Algebra 1

Universität Heidelberg, Wintersemester 2025/26

Florent Schaffhauser

2025.10.31

Inhaltsverzeichnis

Kursübersicht

Kapitel 1 - Elementare Gruppentheorie (4 Wochen)

1. Gruppen
2. Nebenklassen und Faktorgruppen
3. Struktur endlich erzeugter abelschen Gruppen
4. Gruppenoperationen

Kapitel 2 - Ringe und Körper (3 Wochen)

5. Ringe und Ideale
6. Teilbarkeit und Faktorisierung
7. Primfaktorzerlegung in Polynomringen

Kapitel 3 - Algebraische Körpererweiterungen (3 Wochen)

8. Endliche und algebraische Erweiterungen
9. Normale und separable Erweiterungen
10. Endliche Körper

Kapitel 4 - Galois-Theorie (4 Wochen)

11. Die Galois-Korrespondenz
12. Auflösbarkeit algebraischer Gleichungen
13. Zyklische Erweiterungen
14. Anwendungen der Galois-Theorie

Vorlesungsplan

Tabelle 1.: Algebra 1 - Winter Semester 2025/26

Vortrag	Datum	Thema
1.a	15.10.2025	Gruppen und Gruppenhomomorphismen
1.b	17.10.2025	Untergruppen und endlich erzeugte Gruppen
2.a	22.10.2025	Nebenklassen und der Satz von Lagrange
2.b	24.10.2025	Faktorgruppen und Isomorphiesätze
3.a	29.10.2025	Struktur endlicher abelschen Gruppen
3.b	31.10.2025	Struktur endlich erzeugter abelschen Gruppen
4.a	05.11.2025	Transformationengruppen und der Satz von Cayley

Vortrag	Datum	Thema
4.b	07.11.2025	Sylow-Untergruppen
5.a	12.11.2025	Ringe und Ringhomomorphismen
5.b	14.11.2025	Nullteilerfreien Ringe und Körper
6.a	19.11.2025	Polynomringe und Algebren, Diskriminante und resultante
6.b	21.11.2025	Euklidische Ringe und Hauptidealringe
7.a	26.11.2025	Faktorielle Ringe und Der Satz von Gauß
7.b	28.11.2025	Irreduzibilitätskriterien für Polynome
8.a	03.12.2025	Algebraische Elemente und endliche Erweiterungen
8.b	05.12.2025	Zerfällungskörper und algebraischer Abschluss
9.a	10.12.2025	Normale Erweiterungen
9.b	12.12.2025	Separabilität und der Satz vom primitiven Element
10.a	17.12.2025	Konstruktion endlicher Körper
10.b	19.12.2025	Algebraischer Abschluss eines endlichen Körpers
11.a	07.01.2026	Galois-Erweiterugen
11.b	09.01.2026	Die Galois-Gruppe einer Polynomgleichung
12.a	14.01.2026	Radikalerweiterungen
12.b	16.01.2026	Auflösbare Gruppen
13.a	21.01.2026	Charakteren, Norm, und Spur
13.b	23.01.2026	Einheitswurzeln und Kreisteilungskörper
14.a	28.01.2026	Konstruktionen mit Zirkel und Lineal
14.b	30.01.2026	Galois-Descent für Vektorräume

Teil I.

Gruppen

1. Gruppen und Gruppenhomomorphismen

 .

Niels Henrik Abel (1802-1829) war ein norwegischer Mathematiker, der die Unlösbarkeit bewies, von Gleichungen fünften Grades durch Adjunktion von Wurzeln.

1.1. Beispiel und Motivation

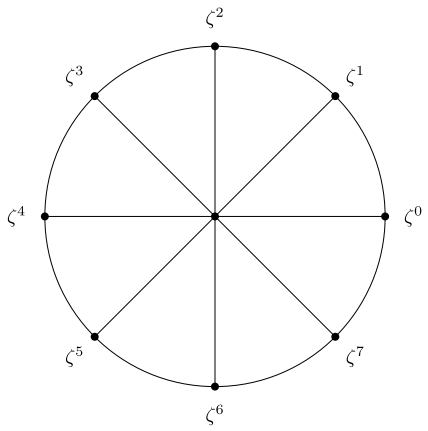

Abbildung 1.1.: Acht Punkte, die regelmäßig entlang eines Kreises angeordnet sind, um eine Rotationsgruppe zu veranschaulichen.

