Algebra I

Jean-Stefan Koskivirta

Universität Paderborn WS2015

Inhaltsverzeichnis

1 Gruppen

1.1 Kürzbarkeit, Invertierbarkeit

Sei M eine Menge. Eine Verknüpfung auf M ist eine Abbildung

$$M \times M \to M,\ (a,b) \mapsto a \cdot b$$

Diese Verknüpfung heißt *assoziativ*, falls für alle $a, b, c \in M$ die Gleichung

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

gilt.

Definition 1.1. Eine *Halbgruppe* $(M, \cdot)$ ist eine Menge M zusammen mit einer azossiativen Verknüpfung $(a, b) \mapsto a \cdot b$.

Eine Halbgruppe M heißt *kommutativ* oder *abelsch* falls für alle $a, b \in M$ die Gleichung $a \cdot b = b \cdot a$ gilt.

Bemerkung 1.2. Wir schreiben manchmal ab statt $a \cdot b$. Die Verknüpfung wird auch Multiplikation genannt, oder Addition im kommutativen Fall.

Beispiel 1.3.

(a) $(\mathbb{N}, +)$ ist eine kommutative Halbgruppe.

(b) $(\mathbb{N}, \times)$ ist eine kommutative Halbgruppe.

(c) Sei X eine Menge. Sei $\mathrm{Abb}(X)$ die Menge aller Abbildungen von X nach X. Dann ist $(\mathrm{Abb}(X), \circ)$ eine Halbgruppe.

Definition 1.4. Sei M eine Halbgruppe. Ein Element $e \in M$ heißt *linksneutral*, falls für alle $a \in M$ die Gleichung $e \cdot a = a$ gilt. Ein Element $e \in M$ heißt *rechtsneutral*, falls für alle $a \in M$ die Gleichung $a \cdot e = a$ gilt.

Lemma 1.5. *Sei M eine Halbgruppe. Sei e ein linksneutrales Element und sei e' ein rechtsneutrales Element. Dann gilt $e = e'$.*

Beweis. $e' = e \cdot e' = e$. □

Definition 1.6. Ein Element das sowohl rechts- als auch linksneutral ist heißt *das neutrale Element*, *das Einselement*, oder *die Eins*.

Bemerkung 1.7. Nach Lemma 1.5 is das neutrale Element eindeutig, wenn es existiert.

Beispiel 1.8.

(a) 0 ist das neutrale Element von $(\mathbb{N}, +)$.

(b) 1 ist das neutrale Element von $(\mathbb{N}, \times)$.

(c) Die Identitätsabbildung id_X ist das neutrale Element von $(\mathrm{Abb}(X), \circ)$.

Sei M eine Halbgruppe. Für jedes $a \in M$, definiert man zwei Abbildungen:

$$R_a : M \to M, \quad x \mapsto x \cdot a$$

$$L_a : M \to M, \quad x \mapsto a \cdot x.$$

Definition 1.9. Sei M eine Halbgruppe. Ein Element $a \in M$ heißt *linkskürzbar*, falls für alle $x, y \in M$

$$a \cdot x = a \cdot y \Longrightarrow x = y$$

gilt, bzw. *rechtskürzbar*, falls für alle $x, y \in M$

$$x \cdot a = y \cdot a \Longrightarrow x = y$$

gilt. Ein Element, das sowohl links- als auch rechtskürzbar ist, heißt *kürzbar*.

Bemerkung 1.10. Mit anderen Worten ist a genau dann linkskürzbar, wenn die Abbildung L_a injektiv ist. Entsprechend ist a genau dann rechtskürzbar, wenn die Abbildung R_a injektiv ist.

Sei nun M eine Halbgruppe mit Einselement e.

Definition 1.11. Sind $a, b \in M$ und gilt $a \cdot b = e$, so heißt a ein *Linksinverses* zu b und entsprechend b ein *Rechtsinverses* zu a. Außerdem heißt ein Element *rechtsinvertierbar* falls es ein Rechtsinverses besitzt, bzw. *linksinvertierbar* falls es ein Linksinverses besitzt. Ein *invertierbares Element* ist ein Element, das sowohl linksinvertierbar, als auch rechtsinvertierbar ist.

Bemerkung 1.12. Ein Element $a \in M$ ist genau dann linksinvertierbar, wenn die Abbildung R_a surjektiv ist. Entsprechend ist a rechtsinvertierbar, falls die Abbildung L_a surjektiv ist.

Lemma 1.13. *Ein linksinvertierbares Element ist linkskürzbar. Ein rechtsinvertierbares Element ist rechtskürzbar. Ein invertierbares Element ist kürzbar.*

Beweis. Sei $a' \in M$ ein Linksinverses von $a \in M$. Für $x, y \in M$ gilt

$$\begin{aligned} a \cdot x = a \cdot y &\Longrightarrow a' \cdot (a \cdot x) = a' \cdot (a \cdot y) \\ &\Longrightarrow (a' \cdot a) \cdot x = (a' \cdot a) \cdot y \\ &\Longrightarrow e \cdot x = e \cdot y \\ &\Longrightarrow x = y. \end{aligned}$$

□

Lemma 1.14. *Sei $a \in M$ und seien $a' \in M$ ein Linksinverses und $a'' \in M$ ein Rechtsinverses von a. Dann gilt $a' = a''$.*

Beweis. $a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''$ □

Definition 1.15. Ein zu a sowohl linksinverses als auch rechtsinverses Element heißt *das Inverse* zu a, und wird mit a^{-1} bezeichnet.

Bemerkung 1.16. Ist a invertierbar, so ist das Inverse zu a eindeutig nach Lemma 1.14.

Bemerkung 1.17. Für invertierbare Elemente $a_1, ..., a_n$ einer Halbgruppe ist das Produkt $a_1 a_2 ... a_n$ inertierbar, und es gilt : $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} ... a_2^{-1} a_1^{-1}$.

Potenzschreibweise Für ein Element a einer Halbgruppe und $n \in \mathbb{Z}$, definiert man

$$a^n := \begin{cases} a \cdot a \cdot ... \cdot a \quad (n\text{-mal}) & \text{falls } n \geq 1 \\ e & \text{falls } n = 0 \\ a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1} \quad (-n\text{-mal}) & \text{falls } n \leq -1 \text{ und } a \text{ invertierbar.} \end{cases}$$

Für $r, s \in \mathbb{Z}$, gilt $a^{r+s} = a^r \cdot a^s$ und $(a^r)^s = a^{rs}$.

Anmerkung zur Notation. Wenn die Halbgruppe M kommutativ ist, notiert man die Verknüpfung oft auch durch "+ßtatt "·". In diesem Fall wird das Einselement mit 0 bezeichnet, und heißt das Nullelement, oder die Null. Außerdem notiert man das Inverse zu a durch $-a$ statt a^{-1} und man schreibt oft na statt a^n für $n \in \mathbb{Z}$.

Verknüpfung	Neutrales Element	Inverse	Potenz
$\cdot$ oder $\times$	e oder 1	a^{-1}	a^n
$+$	0	$-a$	na

Wenn die Verknüpfung durch + bezeichnet wird, schreibt man oft $a-b$ statt $a+(-b)$ für Elemente a, b, mit b invertierbar. Wenn $(M, \cdot)$ eine kommutative Halbgruppe ist, schreibt man manchmal $\frac{a}{b}$ statt $a \cdot (b^{-1})$ für a, b Elemente in M mit b invertierbar. Im nichtkommutativen Fall soll man diese Notation vermeiden, denn man weiß nicht, ob $a \cdot b^{-1}$ oder $b^{-1} \cdot a$ gemeint ist.

Definition 1.18. Eine *Gruppe* ist eine Halbgruppe, in der ein neutrales Element und zu jedem Element ein Inverses existieren.

Beispiel 1.19.

(a) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe.

(b) $(\mathbb{Q}_{>0}, \times)$ und $(\mathbb{Q}^*, \times)$ sind kommutative Gruppen

(c) $(GL_n(\mathbb{R}), \times)$ ist eine Gruppe (nicht kommutativ für $n \geq 2$.)

Lemma 1.20. *Sei $(M, \cdot)$ eine Halbgruppe mit Einselement e. Die Menge der invertierbaren Elemente:*

$$\mathrm{inv}(M) := \{a \in M, \text{ invertierbar}\}$$

mit der Verknüpfung $\cdot$ ist eine Gruppe.

Beweis. Sind a, b invertierbar, so ist ab auch invertierbar. Die Verknüpfung $\cdot$ induziert also durch Einschränkung eine assoziative Verknüpfung $\mathrm{inv}(M) \times \mathrm{inv}(M) \to \mathrm{inv}(M)$. Es gilt natürlich $e \in \mathrm{inv}(M)$. Ist $a \in \mathrm{inv}(M)$, so gilt $aa^{-1} = a^{-1}a = e$. Dann ist $a^{-1} \in \mathrm{inv}(M)$ mit $(a^{-1})^{-1} = a$. Es folgt, dass $\mathrm{inv}(M)$ eine Gruppe ist. □

Beispiel 1.21.

(a) Für $(M, \cdot) = (\mathbb{N}, +)$ gilt $\mathrm{inv}(M) = \{0\}$.

(b) Für $(M, \cdot) = (\mathbb{Z}, \times)$ gilt $\mathrm{inv}(M) = \{1, -1\}$.

(c) Sei X eine Menge. Für $(M, \cdot) = (\mathrm{Abb}(X), \circ)$ ist $\mathrm{inv}(M)$ die Menge der bijektiven Abbildungen von X nach X und heißt die symmetrische Gruppe von X, und wird mit $\mathrm{Sym}(X)$ bezeichnet.

(d) In der Halbgruppe $(M_n(\mathbb{R}), \times)$ gilt $\mathrm{inv}(M) = GL_n(\mathbb{R})$.

Übung 1.22.

(a) Sei $f \in \mathrm{Abb}(X)$ eine Abbildung $f : X \to X$. Zeige:

  (i) f ist genau dann rechtskürzbar, wenn f surjektiv ist.

  (ii) f ist genau dann linkskürzbar, wenn f injektiv ist.

  (iii) f ist genau dann invertierbar, wenn f bijektiv ist.

(b) Sei M eine endliche Halbgruppe mit Einselement e, in der jedes Element linkskürzbar ist. Dann ist M eine Gruppe.

1.2 Kürzbare Halbgruppen und die Grothendieck-Gruppe

Eine Relation auf einer Menge X ist eine Teilmenge $R \subset X \times X$. Gilt $(x, y) \in R$, so schreibt man $x \sim y$. Eine Relation $\sim$ auf einer Menge X heißt Äquivalenzrelation, falls die folgenden Eigenschaften erfüllt sind:

(i) Für alle $x \in X$ gilt $x \sim x$ (Reflexivität).

(ii) Für alle $x, y \in X$ gilt $x \sim y \Rightarrow y \sim x$ (Symmetrie).

(iii) Für alle $x, y, z \in X$ gilt $x \sim y$ und $y \sim z \Rightarrow x \sim z$ (Transitivität).

Für $x \in X$ definiert man dann die Äquivalenzklasse von x durch:

$$[x] := \{y \in X,\ x \sim y\}.$$

Die Menge der Äquivalenzklassen wird mit $X/\sim$ bezeichnet.

Lemma 1.23. *Die Äquivalenzklassen bilden eine Partition von X, d.h X ist die disjunkte Vereinigung aller Äquivalenzklassen.*

Beweis. Wir müssen zeigen, dass jedes Element von X in einer Klasse liegt, und dass zwei Klassen entweder disjunkt oder gleich sind. Es gilt $x \in [x]$ für alle $x \in X$, weil $\sim$ reflexiv ist. Wenn $z \in [x] \cap [y]$ gilt, dann gilt per Definition $z \sim x$ und $z \sim y$. Es folgt $x \sim y$. Für alle $w \in X$ gilt also

$$w \in [x] \Longleftrightarrow w \sim x \Longleftrightarrow w \sim y \Longleftrightarrow w \in [y]$$

und es folgt $[x] = [y]$. □

Sei $(M, +)$ eine kommutative Halbgruppe mit Nullelement 0. Wir definieren eine Relation auf $M \times M$ durch:

$$(a, b) \sim (a', b') \Longleftrightarrow \exists c \in M \text{ mit } a + b' + c = a' + b + c.$$

Lemma 1.24. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $M \times M$.*

Beweis. Die Reflexivität und die Symmetrie von $\sim$ sind klar. Wir zeigen die Transitivität. Seien a, b, a', b', a'', b'' in M mit $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$. Es existiert $c, d \in M$ mit

$$\begin{cases} a + b' + c = a' + b + c' \\ a' + b'' + d = a'' + b' + d. \end{cases}$$

Dann gilt

$$a + b'' + (a' + b' + c + d) = b + a'' + (a' + b' + c + d)$$

also es gilt auch $(a, b) \sim (a'', b'')$. □

Sei

$$\mathcal{G}(M) = (M \times M)/\sim$$

die Menge der Äquivalenzklassen. Wir schreiben $[a, b]$ (statt $[(a, b)]$) für die Äquivalenzklasse von $(a, b) \in M \times M$. Wir definieren eine Verknüpfung $\oplus$ auf $\mathcal{G}(M)$ durch

$$[a, b] \oplus [a', b'] := [a + a', b + b'].$$

Wir müssen zeigen, dass diese Definition sinnvoll ist. Wenn die Gleichungen $[a, b] = [a_1, b_1]$ und $[a', b'] = [a'_1, b'_1]$ gelten, so muss die Gleichung $[a+a', b+b'] = [a_1+a'_1, b_1+b'_1]$ auch gelten. Das ist tatsächlich der Fall. Angenommen es gilt

$$\begin{cases} a + b_1 + c = a_1 + b + c \\ a' + b'_1 + d = a'_1 + b' + d \end{cases}$$

für Elemente c, d in M. Dann gilt es

$$a + a' + b_1 + b'_1 + c + d = b + b' + a_1 + a'_1 + c + d$$

und dies zeigt, dass die Verknüpfung $\oplus$ wohldefiniert ist. Sie ist assoziativ und kommutativ, und das Element $[0, 0]$ ist das neutrale Element. Für $(a, b) \in M \times M$ gilt

$$[a, b] \oplus [b, a] = [a + b, a + b] = [0, 0]$$

weil $(c, c) \sim (0, 0)$ für alle $c \in M$ gilt. Diese Gleichung zeigt, dass jedes Element $[a, b] \in \mathcal{G}(M)$ invertierbar ist.

Satz 1.25. *$(\mathcal{G}(M), \oplus)$ ist eine kommutative Gruppe. Sie heißt die Grothendieck-Gruppe von M.*

Wir definieren eine Abbildung

$$\alpha : M \to \mathcal{G}(M), \quad a \mapsto [a, 0].$$

Man sieht sofort, dass die Gleichung $\alpha(a + b) = \alpha(a) \oplus \alpha(b)$ für alle $a, b \in M$ gilt.

Definition 1.26. Eine Halbgruppe M heißt *kürzbar* falls jedes Element von M kürzbar ist.

Eine Gruppe ist natürlich kürzbar, weil jedes Element sogar invetierbar ist, und ein invertierbares Element ist insbesondere kürzbar (Lemma 1.13).

Proposition 1.27. *Die Abbildung α ist genau dann injektiv, wenn M kürzbar ist. Ist $(M, +)$ eine Gruppe, so ist α bijektiv.*

Beweis. Wenn α injektiv ist, so gilt für alle $(a, b) \in M \times M$:

$$\begin{aligned} a + c = b + c &\Longrightarrow \alpha(a) \oplus \alpha(c) = \alpha(b) \oplus \alpha(c) \\ &\Longrightarrow \alpha(a) = \alpha(b) \\ &\Longrightarrow a = b. \end{aligned}$$

Die Halbgruppe M ist also kürzbar. Umgekehrt, seien $a, b \in M$ mit $\alpha(a) = \alpha(b)$. Dann existiert $c \in M$ mit $a + c = b + c$. Ist M kürzbar, so folgt daraus $a = b$, also α ist injektiv.

Angenommen M ist eine Gruppe. Für $(a, b) \in M \times M$ gilt $[a, b] = [a-b, 0] = \alpha(a-b)$, also α ist auch surjektiv. □

Beispiel 1.28. Sei M die abelsche Halbgruppe $(\mathbb{N}, +)$. Für $(a, b) \in \mathbb{N} \times \mathbb{N}$ ist die Äquivalenzklasse $[a, b]$ die Menge der Paare $(a', b') \in \mathbb{N} \times \mathbb{N}$, so dass ein $c \in \mathbb{N}$ existiert mit $a + b' + c = a' + b + c$. Da $(\mathbb{N}, +)$ kürzbar ist, folgt es dann $a + b' = a' + b$. Es gilt also:

$$[a, b] = \{(a', b') \in \mathbb{N} \times \mathbb{N}, \quad \text{mit } a + b' = a' + b\}.$$

Wir definieren eine Abbildung:

$$\beta : \mathcal{G}(M) \longrightarrow \mathbb{Z} \tag{1.1}$$

durch $\beta([a, b]) = a - b$. Diese Abbildung ist wohldefiniert: Wenn $[a, b] = [a', b']$ gilt, dann ist $a + b' = a' + b$, also $a - b = a' - b'$. Die Abbildung β ist injektiv: Wenn $\beta([a, b]) = \beta([a', b'])$ gilt, dann ist $a - b = a' - b'$, also $a + b' = a' + b$, und es folgt $[a, b] = [a', b']$. Die Abbildung β ist auch surjektiv: Für alle $c \in \mathbb{Z}$ existieren $a, b \in \mathbb{N}$ mit $c = a - b$. Dann gilt $c = \beta([a, b])$.

Proposition 1.29. *Die Abbildung β ist bijektiv.*

Außerdem besitzt β die folgende Eigenschaft:

$$\begin{aligned} \beta([a, b] \oplus [a', b']) &= \beta([a + a', b + b']) \\ &= (a + a') - (b + b') \\ &= (a - b) + (a' - b') \\ &= \beta([a, b]) + \beta([a', b']). \end{aligned}$$

Unten ist eine Darstellung der Äquivalenzklassen in $\mathbb{N} \times \mathbb{N}$ und der Abbildung β. Für $(a, b) \in \mathbb{N} \times \mathbb{N}$, sei $L(a, b)$ die Gerade in der Ebene mit Steigung 1, die den Punkt (a, b) enthält. Die Äquivalenzklasse von (a, b) ist dann der Durchschnitt von $L(a, b)$ und $\mathbb{N} \times \mathbb{N}$. Die Zahl $\beta([a, b])$ ist der Schnittpunkt von $L(a, b)$ mit der Abszissenachse.

Übung 1.30. Sei $(M, \cdot)$ eine Halbgruppe.

(a) Zeige: Sind $a, b \in M$ kürzbar, so ist das Produkt ab auch kürzbar.

(b) Sei $\mathrm{KB}(M)$ die Menge der kürzbaren Elemente von M. Zeige, dass die Verknüpfung $\cdot$ durch Einschränkung eine Struktur einer Halbgruppe auf $\mathrm{KB}(M)$ induziert.

(c) Angenommen M ist abelsch, zeige, dass die Umkehrung von (i) gilt, d.h. wenn ab kürzbar ist, so sind a und b auch kürzbar.

Übung 1.31. Was ist die Grothendieck-Gruppe von $(\mathbb{N}, \times)$?

Übung 1.32.

(a) Für $a, b \in \mathbb{N}$, sei $a \cdot b := \max\{a, b\}$. Zeige, dass $\cdot$ eine assoziative kommutative Verknüpfung ist, und dass ein Einselement existiert.

(b) Was sind die invertierbaren Elemente ?

(c) Was sind die kürzbaren Elemente ?

(d) Zeige, dass die Grothendieck-Gruppe von $(M, \cdot)$ trivial ist. (Die triviale Gruppe ist die Gruppe, die nur aus einem Element besteht.)

1.3 Homomorphismen von Gruppen

Definition 1.33. Seien G, H zwei Gruppen. Eine Abbildung $f : G \to H$ heißt *Homomorphismus von Gruppen*, oder kurz *Homomorphismus* falls für alle $x, y \in G$ die Gleichung

$$f(x \cdot y) = f(x) \cdot f(y)$$

gilt.

Um eine Verwechslung zu vermeiden, schreiben wir manchmal e_G für das Einselement in G.

Lemma 1.34. *Ist $f : G \to H$ ein Homomorphismus, so ist $f(e_G) = e_H$ und $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.*

Beweis. Es ist $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$, und wir erhalten die Gleichung $f(e_G) = e_H$ durch Linksmultiplikation mit $f(e_G)^{-1}$. Dann ist $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$, also $f(a^{-1}) = f(a)^{-1}$. □

Ein Endomorphismus von G ist ein *Homomorphismus* $G \to G$. Ein Homomorphismus $f : G \to H$ heißt *Isomorphismus*, falls ein Homomorphismus $g : H \to G$ existiert mit $f \circ g = \mathrm{id}_H$ und $g \circ f = \mathrm{id}_G$. Die Gruppen G und H sind *isomorph*, falls ein Isomorphismus existiert. Ein *Automorphismus* von G ist ein Isomorphismus $G \to G$.

Proposition 1.35. *Ein Homomorphismus $f : G \to H$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.*

Beweis. Angenommen f ist ein Isomorphismus. Aus den Gleichungen $f \circ g = \mathrm{id}_H$ und $g \circ f = \mathrm{id}_G$ folgt f bijektiv und $f^{-1} = g$. Umgekehrt, sei f ein bijektiver Homomorphismus. Es reicht zu zeigen, dass f^{-1} ein Homomorphismus ist. Für $a, b \in H$ ist

$$f(f^{-1}(a) \cdot f^{-1}(b)) = f(f^{-1}(a)) \cdot f(f^{-1}(b)) = a \cdot b$$

also es gilt $f^{-1}(a \cdot b) = f^{-1}(a) \cdot f^{-1}(b)$. □

Beispiel 1.36.

(a) Die Determinante ist ein Homomorphismus $GL_n(\mathbb{R}) \to \mathbb{R}^*$.

(b) Die Exponentialfunktion $\mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto \exp(x)$ ist bijektiv, und es gilt

$$\exp(a+b) = \exp(a)\exp(b)$$

für alle $a, b \in \mathbb{R}$. Sie liefert also einen Isomorphismus zwischen den Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \times)$.

(c) Sei M die abelsche Halbgruppe $(\mathbb{N}, +)$. Die Abbildung $\beta : \mathcal{G}(M) \to \mathbb{Z}$ (siehe oben (1.1)) ist ein Isomorphismus von Gruppen.

Übung 1.37.

(a) Sei G eine Gruppe. Zeige, dass die Abbildung $G \to G$, $g \mapsto g^{-1}$ genau dann ein Homomorphismus ist, wenn G kommutativ ist.

(b) Zeige, dass die Grothendieck-Gruppe von $(\mathbb{N}^*, \times)$ isomorph zu $\mathbb{Q}_{>0}$ ist.

(c) Sei f, g zwei Homomorphismen $G \to H$. Wir definieren:

$$f \cdot g : G \to H, \quad x \mapsto f(x) \cdot g(x)$$

Wenn H abelsch ist, zeige, dass $f \cdot g$ ein Homomorphismus $G \to H$ ist. Zeige, dass dies eine Gruppenstruktur auf der Menge der Homomorphismen $G \to H$ definiert.

Lemma 1.38. *Sind $f : G \to H$ und $f' : K \to G$ zwei Homomorphismen, so ist $f \circ f' : K \to H$ ein Homomorphismus.*

Beweis. Für alle $a, b \in K$ gilt $(f \circ f')(a \cdot b) = f(f'(a) \cdot f'(b)) = f(f'(a)) \cdot f(f'(b))$. □

Die Menge der Endomorphismen von einer Gruppe G wird $\mathrm{End}(G)$ bezeichnet. Nach Lemma 1.38 ist $(\mathrm{End}(G), \circ)$ eine Halbgruppe mit Einselement id_G. Die invertierbaren Elemente von $\mathrm{End}(G)$ sind die Automorphismen von G.

1.4 Untergruppen

Definition 1.39. Eine Teilmenge $U \subset G$ einer Gruppe heißt Untergruppe, falls die folgenden Bedingungen erfüllt sind:

(i) Für alle $a, b \in U$ gilt $a \cdot b \in U$ (d.h. U ist stabil unter der Verknüpfung).

(ii) $(U, \cdot)$ ist eine Gruppe.

Proposition 1.40. *Eine Teilmenge $U \subset G$ einer Gruppe ist genau dann eine Untergruppe, wenn gilt:*

(i) $e_G \in U$.

(ii) Für alle $a, b \in U$ gilt $a \cdot b^{-1} \in U$.

Beweis. Angenommen $U \subset G$ ist eine Untergruppe. Es gilt $e_U \cdot e_U = e_U$, also $e_U = e_G$. Für $a \in U$, sei a' das Inverse zu a in U. Es ist $a \cdot a' = e_U = e_G$, also $a' = a^{-1}$. Es folgt: für alle $a, b \in U$ gilt $a \cdot b^{-1} \in U$.

Umkehrt, nehmen wir an, dass die Bedingungen (i) und (ii) erfüllt sind. Für alle $a \in U$ gilt $a^{-1} = e_G \cdot a^{-1}$. Aus (ii) folgt also $a^{-1} \in U$. Dann für alle $a, b \in U$ gilt $a \cdot b = a \cdot (b^{-1})^{-1} \in U$. Also U ist stabil unter der Verknüpfung. Schließlich ist $(U, \cdot)$ eine Gruppe. □

Bemerkung 1.41. Das Einselement von U ist auch das Einselement von G, und das Inverse von $a \in U$ in U ist auch das Inverse in G.

Bemerkung 1.42. Die Menge $\{e_G\} \subset G$ und die ganze Menge G sind Untergruppen von G. Sie heißen die *trivialen* Untergruppen von G.

1.5 Untergruppen von $(\mathbb{Z}, +)$

Für $m \in \mathbb{Z}$ definieren wir die Teilmenge:

$$m\mathbb{Z} = \{mx,\ x \in \mathbb{Z}\}.$$

Man sieht sofort, dass $m\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ ist. Umgekehrt, wir zeigen nun, dass jede Untergruppe von $\mathbb{Z}$ dieser Form ist.

Sei $G \subset \mathbb{Z}$ eine Untergruppe, mit $G \neq \{0\}$. Ist x ein Element von G, so ist $-x$ auch in G. Es folgt, dass der Durchschnitt $G \cap \mathbb{N}_{>0}$ nicht leer ist. Sei $m > 0$ die kleinste positive Zahl in G. Natürlich gilt $m\mathbb{Z} \subset G$. Sei $x \in G$. Es existiert $q, r \in \mathbb{Z}$ mit $x = mq + r$ und $0 \leq r < m$ (die Division mit Rest). Da x und mq Elemente in G sind, ist $r = x - mr$ auch in G. Es folgt $r = 0$ weil m die kleinste positive Zahl in G ist. Es gilt also $x = mq \in m\mathbb{Z}$, und es folgt $G = m\mathbb{Z}$.

Satz 1.43. *Zu jeder Untergruppe G von $\mathbb{Z}$ existiert eine eindeutige Zahl $m \in \mathbb{N}$ so dass $G = m\mathbb{Z}$ gilt.*

Ist $m \in \mathbb{Z}$ und $G = m\mathbb{Z}$, so sagt man, dass die Gruppe G von m *erzeugt* wird, und m heißt *Erzeuger* von G. Wir bemerken, dass $m\mathbb{Z} = (-m)\mathbb{Z}$. Eine Untergruppe $G \neq 0$ von $\mathbb{Z}$ hat also genau zwei Erzeuger, und einen einzigen positiven Erzeuger.

Der größte gemeinsame Teiler, Das kleinste gemeinsame Vielfache Seien $a, b \in \mathbb{Z}$. Die Zahl a ist ein Teiler von b (oder a teilt b), falls ein $d \in \mathbb{Z}$ existiert mit $b = da$. Dies ist äquivalent zur Inklusion $b\mathbb{Z} \subset a\mathbb{Z}$. Ist a ein Teiler von b, so notiert man $a|b$.

Seien $a, b \in \mathbb{Z}$ beide nicht Null. *Der größte gemeinsame Teiler* (kurz g.g.T., Notation: $\mathrm{ggT}(a, b)$) von a und b ist die größte Zahl die sowohl Teiler von a als auch von b ist. *Das kleinste gemeinsame* Vielfache (kurz k.g.V., Notation: $\mathrm{kgV}(a, b)$) ist die kleinste positive Zahl, die sowohl Vielfaches von a als auch von b ist.

Für $a, b \in \mathbb{Z}$ sieht man sofort, dass die Teilmenge:

$$a\mathbb{Z} + b\mathbb{Z} := \{ax + by,\ x, y \in \mathbb{Z}\}$$

auch eine Untergruppe von $\mathbb{Z}$ sind. Sie heißt *die Summe* von $a\mathbb{Z}$ und $b\mathbb{Z}$. Der Durchschnitt $a\mathbb{Z} \cap b\mathbb{Z}$ ist auch eine Untergruppe von $\mathbb{Z}$.

Definition 1.44 (Alternative Definition)**.** Der g.g.T. von a und b ist der nicht-negative Erzeuger der Untergruppe $a\mathbb{Z} + b\mathbb{Z}$ von $\mathbb{Z}$. Das k.g.V. von a und b ist der nicht-negative Erzeuger der Untergruppe $a\mathbb{Z} \cap b\mathbb{Z}$ von $\mathbb{Z}$.

Definition 1.45. Die Zahlen $a, b \in \mathbb{Z}$, beide nicht Null, heißen *teilerfremd*, falls eine der folgenden äquivalenten Aussagen erfüllt ist:

(i) Es gilt $\mathrm{ggT}(a, b) = 1$.

(ii) Es gilt $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

(iii) Es existiert $u, v \in \mathbb{Z}$ mit $au + bv = 1$.

Proposition 1.46. *Sind a, b teilerfremd und gilt $a|m$ und $b|m$, so gilt auch $ab|m$. Insbesondere gilt $kgV(a, b) = |ab|$.*

Beweis. Seien $u, v \in \mathbb{Z}$ mit $ua + vb = 1$ und $r, s \in \mathbb{Z}$ mit $m = ar = bs$. Dann gilt $r = uar + vbr = b(us + vr)$, also b teilt r. Es folgt : $ab|m$. □

Lemma 1.47. *Ist a teilerfremd sowohl zu b als auch zu c, so ist a teilerfremd zu bc.*

Beweis. Seien $u, v, u', v' \in \mathbb{Z}$ mit $au + bv = 1$ und $au' + cv' = 1$. Dann gilt

$$\begin{aligned} 1 &= (au + bv)(au' + cv') \\ &= a(auu' + ucv + bvu') + vv'bc. \end{aligned}$$

Es gilt also $ggT(a, bc) = 1$. □

Eine *Primzahl* ist eine Zahl $p > 1$, die genau zwei positive Teiler besitzt, nämlich 1 und p. Mit anderen Worten ist die Untergruppe $p\mathbb{Z}$ maximal, d.h. die einzigen Untergruppen die $p\mathbb{Z}$ enthalten sind $p\mathbb{Z}$ und $\mathbb{Z}$.

