal ist und sei $[a] \in R/I, [a] \neq 0$. Das bedeutet dass $a \in R, a \notin I$. Da I maximal ist, und $(a) + I \supsetneq I$ es muss sein dass $(a) + I = R$ so dass es gibt $b \in R, i \in I$ so dass $ab + i = 1$. Dann $[1] = [ab + i] = [ab]$ in R/I. Das zeigt dass $[a]$ invertierbar in R/I ist, und, da es für alle $[a] \in R/I, [a] \neq 0$ gilt, das zeigt dass R/I ein Körper ist.

   Andererseits, nehmen wir an dass R/I ein Körper ist und sei $J \subseteq R$ ein Ideal so dass $I \subsetneq J$. Dann existiert $a \in J \setminus I$ so dass $[a] \neq 0$ in R/I. Dann existiert $[b] \in R/I$ so dass $[ab] = [1]$ in R/I, und das bedeutet dass $1 = ab + i$ in R, für ein $i \in I$. Dann $1 \in J$ und $J = R$.

2. Das Ideal I ist prim genau dann, wenn die folgende Aussage für alle $a, b \in R$ gilt:

   $$ab \in I \implies a \in I \text{ oder } b \in I.$$

   Wir können die Aussage auch als

   $$[ab] = 0 \text{ in } R/I \implies [a] = 0 \text{ oder } [b] = 0 \text{ in } R/I$$

   schreiben, und das bedeutet genau dass R/I ein Integritätsbereich ist.

3. Das Ideal I ist radikal genau dann, wenn die folgende Aussage für alle $a \in R, n \in \mathbb{N}$ gilt:

$$a^n \in I \implies a \in I.$$

Wir können die Aussage auch als

$$[a]^n = 0 \text{ in } R/I \implies [a] = 0 \text{ in } R/I$$

schreiben, und das bedeutet genau dass R/I ein reduzierter Ring ist.

□

Korollar 2.2.18. *Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Dann*

$$I \text{ maximal} \implies I \text{ prim} \implies I \text{ radikal}$$

Beweis. Dies ergibt sich aus der Proposition 2.2.17 sowie aus der folgenden, bereits bewiesenen Tatsache: R/I Körper $\implies$ R/I Integritätsbereich $\implies$ R/I reduzierter Ring. □

Korollar 2.2.19. *Sei R ein kommutativer Ring. Dann*

1. *R ist ein Körper genau dann,wenn (0) ein maximales ideal ist.*
2. *R ist ein Integritätsbreich genau dann, wenn (0) ein Primideal ist.*
3. *R ist reduziert genau dann, wenn (0) ein radikales Ideal ist.*

Beweis. Dies ergibt sich aus der Proposition 2.2.17 sowie aus der Tatsache dass $R/(0)$ genau der Ring R ist. □

2.3 Homomorphismen

Definition 2.3.1 (Ringhomomorphismus)**.** Seien R, S zwei kommutative Ringe. Eine Abbildung

$$\phi\colon R \to S$$

heißt Ringhomomorphismus wenn sie die folgende Eigenschaft hat:

1. $\phi(a+b) = \phi(a) + \phi(b)$ für alle $a, b \in R$.
2. $\phi(ab) = \phi(a)\phi(b)$ für alle $a, b \in R$.
3. $\phi(1) = 1$.

Bemerkung 2.3.2. Ein Ringhomomorphismus ist insbesondere ein Gruppenhomomorphismus $\phi\colon (R, +) \to (S, +)$.

Lemma 2.3.3. *Sei $\phi\colon R \to S$ ein Ringhomomorphismus.*

1. *$\phi(-a) = -\phi(a)$ für alle $a \in R$.*
2. *Wenn $a \in R$ invertierbar ist, dann ist $\phi(a) \in S$ auch invertierbar und $\phi(a^{-1}) = \phi(a)^{-1}$.*
3. *$\phi(a^n) = \phi(a)^n$ für alle $a \in R, n \in \mathbb{N}$.*

Beweis. 1. Das gilt weil ϕ ein Gruppenhomomorphismus ist.

2. Da $aa^{-1} = 1$, wissen wir dass $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1$. Das zeigt dass $\phi(a)$ invertierbar ist und dass $\phi(a^{-1}) = \phi(a)^{-1}$.

3. Wenn $n = 0$, dann $\phi(a^0) = \phi(1) = 1 = \phi(a)^0$. Wenn $n > 0$ dann $\phi(a^n) = \phi(a \cdot a \cdot \cdots \cdot a) = \phi(a) \cdot \phi(a) \cdot \cdots \cdot \phi(a) = \phi(a)^n$. Wenn $n < 0$, dann $n = -|n|$ mit $|n| > 0$ und Punkt (2) zeigt dass $\phi(a^n) = \phi(a^{-|n|}) = \phi(a^{|n|})^{-1} = (\phi(a)^{|n|})^{-1} = \phi(a)^{-|n|} = \phi(a)^n$.

□

Lemma 2.3.4. *Sei $\phi\colon R \to S$ ein invertierbares Ringhomomorphismus. Dann ist die Umkehrabbildung $\phi^{-1}\colon S \to R$ ein Ringhomomorphismus.*

Beweis. Wir wissen dass ϕ^{-1} ein Gruppenhomomorphismus, und wir wissen dass $\phi^{-1}(1) = 1$, da $\phi(1) = 1$. Wir müssen nur zeigen dass $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$ für alle $x, y \in S$. Da ϕ injektiv ist, das ist äquivalent zu $\phi(\phi^{-1}(xy)) = \phi(\phi^{-1}(x)\phi^{-1}(y))$, aber

$$\phi(\phi^{-1}(xy)) = xy = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y))) = \phi(\phi^{-1}(x)\phi^{-1}(y)).$$

□

Definition 2.3.5 (Isomorphismus)**.** Ein Ringhomomorphismus $\phi\colon R \to S$ ist ein Isomorphismus wenn es invertierbar ist.

Beispiel 2.3.6. Sei R ein Ring. Wir wollen alle Ringhomomorphismen $\phi\colon \mathbb{Z} \to R$ bestimmen. Es gibt immer das Ringhomomorphismus

$$\phi\colon \mathbb{Z} \longrightarrow R \qquad \phi(n) = n$$

Wir zeigen dass dieses das einzige Ringhomomorphismus ist. Sei $\psi\colon \mathbb{Z} \to R$ ein Ringhomomorphismus, wir wissen dass $\psi(1) = 1$, und wenn $n > 0$ dann $\psi(n) = \psi(1 + 1 + \cdots + 1) = \psi(1) + \psi(1) + \cdots + \psi(1) = 1 + 1 + \cdots + 1 = n$. Wenn $n < 0$, dann $\psi(n) = \psi(-|n|) = -\psi(|n|) = -|n| = n$.

