Mitschrieb

Algebra und Zahlentheorie

Emma Bach

Basierend auf:

Vorlesung Algebra und Zalentheorie von
Prof. Dr. Wolfgang Soergel

2025-11-25

Inhalt

Chapter 1

Elementare Zahlentheorie

1.1 Primzahlen

Definition 1.1.1. $H \subseteq \mathbb{Z}$ heißt Untergruppe von $\mathbb{Z}$, wenn

$$n \in H \implies -n \in H,$$

und

$$m, n \in H \implies m + n \in H$$

Satz 1.1.2. *Es gibt eine Bijektion*

$$\begin{aligned} \mathbb{N} &\leftrightarrow \{\text{Untergruppen von } (\mathbb{Z}, +)\} \\ n &\mapsto n\mathbb{Z} \end{aligned}$$

Beweis. Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Entweder $H = \{0\} = 0\mathbb{Z}$, oder $H \neq \{0\}$.

Sei also $H \neq \{0\}$. Dann gibt es ein kleinstes Element m der Menge $\{n \in H \mid n > 0\}$. Aus den Untergruppenaxiomen folgt $m\mathbb{Z} \subseteq H$. Gleichzeitig kann kein Element $n \notin m\mathbb{Z}$ in H enthalten sein, denn sonst wäre auch $r = n \mod m \neq 0$ in H enthalten. Dann hätten wir aber $r < m$, was ein Widerspruch ist.

Als Umkehrfunktion wählen wir das kleinste positive Element von H. □

Definition 1.1.3. Eine **Primzahl** ist eine natürliche Zahl $p \in \mathbb{N}_{\geq 2}$, die nicht als Produkt zweier Zahlen $a, b < p$ geschrieben werden kann.

Satz 1.1.4. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, es gäbe endlich viele Primzahlen. Sei also $p_1, \ldots, p_r$ eine vollständige Liste aller Primzahlen. Dann wäre aber

$$q = 1 + \prod_{i=1}^{r} p_i$$

durch keine Primzahl teilbar, also selbst eine Primzahl. Widerspruch! □

Satz 1.1.5. *Jede Zahl $n \in \mathbb{N}$ kann als Produkt von Primzahlen geschrieben werden:*

$$n = p_1 \cdot \ldots \cdot p_r \quad (r \geq 0)$$

Beweis. Der Fall $n = 1$ gilt per Konvention durch das leere Produkt.

Sei $n \geq 2$ gegeben. Es gilt entweder:

- n ist eine Primzahl.
- n ist von der Gestalt $n = a \cdot b$, mit $a, b < n$.

Der Satz folgt durch Induktion über die entstehende Baumstruktur - nach Induktionsannahme haben a und b eine Primfaktorzerlegung. Also hat auch n eine Primfaktorzerlegung. □

Definition 1.1.6. Der **größte gemeinsame Teiler** von $a, b \in \mathbb{Z}$ mit $a \neq 0$ oder $b \neq 0$ ist die Zahl:

$$\mathrm{ggT}(a, b) = \max\{d \in \mathbb{N} : d \mid a \wedge d \mid b\}$$

Satz 1.1.7. **<u>Über den größten gemeinsamen Teiler</u>***: Seien $a, b \in \mathbb{Z}$. So gibt es $r, s \in \mathbb{N}$ mit*

$$\mathrm{ggT}(a, b) = ra + sb$$

Gegeben $d \mid a$ und $d \mid b$ gilt außerdem $d \mid \mathrm{ggT}(a, b)$.

Beweis. Die Menge

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

bildet eine Untergruppe von Z, ist also eine Gruppe der Form $m\mathbb{Z}$ mit $m > 0$. Da $a \in m\mathbb{Z}$ und $b \in m\mathbb{Z}$ ist m ein gemeinsamer Teiler. Da m ein Element in H ist existiert außerdem per Definition eine Darstellung $m = r'a + s'b$. Es gilt also

$$(d \mid a) \wedge (d \mid b) \implies d \mid r'a + s'b \implies d \mid m.$$

Aus $(d \mid a) \land (d \mid b) \implies d \mid m$ folgt nun, dass jeder Teiler von a und b m teilt, also kann es keinen Teiler von a und b geben, welcher größer als m ist. □

Die Existenz der Darstellung $\text{ggT}(a, b) = ra + sb$ ist auch als das **Lemma von Bézout** oder die **Bézoutsche Identät** bekannt.

Lemma 1.1.8. **Lemma von Euklid:** *Sei p eine Primzahl und $a, b \in \mathbb{Z}$. Dann gilt:*

$$p \mid ab \implies (p \mid a) \lor (p \mid b)$$

Beweis. Es reicht zu Zeigen:

$$(p \nmid a) \land (p \mid ab) \implies p \mid b$$

Aus $p \nmid a$ folgt $\text{ggT}(p, a) = 1$. Nach dem Lemma von Bézout können wir also 1 darstellen als:

$$1 = rp + sa$$

also:

$$b = rpb + sab$$

Es gilt trivial $p \mid prb$, außerdem gilt per Annahme $p \mid ab$. Es folgt $p \mid rpb + sab = b$. □

Satz 1.1.9. **Eindeutigkeit der Primfaktorzerlegung im Ring $\mathbb{Z}$:** *Sei $n \in \mathbb{N}_{\geq 1}$ und*

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

wobei alle q_i und r_i Primzahlen sind. So gilt $r = s$ und es gilt eine Permutation $\sigma \in S_r$ mit $p_i = q_{\sigma(i)}$.

Äquivalente Formulierungen:

- Falls die p_i und q_i Aufsteigend oder Absteigend sortiert sind, gilt $\forall i : p_i = q_i$
- Es existiert eine Bijektion zwischen endlichen Multimengen von Primzahlen und $\mathbb{N}_{\geq 1}$.

Beweis. Per Induktion folgt aus dem Lemma von Euklid schnell:

$$p_1 \mid p_1 \implies \bigvee_{i=1}^{s} p_1 \mid q_i$$

> Also existiert ein q_i mit $p_1 = q_i$. Teilen wir nun beide Seiten durch p_1, folgt die Aussage durch die Induktionsannahme. □

Definition 1.1.10. Euklidischer Algorithmus

Chapter 2

Gruppen

Definition 2.0.1.

1. Eine Menge M mit Verknüpfung $\top : M \times M \to M$ heißt **Magma**.
2. Ein Magma mit neutralem Element heißt **unitäres Magma**.
3. Ein unitäres Magma mit assoziativer Verknüpfung heißt **Monoid**.
4. Ein Monoid mit inversen Elementen heißt **Gruppe**.
5. Eine Gruppe mit kommutativer Gruppe heißt **kommutative Gruppe** oder **abelsche Gruppe**.

Beispiel 2.0.2.

1. $(\mathbb{Z}, -)$ ist ein nichtunitäres Magma.
2. ?
3. $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ sind Monoide.
4. $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.

Satz 2.0.3. *Das neutrale Element einer Gruppe ist eindeutig.*

- Es gibt keine Gruppe mit 0 Elementen, da die Leere Menge kein neutrales Element hat.
- Es gibt genau eine Gruppe mit einem Element, die Gruppe $\{e\}$.

Satz 2.0.4. *Es gibt genau eine Gruppe mit zwei Elementen, nämlich die Gruppe $\{e, a\}$, mit Verknüpfungstabelle:*

	e	a
e	e	a
e	a	e

Beweis. Durch die Definition von e sind drei Teile der Tabelle schon eindeutig festgelegt. $a \cdot a = e$, da sonst a kein Inverses hätte. □

Satz 2.0.5. *Gilt für ein Gruppenelement $a \in G$ $a^2 = a$, so gilt $a = e$.*

Beweis.

$$a = ae = aaa^{-1} = aa^{-1} = e$$

□

Satz 2.0.6. *Aus $a \cdot x = a \cdot y$ folgt $x = y$.*

Beweis.

$$\begin{aligned} ax &= ay \\ a^{-1}ax &= a^{-1}ay \\ ex &= ey \\ x &= y \end{aligned}$$

□

Es folgt, dass in einer Gruppentabelle in jeder Spalte und jeder Zeile kein Element doppelt vorkommen kann.

Korollar 2.0.7. *Es gibt nur eine Gruppe mit drei Elementen, nämlich:*

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Satz 2.0.8. *Es gibt zwei Gruppen mit vier Elementen, nämlich:*

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\simeq \mathbb{Z}/4\mathbb{Z}$

Definition 2.0.9. Ein Gruppenhomomorphismus ist eine Abbildung

$$\varphi : (G, \top) \to (H, \bot)$$

mit

$$\varphi(a \top b) = \varphi(a) \bot \varphi(b)$$

Wir schreiben die Menge der Gruppenhomomorphismen von G nach H als $\mathrm{Grp}(G, H)$.

Satz 2.0.10. $\mathrm{Grp}((\mathbb{Z}, +), G) \simeq G$

Beweis. Ordne jedem Gruppenelement g die Abbildung $\varphi(n) : g \to g^n$ zu. □

Satz 2.0.11. *Sind G und H Gruppen, so gilt* $\mathrm{Mag}(G, H) = \mathrm{Mon}(G, H) = \mathrm{Grp}(G, H)$.

Definition 2.0.12. Eine Teilmenge $H \subseteq G$ einer Gruppe G heißt **Untergruppe**, wenn sie so mit einer Gruppenstruktur versehen werden kann, dass die Einbettungsabbildung $i : H \to G$ ein Gruppenhomomorphismus ist.

Dies ist eine sehr allgemeine Definition, die analog für Untervektorräume, Untermagmas etc. funktioniert. In der Praxis verwendet man meistens folgendes Kriterium:

Satz 2.0.13. *H ist genau dann eine Untergruppe, wenn $e \in H$ und wenn für jedes $a, b \in H$ auch $ab \in H$ und $a^{-1}, b^{-1} \in H$.*

Satz 2.0.14. **Satz von Lagrange:** *Sei G eine endliche Gruppe und H eine Untergruppe. So ist die Zahl der Elemente von H ein Teiler der Zahl der Elemente von G.*

Der Beweis folgt nach einigen weitern Definitionen und Sätzen.

Definition 2.0.15. Sei G eine Gruppe mit Untergruppe H. Wir definieren:

$$gH = \{gh \mid h \in H\} \subseteq G$$
$$G/H = \{gH \mid g \in G\} \subseteq \mathcal{P}(G)$$

Lemma 2.0.16. *Sei $h \in H$. Dann gilt $hH = H$.*

Lemma 2.0.17. *Je zwei Nebenklassen gH und $g'H$ sind entweder gleich oder disjunkt.*

Aus diesen beiden Lemmas folgt $|G| = |G/H| \cdot |H|$, was den Satz von Lagrange impliziert.

Satz 2.0.18. *Der Schnitt beliebig vieler Untergruppen bildet eine Untergruppe.*

Definition 2.0.19. Sei G eine Gruppe und $T \subseteq G$ eine Teilmenge. Die **durch T erzeugte Untergruppe** $\langle T \rangle$ ist die kleinste Untergruppe, welche T enthält.

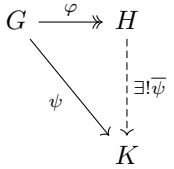
$\langle T \rangle$ besteht aus allen Elementen von G, welche durch beliebig häufige Anwendung von Inversionen und Gruppenoperationen entstehen kann, wobei wir die "leere Gruppenoperation" als e definieren (für den Fall $\langle \emptyset \rangle = \{e\}$.)