Ist p eine Primzahl und $a \in \mathbb{Z}$ eine beliebige Zahl, so ist p entweder ein Teiler von a oder teilfremd zu a.

Proposition 1.48. *Ist p eine Primzahl und gilt $p|ab$, so gilt entweder $p|a$ oder $p|b$.*

Beweis. Ansonsten wäre p teilerfremd sowohl zu a als auch zu b. Nach Lemma 1.47 wäre p teilerfremd zu ab, im Widerspruch zur Voraussetzung. □

Satz 1.49. *Jede natürliche Zahl $n \geq 2$ ist ein Produkt aus Primzahlen. Diese Darstellung ist bis auf Reihenfolge der Faktoren eindeutig.*

Beweis. Wir zeigen zunächst die Existenz per Induktion. Für $n = 2$ gibt es eine solche Zerlegung. Sei $n > 2$ und p der kleinste Teiler $p > 1$ von n. Dann ist p eine Primzahl und es ist $n = pn'$ mit einem $n' \geq 1$. Nach der Induktionsvoraussetzung existiert eine Primfaktorzerlegung für n'. Dies liefert eine Primfaktorzerlegung für n.

Sei nun $n = p_1 ... p_r = q_1 ... q_s$ zwei Primfaktorzerlegungen für n (wobei eine Primzahl mehrere Male vorkommen kann). Nach Proposition 1.48 gilt $p_1 = q_i$ für ein $1 \leq i \leq s$. Setze $n' = p_2 ... p_r = q_1 ... q_{i-1} q_{i+1} ... q_r$. Die Eindeutigkeit bis auf Reihenfolge gilt für n' nach Induktionsvoraussetzung, also auch für n. □

Satz 1.50 (Satz von Euklid)**.** *Die Menge der Primzahlen ist unendlich.*

Beweis. Sei $\mathcal{P}$ die Menge der Primzahlen. Nehmen wir an, dass P endlich ist: $\mathcal{P} = \{p_1, ..., p_n\}$. Setze $N := p_1...p_n + 1$. Dann gilt $N > 1$ aber N hat keinen Primteiler, im Widerspruch zum Satz 1.49. □

1.6 Erzeugte Untergruppe

Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Wir wollen zeigen, dass es eine kleinste Untergruppe von G gibt, die S enthält.

Lemma 1.51. *Ist $(H_i)_{i\in I}$ eine Familie von Untergruppen von G, so ist der Durchschnitt $H = \bigcap_{i\in I} H_i$ eine Untergruppe von G.*

Beweis. Die Teilmenge H ist nicht leer, denn es gilt $e_G \in H_i$ für alle $i \in I$, also auch $e_G \in H$. Für alle $a, b \in H$, gilt $ab^{-1} \in H_i$, also $ab^{-1} \in H$. Nach Proposition 1.40 ist H eine Untergruppe von G. □

Betrachten wir nun die Familie I der Untergruppen $U \subset G$, die die Teilmenge S enthalten. Natürlich ist G ein Element von I. Wir setzen:

$$\langle S\rangle := \bigcap_{U\in I} U$$

Nach Lemma 1.51 ist $\langle S\rangle$ eine Untergruppe von G. Sie ist die kleinste Untergruppe die S enthält. Sei S^{-1} die Menge der Inversen der Elemente in S, das heißt:

$$S^{-1} := \{a^{-1},\ a \in S\}.$$

Dann hat man auch die folgende Beschreibung von $\langle S\rangle$:

Proposition 1.52. *Es gilt*

$$\langle S\rangle = \{e_G\} \cup \{a_1a_2...a_n,\ n \geq 1,\ a_i \in S \cup S^{-1}, \forall i = 1, ..., n\}. \tag{1.2}$$

Das heißt, die Elemente von $\langle S\rangle$ sind die, die man durch Multiplikation von endlich vielen $a_i \in S \cup S^{-1}$ erhält, und das Einselement e_G.

Beweis. Sei U die Teilmenge auf der rechten Seite der Gleichung (1.2). Da $\langle S\rangle$ eine Untergruppe ist, gilt $U \subset \langle S\rangle$. Außerdem gilt auch $S \subset U$. Es genügt also zu zeigen, dass U eine Untergruppe ist. Zunächst ist e_G ein Element von U. Für $a, b \in U$ ist ab^{-1} noch ein Produkt von endlich vielen Elementen in $S \cup S^{-1}$, also es ist $ab^{-1} \in U$. Nach Proposition 1.40 ist U eine Untergruppe. □

Definition 1.53. Die Untergruppe $\langle S\rangle$ heißt *die von S erzeugte Untergruppe*. Wenn $\langle S\rangle = G$ gilt, heißt S ein *Erzeugendensystem* von G, und man sagt, dass G von S *erzeugt* wird.

Wenn $S = \{g\}$ schreibt man oft $\langle g\rangle$ statt $\langle\{g\}\rangle$. Besitzt G ein Erzeugendensystem aus einem Element, so heißt G zyklisch. Zum Beispiel ist die Gruppe $\mathbb{Z}$ zyklisch mit Erzeugendensystem $\{1\}$.

Übung : Untergruppen von $(\mathbb{R}, +)$. Eine Teilmenge $X \subset \mathbb{R}$ heißt *dicht*, falls für alle $y \in \mathbb{R}$ und alle $\epsilon > 0$ ein $x \in X$ existiert, mit $y - \epsilon < x < x + \epsilon$. Sei nun $G \subset \mathbb{R}$ eine Untergruppe von $(\mathbb{R}, +)$, mit $G \neq \{0\}$.

(a) Angenommen G ist nicht dicht in $\mathbb{R}$, zeige, dass $\mathbb{R}_{>0} \cap G$ ein minimales Element x besitzt.

(b) Folgere, dass G von x erzeugt wird.

(c) Zeige: Eine Untergruppe von $\mathbb{R}$ ist entweder dicht oder zyklisch.

1.7 Ordnung der Gruppe, Ordnung eines Elements

Sei G eine endliche Gruppe. Die Kardinalität von G heißt *die Ordnung* von G und wird mit $|G|$ bezeichnet.

Definition 1.54. Sei G eine Gruppe. Ein Element $g \in G$ hat *unendliche Ordnung*, falls die Gruppe $\langle g \rangle$ unendlich ist. Ansonsten hat g *endliche Ordnung* und die Kardinalität von $\langle g \rangle$ heißt *die Ordnung* von g und wird mit $\mathrm{ord}(g)$ bezeichnet.

Proposition 1.55. *Ist g ein Element von endlicher Ordnung n, so gilt:*

$$\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\} \quad \text{und} \quad g^n = e.$$

Außerdem ist n die kleinste Zahl $m \geq 1$ mit $g^m = e$.

Beweis. Nach Proposition 1.52 gilt $\langle g \rangle = \{g^d,\ d \in \mathbb{Z}\}$. Da $\langle g \rangle$ endlich ist, existieren $r, s \in \mathbb{Z}$ mit $r > s$ und $g^r = g^s$. Dann ist $g^{r-s} = e$ und $r - s > 0$. Es existiert also eine kleinste echt positive Zahl m mit $g^m = e$.

Für $d \in \mathbb{Z}$ existieren $q, r \in \mathbb{Z}$ mit $d = qm + r$ und $0 \leq r < m$. Dann gilt $g^d = g^{qm+r} = (g^m)^q g^r = e \cdot g^r = g^r$. Es folgt, dass $\langle g \rangle = \{g^d,\ 0 \leq d < m\}$ gilt. Die Elemente g^d mit $0 \leq d < m$ sind paarweise verschieden. Ansonsten würde d, d' existieren, mit $g^d = g^{d'}$ und $0 \leq d < d' < m$. Dann ist $g^{d'-d} = e$ und $0 < d' - d < m$, im Widerspuch zur Definition von m. Die Kardinalität von $\langle g \rangle$ ist also m, und schließlich gilt $m = n$. □

Beispiel 1.56. Seien A und B die Matrizen

$$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{1.3}$$

Die Matrix A hat Ordnung 2 in der Gruppe $GL_2(\mathbb{R})$ denn es gilt $A^2 = E_2$. Für $n \geq 1$ gilt:

$$B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Die Matrix B hat also unendliche Ordnung in $GL_2(\mathbb{R})$.

Beispiel 1.57. Sei $n \geq 1$ eine natürliche Zahl. Definiere:

$$\mu_n := \{z \in \mathbb{C}^*, z^n = 1\}.$$

Es ist eine Untergruppe von $(\mathbb{C}^*, \times)$. Die Gruppe μ_n ist eine zyklische Gruppe der Ordnung n. Ein Erzeuger von μ_n ist zum Beispiel die komplexe Zahl $\exp(\frac{2i\pi}{n})$.

Proposition 1.58. *Ist g ein Element einer Gruppe, so ist*

$$\Lambda = \{d \in \mathbb{Z}, g^d = e\} \subset \mathbb{Z}$$

eine Untergruppe von $\mathbb{Z}$. Hat g unendliche Ordnung hat, so gilt $\Lambda = 0$. Ansonsten gilt $\Lambda = n\mathbb{Z}$, wobei n die Ordnung von g ist.

Beweis. Es ist $g^0 = e$, also $0 \in \Lambda$. Seien $d, d' \in \Lambda$. Es gilt $g^{d-d'} = g^d(g^{d'})^{-1} = e$, also $d - d' \in \Lambda$. Nach Proposition 1.40 ist Λ eine Untergruppe von $\mathbb{Z}$. Hat g endliche Ordnung, so gilt $\Lambda \neq 0$, also es ist $\Lambda = r\mathbb{Z}$ wobei r die kleinste positive Zahl in Λ ist (Satz 1.43). Nach Proposition 1.55 ist r die Ordnung von g. Hat g unendliche Ordnung, so gilt natürlich $\Lambda = 0$. □

Korollar 1.59. *Sei g ein Element endlicher Ordnung einer Gruppe G und $n \geq 1$ eine ganze Zahl. Die folgenden Aussagen sind äquivalent:*

(i) Es gilt $g^n = e$.

(ii) Die Ordnung von g teilt n.

Übung Sei G eine abelsche Gruppe. Setze:

$$G_{\text{tor}} := \{g \in G \text{ von endlicher Ordnung}\}.$$

(a) Zeige, dass G_{tor} eine Untergruppe von G ist. Bestimme G_{tor} für die folgenden Gruppen: $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{C}^*, \times)$.

(b) In der Gruppe $GL_2(\mathbb{R})$, zeige dass die Elemente von endlicher Ordnung keine Untergruppe bilden. Hinweis: Benutze die oben definierten Matrizen A und B (1.3).

(c) Seien $g, h \in G$ zwei Elemente von endlicher Ordnung. Setze $n = \text{ord}(g)$ und $m = \text{ord}(h)$. Angenommen n und m sind teilerfremd, zeige, dass $\text{ord}(gh) = mn$ gilt.

1.8 Direktes Produkt

Seien G und H zwei Gruppen. Auf dem direkten Produkt $G \times H$ kann man durch komponenterweise Multiplikation eine Gruppenstruktur definieren:

$$(g, h) \cdot (g', h') := (gg', hh')$$

für alle $g, g' \in G$ und $h, h' \in H$. Dann ist $G \times H$ zusammen mit dieser Verknüpfung eine Gruppe, und heißt *das direkte Produkt* von G und H. Auf derselben Weise kann man das direkte Produkt

$$\prod_{i \in I} G_i$$

einer beliebigen Famile $(G_i)_{i \in I}$ von Gruppen definieren.

Sei G das direkte Produkt der G_i. Für $i \in I$, sei $\pi_i : G \to G_i$ die natürliche Projektion. Sie ist natürlich ein Homomorphismus. Das direkte Produkt hat die folgende

Eigenschaft: Für jede Gruppe H und jede Familie von Homomorphismen $f_i : H \to G_i$, existiert ein eindeutiger Homomorphismus $f : H \to G$ mit $\pi_i \circ f = f_i$ für alle $i \in I$. Der Homomorphismus f ist durch:

$$f(x) := (f_i(x))_{i \in I}$$

definiert. Diese Eigenschaft heißt *die universelle Eigenschaft des Produkts*. Für eine beliebige Gruppe G und eine Menge I, definiert man die Gruppe G^I als das Produkt der Familie $(G_i)_{i \in I}$ mit $G_i = G$ für alle $i \in I$.

Beispiel 1.60. Die Teilmenge $\mu := \{z \in \mathbb{C}^*,\ |z| = 1\}$ ist eine Untergruppe von $\mathbb{C}^*$, und die Abbildung

$$\mu \times \mathbb{R}_{>0} \to \mathbb{C}^*, \quad (z, r) \mapsto rz$$

ist ein Isomorphismus.

Übung

(a) Zeige, dass die Gruppe $\mathbb{Z} \times \mathbb{Z}$ nicht zyklisch ist.

(b) Folgere, dass $\mathbb{Z}$ und $\mathbb{Z} \times \mathbb{Z}$ nicht isomorph sind.

1.9 Direkte Summe abelscher Gruppen

Seien $(A_i)_{i \in I}$ eine Famile abelscher Gruppen. Das Nullelement in A_i wird mit 0 bezeichnet. Die Summe von dieser Familie ist die Menge:

$$\bigoplus_{i \in I} A_i = \{(x_i)_{i \in I} \in \prod_{i \in I} A_i,\ x_i \neq 0 \text{ nur für endlich viele } i \in I\}$$

Diese ist eine Untergruppe vom direkten Produkt der A_i. Ist I endlich, so ist die direkte Summe gleich das direkte Produkt. Bezeichnen wir mit A die direkte Summe der A_i. Für $j \in I$, sei $\alpha_j : A_j \to A$ die natürliche Abbildung

$$\alpha_j(x) = (a_i)_{i \in I} \text{ mit } a_i = \begin{cases} 0 & \text{falls } i \neq j \\ x & \text{falls } i = j. \end{cases}$$

Sie ist natürlich ein Homomorphismus. Die direkte Summe hat die folgende Eigenschaft: Für jede abelsche Gruppe B und jede Familie von Homomorphismen $g_i : A_i \to B$, existiert ein eindeutiger Homomorphismus $g : A \to B$ mit $g \circ \alpha_i = g_i$ für alle $i \in I$. Der Homomorphismus g ist durch:

$$g((x_i)_{i \in I}) := \sum_{i \in I} g_i(x_i)$$

definiert. Diese Summe hat nur endlich viele Terme ungleich Null, und ist also wohldefiniert. Diese Eigenschaft heißt *die universelle Eigenschaft der Summe*. Für eine abelsche Gruppe A und eine Menge I, definiert man die Gruppe $A^{(I)}$ als die Summe der Familie $(A_i)_{i \in I}$ mit $A_i = A$ für alle $i \in I$.

Beispiel 1.61. Sei $\mathcal{P}$ die Menge der Primzahlen. Für $p \in \mathcal{P}$, sei $g_p : \mathbb{Z} \to \mathbb{Q}_{>0}$ der Homomorphismus $k \mapsto p^k$. Nach der universellen Eigenschaft der Summe existiert ein Homomorphismus:

$$\mathbb{Z}^{(\mathcal{P})} \longrightarrow \mathbb{Q}_{>0}, \quad (k_p)_{p\in\mathcal{P}} \mapsto \prod_{p\in\mathcal{P}} p^{k_p}.$$

Der Satz von der eindeutigen Primfaktorzerlegung sagt, dass dieser Homomorphismus bijektiv ist (die Existenz der Zerlegung entspricht der Surjektivität, und die Eindeutigkeit der Injektivität). Man kann auch die Gruppenstruktur von $(\mathbb{Q}^*, \times)$ folgern:

Proposition 1.62. *Die folgende Abbildung ist ein Isomorphismus von Gruppen:*

$$\{\pm 1\} \times \mathbb{Z}^{(\mathcal{P})} \longrightarrow \mathbb{Q}^*, \quad (\varepsilon, (k_p)_{p\in\mathcal{P}}) \mapsto \varepsilon \prod_{p\in\mathcal{P}} p^{k_p}.$$

1.10 Kerne und Bilder

Sei $f : G \to H$ ein Homomorphismus. Das *Bild* von f ist die Teilmenge:

$$\text{Bild}(f) := \{f(a),\ a \in G\}.$$

Man sieht sofort, dass $\text{Bild}(f)$ eine Untergruppe von H ist. Der *Kern* von f ist:

$$\text{Kern}(f) := \{a \in G,\ f(a) = e_H\}.$$

Wir zeigen nun, dass der Kern eine Untergruppe von G ist. Das Einselement e_G ist in $\text{Kern}(f)$ weil $f(e_G) = e_H$ gilt (Proposition 1.34). Seien $a, b \in \text{Kern}(f)$. Dann ist $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$. Nach Proposition 1.40 ist $\text{Kern}(f)$ eine Untergruppe von G.

Beispiel 1.63. Der Kern des Determinantenhomomorphismus $GL_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det(A)$ ist die Untergruppe

$$SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}),\ \det(A) = 1\}.$$

Definition 1.64. Eine Untergruppe $N \subset G$ heißt Normalteiler, falls für alle $g \in G$ und $h \in N$ gilt: $ghg^{-1} \in N$.

Die Abbildung $\text{int}_g : G \to G$, $x \mapsto gxg^{-1}$ heißt *Konjugation mit g*. Ein Normalteiler ist also eine Untergruppe, die invariant unter Konjugation ist. Ist G abelsch, so ist jede Untergruppe ein Normalteiler.

Proposition 1.65. *Ist $f : G \to H$ ein Homomorphismus, so ist der Kern von f ein Normalteiler von G.*

Beweis. Seien $g \in G$ und $h \in \text{Kern}(f)$. Es gilt $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e_G$, also $ghg^{-1} \in \text{Kern}(f)$. □

Proposition 1.66. *Ein Homomorphismus $f : G \to H$ ist genau dann injektiv, wenn $\text{Kern}(f) = \{e_G\}$ gilt.*

Beweis. Es gilt $f(a) = e_H = f(e_G)$ für alle $a \in \text{Kern}(f)$. Ist f injektiv, so folgt es dann $a = e_G$, also $\text{Kern}(f) = \{e_G\}$.

Umgekehrt, seien $a, b \in G$ mit $f(a) = f(b)$. Dann gilt $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$, also $ab^{-1} \in \text{Kern}(f) = \{e_G\}$. Es folgt $ab^{-1} = e_G$, also $a = b$. □

Bemerkung 1.67. Ein Homomorphismus $f : G \to H$ ist genau dann ein Isomorphismus, wenn $\text{Kern}(f) = \{e_G\}$ und $\text{Bild}(f) = H$ gilt.

1.11 Nebenklassen

Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Eine *Linksnebenklasse* ist eine Teilmenge von G der Form

$$aH = \{ah,\ h \in H\}, \quad a \in G.$$

Entsprechend ist eine *Rechtsnebenklasse* eine Teilmenge der Form Ha für ein $a \in G$. Insbesondere ist H eine Links- und Rechtsnebenklasse (denn es gilt $H = e_G H = He_G$). Wir bemerken, dass ein Element $a \in G$ in den Nebenklassen aH und Ha enthalten ist. Die Menge der Linksnebenklassen wird mit G/H bezeichnet. Entsprechend notiert man die Menge der Rechtsnebenklassen durch $H\backslash G$. Ist H ein Normalteiler, so gilt $aH = Ha$ für alle $a \in G$, also ist jede Linksnebenklasse auch eine Rechtsnebenklasse und umgekehrt. In diesem Fall sagt man einfach "Nebenklasseßtatt Rechts- oder Linksnebenklasse.

Wir definieren eine Relation auf G durch:

$$x \sim y \iff \exists h \in H \text{ mit } y = xh.$$

Lemma 1.68. *Dies ist eine Äquivalenzrelation auf G, und die Äquivalenzklassen sind genau die Linksnebenklassen von H.*

Beweis. Die Relation ist reflexiv, denn es gilt $x = x \cdot e_G$ und $e_G \in H$. Sie ist auch symmetrisch: Wenn $x \sim y$ gilt, dann existiert ein $h \in H$ mit $y = xh$. Dann gilt $x = yh^{-1}$, also $y \sim x$. Sie ist transitiv: Seien $x, y, z \in G$ mit $x \sim y$ und $y \sim z$. Dann existieren h, h' mit $y = xh$ und $z = yh'$. Es folgt $z = xhh'$, also es gilt $x \sim z$. Die Relation $\sim$ ist eine Äquivalenzrelation. Die Äquivalenzklassen sind genau die Linksnebenklassen. □

Insbesondere ist also die Gruppe G die disjunkte Vereinigung aller Linksnebenklassen (Lemma 1.23):

$$G = \bigsqcup_{C \in G/H} C \tag{1.4}$$

Analoges gilt auch für die Rechtsnebenklassen. Die Anzahl der Linksnebenklassen einer Untergruppe H heißt *Index* von H in G und wird mit $[G : H]$ bezeichnet.

Übung

(a) Zeige, dass die Abbildung $G/H \to H\backslash G$, $aH \mapsto Ha^{-1}$ wohldefiniert und bijektiv ist.

(b) Folgere, dass die Anzahl der Rechtsnebenklasse auch $[G : H]$ ist.

Ist aH eine Linksnebenklasse, so ist die Abbildung $H \to aH$, $x \mapsto ax$ eine Bijektion. Jede Nebenklasse hat also gleichviele Elemente wie H. Sei nun eine endliche Gruppe G, und $H \subset G$ eine Untergruppe. Aus der Gleichung (1.4) folgt:

$$|G| = [G : H] \times |H|.$$

Korollar 1.69 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und H eine Untergruppe von G. Die Ordnung von H ist ein Teiler der Ordnung von G. Insbesondere ist die Ordnung jedes Elements von G ein Teiler der Ordnung von G.*

Korollar 1.70. *Sei G eine endliche Gruppe der Ordnung $n \geq 1$. Dann gilt die Gleichung $g^n = e$ für jedes Element $g \in G$.*

Korollar 1.71. *Sei p eine Primzahl und G eine Gruppe von Ordnung p. Dann ist G zyklisch und jedes Element $g \neq e$ erzeugt G.*

Beweis. Sei $g \in G$ mit $g \neq e$. Die Ordnung von g ist ein Teiler von $p = |G|$ und ist $\neq 1$. Es gilt also $\mathrm{ord}(g) = p$ und deswegen gilt $\langle g \rangle = G$. □

1.12 Faktorgruppen

Wir haben gesehen, dass der Kern eines Homomorphismus immer ein Normalteiler ist. Umgekehrt, wir zeigen nun dass jeder Normalteiler der Kern eines Homomorphismus ist. Dafür, dass eine Untergruppe N der Kern eines Homomorphismus sei, ist also notwendig und hinreichend, dass N ein Normalteiler ist. Sei G eine Gruppe und $N \subset G$ ein Normalteiler. Wir wollen eine Gruppenstruktur auf der Menge G/N der Nebenklassen definieren, so dass die natürliche Abbildung

$$\pi : G \longrightarrow G/N, \quad a \mapsto aN$$

ein Homomorphismus ist.

Definition 1.72. Seien $A, B \subset G$ zwei Teilmengen. *Die Produktmenge* oder *das Produkt* von A und B ist die Teilmenge

$$AB := \{ab,\ a \in A,\ b \in B\}.$$

Sind A, B, C Teilmengen von G, so gilt die Gleichung

$$(AB)C = A(BC).$$

Das Produkt von Teilmengen ist also eine assoziative Verknüpfung $(A, B) \mapsto AB$ auf der Potenzmenge $\mathcal{P}(G)$ von G. Das Einselement ist $\{e\}$. Ist g ein Element von G und $A \subset G$ eine Teilmenge, so schreibt man gA statt $\{g\}A$ für das Produkt von $\{g\}$ und A.

Übung 1.73.

(a) Was sind die invertierbaren Elemente in der Halbgruppe $\mathcal{P}(G)$ (versehen mit der oben definierten Verknüpfung) ?

(b) Was sind die kürzbaren Elemente ?

(c) Zeige, dass die Grothendieck-Gruppe von $\mathcal{P}(G)$ trivial ist.

(d) Sei nun $G = (\mathbb{Z}, +)$. Für $A, B \subset \mathbb{Z}$ endlich, zeige, dass $A + B$ auch endlich ist. Die Menge der endlichen Teilmengen von $\mathbb{Z}$ wird mit $\mathcal{E}(\mathbb{Z})$. Die Verknüpfung $(A, B) \mapsto A + B$ induziert also durch Einschränkung eine Verknüpfung auf $\mathcal{E}(\mathbb{Z})$, und $\mathcal{E}(\mathbb{Z})$ ist dann eine kommutative Halbgruppe.

(e) Für $A \in \mathbb{Z}$ endlich, sei $\gamma(A) := (\min(A), \max(A))$. Dies definiert eine Abbildung $\mathcal{E}(\mathbb{Z}) \to \mathbb{Z}$. Sind $A, B \subset \mathbb{Z}$ endliche Teilmengen, zeige, dass die Gleichung

$$\gamma(A + B) = \gamma(A) + \gamma(B)$$

gilt.

(f) Zeige, dass γ einen Isomorphismus:

$$\mathcal{G}(\mathcal{E}(\mathbb{Z})) \longrightarrow \mathbb{Z}^2$$

induziert.

Lemma 1.74. *Sei H ein Normalteiler und $a, b \in G$. Dann ist das Produkt der Nebenklassen aH und bH die Nebenklasse abH.*

Beweis. Es gilt $(aH)(bH) = a(Hb)H = a(bH)H = abH$. □

Die Menge $G/N \subset \mathcal{P}(G)$ ist also stabil unter der Verknüpfung $(A, B) \mapsto AB$. Die Nebenklasse N ist das Einselement von G/N, denn es gilt $N(aN) = (Na)N = (aN)N = aN$ für alle $a \in G$. Ausserdem gilt $(aN)(a^{-1}N) = (Na)(a^{-1}N) = N(aa^{-1})N = NeN = N$. Dies zeigt, dass jedes Element von G/N invertierbar ist, und dass $(aN)^{-1} = a^{-1}N$ gilt.

Satz 1.75. *Mit der Verknüpfung $(A, B) \mapsto AB$ bildet G/N eine Gruppe, und die natürliche Abbildung $\pi : G \to G/N$ ist ein surjektiver Homomorphismus mit Kern N.*

Beweis. Wir haben schon bewiesen, dass G/N eine Gruppe ist. Lemma 1.74 zeigt, dass $\pi(ab) = \pi(a)\pi(b)$ für alle $a, b \in G$ gilt. Die Abbildung π ist also ein Homomorphismus. Schließlich gilt

$$\mathrm{Kern}(\pi) = \{g \in G,\ \pi(g) = N\} = \{g \in G,\ gN = N\} = N.$$

□

Die Gruppe G/N heißt *die Faktorgruppe* oder *die Quotientengruppe* von G nach N.

Übung

1. Zeige, dass jedes Element in $\mathbb{Q}/\mathbb{Z}$ von endlicher Ordnung ist.

2. Für $n \geq 1$, zeige, dass $\mathbb{Q}/\mathbb{Z}$ eine einzige Untergruppe der Ordnung n besitzt, und dass diese zyklisch ist.

Satz 1.76 (Erster Isomorphiesatz)**.** *Sei $f : G \to H$ ein Homomorphismus mit $\mathrm{Kern}(f) = N$. Sei $\pi : G \to G/N$ die natürliche Projektion, und $\iota : \mathrm{Bild}(f) \to H$ die Inklusionsabbildung. Dann existiert ein eindeutiger Isomorphismus:*

$$\tilde{f} : G/N \to \mathrm{Bild}(f)$$

so dass die Gleichung $f = \iota \circ \tilde{f} \circ \pi$ gilt.

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/N & \xrightarrow[\tilde{f}]{\simeq} & \mathrm{Bild}(f) \end{array}$$

Beweis. Die Eindeutigkeit ist klar, denn wir müssen $\tilde{f}(aN) := f(a)$ für alle $a \in G$ setzen. Es bleibt noch zu zeigen, dass die Abbildung $\tilde{f}$ wohldefiniert ist, und dass $\tilde{f}$ ein Isomorphismus ist. Seien $a, b \in G$ mit $aN = bN$. Es existiert $x \in N$ mit $b = ax$. Dann gilt $f(b) = f(a)f(x) = f(a)e_H = f(a)$. Dies zeigt, dass $\tilde{f}$ eine wohldefinierte Abbildung ist.

Seien $a, b \in G$. Es gilt $\tilde{f}((aN)(bN)) = \tilde{f}(abN) = f(ab) = f(a)f(b) = \tilde{f}(aN)\tilde{f}(bN)$. Die Abbildung $\tilde{f}$ ist also ein Homomorphismus. Sei nun $aN \in \mathrm{Kern}(\tilde{f})$. Es gilt $\tilde{f}(aN) = f(a) = e_H$, also $a \in \mathrm{Kern}(f) = N$ und $aN = N$. Der Kern von $\tilde{f}$ ist also $\{N\}$. Das Bild von $\tilde{f}$ ist natürlich $\mathrm{Bild}(f)$. Nach der Anmerkung 1.67 ist $\tilde{f}$ ein Isomorphismus. □

Beispiel 1.77. (a) Der Homomorphismus $GL_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det(A)$ ist surjektiv, und sein Kern ist $SL_n(\mathbb{R})$. Es folgt aus dem Satz 1.76, dass $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}_{>0}$ gilt.

(b) Die Abbildung $\mathbb{R}^* \to \mathbb{R}_{>0}$, $x \mapsto x^2$ ist ein surjektiver Homomorphismus und sein Kern ist $\{-1, 1\}$. Es gilt also $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}_{>0}$.

(c) Die Abbildung $\mathbb{R}^* \to \{-1, 1\}$, $x \mapsto \mathrm{sgn}(x)$ (das Vorzeichen von x) ist ein surjektiver Homomorphismus und sein Kern ist $\mathbb{R}_{>0}$. Es gilt also $\mathbb{R}^*/\mathbb{R}_{>0} \simeq \{-1, 1\}$.

(d) Sei $n \geq 1$ eine natürliche Zahl. Die Abbildung $\mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^n$ ist ein surjektiver Homomorphismus und sein Kern ist μ_n. Es gilt also $\mathbb{C}^*/\mu_n \simeq \mathbb{C}^*$.

(e) Die Abbildung $\mathbb{C} \to \mathbb{C}^*$, $z \mapsto \exp(2i\pi z)$ ist ein surjektiver Homomorphismus und sein Kern ist $\mathbb{Z}$. Es gilt also $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$.

1.13 Zyklische Gruppen

Sei nun $G = \mathbb{Z}$ und $n \geq 1$ eine natürliche Zahl. Die Untergruppe $n\mathbb{Z}$ von $\mathbb{Z}$ ist ein Normalteiler. Die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ ist zyklisch von Ordnung n, und wird von $\bar{1}$ erzeugt. Die Elemente in $\mathbb{Z}/n\mathbb{Z}$ heißen die Kongruenzklassen modulo n. Die Kongruenzklasse einer ganzen Zahl $a \in \mathbb{Z}$ ist das Element:

$$\bar{a} := a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}.$$

Es gilt:

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}.$$

Für $a, b \in \mathbb{Z}$, gilt es:

$$\bar{a} + \bar{b} = \overline{a+b}.$$

Bemerkung 1.78. Wenn $\bar{a} = \bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$ schreibt man auch oft $a \equiv b \pmod{n}$.