- Sei die komplexe Zahl $\zeta := e^{i\frac{\pi}{4}}$. Die Multiplikation mit ζ^k bewirkt eine Rotation um dem Winkel $\frac{k\pi}{4}$ in $\mathbb{C}$. Rotationen können *zusammengesetzt* und *umgekehrt* werden.
- Sei die Menge $A := \{\zeta^0, \zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7\}$. Elemente von A können *multipliziert* und *invertiert* werden: $\zeta^k * \zeta^\ell = \zeta^{k+\ell}$ und $\zeta^k * \zeta^{-k} = 1$.

1.2. Verknüpfung auf einer Menge

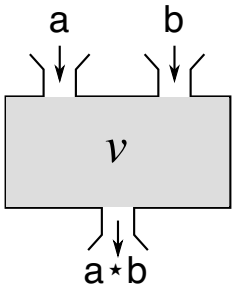

Abbildung 1.2.: Eine Verknüpfung dargestellt als *Black-Box*, die zwei Eingaben nimmt und eine Ausgabe produziert.

- Sei A eine Menge und sei $A \times A$ das kartesische Produkt von A mit sich selbst. Unter einer **Verknüpfung** auf A versteht man eine Abbildung

$$v : A \times A \to A.$$

- Das heißt, wenn a, b Elemente in A sind, dann gibt es ein Element $v(a, b)$ in A.

1.2.1. Beispiele für Verknüpfungen

- Die Addition $v(n, m) := n + m$ ist eine Verknüpfung auf $\mathbb{Z}$. So ist die Multiplikation $v(n, m) := n * m$. Dies zeigt, dass eine Menge verschiedene Verknüpfungen ausführen kann.
- Sei X eine Menge und sei $A := \mathrm{Abb}(X, X)$ die Menge, deren Elemente die Abbildungen $f : X \to X$ sind. Dann definiert die Komposition solcher Abbildungen eine Verknüpfung auf A:
$$v(g, f) := \text{fun } x \mapsto g(f(x)).$$
- Auf der Menge alle 2×2 Matrizen mit komplexen Koeffizienten ist die Ableitung $[m_1, m_2] := m_1 m_2 - m_2 m_1$ eine Verknüpfung.

1.3. Infix-Notation

- Man benutzt fast immer eine Infix-Notation für m. Das heißt, man schreibt v als $(\cdot \star \cdot)$, oder einfach $\star$, und das Element $v(a, b)$ als $a \star b$. Dieses Element wird als **Produkt** von a und b bezeichnet.
- Zum Beispiel schreibt man die Addition ganzer Zahlen, oder die Komposition $g \circ f$ von Abbildungen von X nach X, immer mit Infix-Notation.
- Die übliche Konvention für die Infix-Notation einer Verknüpfung ist, dass der Ausdruck $a \star b \star c$, als $(a \star b) \star c$ verstanden werden sollte (ohne solche Konvention, müsste man *immer* Klammern verwenden).

1.4. Assoziativität

- Mit der Infix-Notation ist es oft einfacher, die Eigenschaften einer Verknüpfung zu schreiben, zum Beispiel die Folgende.
- Eine Verknüpfung $(\cdot \star \cdot)$ auf einer Menge A heißt **assoziativ**, falls die folgende *Eigenschaft* gilt:
$$\forall\ a, b, c : A,\ (a \star b) \star c = a \star (b \star c).$$
- Äquivalent dazu haben wir: $a \star b \star c = a \star (b \star c)$.
- Die Addition $(\cdot + \cdot) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und die Komposition $(\cdot \circ \cdot) : \mathrm{Abb}(X, X) \times \mathrm{Abb}(X, X) \to \mathrm{Abb}(X, X)$ beide sind assoziativ (Übung).
- Auf der Menge alle 2×2 Matrizen mit komplexen Koeffizienten ist die Ableitung $[m_1, m_2] := m_1 m_2 - m_2 m_1$ nicht assoziativ.