Satz 2.0.20. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Sei A eine Untergruppe von G und B eine Untergruppe von H. So ist $\varphi(A)$ eine Untergruppe von H und $\varphi^{-1}(B)$ eine Untergruppe von G.*

Satz 2.0.21. **Universelle Eigenschaft surjektiver Gruppenhomomorphismen:** *Sei $\varphi : G \twoheadrightarrow H$ ein surjektiver Gruppenhomomorphismus. Sei $\psi : G \to K$ ein Gruppenhomomorphismus, sodass $\ker \psi \supseteq \ker \varphi$. So existiert genau ein Gruppenhomomorphismus $\overline{\psi}$, sodass:*

$$\psi = \overline{\psi} \circ \varphi$$

Also sodass das folgende Diagramm kommutiert:



Beweis. Sei $\varphi(x) = \varphi(y)$, also $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(\varphi(y))$. Dann gilt

$$\varphi(xy^{-1}) = \varphi(1) = 1,$$

also $xy^{-1} \in \ker \varphi$, also $y \in x \cdot \ker \varphi$. Somit gilt

$$\varphi^{-1}(\varphi(g)) = g \cdot \ker \varphi.$$

Es gilt außerdem

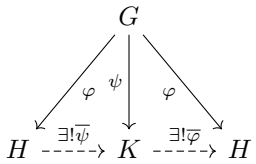
$$\psi(g \cdot \ker \varphi) = \psi(g) \cdot \psi(\ker(\varphi)) = \varphi(g),$$

also ist ψ konstant auf den Fasern (also den Urbildern einzelner Elemente) von φ. Somit existiert ein $\overline{\psi}$ Aufgrund der "universellen Eigenschaft surjektiver Funktionen", welche noch nicht eingeführt wurde :), folgt die Existenz eines $\overline{\psi}$ mit den gefragten Eigenschaften.

Zu zeigen ist noch, dass $\overline{\psi}$ ein Gruppenhomomorphismus ist.
Wähle hierfür $g \in G, g' \in G$ und $\varphi(g) = h$ und $\varphi(g') = h'$. Dann gilt

$$\overline{\psi}(hh') = \overline{\psi}(\varphi(gg')) = \psi(gg') = \psi(g) \cdot \psi(g') = \overline{\psi}(h) \cdot \overline{\psi}(h')$$

□



Die "Moral" dieses Satzes: Ein surjektiver Gruppenhomomorphismus $\varphi : G \twoheadrightarrow H$ wird durch $(G, \ker \varphi)$ "im wesentlichen eindeutig" festgelegt.

Die Frage ist nun, ob jede Untergruppe einer Gruppe G als Kern eines surjektiven Gruppenhomomorphismus festgelegt ist. Die Antwort auf diese Frage: Nein! Die einzigen Untergruppen, welche als solche Kerne auftreten, sind sogenannte **Normalteiler**.

Definition 2.0.22. Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt **Normalteiler**, falls

$$\forall g \in G : gN = Ng$$

Beispiel 2.0.23. Wir betrachten die Gruppe $Q \subset GL(2, \mathbb{R})$ aller linearen Abbildungen, welche ein Quadrat auf sich selbst abbilden. Prof. Soergel nennt diese Gruppe auch gerne die "Bierdeckelgruppe B". Die Gruppe hat acht Elemente:

- Die Rotationen d_0, d_1, d_2 und d_3 um Vielfache von 90°,
- die Spiegelungen s_x und s_y an den Koordinatenachsen,
- und die Spiegelungen s_+ und s_- an den Diagonalachsen.

Diese Gruppe ist nicht kommutativ! Zum Beispiel ist $d_1 s_+ = s_y$, aber $s_+ d_1 = s_x$ (Wir notieren die Elemente als Abbildungen, also wird links zuerst s_+ und dann d_1 angewandt.

Wir betrachten nun die Untergruppe $H = \langle s_+ \rangle$. So gilt $d_1 H = \{s_y, d_1\}$, aber $H d_1 = \{s_x, d_1\}$

Satz 2.0.24. *Der Kern eines Gruppenhomomorphismus ist immer ein Normalteiler.*

Beweis. Sei $\varphi : G \to H$. So ist $(\ker \varphi)x = \varphi^{-1}(\varphi(x)) = x(\ker \varphi)$. □

Satz 2.0.25. *Für jeden Normalteiler $N \subseteq G$ gibt es einen surjektiven Gruppenhomomorphismus $\varphi : G \twoheadrightarrow H$ mit $\ker \varphi = N$.*

> *Beweis.* Wir wählen $H := G/N = \{xN : x \in G\}$. Für je zwei Teilmengen $A, B \subseteq G$ definieren wir $AB = \{ab : a \in A, b \in B\}$ und erhalten eine assoziative Verknüpfung auf $\mathcal{P}(G)$. Für einen Normalteiler $N \subseteq G$ ist G/N unter dieser Verknüpfung stabil (geschlossen), denn durch Abuse of Notation folgt $xNyN = xyNN = xyN$. Unter dieser Verknüpfung wird G/N eine Gruppe mit neutralem Element $1N = N$ und $x^{-1}N = (xN)^{-1}$.
>
> Dadurch wird dann $\varphi : G \to G/N$, $x \to xN$ ein Gruppenhomomorphismus mit $\ker \varphi = N$. □

Beispiel 2.0.26. Die Menge $D \subsetneq Q$ der Drehungen eines Quadrats ist ein Normalteiler der vollen Symmetriegruppe Q.

> *Beweis.* Sei s eine Beliebige Spiegelung. So gilt $Ds = \{s_+, s_-, s_x, s_y\} = sD$. Einzelne Spiegelungen kommutieren also nicht mit einzelnen Gruppenelementen, es ist jedoch trotzdem eine Art "Kommutativität mit der Gruppe als Ganzes" vorhanden. □

Die Menge der Drehungen ist desweiteren gegeben als der Kern der Determinante, welche ein Gruppenhomomorphismus in die Gruppe mit zwei Elementen ist (genauer in die Gruppe $\{\pm 1, \cdot\}$).

Satz 2.0.27. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. So induziert φ einen Isomorphismus $G/\ker \varphi \to \mathrm{im}\varphi$.*

Sei G eine Gruppe mit $|G| = 5$. Gemäß Lagrange hat G nur die triviale Gruppe und sich selbst als Untergruppe. Sei $g \in G \setminus \{1\}$. So haben wir einen Gruppenhomomorphismus

$$\begin{aligned} \varphi : (\mathbb{Z}, +) &\to G \\ n &\mapsto g^n \end{aligned}$$

Wir wissen nun, das das Bild von φ eine Untergruppe von G bildet. Da $g \neq 1$ handelt es sich nicht um die triviale Gruppe, also ist $G = \mathrm{im}\varphi$.

$\ker \varphi \subsetneq \mathbb{Z}$ ist eine Untergruppe, also existiert genau ein $n \in \mathbb{N}$, sodass $\ker \varphi = \mathbb{Z}n$. Da G 5 Elemente hat, muss $n = 5$. Die einzige Gruppe mit 5 Elementen ist also $\mathbb{Z}/5\mathbb{Z}$.

Korollar 2.0.28. *Ist p eine Primzahl, so ist jede Gruppe mit p Elementen isomorph zu $\mathbb{Z}/p\mathbb{Z}$.*

Lemma 2.0.29. *Sei $\pi : G \to H$ ein surjektiver Gruppenhomomorphismus und $N \subseteq G$ ein Normalteiler. So ist $\pi(N)$ ein Normalteiler von H.*

Satz 2.0.30. **Noetherscher Isomorphiesatz:** *Sei G eine Gruppe und seien H und K Normalteiler. So ist H/K ein Normalteiler von G/K und die Komposition kanonischer Abbildungen $G \twoheadrightarrow G/K \twoheadrightarrow (G/K)/(H/K)$ induziert einen Isomorphismus $G/H \to (G/K)/(H/K)$*

Definition 2.0.31. Sei G eine Gruppe und $g \in G$. Wir definieren die Ordnung eines Elements als:

$$\operatorname{ord}(g) = \inf\{n \in \mathbb{N}_{\geq 1} \mid g^n = e\}$$

Erinnerung: Das Infimum der leeren Menge ist ∞, also gilt $\operatorname{ord}(g) = \infty$ falls kein solches n existiert.

Proposition 2.0.32. *Sei G eine Gruppe und $g \in G$.*

1. $\operatorname{ord}(g) = |\langle g \rangle|$
2. *$\langle g \rangle$ ist isomorph zu $\mathbb{Z}/(\operatorname{ord}(g))\mathbb{Z}$, falls die Ordnung endlich ist, und zu $\mathbb{Z}$, falls die Ordnung unendlich ist.*
3. *Falls $\operatorname{ord}(g) < \infty$, so gilt $g^n = e \Leftrightarrow \operatorname{ord}(g) \mid n$*

Definition 2.0.33. Sei G eine Gruppe. So heißt $|G|$ die **Ordnung** der Gruppe.

Satz 2.0.34. *Sei $g \in G$ ein Element einer endlichen Gruppe. So ist $\operatorname{ord}(g)$ ein Teiler von $|G|$.*

> *Beweis.* $\operatorname{ord}(g) = |\langle g \rangle|$. Nach Lagrange teilt die Größe der Untergruppe $\langle g \rangle$ die Größe der Gruppe G. □

Im Allgemeinen gibt es aber nicht für jeden Teiler ein Element mit der jeweiligen Ordnung. Zum Beispiel fehlt bei jeder nicht zyklischen Gruppe bereits die Ordnung selbst. Wohl aber gilt:

Satz 2.0.35. **Cauchy:** *Sei p eine Primzahl mit $p \mid |G|$. So gibt es ein $g \in G$ mit $\operatorname{ord}(g) = p$.*

Ein Beweis folgt aber erst später.