Proposition 1.79. *Ist G eine zyklische Gruppe, so gilt:*

$$G \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, \textit{ falls } G \textit{ von endlicher Ordnung } n \textit{ ist,} \\ \mathbb{Z}, \textit{ falls } G \textit{ unendlich ist.} \end{cases}$$

Beweis. Sei $g \in G$, so dass G von g erzeugt wird. Die Abbildung $\alpha : \mathbb{Z} \to G$, $d \mapsto g^d$ ist ein surjektiver Homomorphismus. Das Element g hat Ordnung n, also $\text{Kern}(\alpha) = n\mathbb{Z}$ (nach Proposition 1.58). Nach dem ersten Isomorphiesatz 1.76 gilt $\mathbb{Z}/n\mathbb{Z} \simeq G$. Ansonsten ist α auch injektiv und es gilt $G \simeq \mathbb{Z}$. □

Es gibt also eine einzige Isomorphieklasse zyklischer Gruppen von bestimmter Ordnung. Der Isomorphismus $G \simeq \mathbb{Z}/n\mathbb{Z}$ von Proposition 1.79 ist nicht eindeutig.

Proposition 1.80. *Sei G eine zyklische Gruppe der Ordnung $n \geq 1$ und sei g ein Erzeuger. Für alle $k \in \mathbb{Z}$ hat das Element g^k Ordnung $\frac{n}{d}$, wobei $d = \text{ggT}(k, n)$. Insbesondere wird G genau dann von g^k erzeugt, wenn k und n teilerfremd sind.*

Beweis. Es gilt für alle $m \geq 1$:

$$\begin{aligned} g^{km} = e &\iff n \text{ teilt } km \\ &\iff \frac{n}{d} \text{ teilt } m\frac{k}{d} \\ &\iff \frac{n}{d} \text{ teilt } m \end{aligned}$$

da $\text{ggT}\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ gilt. Es folgt, dass die Ordnung von $\bar{k}$ gleich $\frac{n}{d}$ ist. □

Bemerkung 1.81. Es folgt, dass die Elemente g^k und $g^{\text{ggT}(k,n)}$ dieselbe Ordnung haben. Es gilt also $\langle g^k \rangle = \langle g^{\text{ggT}(k,n)} \rangle$.

Proposition 1.82. *Sei G eine zyklische Gruppe der Ordnung $n \geq 1$. Für jeden positiven Teiler d von n existiert eine einzige Untergruppe $H_d \subset G$ der Ordnung d, und die Gruppe H_d ist zyklisch.*

Beweis. Sei g ein Erzeuger von G. Setze $k = \frac{n}{d}$. Das Element g^k hat dann Ordnung d (Proposition 1.80), die Untergruppe $H := \langle g^k \rangle$ hat Ordnung d. Zur Eindeutigkeit: Sei nun $H' \subset G$ eine Untergruppe von Ordnung d. Sei $x \in H'$ und sei r die Ordnung von x. Nach dem Satz von Lagrange ist r ein Teiler von d. Es existiert $m \geq 1$ mit $x = g^m$. Wir wollen zeigen, dass x ein Element von H ist. Nach Proposition 1.80 hat x Ordnung $\frac{n}{\mathrm{ggT}(n,m)}$. Es gilt also $r = \frac{n}{\mathrm{ggT}(n,m)}$ und diese Zahl teilt $d = \frac{n}{k}$. Es folgt, dass k ein Teiler von $\mathrm{ggT}(n,m)$ ist, und dass $g^{\mathrm{ggT}(n,m)}$ ein Element von H ist. Nach der Bemerkung 1.81 ist g^m also ein Element in H. Wir haben bewiesen, dass $H' \subset H$ gilt, also $H = H'$ denn diese Gruppen haben dieselbe Ordnung. □

Bemerkung 1.83. Ist d ein Teiler von n, so ist $n\mathbb{Z}$ eine Untergruppe von $d\mathbb{Z}$. Die Faktorgruppe $d\mathbb{Z}/n\mathbb{Z}$ ist die Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ die von $\bar{d}$ erzeugt wird. Sie hat Ordnung $\frac{n}{d}$.

1.14 Kongruenzen

Sei $n \geq 1$ eine ganze Zahl. Man kann Kongruenzklassen auch multiplizieren. Wir definieren:

$$\bar{a} \times \bar{b} := \overline{ab}$$

für alle $a, b \in \mathbb{Z}$. Wir müssen noch zeigen, dass diese Definition sinnvoll ist. Das heißt, wenn $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$, so muß auch $\overline{ab} = \overline{a'b'}$ gelten. Das ist tatsächlich der Fall: Es existieren $r, s \in \mathbb{Z}$ mit $a' = a + nr$ und $b' = b + ns$. Dann gilt:

$$\begin{aligned} a'b' &= (a + nr)(b + ns) \\ &= ab + nrb + nsa + n^2sr \\ &= ab + n(rb + sa + nsr). \end{aligned}$$

Wir verfügen also über zwei Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$, und zwar eine Addition $+$ und eine Multiplikation $\times$. Die Multiplikation ist azossiativ und kommutativ und liefert eine Halbgruppe $(\mathbb{Z}/n\mathbb{Z}, \times)$ mit Einselement $\bar{1}$. Diese ist aber nicht eine Gruppe.

Proposition 1.84. *Die invertierbaren Elemente der Halbgruppe $(\mathbb{Z}/n\mathbb{Z}, \times)$ sind die Kongruenzklassen $\bar{a}$ mit a und n teilerfremd.*

Beweis. Es gilt:

$$\begin{aligned} \bar{a} \text{ ist invertierbar in } \mathbb{Z}/n\mathbb{Z} &\iff \exists \bar{b} \in \mathbb{Z}/n\mathbb{Z},\ \overline{ab} = 1 \\ &\iff \exists b, r \in \mathbb{Z},\ ab = 1 + nr \\ &\iff \mathrm{ggT}(a, n) = 1. \end{aligned}$$

□

Die Menge der invertierbaren Kongruenzklassen modulo n wird mit $(\mathbb{Z}/n\mathbb{Z})^\times$ bezeichnet. Wir werden die Kardinalität von $(\mathbb{Z}/n\mathbb{Z})^\times$ später bestimmen. Wenn $n = p$ eine Primzahl ist, so ist jede ganze Zahl entweder teilerfremd zu p oder ein Vielfaches von p. Es gilt also:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, ..., \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}. \tag{1.5}$$

Die Ordnung der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist also $p - 1$.

Satz 1.85 (Kleiner Fermatscher Satz)**.** *Sei p eine Primzahl und $a \in \mathbb{Z}$. Dann gilt $a^p \equiv a \pmod{p}$. Sind a und p teilerfremd, so gilt $a^{p-1} \equiv 1 \pmod{p}$.*

Beweis. Ist p ein Teiler von a, so gilt natürlich $a^p \equiv a \equiv 0 \pmod{p}$. Sind a und p teilerfremd, so ist $\bar{a}$ ein Element in $(\mathbb{Z}/p\mathbb{Z})^\times$. Die Ordnung dieser Gruppe ist $p-1$. Nach dem Satz von Lagrange (Korollar 1.69), gilt $\bar{a}^{p-1} = \bar{1}$. Das heißt, $a^{p-1} \equiv 1 \pmod{p}$. Es folgt auch daraus: $a^p \equiv a \pmod{p}$. □

Beispiel 1.86. Was ist die Kongruenzklasse modulo 17 von 7^{33} ? Wir bemerken, dass 17 eine Primzahl ist, und dass 7 und 17 teilerfremd sind. Nach dem kleinen Fermatschen Satz gilt es also $7^{16} \equiv 1 \pmod{17}$. Es ist $33 = 2 \times 16 + 1$. Wir folgern:

$$7^{33} = 7^{2\times 16+1} = (7^{16})^2 \times 7 \equiv 7 \pmod{17}$$

Übung

1. Bestimme die Kongruenzklasse modulo 19 von 8^{2593}.
2. Zeige: Eine natürliche Zahl ist genau dann durch 3 teilbar, wenn die Quersumme ihrer Ziffern durch 3 teilbar ist.

2 Ringe

2.1 Definition

Definition 2.1. Ein *Ring* ist eine Menge R mit zwei azossiativen Verknüpfungen, *die Addition* $+$ und *die Multiplikation* $\cdot$ (oder $\times$), mit den folgenden Eigenschaften:

(i) $(R, +)$ ist eine kommutative Gruppe. Das neutrale Element bezüglich $+$ wird mit 0 bezeichnet.

(ii) Es gilt:
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$
für alle $a, b, c \in R$. Diese Eigenschaft heißt *Distributivität.*

(iii) Die Halbgruppe $(R, \cdot)$ besitzt ein neutrales Element. Es wird mit 1 bezeichnet.

Der Ring heißt kommutativ, falls die Multiplikation kommutativ ist.

Lemma 2.2. *Ist R ein Ring, so gilt für alle $a \in R$:*

$$a \cdot 0 = 0 \cdot a = 0$$

$$a \cdot (-1) = (-1) \cdot a = -a.$$

Beweis. Es ist $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Es folgt $0 \cdot a = 0$. Entsprechend gilt $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ und daraus folgt $a \cdot 0 = 0$. Es gilt $0 = a \cdot 0 = a \cdot (1-1) = a \cdot 1 + a \cdot (-1) = a + a \cdot (-1)$. Es folgt $a \cdot (-1) = -a$. Analoger Beweis für $(-1) \cdot a = -a$. □

Der Nullring ist der Ring mit einem einzigen Element. Für alle anderen Ringe gilt $1 \neq 0$. Die Menge R mit der Verknüpfung $\times$ ist eine Halbgruppe mit Einselement 1.

Beispiel 2.3.

(a) Das Tripel $(\mathbb{Z}, +, \times)$ ist ein kommutativer Ring.

(b) Für $n \geq 1$ ist $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ ein kommutativer Ring.

Definition 2.4. Ein Element $a \in R$ heißt *invertierbar* oder eine *Einheit*, falls es in der Halbgruppe $(R, \cdot)$ invertierbar ist, das heißt, falls es $b \in R$ existiert mit $a \cdot b = b \cdot a = 1$. Wir schreiben dann $b = a^{-1}$. Die multiplikative Gruppe der Einheiten wird mit $R^\times$ bezeichnet.

Beispiel 2.5.

(a) Die Menge der Einheiten des Rings $\mathbb{Z}$ ist $\{-1, 1\}$.

(b) Die Einheiten des Rings $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ sind die Kongruenzklassen $\bar{a}$ mit a teilerfremd zu n.

Die meisten Ringe, die wir betrachten werden, sind kommutativ. Hier sind einige Beispiele für nicht kommutative Ringe:

(a) Für $n \geq 2$ ist der Ring $(M_n(\mathbb{R}), +, \times)$ nicht kommutativ. Die Gruppe der invertierbaren Elemente dieses Rings ist $GL_n(\mathbb{R})$.

(b) Sei $(G, +)$ eine abelsche Gruppe. Sei $\mathrm{End}(G)$ die Menge der Endomorphismen von G. Definere die Addition auf $\mathrm{End}(G)$ durch:

$$(f+g)(x) := f(x) + g(x), \quad f, g \in \mathrm{End}(G),\ x \in G$$

Dann ist $(\mathrm{End}(G), +, \circ)$ ein Ring. Dies folgt aus den folgenden einfachen Gleichungen:

$$(f+g) \circ h = f \circ h + g \circ h$$

$$h \circ (f+g) = h \circ f + h \circ g.$$

Das neutrale Element bezüglich $+$ ist der triviale Endomorphismus $0 : G \to G$, $x \mapsto 0$. Das neutrale Element bezüglich $\circ$ ist die Identitätsabbildung. Die Einheiten des Rings $End(G)$ sind die Automorphismen von G. Der Ring $\mathrm{End}(G)$ ist nicht unbedingt kommutativ.

2.2 Homomorphismen von Ringen

Definition 2.6. Seien R und S zwei Ringe. Eine Abbildung $f : R \to S$ heißt *Homomorphismus von Ringen*, falls die folgenden Bedingungen erfüllt sind:

(i) Es gilt $f(1_R) = 1_S$

(ii) Für alle $a, b \in R$ gilt $f(a + b) = f(a) + f(b)$, d.h. f ist ein Homomorphismus von Gruppen $(R, +) \to (S, +)$.

(iii) Für alle $a, b \in R$ gilt $f(a \cdot b) = f(a) \cdot f(b)$.

Wir definieren auch *Endomorphismen*, *Isomorphismen*, *Automorphismen* auf derselben Weise wie für Gruppen. Ein bijektiver Homomorphismus ist ein Isomorphismus. Ist $f : R \to S$ ein Homomorphismus von Ringen und $a \in R$ eine Einheit, so ist $f(a)$ eine Einheit in S. Der Homomorphismus f induziert also durch Einschränkung einen Homomorphismus von Gruppen:

$$f : (R^\times, \cdot) \longrightarrow (S^\times, \cdot).$$

Sind K und L zwei Körper und $f : K \to L$ ein Homomorphismus von Ringen, so heißt f ein *Homomorphismus von Körpern*.

Beispiel 2.7. Was sind die Endomorphismen des Rings $\mathbb{Z}$? Sei $f : \mathbb{Z} \to \mathbb{Z}$ ein Endomorphismus von Ringen. Es gilt per Definition $f(1) = 1$. Es folgt $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$. Per Induktion sieht man sofort, dass $f(a) = a$ für alle $a \in \mathbb{N}$ gilt. Es gilt auch $f(-k) = -f(k) = -k$ für alle $k \geq 0$. Die Identitätsabbildung ist also der einzige Endomorphismus des Rings $\mathbb{Z}$. Für einen beliebigen Ring R existiert ein einziger Homomorphismus von Ringen $\mathbb{Z} \to R$. Der ist durch $n \mapsto n \cdot 1_R$ definiert.

Übung Sei $G = (\mathbb{Z}/n\mathbb{Z}, +)$ und sei $\mathrm{End}(G)$ die Menge der Endomorphismen von G. Zeige, dass die Abbildung

$$\mathrm{End}(G) \to \mathbb{Z}/n\mathbb{Z}, \quad f \mapsto f(\bar{1})$$

einen Isomorphismus von Ringen $(\mathrm{End}(G), +, \circ) \to (\mathbb{Z}/n\mathbb{Z}, +, \times)$ liefert.

2.3 Integritätsbereich, Körper

Definition 2.8. Ein Ring ist ein *Schiefkörper*, falls $1 \neq 0$ gilt, und alle Elemente $a \neq 0$ invertierbar sind, d.h. $R^\times = R - \{0\}$. Ein kommutativer Schiefkörper ist ein *Körper*.

Beispiel 2.9. Die Mengen $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ zusammen mit der natürlichen Addition und Multiplikation sind Körper.

Definition 2.10. Sei R ein kommutativer Ring.

(i) Sind $a, b \in R$, so heißt a ein Teiler von b, falls es ein $d \in R$ existiert mit $ad = b$ (man sagt auch, a *teilt* b). Man schreibt $a|b$.

(ii) Ein Element $a \in R$ heißt *Nullteiler*, falls es ein $b \neq 0$ gibt mit $ab = 0$.

(iii) R heißt *nullteilerfrei*, falls 0 der einzige Nullteiler ist.

(iv) R heißt *Integritätsbereich*, falls $1 \neq 0$ gilt, und R nullteilerfrei ist.

Bemerkung 2.11. Sei R ein Integritätsbereich.

(a) Aus $ab = ac$ und $a \neq 0$ folgt $a(b - c) = 0$, also $b = c$.

(b) Die Teilmenge $R \setminus \{0\}$ ist stabil unter Multiplikation. Das Paar $(R \setminus \{0\}, \cdot)$ ist also eine kürzbare kommutative Halbgruppe.

Beispiel 2.12.

(a) Ein Körper ist ein Integritätsbereich.

(b) Der Ring $\mathbb{Z}$ ist ein Integritätsbereich.

Lemma 2.13. *Ein endlicher Integritätsbereich ist ein Körper.*

Beweis. Ist R ein endlicher Integritätsbereich, so ist die endliche kürzbare Halbgruppe $(R - \{0\}, \cdot)$ eine Gruppe, also R ist ein Körper (siehe Übungsblatt 1). □

Proposition 2.14. *Sei $n \geq 1$ eine natürliche Zahl. Äquivalent sind:*

(i) Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper.

(ii) Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist ein Integritätsbereich.

(iii) Die Zahl n ist ein Primzahl.

Beweis. Die Aussagen (i) und (ii) sind äquivalent nach Lemma 2.13. Ist p eine Primzahl, so gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, also $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Wenn n keine Primzahl ist existieren $a, b > 1$ mit $n = ab$. Dann sind $\bar{a}$ und $\bar{b}$ nicht gleich Null, aber es gilt $\bar{a}\bar{b} = 0$. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist also kein Integritätsbereich. □

2.4 Unterring

Definition 2.15. Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt *Unterring*, falls die folgenden Bedingungen erfüllt sind:

(i) Es gilt $1 \in S$ und $0 \in S$.

(ii) Für alle $a, b \in S$ gilt $a - b \in S$.

(iii) Für alle $a, b \in S$ gilt $a \cdot b \in S$.

Zum Beispiel, in der Kette $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ ist jeder Ring ein Unterring des nächsten.

Beispiel 2.16. Sei R die Menge der Matrien in $M_2(\mathbb{R})$ der Form

$$M(a,b) := \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

für $a, b \in \mathbb{R}$. Es gilt $M(0,0) = 0$ und $M(1,0) = E_2$. Für $a, b, c, d \in \mathbb{R}$ gilt:

$$M(a,b) + M(c,d) = M(a+b, c+d)$$

$$M(a,b) \times M(c,d) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \times \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = M(ac, ad+bc).$$

Die Teilmenge R ist also ein Unterring von $M_2(\mathbb{R})$. Die zweite obige Gleichung zeigt, dass R kommutativ ist. Die Einheiten sind die Matrizen $M(a,b)$ mit $a \neq 0$. Der Ring R ist kein Integritätsbereich, denn es gilt:

$$M(0,1) \times M(0,1) = 0.$$

Lemma 2.17. *Ist $f : R \to S$ ein Homomorphismus von Ringen, so ist das Bild von f ein Unterring von S.*

Beweis. Wir wissen schom, dass Bild(f) eine Untergruppe von $(S, +)$ ist. Es gilt $f(1) = 1$, also $1 \in$ Bild(f). Schliesslich ist Bild(f) auch stabil unter Multiplikation, denn es gilt $f(a) \cdot f(b) = f(a \cdot b)$ für alle $a, b \in R$. □

Ein Unterring eines Körpers ist natürlich ein Integritätsbereich. Umgekehrt, wir zeigen nun, dass jeder Integritätsbereich ein Unterring eines Körpers ist. Sei R ein Integritätsbereich. Wir definieren auf dem Produkt $R \times (R \setminus \{0\})$ eine Äquivalenzrelation durch:

$$(a,b) \sim (a',b') \Longleftrightarrow ab' = a'b.$$

Sei K die Menge der Äquivalenzklassen:

$$K = (R \times (R \setminus \{0\})) / \sim .$$

Wir schreiben $\frac{a}{b}$ für die Klasse des Elements (a,b) in $R \times (R \setminus \{0\})$. Wir definieren eine Addition und eine Multiplikation auf K durch:

$$\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + a'b}{bb'}$$

$$\frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}.$$

Wir bemerken, dass das Element bb' nicht gleich Null ist, weil R ein Integritätsbereich ist. Wir müssen noch zeigen, dass diese Definition sinnvoll ist. Angenommen die Gleichungen $\frac{a}{b} = \frac{a_1}{b_1}$ und $\frac{a'}{b'} = \frac{a'_1}{b'_1}$ gelten. Per Definition ist dann $ab_1 = a_1 b$ und $a'b'_1 = a'_1 b'$. Das Produkt dieser Gleichungen ist $b_1 b'_1 aa' = bb' a_1 a'_1$, und es folgt: $\frac{aa'}{bb'} = \frac{a_1 a'_1}{b_1 b'_1}$. Es gilt auch:

$$\begin{aligned} b_1 b'_1 (ab' + a'b) &= b_1 b'_1 ab' + b_1 b'_1 a'b \\ &= bb' a_1 b'_1 + bb' a'_1 b_1 \\ &= bb'(a_1 b'_1 + a'_1 b_1) \end{aligned}$$

und es folgt also $\frac{ab'+a'b}{bb'} = \frac{a_1b_1'+a_1'b_1}{b_1b_1'}$. Die Verknüpfungen + und · auf K sind wohldefiniert. Die folgenden Eigenschaften sind einfach zu beweisen:

(1) Die Verknüpfungen + und · sind assoziativ, und das Distributivgesetz gilt.

(2) Das neutrale Element von + ist $\frac{0}{1}$ und das neutrale Element von · ist $\frac{1}{1}$. Das Inverse von $\frac{a}{b}$ bezüglich + ist $\frac{-a}{b}$.

(3) $(K, +, \cdot)$ ist ein Körper. Für $a, b \neq 0$ ist das Element $\frac{a}{b}$ invertierbar (bezüglich ·) und das Inverse ist $\frac{b}{a}$.

Die Abbildung $\iota : R \to K$ durch $x \mapsto \frac{x}{1}$ ist ein injektiver Homomorphismus von Ringen. Man kann also R als Unterring von K betrachten. Für alle $a, b \in R$ mit $b \neq 0$ ist b invertierbar in K, und es gilt:

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

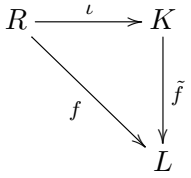
Definition 2.18. Der Körper $(K, +, \cdot)$ heißt der Quotientenkörper von R. Er wird oft mit $\mathrm{Quot}(R)$ bezeichnet.

Beispiel 2.19. Der Quotientenkörper von $\mathbb{Z}$ ist isomorph zu $\mathbb{Q}$. Die abbildung

$$\mathrm{Quot}(\mathbb{Z}) \longrightarrow \mathbb{Q}, \quad \frac{a}{b} \mapsto \frac{a}{b}$$

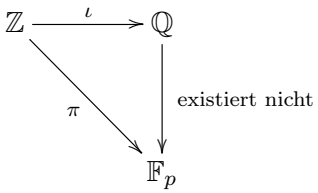
ist ein Isomorphismus von Körpern (auf der linken Seite ist der Bruch $\frac{a}{b}$ die Äquivalenzklasse von (a, b) !)

Proposition 2.20. *Sei L ein Körper und $f : R \to L$ ein injektiver Homomorphismus von Ringen. Dann existiert ein eindeutiger Homomorphismus von Ringen $\tilde{f} : K \to L$ mit $f = \tilde{f} \circ \iota$.*



Beweis. Für $x = \frac{a}{b} \in K$ definiert man $\tilde{f}(x) := f(a)f(b)^{-1}$. Diese Abbildung ist wohldefiniert: Da f injektiv ist, ist $f(b) \neq 0$. Gilt $\frac{a}{b} = \frac{a'}{b'}$, so gilt $ab' = a'b$, also $f(a)f(b') = f(a')f(b')$, und es folgt $f(a)f(b)^{-1} = f(a')f(b')^{-1}$. Man sieht sofort, dass $\tilde{f}$ ein Homomorphismus von Ringen ist. □

Bemerkung 2.21. Diese Aussage gilt nicht wenn f nicht injektiv ist. Zum Beispiel, sei $R = \mathbb{Z}$ und sei p eine Primzahl. Dann gilt $\mathrm{Quot}(R) = \mathbb{Q}$ und es existiert kein Homomorphismus von Ringen $\mathbb{Q} \to \mathbb{F}_p$.



2.5 Ideale

Definition 2.22. Eine Teilmenge $I \subset R$ eines Rings heißt *Ideal*, falls die folgenden Bedingungen erfüllt sind:

(i) I ist eine Untergruppe von $(R, +)$.

(ii) Für alle $a \in R$ und $x \in I$ gilt $a \cdot x \in I$ und $x \cdot a \in I$.

Beispiel 2.23. Das Nullideal 0 ist das Ideal, das nur aus 0 besteht. Der ganze Ring R ist auch ein Ideal von R.

Beispiel 2.24. Ein Ideal von $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ ist einfach eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z}, +)$ (die Bedingung (ii) ist automatisch erfüllt). Die Ideale von $\mathbb{Z}$ sind also die Teilmengen der Form $d\mathbb{Z}$, $d \in \mathbb{Z}$. Die Ideale von $\mathbb{Z}/n\mathbb{Z}$ sind die Teilmengen $d\mathbb{Z}/n\mathbb{Z}$ mit d Teiler von n.

Beispiel 2.25. Sei X eine Menge und sei

$$R := \{\text{Abbildungen } X \to \mathbb{R}\}.$$

Sind $f, g \in R$ zwei Abbildungen, so definiert man

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)g(x)$$

für alle $x \in X$. Mit diesen Verknüpfungen ist $(R, +, \cdot)$ ein kommutativer Ring. Die Eins ist die konstante Funktion $x \mapsto 1$ und die Null ist die konstante Funktion $x \mapsto 0$. Für eine Teilmenge $Y \subset X$ definieren wir:

$$I_Y := \{f \in R,\ f(x) = 0,\ \forall x \in Y\}.$$

Dann ist I_Y ein Ideal von R.

Existiert in einem Ideal $I \subset R$ ein invertierbares Element x, so ist $y = yx^{-1}x$ auch ein Element in I für alle $y \in R$, und es folgt also $I = R$. Insbesondere gilt folgende Proposition:

Proposition 2.26. *Sei K ein Schiefkörper und $I \subset K$ ein Ideal. Dann gilt entweder $I = 0$ oder $I = K$.*

Im kommutativen Fall gilt auch die Umkehrung:

Proposition 2.27. *Sei R ein kommutativer Ring, der nur die Ideale 0 und R besitzt. Dann ist R ein Körper.*

Beweis. Für $x \in R \setminus \{0\}$ gilt $(x) \neq \{0\}$, also es folgt $(x) = R$. Dann existiert ein $y \in R$ mit $xy = 1$, also x ist invertierbar. □

Erzeugtes Ideal Ist $(I_t)_{t\in T}$ eine Famile von Idealen eines Rings R, so ist der Durchschnitt

$$\bigcap_{t\in T} I_t$$

auch ein Ideal. Sei nun $S \subset R$ eine Teilmenge. Wir definieren das Ideal (S) als den Durchschnitt über alle Ideale $I \subset R$, die S enthalten. Dann ist (S) das kleinste Ideal, das S enthält. Es heißt *das von S erzeugte Ideal*. Ist I ein Ideal und $S \subset I$ eine Teilmenge, so sagt man dass I *von S erzeugt* wird, falls $I = (S)$. Besteht S aus einem einzigen Element, so heißt (S) ein *Hauptideal*. Es gilt:

$$(S) = \{a_1x_1b_1 + ... + a_nx_nb_n,\ n \geq 1,\ a_i, b_i \in R,\ x_i \in X,\ \forall 1 \leq i \leq n\} \tag{2.1}$$

Sei x ein Element in R. Das von x erzeugtes Hauptideal ist also:

$$(x) = \{axb,\ a, b \in R\}.$$

Ist R kommutativ, so gilt $(x) = \{ax,\ a \in R\}$.

Beispiel 2.28. Sei R der Ring von Beispiel 2.25. Sei $Y \subset X$ eine Teilmenge und $I_Y \subset R$ das gehörige Ideal. Definiere eine Funktion

$$f_Y : X \to \mathbb{R}, \quad x \mapsto \begin{cases} 0 & \text{falls } x \in Y \\ 1 & \text{falls } x \notin Y. \end{cases}$$

Dann gilt $I_Y = (f_Y)$. Das Ideal I_Y ist also ein Hauptideal.

Summe, Produkt zweier Ideale Sei R ein Ring und I, J zwei Ideale von R. Wir definieren:

$$I + J := \{x + y,\ x \in I,\ y \in J\}$$

$$I \cdot J := \{a_1 \cdot b_1 + ... + a_n \cdot b_n,\ n \geq 1,\ a_i \in I, b_i \in J,\ \forall i \in \{1, ..., n\}\}.$$

Man sieht sofort, dass $I + J$ und $I \cdot J$ Ideale sind. Das Ideal $I + J$ heißt die Summe von I und J, und ist das von $I \cup J$ erzeugtes Ideal. Das Ideal $I \cdot J$ heißt das Produkt von I und J, und ist das Ideal, das von Produkten $x \cdot y$ mit $x \in I$ und $y \in J$ erzeugt wird. Es gilt natürlich $I \subset I + J$, $J \subset I + J$, und $I \cdot J \subset I \cap J$. Die Menge der Ideale von R wird mit $\mathcal{I}(R)$ bezeichnet.

Bemerkung 2.29.

(a) Die Verknüpfungen $+$ und $\cdot$ auf $\mathcal{I}(R)$ sind assoziativ. Die Verknüpfung $+$ ist kommutativ. Ist R kommutativ, so ist die Verknüpfung $\cdot$ auf $\mathcal{I}(R)$ auch kommutativ.

(b) Das neutrale Element von $\mathcal{I}(R)$ bezüglich der Verknüpfung $+$ ist das Nullideal 0. Das neutrale Element von $\mathcal{I}(R)$ bezüglich der Verknüpfung $\cdot$ ist das Ideal R.

Lemma 2.30. *Sei R ein kommutativer Ring. Sind I, J zwei Ideale mit $I + J = R$, so gilt $I \cdot J = I \cap J$.*

Beweis. Seien $a \in I$ und $b \in J$ mit $a+b=1$. Für alle $x \in I \cap J$ gilt dann $x = x\cdot(a+b) = x \cdot a + x \cdot b$. Es gilt $x \cdot a = a \cdot x \in I \cdot J$ und $x \cdot b \in I \cdot J$, also $x \in I \cdot J$. □

Definition 2.31. Sei R ein kommutativer Ring. Zwei Ideale I, J sind *koprim* (oder *teilerfremd*), falls die Gleichung $I + J = R$ gilt.

Bemerkung 2.32. Die Ideale $a\mathbb{Z}$ und $b\mathbb{Z}$ sind genau dann koprim, wenn a und b teilerfremd sind.

Lemma 2.33. *Seien I, J, K drei Ideale eines Rings R. Ist I koprim sowohl zu J als auch zu K, so ist I auch koprim zu $J \cdot K$.*

Beweis. Es existieren $a, a' \in I$ und $b \in J$, $c \in K$ mit $1 = a + b = a' + c$. Es folgt

$$1 = (a + b) \cdot (a' + c) = a \cdot a' + a \cdot c + b \cdot a' + b \cdot c.$$

Es gilt $a \cdot a' + a \cdot c + b \cdot a' \in I$ und $b \cdot c \in J \cdot K$. Die Behauptung folgt. □

Der Kern eines Homomorphismus

Definition 2.34. Sei $f : R \to S$ ein Homomorphimus von Ringen. Der Kern von f ist

$$\mathrm{Kern}(f) := \{x \in R, f(x) = 0\}.$$

Mit anderen Worten, der Kern von f als Homomorphismus von Ringen ist der Kern des Gruppenhomomorphismus $f : (R, +) \to (S, +)$. Insbesondere ist f genau dann injektiv, wenn $\mathrm{Kern}(f) = \{0\}$ gilt (Proposition 1.66).