Beispiel 2.3.7. Sei $\phi\colon \mathbb{Q} \to \mathbb{R}$ ein Ringhomomorphismus. Die Einschränkung $\phi_{|\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{R}$ ist ein Ringhomomorphismus, so dass $\phi(n) = n$ für alle $n \in \mathbb{Z}$. Außerdem, n ist in $\mathbb{Q}$ invertierbar, so dass $\phi(n^{-1}) = \phi(n)^{-1} = n^{-1}$. Dann

$$\phi\left(\frac{m}{n}\right) = \phi(mn^{-1}) = \phi(m)\phi(n^{-1}) = mn^{-1} = \frac{m}{n} \qquad \text{für alle } \frac{m}{n} \in \mathbb{Q}.$$

Das zeigt dass das einzige Ringhomomorphismus die Inklusion $\mathbb{Q} \hookrightarrow \mathbb{R}$ ist.

Beispiel 2.3.8. Sei $\phi\colon \mathbb{R} \to \mathbb{R}$ ein Ringhomomorphismus. Wir wollen zeigen dass ϕ die Identität ist: $\phi(x) = x$ für alle $x \in \mathbb{R}$.

- Die Einschränkung $\phi_{|\mathbb{Q}}\colon \mathbb{Q} \to \mathbb{R}$ ist ein Ringhomomorphismus, sodass $\phi(q) = q$ für alle $q \in \mathbb{Q}$.
- Wir zeigen dass $\phi(x) \geq 0$ für alle $x \geq 0$. Wenn $x \geq 0$, dann existiert eine Quadratwurzel $\sqrt{x} \in \mathbb{R}$ so dass $\phi(x) = \phi(\sqrt{x}^2) = \phi(\sqrt{x})^2$. Dann $\phi(x) \geq 0$ weil alle Quadrate in $\mathbb{R}$ nicht negativ sind.

- Wir zeigen dass ϕ monoton steigend ist. Wenn $x \leq y$, dann $y - x \geq 0$ so dass $\phi(y-x) \geq 0$. Aber $\phi(y-x) = \phi(y) - \phi(x)$ und dann $\phi(x) \leq \phi(y)$.
- Wir zeigen dass ϕ stetig ist. Seien $x \in \mathbb{R}$ und $\varepsilon > 0$. Wir wollen $\delta > 0$ finden so dass wenn $|x-y| \leq \delta$, dann $|\phi(x) - \phi(y)| < \varepsilon$. Sei $n > 0$ so dass $\frac{1}{n} < \varepsilon$ und sei $y \in \mathbb{R}$ so dass $|x-y| \leq \frac{1}{n}$. Das bedeutet dass $-\frac{1}{n} \leq y - x \leq \frac{1}{n}$ und da ϕ monoton steigend ist, wissen wir dass
$$-\frac{1}{n} = \phi\left(-\frac{1}{n}\right) \leq \phi(y) - \phi(x) \leq \phi\left(\frac{1}{n}\right) = \frac{1}{n},$$
so dass $|\phi(y) - \phi(x)| \leq \frac{1}{n} < \varepsilon$.
- Die Teilmenge $\mathbb{Q}$ ist dicht in $\mathbb{R}$, so dass für alle $x \in \mathbb{R}$ existiert eine Folge (q_n), mit $q_n \in \mathbb{Q}$ so dass $\lim_{n\to\infty} q_n = x$. Da ϕ stetig ist, folgt daraus, dass
$$\phi(x) = \phi\left(\lim_{n\to+\infty} q_n\right) = \lim_{n\to\infty} \phi(q_n) = \lim_{n\to\infty} q_n = x.$$

Beispiel 2.3.9. Es gibt mindestens zwei Ringhomomorphismen $\mathbb{C} \to \mathbb{C}$. Ein ist die Identiät, ein anderes ist die komplexe Konjugation
$$\phi\colon \mathbb{C} \to \mathbb{C}, \qquad \phi(z) = \overline{z}.$$
Diese ist ein Ringhomomorphismus weil $\overline{z+w} = \overline{z} + \overline{w}, \overline{z \cdot w} = \overline{z} \cdot \overline{w}$ für alle $z, w \in \mathbb{C}$ und $\overline{1} = 1$. Es gibt eigentlich viele andere "wilde" Ringhomomorphismen die man aber nicht leicht beschreiben kann: mehr Informationen befinden sich im Artikel *Automorphisms of the Complex Numbers*, Paul B. Yale, Mathematics Magazine Volume 39, 1966, pages 135-141, `https://doi.org/10.1080/0025570X.1966.11975699`.

Proposition 2.3.10. *Sei $\phi\colon R \to S$ ein Ringhomomorphismus. Der Kern $\ker\phi \subseteq R$ ist ein Ideal von R und das Bild $\operatorname{Im}\phi \subseteq S$ ist ein Unterring von S.*

Beweis. Wir zeigen dass $\ker\phi$ ein Ideal von R ist. Wir wissen schon dass der Kern eine Untegruppe ist. Wir müssen denn zeigen dass, wenn $a \in R, x \in \ker\phi$, dann $ax \in \ker\phi$, aber $\phi(ax) = \phi(a) \cdot \phi(x) = \phi(a) \cdot 0 = 0$.

Es ist leicht zu überprüfen dass das Bild ein Unterring von S ist. □

Wir führen nun eine Reihe von Aussagen auf, deren Beweis analog zu den ähnlichen Aussagen für Gruppen ist, so dass wir sie nicht explizit schreiben.

Lemma 2.3.11. *Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Die Projektion $\pi\colon R \to R/I$ ist ein surjektives Gruppenhomomorphismus und $\ker\pi = I$.*

Damit ist es einfach, die universelle Eigenschaft der Faktorgruppe zu beweisen

Satz 2.3.1 (Universelle Eigenschaft des Faktorrings)**.** *Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Sei $\phi\colon R \to S$ ein Ringhomomorphismus. Es gibt ein Ringhomomorphismus $\overline{\phi}\colon R/I \to S$ so dass*
$$\phi = \overline{\phi} \circ \pi,$$
genau dann, wenn $I \subseteq \ker\phi$. Außerdem ist $\overline{\phi}$, wenn es existiert, eindeutig

Satz 2.3.2 (Homomorphiesatz)**.** *Sei $\phi\colon R \to S$ ein Ringhomomorphismus. Dann die Abbildung*

$$\overline{\phi}\colon R/\ker\phi \longrightarrow \operatorname{im}\phi, \quad [x] \mapsto \phi(x)$$

ist ein Isomorphismus von Ringe.

Wir betrachten jetzt die Ideale von eines Faktorrings R/I. Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal $\pi\colon R \to R/I$ die Projektion. Sei $H \subseteq R$ ein Ideal so dass $I \subseteq H$: wir betrachten H/I als Teilmenge von R/I:

$$H/I = \{[h] \in R/I \mid h \in H\}$$

Satz 2.3.3. *Seien R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Jedes Ideal von R/I hat die Form H/I für genau ein Ideal $H \subseteq R$ so dass $I \subseteq H$.*

Satz 2.3.4. *Seien R ein kommutativer Ring, und $I \subseteq H$ zwei Ideale. Dann die Abbildung*

$$(R/I)/(H/I) \longrightarrow R/H, \qquad [a] \mod H/I \mapsto [a] \mod H$$

ist ein Isomorphismus von Ringe.

2.4 Teilbarkeit und Primfaktorzerlegung

In der Schule haben wir gelernt, dass eine ganze Zahl eindeutig in Primfaktoren zerlegt werden kann. Wir diskutieren nun, wie man diese Theorie auf andere Ringe verallgemeinern kann.