Korollar 2.0.36. *Sei $g \in G$ ein Element einer endlichen Gruppe. So gilt*

$$g^{|G|} = e.$$

> *Beweis.* $g^{|G|} = g^{r \cdot |\operatorname{ord}(g)|} = e^r = e.$ □

Satz 2.0.37. **Kleiner Satz von Fermat:** *Sei p eine Primzahl und $a \in \mathbb{Z}$. So gilt*

$$a^p \equiv a \mod p$$

Beweis. Wir betrachten $\mathbb{Z}/p\mathbb{Z}$. Falls $\alpha \equiv 0 \mod p$ ist die Aussage trivial. Da außerdem die Multiplikative Gruppe die Ordnung $p-1$ hat gilt im Fall $\alpha \not\equiv 0$ ebenfalls trivial $\alpha^{p-1} \equiv 1 \mod p$, also $\alpha^p \equiv \alpha \mod p$. □

Alternativ kann der Beweis auch auf "Allgemeinbildungsniveau" geführt werden:

Beweis. (Ohne Gruppentheorie): Sei $a \in \{0, \dots, p-1\}$. So sind die Zahlen $a, 2a, 3a, \dots, (p-1)a$ paarweise verschieden, also ist nach Schubfachprinzip ein Element jeder Restklasse $\mod p$ enthalten. Also gilt:

$$\begin{aligned} \prod_{k=1}^{p-1} ka &\equiv \prod_{k=1}^{p-1} k \mod p \\ \implies (p-1)!a^{p-1} &\equiv (p-1)! \mod p. \end{aligned}$$

Allerdings ist $(p-1)!$ teilerfremd zu p, also können wir durch $(p-1)!$ teilen und erhalten $a^{p-1} \equiv 1 \mod p$. □

Satz 2.0.38. *Seien $a, b \in \mathbb{N}_{\geq 1}$ teilerfremd. So induziert*

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ n &\mapsto (n + a\mathbb{Z}, n + b\mathbb{Z}) \end{aligned}$$

einen Isomorphismus:

$$\mathbb{Z}/ab\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Beweis. Nach Bézout gibt es $x, y \in \mathbb{Z}$ mit

$$xa + yb = 1.$$

Nun gilt:

$$\begin{aligned} n = xy = 1 - yb &\overset{\varphi}{\mapsto} (0, 1) \\ m = yb = 1 - xy &\overset{\varphi}{\mapsto} (1, 0) \end{aligned}$$

Diese Tupel bilden eine Basis des Bildraums, also ist φ surjektiv:

$$\begin{aligned} \varphi(\alpha n + \beta m) &= \varphi(\alpha n) + \varphi(\beta m) \\ &= \alpha\varphi(n) + \beta\varphi(m) \\ &= (\beta, \alpha) \end{aligned}$$

Da beide Seiten gleich viele Elemente haben handelt es sich sogar um einen Isomorphismus. □

Beispiel 2.0.39. Das Kongruenzensystem

$$\begin{aligned} n &\equiv 3 \mod 17 \\ n &\equiv 5 \mod 9 \\ n &\equiv 1 \mod 12 \end{aligned}$$

hat keine Lösung, denn aus $n \equiv 5 \mod 9$ folgt $n \equiv 2 \mod 3$, also $n \not\equiv 1 \mod 12$. Ersetzen wir jedoch 12 durch 13, so sind die Teiler teilerfremd und der chinesische Restsatz garantiert eine Lösung.

Satz 2.0.40. **Chinesischer Restsatz / Satz von Sunzi / Satz von Aryabhata:** *Satz 2.0.38 funktioniert auch für mehr als zwei Zahlen - sind $q_1, \ldots, q_r \in \mathbb{N}_{\geq 1}$ teilerfremd, so ist*

$$\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_r\mathbb{Z}$$

surjektiv und induziert eines Isomorphismus

$$\mathbb{Z}/q_1 \ldots q_r\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_r\mathbb{Z}$$

Genauer kann man isomorph jedem Element n das Tupel $(n \mod q_1, \ldots, n \mod q_r)$ zuordnen - so kommt man zurück zur "klassischen" Formulierung des Chinesischen Restsatzes.

Korollar 2.0.41. *Die Gruppe $\mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_r\mathbb{Z}$ wird durch das Element $(1, \ldots, 1)$ erzeugt und ist somit zyklisch.*

Lemma 2.0.42. **Zentrales Lemma der RSA-Verschlüsselung:** *Seien p und q prim und $st \equiv 1 \mod (p-1)(q-1)$. So ist $(a^t)^s \equiv \mod a \mod pq$.*

> *Beweis.* Wir wissen $a^x = a \mod p$ falls $x \equiv 1 \mod (p-1)$.
>
> Also $a^x = a \mod pq$, wenn $x \equiv 1 \mod (p-1)$ und $x \equiv 1 \mod (q-1)$, also insbesondere $a^x = a \mod p$ wenn $x \equiv 1 \mod (p-1)(q-1)$. □

In der RSA-Verschlüsselung werden dann letztendlich pq und t veröffentlicht, a^t als Nachricht zurückgeschickt, und dann durch Exponentiation mit s die Nachricht entschlüsselt.

Definition 2.0.43. Sei A eine abelsche Gruppe und p eine Primzahl. Wir definieren:

$$A(p) = \{a \in A \mid \exists n \in \mathbb{N} : \operatorname{ord}(a) = p^n\}$$

Satz 2.0.44. *Sei $(A, +)$ eine abelsche Gruppe. Für jede Primzahl p ist $A(p) \subseteq A$ eine Untergruppe.*

Beweis. Seien $x, y \in A(p)$. So existieren $r, s \in \mathbb{N}_{\geq 0}$, sodass $p^r x = p^s y = 0$. Da A abelsch ist folgt

$$p^{r+s}(x+y) = p^r x + p^s y = 0$$

Also $x + y \in A(p)$.

Es gilt außerdem $p0 = 0$, also $0 \in A(p)$, und $p^r(-x) = -(p^r x) = -0 = 0$, also $-x \in A(p)$. □

Satz 2.0.45. *Sei $(A, +)$ eine abelsche Gruppe und seien $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen. So liefert die Gruppenverknüpfung eine Injektion*

$$A(p_1) \times \ldots \times A(p_r) \hookrightarrow A$$

mit Bild alle Elemente endlicher Ordnung, in deren Ordnung nur die Primfaktoren $p_1, \ldots, p_r$ vorkommen.

Beweis. Sei sonst $(a_1, \ldots, a_r) \neq (0, \ldots, 0)$ ein Tupel mit $a_i \in A(p_i)$ und

$$a_1 + \ldots + a_r = 0.$$

Sei OBdA $a_1 \neq 0$. So gilt:

$$-a_1 = a_2 + \ldots + a_r$$

Für hinreichend großes n gilt nun

$$-(p_2 \ldots p_r)^n a_1 = (p_2 \ldots p_r)^n (a_2 + \ldots + a_r) = 0$$

Allerdings gilt

$$(p_2 \ldots p_r)^n a_1 \neq 0$$

Da die Primzahlen $p_2, \ldots, p_r$ alle die Ordnung von a_1 nicht Teilen. Widerspruch!

Sei nun $a \in A$, $\mathrm{ord}(a) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. So gilt:

$$\begin{aligned} \langle a \rangle &\cong \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z} \\ &= \mathbb{Z}/p_1^{\alpha_1} \ldots p_r^{\alpha_r}\mathbb{Z} \\ &\cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} \end{aligned}$$

□

Dieser Satz ist analog zur Hauptraumzerlegung eines Vektorraums - wir zerlegen A in eine direkte Summe aus Untergruppen. Es gibt in der kommutativen Algebra einen Satz

über Module über Ringe, welcher sowohl diesen Satz als auch die Hauptraumzerlegung gemeinsam verallgemeinert.

Korollar 2.0.46. *Sei E eine endliche abelsche Gruppe. Seien $p_1, \ldots, p_r$ die Primfaktoren der Kardinalität $|E|$ von E. So gilt:*

1. *Die Verknüpfung liefert eine Bijektion*

$$E(p_1) \times \ldots \times E(p_r) \xrightarrow{\sim} E$$

2. *Für alle i ist $|E(p_i)|$ eine Potenz von p_i.*

Beweis.

1. Folgt direkt aus dem vorherigen Satz, da die Elemente endlicher Ordnung, in deren Ordnung nur die Primfaktoren $p_1, \ldots, p_r$ vorkommen, nun die ganze Gruppe ausmachen.

2. Folgt aus Induktion über $|E_p|$. Der Fall $|E_p| = 1$ ist klar:

$$|E_p| = 1 = p^0$$

Für $|E_p| > 1$ existiert ein Element $x \neq 0$. Es gilt $|\langle x \rangle| = p^r$ nach Annahme. Dann folgt

$$|E(p)/\langle x \rangle| = p^s$$

nach Induktionsannahme, da der Quotient kleiner ist. Somit folgt nach Lagrange

$$|E_p| = |E(p)/\langle x \rangle| \cdot |\langle x \rangle| = p^s \cdot p^r$$

□

Proposition 2.0.47. *Sei E eine endliche abelsche Gruppe, sodass die Ordnung jedes $x \in E$ eine Potenz von p prim ist. So ist $|E|$ ebenfalls eine p-Potenz.*

Proposition 2.0.48. *Es existiert eine Bijektion zwischen der Menge der endlichen abelschen Gruppen bis auf Isomorphismus und den endlichen Multimengen echter Primpotenzen. Genauer hat jede endliche abelsche Gruppe die Form*

$$\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z}$$

Für $p_1, \ldots, p_r$ prim.

Zum Beispiel ist jede abelsche Gruppe der Ordnung 8 isomorph zu $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Satz 2.0.49. *Sei K ein Körper und $K^\times$ dessen multiplikative Gruppe. So ist jede endliche Untergruppe von $K^\times$ zyklisch.*

Definition 2.0.50. Sei G eine Gruppe und X eine Menge. Eine Operation von G auf X ist eine Abbildung

$$\begin{aligned} G \times G &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

Sodass:

1. $\forall g, h \in G : (gh)x = g(hx)$
2. $1x = x$

Beispiel 2.0.51. Sei X eine Menge und

$$\mathrm{Ens}^\times(X) := \{f : X \to X \mid f \text{ bijektiv}\}$$

So ist $\mathrm{Ens}^\times$ eine Gruppe, welche durch Anwendung der jeweiligen Funktion auf kanonische Weise auf X operiert:

$$\begin{aligned} \mathrm{Ens}^\times(X) \times X &\to X \\ (f, x) &\mapsto f(x) \end{aligned}$$

Beispiel 2.0.52. $\mathcal{S}_n$ operiert durch Anwendung der jeweiligen Permutation auf $\{1, \ldots, n\}$.

Beispiel 2.0.53. Analog operiert $\mathrm{GL}(n, \mathbb{R})$ auf $\mathbb{R}^n$.

Definition 2.0.54. Sei G eine Gruppe, welche auf eine Menge X operiert. So nennen wir für $x \in X$ die Menge

$$Gx = \{gx \mid g \in G\}$$

die **Bahn** von x.

Beispiel 2.0.55. Wir lassen die Gruppe $\mathrm{SO}(2)$ der zweidimensionalen Rotationsmatrizen auf $\mathbb{R}^2$ operieren. So ist die Bahn eines Vektors $\vec{v}$ der Kreis mit Radius $\|\vec{v}\|$.

Beispiel 2.0.56. Sei H eine Untergruppe einer Gruppe G. So operiert H durch die Gruppenoperation auf G und die Bahnen Hg sind genau die Nebenklassen.

Proposition 2.0.57. *Die Bahnen der Operation einer Gruppe auf einer Menge sind paarweise disjunkt.*

Proposition 2.0.58. *Die Bahnen der Operation eines Monoids auf einer Menge sind nicht umbedingt paarweise disjunkt.*

Definition 2.0.59. Sei G eine Gruppe, welche auf einer Menge X operiert. Sei $x \in X$. Wir nennen die Menge

$$G_x := \{g \in G \mid gx = x\}$$

die **Standgruppe** oder **Isotropiegruppe** von x.

Lemma 2.0.60. *Die Abbildung $G \to X : g \to gx$ induziert eine Bijektion*

$$G/G_x \xrightarrow{\sim} Gx$$

Beweisskizze. Für jede G_x-Linksnebenklasse $L \subset G$ besteht die Menge Lx nur aus einem Punkt. Falls $L = gG_x$ haben wir genauer $Lx = gG_xx = \{gx\}$. Wir können nun unsere Bijektion definieren, indem wir jeder Linksnebenklasse $L \in G/G_x$ das einzige Element von Lx zuordnen. Sie ist trivial surjektiv, gleichzeitig ist sie injektiv, denn aus $gG_xx = hG_xx$ folgt $gx = hx$, also $h^{-1}g \in G_x$, also $gG_x = hG_x$. "□"

Korollar 2.0.61. **Bahnformel:**

$$|G| = |Gx| \cdot |G_x| = |G/G_x| \cdot |G_x|$$

Frage: Was sind die endlichen Untergruppen der dreidimensionalen Drehgruppe SO_3?