Proposition 2.35. *Sei $f : R \to S$ ein Homomorphismus von Ringen. Sei $I \subset S$ ein Ideal. Dann ist $f^{-1}(I)$ ein Ideal von R.*

Beweis. Wir wissen, dass $f^{-1}(I)$ eine Untergruppe von $(R, +)$ ist. Sei nun $a \in R$ und $x \in f^{-1}(I)$. Dann gilt $f(a \cdot x) = f(a) \cdot f(x) \in I$, also $a \cdot x \in f^{-1}(I)$. Es ist auch $f(x \cdot a) = f(x) \cdot f(a) \in I$, also $x \cdot a \in f^{-1}(I)$. □

Mit $I = 0$ (das Nullideal), enthalten wir folgendes Korrollar:

Korollar 2.36. *Ist $f : R \to S$ ein Homomorphismus von Ringen, so ist* $\mathrm{Kern}(f)$ *ein Ideal von R.*

Korollar 2.37. *Sei K ein Schiefkörper und $f : K \to R$ ein Homomorphismus von Ringen. Ist R nicht der Nullring, so ist f injektiv.*

Beweis. Der Kern von f ist ein Ideal von K, und es gilt $f(1) = 1 \neq 0$, also $1 \notin \mathrm{Kern}(f)$. Es folgt $\mathrm{Kern}(f) = \{0\}$ nach Proposition 2.26. □

Faktorring Sei I ein Ideal eines Rings R. Insbesondere ist I eine Untergruppe von R bezüglich der Addition. Wir werden auf der Faktorgruppe R/I eine Ringstruktur definieren. Sei $\pi : R \to R/I$ die natürliche Projektion. Wir definieren das Produkt der Nebenklassen $a + I$ und $b + I$ durch:

$$(a + I) \cdot (b + I) := (a \cdot b + I) \tag{2.2}$$

Wir müssen zuerst zeigen, dass diese Verknüpfung wohldefiniert ist. Seien $a, b, a', b' \in R$ mit $a + I = a' + I$ und $b + I = b' + I$. Es existieren also $x, y \in I$ mit $a' = a + x$ und $b' = b + y$. Dann gilt

$$a' \cdot b' = (a + x) \cdot (b + y) = a \cdot a' + a \cdot y + x \cdot b + x \cdot y.$$

Es folgt: $a \cdot b - a' \cdot b' \in I$ und $a \cdot b + I = a' \cdot b' + I$. Diese definition ist also sinnvoll. Die Nebenklasse $1 + I$ ist das neutrale Element für diese Verknüpfung.

Satz 2.38. *Die Verknüpfung (2.2) definert eine Multiplikation auf R/I, und $(R/I, +, \cdot)$ ist ein Ring. Die Abbildung $\pi : R \to R/I$ ist dann ein Homomorphismus von Ringen, und der Kern von π ist I.*

Beweis. Wir wissen schon, dass $(R/I, +)$ eine Gruppe ist, und dass π ein Gruppenhomomorphismus mit Kern I ist. Die Assoziativität und die Distributivität des Produkts gelten in R/I, weil sie schon im Ring R gelten. Es gilt $\pi(a \cdot b) = \pi(a) \cdot \pi(b)$, also π ist ein Homomorphismus von Ringen. □

Der Ring R/I heißt der Faktorring R modulo I. Sei $\pi : R \to R/I$ die natürliche Projektion. Ist $J' \subset R/I$ ein Ideal, so ist $\pi^{-1}(J')$ ein Ideal von R, das I enthält. Wir erhalten eine Abbildung:

$$\mathcal{I}(R/I) \longrightarrow \{J \in \mathcal{I}(R),\ I \subset J\}, \quad J' \mapsto \pi^{-1}(J').$$

Diese Abbildung ist eine Bijektion. Die Umkehrabbildung ist $J \mapsto J/I$, wobei

$$J/I := \{x + I \in R/I,\ x \in J\}. \tag{2.3}$$

Man sieht sofort, dass J/I ein Ideal von R/I ist.

Satz 2.39 (Isomorphiesatz für Ringe)**.** *Sei $f : R \to S$ ein Homomorphismus von Ringen mit* $\mathrm{Kern}(f) = I$. *Sei $\pi : R \to R/I$ die natürliche Projektion und $\iota : \mathrm{Bild}(f) \to S$ die Inklusionsabbildung. Dann existiert ein eindeutiger Isomorphismus:*

$$\tilde{f} : R/I \to \mathrm{Bild}(f)$$

so dass die Gleichung $f = \iota \circ \tilde{f} \circ \pi$ gilt.

Beweis. Nach dem Satz 1.76 existiert ein eindeutiger Gruppenhomomorphismus $\tilde{f}$ mit $f = \iota \circ \tilde{f} \circ \pi$. Der ist durch

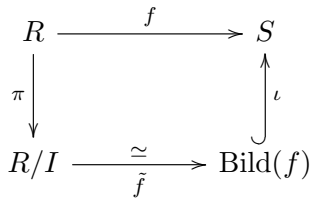
$$\tilde{f}(a + I) = f(a)$$

definiert. Es bleibt nur zu zeigen, dass $\tilde{f}$ ein Homomorphismus von Ringen ist. Es gilt:

$$\tilde{f}((a + I) \cdot (b + I)) = \tilde{f}(a \cdot b + I) = f(a \cdot b) = f(a) \cdot f(b) = \tilde{f}(a + I) \cdot \tilde{f}(b + I).$$

□

Diesen Satz kann man mit folgendem Diagram zusammenfassen:



Beispiel 2.40. Sei X eine Menge und sei

$$R := \mathbb{R}^X := \{\text{Abbildungen } X \to \mathbb{R}\}$$

der Ring von Beispiel 2.25. Für eine Teilmenge $Y \subset X$ haben wir das Ideal

$$I_Y := \{f \in R,\ f(x) = 0, \forall x \in Y\}$$

definiert. Es gibt eine natürliche Abbildung $f_Y : \mathbb{R}^X \to \mathbb{R}^Y$, definiert durch Einschränkung der Abbildungen. Diese Abbildung ist ein surjektiver Homomorphismus von Ringen und es gilt:

$$\text{Kern}(f_Y) = I_Y.$$

Es folgt nach dem Isomorphiesatz: $R/I_Y \simeq \mathbb{R}^Y$.

2.6 Der chinesische Restsatz

Direktes Produkt von Ringen Seien $(R_i)_{i\in\mathcal{I}}$ eine Familie von Ringen. Man kann auf dem direkten Produkt

$$R = \prod_{i\in\mathcal{I}} R_i$$

durch komponenterweise Addition und Multiplikation eine Ringstruktur definieren:

$$(x_i)_i + (y_i)_i := (x_i + y_i)_i$$

$$(x_i)_i \cdot (y_i)_i := (x_i \cdot y_i)_i.$$

Die Null ist das Element $(x_i)_i$ mit $x_i = 0$ für alle $i \in \mathcal{I}$. Die Eins ist das Element $(y_i)_i$ mit $y_i = 1$ für alle $i \in \mathcal{I}$. Die Projektionsabbildung $p_i : R \to R_i$ ist dann ein Homomorphismus von Ringen. Es gilt:

$$R^\times = \prod_{i\in\mathcal{I}} R_i^\times \tag{2.4}$$

Bemerkung 2.41. Die direkte Summe der Gruppen $(R_i, +)$

$$\bigoplus_{i\in\mathcal{I}} R_i \subset \prod_{i\in\mathcal{I}} R_i$$

ist kein Unterring vom direkten Produkt, die Eins ist nicht ein Element von $\bigoplus_{i\in\mathcal{I}} R_i$.

Satz 2.42. *Sei R ein kommutativer Ring. Seien $I_1, ..., I_n$ paarweise koprime Ideale von R (d.h. es gilt $I_i + I_j = R$ für $i \neq j$). Sei $\pi_i : R \to R/I_i$ die Projektion. Der Homomorphismus*

$$\pi : R \to R/I_1 \times ... \times R/I_n, \quad x \mapsto (\pi_1(x), ..., \pi_n(x))$$

ist surjektiv und es gilt $\mathrm{Kern}(\pi) = \bigcap_{i=1}^n I_i = I_1 \cdot ... \cdot I_n$. *Er induziert also einen Isomorphismus von Ringen:*

$$R/\bigcap_{i=1}^n I_i \simeq R/I_1 \times ... \times R/I_n.$$

Beweis. Wir beweisen zuerst den Satz für zwei koprime Ideale I, J. Sei $a \in I$ und $b \in J$ mit $a + b = 1$. Seien $x, y \in R$ und $z := bx + ay$. Es gilt:

$$z - x = bx + ay - (a + b)x = a(y - x) \tag{2.5}$$

$$z - y = bx + ay - (a + b)y = b(x - y). \tag{2.6}$$

Es folgt also $z - x \in I$ und $z - y \in J$. Das Element $z \in R$ wird also von $\pi : R \to R/I \times R/J$ auf $(x + I, y + J)$ geschickt. Die Abbildung π ist also surjektiv. Der Kern von π ist $I \cap J = I \cdot J$ (Lemma 2.30).

Sei nun $n \geq 3$. Wir zeigen jetzt den Satz per Induktion nach n. Setze $J = \bigcap_{i=2}^n I_i$. Nach Lemma 2.33 sind I_1 und J koprim. Wir haben gerade bewiesen, dass die Abbildung $R \to R/I_1 \times R/J$, $x \mapsto (\pi_1(x), \pi_J(x))$ surjektiv ist, und dass sein Kern $I_1 \cap J$ ist. Nach der Induktionsvoraussetzung gilt die Behauptung für die Ideale $I_2, ..., I_n$. Sei π' die natürliche Abbildung $R \to \prod_{i=2}^n R/I_i$. Sie induziert einen Isomorphismus $\pi' : R/J \to \prod_{i=2}^n R/I_i$ Die Abbildung π ist dann die Komposition:

$$R \xrightarrow{\pi_1 \times \pi_J} R/I_1 \times R/J \xrightarrow{\mathrm{id} \times \pi'} R/I_1 \times R/I_2 \times ... \times R/I_n$$

wobei die zweite Abbildung ein Isomorphismus ist. Der Homomorphismus π ist also surjektiv. Nach der Induktionsvoraussetzung gilt

$$\mathrm{Kern}(\pi) = I_1 \cap J = \bigcap_{i=1}^n I_i = I_1 \cdot I_2 \cdot ... \cdot I_n.$$

□

Korollar 2.43. *Seien $n_1, ..., n_k$ paarweise teilerfremde ganze Zahlen. Setze $n := n_1 ... n_k$. Dann induziert der kanonische Homomorphismus $\pi : \mathbb{Z} \to \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$ einen Isomorphismus von Ringen:*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}.$$

Beispiel 2.44. Die Zahlen 7 und 5 sind teilerfremd. Wir erhalten also einen Isomorphismus von Ringen:

$$\mathbb{Z}/35\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \quad m + 35\mathbb{Z} \mapsto (m + 7\mathbb{Z}, m + 5\mathbb{Z}). \tag{2.7}$$

Was ist die Umkehrabbildung dieses Isomorphismus ? Schreiben wir $I = 7\mathbb{Z}$ und $J = 5\mathbb{Z}$. Wir suchen $a \in I$ und $b \in J$ mit $a + b = 1$. Zum Beispiel kann man $a = -2 \times 7 = -14$ und $b = 3 \times 5 = 15$ wählen. Nach dem Beweis des chinesichen Restsatzes ist das Element $bx + ay = 15x - 14y$ ein Urbild von $(x + I, y + J)$ für alle $x, y \in \mathbb{Z}$. Die Umkehrabbildung des Isomorphismus (2.7) ist also die Abbildung:

$$(x + 7\mathbb{Z}, y + 5\mathbb{Z}) \mapsto (15x - 14y) + 35\mathbb{Z}.$$

Zum Beispiel, sei n eine ganze Zahl mit $n \equiv 1 \pmod 7$ und $n \equiv 2 \pmod 5$. Dann gilt:

$$n \equiv 15 \times 1 - 14 \times 2 \equiv -13 \equiv 22 \pmod{35}.$$

Beispiel 2.45. Sei X eine Menge und sei

$$R := \mathbb{R}^X := \{\text{Abbildungen } X \to \mathbb{R}\}$$

der Ring von Beispiel 2.25. Für zwei Teilmengen Y und Z von X gilt:

$$I_Y \text{ und } I_Z \text{ koprim } \iff Y \cap Z = \emptyset.$$

Die Funktion $f_Y + f_Z$ ist dann invertierbar. In diesem Fall gilt: $I_Y \cap I_Z = I_{Y \cup Z}$, und es folgt aus dem chinesichen Restsatz: $R/I_{Y \cup Z} \simeq R/I_Y \times R/I_Z$. Nach Beispiel 2.40 liefert dies einen Isomorphismus:

$$\mathbb{R}^{Y \cup Z} \simeq \mathbb{R}^Y \times \mathbb{R}^Z.$$

Übung 2.46.

(a) Sei n eine ungerade ganze Zahl mit der Eigenschaften $n \equiv 2 \pmod 5$. Was ist die letzte Ziffer von n ?

(b) Mit welcher Ziffer endet 7777^{7777} ?

(c) Seien n, m zwei ganze Zahlen, die nur die Ziffer 3 in ihren Darstellungen besitzen. Mit welcher Ziffer endet n^m ?

2.7 Polynomringe und Potenzreihen

Potenzreihen Sei R ein kommutativer Ring. Sei $R[[X]]$ die Menge der Folgen von Elementen in R, d.h. der Abbildungen $a : \mathbb{N} \to R$. Man definiert die Addition und die Multiplikation von zwei Folgen $(a_n)_{n \in \mathbb{N}}$ und $(b_n)_{n \in \mathbb{N}}$ durch:

$$(a + b)_n := a_n + b_n, \ \forall n \in \mathbb{N}$$

$$(a \cdot b)_n := \sum_{i=0}^{n} a_i b_{n-i}, \forall n \in \mathbb{N}.$$

Diese Verknüpfungen sind offensichtlich kommutativ, und die Addition ist assoziativ. Die Multiplikation ist auch assoziativ: Seien a, b, c drei Folgen. Es gilt für alle $n \in \mathbb{N}$:

$$\begin{aligned}(a \cdot (b \cdot c))_n &= \sum_{i=0}^{n} a_i (b \cdot c)_{n-i} \\ &= \sum_{i=0}^{n} \sum_{j=0}^{n-i} a_i b_j c_{n-i-j} \\ &= \sum_{\substack{i,j,k \geq 1 \\ i+j+k=n}} a_i b_j c_k\end{aligned}$$

Diese Formel ist symmetrisch in a, b, c, also es folgt : $(a \cdot (b \cdot c)) = (c \cdot (a \cdot b)) = (a \cdot b) \cdot c$ und die Behauptung folgt.

Proposition 2.47. $(R[[X]], +, \cdot)$ *ist ein kommutativer Ring.*

Die Null ist die Nullfolge und die Eins ist die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_0 = 1$ und $a_n = 0$ für $n > 1$. Wir ändern jetzt die Notation und schreiben eine Folge $(a_n)_{n\in\mathbb{N}}$ wie eine Potenzreihe

$$\sum_{n=0}^{\infty} a_n X^n.$$

Dies ist nicht eine unendliche Summe von Elementen, sondern nur eine Schreibweise. Die Eins wird mit 1 bezeichnet. Das Element $0 + 1X + 0X^2 + 0X^3 + ...$ (d.h. die Folge $(0, 1, 0, 0, ...)$) wird mit X bezeichnet. Für $k \geq 1$ wird das Element $0+0X+...+0X^{k-1}+1X^k+0X^{k+1}+...$ einfach mit X^k bezeichnet. Diese Notation ist nicht irreführend, denn man sieht sofort, dass X^k eigentlich X zur k-ten Potenz gleich ist.

Es ist wichtig zu bemerken, dass zwei Elemente $\sum_{n=0}^{\infty} a_n X^n$ und $\sum_{n=0}^{\infty} b_n X^n$ genau dann gleich sind, wenn für alle $n \in \mathbb{N}$ die Gleichung $a_n = b_n$ gilt. Es folgt direkt aus der Definition des Produkts in $R[[X]]$ dass die Abbildung

$$R[[X]] \to R, \quad \sum_{n=0}^{\infty} a_n X^n \mapsto a_0 \tag{2.8}$$

ein Homomorphismus von Ringen ist. Der Kern ist das Ideal der Potenzreihen der Form $f = \sum_{n=0}^{\infty} a_n X^n$ mit $a_0 = 0$. Es folgt $f = X \cdot (\sum_{n=0}^{\infty} a_{n+1} X^n)$ und der Kern von diesem Homomorphismus ist also das Hauptideal (X).

Proposition 2.48. *Sei $f = \sum_{n=0}^{\infty} a_n X^n$ eine Potenzreihe mit Koeffizienten in R. Dann ist f genau dann invertierbar in $R[[X]]$, wenn a_0 in R invertierbar ist.*

Beweis. Ist f invertierbar in $R[[X]]$, so ist a_0 invertierbar R, weil die Abbildung (2.8) ein Homomorphismus von Ringen ist. Die Umkehrung ist schwieriger. Wir konstruieren per Induktion nach $N \geq 0$ eine Folge $(b_n)_{0\leq n\leq N}$ mit den folgenden Eigenschaften: $b_0 = \frac{1}{a_0}$ und für alle $1 \leq n \leq N$ gilt die Gleichung:

$$\sum_{i=0}^{n} a_i b_{n-i} = 0. \tag{2.9}$$

Für $N = 0$ definieren wir einfach $b_0 = \frac{1}{a_0}$. Angenommen wir haben $(b_n)_{0 \leq n \leq N}$ konstruiert für $N \geq 0$. Dann definieren wir b_{N+1} durch:

$$b_{N+1} = -\frac{1}{a_0} \sum_{i=1}^{n} a_i b_{N+1-i}.$$

Dann gilt die Gleichung (2.9) auch für $N + 1$. Dies liefert eine Folge $(b_n)_{n \in \mathbb{N}}$ mit den gewünschten Eigenschaften. Die Potenzreihe $g = \sum_{n=0}^{\infty} b_n X^n$ ist das Inverse zu f. $\square$

Beispiel 2.49. Sei R ein kommutativer Ring. Die Potenzreihe $1 - X$ ist invertierbar in $R[[X]]$, weil $1 \in R$ invertierbar ist. Wir bemerken:

$$(1 - X) \cdot \sum_{n=0}^{\infty} X^n = \sum_{n=0}^{\infty} X^n - \sum_{n=1}^{\infty} X^n = 1.$$

Das Inverse von $1 - X$ ist die Potenzreihe $\sum_{n=0}^{\infty} X^n$.

Polynome Ein Polynom mit Koeffizienten in R ist eine Potenzreihe, deren Koeffizienten fast alle gleich Null sind. Die Menge der Polynome mit Koeffizienten in R wird mit $R[X]$ bezeichnet. Es gilt also:

$$R[X] := \left\{ f = \sum_{n=0}^{\infty} a_n X^n, \ \exists N \geq 0 \ \text{ mit } a_n = 0 \text{ für } n \geq N \right\}.$$

Der *Grad* eines Polynoms $f = \sum_{n=0}^{\infty} a_n X^n$ ist die größte Zahl $n \geq 0$ mit $a_n \neq 0$, und der Koeffizient a_n heißt *Leitkoeffizient*. Der Grad des Nullpolynoms wird als $-\infty$ definiert und man schreibt $\mathrm{Grad}(f)$ für den Grad von $f \in R[X]$. Zum Beispiel ist $\mathrm{Grad}(X) = 1$. Ein Polynom P heißt *konstant* falls $P = 0$ oder $\mathrm{Grad}(P) = 0$ gilt. Man kann die konstanten Polynome mit den Elementen von R identifizieren, weil die Abbildung

$$R \longrightarrow R[X], \quad x \mapsto \text{konstantes Polynom } x$$

ein injektiver Homomorphismus von Ringen ist. Es gilt natürlich:

$$\mathrm{Grad}(f + g) \leq \max\{\mathrm{Grad}(f), \mathrm{Grad}(g)\}$$

für alle Polynome $f, g \in R[X]$. Seien $f = \sum_{k=0}^{n} a_k X^k$ und $g = \sum_{k=0}^{m} b_k X^k$ zwei Polynome, mit $\mathrm{Grad}(f) = n$ und $\mathrm{Grad}(g) = m$. Sei $f \cdot g = \sum_{k=0}^{\infty} c_k X^k$ das Produkt von f und g. Es gilt für $k > n + m$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0$$

denn jeder Summand dieser Summe ist gleich Null. Insbesondere ist $f \cdot g$ auch ein Polynom, und es gilt die Ungleichung

$$\mathrm{Grad}(fg) \leq \mathrm{Grad}(f) + \mathrm{Grad}(g).$$

Die Menge $R[X]$ ist also ein Unterring von $R[[X]]$.

Proposition 2.50. *Ist R ein Integritätsbereich, so gilt*

$$\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$$

für alle Polynome $f, g \in R[X]$.

Beweis. Setze $n := \mathrm{Grad}(f)$ und $m := \mathrm{Grad}(g)$ mit $f = \sum_{k=0}^{n} a_k X^k$ und $g = \sum_{k=0}^{m} b_k X^k$. Sei $f \cdot g = \sum_{k=0}^{\infty} c_k X^k$. Es gilt

$$c_{n+m} = \sum_{i=0}^{n+m} a_i b_{k-i} = a_n b_m.$$

Per Definition gilt $a_n \neq 0$ und $b_m \neq 0$. Es folgt $a_n b_m \neq 0$ weil R eine Integritätsbereich ist. Es gilt also $\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$. □

Korollar 2.51. *Ist R ein Integritätsbereich, so ist $R[X]$ ein Integritätsbereich.*

Sei $P = \sum_{i=0}^{N} a_i X^i$ ein Polynom mit Koeffizienten in R, und x ein Element in R. Man definiert das Element

$$P(x) := \sum_{i=0}^{N} a_i x^i.$$

Die Abbildung:

$$\mathrm{ev}_x : R[X] \longrightarrow R, \quad P \mapsto P(x)$$

ist ein surjektiver Homomorphismus von Ringen.

Division mit Rest in $R[X]$ Sei R ein kommutativer Ring.

Satz 2.52. *Sei P ein Polynom von Grad n mit Koeffizienten in R und mit invertierbarer Leitkoeffizient. Für jedes Polynom $Q \in R[X]$ existieren zwei Polynome $A, B \in R[X]$ mit $Q = AP + B$ und mit entweder $B = 0$ oder $0 \leq \mathrm{Grad}(B) < \mathrm{Grad}(P)$. Die Polynome A, B sind eindeutig bestimmt.*

Beweis. Sei m der Grad von Q. Wir beweisen die Existenz von A, B per Induktion nach m. Ist $Q = 0$, so ist die Behauptung offensichtlich. Schreiben wir $P = \sum_{i=0}^{n} a_i X^i$ und $Q = \sum_{i=0}^{m} b_i X^i$. Wenn $m < n$ gilt, so kann man $A = 0$ und $B = Q$ wählen. Ansonsten gilt $m \geq n$. Das Polynom $a_n^{-1} b_m X^{m-n} P$ hat Grad m und Leitkoeffizient b_m. Es folgt, dass der Grad von $Q - a_n^{-1} b_m X^{m-n} P$ kleiner als m ist. Nach der Induktionsvoraussetzung existieren $A', B' \in R[X]$ mit

$$Q - a_n^{-1} b_m X^{m-n} P = A'P + B'$$

und mit entweder $B' = 0$ oder $0 \leq \mathrm{Grad}(B') < \mathrm{Grad}(P)$. Es folgt also

$$Q = (b_m X^{m-n} a_n^{-1} + A')P + B'$$

und die Behauptung folgt.

Wir zeigen nun die Eindeutigkeit. Seien $A.B, A', B'$ mit $AP+B = A'P+B'$. Dann gilt $B-B' = (A-A')P$. Ist $A-A' \neq 0$, so gilt $\mathrm{Grad}((A-A')P) = \mathrm{Grad}(A-A') + \mathrm{Grad}(P)$ weil die Leitkoeffizient von P invertierbar ist. Aber der Grad von $B - B'$ ist kleiner als $\mathrm{Grad}(P)$. Es folgt also $A = A'$ und $B = B'$. □

Der Polynom B heißt der Rest der Division von Q durch P.

Nullstellen eines Polynoms

Definition 2.53. Sei R ein kommutativer Ring und sei $P \in R[X]$ ein Polynom mit Koeffizienten in R. Ein Element $x \in R$ heißt *Nullstelle* oder *Wurzel* von P, falls $P(x) = 0$ gilt.

Satz 2.54. *Sei R ein kommutativer Ring und $P \in R[X]$ ein Polynom. Ein Element x in R ist genau dann eine Nullstelle von P, wenn ein Polynom $A \in R[X]$ existiert mit $P = (X - x)A$.*

Beweis. Ist $P = (X - x)A$ mit $A \in R[X]$, so gilt $P(x) = (x - x)A(x) = 0$. Umgekehrt, nehmen wir an, dass x eine Nullstelle von P ist. Sei $P = (X - x)A + B$ die Division mit Rest von P durch $X - x$ (Satz 2.52)). Es gilt entweder $B = 0$ oder $\mathrm{Grad}(B) < \mathrm{Grad}(X - x) = 1$. Das Polynom B ist also konstant, d.h. $B = b \in R$. Es folgt $P(x) = b = 0$, also $P = (X - x)A$ und die Behauptung folgt. □

Beispiel 2.55. Das Polynom $P = X^2 + 1$ hat keine Nullstelle in $\mathbb{R}$, weil $x^2 + 1 > 0$ für alle $x \in \mathbb{R}$ gilt. Es gilt aber $P(i) = P(-i) = 0$. In $\mathbb{C}[X]$ gilt die Gleichung $X^2 + 1 = (X - i)(X + i)$.

Korollar 2.56. *Sei R ein Integritätsbereich. Ist $P \in R[X]$ ein Polynom von Grad $n \geq 0$, so hat P höchstens n Nullstellen in R.*

Beweis. Die Aussage gilt natürlich für $n = 0$. Wir dürfen also annehmen, dass n positiv ist. Sei a eine Nullstelle von P. Es gilt $P = (X - a)Q$ mit $Q \in K[X]$. Der Grad von Q ist $n - 1$. Die Nullstellen von P sind dann genau a zusammen mit den Nullstellen von Q, weil R ein Integritätsbereich ist. Nach der Induktionsvoraussetzung hat Q höchstens $n - 1$ Nullstellen, also P hat höchstens n Nullstellen. □

Beispiel 2.57. Für einen beliebigen Ring gilt die Aussage von Korollar 2.56 im allgemeinen nicht. Zum Beispiel im Ring $\mathbb{Z}/9\mathbb{Z}$ gilt $\bar{0}^2 = \bar{3}^2 = \bar{6}^2 = \bar{0}$. Das Polynom $P = X^2$ hat also drei Nullstellen in $\mathbb{Z}/9\mathbb{Z}$. Es gilt:

$$X^2 = (X - 3)(X + 3) = (X - 6)(X + 6)$$

im Ring $(\mathbb{Z}/9\mathbb{Z})[X]$.

2.8 Quotientenkörper von $R[X]$ und von $R[[X]]$

Ist K ein Körper, so ist der Ring $K[X]$ ein Integritätsbereich. Der Quotientenkörper von $K[X]$ wird mit $K(X)$ bezeichnet. Er besteht aus den Brüchen $\frac{P}{Q}$ mit $P, Q \in K[X]$, $Q \neq 0$. Sei R ein Integritätsbereich und K der Quotientenkörper von R. Dann ist $K(X)$ der Quotientenkörper von $R[X]$.

Ist $f = \sum_{n=0}^{\infty} a_n X^n$ eine Potenzreihe mit Koeffizienten in einem kommutativen Ring R, so definiert man die Bewertung von f durch:

$$\nu(f) := \min\{n \geq 0,\ a_n \neq 0\}$$

falls $f \neq 0$ und $\nu(f) = +\infty$ falls $f = 0$. Die Bewertung der Potenzreihe X ist also 1, und die Bewertung von $1+X$ ist 0. Eine Potenzreihe mit Bewertung n ist also der Form

$$a_n X^n + a_{n+1} X^{n+1} + ... = X^n \cdot (a_n + a_{n+1} X + ...)$$

wobei $a_n \neq 0$. Die Bewertung einer Potenzreihe f ist die größte Zahl n, so dass f durch X^n teilbar ist. Es gilt die folgenden Ungleichungen:

$$\nu(f+g) \geq \min\{\nu(f), \nu(g)\} \tag{2.10}$$

$$\nu(fg) \geq \nu(f) + \nu(g) \tag{2.11}$$

für alle $f, g \in R[[X]]$.

Lemma 2.58. *Ist R ein Integritäts bereich, so gilt die Gleichung*

$$\nu(fg) = \nu(f) + \nu(g) \tag{2.12}$$

für alle $f, g \in R[[X]]$.

Beweis. Wir können annehmen, dass f und g verschieden von Null sind. Setze: $f = \sum_{k=0}^{\infty} a_k X^k$, $g = \sum_{k=0}^{\infty} b_k X^k$, $fg = \sum_{k=0}^{\infty} c_k X^k$ und $n = \nu(f)$ und $m = \nu(g)$. Es gilt $c_{n+m} = a_n b_m$ mit $a_n \neq 0$ und $b_m \neq 0$. Ist R ein Integritätsbereich, so folgt es $c_{n+m} \neq 0$, also $\nu(fg) = n + m$. □

Korollar 2.59. *Ist R ein Integritätsbereich, so ist $R[[X]]$ ein Integritätsbereich.*

Eine Laurent-Reihe mit Koeffizienten in R ist eine Abbildung $a : \mathbb{Z} \to R$, $n \mapsto a_n$, so dass ein $N \in \mathbb{Z}$ existiert mit $a_n = 0$ für $n < N$. Man bezeichnet diese Abbildung mit

$$\sum_{-\infty}^{\infty} a_n X^n$$

und heißt *Laurent-Reihe*. Eine Potenzreihe ist insbesondere eine Laurent-Reihe. Die Menge der Laurent-Reihen mit Koeffizienten in R wird mit $R((X))$ bezeichnet. Man definiert eine Addition und eine Multiplikation auf $R((X))$ genauso wie für Potenzreihen: Sind $f = \sum_{-\infty}^{\infty} a_n X^n$ und $g = \sum_{-\infty}^{\infty} b_n X^n$ zwei Laurent-Reihen, so definiert man

$$f + g = \sum_{-\infty}^{\infty} (a_n + b_n) X^n$$

$$fg = \sum_{-\infty}^{\infty} (cn) X^n \quad \text{mit } c_n = \sum_{r,s \in \mathbb{Z}, r+s=n} a_r b_s$$

Der Koeffizient c_n ist wohldefiniert, weil die Summe $\sum_{r,s \in \mathbb{Z}, r+s=n} a_r b_s$ mur endlich viele Terme ungleich Null enthält (denn es gilt $a_r = b_r = 0$ für r ßehr negativ"). Diese Verknüpfungen definieren eine Struktur eines Rings auf $R((X))$, und $R[[X]]$ ist ein Unterring von $R((X))$. Man kann die Bewertung ν auf $R((X))$ erweitern:

$$\nu(f) := \min\{n \in \mathbb{Z},\ a_n \neq 0\}$$

für alle $f = \sum_{-\infty}^{\infty} a_n X^n$ in $R((X))$. Dies definiert eine Abbildung $\nu : R((X)) \to \mathbb{Z} \cup \{\infty\}$, und die Ungleichungen 2.10 gelten auch in $R((X))$. Ist R ein Integritätsbereich, so gilt die Gleichung 2.12 in $R((X))$.