Definition 2.4.1 (Teilbarkeit)**.** Seien R ein kommutativer Ring und $a, b \in R$. Wir sagen dass a teilt b wenn $h \in R$ existiert so dass $b = a \cdot h$. Das ist äquivalent zu $b \in (a)$ oder auch $(b) \subseteq (a)$. Wir schreiben $a|b$.

Definition 2.4.2 (Assoziertes Element)**.** Sei R ein kommutativer Ring. Zwei Elementen $a, b \in R$ sind assoziert wenn eine Einheit $u \in R^*$ existiert so dass $a = bu$.

Bemerkung 2.4.3. Sei R ein Integritätsbereich. Dann sind $a, b \in R$ assoziert genau dann, wenn $(a) = (b)$. Wir beweisen das: seien a, b assoziert, dann existiert eine Einheit $u \in R^*$ so dass $a = bu$ und $b = au^{-1}$, so dass $(a) \subseteq (b)$ und $(b) \subseteq (a)$. Andererseits, wenn $(a) = (b)$ dann existieren $h, k \in R$ so dass $a = bh$ und $b = ak$, so dass $a = ahk, b = bhk$. Das bedeutet $a(hk - 1) = b(1 - hk) = 0$ und wenn R ein Integritätsbereich ist, dann entweder $a = b = 0$ oder $hk = 1$. in beiden Fällen sind a, b assoziert.

Definition 2.4.4 (Primelement)**.** Sei R ein kommutativer Ring. Ein Element $p \in R$ heißt prim, wenn $p \neq 0$, p keine Einheit ist und für alle $a, b \in R$ gilt:

$$p|ab \implies p|a, \text{ oder } p|b$$

Das bedeutet genau dass das Ideal (p) prim ist.

Definition 2.4.5 (Irreduzibel Element)**.** Sei R ein kommutativer Ring. Ein Element $f \in R$ heißt irreduzibel, wenn $f \neq 0$, f keine Einheit ist und aus $f = ab$ folgt dass entweder a oder b eine Einheit ist.

Bemerkung 2.4.6. Ein Element $f \in R$ ist irreduzibel ist, genau dann wenn, für jedes Element $a \in R$ mit $a|f$, a ist entweder invertierbar oder assoziert zu f.

Lemma 2.4.7. *Seien R ein Integritätsbereich und $p \in R$ ein Primelement. Dann ist p auch irreduzibel.*

Beweis. Seien $a, b \in R$ so dass $p = ab$. Dann $p|ab$ und dann $p|a$ oder $p|b$. Nehmen wir an, dass $p|a$. Dann existiert $h \in R$ so dass $a = ph$, und $p = ab = phb$. Das bedeutet dass $p(1 - hb) = 0$ und da R ein Integritätsbereich ist und $p \neq 0$, folgt dass $hb = 1$, so dass b eine Einheit ist. □

Bemerkung 2.4.8. Es ist nicht immer wahr dass ein irreduzibel Element auch prim ist. Wir werden zeigen dass das in Ringe wie $\mathbb{Z}$ oder $\mathbb{R}[x, y]$ gilt aber wir werden auch ein Gegenbeispiel geben.

2.4.1 Euklidische Ringe, Hauptidealringe und faktorielle Ringe

Definition 2.4.9. Ein Integritätsbereich R heißt Euklidisch, falls eine Bewertungsfunktion

$$v \colon R \setminus \{0\} \to \mathbb{N}$$

existiert so dass für alle $a, b \in R, b \neq 0$ ein Quotient $q \in R$ und ein Rest $r \in R$ existieren so dass

- $a = qb + r$.
- $r = 0$ oder $v(r) < v(b)$.

Beispiel 2.4.10. Die ganze Zählen $\mathbb{Z}$ sind ein euklidische Ring mit der Bewertungsfunktion $v(n) = |n|$.

Beispiel 2.4.11. Sei K ein Körper, z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{Z}$. Dann ist der Polynomring $K[x]$ mit der Bewertungsfunktion $v(f) = \deg(f)$ ein euklidische Ring. Wir zeigen das: seien $f, g \in K[x]$ zwei Polynome mit $g \neq 0$. Wenn $\deg(f) < \deg(g)$ dann können wir einfach $f = 0 \cdot g + f$ schreiben. Wenn $\deg(g) \leq \deg(f)$, dann existieren $n \geq 0, k \geq 0$ so dass

$$\begin{aligned} g &= a_n x^n + \cdots + a_0, \qquad a_n \neq 0 \\ f &= b_{n+k} x^{n+k} + \cdots + b_0 \qquad b_{n+k} \neq 0 \end{aligned}$$

Und dann

$$f = \left(\frac{b_{n+k}}{a_n} \cdot x^k \right) \cdot g + \left(f - \frac{b_{n+k}}{a_n} x^k \cdot g \right) = q_1 \cdot g + f_1$$

Hier brauchen wir dass K ein Körper ist, so dass $a_n \neq 0$ invertierbar ist. Falls $f_1 = 0$ sind wir fertig. Falls $f_1 \neq 0$, dann $\deg(f_1) < \deg(f)$. Falls $\deg(f_1) < \deg(g)$ dann sind wir fertig. Falls $\deg(f_1) \geq \deg(g)$ können wir das Verfahren wiederholen, und wir finden q_2, f_2 so dass

$$\begin{aligned} f_1 &= q_2 \cdot g + f_2 \\ f &= q_1 \cdot g + f_1 = (q_1 + q_2) \cdot g + f_2 \end{aligned}$$

mit $f_2 = 0$ oder $f_2 \neq 0$ und $\deg(f_2) < \deg(f_1)$. Wenn $f_2 = 0$ oder $f_2 \neq 0$ und $\deg(f_2) < \deg(g)$ dann sind wir fertig. Sonst, wenn $f_2 \neq 0$ und $\deg(g) \leq \deg(f_2)$, können wir das Verfahren wiederholen und wir finden q_3, f_3 so dass

$$\begin{aligned} f_2 &= q_3 \cdot g + f_3 \\ f &= (q_1 + q_2 + q_3) \cdot g + f_3 \end{aligned}$$

mit $f_3 = 0$ oder $f_3 \neq 0$ und $\deg(f_3) < \deg(f_2)$. Wir können das Verfahren nicht für immer wiederholen, sonst haben wir eine unendliche Folge $\deg(f) > \deg(f_1) > \deg(f_2) > \deg(f_3) > \ldots$ von nicht-negative ganze Zählen, was unmöglich ist. Das bedeutet dass wir können schreiben

$$f = (q_1 + q_2 + \cdots + q_h) \cdot g + f_h$$

mit $f_h = 0$ oder $f_h \neq 0$ und $\deg(f_n) < \deg(g)$.