Vorüberlegung: Jede Gruppe G mit $x \in G$ operiert auf sich selber durch $g.x = gxg^{-1}$, auch notiert als $(\text{int}g)(x)$ für "interior", da dies einen sogenannten **inneren Automorphismus** bildet. Es gilt nämlich:

$$\begin{aligned} \text{int} : G &\to \text{Aut}(G) \\ g &\mapsto (x \mapsto gxg^{-1}) \end{aligned}$$

Wir nennen diese Operation die "**Operation durch Konjugation**".

Dabei gilt:

$$\begin{aligned} (hg).x &= hgx(hg)^{-1} \\ &= hgxg^{-1}h^{-1} \\ &= h(gxg^{-1})h^{-1} \\ &= h.(g.x) \end{aligned}$$

und außerdem:

$$g.(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = (g.x)(g.y)$$

Intuitiv sind Drehungen, welche zueinander konjugiert werden können, "quasi die gleichen" - die Symmetriegruppe, welche den Raum an einer Achse um 180 Grad dreht, ist die gleiche, welche den Raum an einer anderen Achse um 180 Grad dreht. Es ist also sinnvoll, die Frage einzuschränken auf "Was sind die endlichen Untergruppen von SO_3 *bis auf Konjugation*? Die Antwort ist nun:

Satz 2.0.62. *Die endlichen Untergruppen der Drehgruppe SO_3 bis auf Konjugation sind genau:*

1. *Die zyklischen Gruppen C_k, für $k \geq 1$*
2. *Die **Diedergruppen** D_k, für $k \geq 2$ (die Verallgemeinerungen unserer Quadratgruppe)*
3. *Die Symmetriegruppen des Würfels (= die Symmetriegruppe des Oktaeders), des Tetraeders, und des Ikosaeders (= die Symmetriegruppe des Dodekaeders)*

Beweis.

Proposition 2.0.63. *$g \in SO_3 \setminus \mathrm{id}$ hält genau eine Gerade punktweise fest. Diese sticht an zwei Punkten durch die Einheitssphäre S^2.*
Wir nennen diese Punkte die Pole $P \subset S^2$ von g. Sei also $G \subset \mathrm{SO}(3)$ eine endliche Untergruppe. Wir definieren

$$M \in \{(g,p) \mid g \in G \setminus \mathrm{id}, p \in P\}$$

Als die Menge der Pole der Drehachsen der Gruppe. Es gilt

$$|M| = 2(|G| - 1)$$
$$|M| = \sum_{p \in P} (|G_p| - 1)$$

Die Gruppe operiert außerdem auf der Menge der Pole ($G \searrow P$). Wir können die Menge der Pole somit Zerlegen in ihre G-Bahnen, also $P \to P_1 \sqcup \ldots \sqcup P_r$. Die Ordnung der Pole einer Bahn ist konstant, wir definieren also die **Polordnung** der Pole der i-ten Bahn als

$$\forall p \in P_i : n_i := |G_p|$$

Und erhalten

$$\sum_{p \in P} (|G_p| - 1) = \sum_{i=1}^{r} |P_i| \cdot (n_i - 1)$$

Aus der Bahnformel erhalten wir

$$|P_i| \cdot n_i = |G|$$

Also gilt:

$$2(|G| - 1) = \sum_{i=1}^{r} |P_i| \cdot (n_i - 1)$$
$$\implies 2 - \frac{2}{|G|} = \sum_{i=1}^{r} 1 - \frac{1}{n_i}$$

Fall $r = 0$**:** Es gibt keine Pole, also ist die Gruppe trivial. Die triviale Gruppe kann auch betrachtet werden als die zyklische Gruppe C_1 mit nur einem Element.

Fall $r = 1$**:** Dann gilt:

$$2 - \frac{2}{|G|} = 1 - \frac{1}{n_1}$$

Die Gruppe muss mindestens 2 Elemente haben, also ist der linke Term größer als 1 und der rechte Term kleiner als 1, was ein Widerspruch ist.

Fall $r = 2$**:** Dann gilt:

$$2 - \frac{2}{|G|} = 2 - \frac{1}{n_1} - \frac{1}{n_2}$$

Es gilt $n_i \leq |G|$, also ist die Gleichung genau dann erfüllt, wenn $n_1 = n_2 = |G|$. Wir haben also eine Gruppe mit zwei Polen, deren Ordnung die Ordnung der gesamten Gruppe ist. Die ganze Gruppe hat also nur eine Symmetrieachse, die Gruppe muss dann eine zyklische Gruppe sein.

Fall $r = 3$**:** Dann gilt:

$$\begin{aligned} 2 - \frac{2}{|G|} &= 3 - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3} \\ \implies 1 + \frac{2}{|G|} &= \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \end{aligned}$$

Sei OBdA $n_1 \leq n_2 \leq n_3$. Behauptung: Dann muss $n_1 = 2$ sein.

Fall $3a$**:** $n_2 = 2$**:** Dann gilt $2n_3 = |G|$. Nach Bahnformel folgt $|P_3| = 2$. Bei einer Polbahn mit zwei Elementen müssen sich die Pole gegenüberliegen. Wir erhalten die Diedergruppe D_{n_3} - n_3 entspricht der zentralen Drehsymmetrie und n_1 und n_2 entsprechen den seitlichen Symmetrieachsen durch die Ecken und Kanten.

Fall $3a$**:** $n_2 > 2$**:**

$$\frac{1}{2} + \frac{1}{n_2} + \frac{1}{n_3} > 1 + \frac{2}{|G|}$$

Also $n_2 = 3$ und $n_3 = 3$ oder $n_3 = 4$ oder $n_3 = 5$. Der erste Fall liefert den Tetraeder, der zweite Fall den Würfel und der dritte Fall den Ikosaeder.

Fall $r \geq 4$**:** Die Gleichungen sind nicht mehr lösbar.

□

Definition 2.0.64. Eine Gruppe $G \neq 1$ heißt **einfach**, falls ihre einzigen Normalteiler

die triviale Gruppe 1 und die Gruppe G selbst sind.

Proposition 2.0.65. *Jede Gruppe mit Primzahlordnung ist einfach (also $\mathbb{Z}/p\mathbb{Z}$ für p prim). Diese Gruppen sind die einzigen abelschen einfachen Gruppen.*

Beweis. Satz von Lagrange. □

Proposition 2.0.66. *Für fast alle Körper k ist $GL(n,k)/k^\times$ einfach.*

Satz 2.0.67. *Die Ikosaedergruppe I ist einfach.*

Beweis. Wir haben:

- Ein Element der Ordnung 1 (die Identität)
- 15 Elemente der Ordnung 2 (Drehungen um Kantenmitten, da wir 30 Kanten haben und je zwei gegenüberliegende Kanten die selben Drehungen haben)
- 20 Elemente der Ordnung 3 (Drehungen um Flächenmitten, da wir 20 Flächen haben)
- Keine Elemente der Ordnung 4
- 24 Elemente der Ordnung 5 (Drehungen an Ecken, da wir 12 Ecken haben, an jeder Ecke vier Drehungen, aber je zwei gegenüberliegende Ecken die gleichen Drehungen haben)

Wir wollen die Elemente nun in Konjugationsklassen zerlegen. Die Elemente der Ordnung 2 und der Ordnung 3 bilden jeweils eine Konjugationsklasse. Die Drehungen um Ecken können jedoch nicht alle in der selben Konjugationsklasse liegen, da 24 kein Teiler von 60 ist. Die Drehungen um Ecken zerfallen also in zwei Konjugationsklassen - es handelt sich um die Drehungen um $2\pi/5$ (72°, "Eine Ecke weiter"), und die Drehungen um $4\pi/5$ (144, "zwei Ecken weiter"). Größere Drehungen existieren nicht, da eine Drehung drei Ecken weiter einer Drehung um zwei Ecken in die andere Richtung entspricht und eine Drehung vier Ecken weiter einer Drehung um eine Ecke in die andere Richtung entspricht.

Sei also nun N ein Normalteiler von I. So muss $|N|$ ein Teiler von $|I|$ sein, also $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

Proposition 2.0.68. *Sei N ein Normalteiler einer Gruppe G. So ist N eine Vereinigung von Konjugationsklassen von G.*

Aus der Proposition folgt, dass $|I|$ außerdem eine Summe von $1, 20, 15, 12, 12$ sein muss, wobei die 1 in der Sumume enthalten sein muss (da N sonst nicht

das neutrale Element enthalten würde). Die einzigen Möglichkeiten sind also $|N| = 1 = 1$ und $|N| = 60 = 1 + 20 + 15 + 12 + 12$. Also sind die einzigen Normalteiler von I die triviale Gruppe und I selbst. □

Proposition 2.0.69. *Die **alternierenden Gruppen***

$$A_r := \ker(\text{sgn} : \mathcal{S}_r \to \{\pm 1\})$$

sind für $r \geq 5$ einfach. (Wobei der Kern genau den Permutationen mit $\text{sgn}(\sigma) = 1$ entspricht). Insbesondere ist A_5 isomorph zur Ikosaedergruppe, und diese ist die kleinste nichtabelsche einfache Gruppe.

Beweis. Ein Ikosaeder hat die selbe Symmetriegruppe wie ein Dodekaeder, da die beiden Körper dual zueinander sind (also können die Ecken des einen den Flächenmitten des anderen zugeordnet werden und umgekehrt).

Proposition 2.0.70. *Ein Dodekaeder enthält fünf eingeschriebene Würfel.*

Wir erhalten einen Gruppenhomomorphismus $\varphi : I \to \mathcal{S}_5$, welcher beschreibt, wie eine Symmetrie des Ikosaeders/Dodekaeders die eingeschriebenen Würfel permutiert. So ist $\text{sgn} \circ \varphi$ ein Homomorphismus $I \to \{\pm 1\}$. Da I einfach ist und $|I| \geq 2$ ist $\ker(\text{sgn} \circ \varphi) = I$.

$\ker(\varphi)$ ist ein von I verschiedener Normalteiler, also ist $\ker(\varphi) = 1$, also ist φ injektiv. Es gilt $|I| = 60$ und $|\mathcal{S}_5| = 120 \implies |A_5| = 60$, also ist φ auch surjektiv, also bijektiv, also ein Isomorphismus. □

Definition 2.0.71. Eine **Kompositionsreihe** einer Gruppe G ist eine Folge von Untergruppen

$$1 = G_0 \subset G_1 \subset \ldots \subset G_{r-1} \subset G_r = G$$

sodass jedes G_i Normalteiler von G_{i+1} ist und alle **Subquotienten** G_i/G_{i-1} einfach sind.

Satz 2.0.72. **Jordan-Hölder:** *Je zwei Kompositionsreihen einer endlichen Gruppe G haben die selbe Länge und bis auf Reihenfolge die selben Subquotienten.*

Dieser Satz gibt uns eine "Primfaktorzerlegung" von Gruppen, in der die "Primfaktoren" die Subquotienten sind.