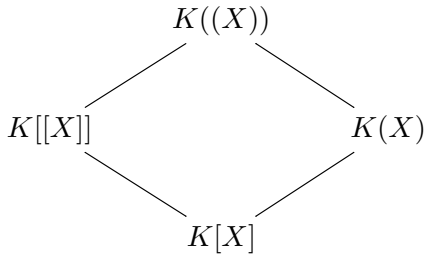
Proposition 2.60. *Sei K ein Körper. Der Ring $K((X))$ ist der Quotientenkörper von $K[[X]]$.*

Beweis. Sei $f = \sum_{-\infty}^{\infty} a_n X^n$ eine Laurent-Reihe mit $f \neq 0$. Setzte $N = \nu(f)$. Es gilt:

$$f = X^N \cdot f = X^n \cdot \sum_{n=0}^{\infty} a_{n+N} X^n \tag{2.13}$$

und $a_N \neq 0$. Die Potenzreihe $g = \sum_{n=0}^{\infty} a_{n+N} X^n$ ist eine Einheit von $K[[X]]$ nach Proposition 2.48. Insbesondere ist g auch in $K((X))$ invertierbar. Das Element X^N ist auch invertierbar in $K((X))$ (das Inverse ist X^{-N}). Das Element f ist also invertierbar in $K((X))$, und $K((X))$ ist somit ein Körper. Die Gleichung 2.13 zeigt, dass $K((X))$ der Quotientenkörper von $K[[X]]$ ist. □

Ist K ein Körper, so haben wir folgendes Diagram:



2.9 Primideale, Maximale Ideale

Sei R ein kommutativer Ring, mit $R \neq \{0\}$.

Definition 2.61.

(i) Ein Ideal $\mathfrak{p} \subset R$ heißt *prim* oder *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn die folgende Eigenschaft gilt: Für alle $x, y \in R$,

$$xy \in \mathfrak{p} \Longrightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}) .$$

(ii) Ein Ideal $\mathfrak{m} \subset R$ heißt maximal, wenn $\mathfrak{m} \neq R$ ist, und wenn gilt: Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a} \subset R$, so folgt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Proposition 2.62.

(i) Ein Ideal $\mathfrak{p} \subset R$ ist genau dann ein Primideal, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsbereich ist.

(ii) Ein Ideal $\mathfrak{m} \subset R$ ist genau dann ein maximales Ideal, wenn der Faktorring $R/\mathfrak{m}$ ein Körper ist.

Beweis. Der Faktorring $R/\mathfrak{p}$ ist ein Integritätsbereich, wenn gilt: Für alle $\bar{x}, \bar{y} \in R/\mathfrak{p}$ mit $\bar{x}\bar{y} = 0$, so ist $\bar{x} = 0$ oder $\bar{y} = 0$. Aber $\bar{x} = 0$ in $R/\mathfrak{p}$ is äquivalent zu $x \in \mathfrak{p}$, also die Behauptung folgt.

Der Ring $R/\mathfrak{m}$ ist genau dann ein Körper, wenn $\mathcal{I}(R/\mathfrak{m})$ nur aus den Idealen 0 und $R/\mathfrak{m}$ besteht (Proposition 2.27). Die Ideale die $\mathfrak{m}$ enthalten entsprechen den Idealen von $R/\mathfrak{m}$ durch die Bijektion (2.3). Es folgt, dass $R/\mathfrak{m}$ genau dann ein Körper ist, wenn die einzigen Ideale von R die $\mathfrak{m}$ enthalten sind $\mathfrak{m}$ und R. □

Proposition 2.63. *Sei $f : R \to S$ ein Homomorphismus von Ringen. Ist $\mathfrak{p} \subset S$ ein Primideal, so ist $f^{-1}(\mathfrak{m})$ ein Primideal von R.*

Beweis. Sei $\pi : S \to S/\mathfrak{p}$ die natürliche Projektion und sei $g = \pi \circ f$. Es gilt $\mathrm{Kern}(g) = f^{-1}(\mathfrak{p})$, also wir erhalten einen injektiven Homomorphismus von Ringen:

$$R/f^{-1}(\mathfrak{p}) \to S/\mathfrak{p}.$$

Ein Unterring eines Integritätsbereichs ist ein Integritätsbereich, also $f^{-1}(\mathfrak{p})$ ist ein Primideal. □

Satz 2.64. *Sei R ein kommutativer Ring, und sei $I \subset R$ ein Ideal mit $I \neq R$. Dann existiert ein maximales Ideal $\mathfrak{m}$ mit $I \subset \mathfrak{m}$.*

Der Beweis benutzt das Lemma von Zorn. Es ist äquivalent zum Auswahlaxiom. Sei X eine Menge. Eine partielle Ordnung auf X ist eine Relation $\leq$ auf X mit den folgenden Eigenschaften:

(i) Es gilt $x \leq x$ für alle $x \in X$ (Reflexivität)

(ii) Aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in X$ (Antisymmetrie)

(iii) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z \in X$ (Transitivität)

Die partielle Ordnung $\leq$ heißt *totale Ordnung*, wenn für alle $x, y \in X$ entweder $x \leq y$ oder $y \leq x$ gilt. Die Menge X heißt dann *total geordnet*.

Beispiel 2.65.

(a) Die Menge der natürlichen Zahlen ist total geordnet bezüglich der natürlichen Ordnung $\leq$.

(b) Die Relation $a|b$ (a teilt b) auf $\mathbb{N}^*$ ist eine partielle Ordnung, die nicht total ist, weil weder $2|3$ noch $3|2$ gelten.

(c) Sei X eine Menge. Die Potenzmenge $\mathcal{P}(X)$ von X ist partiell geordnet bezüglich der Relation $A \subset B$ für $A, B \subset X$. Die Menge $(\mathcal{P}(X), \subset)$ ist genau dann total geordnet, wenn X eine einelementige Menge ist.

Ist $(X, \leq)$ eine partiell geordnete Menge und $Y \subset X$ eine Teilmenge, so heißt $x \in X$ eine obere Schranke von Y, falls $y \leq x$ für alle $y \in Y$ gilt. Ein *maximales Element* von X ist ein Element $x \in X$, sodass gilt: Aus $x \leq y$ für $y \in X$ folgt $x = y$.

Lemma 2.66 (Lemma von Zorn)**.** *Sei $(X, \leq)$ eine partiell geordnete Menge, in der jede total geordnete Teilmenge eine obere Schranke besitzt. Dann existiert in X mindestens ein maximales Element.*

Dieses Lemma kann mit den anderen Axiomen der Mengenlehre nicht bewiesen werden, und wird als Axiom hinzugefügt. Wir beweisen nun den Satz 2.64 mit Hilfe des Lemmas von Zorn:

Sei X die Menge der idealen $\mathfrak{a} \neq R$, die das Ideal I enthalten. Die Menge X ist nicht leer denn es gilt $I \in X$. Die Inklusion $\subset$ ist eine partielle Ordnung auf X. Sei $Y \subset X$ eine Teilmenge, sodass $(Y, \subset)$ eine total geordnete Menge ist. Wir zeigen, dass Y eine obere Schranke in X hat. Sei:

$$\mathfrak{b} := \bigcup_{\mathfrak{a} \in Y} \mathfrak{a}.$$

Die Teilmenge $\mathfrak{b} \subset R$ ist ein Ideal: Für $x, y \in \mathfrak{b}$ existiert $\mathfrak{a}, \mathfrak{a}' \in Y$ mit $x \in \mathfrak{a}$ und $y \in \mathfrak{a}'$. Da $(Y, \subset)$ total geordnet ist, existiert $\mathfrak{a}'' \in Y$ mit $\mathfrak{a} \subset \mathfrak{a}''$ und $\mathfrak{a}' \subset \mathfrak{a}''$. Es folgt $x + y \in \mathfrak{a}'' \subset \mathfrak{b}$. Es ist auch klar, dass $rx \in \mathfrak{b}$ für alle $x \in \mathfrak{b}$ und $r \in R$ gilt. Das Ideal $\mathfrak{b}$ ist verschieden von R, weil keines der Ideale $\mathfrak{a} \in Y$ das Element 1 enthält. Das Ideal $\mathfrak{b}$ ist also eine obere Schranke von Y. Es folgt nach dem Lemma von Zorn, dass ein maximales Element $\mathfrak{m}$ in X existiert. Man sieht sofort, dass es ein maximales Ideal ist, das I enthält.

2.10 Irreduzible Elemente, Primelemente

Sei R ein kommutativer Ring.

Definition 2.67.

(i) Ein Element x heißt *irreduzibel*, wenn es nicht invertierbar ist, und wenn aus jeder Darstellung $x = yz$ mit $y, z \in R$ folgt, dass entweder y oder z invertierbar ist.

(ii) Ein Element $x \neq 0$ heißt *Primelement* oder *prim*, wenn das Ideal (x) prim ist.

Ein Element ist also prim, wenn x nicht invertierbar ist, und wenn die folgende Eigenschaft erfüllt ist: Teilt x ein Produkt ab, so ist x entweder ein Teiler von a oder ein Teiler von b. Ein Element x ist *reduzibel* oder *zerlegbar*, falls es nicht irreduzibel ist, d.h. falls nicht-invertierbare Elemente $y, z \in R$ exitieren mit $x = yz$.

Beispiel 2.68.

(a) Die irreduziblen Elemente von $\mathbb{Z}$ sind die Zahlen $\pm p$, wo p eine Primzahl ist.

(b) Sei R ein Integritätsbereich und $P \in R[X]$ ein Polynom von Grad 2 oder 3. Ist P reduzibel, so existieren zwei Polynome $A, B \in R[X]$ von Grad ≥ 1 mit $P = AB$. Dann hat entweder A oder B Grad 1. Es folgt aus Satz 2.54 : Das Polynom P ist genau dann irreduzibel in $R[X]$, wenn es keine Nullstelle hat.

(c) Das Polynom $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$ aber nicht in $\mathbb{C}[X]$.

Proposition 2.69. *Ist R ein Integritätsbereich, so ist jedes Primelement irreduzibel.*

Beweis. Sei x ein Primelement, und sei $x = yz$ mit $y, z \in R$. Es folgt, dass x entweder ein Teiler von y oder ein Teiler von z ist. Ohne Beschränkung gilt $y = xa$ mit $a \in R$. Dann ist $x = xaz$, und es folgt $az = 1$ weil $x \neq 0$ ist, und weil R ein Integritätsbereich ist. Das Element z ist also invertierbar. □

Beispiel 2.70. Hier ist ein Gegenbeispiel für ein irreduzibles Element, das nicht prim ist. Sei R die Menge der komplexen Zahlen der Form: $a+i\sqrt{5}b$ mit $a, b \in \mathbb{Z}$. Die Summe zweier solchen Elemente ist noch dieser Form, und für $a, b, c, d \in \mathbb{Z}$ gilt die Gleichung

$$(a + i\sqrt{5}b)(c + i\sqrt{5}d) = (ac - 5bd) + i\sqrt{5}(ad + bc).$$

Es folgt, dass R ein Unterring von $\mathbb{C}$ ist. Er wird mit $\mathbb{Z}[i\sqrt{5}]$ bezeichnet. Ist $z \in R$ ein Element in R, so ist $\bar{z}$ auch in R. Das Produkt $N(z) := z\bar{z}$ ist also ein Element von $R \cap \mathbb{R}_+ = \mathbb{N}$. Dieses Element heißt die Norm von z. Es gilt natürlich $N(zz') = N(z)N(z')$ für alle $z, z' \in R$. Für $z = a + i\sqrt{5}b$ mit $a, b \in \mathbb{Z}$ gilt

$$N(z) = a^2 + 5b^2. \tag{2.14}$$

Lemma 2.71. *Ein Element $z \in R$ ist genau dann invertierbar in R, wenn $N(z) = 1$ gilt.*

Beweis. Ist $z \in R$ invertierbar, so existiert $z' \in R$ mit $zz' = 1$. Es folgt $N(z)N(z') = N(1) = 1$. Da $N(z)$ und $N(z')$ natürliche Zahlen sind, folgt es $N(z) = 1$. Umgekehrt, wenn $N(z) = z\bar{z} = 1$ gilt, ist $\bar{z}$ das Inverse zu z. □

Korollar 2.72. *Die invertierbaren Elemente von R sind $\{1, -1\}$.*

Beweis. Es folgt sofort aus der Formel (2.14), dass $\{1, -1\}$ die einzigen Lösungen der Gleichung $N(z) = 1$, $z \in R$ sind. □

Es gilt die Gleichung:

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6.$$

Das Element 2 teilt also dieses Produkt, aber es ist klar, dass weder $(1 + i\sqrt{5})$ noch $(1 - i\sqrt{5})$ durch 2 teilbar sind. Das Element 2 ist also nicht prim.

Es ist aber irreduzibel: Angenommen es gilt $2 = zz'$ mit $z, z' \in R$. Dann gilt $N(z)N(z') = N(2) = 4$, und es folgt $N(z), N(z') \in \{1, 2, 4\}$. Die Gleichung $N(y) = 2$ mit $y \in R$ hat keine Lösung (Formel (2.14)), also es gilt entweder $N(z) = 1$ oder $N(z') = 1$. Dann ist z oder z' invertierbar. Das Element 2 ist also irreduzibel.

2.11 Euklidischer Ring, Hauptidealring

Definition 2.73. Ein Integritätsbereich R heißt *Hauptidealring*, falls jedes Ideal in R ein Hauptideal ist.

Beispiel 2.74. Der Ring $\mathbb{Z}$ ist ein Hauptidealring (Satz 1.43).

Proposition 2.75. *Sei R ein Hauptidealring und $f \in R \setminus \{0\}$. Die folgenden Aussagen sind äquivalent:*

(i) Das Element f ist prim.

(ii) Das Element f ist irreduzibel.

(iii) Das Ideal (f) ist maximal.

(iv) Das Ideal (f) ist prim.

Beweis. Wir wissen schon, dass $(i) \Longrightarrow (ii)$, $(iii) \Longrightarrow (iv)$ und $(iv) \Longrightarrow (i)$ gelten. Es bleibt zu beweisen, dass $(ii) \Longrightarrow (iii)$ gilt. Nehmen wir an, dass f irreduzibel ist. Ist $I = (a)$ ein Ideal mit $(f) \subset I \subset R$, so gilt $f = ab$ mit $b \in R$. Es folgt, dass entweder a oder b invertierbar ist. Es gilt also entweder $I = R$ oder $I = (f)$. Das Ideal (f) ist somit maximal. □

Sei R ein kommutativer Ring. Eine *Gradfunktion* auf R ist eine Funktion

$$g : R \setminus \{0\} \to \mathbb{N}$$

mit der folgenden Eigenschaft: Für alle $a, b \in R$ mit $b \neq 0$ existieren Elemente $q, r \in R$ mit $a = qb + r$, wobei entweder $r = 0$ oder $g(r) < g(b)$ ist.

Definition 2.76. Ein Integritätsbereich R heißt euklidischer Ring, falls eine Gradfunktion auf R existiert.

Satz 2.77. *Ein euklidischer Ring ist ein Hauptidealring.*

Beweis. Sei $I \subset R$ ein Ideal. Sei $x \in I$, $x \neq 0$ ein Element mit $g(x)$ minimal. Sei $y \in I$ ein Element. Dann existiert $q, r \in R$ mit $y = qx+r$ mit entweder $r = 0$ oder $g(r) < g(x)$. Angenommen es gilt $r \neq 0$, dann ist $r = y - qx$ ein Element in I mit $g(r) < g(x)$, aber dies widerspricht der Minimalität von $g(x)$. Es folgt also $r = 0$ und $y = qx$, und somit $I = (x)$. □

Der Ring $\mathbb{Z}$ ist ein euklidischer Ring. Der Betrag $g : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, $k \mapsto |k|$ ist eine Gradfunktion: Sind $x, y \in \mathbb{Z}$ mit $x \neq 0$, so existiert $q, r \in \mathbb{Z}$ mit $y = xq + r$ und $0 \leq r < |x|$ (Division mit Rest).

Sei K ein Körper. Es folgt aus der Polynomdivision (Satz (2.52)), dass die Abbildung $K[X] \setminus \{0\} \to \mathbb{N}$, $P \mapsto \mathrm{Grad}(P)$ eine Gradfunktion ist. Wir erhalten also folgendes Ergebnis:

Satz 2.78. *Der Ring $K[X]$ ist ein euklidischer Ring, insbesondere ein Hauptidealring.*

2.12 Noetherscher Ring

Sei R ein kommutativer Ring. Ein Ideal $I \subset R$ heißt *von endlichem Typ*, falls es Elemente $a_1, ..., a_r \in I$ gib mit $I = Ra_1 + ... + Ra_r$, d.h. falls I von endlich vielen Elementen erzeugt wird.

Satz 2.79. *Die folgende Aussagen sind Äquivalent:*

(i) Jedes Ideal von R ist von endlichem Typ.

(ii) *Jede aufsteigende Kette von Idealen* $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ *wird stationär, d.h. es existiert* $n \in \mathbb{N}$ *mit* $\mathfrak{a}_i = \mathfrak{a}_n$ *für alle* $i \geq n$.

(iii) *Für jede nicht-leere Teilmenge* $T \subset \mathcal{I}(R)$ *existiert* $\mathfrak{a} \in T$, *so dass für alle* $\mathfrak{b} \in T$ *gilt:*

$$\mathfrak{a} \subset \mathfrak{b} \Longrightarrow \mathfrak{a} = \mathfrak{b}$$

d.h. die partiell geordnete Menge $(T, \subset)$ *besitzt ein maximales Element.*

Vorsicht: Das Ideal $\mathfrak{a} \in T$ in (iii) ist ein maximales Element von T, aber das bedeutet nicht, das $\mathfrak{a}$ ein maximales Ideal ist.

Beweis. Die Aussage (ii) folgt aus der Aussage (iii) wenn man $T = \{\mathfrak{a}_i,\ i \geq 0\}$ wählt. Umgekehrt, wenn T in (iii) kein maximales Element besitzt, kann man per Induktion eine nicht-stationäre aufsteigende Kette von Idealen konstruieren.

Sei I ein Ideal von R. Angenommen die Aussage (iii) gilt, sei T die Familie der Idealen von endlichem Typ $J \subset I$. Die Menge T ist offensichtlich nicht leer. Sei $\mathfrak{a} \in T$ wie in (iii) ein maximales Element von T. Für ein Element x in I ist das Ideal $J = \mathfrak{a} + Rx$ von endlichem Typ und in I enthalten, und es gilt $\mathfrak{a} \subset J$. Es folgt aus der Maximalität von $\mathfrak{a}$ in T, dass $\mathfrak{a} = J$ gilt. Insbesondere ist x ein Element in $\mathfrak{a}$. Es gilt also $J = I$, und I ist somit von endlichem Typ.

Es bleibt noch zu zeigen, dass $(i) \Longrightarrow (ii)$ gilt. Sei $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ eine aufsteigende Kette von Idealen in R. Die Vereinigung

$$I = \bigcup_{i \in \mathbb{N}} \mathfrak{a}_i$$

ist ein Ideal. Es existieren Elemente $a_1, ..., a_r \in I$ mit $I = Ra_1 + ... + Ra_r$. Sei $n \in \mathbb{N}$ so dass alle Elemente $a_1, ..., a_r$ in $\mathfrak{a}_n$ enthalten sind. Dann gilt $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$. □

Definition 2.80. Ein kommutativer Ring heißt *noethersch*, wenn diese Eigenschaften erfüllt sind.

Beispiel 2.81. Ein Hauptidealring ist noethersch.

Satz 2.82. *In einem noetherschen Ring besitzt jedes Element in* $R \setminus (R^\times \cup \{0\})$ *eine Zerlegung in ein Produkt irreduzibler Elemente.*

Beweis. Sei T die Familie der Ideale (x), wo $x \in R \setminus (R^\times \cup \{0\})$ ein Element ist, das keine Zerlegung in ein Produkt irreduzibler Elemente besitzt. Angenommen T ist nicht leer, existiert dann ein Ideal $\mathfrak{a} = (a)$ wie in der Aussage (iii) von Satz 2.79 (ein "maximales Element"von T). Das Element a ist nicht irreduzibel. Es existiert also $b, c \in R$ nicht invertierbar mit $a = bc$. Es gilt $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Es folgt aus der Maximalität von (a) in T, dass die Ideale (b) und (c) keine Elemente von T sind. Die Elemente b und c besitzen also eine Zerlegung in ein Produkt irreduzibler Elemente. Aber dann gilt diese Eigenschaft offensichtlich auch für das Produkt $a = bc$, und dies ist ein Widerspruch. □

Satz 2.83. *Ist* R *ein noetherscher Ring, so ist* $R[X]$ *auch noethersch.*

Beweis. Sei $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ eine aufsteigende Kette von Idealen von $R[X]$. Nehmen wir an, dass diese Kette nicht stationär wird. Sei $\mathfrak{a} = \bigcup_{i\geq 1} \mathfrak{a}_i$. Man sieht sofort, dass $\mathfrak{a}$ ein Ideal von $R[X]$ ist. Für $n \geq 1$, sei P_n ein Element von $\mathfrak{a} \setminus \mathfrak{a}_n$ minimalen Grades. Es ist klar, dass die Folge $g_n := \mathrm{Grad}(P_n)$ eine aufsteigende Folge ist. Sei a_n der Leitkoeffizient von P_n und sei

$$I = \langle a_i,\ i \geq 1\rangle \subset R$$

das von den a_i erzeugte Ideal. Da R noethersch ist, existiert $k \geq 1$ mit $I = \langle a_i,\ 1 \leq i \leq k\rangle$. Sei $N \geq k$ sodass $P_i \in \mathfrak{a}_N$ für alle $1 \leq i \leq k$ gilt. Für $n \geq N$ existiert also Elemente $b_1, ..., b_k \in R$ mit

$$a_n = \sum_{i=1}^{k} a_i b_i.$$

Der Grad des Polynoms

$$Q := P_n - \sum_{i=0}^{k} b_i X^{g_n - g_i} P_i$$

ist kleiner als g_n, also Q ist ein Element in $\mathfrak{a}_n$. Für $1 \leq i \leq k$ sind die Polynome P_i auch in $\mathfrak{a}_N \subset \mathfrak{a}_n$. Es folgt, dass P_n ein Element in $\mathfrak{a}_n$ ist, im Widerspruch zur Definition von P_n. □

Definition 2.84. Ein kommutativer Ring R erfüllt die Bedingung (ACCP), falls jede aufsteigende Kette von Hauptidealen in R stationär wird.

Natürlich erfüllen alle noethersche Ringe diese Bedingung. Die Buchstaben (ACCP) stehen für äscending chain condition on principal ideals".

Bemerkung 2.85. Der Beweis von Proposition 2.82 funktioniert auch für Ringe, die die Bedingung (ACCP) erfüllen. In einem solchen Ring R besitzt also jedes Element in $R \setminus (R^\times \cup \{0\})$ eine Zerlegung in ein Produkt irreduzibler Elemente.

2.13 Faktorieller Ring

Definition 2.86. Ein Integritätsbereich R heißt *faktoriell*, falls jedes Element $x \in R \setminus (R^\times \cup \{0\})$ eine Zerlegung in ein Produkt von Primelementen besitzt.

Man sagt, dass zwei Elemente a, b eines kommutativen Rings R *assoziiert* sind, wenn ein invertierbares Element $x \in R$ existiert mit $a = bx$. Dies ist eine Äquivalenzrelation auf R. Ist a assoziiert zu einem primen (bzw. irreduziblen) Element, so ist a auch prim (bzw. irreduzibel). Sei R ein faktorieller Ring. Ein *Repräsentantensystem der irreduziblen Elemente* in R ist eine Teilmenge $\mathcal{P} \subset R$ mit den Eigenschaften:

(i) Alle Elemente in $\mathcal{P}$ sind irreduzibel.

(ii) Jedes irreduzible Element in R ist genau zu einem Element aus $\mathcal{P}$ assoziiert.

Beispiel 2.87. Die Menge der Primzahlen ist ein Repräsentantensystem der irreduziblen Elemente von $\mathbb{Z}$.

Satz 2.88. *Sei R ein faktorieller Ring und sei $\mathcal{P} \subset R$ ein Repräsentantensystem der irreduziblen Elemente in R. Es gilt:*

(i) Ein Element ist genau dann irreduzibel, wenn es prim ist.

(ii) Zu jedem Element $x \in R\backslash\{0\}$ existieren paarweise verschiedene Elemente $p_1, ..., p_r \in \mathcal{P}$, positive natürliche Zahlen $k_1, ..., k_r \geq 1$ und ein invertierbares Element $u \in R^\times$ mit

$$x = up_1^{k_1}...p_r^{k_r}. \tag{2.15}$$

Diese Zerlegung ist eindeutig bis auf Reihenfolge der Faktoren p^{k_i}.

Beweis. Sei $a \in R$ ein irreduzibles Element. Es existieren primelemente $b_1, ..., b_n$ mit $a = b_1...b_n$. Da a irreduzibel ist, folgt es $n = 1$, d.h. a ist ein Primelement. Die Existenz der Zerlegung (2.15) ist klar. Wir beweisen per Induktion (nach r) die Eindeutigkeit. Seien

$$x = up_1^{k_1}...p_r^{k_r} = u'q_1^{m_1}...q_s^{m_s} \tag{2.16}$$

zwei Zerlegungen der Form (2.15). Das Primelement p_1 teilt das Produkt $u'q_1^{m_1}...q_s^{m_s}$, also es existiert $i \in \{1, ..., s\}$ mit $p_1|q_i$. Es gibt ein $z \in R$ mit $q_i = yp_1$. Dann muss y invertierbar sein, also p_1 und q_i sind assozierte Elemente von $\mathcal{P}$. Es folgt $p_1 = q_i$. Dann erhalten wir aus (2.16) die Gleichung

$$up_2^{k_1-1}...p_r^{k_r} = u'q_1^{m_1}...q_i^{m_i-1}...q_s.$$

Die Eindeutigkeit gilt nach der Induktionsvoraussetzung. □

Sei R ein faktorieller Ring mit Quotientenkörper K, und sei $\mathcal{P}$ ein Repräsentantensystem der irreduziblen Elemente von R. Für jedes Element $x \in K \setminus \{0\}$ existiert dann eine eindeutige Darstellung:

$$x = u \prod_{p \in \mathcal{P}} p^{k_p} \tag{2.17}$$

mit $u \in R^\times$ und $(k_p)_{p\in\mathcal{P}} \in \mathbb{Z}^{(\mathcal{P})}$ eine Familie von ganzen Zahlen, die fast alle gleich Null sind. Dies folgt sofort aus dem Satz 2.88. Für $p \in \mathcal{P}$ definieren wir die Zahl $\nu_p(x) \in \mathbb{Z}$ als die Zahl k_p in der obigen Primfaktorzerlegung von x. Für alle $x \in K \setminus \{0\}$ sind dann die folgenden Aussagen äquivalent:

(i) Das Element x ist in R.

(ii) Für alle $p \in \mathcal{P}$ gilt $v_p(x) \geq 0$.

Korollar 2.89. *Sei R ein faktorieller Ring mit Quotientenkörper K, und sei $R^\times$ die multiplikative Gruppe der invertierbaren Elemente von R. Sei $\mathcal{P}$ ein Repräsentantensystem der irreduziblen Elemente von R. Die Abbildung*

$$R^\times \times \mathbb{Z}^{(\mathcal{P})} \longrightarrow K \setminus \{0\}, \quad (u, (k_p)_{p\in\mathcal{P}}) \mapsto u \prod_{p\in\mathcal{P}} p^{k_p}$$

ist ein Isomorphismus von Gruppen, wobei $K \setminus \{0\}$ mit der Multiplikation versehen ist.

Beispiel 2.90. Der Ring $\mathbb{F}_3[X]$ ist faktoriell und es gilt $\mathbb{F}_3[X]^\times = \mathbb{F}_3^\times$. Die Gruppe $(\mathbb{F}_3(X) \setminus \{0\}, \times)$ ist also isomorph zu $\mathbb{F}_3^\times \times \mathbb{Z}^{(\mathcal{P}(\mathbb{F}_3[X]))}$, wobei $\mathcal{P}(\mathbb{F}_3[X])$ die Menge der irreduziblen Polynome in $\mathbb{F}_3[X]$ ist. Sei $\mathcal{P}(\mathbb{Z})$ die Menge der Primzahlen. Es ist einfach zu sehen, dass eine Bijektion $\mathcal{P}(\mathbb{F}_3[X]) \to \mathcal{P}(\mathbb{Z})$ existiert (beide Mengen sind abzählbar, siehe Definition 4.12). Es existiert also ein Isomorphismus von Gruppen:

$$(\mathbb{F}_3(X) \setminus \{0\}, \times) \simeq (\mathbb{Q}^*, \times).$$

(siehe Beispiel 1.61).

In einem faktoriellen Ring kann man den größten gemeinsammen Teiler und das kleinste gemeinsamme Vielfache defniieren.

Definition 2.91. Sind x, y zwei Elemente eines faktoriellen Rings R, beide nicht Null. Man definiert:

$$\mathrm{ggT}(x,y) = \prod_{p \in \mathcal{P}} p^{\min\{\nu_p(x), \nu_p(y)\}}$$

$$\mathrm{kgV}(x,y) = \prod_{p \in \mathcal{P}} p^{\max\{\nu_p(x), \nu_p(y)\}}.$$

Man kann auch den g.g.T. und das k.g.V von endlich vielen Elementen $x_1, ..., x_k$ definieren:

$$\mathrm{ggT}(x_1, ..., x_k) = \prod_{p \in \mathcal{P}} p^{\min\{\nu_p(x_1), ..., \nu_p(x_k)\}}$$

$$\mathrm{kgV}(x_1, ..., x_k) = \prod_{p \in \mathcal{P}} p^{\max\{\nu_p(x_1), ..., \nu_p(x_k)\}}.$$

Zwei Elemente x, y in $R \setminus \{0\}$ sind teilerfremd, falls sie keinen gemeinsamen irreduziblen Teiler besitzen. Dies ist äquivalent zur Gleichung $\mathrm{ggT}(x, y) = 1$.