Beispiel 2.4.12. Das ist vielleicht kompliziert. Um das besser zu verstehen, betrachten wir ein konkretes Beispiel, mit $f = x^4 - 1, g = x^2 + 2x + 1$.

$$\begin{aligned} f &= x^2 \cdot g + (f - x^2 \cdot g) \\ &= x^2 \cdot g + (x^4 - 1 - x^4 - 2x^3 - x^2) \\ &= x^2 \cdot g + (-2x^3 - x^2 - 1) \\ &= q_1 \cdot g + f_1 \end{aligned}$$

mit $q_1 = x^2, f_1 = -2x^3 - x^2 - 1$. Da $f_1 \neq 0, \deg(f_1) > \deg(g)$ wir wiederholen

$$\begin{aligned} f_1 &= -2x \cdot g + (f_1 + 2x \cdot g) \\ &= -2x \cdot g + (-2x^3 - x^2 - 1 + 2x^3 + 4x^2 + 2x) \\ &= -2x \cdot g + (3x^2 + 2x - 1) \\ &= q_2 \cdot g + f_2 \end{aligned}$$

mit $q_2 = -2x, f_2 = 3x^2 + 2x - 1$. Da $\deg(f_2) \geq \deg(g)$ wir wiederholen:

$$\begin{aligned} f_2 &= 3 \cdot g + (f_2 - 3 \cdot g) \\ &= 3 \cdot g + (3x^2 + 2x - 1 - 3x^2 - 6x - 3) \\ &= 3 \cdot g + (-4x - 4) \\ &= q_3 \cdot g + f_3 \end{aligned}$$

mit $q_3 = 3$ und $f_3 == 4x - 4$. Da $\deg(f_3) < \deg(g)$, sind wir fertig und wir finden dass

$$\begin{aligned} f &= (q_1 + q_2 + q_3) \cdot g + f_3 \\ &= (x^2 - 2x + 3) \cdot g + (-4x - 4). \end{aligned}$$

Satz 2.4.1. *Sei R ein euklidischer Ring. Dann ist jedes Ideal $I \subseteq R$ ein Hauptideal: $I = (b)$ für ein $b \in R$.*

Beweis. Wenn $I = (0)$ dann ist I ein Hauptideal. Wenn $I \neq 0$, sei $b \in I$ so dass $v(b) = \min\{v(x) \mid x \in I, x \neq 0\}$. Wir zeigen dass $I = (b)$. Sei $a \in I, a \neq 0$. Dann existieren $q, r \in R$ so dass $a = q \cdot b + r$, mit $r = 0$ oder $v(r) < v(b)$. Da $r = a - qb$, sehen wir dass $r \in I$, weil $a \in I$ und $b \in I$. Wenn $r \neq 0$, dann $v(r) \leq v(b)$ aber das ist unmöglich. Dann es muss sein dass $r = 0$ und $a = qb$. Das zeigt dass $a \in (b)$ so dass $I \subseteq (b)$. Da $b \in I$, gilt auch $(b) \subseteq I$, und $I = (b)$. □

Definition 2.4.13 (Hauptidealring)**.** Ein Hauptidealring ist ein Integritätsbereich wo alle ideale Hauptideale sind.

Bemerkung 2.4.14. Wir haben gerade gezeigt dass jeder euklidischer Ring ein Hauptidealring ist. Insbesondere, sind $\mathbb{Z}$ und $K[x]$ mit K Körper, Hauptidealringe. Es ist aber nicht wahr dass jeder Hauptidealring ein euklidischer Ring ist: ein Gegenbeispiel ist der folgende Unterring von $\mathbb{C}$

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + \left(\frac{1+\sqrt{-19}}{2}\right) b \,|\, a, b \in \mathbb{Z}\right\}$$

Wir werden nicht zeigen dass dieser Ring ein Hauptidealring und kein euklidischer Ring ist. Als Hausaufgabe kann man aber zeigen dass diese Menge ein Unterring von $\mathbb{C}$ ist.

Wir wollen jetzt Zeigen dass wir in einem Hauptidealring eine Primfaktorzerlegung haben. Wir beginnen mit einigen vorbereitenden Arbeiten:

Proposition 2.4.15. *Sei R ein Hauptidealring und sei*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

eine unendliche aufsteigende Kette von echte Ideale $I_n \subsetneq R$. Dann die Kette ist stationär: es gibt $n_0 \in \mathbb{N}$ so dass $I_n = I_{n_0}$ für alle $n \geq n_0$.

Beweis. Sei $I = \bigcup_{n\geq 1} I_n$. Das ist ein Ideal von R: $0 \in I$ da $0 \in I_1$, wenn $a, b \in I$ dann existieren $n_1, n_2 \in \mathbb{N}$ so dass $a \in I_{n_1}, b \in I_{n_2}$. Ohne Einschränkung der Allgemeinheit, nehmen wir an dass $n_1 \leq n_2$. Dann $a, b \in I_{n_2}$ so dass $a + b \in I_{n_2}, -a \in I_{n_2}, xa \in I_{n_2}$ für alle $x \in R$. Dann $a + b \in I, -a \in I, ax \in I$ für alle $x \in R$. Das zeigt dass I ein Ideal ist. Das Ideal I müss auch ein echtes Ideal sein: sonst $1 \in I$ und dann existiert $n \in I_n$ mit $1 \in I_n$. Aber das ist unmöglich weil I ein echtes Ideal ist. Das zeigt dass I ein echtes Ideal ist. Da R ein Hauptidealring ist, existiert $d \in R$ mit $I = (d)$. Dann $d \in I$ und $d \in I_{n_0}$ für einem $n_0 \in \mathbb{N}$. Aber dann $I \leq I_{n_0}$ so dass $I_n \subseteq I_{n_0}$ für alle $n \geq n_0$. Das ist was wir zeigen wollten. □

Bemerkung 2.4.16. Die Proposition bedeutet genau dass keine undendliche aufsteigende Kette von echte Ideale existiert:

$$I_1 \subsetneq I_2 \subseteq I_3 \subsetneq I_4 \subsetneq \dots$$

Ein Ring mit dieser Eigenschaft heißt noetersch (nach die Mathematikerin Emmy Noether).

Proposition 2.4.17. *Sei R ein Hauptidealring. Ein Element $p \in R$ ist prim genau dann wenn es irreduzibel ist.*

Beweis. Da R ein Integritätsbereich ist, wissen wir dass ein Primelement auch irreduzibel ist. Andererseits, sei $p \in R$ irreduzibel und seien $a, b \in R$ so dass $p|ab$: $ab = pc$ für ein $c \in R$. Wir wollen zeigen dass $p|a$ oder $p|b$. Das bedeutet $a \in (p)$ oder $b \in (p)$. Wir betrachten das Ideal (a, p): da R ein Hauptidealring ist, existiert $d \in (a, p)$ so dass $(a, p) = (d)$. Insbesondere $d|p$. Da p irreduzibel ist, muss d entweder invertierbar oder assoziert zu p sein. Wenn d assoziert zu p ist, dann $(d) = (p)$ und $(a, p) = (d) = (p)$ so dass $a \in (p)$ und wir sind fertig. Wenn d invertierbar ist, dann $(a, p) = (d) = R$ so dass existieren $h, k \in R$ mit $ha + kp = 1$. Dann $hab + kpb = b$ und da $ab = pc$, sehen wir dass

$$b = hab + kbp = hcp + kbp = (hc + kb)p$$

so dass $b \in (p)$. □

Lemma 2.4.18. *Sei R ein Hauptidealring und $a \in R$, $a \neq 0, a \notin R^*$. Dann existiert $p \in R$ irreduzibel so dass $p|a$.*