Beispiel 2.0.73. Sei $G = \mathbb{Z}/20\mathbb{Z}$. Eine mögliche Kompositionsreihe ist nun:

$$\mathbb{Z}/20\mathbb{Z} \supset 2\mathbb{Z}/20\mathbb{Z} \supset 10\mathbb{Z}/20\mathbb{Z} \supset 0$$

Die Subquotienten hier sind dann $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}$.

Proposition 2.0.74. *Es existiert eine universelle Eigenschaft surjektiver linearer Abbildungen, welche exakt analog zur universellen Eigenschaft surjektiver Gruppenhomomorphismen funktioniert.*

Eine lineare Abbildung ist also im Wesentlichen eindeutig durch ihren Kern bestimmt - alle surjektiven linearen Abbildungen mit dem selben Kern können durch Verkettung mit einem eindeutigen Isomorphismus ineinander überführt werden.

Proposition 2.0.75. *Für jeden Untervektorraum $U \subset V$ gibt es eine surjektive lineare Abbildung $s : V \twoheadrightarrow W$ mit $\ker s = U$. Dies ist genau die Abbildung $V \twoheadrightarrow V/U$.*

Proposition 2.0.76. *Für Vektorräume gilt $\dim V = \dim U + \dim V/U$. Diese Formel kann als Analogon zum Satz von Lagrange gesehen werden.*

Beispiel 2.0.77. Betrachte einen 3-dimensionalen Vektorraum V über $\mathbb{F}_7$. Eine mögliche Kompositionsreihe ist

$$V \supset W \supset U \supset \{0\}$$

mit $\dim W = 2$ und $\dim U = 1$. Die Subquotienten V/W, W/U und $U/\{0\}$ sind jeweils eindimensionale Untervektorräume von V, also isomorph zur additiven Gruppe von $\mathbb{F}_7$.

Beweis (Jordan-Hölder): Per Induktion über $|G|$. Ist $|G| = 1$, ist G die triviale Gruppe und somit insbesondere bereits alleine die vollständige Kompositionsreihe und die Aussage gilt trivial.

Seien nun $G \supset M \supset \ldots$ und $G \supset N \supset \ldots$ Kompositionsreihen. M und N müssen beide Ordnungen kleiner G haben, falls also $M = N$ ist gilt die Aussage per Induktion. Ist $N \neq M$, existiert ein surjektiver Homomorphismus $N \twoheadrightarrow G/M$ mit Kern $N \cap M$. Somit geht $N/N \cap M$ isomorph auf G/M.

Wir wissen also, dass der Subquotient G/M isomorph zu $N/N \cap M$ ist. Analog ist der Subquotient G/N isomorph zu $M/M \cap N$. Also sind $G \supset M \supset M \cap N \supset \ldots$ und $G \supset N \supset M \cap N \supset \ldots$ valide Kompositionsreihen, welche per Induktion äquivalent zu den ursprünglichen Kompositionsreihen sind. Somit folgt auch die gesuchte Aussage per Induktion. □

Definition 2.0.78. Sei p eine Primzahl. Eine endliche Gruppe G heißt **p-Gruppe**, wenn

$$|G| = p^n.$$

Definition 2.0.79. Sei G eine Gruppe. Das **Zentrum** Z einer Gruppe ist die Menge der Elemente, welche mit allen anderen Gruppenelementen kommutieren:

$$Z(G) = \{z \in G \mid \forall g \in G : zg = gz\}$$

Satz 2.0.80. *Sei G eine nichttriviale p-Gruppe. So ist auch das Zentrum von G nichttrivial.*

Beweis. Sei $|G| = p^r$. Wir zerlegen G in ihre Konjugationsklassen $C_1, \ldots, C_s$. $|C_i|$ teilt $|G| = p^r$, also haben insbesondere alle Konjugationsklassen eine p-Potenz als Ordnung.

Ist $|C_i| = 1$, gilt $C_i = \{z\}$ mit $z \in Z(G)$. Also:

$$|G| \equiv |Z(G)| \mod p$$

Ist $|G| \neq 1$, folgt $|Z(G)| \neq 1$. □

Satz 2.0.81. *Sei p prim und $|G| = p^2$. So ist G abelsch und isomorph zu $\mathbb{Z}/p^2\mathbb{Z}$ oder $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Wir wissen $Z(G) \neq 1$. Wäre $Z(G) \neq G$, so wäre $|Z(G)| = p$ und für $x \in G \setminus Z(G)$ wäre

$$\langle Z(G), x \rangle = G$$

Aber diese erzeugte Gruppe ist abelsch! Widerspruch!!!!!! □

Definition 2.0.82. Sei G eine endliche Gruppe, p eine Primzahl, und p^r die größte p-Potenz, die $|G|$ teilt. Eine Untergruppe $S \subset G$ mit $|S| = p^r$ heißt **p-Sylow** von G

Satz 2.0.83. *In jeder p-Gruppe $G \neq 1$ gibt es ein Element $g \in G$ der Ordnung p.*

Satz 2.0.84. *Jede p-Gruppe ist nilpotent.*

Satz 2.0.85. **Sylow-Sätze:** *Sei G eine endliche Gruppe und p prim, sodass p^r G maximal teilt.. So gilt:*

1. *Es gibt p-Sylows in G.*
2. *Je zwei p-Sylows in G sind zueinander konjugiert.*
3. *Jede Untergruppe $H \subset G$, deren Ordnung eine p-Potenz ist, liegt in einer p-Sylow.*
4. *Die Zahl der p-Sylows von G ist kongruent zu 1 modulo p und teilt $|G|/p^r$*

Beispiel 2.0.86. In der Würfelgruppe W ist $|W| = 24$. Ein 2-Sylow ist also eine Untergruppe mit Ordnung $2^3 = 8$. Davon gibt es drei, und zwar die Untergruppen, die Isomorph zur Diedergruppe D_4 sind.

Beweis (Erster Sylowsatz): Seien $C_1, \ldots, C_r$ die Konjugationsklassen von G. Wir können diese weiter Zerlegen in $C_1, \ldots, C_s$ mit $s < r$ und $Z(G)$. Wir wählen ein $g_i \in C_i$ und erhalten (warum?)

$$|G| = |G/Z_G(g_1)| + \ldots + |G/Z_G(g_s)| + |Z(G)|$$

Wobei $Z_G(x) = \{g \in G : gxg^{-1} = x\}$.

Wir führen nun einen Beweis durch Induktion durch. Gibt es ein i, sodass p^r $|Z_G(g_i)|$ teilt, dann folgt die Aussage direkt per Induktion.

Andernfalls teilt p $|G/Z_G(g_i)|$ für alle i, also teilt p auch $|Z(G)|$, also existiert ein $z \in Z(G)$ mit $\text{ord}(z) = p$.

Wir wissen $|G| = kp^r$ mit $k < p$, also gilt $|G/\langle z\rangle| = kp^{r-1}$. Insbesondere existiert eine Untergruppe $\bar{S} \subset G/\langle z\rangle$ mit $\left|\bar{S}\right| = p^{r-1}$, falls $k = 1$ ist dies die Gruppe $G/\langle z\rangle$ selbst. Wir definieren nun $S := \pi^{-1}(\bar{S}) \subset G$ - also ist S die Gruppe, die durch die Quotientenabbildung auf $\bar{S}$ abgebildet wird - und es folgt $|S| = p^r$. □

Lemma 2.0.87. *Sei G eine Gruppe. Sei*

$$\mathcal{S} = \{Q \subset G : |Q| = p^r\}$$

die Menge der p-Sylows von G. Ist $Q \in \mathcal{S}$ schreiben wir $g.Q = gQg^{-1}$ oder ist $x \in \mathcal{S}$ schreiben wir einfach $gx = gxg^{-1}$.

Ist $H \subset G$ eine p-Gruppe und $x = Q \in \mathcal{S}$ ein Fixpunkt von H in der Menge $\mathcal{S}$ der p-Sylows, so gilt $H \subset Q$.

Beweis. $\forall h \in H : hx = x$ bedeuted $\forall h \in H : hQ = Qh$. Daraus folgt, dass HQ eine Untergruppe von G ist.

Also gilt gemäß Bahnformel $|HQ| = |QH/H| \cdot |H|$. Wir wissen $|H| = p^r$, da QH/H eine Q-Bahn ist, gilt außerdem $|QH/H| = p^s$. Also ist die Ordnung von HQ ebenfalls eine p-Potenz. Da die p-Potenz, die die Ordnung von Q teilt, bereits maximal ist, folgt $|HQ| = |Q|$, also $HQ = Q$. □

Beweis (Zweiter Sylowsatz, Dritter Sylowsatz): Sei $P = x \in \mathcal{S}$ eine beliebige p-Sylow. Es gilt $P \subset G_P$, also gemäß Bahnformel $|GP| = |G|/|G_P|$, also teilt p nicht die Ordnung von GP. Ist jetzt also $H \subset G$ eine p-Gruppe, können wir GP in H-Bahnen $B_1, \ldots, B_r$ zerlegen. Da H eine p-Gruppe ist, ist für alle i

die Ordnung $|B_i|$ eine p-Potenz. Da p aber nicht $|GP|$ teilt, muss es B_i mit $|B| = 1$ geben. Also existiert ein $y \in GP \subset \mathcal{S}$, welche Fixpunkte von H sind. Also existiert ein Q der Gestalt gPg^{-1}, welches ein Fixpunkt von H ist, sodass $H \subset Q$. □

Beweis (Vierter Sylowsatz): Ganz $\mathcal{S}$ ist eine G-Bahn GP mit $P \in \mathcal{S}$ beliebig. Da es nur einen Fixpunkt gibt, und da alle Bahnen p-Potenzordnung haben, gilt $|\mathcal{S}| \equiv 1 \mod p$. Es gilt außerdem $|GP| = |G|/|G_p| \mid |G|/|P| = |G|/p^r$. □

Korollar 2.0.88. *Sei G eine endliche Gruppe und p eine Primzahl, die die Gruppenordnung teilt. So gibt es ein Element von G der Ordnung p.*

Beweis. Gemäß der Sylowsätze existiert ein p-Sylow und darin ein Element der Ordnung p. □

Korollar 2.0.89. *Jede Gruppe mit 6 Elementen ist isomorph zu $\mathcal{S}_3$ oder $\mathbb{Z}/6\mathbb{Z}$.*

Beweis. Gemäß Sylowsätzen existiert ein $a \in G$ mit $|\langle a \rangle| = 2$ und ein $b \in G$ mit $|\langle b \rangle| = 3$. Also gilt

$$\langle a \rangle \times \langle b \rangle \hookrightarrow G,$$

also

$$G = \{1, b, b^2, a, ab, ab^2\}$$

Es folgt, dass entweder $ba = ab$ oder $ba = ab^2$. Wählen wir eine dieser beiden Möglichkeiten ist bereits die gesamte Gruppe festgelegt. Der erste Fall ergibt $\mathbb{Z}/6\mathbb{Z}$, der zweite Fall ergibt $\mathcal{S}_3$. □

Chapter 3

Ringe

3.1 Grundbegriffe

Beispiel 3.1.1. Die Abbildung $\mathbb{Z} \to \mathbb{Z}$, welche jedes Element auf 0 abbildet, ist kein Ringhomomorphismus, da das Einselement auf das Nullelement abgebildet wird. Wohl aber ist für einen beliebigen Ring R die Abbildung $R \to 0$ in den Nullring ein Ringhomomorphismus.