Satz 2.92. *Sei R ein Integritätsbereich. Die folgenden Aussagen sind äquivalent:*

(i) Der Ring R ist faktoriell.

(ii) Der Ring R erfüllt die Bedingung (ACCP) von Definition 2.84 und jedes irreduzible Element in R ist ein Primelement.

Beweis. Die Implikation $(ii) \Rightarrow (i)$ folgt sofort aus Bemerkung 2.85. Umgekehrt, sei R ein faktorieller Ring, und sei $a_0, a_1, a_2, ...$ eine Folge von Elementen aus R mit der Eigenschaft $a_{i+1} | a_i$ für alle $i \geq 0$. Schreibe

$$a_0 = u p_1^{k_1} ... p_r^{k_r}$$

mit $u \in R^\times$, $k_1, ..., k_r \in \mathbb{N}^*$, und $p_1, ..., p_r$ paarweise verschiedene Primelemente in R. Dann gilt

$$(a_i) = \left(p_1^{k_1'} ... p_r^{k_r'}\right)$$

für natürliche Zahlen $k_1', ..., k_r' \in \mathbb{N}^*$ mit $k_j' \leq k_j$ für alle $j \in \{1, ..., r\}$. Es gibt also endlich viele Möglichkeiten für die natürlichen Zahlen k_j'. Die Behauptung folgt. $\square$

Korollar 2.93. *Ein noetherscher Integritätsbereich wo jedes Primelement irreduzibel ist, ist ein faktorieller Ring.*

Beweis. Es folgt direkt aus dem Satz 2.82. □

Korollar 2.94. *Ein Hauptidealring ist ein faktorieller Ring.*

Beispiel 2.95. Die Ringe $\mathbb{Z}$ und $K[X]$ (mit K ein Körper) sind faktoriell, weil sie Hauptidealringe sind.

Proposition 2.96. *Sind x, y zwei Elemente eines Hauptidealrings R, so gilt:*

$$(x) + (y) = (\mathrm{ggT}(x, y))$$

$$(x) \cap (y) = (\mathrm{kgV}(x, y)).$$

Beweis. Es folgt direkt aus dem Satz 2.88. □

Sei R ein faktorieller Ring und sei $\mathcal{P}$ ein Repräsentantensystem der irreduziblen Elemente. Für ein Polynom $f \in R[X] \setminus \{0\}$ und $p \in \mathcal{P}$ definiert man den Inhalt ("le contenuäuf französisch) als der g.g.T. der Koeffizienten von f. Er wird mit $\mathrm{Inhalt}(f)$ oder $\mathrm{cont}(f)$ bezeichnet. Ein Polynom heißt primitiv, falls sein Inhalt 1 ist.

Lemma 2.97 (Gauß)**.** *Sind f, g zwei Polynome in $R[X] \setminus \{0\}$, so gilt*

$$\mathrm{Inhalt}(fg) = \mathrm{Inhalt}(f)\,\mathrm{Inhalt}(g).$$

Insbesondere ist fg genau dann primitiv, wenn f und g primitiv sind.

Beweis. Wir zeigen zunächst dass das Produkt zweier primitiven Polynome primitiv ist. Nehmen wir also an, dass f und g primitiv sind. Wenn fg nicht primitiv wäre, gäbe es ein irreduzibles Element $p \in R$ das alle Koeffizienten von fg teilt. Für ein Polynom $h \in R[X]$ bezeichnen wir mit $\bar{h}$ das Bild von h unter dem natürlichen Homomorphismus von Ringen

$$R[X] \to (R/(p))[X].$$

Dann würde die Gleichung $\bar{f}\bar{g} = 0$ im Ring $(R/(p))[X]$ gelten. Das Ideal (p) ist prim, also der Faktorring $R/(p)$ ist ein Integritätsbereich (Proposition 2.62). Dann ist $(R/(p))[X]$ auch ein Integritätsbereich (Korollar 2.51). Es folgt, dass entweder $\bar{f}$ oder $\bar{g}$ Null ist, im Widerspruch zur Voraussetzung.

Setze nun $a := \mathrm{Inhalt}(f)$ und $b := \mathrm{Inhalt}(g)$ für beliebige Polynome f, g. Seien a^{-1} und b^{-1} die Inversen von a und b im Quotientenkörper. Dann sind die Polynome $a^{-1}f$ und $b^{-1}g$ Elemente in $R[X]$ und sie sind primitiv. Es folgt, dass $(ab)^{-1}fg$ primitiv ist, also $\mathrm{Inhalt}(fg) = ab$. □

2.14 Wann ist ein Ring ein Hauptidealring ?

Proposition 2.98. *Sei R ein faktorieller Ring. Die folgenden Aussagen sind äquivalent:*

(i) Der Ring R ist ein Hauptidealring.

(ii) Jedes Primideal $\mathfrak{p} \neq 0$ in R ist maximal.

Beweis. Die Implikation $(i) \Rightarrow (ii)$ folgt aus Proposition 2.75. Zur Umkehrung: Sei $\mathfrak{m}$ ein maximales Ideal und sei $x \in \mathfrak{m} \setminus \{0\}$. Sei $x = p_1 ... p_k$ eine Primfaktorzerlegung von x. Dann gilt $p_i \in \mathfrak{m}$ für ein $i \in \{1, ..., k\}$. Das Ideal (p_i) ist ein Primideal. Es ist maximal nach der Voraussetzung. Es folgt $\mathfrak{m} = (p_i)$. Jedes maximale Ideal ist ein Hauptideal. Sei nun X die Menge der Ideale in R, die nicht Hauptideale sind. Nehmen wir an, dass X nicht leer ist. Wir beweisen zuerst, dass jede total geordnete Teilmenge von X eine obere Schranke besitzt. Sei $Y \subset X$ eine total geordnete Teilmenge. Sei $\mathfrak{a}$ die Vereinigung aller Elemente aus Y. Dann ist $\mathfrak{a}$ ein Ideal von R (siehe Beweis von Satz 2.64). Wenn $\mathfrak{a}$ ein Hauptideal wäre, würde ein $x \in \mathfrak{a}$ existieren mit $\mathfrak{a} = (x)$. Dann gilt $x \in I$ für ein $I \in Y$ und es folgt $I = (x)$, im Widerspruch zur Definition von X. Das Ideal $\mathfrak{a}$ ist also kein Hauptideal, und ist eine obere Schranke von Y in X. Nach dem Lemma von Zorn (2.66) existiert ein maximales Element I in X. Sei $\mathfrak{m}$ ein maximales Ideal mit $I \subset \mathfrak{m}$, und sei $p \in R \setminus \{0\}$ mit $\mathfrak{m} = (p)$. Definiere

$$p^{-1}I := \left\{ \frac{x}{p} \in K,\ x \in I \right\} \subset R$$

wobei K der Quotientenkörper von R ist. Dann ist $p^{-1}I$ ein Ideal von R und es gilt natürlich $I \subset p^{-1}I \subset R$. Außerdem gilt $I \neq p^{-1}I$. Ansonsten würde die Gleichung $p^m I = I$ für alle $m \geq 0$ gelten. Es würde folgen:

$$I \subset \bigcap_{n \geq 0} p^n R = \{0\}$$

also $I = \{0\}$: Widerspruch. Es gilt also $I \subsetneq p^{-1}I$. Es folgt aus der Maximalität von I, dass $p^{-1}I$ ein Hauptideal ist, also $p^{-1}I = (x)$ für ein $x \in R \setminus \{0\}$. Dann gilt $I = (px)$, und I ist ein Hauptideal: Widerspruch. □

Aus demselben Beweis folgt folgende Proposition:

Proposition 2.99. *Sei R ein Integritätsbereich. Die folgende Eigenschaften sind äquivalent:*

(i) Der Ring R ist ein Hauptidealring.

(ii) Jedes maximale Ideal ist ein Hauptideal, und es gilt:

$$\bigcap_{n \geq 0} p^n R = \{0\}$$

für alle Primelemente p.

Korollar 2.100. *Sei R ein noetherscher Integritätsbereich. Die folgende Eigenschaften sind äquivalent:*

(i) Der Ring R ist ein Hauptidealring.

(ii) Jedes maximale Ideal ist ein Hauptideal.

Beweis. Es reicht zu zeigen, dass $\bigcap_{n\geq 0} p^n R = \{0\}$ für alle Primelemente $p \in R$ gilt. Sei x ein Element in $\bigcap_{n\geq 0} p^n R$. Für alle $n \geq 0$ existiert ein $x_n \in R$ mit $x = p^n x_n$. Es gilt also $x_n = px_{n+1}$ für alle $n \geq 0$. Wir erhalten eine aufsteigende Kette von Idealen:

$$(x) \subset (x_1) \subset (x_2) \subset ...$$

Da R noethersch ist, existiert ein $n \geq 0$ mit $(x_n) = (x_{n+1})$. Es folgt $(x_n) = (px_n)$, also $x_n = upx_n$ mit $u \in R^\times$. Es gilt also $x_n = 0$ und somit $x = 0$.

□

2.15 Der Satz von Gauß

Satz 2.101 (Satz von Gauß)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K. Der Ring $R[X]$ ist auch faktoriell und die irreduziblen Elemente in $R[X]$ sind:*

(i) Die irreduziblen Elemente $p \in R$.

(ii) Die primitiven Polynome $P \in R[X]$, die irreduzibel in $K[X]$ sind.

Beweis. Wir zeigen zunächst, dass die Elemente der Form (i) und (ii) Primelemente in $R[X]$ sind. Sei $p \in R$ ein irreduzibles Element. Teilt p ein Produkt fg mit $f, g \in R[X] \setminus \{0\}$ so gilt $\bar{f}\bar{g} = 0$ im Ring $(R/(p))[X]$. Der Ring $(R/(p))[X]$ ist ein Integritätsbereich, also es gilt entweder $\bar{f} = 0$ oder $\bar{g} = 0$. Es folgt, dass entweder f oder g durch p teilbar ist.

Sei nun P ein primitives Polynom in $R[X]$, das irreduzibel in $K[X]$ ist. Angenommen P teilt ein Produkt fg mit $f, g \in R[X] \setminus \{0\}$. Dann ist f oder g durch P teilbar im Ring $K[X]$. Wir können ohne Beschränkung annehmen, dass ein $Q \in K[X]$ existiert mit $f = P \cdot Q$. Sei $a \in R \setminus \{0\}$ mit $aQ \in R[X]$, und sei $c := \text{Inhalt}(aQ)$. Dann gilt nach dem Lemma von Gauß

$$\text{Inhalt}(af) = a\,\text{Inhalt}(f) = \text{Inhalt}(P \cdot (aQ)) = c.$$

Es folgt

$$f = \text{Inhalt}(f) P \cdot \frac{aQ}{c}$$

und das Polynom $\frac{aQ}{c}$ hat Koeffizienten in R. Dies zeigt, dass P ein Teiler von f im Ring $R[X]$ ist.

Wir zeigen nun, dass jedes Element in $R[X] \setminus \{0\}$ ein Produkt von Elementen der Form (i) oder (ii) ist. Sei $P \in R[X] \setminus \{0\}$ ein primitives Polynom. Da $K[X]$ faktoriell ist (Beispiel 2.95), existieren irreduzible unitäre Polynome $P_1, ..., P_r \in K[X]$ und $a \in R$

mit $P = aP_1...P_r$. Sei $b \in R \setminus \{0\}$ ein Element, so dass $bP_i \in R[X]$ für alle $i \in \{1, ..., r\}$ gilt. Setze $c_i := \text{Inhalt}(bP_i)$ für alle $i \in \{1, ..., r\}$. Dann gilt nach dem Lemma von Gauß:

$$\text{Inhalt}(b^r P) = b^r = \text{Inhalt}(a(bP_1)...(bP_r)) = ac_1...c_r.$$

Es folgt

$$P = aP_1...P_r = \frac{bP_1}{c_1}...\frac{bP_r}{c_r}.$$

Die Polynome $\frac{bP_i}{c_i}$ für $1 \leq i \leq r$ sind der Form (ii). Es folgt, dass jedes primitives Polynom in $R[X] \setminus \{0\}$ eine Zerlegung in ein Produkt von Elementen der Form (ii) besitzt. Ist dann P ein beliebiges Polynom in $R[X] \setminus \{0\}$, so gilt $P = a\frac{P}{a}$ mit $a := \text{Inhalt}(P)$. Das Polynom $\frac{P}{a}$ ist primitiv, und das Element a ist ein Produkt von irreduziblen Elementen aus R.

Wir haben also bewiesen, dass die Elemente der Form (i) und (ii) Primelemente in $R[X]$ sind, und das jedes Element in $R[X] \setminus \{0\}$ ein Produkt von Elementen der Form (i) oder (ii) ist. Die Behauptung folgt. □

Beispiel 2.102. Das Polynom $2X + 1$ ist irreduzibel in $\mathbb{Z}[X]$ weil es primitiv und irreduzibel in $\mathbb{Q}[X]$ ist. Das Polynom $2X + 4$ ist irreduzibel in $\mathbb{Q}[X]$ aber nicht in $\mathbb{Z}[X]$, denn es gilt $2X + 4 = 2(X + 2)$.

Korollar 2.103. *Sei R ein faktorieller Ring mit Quotientenkörper K, und sei $P \in R[X]$ ein Polynom mit* $\text{Inhalt}(P) = 1$. *Ist $Q \in K[X]$ ein Polynom mit $PQ \in R[X]$, so gilt $Q \in R[X]$.*

Beweis. Setze $R := PQ$ und sei $a \in R \setminus \{0\}$ mit $aQ \in R[X]$. Es gilt:

$$\text{Inhalt}(aR) = a\,\text{Inhalt}(R) = \text{Inhalt}(P)\,\text{Inhalt}(aQ) = \text{Inhalt}(aQ).$$

Es folgt, dass a ein Teiler der Koeffizienten von aQ ist, also $\frac{aQ}{a} = Q \in R[X]$. □

2.16 Ein Gegenbeispiel

Wir konstruieren nun ein Beispiel für einen Hauptidealring, der kein euklidischer Ring ist. Sei

$$\alpha := \frac{1 + i\sqrt{19}}{2}.$$

Man sieht sofort, dass die folgende Gleichung gilt:

$$\alpha^2 - \alpha + 5 = 0.$$

Sei R die Menge der komplexen Zahlen

$$R := \{a + b\alpha,\ a, b \in \mathbb{Z}\}.$$

Sind $a + b\alpha$ und $a' + b'\alpha$ zwei Elemente aus R, so gilt

$$\begin{aligned}(a + b\alpha)(a' + b'\alpha)6 &= aa' + bb'\alpha^2 + (ab' + a'b)\alpha \\ &= aa' - 5bb' + (ab' + a'b + bb')\alpha\end{aligned}$$

und es folgt, dass R ein Unterring von $\mathbb{C}$ ist. Der Ring R ist stabil unter komplexer Konjugation $z \mapsto \bar{z}$, denn es gilt $\bar{\alpha} = 1 - \alpha$. Wir definieren die Norm von $z \in R$ als die Zahl

$$N(z) := z\bar{z}.$$

Ist $z = a + b\alpha$ mit $a, b \in \mathbb{Z}$, so gilt:

$$N(z) = (a + b\alpha)(a + b(1 - \alpha)) = a^2 + ab + 5b^2.$$

Insbesondere gilt $N(z) \in \mathbb{N}$.

Lemma 2.104. *Der Quotientenkörper von R ist*

$$\mathbb{Q}(\alpha) := \{a + b\alpha,\ a, b \in \mathbb{Q}\}.$$

Beweis. Die Menge $\mathbb{Q}(\alpha)$ ist ein Unterring von $\mathbb{C}$ (der Beweis ist analog zum Beweis für R). Für $z = a + b\alpha$, $a, b \in \mathbb{Q}$ gilt

$$\frac{1}{z} = \frac{\bar{z}}{N(z)} = \frac{a + b - b\alpha}{a^2 + ab + 5b^2}$$

also $\frac{1}{z} \in \mathbb{Q}(\alpha)$. Außerdem ist jedes Element in $\mathbb{Q}(\alpha)$ ein Quotient zweier Elemente aus R. Die Behauptung folgt. □

Lemma 2.105. *Der Homomorphismus $f : \mathbb{Z}[X] \longrightarrow R$, $P \mapsto P(\alpha)$ ist surjektiv und es gilt* $\mathrm{Kern}(P) = (X^2 - X + 5)$. *Insbesondere induziert f einen Isomorphismus:*

$$\frac{\mathbb{Z}[X]}{(X^2 - X + 5)} \longrightarrow R.$$

Beweis. De Homomorphismus f ist natürlich surjektiv, und das Polynom $X^2 - X + 5$ ist ein Element in $\mathrm{Kern}(f)$. Das Polynom $X^2 - X + 5$ ist irreduzibel in $\mathbb{Q}[X]$. Ist $P \in \mathrm{Kern}(f)$, so existiert also $Q \in \mathbb{Q}[X]$ mit $P = (X^2 - X + 5)Q$. Aus Korollar 2.103 folgt $Q \in \mathbb{Z}[X]$, und damit $P \in (X^2 - X + 5)\mathbb{Z}[X]$ wie behauptet. □

Lemma 2.106. *Ein Element $z \in R$ ist genau dann invertierbar, wenn $N(z) = 1$ gilt. Es folgt:*

$$R^\times = \{-1, 1\}.$$

Beweis. Der Beweis ist derselbe wie in Lemma 2.71. □

Proposition 2.107. *Der Ring R ist kein euklidischer Ring ist.*

Wir werden folgendes Lemma benutzen:

Lemma 2.108. *Sei A ein euklidischer Ring und sei $A^\times$ die Menge der invertierbaren Elemente in R. Dann existiert ein $x \in A \setminus A^\times$ so dass die Abbildung*

$$A^\times \cup \{0\} \longrightarrow \frac{A}{(x)}, \quad a \mapsto a + (x)$$

surjektiv ist.

Beweis. Sei $g : A \setminus \{0\} \to \mathbb{N}$ eine Gradfunktion, und sei $x \in A \setminus (A^\times \cup \{0\})$ ein Element mit

$$g(x) = \min\{g(y),\ y \in A \setminus (A^\times \cup \{0\})\}.$$

Für jedes Element $y \in A$ existieren $q, r \in A$ mit $y = qx + r$ mit entweder $r = 0$ oder $g(r) < g(x)$. Gilt $r \neq 0$ und $g(r) < g(x)$ so folgt aus der Definition von x, dass r kein Element in $A \setminus A^\times$ ist, also $r \in A^\times$. Jedes Element $y \in A$ ist also kongruent modulo das Ideal (x) zu einem Element aus $A^\times \cup \{0\}$. Die Behauptung folgt. □

Die Menge $R^\times \cup \{0\}$ hat nur drei Elemente (Lemma 2.106). Es reicht also zu zeigen, dass kein Element $x \in R \setminus R^\times$ existiert, so dass $\frac{R}{(x)}$ höchstens drei Elemente hat. Sei $x \in R \setminus R^\times$ ein Element und sei β das Bild von α unter dem Homomorphismus $R \to \frac{R}{(x)} =: R'$. Dann gilt natürlich auch die Gleichung $\beta^2 - \beta + 5 = 0$ im Ring R'.

Lemma 2.109. *Ist A ein Ring mit $|A| = 2$, so gilt $A \simeq \mathbb{F}_2$. Ist A ein Ring mit $|A| = 3$, so gilt $A \simeq \mathbb{F}_3$.*

Beweis. In beiden Fällen ist der natürliche Homomorphimus $\mathbb{Z} \to A$ surjektiv, also R ist ein Faktorring von $\mathbb{Z}$. □

Aber man sieht sofort, dass das Polynom $X^2 - X + 5$ weder in $\mathbb{F}_2$ noch in $\mathbb{F}_3$ eine Nullstelle hat. Der Ring R' ist also isomorph weder zu $\mathbb{F}_2$ oder zu $\mathbb{F}_3$. Es folgt aus dem Lemma, dass R' mindestens 4 Elemente hat. Nach Lemma 2.108 ist R kein euklidischer Ring.

Wir zeigen nun, dass R ein Hauptidealring ist. Wir brauchen eine schwache Version der Division mit Rest:

Lemma 2.110. *Seien $x, y \in R \setminus \{0\}$ zwei Elemente. Dan existieren $q, r \in R$ mit*

1. *$a = bq + r$ oder $2a = bq + r$.*
2. *$N(r) < N(b)$.*

Beweis. Setze $x := \frac{a}{b} \in \mathbb{Q}(\alpha)$ und schreibe $x = u + v\alpha$ mit $u, v \in \mathbb{Q}(\alpha)$. Sei $n = \lfloor v \rfloor$ die nächstkleinere Ganzzahl.

Erster Fall: $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$
Dann existieren $s, t \in \mathbb{Z}$ mit $|s - u| \leq \frac{1}{2}$ und $|t - v| \leq \frac{1}{3}$. Setze $q = r + s\alpha$. Dann gilt:

$$\begin{aligned} N(x - q) &= N(u - s + \alpha(v - t)) \\ &= (u - s)^2 + (u - s)(v - t) + 5(v - t)^2 \\ &\leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} \\ &= \frac{35}{36} \end{aligned}$$

Sei $r := a - bq \in R$. Dann gilt $N(r) = N(x - q)N(b) < N(b)$.

Zweiter Fall:$v \in]n+\frac{1}{3}, n+\frac{2}{3}[$
Ersetzen wir a durch $2a$. Es gilt $\frac{2a}{b} = 2x = 2u + 2v\alpha$ und $2v \in]2n+\frac{2}{3}, 2n+1+\frac{1}{3}[$. Die rationale Zahl $2v$ erfüllt also die Bedingung des ersten obigen Falls. Es folgt dass $q, r \in R$ existieren mit $2a = bq + r$ mit $N(r) < N(b)$. □

Proposition 2.111. *Der ring R ist ein Hauptidealring.*

Beweis. Sei $I \subset R$ ein Ideal mit $I \neq \{0\}$ und sei $b \in I \setminus \{0\}$ ein Element mit $N(b)$ minimal. Wir werden zeigen, dass $I = (b)$ gilt. Sei $a \in I \setminus \{0\}$ ein beliebiges Element. Es existiert $q, r \in R$ mit $N(r) < N(b)$ und entweder $a = bq + r$ oder $2a = bq + r$. In beiden Fällen ist r ein Element in I mit $N(r) < N(b)$. Es folgt $r = 0$ aus der Minimalität von $N(b)$. Gilt $a = bq$ so ist also a ein Element im Ideal (b). Ansonsten gilt $2a = bq$.

Lemma 2.112. *Das Ideal (2) in R ist ein maximales Ideal*

Beweis. Es folgt aus Lemma 2.105:

$$\frac{R}{(2)} \simeq \frac{\mathbb{Z}[X]}{(2, X^2 - X + 5)} \simeq \frac{\mathbb{F}_2[X]}{(X^2 - X + 5)}.$$

Das Polynom $X^2 - X + 5$ ist irreduzibel über $\mathbb{F}_2$ weil es Grad 2 hat und weil es keine Nullstelle in $\mathbb{F}_2$ hat. Der Faktorring $\frac{\mathbb{F}_2[X]}{(X^2-X+5)}$ ist also ein Körper. □

Wenn $q \notin (2)$, so folgt aus Lemma 2.112: $(2, q) = R$. Es existieren also Elemente $s, t \in R$ mit $2s + qt = 1$. Es folgt: $b = 2sb + bqt = 2sb + 2at = 2b'$ mit $b' = sb + at$. Das Element b' ist in $I \setminus \{0\}$ und es gilt $N(b') < N(b)$ im Widerspruch zur Minimalität von $N(b)$. Es folgt also $q \in (2)$, $q = 2q'$ mit $q' \in R$. Dann gilt $a = bq' \in (b)$. Wir haben bewiesen, dass das Ideal I von b erzeugt wird. Der Ring R ist ein Hauptidealring. □

2.17 Diskreter Bewertungsring

Ein *lokaler Ring* ist ein kommutativer Ring, der nur ein einziges maximales Ideal besitzt. Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Nach dem Satz 2.64 ist jedes Ideal $I \subsetneq R$ in $\mathfrak{m}$ enthalten. Insbesondere gilt $(x) = R$ für alle $x \in R \setminus \mathfrak{m}$, also x ist invertierbar.

Proposition 2.113. *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Die Menge der invertierbaren Elemente von R ist $R \setminus \mathfrak{m}$.*

Definition 2.114. Ein lokaler Hauptidealring heißt *diskreter Bewertungsring.*

Ein Erzeuger des maximalen Ideals heißt *uniformisierendes Element* oder kurz *Uniformisierendes.* Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$ und sei $\pi \in \mathfrak{m}$ ein Uniformisierendes. Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$ und sei $\pi \in \mathfrak{m}$ ein Uniformisierendes. Jedes irreduzibles Element π' erzeugt ein maximales Ideal (Proposition 2.75), also es gilt $(\pi') = \mathfrak{m} = (\pi)$. Es folgt, dass die Elemente π und π' sind assoziiert. Die einelementige Menge $\{\pi\}$ ist also ein Repräsentantensystem der irreduziblen Elemente von R. Sei K der Quotientenkörper von R. Jedes Element $x \in K \setminus \{0\}$ besitzt eine eindeutige Zerlegung

$$x = u\pi^k$$

mit $u \in R \setminus \mathfrak{m}$ invertierbar und $k = \nu_\pi(x)) \in \mathbb{Z}$ eine ganze Zahl (siehe Satz 2.88 und (2.17)). Wir schreiben kurz $\nu(x)$ für $\nu_\pi(x)$. Die Abbildung $\nu : K \setminus \{0\} \to \mathbb{Z}$ erfüllt die folgenden Eigenschaften:

(i) Die Abbildung ν ist surjektiv.

(ii) Es gilt $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ für alle $x, y \in K \setminus \{0\}$ mit $x + y \in K \setminus \{0\}$.

(iii) Es gilt $\nu(xy) = \nu(x) + \nu(y)$ für alle $x, y \in K \setminus \{0\}$.

Ist K ein Körper und $\nu : K \setminus \{0\} \to \mathbb{Z}$ eine Abbildung die die Eigenschaften (i), (ii) und (iii) erfüllt, so sagt man dass ν eine diskrete Bewertung auf K ist.

Proposition 2.115. *Sei K ein Körper und sei $\nu : K \setminus \{0\} \to \mathbb{Z}$ eine diskrete Bewertung. Definiere*

$$R := \{x \in K \setminus \{0\}, \nu(x) \geq 0\} \cup \{0\}$$

$$\mathfrak{m} := \{x \in K \setminus \{0\}, \nu(x) > 0\} \cup \{0\}.$$

Die Menge R ist ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$ und Quotientenkörper K. Die Uniformisierenden sind die Elemente $x \in K \setminus \{0\}$ mit $\nu(x) = 1$. Die invertierbaren Elemente von R sind die Elemente x mit $\nu(x) = 0$.

Beweis. Man sieht sofort, dass R ein Unterring von K ist, und dass $\mathfrak{m}$ ein Ideal von R ist. Sei $x \in R$ ein invertierbares Element in R. Dann existiert $y \in R$ mit $xy = 1$ es folgt $\nu(x) + \nu(y) = \nu(1) = 0$ (denn ν ist ein Homomorphismus von Gruppen $(K \setminus \{0\}, \times) \to (\mathbb{Z}, +)$). Es folgt $\nu(x) = 0$. Umgekehrt, sei $x \in R \setminus \{0\}$ ein Element mit $\nu(x) = 0$. Dann gilt $\nu(x^{-1}) = -\nu(x) = 0$, und es folgt $x^{-1} \in R$, also x ist invertierbar in R.

Jedes Ideal $I \subsetneq R$ muss also in $\mathfrak{m}$ enthalten sein. Es folgt, dass R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ ist. Es bleibt zu zeigen, dass R ein Hauptidealring ist. Sei $I \subset R$ ein Ideal mit $I \neq 0$. Definiere die Zahl:

$$k := \min\{\nu(x),\ x \in I \setminus \{0\}\}.$$

Sei $x \in I$ ein Element mit $\nu(x) = k$. Wir zeigen, dass I von x erzeugt wird. Sei $y \in I$ ein Element mit $y \neq 0$ und setze $z := yx^{-1}$. Es gilt $\nu(z) = \nu(y) - \nu(x) \geq 0$, also z ist ein Element in R. Aus der Gleichung $y = xz$ folgt, dass $y \in (x)$. Dies zeigt, dass $I = (x)$. Der Ring R ist also ein diskreter Bewertungsring.

Es existiert ein Element $\pi \in \mathfrak{m}$ mit $\nu(\pi) = 1$ (weil ν surjektiv ist). Wir haben gezeigt, dass $\mathfrak{m}$ von π erzeugt wird. Es ist also ein Uniformisierendes. □

Sei K ein Körper. Für eine Potenzreihe $f = \sum_{i=0}^{\infty} a_i X^i \in K[[X]]$ definieren wir:

$$\nu(f) := \min\{i \geq 0,\ a_i \neq 0\}. \tag{2.18}$$

Die invertierbaren Elemente von $K[[X]]$ sind also die Elemente f mit $\nu(f) = 0$ (Proposition 2.48). Für $f \in K[[X]]$ existiert also eine (eindeutige) invertierbare Potenzreihe

$g \in K[[X]]$ mit $f = X^{\nu(f)}g$. Der Quotientenkörper von $K[[X]]$ wird mit $K((X))$ bezeichnet. Ein Element in $K((X))$ ist der Form $\frac{a}{b}$ mit $a, b \in K[[X]]$ und $b \neq 0$. Schreiben wir $a = X^{\nu}(a)a'$ und $b = X^{\nu}(b)b'$ mit a', b' invertierbar. Dann gilt:

$$\frac{a}{b} = \frac{a'}{b'} X^{\nu(a)-\nu(b)}.$$

Für jedes Element $y \in K((X)) \setminus \{0\}$ existiert also eine eindeutige ganze Zahl $\nu(y) \in \mathbb{Z}$ und ein eindeutiges invertierbares Element $f \in R[[X]]$ mit $y = X^{\nu}(y)f$. Die Abbildung $\nu : K \setminus \{0\} \to \mathbb{Z}$ ist eine Erweiterung von der Abbildung (2.18). Man sieht einfach, dass ν eine diskrete Bewertung ist.

Satz 2.116. *Sei K ein Körper. Der Ring $K[[X]]$ ist ein diskreter Bewertungsring. Das Element X ist ein Uniformisierendes.*

3 Körper

3.1 Die Charakteristik eines Körpers

Sei R ein kommutativer Ring. Der Kern des natürlichen Homomorphismus $\varphi_R : \mathbb{Z} \to R$, $k \mapsto k \cdot 1_R$ ist der Form $n\mathbb{Z}$ mit einem eindeutigen $n \in \mathbb{N}$.

Lemma 3.1. *Ist R ein Integritätsbereich, so gilt entweder* $\mathrm{Kern}(\varphi_R) = p\mathbb{Z}$ *mit einer Primzahl $p \in \mathbb{N}$ oder* $\mathrm{Kern}(\varphi_R) = \{0\}$.