Beweis. Wenn a irreduzibel ist, dann sind wir fertig. Wenn a nicht irreduzibel ist, existieren a_1, b_1 nicht invertierbar und nicht zu a assoziert so dass $a = a_1 b_1$. Insbesondere $(a) \subsetneq (a_1)$. Wenn a_1 oder b_1 irreduzibel ist, dann sind wir fertig. Sonst nehmen wir ohne Einschrankung der Allgemeinheit an dass a_1 nicht irreduzibel ist, so dass a_2, b_2 nicht invertierbar und nicht zu a_1 assoziert existieren mit $a_1 = a_2 b_2$. Insbesondere $(a) \subsetneq (a_1) \subsetneq (a_2)$. Wenn man so vorgeht, findet man eine aufsteigende Kette von echte Idealen:

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

Da R noetersch ist, die Kette kann nicht unendlich sein, so dass k existiert mit a_k irreduzibel. Dann gilt $a_k|a$. □

Satz 2.4.2. *Sei R ein Hauptidealring. Für jede $a \in R, a \neq 0$ und existieren $u \in R^*$ und $p_1, \dots, p_k \in R$ irreduzibel so dass*

$$a = u \cdot p_1 \cdot p_2 \cdot \dots p_k$$

Außerdem, wenn $a = u' \cdot p_1' \cdot p_2' \dots p_h'$ eine andere Zerlegung durch irreduzibel Elementen ist, dann $h = k$ und und jedes p_i ist mit einem der p_i' assoziiert und vice versa

Beweis. Wir zeigen zuerst dass eine Zerlegung existiert. Sei $a \in R, a \neq 0$ und a nicht invertierbar. Wir zeigen dass $p_1, a_1 \in R$ existieren mit p_1 irreduzibel, $a = p_1 a_1$ und $(a) \subsetneq (a_1)$. Um das zu zeigen, nutzen wir das vorheriges Lemma: es zeigt dass $p_1 \in R$ irreduzibel existiert mit $p_1|a$. Das bedeutet dass $a = p_1 a_1$ für ein $a_1 \in R$. Insbesondere $(a) \subseteq (a_1)$. Wenn $(a) = (a_1)$ dann sind a und a_1 assoziert, so dass $u \in R^*$ existiert mit $a = ua_1$. Dann $ua_1 = a = pa_1$ so dass $(u - p)a_1 = 0$. Da R ein Integritätsbereich ist, und $a_1 \neq 0$ das bedeutet dass $p = u$. Aber das ist unmöglich da p irreduzibel ist. Das zeigt dass $(a) \subsetneq (a_1)$.

Wir haben eine Zerlegung $a = p_1 a_1$ gefunden. Wenn a_1 invertierbar ist, dann sind wir fertig. Wenn nicht, existieren $p_2 \in R$ irreduzibel und $a_2 \in R$ mit $(a_1) \subsetneq (a_2)$ so dass $a_1 = p_2 a_2$. Dann $a = p_1 p_2 a_2$ und $(a) \subsetneq (a_1) \subsetneq (a_2)$. Da R noetersch ist, können wir diesen Vorgang nicht unendlich oft wiederholen, so dass ein a_k invertierbar sein muss und wir finden eine Zerlegung $a = up_1 p_2 \dots p_k$ mit p_i irreduzibel und $u = a_k$ invertierbar.

Das zeigt dass eine Zerlegung durch irreduzibel Elementen existiert. Seien jetzt $a = up_1 p_2 \dots p_k = u' p_1' p_2' \dots p_h'$, zwei Zerlegungen mit p_i, p_j' irreduzibel und $u, u' \in R^*$. Ohne Einschränkung der Allgemeinheit, nehmen wir an dass $k \leq h$. Wir haben dass $p_k|a$ und da p_k prim ist, existiert j so dass $p_k|p_j'$. Mit einer möglicher Umbenennung können wir davon ausgehen, dass $p_k|p_h'$. Da p_h' irreduzibel ist, sind p_k und p_h' assoziert, so dass $p_h' = u'' p_k$ mit u'' invertierbar. Dann

$$a = up_1 \dots p_{k-1} p_k = u' \cdot u'' p_1' \dots p_{h-1}' p_k$$

so dass

$$u \cdot p_1 \dots p_{k-1} = (u' \cdot u'') p_1' \cdot \dots p_{h-1}'$$

weil $p_k \neq 0$ ist und R ein Integritätsbereich ist. Wir können das Verfahren wiederholen und mit einer möglicher Umbenennung wir finden dass p_i und $p_{i+(h-k)}'$ für $i = 1, \dots, k$ assoziert sind, und

$$u = v \cdot p_1' \dots p_{h-k}'$$

mit $u, v \in R^*$. Wenn $h > k$ dann erscheint ein irreduzibel Element p'_1 an der rechte Seite, aber das ist unmöglich, weil diese Gleichung impliziert dass p'_1 invertierbar ist, da u invertierbar ist. Dann $h = k$ und p_i, p'_i sind assoziert für alle $i = 1, \ldots, k$. □

Definition 2.4.19 (Faktorieller Ring)**.** Ein Integritätsbereich R heißt faktoriell wenn jedes Element $a \in R, a \neq 0$ eine Zerlegung durch irreduzibel Elementen hat:

$$a = up_1p_2 \ldots p_k$$

mit $u \in R^*$ und p_i irreduzibel. Außerdem, wenn $a = u' \cdot p'_1 \cdot p'_2 \ldots p'_h$ eine andere Zerlegung durch irreduzibel Elementen ist, dann $h = k$ und und jedes p_i ist mit einem der p'_i assoziiert und vice versa

Bemerkung 2.4.20. Wir haben gezeigt dass Hauptidealringe und besonders Euklidische Ringe faktoriell sind. Nicht alle faktorielle Ringe sind aber Hauptidealringe: ein Gegenbeispiel ist $\mathbb{Z}[x]$.

Bemerkung 2.4.21. Sei R ein faktorieller Ring und sei $a \in R, a \neq 0$ und $a \notin R^*$. Wir können a als

$$a = p_1^{e_1} \ldots p_k^{e_k}$$

schreiben, womit $k > 0, e_i > 0$ und die p_i sind irreduzibel und paarweise nicht assoziert. Außerdem, wenn $a = {p'_1}^{e'_1} \ldots {p'_h}^{e'_k}$ mit $h > 0, e'_i > 0$ und die p'_i irreduzibel und paarweise nicht assoziert, dann $h = k$, und und wenn wir die Elemente umbenennen, können wir davon ausgehen, dass p_i und p'_i assoziert sind, und dass $e_i = e'_i$.