Lemma 3.1.2. *Es gibt keinen Ringhomomorphismus $\varphi : \mathbb{Q} \to \mathbb{Z}$.*

Beweis. Es müsste gelten $\varphi(1) = 1$, also $\varphi(2) = 2$, und $\varphi(2) \cdot \varphi(\frac{1}{2}) = 2 \cdot \varphi(\frac{1}{2}) = 1$. Allerdings gibt es kein solches Element in $\mathbb{Z}$. □

Satz 3.1.3. *Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$.*

Beweis. Analog wie für einen Gruppenhomomorphismus aus einer zyklischen Gruppe:

Es gibt genau einen Gruppenhomomorphismus $\varphi : (\mathbb{Z}, +) \to (R, +)$ mit $1_{\mathbb{Z}} \to 1_R$. Dieser bildet auch einen Ringhomomorphismus, denn für natürliches a, b gilt:

$$\begin{aligned}
\varphi(a \cdot b) &= \sum_{i=1}^{ab} 1_R \\
&= \sum_{i=1}^{a} 1_R \cdot \sum_{i=1}^{b} 1_R && \text{(Induktiv per Distributivgesetz)} \\
&= \varphi\left(\sum_{i=1}^{a} 1\right) \cdot \varphi\left(\sum_{i=1}^{b} 1\right) \\
&= \varphi(a) \cdot \varphi(b)
\end{aligned}$$

Und für negative $a, b \in \mathbb{Z}$ folgt das Selbe, wenn man eine Summe bis zu einer negativen Zahl als Summe der Inversen definiert. □

Satz 3.1.4. *Sei R ein Ring. So ist $\ker(Z \to R) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$. Wir nennen dieses n die **Charakteristik** von R.*

Beweis. Jeder Ringhomomorphismus bildet einen Gruppenhomomorphismus. Der Kern muss also eine Untergruppe von $\mathbb{Z}$ sein, also die Form $n\mathbb{Z}$ haben. □

Satz 3.1.5. *Die Charakteristik von R ist das kleinste $m \geq 1$ mit $\sum_{i=1}^{m} 1_R = 0_R$, falls es ein solches m gibt, ansonsten 0.*

Beispiel 3.1.6.

- Es gilt $\text{char}(\mathbb{Z}) = \text{char}(bQ) = \text{char}(\mathbb{R}) = 0$.
- Der einzige Ring mit Charakteristik 1 ist der Nullring.
- $\text{char}(\mathbb{F}_p) = p$.

Satz 3.1.7. *Sei R ein Kring (kommutativer Ring) der Charakteristik p, mit p prim. So ist der **Frobeniushomomorphismus***

$$\begin{aligned} Fr : R &\to R \\ a &\mapsto a^p := \prod_{i=1}^{p} a \end{aligned}$$

ein Ringhomomorphismus.

Beweis. Es gilt:

- $\varphi(1) = 1)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$

  In der letzten Summe haben alle Terme außer dem ersten und dem letzten nun durch den Binomialkoeffizienten einen Faktor p und sind im Ring somit

0. Also

$$\begin{aligned}\sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} &= a^p + b^p \\ &= \varphi(a) + \varphi(b)\end{aligned}$$

□

Satz 3.1.8. **Universelle Eigenschaft surjektiver Ringhomomorphismen:** *Sei* $s : R \twoheadrightarrow Q$ *ein surjektiver Ringhomomorphismus und* $\varphi : R \to S$ *ein beliebiger Ringhomomorphismus. So existiert genau dann ein Ringhomomorphismus* $\bar{\varphi}$ *mit* $\bar{\varphi} \circ s = \varphi$*, wenn* $\ker \varphi \supseteq \ker s$*. Falls* $\bar{\varphi}$ *existiert, ist es eindeutig.*

Beweis. Es ist bereits bekannt, dass ein eindeutiger Gruppenhomomorphismus $\bar{\varphi}$ zwischen den additiven Gruppen existiert. Zu zeigen ist, dass $\bar{\varphi}$ ein Ringhomomorphismus ist. Dies ist jedoch simpel - es gilt:

- $\bar{\varphi}(1_Q) = (\bar{\varphi} \circ s)(1_R) = \varphi(1_Q) = 1_S$
- Da s surjektive ist, reicht für die Multiplikativität $\bar{\varphi}(s(a) \cdot s(b)) = \bar{\varphi}(s(a)) \cdot \bar{\varphi}(s(b))$.

$$\begin{aligned}\bar{\varphi}(s(a) \cdot s(b)) &= \bar{\varphi}(s(ab) \\ &= \varphi(ab) \\ &= \varphi(a) \cdot \varphi(b) \\ &= \bar{\varphi}(s(a)) \cdot \bar{\varphi}(s(b))\end{aligned}$$

□

Wie im Fall für Gruppen existiert also genau ein Ringisomorphismus zwischen den Bildern zweier Ringhomomorphismen mit gleichem Kern. Wir fragen uns nun: Gegeben einen Ring R - welche Untergruppen von $(R, +)$ sind Kerne von Ringhomomorphismen? Die Antwort sind **Ideale**.

Definition 3.1.9. Eine Untergruppe I der Additiven Gruppe $(R, +)$ eines Rings R heißt **Ideal**, falls $RI \subset I$ und $IR \subset I$ (also wenn das Produkt eines Ideals mit einem beliebigen Ringelement immer im Ideal liegt)

Definition 3.1.10. Ein zyklisches Ideal heißt **Hauptideal**.

Lemma 3.1.11. *Sei* $\varphi : R \to S$ *ein Ringhomomorphismus. So ist* $\ker \varphi \subset R$ *ein Ideal.*

Beweis. $\varphi(x) = 0 \implies \varphi(ax) = \varphi(xa) = 0$ □

Satz 3.1.12. *Gegeben einen Ring R mit Ideal I gibt es einen surjektiven Ringhomomorphismus $s : R \twoheadrightarrow Q$ mit Kern I.*

Beweis. Betrachte die Gruppe $(R/I, +)$. Wir behaupten, dass es darauf genau eine Multiplikation gibt, die verträglich ist mit $\varphi : R \to R/I$. Zu zeigen ist nur, dass die Abbildung $s \circ \cdot_R$ konstant auf den Fasern von $s \times s : R \times R \to R/I \times R/I$ ist. Diese Fasern haben genau die Form $(a + I) \times (b + I)$. Es gilt:

$$\begin{aligned} (a+I) \circ (b+I) &= ab + aI + Ib + II \\ \implies s(ab + aI + Ib + II) &= ab + I \end{aligned}$$

(Da $aI + Ib + II \subset I$.) □

Satz 3.1.13. *$n \in \mathbb{N}$ lässt beim Teilen durch 9 den selben Rest wie seine Quersumme und beim Teilen durch 11 den selben Rest wie seine alternierende Quersumme.*

Beweis. $10^n \equiv 1^n \mod 9$ und $10^n \equiv -1^n \mod 11$ □

Definition 3.1.14. Sei R ein Kring.

1. Seien $a, b \in R$. Wir sagen, a **teilt** b, falls ein $c \in R$ existiert, sodass $ac = b$.
2. Ein Element $a \in R$ heißt **kürzbar**, wenn die Multiplikation $a\cdot : R \to R$ injektiv ist, also wenn $ax = ay \implies x = y$.
3. R heißt **Integritätskring**, wenn genau ein nicht kürzbare Element in R existiert (Dieses ist dann zwingend die 0_R).

Beispiel 3.1.15.

- Alle $a \in \mathbb{Z} \setminus 0$ sind kürzbar.
- $\mathbb{Z}/12\mathbb{Z}$ ist kein Integritätsring, da $3 \cdot 4 = 3 \cdot 8 = 3 \cdot 0$. Im Allgemeinen ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Integritätsring, wenn m prim ist.
- Jeder Körper ist ein Integritätsring.
- Jeder Teilring eines Körpers ist ein Intergritätsring.

Korollar 3.1.16. *Die Ringmultiplikation ist genau dann injektiv, wenn ihr Kern trivial ist, also wenn der Ring Nullteilerfrei ist.*

Lemma 3.1.17. *Jeder endliche kommutative Integritätsring R ist ein Körper.*

Beweis. Sei $a \in R \setminus 0$ kürzbar. Dann ist die Multiplikation mit a injektiv. Da R endlich ist, ist die Multiplikation auch bijektiv, also existiert ein multiplikatives Inverses. Jeder kommutative Ring mit multiplikativen Inversen ist per Definition ein Körper. □

Korollar 3.1.18. *Die Charakteristik eines Körpers ist* 0 *oder eine Primzahl.*

Beweis. $\mathbb{Z}/(\mathrm{char}K)\mathbb{Z} \hookrightarrow K$ ist injektiv. Dies ist nur möglich, wenn $(\mathrm{char}K)$ 0 oder prim ist. □

Definition 3.1.19. Sei R ein kommutativer Ring. $a \in R$ heißt **Einheit**, wenn es ein multiplikatives Inverses gibt. Einheiten sind also quasi die "Einsteiler". Wir schreiben die Menge der Einheiten als $R^\times$ (da die Einheiten die größte multiplikativen Gruppe des Rings bilden).

Beispiel 3.1.20.

- $\mathbb{Z}^\times = \{-1, 1\}$
- $\mathbb{Q}^\times = \mathbb{Q} \setminus 0$
- $0^\times = 0$
- $\mathbb{R}[X]^\times = \mathbb{R}^\times$

In der Physik hat man einen eindimensionalen $\mathbb{R}$-Vektorraum V der Länge, der Zeit, etc. Die Einheiten sind genau die Basen dieses Vektorraums, also bildet die Multiplikation eine Bijektion $\mathbb{R} \xrightarrow{\sim} V$. Analog ist die Multiplikation mit einer Einheit eine Bijektion $R \xrightarrow{\sim} R$.

Korollar 3.1.21. *In jedem endlichen kommutativen Ring sind die Einheiten genau die kürzbaren Elemente.*

Beispiel 3.1.22.

- $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$
- $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \mid \mathrm{ggT}(a, m) = 1\}$

Definition 3.1.23. **Diffie-Hellman-Verschlüsselung:**

1. Alice wählt eine beliebige Gruppe G und eine natürliche Zahl $a \in \mathbb{N}$. Sie wählt ein Element $g \in G$ und veröffentlicht G, g^a und g.
2. Daraufhin wählt Bob ein $b \in \mathbb{N}$ und sendet g^b.
3. Alice rechnet nun $(g^b)^a$ und Bob rechnet $(g^a)^b$. Dies ist der gemeinsame geheime Schlüssel.

Die Sicherheit des Algorithmus beruht darauf, dass der diskrete Logarithmus (also das berechnen von a aus g^a) im Allgemeinen sehr ineffizient ist. Die häufigste Wahl ist $G = (\mathbb{Z}/p\mathbb{Z})^\times$ für eine sehr große Primzahl p, in besonders sicherheitskritischen Fällen wird als Gruppe oft eine elliptische Kurve über einem endlichen Körper genommen.