Beweis. Ist R ein Integritätsbereich, so ist das Nullideal prim. Das Urbild eines Primideals durch einen Homomorphismen von Ringen ist prim (Proposition 2.63). □

Die Zahl $n \in \mathbb{N}$ mit $\mathrm{Kern}(\varphi_R) = n\mathbb{Z}$ heißt die Charakteristik des Rings R. Die Charakteristik eines Integritätsbereichs (insbesondere eines Körpers) ist entweder eine Primzahl oder 0. Sie wird mit $\mathrm{char}(R)$ bezeichnet.

Definition 3.2. Sei K ein Körper. Ein Teilkörper von K ist ein Unterring $L \subset K$, der ein Körper ist.

Beispiel 3.3. $\mathbb{R}$ ist ein Teilkörper von $\mathbb{C}$.

Ist $S \subset K$ eine Teilmenge eines Körpers K, so existiert ein kleinster Teilkörper von K, der S enthält. Der Beweis ist derselbe wie für Gruppen : Man zeigt zunächst dass ein Durchschnitt einer Famile von Teilkörpern von K ein Teilkörper ist. Dann betrachtet man die Familie der Teilkörper von K, die S enthalten. Der Durchschnitt ist der gesuchte Teilkörper. Er heißt der von S erzeugte Teilkörper.

Insbesondere existiert in K ein kleinster Teilkörper (wähle $S = \emptyset$). Er heißt der *Primkörper* von K.

Charakteristik Null Sei K ein Körper mit $\mathrm{char}(K) = 0$. Dann ist $\varphi_K : \mathbb{Z} \to K$ ein injektiver Homomorphismus von Ringen. Dann ist das Bild $\mathrm{Bild}(\varphi_K)$ ein Unterring von K, der isomorph zu $\mathbb{Z}$ ist. Der Primkörper ist der Quotientenkörper von $\mathrm{Bild}(\varphi_K)$, und ist isomorph zu $\mathbb{Q}$.

Charakteristik $p > 1$ Sei K ein Körper von Charakteristik $p > 1$. Wir erhalten einen injektiven Homomorphismus von Ringen

$$\mathbb{Z}/p\mathbb{Z} \to K.$$

Da p eine Primzahl ist, ist der Ring $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Der Primkörper ist also isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Man schreibt auch oft $\mathbb{F}_p$ für den Körper $\mathbb{Z}/p\mathbb{Z}$.

Lemma 3.4. *Sei p eine Primzahl und sei $1 \leq i \leq p-1$ eine natürliche Zahl. Dann ist $\binom{p}{i}$ durch p teilbar.*

Beweis. Sei $k = \binom{p}{i}$. Es gilt $ki! = p!$, und p ist zu $i!$ teilerfremd. Es folgt, dass k durch p teilbar ist. □

Proposition 3.5. *Sei K ein Körper von Charakteristik $p > 1$. Die Abbildung:*

$$\mathrm{Fr}_p : K \longrightarrow K, \quad x \mapsto x^p$$

ist ein Homomorphismus von Körpern. Er heißt der Frobeniushomomorphismus.

Beweis. Seien $x, y \in K$. Es gilt:

$$\begin{aligned}(x+y)^p &= \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} \\ &= x^p + y^p.\end{aligned}$$

nach Lemma 3.4. □

Es folgt auch aus dieser Proposition, dass die Abbildung $\mathrm{Fr}_p^n : K \to K$, $x \mapsto x^{p^n}$ ein Homomorphismus von Körpern ist.

3.2 Körpererweiterungen

Ist $K \subset L$ ein Teilkörper von L, so heißt die Inklusion $K \subset L$ eine Körpererweiterung von K. Der Körper L heißt ein *Erweiterungskörper* von K. Die Multiplikation $L \times L \to L$ induziert durch Einschränkung eine Abbildung $K \times L \to L$, die eine Struktur eines K-Vektorraums auf L definiert.

Definition 3.6. Eine Körpererweiterung $K \subset L$ heißt endlich, falls L ein endlichdimensionaler K-Vektroraum ist. Die Dimension $\dim_K(L)$ heißt *der Grad* der Körpererweiterung und wird mit $[L : K]$ bezeichnet. Man definiert auch $[L : K] = +\infty$ für eine unendliche Körpererweiterung $K \subset L$.

Satz 3.7. *Sind $K \subset L \subset M$ Körpererweiterungen, so gilt die Gleichung*

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

Beweis. Ist entweder $[M : L] = +\infty$ oder $[L : K] = +\infty$ so gilt natürlich auch $[M : K] = +\infty$. Wir können also annehmen, dass $[M : L]$ und $[L : K]$ endlich sind. Sei $(x_1, ..., x_n)$ eine Basis von M als L-Vektorraum und sei $(y_1, ..., y_m)$ eine Basis von L als K-Vektorraum. Wir werden zeigen, dass die Familie $(x_i y_j)$ für $1 \leq i \leq n$ und $1 \leq j \leq m$ eine Basis von M als K-Vektorraum ist. Jedes Element in M ist ein Linearkombination der x_i mit Koeffizienten in L. Jeden Koeffizienten kann man als eine Linearkombination der y_j mit Koeffizienten in K ausdrücken. Wir erhalten also eine Linearkombination der $x_i y_j$ mit Koeffizienten in K. Die $x_i y_j$ bilden also ein Erzeugendensystem von M als K-Vektorraum. Seien nun $a_{i,j} \in K$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$ Elemente mit

$$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} a_{i,j} x_i y_j = 0.$$

Es folgt: Für alle $1 \leq i \leq n$ gilt

$$\sum_{j=1}^{m} a_{i,j} y_j = 0$$

und wir folgern: $a_{i,j} = 0$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$. Der K-Vektorraum M ist also endlichdimensional von Dimension nm. □

Ist $K \subset L$ eine Körpererweiterung und $S \subset L$ eine Teilmenge, so definiert man $K(S)$ als den Teilkörper von L, der von $K \subset S$ erzeugt wird. Wenn $S = \{x_1, ..., x_n\}$ endlich ist schreibt man $K(x_1, ..., x_n)$ statt $K(\{x_1, ..., x_n\})$. Eine Körpererweiterung $K \subset L$ heißt *endlich erzeugt*, falls Elemente $x_1, ..., x_n$ in L existieren mit $L = K(x_1, ..., x_n)$. Man sieht sofort, dass die Gleichung

$$K(x_1, ..., x_n) = K(x_1)(x_2)...(x_n)$$

gilt.

Beispiel 3.8. Jedes Element in $\mathbb{C}$ ist der Form $a + bi$, $a, b \in \mathbb{R}$. Es gilt also $\mathbb{C} = \mathbb{R}(i)$.

3.3 Algebraische Elemente

Definition 3.9. Sei $K \subset L$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt algebraisch über K falls ein Polynom $P \neq 0$ existiert mit $P(\alpha) = 0$. Die Erweiterung $K \subset L$ heißt algebraisch, falls jedes Element in L algebraisch über K ist. Ein Element in L, das nicht algebraisch über K ist, heißt *transzendent*.

Beispiel 3.10.

(a) Das Element $\alpha = \sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$, denn es gilt $P(\alpha) = 0$ mit $P = X^3 - 2$.

(b) Sei K ein Körper und sei $L = K(X)$ der Quotientenkörper von $K[X]$. Das Element X ist transzendent über K.

Proposition 3.11. *Sei $K \subset L$ eine Körpererweiterung. Ist $\alpha \in L$ algebraisch über K, so existiert ein eindeutiges normiertes Polynom kleinsten Grades P mit $P(\alpha) = 0$. Der Körper $K(\alpha)$ ist das Bild des Homomorphismus von Ringen:*

$$f : K[X] \longrightarrow L, \quad Q \mapsto Q(\alpha).$$

Der Kern von f ist das von P erzeugte Ideal. Das Polynom P ist irreduzibel und der Grad von P ist der Grad der Körpererweiterung $K \subset K(\alpha)$. Es gilt also $\mathrm{Grad}(P) = [K(\alpha) : K]$. *Insbesondere induziert f einen Isomorphismus*

$$\frac{K[X]}{(P)} \longrightarrow K(\alpha).$$

Beweis. Da a algebraisch ist, ist der Homomorphismus von Ringen

$$f : K[X] \longrightarrow L, \quad Q \mapsto Q(\alpha)$$

nicht injektiv. Der Kern von f ist ein Primideal von $K[X]$, also es gilt $\mathrm{Kern}(f) = (P)$ für ein irreduzibles Polynom P von Grad ≥ 1. Außerdem ist P eindeutig bis auf eine multiplikative Konstante in $K^\times$. Dies zeigt das erste Teil der Behauptung. Der Faktorring $\frac{K[X]}{(P)}$ ist ein Körper, und wir erhalten einen injektiven Homomorphismus

$$\tilde{f} : \frac{K[X]}{(P)} \to L.$$

Sein Bild ist also ein Teilkörper von L, der K und α enthält. Per Definition enthält er dann auch den Teilkörper $K(\alpha)$. Aber für alle $Q \in K[X]$ gilt $Q(\alpha) \in K(\alpha)$, also es folgt $\mathrm{Bild}(\tilde{f}) = K(\alpha)$ und $\tilde{f}$ induziert einen Isomorphismus $\frac{K[X]}{(P)} \simeq K(\alpha)$. Setze $P = X^n + a_{n-1}X^{n-1} + ... + a_0$. Man sieht sofort, dass die Klassen von $1, X, ..., X^{n-1}$ in $\frac{K[X]}{(P)}$ eine Basis von $\frac{K[X]}{(P)}$ als K-Vektorraum bilden. Es folgt $n = [K(\alpha) : K]$. □

Definition 3.12. Das Polynom P im Satz 3.11 heißt das Minimalpolynom von α über K.

Bemerkung 3.13. (i) Ist $\alpha \in L$ algebraisch mit Minimalpolynom P, so gilt für jedes Polynom $Q \in K[X]$

$$Q(\alpha) = 0 \Longleftrightarrow P|Q.$$

(ii) Ist $\alpha \in L$ algebraisch und gilt $[K(\alpha) : K] = n$, so bilden die Elemente $(1, \alpha, ..., \alpha^{n-1})$ eine Basis von $K(\alpha)$ als K-Vektorraum.

Lemma 3.14. *Sei $K \subset L$ eine Körpererweiterung. Für jedes Element $a \in L$ sind die folgenden Aussagen äquivalent:*

(i) Das Element α ist algebraisch über K.

(ii) Die Körpererweiterung $K \subset K(\alpha)$ ist endlich.

Beweis. Wir haben schon $(i) \implies (i))$ bewiesen. Angenommen $[K(\alpha) : K] = n$ ist endlich, so ist die Elemente $(1, \alpha, \alpha^2, ...)$ linear abhängig über K. Es existiert also $n \geq 1$ und Elemente $a_0, ..., a_n$ in K nicht alle Null, mit $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$. Das Element α ist also algebraisch über K. □

Satz 3.15. *Sei $K \subset L$ eine Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

(i) Die Erweiterung $K \subset L$ ist endlich.

(ii) Die Erweiterung $K \subset L$ ist algebraisch und endlich erzeugt.

(iii) Es existiert Elemente $x_1, ..., x_n \in L$ algebraisch über K mit $L = K(x_1, ..., x_n)$.

Beweis. Ist die Erweiterung $K \subset L$ endlich, so ist die Erweiterung $K \subset K(\alpha)$ auch endlich für alle $\alpha \in L$. Nach Lemma 3.14 ist jedes Element in L algebraisch über K. Es gilt also $(i) \Rightarrow (ii)$. Die Implikation $(ii) \Rightarrow (iii)$ ist offensichtlich.

Angenommen es existiert Elemente $x_1, ..., x_n \in L$ algebraisch über K mit $L = K(x_1, ..., x_n)$. Betrachte die Folge von Körpererweiterungen

$$K \subset K(x_1) \subset ... \subset K(x_1, ..., x_n).$$

Für alle $1 \leq i \leq n$ ist x_i algebraisch auf K, insbesondere auf $K(x_1, ..., x_{i-1})$. Nach Lemma 3.14 folgt es, dass jede Stufe in dieser Folge eine endliche Erweiterung ist. Nach Satz 3.7 ist die Erweiterung $K \subset L$ auch endlich. □

Satz 3.16. *Sei $K \subset L$ eine Körpererweiterung. Die Menge der Elemente in L, die algebraisch über K sind bilden einen Teilkörper von L.*

Beweis. Seien $\alpha, \beta \in L$ algebraisch über K. Dann gilt $K(\alpha - \beta) \subset K(\alpha, \beta)$ und $K(\alpha\beta) \subset K(\alpha, \beta)$. Es folgt nach Satz 3.15 und Lemma 3.14, dass $\alpha - \beta$ und $\alpha\beta$ algebraisch über K sind. Für $\beta \in L \setminus \{0\}$ algebraisch über K gilt $K(\beta) = K(\beta^{-1})$, also β^{-1} ist algebraisch über K. Die Behauptung folgt. □

Sei $P \in K[X]$ ein Polynom. Man sagt, dass P über K zerfällt, wenn Elemente $a_1, ..., a_n$ in K und ein $b \in K^\times$ existieren mit

$$P = b(X - a_1)...(X - a_n).$$

Die Elemente $a_1, ..., a_n$ sind genau die Nullstellen von P und b ist der Leitkoeffizient.

Satz 3.17. *Sei K ein Körper und $P \in K[X]$ ein Polynom. Dann existiert ein Erweiterungskörper L von K, so dass P über L zerfällt.*

Beweis. Wir zeigen zunächst, dass ein erweiterungskörper L_1 existiert, wo P eine Nullstelle hat. Sei Q ein irreduziler Primfaktor von P. Dann ist $\frac{K[X]}{(Q)}$ ein Erweiterungskörper von K. Sei $x \in L_1$ die Klasse von $X \in K[X]$. Es gilt $Q(x) = 0$ in L_1, also Q, und damit P, hat eine Nullstelle in L_1.

Es existiert also ein Polynom $Q_1 \in L_1[X]$ mit $Q = (X - x)Q_1$. Der Grad von Q_1 ist kleiner als der Grad von Q. Nach der Induktionsvoraussetzung zerfällt Q_1 in einem Erweiterungskörper L von L_1. Dann zerfällt auch P in L, und die Behauptung folgt. □

Eine Körpererweiterung $K \subset L$ heißt *primitiv*, falls es ein Element $\alpha \in L$ gibt mit $L = K(\alpha)$. Das Element α heißt *primitives Element* von L über K. Ist α in primitives Element mit Minimalpolynom $P \in K[X]$, so erhalten wir einen Isomorphismus:

$$\frac{K[X]}{(P)} \longrightarrow L, \quad Q \mapsto Q(\alpha).$$

3.4 Algebraisch abgeschlossener Körper

Definition 3.18. Ein Körper heißt algebraisch abgeschlossen, falls jedes Polynom $P \in K[X]$ mit $\text{Grad}(P) \geq 1$ eine Nullstelle in K besitzt.

Lemma 3.19. *Sei K ein algebraisch abgeschlossener Körper. Für jedes Polynom $P \in K[X]$ von Grad $n \geq 0$ existieren bis auf Reihenfolge eindeutige Elemente $a_1, ..., a_n$ und ein eindeutiges Element $b \in K^\times$ mit*

$$P = b(X - a_1)...(X - a_n).$$

Die Elemente $a_1, ..., a_n$ sind genau die Nullstellen von P. Man sagt, dass das Polynom P über K zerfällt.

Beweis. Ohne Beschränkung gilt $\text{Grad}(P) \geq 1$. Sei $a \in K$ eine Nullstelle von P. Es ist $P = (X - a)Q$ für ein $Q \in K[X]$. Die Behauptung folgt dann per Induktion nach dem Grad. □

Lemma 3.20. *Ein Körper K ist genau dann algebraisch abgeschlossen, wenn er keine echten algebraischen Körpererweiterungen $K \subset L$ zulässt.*

Beweis. Sei K algebraisch abegeschlossen und $K \subset L$ eine algebraische Körpererweiterung. Sei $\alpha \in L$ ein Element und sei P das Minimalpoynom von α über K. Das Polynom P zerfällt in K und ist irreduzibel, also $P = X - x$ für ein $x \in K$. Es folgt $\alpha = x \in K$, also $L = K$.

Umgekehrt, nehmen wir an, dass K keine echten algebraischen Körpererweiterungen besitzt und sei $Q \in K[X]$ mit $\text{Grad}(Q) \geq 1$. Sei $P \in K[X]$ ein Primfaktor von Q und setze $\text{Grad}(P) = n$. Dann ist $\frac{K[X]}{(P)}$ eine endlich Körpererweiterung von K von Grad n. Es gilt also $n = 1$. Es folgt, dass P (also auch Q) eine Nullstelle in K hat. □

Lemma 3.21. *Sei $K \subset K(\alpha)$ eine primitive Körpererweiterung. Sei L ein algebraisch abgeschlossener Körper und $\sigma : K \to L$ ein Homomorphismus von Körpern. Dann existiert ein Homomorphismus von Körpern $f : K(\alpha) \to L$ mit $f|_K = \sigma$.*

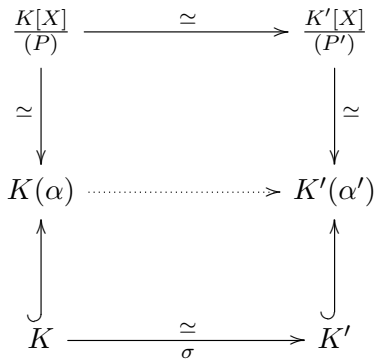
Beweis. Definiere $K' = \sigma(K)$, es ist ein Teilkörper von L. Sei $P = \sum_{i=0}^{n} a_i X^i$ das Minimalpolynom von α über K und sei

$$P' := \sum_{i=0}^{n} \sigma(a_i) X^i \in L[X].$$

Der Homomorphismus σ induziert einen Isomorphismus:

$$\frac{K[X]}{(P)} \longrightarrow \frac{K'[X]}{(P')}.$$

Sei α' eine Nullstelle von P' in L. Wir haben also zwei Isomorphismen $\frac{K'[X]}{(P')} \to K'(\alpha')$ und $\frac{K[X]}{(P)} \to K(\alpha)$ (Satz 3.11). Wir erhalten also ein kommutatives Diagramm:



Der induzierte Isomorphismus $f : K(\alpha) \to K'(\alpha')$ ist der gesuchte Homomorphismus von Körpern. □

Proposition 3.22. *Sei $K \subset L$ eine algebraische Körpererweiterungen. Sei $\sigma : K \to M$ ein Homomorphismus von Körpern, mit M algebraisch abgeschlossen. Dann existiert ein Homomorphismus von Körpern $f : L \to M$ mit $f|_K = \sigma$.*

Beweis. Sei X die Menge der Paare (F, f) wobei $K \subset F \subset L$ eine Körpererweiterung ist, und $f : F \to M$ ein Homomorphismus von Körpern mit $f|_K = \sigma$. Die Menge X ist nicht leer, weil das Paar (K, σ) ein Element in X ist. Wir definieren eine Ordnung auf X durch:

$$(F_1, f_1) \leq (F_2, f_2) \Longleftrightarrow F_1 \subset F_2 \text{ und } f_1 = f_2|_{F_1}.$$

Man sieht sofort, dass dies eine partielle Ordnung auf X definiert. Ist $Y \subset X$ eine total geordnete Teilmenge, so besitzt Y eine obere Schranke (F_0, f_0) in X. Der Körper F_0 ist die Vereinigung aller Körper F so dass $(F, f) \in Y$ für ein f. Die Mange F ist ein Teilkörper von L (der Beweis ist analog zu dem in Satz 2.64). Der Homomorphismus $f_0 : F \to M$ ist definiert durch:

$$f_0(x) = f(x)$$

für ein Element $(F, f) \in Y$ mit $x \in F$. Da Y total geordnet ist ist diese Definition sinnvoll. Es folgt aus dem Lemma von Zorn (Lemma 2.66), das ein maximales Element (F, f) in X existiert. Es reicht zu zeigen, dass $F = L$ gilt. Nehmen wir an, dass F ein echter Teilkörper von L ist, d.h. dass $F \neq L$ gilt. Sei $\alpha \in L \setminus F$ ein Element. Nach Lemma 3.21 existiert ein Homomorphismus $g : F(\alpha) \to M$ mit $g|_F = f$. Es folgt also

$$(F, f) \leq (F(\alpha), g)$$

und $F \neq F(\alpha)$, im Widerspruch zur Maximalität von (F, f). Es gilt also $F = L$, und die Behauptung folgt. □

Satz 3.23. *Zu jedem Körper K existiert ein algebraisch abgeschlossener Erweiterungskörper.*

Beweis. Sei $I := \{f \in K[X],\ \mathrm{Grad}(f) \geq 1$. Für jedes Polynom $f \in I$, sei X_f eine Unbestimmte. Sei $R := K[(X_f)_{f\in I}]$ der Polynomring in der Unbestimmten X_f, $f \in I$.

Lemma 3.24. *Sei*

$$\mathfrak{a} = \langle f(X_f),\ f \in I\rangle$$

das von den $f(X_f)$ erzeugte Ideal in R. Es gilt $\mathfrak{a} \subsetneq R$, d.h. $\mathfrak{a}$ ist ein echtes Ideal von R.

Beweis des Lemmas. Angenommen est gilt $\mathfrak{a} = R$. dann existieren endlich viele Elemente $f_1, ..., f_n$ in I und Elemente $g_1, ..., g_n$ in R mit

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1.$$

Dann existiert eine Erweiterung $K \subset K'$, wo das Polynom f_i eine Nullstelle $\alpha_i \in K'$ für jedes $i \in \{1, ..., n\}$ besitzt. Wenn wir X_{f_i} für α_i substituieren, erhalten wir die Gleichung $0 = 1$: Widerspruch. Es gilt also $\mathfrak{a} \subsetneq R$. □

Nach Satz 2.64 existiert ein maximales Ideal $\mathfrak{m}$ in R mit $\mathfrak{a} \subset \mathfrak{m} \subset R$. Der Faktorring $L_1 := R/\mathfrak{m}$ ist also ein Körper. Die natürliche Inklusion $K \subset R$ induziert einen Homomorphismus von Ringen $K \to L_1$, der injektiv ist (Lemma 2.37). Der Körper L_1 ist also ein Erweiterungskörper von K. Für alle $f \in I$, sei $x_f \in L_1$ die Klasse von $X_f \in R$. Es gilt $f(X_f) \in \mathfrak{m}$, also $f(x_f) = 0$ in L_1. Jedes Polynom $f \in K[X]$ mit $\mathrm{Grad}(f) \geq 1$ besitzt also in L_1 eine Nullstelle.

Auf derselben Weise können wir dann eine Erweiterung $L_1 \subset L_2$ konstruiren, so dass jedes Polynom in $L_1[X]$ eine Nullstelle in L_2 besitzt. Durch Iteration erhalten eine Kette von Körpern:

$$K = L_0 \subset L_1 \subset L_{\subset} ...$$

so dass jedes Polynom $f \in K_n[X]$ mit $\mathrm{Grad}(f) \geq 1$ eine Nullstelle in L_{n+1} hat. Definiere dann

$$L := \bigcup_{n\geq 0} L_n.$$

Man sieht sofort, dass L ein Körper ist. Sei $f \in L[X]$ ein Polynom mit $\mathrm{Grad}(f) \geq 1$. Es existiert $n \geq 0$ mit $f \in L_n[X]$. Dann hat f eine Nullstelle in L_{n+1}, und damit in L. Der Körper L ist algebraisch abgeschlossen. □

Definition 3.25. Ein algebraischer Abschluss eines Körpers K ist ein algebraisch abgeschlossener Erweiterungskörper L, der algebraisch über K ist.

Satz 3.26. *Zu jedem Körper K existiert ein algebraischer Abschluss. Sind L, L' zwei algebraische Abschlüsse von K, so existiert ein Isomorphismus von Körpern $f : L \to L'$ mit $f|_K = \mathrm{id}_K$.*

Beweis. Nach Proposition existiert ein Homomorphismus von Körpern $f : L \to L'$ mit $f|_K = \mathrm{id}_K$. Das Bild $f(L)$ ist ein Teilkörper von L' isomorph zu L. Der Körper $f(L)$ ist also algebraisch abgeschlossen, und $f(L) \subset L'$ ist eine algebraische Erweiterung. Nach Lemma 3.20 gilt $f(L) = L'$ und f ist ein Isomorphismus. □

3.5 Die Körper $\mathbb{R}$ und $\mathbb{C}$

Konstruktion Obwohl wir schon wissen, was eine reelle und eine komplexe Zahl ist, geben wir unten eine präzise Definition für die Körper $\mathbb{R}$ und $\mathbb{C}$. Zuerst definiert man $\mathbb{N} = \{0, 1, 2, ...\}$, die Menge der natürlichen Zahlen. Dann ist $\mathbb{Z}$ die Grothendieck-Gruppe der kommutativen Halbgruppe $(\mathbb{N}, +)$. Der Körper $\mathbb{Q}$ ist der Quotientenkörper des Rings $(\mathbb{Z}, +, \times)$. Außerdem verfügt man über eine totale Ordnung $\leq$ auf $\mathbb{Q}$. Um $\mathbb{R}$ zu konstruieren, brauchen wir den Begriff einer Cauchy-Folgen.

Eine Cauchy-Folge in $\mathbb{Q}$ ist eine Folge $(x_n)_{n\in\mathbb{N}}$ von rationalen Zahlen, sodass die folgende Eigenschaft gilt: Für alle $\varepsilon \in \mathbb{Q}_{>0}$ existiert ein $N \in \mathbb{N}$ mit

$$|x_n - x_m| < \varepsilon$$

für alle $n, m \geq N$. Man sieht sofort, dass die Summe und das Produkt von zwei Cauchy-Folgen eine Cauchy-Folge ist. Man sagt, dass zwei Cauchy-Folgen $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ äquivalent sind, und man schreibt $x \sim y$, wenn $x_n - y_n$ gegen Null konvergiert, d.h. wenn für alle $\varepsilon \in \mathbb{Q}_{>0}$ ein $N \in \mathbb{N}$ existiert mit $|x_n - y_n| < \varepsilon$ für alle $n \geq N$. Dies definiert eine Äquivalenzrelation auf der Menge der Cauchy-Folgen. Ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge, so notiert man ihre Äquivalenzklasse durch $[(x_n)_{n\in\mathbb{N}}]$. Man definiert die Menge der reellen Zahlen durch:

$$\mathbb{R} := \frac{\{\text{Cauchy-Folgen}\}}{\sim} \tag{3.1}$$

Eine reelle Zahl ist also eine Äquivalenzklasse von Cauchy-Folgen. Man definiert eine Addition und eine Multiplikation auf $\mathbb{R}$ durch:

$$[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}] = [(x_n + y_n)_{n\in\mathbb{N}}]$$
$$[(x_n)_{n\in\mathbb{N}}] \times [(y_n)_{n\in\mathbb{N}}] = [(x_n y_n)_{n\in\mathbb{N}}].$$

Man sieht sofort, dass diese Definition sinnvoll ist. Dann ist $(\mathbb{R}, +, \times)$ ein kommutativer Ring. Die Eins ist die konstante Folge mit Wert 1, und die Null ist die konstante Folge mit Wert 0.

Satz 3.27. $(\mathbb{R}, +, \times)$ *ist ein Körper.*

Beweis. Sei $x = (x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge mit $[x] \neq 0$ in $\mathbb{R}$. Es existiert also ein $\varepsilon \in \mathbb{Q}_{>0}$, so dass für alle $N \geq 0$ ein $k \geq N$ existiert mit $|x_k| \geq \varepsilon$. Da $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge ist, existiert ein $N' \geq 0$ mit $|x_n - x_m| < \frac{\varepsilon}{2}$ für alle $n, m \geq N'$. Sei $n \geq N'$ und sei $k \geq N'$ mit $|x_k| \geq \varepsilon$. Es gilt:

$$|x_n| \geq |x_k| - |x_k - x_n| \geq \varepsilon - \frac{\varepsilon}{2} \geq \frac{\varepsilon}{2}.$$

Die rationale Zahl x_n ist also ungleich Null für $n \geq N'$. Sei $y = (y_n)_{n\in\mathbb{N}}$ eine Folge mit $y_n = \frac{1}{x_n}$ für alle $n \geq N'$. Dann ist y eine Cauchy-Folge, denn es gilt für $n, m \geq N'$:

$$|y_n - y_m| = \left|\frac{1}{x_n} - \frac{1}{x_m}\right| = \frac{|x_n - x_m|}{|x_n||x_m|} \leq \frac{4|x_n - x_m|}{\varepsilon^2}.$$

Es gilt natürlich $[x] \times [y] = 1$, also $[x]$ ist invertierbar. □

Man sagt, dass eine reelle Zahl $x = [(x_n)_{n\in\mathbb{N}}]$ positiv ist, und man schreibt $x > 0$, wenn ein $N \in \mathbb{N}$ existiert mit $x_n > 0$ für $n \geq N$. Man schreibt $x \geq 0$ falls $x = 0$ oder $x > 0$, und man sagt, dass x nicht-negativ ist. Man schreibt $x \geq y$ falls $x - y \geq 0$ für $x, y \in \mathbb{R}$. Dies definiert eine totale Ordnung auf $\mathbb{R}$.

Satz 3.28.

(i) Für alle $x, y, z \in \mathbb{R}$ gilt $x \geq y \Longrightarrow x + z \geq y + z$.

(ii) Für alle $x \geq 0$ und $y \geq 0$ gilt $xy \geq 0$.

Man sagt, dass $\mathbb{R}$ ein geordneter Körper ist.

Insbesondere sind Quadratzahlen nichnegativ. Die Gleichung $x^2 + 1 = 0$ hat also keine Lösung in $\mathbb{R}$. Schließlich definiert man die Menge der komplexen Zahlen durch:

$$\mathbb{C} := \frac{\mathbb{R}[X]}{(X^2 + 1)}.$$

Das Polynom X^2+1 ist irreduzibel über $\mathbb{R}$ weil es Grad 2 hat und weil es keine Nullstelle in $\mathbb{R}$ hat (Bemerkung 2.68). Dieser Faktorring ist also eine Körpererweiterung von $\mathbb{R}$ mit Grad 2. Die Klasse des Elements $X \in \mathbb{R}[X]$ wird mit i bezeichnet. Dann gilt

$$i^2 = -1$$

und jede komplexe Zahl besitzt eine eindeutige Darstellung als $a + ib$ mit $a, b \in \mathbb{R}$.

Satz 3.29 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

3.6 Endlicher Körper

Sei K ein endlicher Körper. Die Charakteristik von K ist notwendigerweise eine Primzahl $p > 1$ und sein Primkörper ist isomorph zu $\mathbb{F}_p$. Der Körper K ist dann ein endlich dimensionaler $\mathbb{F}_p$-Vektorraum. Insbesondere existiert eine natürliche Zahl $n = [K : \mathbb{F}_p]$ mit $|K| = p^n$.