Lemma 2.4.22. *Sei R ein faktorieller Ring. Ein Element $p \in R$ ist prim genau dann, wenn es irreduzibel ist.*

Beweis. Sei $p \in R$ irreduzibel. Wir mussen zeigen dass p prim ist. Seien $a, b \in R$ so dass $p|ab$. Wir schreiben $a = u \prod p_i^{e_i}$ und $b = v \prod q_j^{f_j}$ als Produkt von irreduzibeln, so dass $ab = uv \prod p_i^{e_i} \cdot \prod q_j^{f_j}$ eine Zerlegung . Da $p|ab$, ist p ein Faktor in einer Zerlegung von ab in irreduzibeln Faktoren. Da R faktoriell ist, p ist assoziert zu einem von den p_i oder zu einem von den q_j, so dass $p|a$ oder $p|b$. □

Definition 2.4.23 (Größte gemeinsame Teiler und kleinste gemeinsame Vielfache)**.** Sei R ein faktorieller Ring und seien $a, b \in R$. Ein element $d \in R$ ist ein Größte gemeinsame Teiler von a, b wenn $d|a, d|b$ und wenn $d'|a$ und $d'|b$, dann $d'|d$. Wir schreiben

$$d = ggT(a, b).$$

Ein Element $m \in R$ ist ein kleinste gemeinsame Vielfache von $a, b \in R$ wenn $a|m, b|m$ und wenn $a|m', b|m'$, dann $m|m'$ auch. Wir schreiben

$$m = kgV(a, b)$$

Lemma 2.4.24. *Seien R ein faktorieller Ring und $a, b \in R$.*

1. *Seien d, d' zwei größte gemeinsame Teiler von a, b. Dann sind d, d' assoziert. Das gleiches gilt für zwei kleinste gemeinsame Vielfache.*
2. *Seien $d = ggT(a, b)$ und $m = kgV(a, b)$. Dann sind dm und ab assoziert.*

Beweis. Hausaufgabe □

Lemma 2.4.25. *Sei R ein faktorieller Ring und $a, b \in R$ zwei Elementen so dass*

$$a = p_1^{e_1} \dots p_r^{e_r} \cdot q_1^{n_1} \dots q_h^{n_h}$$
$$b = p_1^{e_1'} \dots p_r^{e_r'} \cdot t_1^{m_1} \dots t_k^{m_k}$$

womit alle p_i, q_i, t_i irreduzibel und paarweise nicht assoziert sind. Dann

$$(p_1^{\min\{e_1,e_1'\}} \cdot \dots \cdot p_k^{\min\{e_r,e_r'\}}) = ggT(a,b)$$
$$(p_1^{\max\{e_1,e_1'\}} \cdot \dots \cdot p_k^{\max\{e_r,e_r'\}}) \cdot \prod q_i^{m_i} \cdot \prod t_j^{n_j} = kgV(a,b)$$

Beweis. Hausaufgabe. □

Lemma 2.4.26. *Sei R ein Hauptidealring und seien $a, b \in R$. Es gilt $d = ggT(a,b)$ genau dann, wenn*

$$(a,b) = (d)$$

und es gilt $m = kgV(a,b)$ genau dann, wenn

$$(a) \cap (b) = (m)$$

Beweis. Wir sehen dass $d|a, d|b$ genau dann wenn $a, b \in (d)$ und das ist äquivalent zu $(a,b) \subseteq (d)$. Das bedeutet dass $ggT(a,b) = d$ genau dann wenn das Ideal (d) das kleinstes Hauptideal dass (a,b) enthält ist. Da jedes Ideal in R ein Hauptideal ist, das bedeutet genau dass $(a,b) = (d)$.

Vice versa, $a|m$ und $b|m$ is äquivalent zu $(m) \subseteq (a) \cap (b)$. Das bedeutet dass $m = kgV(a,b)$ genau dann wenn, das Ideal (m) das größte Hauptideal dass in $(a) \cap (b)$ enthält ist ist. Da jedes Ideal in R ein Hauptideal ist, bedeutet das genau dass $(a) \cap (b) = (m)$. □

Korollar 2.4.27 (Lemma von Bezout)**.** *Seien R ein Hauptidealring, $a, b \in R$ und $d = ggT(a,b)$. Dann existieren $h, k \in R$ so dass*

$$h \cdot a + k \cdot b = d.$$

Beweis. Das vorheriges Lemma zeigt dass $d \in (a,b) = \{ha + kb \,|\, h, k \in R\}$. □

In einem euklidischen Ring kann man ein ggT bestimmen auch ohne eine Zerlegung durch das **euklidische Algorithmus**: sei R ein euklidischer Ring mit Bewertungsfunktion $v\colon R \setminus \{0\} \to \mathbb{N}$ und seien $a, b \in R \setminus \{0\}$ mit $v(a) \geq v(b)$. Wir betrachten den folgenden Algorithmus:

- **Schritt 1**: Wir setzen $a_1 = a, b_1 = b$.
- **Schritt 2**: Wir berechnen die Division mit Rest von a_1 durch b_1:

  $$a_1 = q_1 \cdot b_1 + r_1 \qquad \text{mit } r_1 = 0, \text{ oder } v(r_1) < v(b_1).$$

  Insbesondere, sehen wir dass $(a,b) = (b,r)$.
- **Schritt 3**: Wenn $r = 0$, dann $b_1 = ggT(a_1, b_1)$ und wir sind fertig. Wenn, $r \neq 0$, wir setzen $a_2 = b_1, b_2 = r_1$ und wir wiederholen Schritt 2. Wir bemerken dass $(a_1, b_1) = (a_2, b_2)$.

Proposition 2.4.28. *Der euklidische Algorithmus stoppt und stoppt und erzeugt ein ggT von a und b*

Beweis. Das Algorithmus muss irgendwann stoppen, sonst haben wir eine unendliche Folge von nicht negative ganze Zahlen $v(b_1) > v(b_2) > v(b_3) > \dots$. Wenn das Algorithmus stoppt, finden wir b_n so dass $b_n = ggT(a_n, b_n)$, so dass

$$(b_n) = (a_n, b_n) = (a_{n-1}, b_{n-1}) = \cdots = (a_1, b_1) = (a, b)$$

Das zeigt dass $b_n = ggT(a, b)$. □

Beispiel 2.4.29. Wir berechnen das ggT von den zwei Polynome $a(x) = x^3 + 6x + 7$ und $b(x) = x^2 + 3x + 2$ durch den euklidischen Algorithmus: die erste Division ist

$$x^3 + 6x + 7 = (x - 3)(x^2 + 3x + 2) + (13x + 13)$$

Der Rest ist nicht null, so dass wir noch ein mal dividieren

$$x^2 + 3x + 2 = \left(\frac{1}{13}x + \frac{2}{13}\right)(13x + 13) + 0$$

Der Rest ist null, so dass

$$13x + 13 = ggT(a, b).$$

2.4.2 Polynome in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$

Wir wissen das $\mathbb{Q}[x]$ ein euklidischer Ring ist. Insbesondere, ist $\mathbb{Q}[x]$ faktoriell. Was können wir über $\mathbb{Z}[x]$ sagen?

Definition 2.4.30 (Primitives Polynom)**.** Ein Polynom $f(x) \in \mathbb{Z}[x]$ heißt primitiv, wenn

$$f(x) = a_n x^n + \cdots + a_0, \qquad a_i \in \mathbb{Z}, \qquad ggT(a_0, .., a_n) = 1.$$

Lemma 2.4.31. *Sei $f(x) \in \mathbb{Q}[x]$ ein Polynom. Dann existieren $m, n \in \mathbb{Z}$ teilerfremde so dass*

$$f(x) = \frac{a}{b}F(x)$$

mit $F(x) \in \mathbb{Z}[x]$ primitiv. Außerdem $f(x) \in \mathbb{Z}[x]$ genau dann, wenn eine solche Faktorisierung mit $b = 1$ existiert.