3.2 Polynomringe

Definition 3.2.1. Sei R ein Ring und $R[X]$ der Polynomring. Formell kann $R[X]$ auch definiert werden als die Menge aller Abbildungen $\mathbb{N} \to R$, die höchstens an endlich vielen Stellen $\neq 0$ sind (diese Stellen entsprechen dann den Koeffizienten.) Wir unterscheiden zwischen *Polynomen* und *Polynomfunktionen* - Im Allgemeinen ist die kanonische Abbildung $\mathbb{F}_p[X] \hookrightarrow \mathrm{Ens}(\mathbb{F}_p, \mathbb{F}_p)$ nämlich nicht injektiv!

Lemma 3.2.2. *Im Fall eines endlichen Körpers $\mathbb{F}_p$ ist die kanonische Abbildung $\mathbb{F}_p[X] \twoheadrightarrow \mathrm{Ens}(\mathbb{F}_p, \mathbb{F}_p)$ surjektiv. Der Kern dieser Abbildung ist das Ideal, welches von $(x^p - x)$ erzeugt wird.*

Proposition 3.2.3. *Sei R ein kommutativer Ring und $c \in R$. So gibt es genau einen Ringhomomorphismus*

$$E_c : R[X] \to R,$$

sodass $E_c(X) = c$ und $E_c \circ \imath = \mathrm{id}$. (Wobei $\imath$ die kanonische Einbettung $R \to R[X]$ ist, welche ein Element als konstantes Polynom auffasst. Professor Soergel schreibt diese auch als can.*)*

*Wir nennen E_c den **Einsetzungshomomorphismus** und schreiben abkürzend*

$$P(c) := E_c(P)$$

Proposition 3.2.4. *Sei $\varphi : R \to S$ ein Ringhomomorphismus und $c \in S$ (nicht $c \in R$!) ein Element, welches für alle $r \in R$ mit $\varphi(r)$ bezüglich der Multiplikation kommutiert. So gibt es genau einen Ringhomomorphismus*

$$E_{c,\varphi} : R[X] \to S$$

mit $E_{c,\varphi}[X] = c$ und $E_{c,\varphi} \circ \imath = \varphi$.

Diese Proposition verallgemeinert die Vorherige, indem sie uns zum Beispiel erlaubt, Matrizen oder komplexe Zahlen in reelle Polynome einzusetzen.

Proposition 3.2.5. *Jeder Ringhomomorphismus $\varphi : R \to S$ liefert einen Ringhomomorphismus $\varphi[X] : R[X] \to S[X]$.*

Definition 3.2.6. Sei R ein kommutativer Ring und $P \in R[X]$. Ein Element $\lambda \in R$ heißt **Nullstelle von** P, falls $P(\lambda) = 0$.

Definition 3.2.7. Der **Grad** eines Polynoms ist definiert als:

$$\deg(P) = \begin{cases} n & \text{Falls } P = a_n x^n + \ldots + a_0 x^0, a_n \neq 0 \\ -\infty & \text{Falls } P = 0. \end{cases}$$

Korollar 3.2.8. *Sei R ein Integritätsring und $P, Q \in R[X]$. Dann gilt*

$$\deg(PQ) = \deg(P) + \deg(Q)$$

Unser Ziel ist es, folgenden Satz zu beweisen:

Satz 3.2.9. *Sei R ein kommutativen Integritätsring und $P \in R[X] \setminus 0$. Dann hat P höchstens* $\deg(P)$ *Nullstellen.*

> *Beweisskizze.* Die kommutativen Integritätsringe sind genau die Ringe, über denen die gewohnte Zerlegung in Linearfaktoren funktioniert. "□"

Gegenbeispiel 3.2.10. Sei $R = \mathrm{Ens}(M, \mathbb{R})$. Dann ist R ein Ring, aber kein Integritätsring. So hat das Polynom $X^2 - X$ unendlich viele Nullstellen, nämlich alle Abbildungen $f : M \to \{0, 1\}$.

Gegenbeispiel 3.2.11. Ebenso gilt der Satz nicht für nichtkommutative Ringe. Es existieren zum Beispiel Zahlreiche Matrixringe, welche idempotente Matrizen enthalten, also Matrizen M mit $M^n = I$. Somit sind alle skalaren Vielfachen dieser Matrizen Nullstellen von X^n.

Satz 3.2.12. *Sei k ein kommutativer Ring und $P, Q \in k[X]$, wobei Q normiert ist (also Leitkoeffizient* 1 *hat.) Dann existieren eindeutige $A, B \in k[X]$, sodass*

$$P = A \cdot Q + B$$

Wobei $\deg B \leq (\deg Q) - 1$

Beispiel 3.2.13. Der Quotientenring $\mathbb{R}[X]/\left\langle X^2 + 1 \right\rangle$ ist isomorph zu den Komplexen Zahlen (Da $X^2 + 1 = 0 \implies X^2 = -1 \implies i := X$

Satz 3.2.14. *Sei $P \in \mathbb{R}[X]$ ein Polynom vom Grad* 2 *ohne reelle Nullstellen, und sei $\alpha \in \mathbb{C}$ mit $P(\alpha) = 0$. Dann gilt $\mathbb{R}[X]/\langle P \rangle \xrightarrow{\sim} \mathbb{C}$.*

Satz 3.2.15. *Sei R ein Ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subset R$ Ideale mit $i \neq j \implies \mathfrak{a}_i + \mathfrak{a}_j = R$. So ist die durch Restklassen gegebene Abbildung φ eine Surjektion $R \twoheadrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_j$.*

> *Beweis.* Die Abbildung ist klar ein Ringhomomorphismus. Es reicht also zu zeigen, dass alle "Einheitsvektoren" $(0, \ldots, 0, 1, 0, \ldots, 0)$ im Bild liegen, da dann der Rest durch Linearkombination folgt.

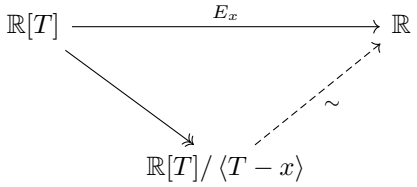
OBdA reicht $(1, 0, \dots, 0) \in \mathrm{im}(\varphi)$. Es gilt:

$$\begin{aligned} & \mathfrak{a}_1 + \mathfrak{a}_i = R \\ \Longrightarrow\ & \exists a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_i : a_i + b_i = 1 \\ \Longrightarrow\ & 1 - a_i = b_i \\ \Longrightarrow\ & \varphi_1(1 - a_i) = [1 - a_i]_{\mathfrak{a}_1} = 1, \\ & \varphi_i(1 - a_i) = [b_i]_{\mathfrak{a}_i} = 0 \\ \Longrightarrow\ & \varphi\left(\prod_{i \geq 2}(1 - a_i)\right) = (1, \dots, 0) \end{aligned}$$

□

Korollar 3.2.16. **Polynominterpolation:** *Gegeben $x_1, \dots, x_r \in \mathbb{R}$ paarweise verschieden und $y_1, \dots, y_r \in \mathbb{R}$ beliebig gibt es ein Polynom $P \in \mathbb{R}[T]$, sodass $\forall i : P(x_i) = y_i$.*

Beweis.



The rest should be entirely obvious and is left as an exercise to the reader. (Maybe coming later :) □

Führt man eine Polynominterpolation durch, findet man die "Basisvektoren", indem man pro x_i für alle x_j die Geraden durch (x_i, y_0) und $(x_j, 0)$ miteinander multipliziert. Diese werden dann aufsummiert. Letztendlich führt man also die selbe Rechnung durch wie in unserem abstrakteren Beweis über Ideale.

Satz 3.2.17. *Es gilt zusätzlich $\ker \varphi = \bigcap_{i=1}^{r} \mathfrak{a}_i$. Ist R kommutativ, ist dies außerdem äquivalent zu $\langle \mathfrak{a}_1 \mathfrak{a}_2 \dots \mathfrak{a}_r \rangle$.*

Beweis. Seien $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ und R kommutativ mit $\mathfrak{a}_1 + \mathfrak{a}_2 = R$. Wir zeigen $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle \mathfrak{a}_1 \mathfrak{a}_2 \rangle$. Die Richtung $\mathfrak{a}_1 \cap \mathfrak{a}_2 \supseteq \langle \mathfrak{a}_1 \mathfrak{a}_2 \rangle$ ist klar.

Es existieren $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, sodass $a_1 + a_2 = 1$. Dann gilt insbesondere

$$\begin{aligned} & \forall x \in \mathfrak{a}_1 \cap \mathfrak{a}_2 : \\ & a_1 x + a_2 x = x \end{aligned}$$

Also $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \langle \mathfrak{a}_1\mathfrak{a}_2 \rangle$, also auch $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \langle \mathfrak{a}_1\mathfrak{a}_2 \rangle$. Der Rest folgt durch Induktion. □

Korollar 3.2.18.

$$\mathbb{R}[T]/\left\langle X^2 - 1 \right\rangle \cong \mathbb{R}[T]/\left\langle X + 1 \right\rangle \times \mathbb{R}[T]/\left\langle X - 1 \right\rangle \cong \mathbb{R} \times \mathbb{R}$$

3.3 Irreduzible Elemente und Faktorielle Ringe

Wir wollen nun eine "Primfaktorzerlegung" für beliebige Ringe definieren:

Definition 3.3.1. Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt **irreduzibel in** R, falls es weder eine Einheit ist noch sich als Produkt von zwei Nichteinheiten darstellen lässt, also:

$$a = bc \implies b \in R^\times \vee c \in R^\times$$

Definition 3.3.2. Ein kommutativer Ring R heißt **faktoriell**, wenn

1. R ein Integritätsring ist,
2. Jedes $a \in R \setminus (R^\times \cup \{0\})$ ist Produkt von irreduziblen Elementen $a = p_1 p_2 \dots p_r$
3. Ist $p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, so ist $s = r$ und es gibt eine Permutation $\sigma \in \mathcal{S}_r$ und ein $u_i \in R^\times$, sodass für alle i

$$p_i = u_i q_{\sigma(i)}$$

Proposition 3.3.3. *Der Ring $C(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen $\mathbb{R} \to \mathbb{R}$ ist nicht faktoriell, zum Beispiel ist die Funktion $|x|$ kein Produkt von irreduziblen Funktionen, da wir die Funktion als ein beliebig langes Produkt von Wurzeln von sich selbst schreiben können.*

Proposition 3.3.4. *$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist nicht faktoriell.*

Beweis. Es gilt $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Alle dieser Faktoren sind irreduzibel. □

Definition 3.3.5. Ein kommutativer Integritätsring R heißt **euklidisch**, falls man "mit Rest teilen kann", also "der Euklidische Algorithmus funktioniert". Formell bedeutet das, dass es eine Abbildung

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

gibt, sodass für alle $a, b \in R$ mit $b \neq 0$ $q, r \in R$ existieren, sodass

$$a = b \cdot q + r$$

und $r = 0$ oder $\sigma(b) > \sigma(r)$.

Anmerkung 3.3.6. Die Abbildung σ kann durch eine Abbildung in eine beliebige wohlgeordnete Menge ersetzt werden.

Beispiel 3.3.7.

1. $R = \mathbb{Z}$, $\sigma(n) = |n|$.
2. $R = K[X]$ (für einen beliebigen Körper K), $\sigma(P) = \deg(P)$.
3. $R = \mathbb{Z}[i]$, $\sigma(a + bi) = a^2 + b^2$. (Ausführlicher später).