Satz 3.30. *Zu jeder Primzahl $p > 1$ und jeder natürlichen Zahl $n \geq 1$ existiert bis auf Isomorphie genau ein Körper von Kardinalität p^n. Er wird mit $\mathbb{F}_{p^m}$ bezeichnet.*

Wir zeigen zuerst die Existenz von einem Körper mit $q := p^n$ Elemente.

Lemma 3.31. *Sei L ein Erweiterungskörper von $\mathbb{F}_p$, indem das Polynom $X^q - X$ vollständig zerfällt. Dann bilden die Nullstellen dieses Polynoms einen Teilkörper von L der Kardinalität q.*

Beweis. Seien $\alpha, \beta \in L$ zwei Nullstellen von $X^q - X$. Es gilt:

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta$$

$$(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta.$$

Ist $\beta \neq 0$ eine Nullstelle von $X^q - X$, so gilt $(\beta^{-1})^q = (\beta^q)^{-1} = \beta^{-1}$. Die Nullstellen von $X^q - X$ bilden also ein Teilkörper von L. Dieses Polynom hat höchstens q Nullstellen in L. Es genügt also zu zeigen, dass die Nullstellen dieses Polynoms paarweise verschieden sind. Sei $\alpha \in L$ mit $\alpha^q = \alpha$. Dann gilt:

$$\begin{aligned} X^q - X &= (X^q - X) - (\alpha^q - \alpha) \\ &= (X^q - \alpha^q) - (X - \alpha) \\ &= (X - \alpha)^q - (X - \alpha) \\ &= (X - \alpha)((X - \alpha)^{q-1} - 1). \end{aligned}$$

und somit ist α nur eine einfache Nullstelle von $X^q - X$. □

Seien nun K und K' zwei Körper mit genau q Elementen. Wir wollen zeigen, dass K und K' isomorph sind. Sei $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann existieren Einbettungen $K \to \overline{\mathbb{F}_p}$ und $K' \to \overline{\mathbb{F}_p}$. Wir können also annehmen, dass K und K' Teilkörper von $\overline{\mathbb{F}_p}$ sind. Für jedes Element $x \in K \setminus \{0\}$ gilt $x^{q-1} = 1$ nach dem Satz von Lagrange. Für alle $x \in K$ gilt also $x^q = x$. Aus demselben Grund gilt $x^q = x$ für alle $x \in K'$. Die Elemente in K und K' sind also Nullstellen in $\overline{\mathbb{F}_p}$ des Polynoms $X^q - X$. Es folgt: $K = K'$. Dies zeigt die Eindeutigkeit.

4 Exkurs

4.1 Die Eulersche φ-Funktion

Sei $n \geq 1$ eine ganze Zahl. Wir definieren:

$$\varphi(n) := |\{k \in \{1, 2, ..., n-1\},\ \mathrm{ggT}(k, n) = 1\}|.$$

Das heißt, $\varphi(n)$ ist die Anzahl der Zahlen in $\{1, 2, ..., n-1\}$, die teilerfremd zu n sind. Die Abbildung $k \mapsto \bar{k}$ liefert eine Bijektion

$$\{k \in \{1, 2, ..., n-1\},\ \mathrm{ggT}(k, n) = 1\} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad k \mapsto \bar{k}.$$

Die Zahl $\varphi(n)$ ist also die Ordnung der Gruppe der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$.

Seien nun m, n zwei positive Zahlen mit m und n teilerfremd. Nach dem Korollar 2.43 haben wir einen Isomorphismus von Ringen

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Dieser Isomorphismus liefert einen Isomorphismus zwischen den Gruppen der invertierbaren Elemente. Nach der Gleichung (2.4) erhalten wir also einen Isomorphismus:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Insbesondere gilt die folgende Gleichung:

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Definition 4.1. Eine multiplikative Funktion ist eine Funktion $f : \mathbb{N}^* \to \mathbb{C}$ mit der Eigenschaft: Sind m, n teilerfremd, so gilt die Gleichung $f(mn) = f(m)f(n)$. Die Menge der multiplikativen Funktionen wird durch $\mathcal{M}$ notiert.

Hier sind einige Beispiele für multiplikative Funktionen:

(a) Die konstante Funktion $\mathbb{N}^* \to \mathbb{C}$ mit Wert 1 ist natürlich multiplikativ, und wird einfach mit 1 bezeichnet.

(b) Die δ-Funktion $\delta : \mathbb{N}^* \to \mathbb{C}$ ist durch

$$\delta(n) = \begin{cases} 1 \text{ falls } n = 1 \\ 0 \text{ falls } n > 1 \end{cases}$$

definiert, und ist auch eine multiplikative Funktion.

(c) Die Eulersche φ-Funktion.

(d) Die Identitätsabbildung von $\mathbb{N}^*$.

Seien $f, g : \mathbb{N}^* \to \mathbb{C}$ zwei Funktionen. Wir definieren die Faltung $f * g$ von f und g als die Funktion

$$\mathbb{N}^* \to \mathbb{C}, \quad n \mapsto \sum_{d|n,\ d\geq 1} f(d)\ g\left(\frac{n}{d}\right).$$

Dies definiert eine Verknüpfung $*$ auf der Menge $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ aller Funktionen $\mathbb{N}^* \to \mathbb{C}$. Man sieht sofort, dass die Distributivgesetze

$$f * (g + h) = f * g + f * h$$

$$(f + g) * h = f * h + g * h$$

gelten.

Lemma 4.2. *Die Verknüpfung $*$ ist kommutativ.*

Beweis. Sei n eine positive Zahl. Die Abbildung $d \mapsto \frac{n}{d}$ ist eine Bijektion von der Menge der Teiler von n. Es gilt also:

$$\begin{aligned}(f * g)(n) &= \sum_{d|n,\ d\geq 1} f(d)\ g\Big(\frac{n}{d}\Big) \\ &= \sum_{d|n,\ d\geq 1} f\left(\frac{n}{d}\right)\ g(d) \\ &= (g * f)(n).\end{aligned}$$

□

Lemma 4.3. *Die Verknüpfung $*$ ist assoziativ.*

Beweis. Seien f, g, h drei Funktionen $\mathbb{N}^* \to M$. Es gilt:

$$\begin{aligned}((f*g)*h)(n) &= \sum_{d|n,\ d\geq 1} (f*g)(d)\ h\Big(\frac{n}{d}\Big) \\ &= \sum_{d|n,\ d\geq 1} \left(\sum_{k|d,\ k\geq 1} f(k)\ g\Big(\frac{d}{k}\Big) \right) h\Big(\frac{n}{d}\Big) \\ &= \sum_{\substack{a,b,c\geq 1 \\ abc=n}} f(a)\ g(b)\ h(c).\end{aligned}$$

Diese letzte Formel ist symmetrisch in f, g, h, also es folgt: $((f*g)*h) = (f*(g*h)$. □

Lemma 4.4. *Die δ-Funktion ist das Einselement von $(\mathcal{F}(\mathbb{N}^*, \mathbb{C}), *)$.*

Beweis. Sei n eine positive Zahl. Es gilt:

$$(f*\delta)(n) = \sum_{d|n,\ d\geq 1} f(d)\ \delta\Big(\frac{n}{d}\Big) = f(n)$$

□

Proposition 4.5. *$(\mathcal{F}(\mathbb{N}^*, \mathbb{C}), +, *)$ ist ein kommutativer Ring. Die Eins ist die Funktion δ. Die invertierbaren Elemente sind die Funktionen $f : \mathbb{N}^* \to \mathbb{C}$ mit $f(1) \neq 0$. Die Abbildung $\mathcal{F}(\mathbb{N}^*, \mathbb{C}) \to \mathbb{C}$, $f \mapsto f(1)$ ist ein surjektiver Homomorphismus von Ringen.*

Beweis. Es folgt sofort aus der Definition, dass die Gleichung $(f*g)(1) = f(1)g(1)$ gilt, also $\mathcal{F}(\mathbb{N}^*, \mathbb{C}) \to \mathbb{C}$, $f \mapsto f(1)$ ist ein surjektiver Homomorphismus von Ringen. Ist f invertierbar, so ist $f(1) \in \mathbb{C}$ invertierbar, also $f(1) \neq 0$.

Umgekehrt, sei $f : \mathbb{N}^* \to \mathbb{C}$ mit $f(1) \neq 0$. Wir suchen eine Funktion $g : \mathbb{N}^* \to \mathbb{C}$, so dass die Gleichung

$$\sum_{d|n, d\geq 1} f(d)\ g\Big(\frac{n}{d}\Big) = \delta(n) \tag{4.1}$$

für alle $n \geq 1$ gilt. Wir definieren die Funktion g per Induktion. Wir müssen $g(1) = \frac{1}{f(1)}$ setzen. Sei $m \geq 2$. Angenommen wir haben den Wert $g(n)$ für alle $1 \leq n \leq m-1$ definiert, so dass die Gleichung (4.1) für alle $1 \leq n \leq m-1$ gilt. Wir setzen:

$$g(m) := -\frac{1}{f(1)} \sum_{d|m,\ d>1} f(d)\ g\Big(\frac{m}{d}\Big).$$

Dann gilt (4.1) auch für $n = m$. Dies definiert per Induktion eine Funktion g, die die gewünschte Eigenschaft besitzt. Es folgt, dass f invertierbar ist. □

Für $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$ mit $f(1) \neq 0$ wird das Inverse zu f mit f^{-1} bezeichnen. Diese Funktion darf nicht mit der Funktion $n \mapsto \frac{1}{f(n)}$ verwechselt werden. Ist $n = p$ eine Primzahl, so gilt die Gleichung:

$$f^{-1}(p) = -\frac{f(p)f^{-1}(1)}{f(1)} = -\frac{f(p)}{f(1)^2}.$$

Lemma 4.6. *Sind f und g multiplikative Funktionen, so ist $f * g$ auch multiplikativ.*

Beweis. Seien m, n zwei positive Zahlen mit m und n teilerfremd. Es gilt:

$$\begin{aligned}(f*g)(mn) &= \sum_{d|mn,\ d\geq 1} f(d)\ g\Big(\frac{mn}{d}\Big)\\ &= \sum_{\substack{d_1|m, d_2|n\\ d_1,d_2\geq 1}} f(d_1d_2)\ g\left(\frac{mn}{d_1d_2}\right)\\ &= \sum_{\substack{d_1|m, d_2|n\\ d_1,d_2\geq 1}} f(d_1)f(d_2)\ g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)\\ &= (f*g)(m)(f*g)(n).\end{aligned}$$

□

Die Verknüpfung $*$ induziert also eine Verknüpfung auf der Menge $\mathcal{M}$ der multiplikativen Funktionen $\mathbb{N}^* \to \mathbb{C}$.

Lemma 4.7. *Ist f eine multiplikative Funktion, so gilt $f(1) \in \{0, 1\}$. Wenn die Gleichung $f(1) = 1$ gilt, dann ist f invertierbar und f^{-1} ist eine multiplikative Funktion.*

Beweis. Es gilt per Definition $f(1) = f(1^2) = f(1)^2$, also $f(1) \in \{0, 1\}$. Nehmen wir an, dass $f(1) = 1$ gilt. Dann ist f invertierbar nach Proposition 4.5. Schreiben wir g für das Inverse f^{-1}. Wir zeigen per Induktion nach $N \geq 1$, dass die folgende Eigenschaft gilt: Für alle m, n teilerfremd mit $mn \leq N$ gilt die Gleichung:

$$g(mn) = g(m)g(n). \tag{4.2}$$

Diese Aussage gilt natürlich für $N = 1$, denn es ist $g(1) = 1$. Seien m, n teilerfremd, mit $mn = N + 1$. Es gilt:

$$\begin{aligned}0 &= \sum_{d|mn, d\geq 1} f(d)\ g\Big(\frac{mn}{d}\Big)\\ &= \sum_{\substack{d_1|m, d_2|n\\ d_1,d_2\geq 1}} f(d_1d_2)\ g\left(\frac{mn}{d_1d_2}\right)\\ &= \left(\sum_{\substack{d_1|m, d_2|n\\ d_1,d_2\geq 1, d_1d_2\neq 1}} f(d_1)f(d_2)\ g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)\right) + g(mn)\\ &= \left(\sum_{d_1|m} f(d_1)\ g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2)\ g\left(\frac{n}{d_2}\right)\right) - g(m)g(n) + g(mn)\\ &= g(mn) - g(m)g(n)\end{aligned}$$

Es folgt: $g(mn) = g(m)g(n)$. □

Wir definieren die Möbiussche Funktion $\mu : \mathbb{N}^* \to \mathbb{C}$ durch:

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1 \\ (-1)^k & \text{falls } n = p_1 ... p_k, \text{ (die } p_i \text{ sind paarweise verschiedene Primzahlen)} \\ 0 & \text{sonst.} \end{cases}$$

Satz 4.8 (Möbiussche Umkehrformel)**.** *Es gilt $1 * \mu = \delta$. Mit anderen Worten, μ ist das Inverse der konstanten Funktion 1. Sei f eine Funktion $\mathbb{N}^* \to \mathbb{C}$. Definiere für $n \geq 1$, $g(n) = \sum_{d|n, d\geq 1} f(d)$. Dann gilt die Umkehrformel:*

$$f(n) = \sum_{d|n, d\geq 1} \mu(d) g\Big(\frac{n}{d}\Big).$$

Beweis. Es gilt $(1 * \mu)(1) = 1$. Sei nun $n \geq 2$ eine natürliche Zahl und sei $n = p_1^{k_1} ... p_r^{k_r}$ ihre Primfaktorzerlegung. Es gilt:

$$\begin{aligned} (1 * \mu)(n) &= \sum_{d|n, d\geq 1} \mu(d) \\ &= \sum_{S \subset \{1,...,r\}} \mu\Big(\prod_{i \in S} p_i\Big) \\ &= \sum_{S \subset \{1,...,r\}} (-1)^{|S|} \\ &= \sum_{i=0}^{r} \binom{r}{i} (-1)^i \\ &= 0. \end{aligned}$$

Es folgt $1 * \mu = \delta$. Es gilt $g = f * 1$, also

$$g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * \delta = f.$$

Dies ist die möbiussche Umkehrformel. □

Satz 4.9. *Es gilt die Gleichungen: $1 * \varphi = \mathrm{id}$ und $\varphi = \mu * \mathrm{id}$. Mit anderen Worten gelten für alle $n \geq 1$ die Gleichungen:*

$$n = \sum_{d|n, d\geq 1} \varphi(d)$$

$$\varphi(n) = n \sum_{d|n, d\geq 1} \frac{\mu(d)}{d}.$$

Beweis. Die zweite Formel ist die Möbiussche Umkehrformel der ersten. Sei $n \geq 1$. Für jeden positiven Teiler d von n, sei A_d die Menge der Elemente der Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ von Ordnung d. Es gilt natürlich:

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n, d\geq 1} A_d$$

und es reicht also zu zeigen, dass $|A_d| = \varphi(d)$ gilt. Jedes Element in A_d erzeugt eine Untergruppe der Ordnung d. Nach Proposition 1.82 existiert eine einzige Untergruppe $H_d \subset \mathbb{Z}/n\mathbb{Z}$ der Ordnung d. Die Menge A_d ist also die Menge der Erzeuger von H_d. Aber H_d ist zyklisch von Ordnung d, also es gilt $|A_d| = \varphi(d)$. □

4.2 Abelsche Gruppen von endlichem Typ

Definition 4.10. Eine abelsche Gruppe $(G, +)$ heißt *frei*, falls eine Teilmenge $X \subset G$ existiert mit den folgenden Eigenschaften:

(i) Die Teilmenge X erzeugt G.

(ii) Aus der Gleichung
$$\sum_{i=0}^{n} k_i x_i = 0$$
folgt $k_1 = ... = k_n = 0$, für alle Elemente $x_1, ..., x_n$ in X und für alle $k_1, ..., k_n \in \mathbb{Z}$.

Die Menge X heißt Basis von G.

Mit anderen Worten, die Abbildung
$$\mathbb{Z}^{(X)} \to G, \quad (k_x)_{x \in X} \mapsto \sum_{x \in X} k_x x$$
ist ein Isomorphismus von Gruppen. Eine freie abelsche Gruppe ist also eine Gruppe, die isomorph zu $\mathbb{Z}^{(X)}$ für eine Menge X ist. Eine Teilmenge $X \subset G$ heißt frei, wenn die Bedingung (ii) in Definition 4.10 erfüllt ist. Eine Basis ist also ein freies Erzeugendensystem.

Beispiel 4.11.

(a) Für $n \geq 1$ ist die Gruppe $\mathbb{Z}^n$ frei.

(b) Die Gruppe $(\mathbb{Z}[X], +)$ ist frei.

(c) Die Gruppe $(\mathbb{Q}_{>0}, \times)$ ist frei (Beispiel 1.61).

(d) Die Gruppe $(\mathbb{Q}, +)$ ist nicht frei: Seien $x, y \in \mathbb{Q} \setminus \{0\}$ mit $x = \frac{a}{b}$ und $y = \frac{c}{d}$ mit $a, b, c, d \in \mathbb{Z} \setminus \{0\}$. Es folgt : $day - bdx = 0$. Eine Teilmenge $X \subset \mathbb{Q}$ mit $|X| \geq 2$ ist also nicht frei.

Es gibt einen großen Unterschied zwischen $\mathbb{Z}^{(\mathbb{N})}$ und $\mathbb{Z}^{\mathbb{N}}$. Letztere ist viel größer als Erstere. Wir werden gleich sehen, dass es keine Bijektion zwischen diesen beiden Mengen gibt.

Definition 4.12. Eine Menge X heißt abzählbar, falls eine Surjektion $\mathbb{N} \to X$ existiert.

Lemma 4.13. *Eine abzählbare Vereinigung abzählbarer Mengen ist abzählbar.*

Beweis. Sei A_n eine Abzählbare Menge für alle $n \in \mathbb{N}$, und sei $A = \bigcup_{m\in\mathbb{N}} A_n$. Für alle $n \in \mathbb{N}$, sei $f_n : \mathbb{N} \to A_n$ eine surjektive Abbildung. Wir definieren eine surjektive Abbildung $\mathbb{N}^2 \to A$ durch:

$$f : (a, b) \mapsto f_a(b).$$

Es reicht also zu zeigen, dass $\mathbb{N}^2$ abzählbar ist. Das folgende Bild ist ein Beispiel für eine bijektive Folge $\mathbb{N} \to \mathbb{N}^2$: □

Beispiel 4.14. (a) Die Menge $\mathbb{N}^n$ ist abzählbar für alle $n \geq 1$ (per Induktion nach n).

(b) Die Menge

$$\mathbb{Q} = \bigcup_{n\geq 1} \left\{ \frac{a}{n},\ a \in \mathbb{Z} \right\}$$

ist eine abzählbare Vereinigung abzählbarer Mengen, also ist abzählbar.

(c) Sei $A := \mathbb{Z}^{(\mathbb{N})}$ und sei $(e_n)_{n\in\mathbb{N}}$ die natürliche Basis von A. Definiere:

$$A_n := \left\{ \sum_{k=0}^{n} a_i e_i,\ a_i \in \mathbb{Z} \text{ für alle } 0 \leq i \leq n \right\}.$$

Dann ist A_n abzählbar und es gilt $A = \bigcup_{n\geq 1} A_n$. Die Menge $A := \mathbb{Z}^{(\mathbb{N})}$ ist also abzählbar.

Proposition 4.15. *Sei X eine Menge. Es existiert keine Surjektion $X \to \mathcal{P}(X)$. Insbesondere ist die Menge $\mathcal{P}(\mathbb{N})$ nicht abzählbar.*

Beweis. Sei $f : X \to \mathcal{P}(X)$ eine Surjektion. Sei

$$A := \{x \in X, x \notin f(x)\}.$$

Sei $a \in X$ ein Element mit $f(a) = A$. Dann gilt

$$a \in A \Longleftrightarrow a \notin f(a) \Longleftrightarrow a \notin A$$

und dies liefert einen Widerspruch. Es existiert also keine Surjektion $X \to \mathcal{P}(X)$. □

Ist $A \subset X$ eine Teilmenge einer Menge, definiert man die Abbildung:

$$f_A : X \longrightarrow \{0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A. \end{cases}$$

Das folgende Lemma ist offensichtlich:

Lemma 4.16. *Die Abbildung*

$$\begin{array}{ccc} \mathcal{P}(X) & \longrightarrow & \{0,1\}^X := \{f : X \to \{0,1\}\} \\ A & \mapsto & f_A \end{array}$$

ist eine Bijektion, und die Umkehrabbildung ist $g \mapsto \{x \in X,\ g(x) = 1\}$.

Die Menge der Folgen von Elementen aus $\{0,1\}$ ist also nicht abzählbar. Insbesondere ist das Produkt $\mathbb{Z}^{\mathbb{N}}$ nicht abzählbar.

Proposition 4.17. *Die Gruppe*

$$G = \mathbb{Z}^{\mathbb{N}} = \prod_{n=0}^{\infty} \mathbb{Z}$$

ist nicht frei.

Lemma 4.18. *Sei G eine freie Gruppe und sei $a \in A \setminus \{0\}$. Die Menge:*

$$E := \{r \in \mathbb{N},\ \textit{die Gleichung } a = rx \textit{ hat eine Lösung in } G\}$$

ist endlich.

Beweis. Sei $(e_i)_{i\in I}$ eine Basis von G, und schreibe $a = \sum_{j=0}^{n} a_j e_{i_j}$ mit $a_j \in \mathbb{Z}$. Existiert eine Lösung zur Gleichung $a = rx$, so teilt r alle Koeffizienten a_j für $0 \leq j \leq n$. Die Menge E ist also endlich. □

Beweis von Proposition 4.17. Nehmen wir an, dass $G = \mathbb{Z}^{\mathbb{N}}$ frei ist, und sei $\{e_\alpha\}_{\alpha\in I}$ eine Basis von G. Für $k \geq 0$ definiere:

$$s_k := (0, ..., 0, 1, 0, ...) \in G$$

wo der Koeffizient 1 an der k-sten Stelle ist. Schreibe

$$s_k = \sum_{\alpha\in I} \lambda_{k,\alpha} e_\alpha$$

für $(\lambda_{k,\alpha}) \in \mathbb{Z}^{(I)}$. Setze:

$$J := \{\alpha \in I,\ \exists k \geq 0,\ \lambda_{k,\alpha} \neq 0\}.$$

Es gilt $J = \bigcup_{k\geq 0} J_k$ mit $J_k = \{\alpha \in I,\ \lambda_{k,\alpha} \neq 0\}$. Die Menge J_k ist endlich, also die Menge J ist abzählbar. Setze $H := \langle e_\alpha,\ \alpha \in J\rangle$. Es gilt natürlich: $s_k \in H$ für alle $k \geq 0$. Sei $\pi : G \to G/H$ die natürliche Abbildung, und sei $e'_\alpha := \pi(e_\alpha)$. Die Elemente e'_α für $\alpha \in I \setminus J$ bilden eine Basis von G/H. Die Gruppe G/H ist also auch frei. Definiere:

$$B := \left\{ x = (x_n)_{n\in\mathbb{N}} \in G,\ \left|\frac{x_{n+1}}{x_n}\right| \in \mathbb{N}_{\geq 2} \right\}.$$

ist $(q_0, q_1, q_2, ...)$ eine beliebige Folge von Elementen aus $\mathbb{N}\setminus\{0,1\}$, so ist $(q_0, q_0q_1, q_0q_1q_2, ...)$ ein Element in B. Dies liefert eine Injektion

$$(\mathbb{N} \setminus \{0,1\})^{\mathbb{N}} \to B.$$

die Menge B ist also unabzählbar. Da H abzählbar ist (Beispiel 4.14 (c)) existiert ein Element $a = (a_n)_{n\in\mathbb{N}}$ so dass $\pi(a) \neq 0$, wobei $\pi : G \to G/H$ die natürliche Abbildung ist. Für jedes $n \geq 0$, definiere

$$b_n = (0, ..., 0, a_{n+1}, a_{n+2}, ...)$$

wo die n ersten Komponenten gleich Null sind. Es gilt $a \equiv b_n \pmod{H}$. Außerdem existiert $c_n \in G$ mit $b_n = a_{n+1}c_n$ (da a_{n+1} die Komponenten von b_n teilt). Es folgt also $a \equiv a_{n+1}c_n \pmod{H}$ für alle $n \geq 0$. Die Menge der Zahlen $r \geq 1$ so dass die Gleichung $a = rx$ eine Lösung hat, ist also unendlich. Aber die Gruppe G/H ist frei, un dies widerspricht dem obigen Lemma. □

Definition 4.19. Eine abelsche Gruppe G heißt torsionsfrei, falls alle Elemente in $G \setminus \{0\}$ von unendlicher Ordnung sind.

Beispiel 4.20.

(a) Eine freie Gruppe ist torsionsfrei.

(b) Die Gruppen $(\mathbb{Q}, +)$ und $\mathbb{Z}^{\mathbb{N}}$ sind torsionsfrei, aber nicht frei.

Lemma 4.21. *Sei G eine abelsche Gruppe, und sei:*

$$G_{\text{tor}} := \{g \in G, \text{ von endlicher Ordnung}\}.$$

Dann ist G_{tor} eine Untergruppe von G, und der Quotient G/G_{tor} ist torsionsfrei.

Beweis. Es gilt natürlich $0 \in G_{\text{tor}}$. Sind $a, b \in G_{\text{tor}}$ so existieren $n, m \geq 1$ mit $na = mb = 0$. Dann gilt $(nm)(a-b) = 0$, also $a-b \in G_{\text{tor}}$. Es folgt, dass G_{tor} eine Untergruppe von G ist. Sei $\tilde{x}$ ein Element von endlicher Ordnung in G/G_{tor} und sei $x \in G$ ein Urbild von x in G. Es existiert $n \geq 1$ mit $n\tilde{x} = 0$, also $nx \in G_{\text{tor}}$. Dann existiert ein $m \geq 1$ mit $mnx = 0$. Es folgt $x \in G_{\text{tor}}$, also $\tilde{x} = 0$. □

Definition 4.22. Eine abelsche Gruppe $(G, +)$ heißt von endlichem Typ, falls ein endliches Erzeugendensystem in G existiert.

Proposition 4.23. *Sei G eine abelsche Gruppe von endlichem Typ, und sei $H \subset G$ eine Untergruppe. Dann ist H von endlichem Typ.*

Proposition 4.24. *Eine freie abelsche Gruppe von endlichem Typ G ist isomorph zu $\mathbb{Z}^n$ für eine eindeutige natürliche Zahl $n \geq 0$. Jede Basis von G besitzt genau n Elemente. Die Zahl n heißt der Rang von G.*

Beweis. Es reicht zu zeigen, dass aus $\mathbb{Z}^n \simeq \mathbb{Z}^m$ folgt $n = m$. Setze $M := \mathbb{Z}^m$ und $N := \mathbb{Z}^n$. Sei p eine Primzahl. Der natürliche Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induziert einen surjektiven Homomorphismus:

$$f : M = \mathbb{Z}^m \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n, \quad (x_1, ..., x_n) \mapsto (x_1 \pmod{p}, ..., x_n \pmod{p})$$

und der Kern von f ist pM. Wir erhalten einen Isomorphismus $M/pM \simeq \mathbb{F}_p^m$. Aus $\mathbb{Z}^n \simeq \mathbb{Z}^m$ folgt also $\mathbb{F}_p^m \simeq \mathbb{F}_p^n$, also $n = m$. □

Proposition 4.25. *Sei G eine freie abelsche Gruppe von endlichem Typ. Jede Untergruppe von G ist frei und von endlichem Typ.*

Beweis. Wir können ohne Beschränkung annehmen, dass $G = \mathbb{Z}^n$ für ein $n \geq 1$ gilt. Für $n = 1$ ist das Ergebnis schon bekannt. Sei $H \subset G$ eine Untergruppe. Sei $p : G \to \mathbb{Z}$ die Projektion auf den ersten Faktor. Definiere $K := \text{Kern}(p) \cap H$ und $B := p(H)$. Es gilt $K \subset \text{Kern}(p) = \{0\} \times \mathbb{Z}^{n-1}$. Nach der Induktionsvoraussetzung ist K frei.

Erster Fall: $B = \{0\}$. In diesem Fall gilt $H = K$, und ist somit frei.

Zweiter Fall: $B \neq \{0\}$. Sei $a \in H$ ein Element mit $B = (f(a))$. Die Abbildung:

$$K \times \mathbb{Z} \longrightarrow H, \quad (x, k) \mapsto x + ka$$

ist ein Gruppenisomorphismus: Aus $x + ka = 0$ mit $x \in K$, $k \in \mathbb{Z}$ folgt $kp(a) = 0$, also $k = 0$ und $x = 0$. Der Homomorphismus ist also injektiv. Für alle $h \in H$ gilt $h = (h - ka) + ka$ wobei $k \in \mathbb{Z}$ ist die ganze Zahl mit $p(h) = kp(a)$. Das Element $h - ka$ ist in K, und dies zeigt dass f auch surjektiv ist. Es folgt

$$H \simeq K \times \mathbb{Z}$$

und H ist also frei. □

Proposition 4.26. *Eine torsionsfreie abelsche Gruppe von endlichem Typ ist frei.*

Beweis. Sei G eine abelsche torsionsfreie Gruppe von endlichem Typ. Sei $X \subset G$ ein endliches Erzeugendensystem von G. Sei $(e_1, ..., e_r)$ ein freies System von Elementen aus X mit r maximal. Sei $H := \langle e_1, ..., e_r \rangle$. Für jedes $x \in X$ ist das System $(e_1, ..., e_r, x)$ nicht frei, also es existiert ein $n \geq 1$ mit $nx \in H$. Da X endlich ist existiert ein $n \geq 1$ mit $nx \in H$ für alle $x \in X$. Es folgt $nG \subset H$, wobei $nG := \{na, a \in G\}$. Die Abbildung $G \to nG$, $a \mapsto na$ ist bijektiv weil G torsionsfrei ist, also G ist isomorph zu einer Untergruppe von H. □

Satz 4.27. *Sei G eine abelsche Gruppe von endlichem Typ. Sei $r \geq 0$ der Rang von G. Es existiert eine eindeutige Folge von Zahlen $a_1, ..., a_n$ mit $a_1 \geq 2$ für alle $1 \leq i \leq n$ und $a_i | a_{i+1}$ für alle $1 \leq i \leq n - 1$, so dass gilt:*

$$G \simeq \mathbb{Z}^r \times \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}.$$

4.3 Devissage von $(\mathbb{Z}/n\mathbb{Z})^\times$

Sind n und m teilerfremd, so gilt

$$(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

Es reicht also die Struktur der Gruppe $(\mathbb{Z}/p^m\mathbb{Z})^\times$ für p eine Primzahl und $m \in \mathbb{N}^*$ zu bestimmen. Wir fangen mit folgendem Satz an:

Satz 4.28. *Sei K ein Körper und sei $G \subset K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Setze $n := |G|$. Für jeden positiven Teiler d von n, sei a_d die Anzahl der Elemente von Ordnung d. □