Beweis. Wir schreiben die Koeffizienten von $f(x)$ als Fraktionen

$$f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}, \quad a_i, b_i \in \mathbb{Z}, b_i \neq 0$$

Wenn $b' = b_0 \cdot \cdots \cdot b_1 b_0$, dann $b \in \mathbb{Z}$ und $f(x) = \frac{1}{b'}g(x)$, mit $g(x) \in \mathbb{Z}[x]$. Wir schreiben noch

$$g(x) = a'_n x^n + \dots a'_1 x + a'_0 = a' \cdot (a''_n x^n + \cdots + a''_1 x + a''_0) = a' \cdot F(x)$$

womit $a' = ggT(a'_0, \dots, a'_n)$ so dass $F(x)$ primitiv ist. Das bedeutet dass $f(x) = \frac{a'}{b'}F(x)$ mit $F(x)$ primitiv. Wir können auch die gemeinsame Primfaktoren von a', b' streichen, so das $\frac{a'}{b'} = \frac{a}{b}$ mit a, b teilerfremd. Das zeigt dass

$$f(x) = \frac{a}{b}F(x)$$

mit $a, b \in \mathbb{Z}$ teilerfremd und $F(x) \in \mathbb{Z}[x]$ primitiv. Wenn $b \in \mathbb{Z}^*$ es ist klar dass $f(x) \in \mathbb{Z}[x]$. Vice versa, wenn $f(x) \in \mathbb{Z}[x]$, dann

$$f(x) = \frac{a}{b}F(x) = \frac{a}{b}\left(c_n x^n + \cdots + c_0\right) = \frac{ac_n}{b}x^n + \cdots + \frac{ac_0}{b}$$

so dass $b|ac_i$ für alle i. Da b, a teilerfremd sind, es muss sein dass $b|c_i$ für alle i, so dass $b|ggT(c_0, \ldots, c_n) = 1$ und $b \in \mathbb{Z}^*$. Dann $\frac{a}{b} = \frac{ab^{-1}}{1}$. □

Lemma 2.4.32 (Lemma von Gauß - I)**.** *Seien $F(x), G(x) \in \mathbb{Z}[x]$ primitiv. Dann ist $F(x)G(x)$ auch primitiv.*

Beweis. Sei $h(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ ein Polynom. Dann $ggT(a_0, \ldots, a_n) = 1$ genau dann, wenn für jeden Primzahl $p \in \mathbb{Z}$ ein a_i existiert so dass $p \nmid a_i$, oder $[a_i] \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Anders ausgedrückt, $h(x)$ ist primitiv genau dann, wenn $[h(x)] = \sum_{i=0}^{n}[a_i]x^i$ nicht null in $(\mathbb{Z}/p\mathbb{Z})[x]$ ist, für alle Primzählen $p \in \mathbb{Z}$. Sei $p \in \mathbb{Z}$ ein Primzahl, da $F(x), G(x)$ primitiv sind, wissen wir dass $[F(x)], [G(x)] \neq 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Da $\mathbb{Z}/p\mathbb{Z}[x]$ ein Integritätsbereich ist, wissen wir dass $[F(x)G(x)] = [F(x)][G(x)] \neq 0$. Das zeigt dass $F(x)G(x)$ primitiv ist. □

Proposition 2.4.33 (Lemma von Gauß - II)**.** *Ein Polynom $f(x) \in \mathbb{Z}[x]$ ist irreduzibel in $\mathbb{Z}[x]$ genau dann, wenn*

1. $\deg(f(x)) = 0$ *und* $f(x) = p$ *mit* $p \in \mathbb{Z}$ *prim.*
2. $\deg(f(x)) > 0, f(x)$ *primitiv und irreduzibel in* $\mathbb{Q}[x]$.

Beweis. Wir lassen den Fall $\deg(f) = 0$ als Hausaufgabe. Wenn $\deg(f) > 0$, sei zuerst $f(x)$ primitiv und irreduzibel in $\mathbb{Q}[x]$. Sei auch $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. Da $f(x)$ irreduzibel in $\mathbb{Q}[x]$ ist, nehmen wir an dass $g(x)$ invertierbar in $\mathbb{Q}[x]$: das bedeutet dass $g(x) = a \in \mathbb{Z}$. Dann $f(x) = ah(x)$ und da $f(x)$ primitiv ist, es muss sein dass $a \in \mathbb{Z}^*$.

Vice versa, sei $f(x)$ irreduzibel in $\mathbb{Z}[x]$ wir schreiben

$$f(x) = aF(x), \quad a \in \mathbb{Z}, \quad F(x) \in \mathbb{Z}[x] \text{ primitiv}$$

Dann muss entweder a oder $F(x)$ invertierbar sein. Da $\deg f(x) > 0$ ist $\deg F(x) > 0$ auch, so dass a muss invertierbar sein. Das bedeutet dass $f(x)$ primitiv ist. Wir zeigen jetzt dass $f(x)$ irreduzibel in $\mathbb{Q}[x]$ ist. Seien $g(x), h(x) \in \mathbb{Q}[x]$ so dass

$$f(x) = g(x)h(x).$$

Wir wollen zeigen dass $g(x) = \frac{c}{d}G(x)$ mit $c, d \in \mathbb{Z}$ teilerfremd und $G(x) \in \mathbb{Z}[x]$ primitiv und $h(x) = \frac{e}{f}H(x)$ mit $e, f \in \mathbb{Z}$ teilerfremd und $H(x) \in \mathbb{Z}[x]$ primitiv. Dann

$$df \cdot f(x) = (c \cdot G(x)) \cdot (e \cdot H(x)) = ce \cdot G(x)H(x)$$

Die erste Version von dem Lemma von Gauß zeigt das $G(x)H(x)$ primitiv ist, so dass das ggT von alle Koeffizienten von $ceG(x)H(x)$ muss ce sein. Wir wissen auch das $f(x)$ primitiv ist, so dass das ggT von alle Koeffizienten von $df \cdot f(x)$ muss df sein. Dann sind df und ce in $\mathbb{Z}$ assoziert, so dass $ce = u \cdot df$ mit $u \in \mathbb{Z}^*$ und dann

$$f(x) = u \cdot G(x)H(x)$$

Da $f(x)$ irreduzibel in $\mathbb{Z}[x]$, es muss sein dass entweder $G(x)$ oder $H(x)$ invertierbar in $\mathbb{Z}[x]$ sind. Dann sind auch entweder $g(x), h(x)$ invertierbar in $\mathbb{Q}[x]$. Das zeigt dass $f(x)$ irreduzibel in $\mathbb{Q}[x]$ ist. □

Satz 2.4.3 (Lemma von Gauß - III)**.** *Der Ring $\mathbb{Z}[x]$ ist faktoriell.*