Satz 3.3.8. *In einem euklidischen Ring R ist jedes Ideal I ein Hauptideal.*

Beweis. Falls $I = \langle 0 \rangle$, so sind wir fertig. Falls $I \neq \langle 0 \rangle$ gibt es ein $b \in I \setminus 0$ mit kleinstmöglichem $\sigma(b)$. So gilt $I = \langle b \rangle$, denn falls $a \in I \setminus Rb$, so wäre $a = b \cdot q + r$, mit $r \neq 0$, $\sigma(r) < \sigma(b)$ und $r = a - bq \in I$. Widerspruch!!!!!! □

Beispiel 3.3.9. Sei K ein Körper und $A \in \mathrm{Mat}(n \times n, K)$. So ist

$$I = \{P \in K[X] \mid P(A) = 0\}$$

ein Ideal, welches vom Minimalpolynom von A erzeugt wird.

Definition 3.3.10. Ein Integritätsring R, welcher kein Körper ist und in dem jedes Ideal ein Hauptideal ist, heißt **Hauptidealring**.

Anmerkung 3.3.11. Körper werden aus den Hauptidealringen ausgeschlossen, da man später in der kommutativen Algebra gerne hätte, dass die faktoriellen Ringe der *Krull-Dimension* 1 die Hauptidealringe sind und die der Dimension 0 die Körper.

Satz 3.3.12. *Jeder Hauptidealring ist faktoriell.*

Beweis.

1. Zeige: Jedes $r \in R \setminus (R^\times \cap \{0\})$ ist ein Produkt $r = p_1 \dots p_r$, $r \geq 1$, mit p_i irreduzibel.

   Sei $r \in R$ ein Gegenbeispiel. Dann gilt:

   - $r \notin R^\times$.
   - $r \neq 0$.
   - r ist nicht irreduzibel.

   Also $r = r_1 \cdot r'$, mit $r_1, r' \notin R^\times$. Also ist entweder r_1 oder r_2 auch ein Gegenbeispiel. Ohne Beschränkung der Allgemeinheit sei dies r_1. Wir wissen nun, dass $\langle r_1 \rangle \supsetneq \langle r \rangle$ sein muss, da r' keine Einheit ist und somit r_1

kein Vielfaches von r sein kann. Wir faktorisieren weiter und finden eine Kette

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \dots$$

Da diese Ideale jeweils ineinander liegen ist diese Vereinigung ein Ideal, also insbesondere ein Hauptideal. Somit existiert ein Element $k \in R$, welches dieses Ideal erzeugt. Insbesondere existiert ein i, sodass $k \in \langle r_i \rangle$. Dann muss aber

$$\langle r_i \rangle = \langle r_{i+1} \rangle = \dots$$

gelten. Widerspruch!

2. Zeige: Die Faktorisierung ist eindeutig. Wir zeigen allgemeiner: Ist p irreduzibel mit $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$. Äquivalent dazu ist: $p \mid ab \wedge \neg(p \mid a) \implies p \mid b$.

   Wir betrachten nun das Ideal $\langle p, a \rangle$. Dieses muss ein Hauptideal $\langle c \rangle$ sein. Dann gilt $c \mid p$ und $c \mid a$. Da p irreduzibel ist gilt $c \in R^\times$ oder $c \in R^\times p$. Da p a nicht teilt, kann c kein Vielfaches von p sein. Also ist c eine Einheit. Das von p und a erzeugte Ideal ist also R. Es folgt

   $$xp + ya = 1,$$

   also

   $$xpb + yab = b.$$

   Nun gilt trivial $p \mid xpb$. Wir wissen außerdem $p \mid ab$, also $p \mid yab$. Es folgt $p \mid b$.

   Die Eindeutigkeit der Faktorisierung folgt nun genau wie im Fall der ganzen Zahlen.

□

Korollar 3.3.13. *Für jeden Körper K existiert eine Bijektion, gegeben durch die Multiplikation, zwischen Multimengen von irreduziblen $K[X]$-Polynomen und normierten $K[X]$-Polynomen.*

Proposition 3.3.14. *Über algebraisch abgeschlossenen Körpern haben alle irreduziblen Polynome den Grad* 1.

Definition 3.3.15. Ein Ideal eines Rings heißt **echtes Ideal**, wenn es nicht der ganze Ring ist. Es heißt außerdem **maximales Ideal**, falls es keine echte Teilmenge eines echten Ideals ist.

Proposition 3.3.16. *Ein Ideal ist genau dann maximal, wenn es ein von einem irreduziblen Element erzeugtes Hauptideal ist.*

Proposition 3.3.17. *Ein Ring ist genau dann ein Körper, wenn das einzige maximale Ideal das Nullideal ist.*

Satz 3.3.18. *Sei R ein Hauptidealring und $a \in R \setminus \{0\}$. So ist $R/\langle a \rangle$ genau dann ein Körper, wenn $\langle a \rangle$ maximal ist.*

3.4 Gaußprimzahlen und Summen zweier Quadrate

Lemma 3.4.1. *Der Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen ist euklidisch und faktoriell.*

Definition 3.4.2. Wir nennen die irreduziblen Elemente von $\mathbb{Z}[i]$ **Gaußprimzahlen**. Außerdem nennen wir die Einheiten von $\mathbb{Z}[i]$ **Gaußeinheiten**.

Proposition 3.4.3. *Es gibt genau vier Gaußeinheiten, nämlich*

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$$

Lemma 3.4.4.

1. *Jede Gaußprimzahl $\pi \in \mathbb{Z}[i]$ teilt genau eine Primzahl $p \in \mathbb{N}$.*
2. *Jede Primzahl $p \in \mathbb{N}$ ist entweder Gaußprim oder zerfällt in das Produkt einer Gaußprimzahl mit ihrer Konjugierten.*

Beweis.

1. Sei $\pi \in \mathbb{Z}[i]$ gaußprim. So ist π nicht Null und keine Gaußeinheit. Somit gilt $\pi\bar{\pi} > 1$. Aus $\pi \mid \pi\bar{\pi}$ folgt $\pi \mid p$ für mindestens einen Primteiler p von $\pi\bar{\pi}$, also teilt π mindestens eine Primzahl. Angenommen, es gilt $\pi \mid p$ und $\pi \mid q$ für Primzahlen p und q. Dann folgt sofort $\pi\bar{\pi} \mid p^2$ und $\pi\bar{\pi} \mid q^2$, also $p = q$, da $\pi\bar{\pi}$ keine Einheit ist.
2. Gegeben eine Primzahl p würde jede Zerlegung $p = \alpha\beta\gamma$ in Nichtgaußeinheiten in $\mathbb{Z}[i]$ eine Zerlegung in Nichteinheiten $p^2 = (\alpha\bar{\alpha})(\beta\bar{\beta})(\gamma\bar{\gamma})$, woraus folgen würde, dass p nicht Prim ist. Folglich ist jede Primzahl das Produkt von höchstens zwei Gaußprimzahlen α und β. Dann folgt sofort $p^2 = (\alpha\bar{\alpha})(\beta\bar{\beta})$, also $p = \alpha\bar{\alpha} = \beta\bar{\beta}$, also $\beta = \bar{\alpha}$.

□

Proposition 3.4.5. *Es gilt:*

- $2 = (1+i)(1-i)$.
- 3 *ist Gaußprim.*

- $5 = (1+2i)(1-2i)$.
- 7 *ist Gaußprim.*
- 11 *ist Gaußprim.*
- $13 = (2+3i)(2-3i)$

Anmerkung 3.4.6. Die 2 spielt hier eine seltsame Sonderrolle, da $(1+i) = i(1-i)$, also $2 = i(1-i)^2$. Die 2 hat also bis auf Einheiten nur einen Gaußprimfaktor - alle anderen Primzahlen haben selbst bis auf Einheiten zwei Gaußprimfaktoren.

Satz 3.4.7. *Für eine Primzahl $p \in \mathbb{N}$ ist gleichbedeutend:*

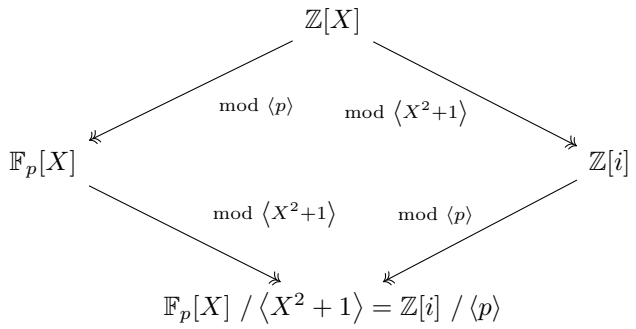
1. *p ist nicht gaußprim;*
2. *p ist eine Summe von zwei Quadraten;*
3. *$p \equiv 1 \mod 4$ oder $p \equiv 2 \mod 4$;*
4. *Das Polynom X^2+1 ist nicht irreduzibel in $\mathbb{F}_p[X]$;*
5. *(-1) ist ein Quadrat in $\mathbb{F}_p$.*

Beweis.

$1 \iff 2$**:** Sei p nicht gaußprim. So gilt $p = \pi\bar{\pi}$. Für $\pi = x+iy$ folgt dann $p = x^2+y^2$. Umgekehrt folgt auch aus $p = x^2+y^2$ direkt $p = (x+iy)(x-iy)$, also ist p nicht Gaußprim.

$2 \implies 3$**:** Die Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind 0 und 1. Somit muss eine Summe von zwei Quadraten modulo 4 kongruent zu $0, 1$ oder 2 sein. Ist die Summe 0, so ist p ein Vielfaches von 4, also nicht prim.

$1 \iff 4$**:** Wir betrachten folgendes Diagramm:



dieses kommutiert gemäß universeller Eigenschaft der Quotientenabbildung.

Somit ist $\langle X^2+1 \rangle$ genau dann nicht irreduzibel, wenn $\mathbb{Z}[i]/\langle p \rangle$ kein Körper ist, also wenn p nicht irreduzibel ist.

$3 \implies 5$**:** Sei $p \equiv 1 \mod 4$. So gilt $p - 1 = 4m$, also

$$\left|\mathbb{F}_p^\times\right| = p - 1 = 4m,$$

also:

$$\left|\mathbb{F}_p^\times\right| \cong (\mathbb{Z}/4m, +)$$

somit existiert ein Element $x \in \mathbb{F}_p^\times$ der Ordnung 4. Somit hat x^2 die Ordnung 2. Da in $(\mathbb{Z}/4m, +)$ nur ein solches Element existieren kann, kann auch in $\mathbb{F}_p^\times$ nur ein solches Element der Ordnung 2 existieren. Wir wissen bereits, dass -1 in $\mathbb{F}_p^\times$ die Ordnung 2 hat, also folgt $x^2 = -1$.

$5 \implies 4$**:** trivial.

□

Korollar 3.4.8. *Wir erhalten direkt einen formellen Beweis von Proposition 3.4.5.*

Korollar 3.4.9. *Eine positive natürliche Zahl $n \in \mathbb{N}_1$ lässt sich genau dann als Summe $n = x^2 + y^2$ zweier Quadratzahlen schreiben, wenn in der Primfaktorzerlegung $n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$ die Primfaktoren, welche Kongruent zu 3 modulo 4 sind, alle in geraden Potenzen auftreten.*