Beweis. Sei $f(x) \in \mathbb{Z}[x]$. Dann $f(x) \in \mathbb{Q}[x]$ und $f(x)$ hat eine Zerlegung:

$$f(x) = \frac{a_0}{b_0} p_1(x) \cdot \cdots \cdot p_h(x)$$

womit $a_0, b_0 \in \mathbb{Z}, b_0 \neq 0$ und $p_i(x)$ irreduzibel in $\mathbb{Q}[x]$. Wir schreiben $p_i(x) = \frac{a_i}{b_i} P_i(x)$ mit $a_i, b_i \in \mathbb{Z}$ teilerfremd und $P_i(x) \in \mathbb{Z}[x]$ primitiv. Da $p_i(x), P_i(x)$ assoziert sind, $P_i(x)$ muss irreduzibel in $\mathbb{Q}[x]$ sein, und da $P_i(x)$ primitiv ist, die zweite Version von dem Lemma von Gauß zeigt dass $P_i(x)$ irreduzibel in $\mathbb{Z}[x]$ ist. Dann $f(x) = \frac{a}{b} \cdot P_1(x) \dots P_h(x)$ so dass $bf(x) = a \cdot P_1(x) \cdot P_h(x)$. Wir sehen dass b teilt alle Koeffizienten von $bf(x)$, so dass b teilt das ggT von alle die Koeffizienten von $a \cdot P_1(x) \cdot P_h(x)$ aber die erste Version von dem Lemma von Gauß zeigt dass $P_1(x) \cdot P_h(x)$ ist primitiv, so dass b muss a teilen: $a = bd$, mit $d \in \mathbb{Z}$. Dann $f(x) = d \cdot P_1(x) \dots P_h(x)$, mit $P_i(x) \in \mathbb{Z}[x]$ primitiv und irreduzibel, und $d \in \mathbb{Z}$. Da d eine Zerlegung durch irreduzibeln in d hat, sehen wir das $f(x)$ eine Zerlegung hat.

Sei

$$d \cdot P_1(x) \dots P_h(x) = f(x) = e \cdot Q_1(x) \dots Q_k(x)$$

eine andere Zerlegung, womit $e \in \mathbb{Z}$ und $Q_i(x) \in \mathbb{Z}[x]$ irreduzibel mit positivem Grad. Die zweite Version von dem Lemma von Gauß zeigt dass die $Q_i(x)$ primitiv und irreduzibel in $\mathbb{Q}[x]$ sind. Da $\mathbb{Q}[x]$ faktoriell ist, es muss sein dass $h = k$ und dass (durch eine eventuelle Umbenennung) $P_i(x)$ und $Q_i(x)$ assoziert in $\mathbb{Q}[x]$ sind. Dann $P_i(x) = \frac{a}{b} Q_i(x)$ mit $a, b \in \mathbb{Z}$ und $bP_i(x) = aQ_i(x)$. Wenn wir dass ggT von alle Koeffizienten betrachten, sehen wir dass a, b assoziert in $\mathbb{Z}$ sind, so dass $P_i(x), Q_i(x)$ assoziert in $\mathbb{Z}[x]$ sind: $Q_i(x) = u_i \cdot P_i(x)$ mit $u_i \in \mathbb{Z}^*$. Dann

$$d = e \cdot (u_1 \cdot \cdots \cdot u_n)$$

und das zeigt dass auch d, e assoziert in $\mathbb{Z}$ sind. □

Bemerkung 2.4.34. Das zeigt dass $\mathbb{Z}[x]$ faktoriell ist. Da das Ideal $(2, x)$ kein Hauptideal ist, das ist auch ein Beispiel von einem faktoriellen Ring der kein Hauptidealring ist.

2.4.3 Das Eisensteinskriterium

Wir stellen jetzt ein nützliches Kriterium für Irreduzibilität in $\mathbb{Z}[x]$ vor:

Proposition 2.4.35 (Eisensteinskriterium)**.** *Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ ein Polynom von Grad $n > 0$ und sei $p \in \mathbb{Z}$ ein Primelement so dass $p \nmid a_n, p \mid a_i$ für alle $i = 0, \dots, n-1$ und $p^2 \nmid a_0$. Dann ist $f(x)$ in $\mathbb{Q}[x]$ irreduzibel.*

Beweis. Wir betrachten zuerst den Fall wo $f(x)$ auch primitiv ist. Wir wollen denn zeigen dass $f(x)$ irreduzibel in $\mathbb{Z}[x]$ ist. Seien $g(x), h(x) \in \mathbb{Z}[x]$ so dass $f(x) = g(x)h(x)$, mit $g(x) = b_m x^m + \cdots + b_0$ und $h(x) = c_\ell x^\ell + \cdots + c_0$. Nehmen wir an dass $m > 0, \ell > 0$. Wir betrachten alles modulo p so dass

$$[a_n] x^n = [f(x)] = [g(x)][h(x)] \qquad \text{in } \mathbb{Z}/p\mathbb{Z}[x]$$

Da $\mathbb{Z}/p\mathbb{Z}[x]$ faktoriell ist, es muss sein dass $[g(x)] = [b_m] x^m$ und $[h(x)] = c_\ell [x^\ell]$. Insbesondere $p | b_0$ und $p | c_0$. Aber dann $p^2 | b_0 c_0 = a_0$ und das ist unmöglich. Ohne Einschränkung der Allgemeinheit,

nehmen wir an dass $m = 0$ so dass $f(x) = b_0 h(x)$. Da $f(x)$ primitiv ist, es muss sein dass b_0 invertierbar in $\mathbb{Z}$ ist.

Wenn $f(x)$ nicht primitiv ist, wir schreiben $f(x) = aF(x)$ mit $a \in \mathbb{Z}$ und $F(x) \in \mathbb{Z}[x]$ primitiv. Dann man kann zeigen dass die Hypothesen vom Kriterium für $F(x)$ gelten. Dann ist $F(x) \in \mathbb{Q}[x]$ irreduzibel, und auch $f(x)$. □

Beispiel 2.4.36. Das Polynom $f(x) = 3x^4 + 15x^2 + 10$ ist irreduzibel in $\mathbb{Q}[x]$ dank dem Eisensteinskriterium mit $p = 5$. Da $f(x)$ primitiv ist, es ist auch in $\mathbb{Z}[x]$ irreduzibel.

Beispiel 2.4.37. Wir betrachten das Polynom $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ womit $p \in \mathbb{N}$ ein Primzahl ist. Wir wollen zeigen dass $f(x)$ irreduzibel ist. Wir können das Eisensteinskriterium hier nicht anwenden, wir betrachten aber das Polynom $f(x+1)$. Um $f(x+1)$ zu berechnen, wir betrachten zuerst dass

$$f(x)(x-1) = x^p - 1$$

so dass

$$f(x+1) \cdot x = (x+1)^p - 1 = \sum_{h=1}^{p} \binom{p}{h} x^h$$

und

$$f(x+1) = \sum_{h=1}^{p} \binom{p}{h} x^{h-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k = \sum_{k=0}^{p-1} a_k x^k.$$

Die Koeffizienten von $f(x+1)$ sind

$$\binom{p}{k+1} = \frac{p(p-1) \cdot \cdots \cdot (p-k)}{(k+1)!}$$

so dass $a_{p-1} = 1, a_0 = p$ und $p | a_k$ für alle $k < p-1$ (Warum?). Wir können das Eisensteinskriterium mit der Primzahl p anwenden und wir sehen dass $f(x+1)$ irreduzibel ist. Es folgt dass $f(x)$ irreduzibel ist (Warum?).