1.5. Kommutativität

- Eine Verknüpfung $(\cdot \star \cdot)$ auf einer Menge A heißt **kommutativ**, falls die folgende *Eigenschaft* gilt:
$$\forall\ a, b : A,\ a \star b = b \star a.$$

- Beispiele und Gegenbeispiele:
  - Die Addition $(\cdot\ +\ \cdot) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ist kommutativ.
  - Die Komposition $(\cdot\ \circ\ \cdot) : \mathrm{Abb}(X, X) \times \mathrm{Abb}(X, X) \to \mathrm{Abb}(X, X)$ ist im Allgemeinen nicht kommutativ (siehe unten, oder betrachten Sie die Multiplikation von 2×2 Matrizen).
  - Auf der Menge der geraden Zahlen, ist die Multiplikation $(\cdot\ \times\ \cdot) : 2\mathbb{Z} \times 2\mathbb{Z} \to 2\mathbb{Z}$ eine kommutative Verknüpfung.

1.6. Eine nichtkommutative Verknüpfung

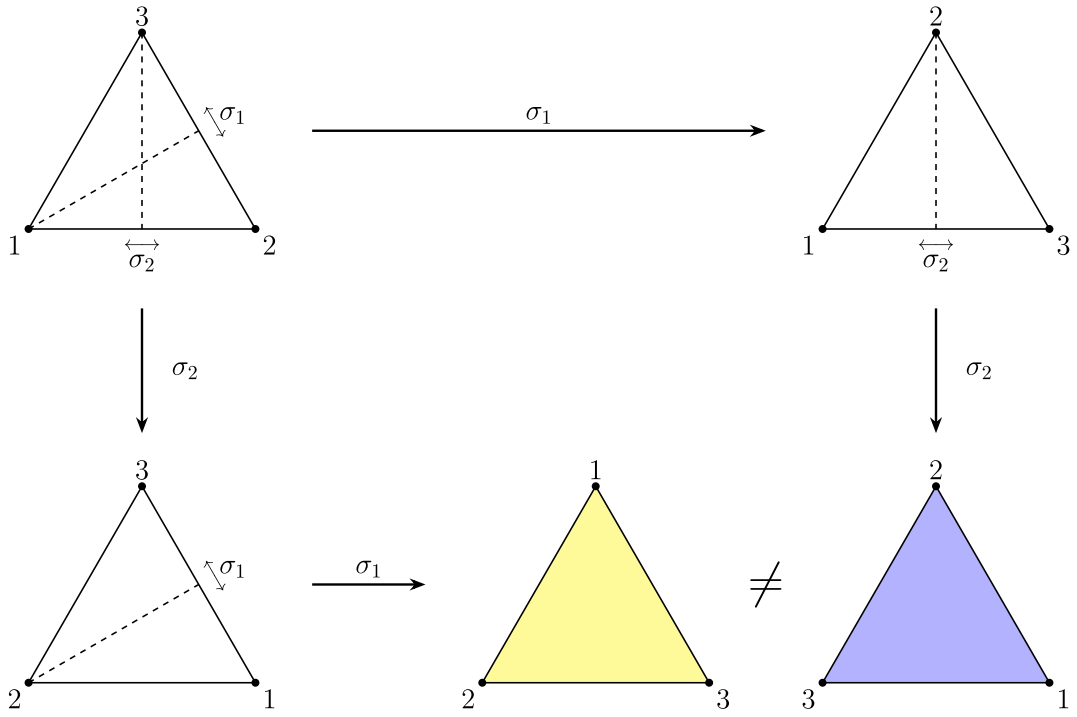

Abbildung 1.3.: Zwei nichtkommutative Symmetrien eines gleichseitigen Dreiecks, gegeben durch Spiegelungen entlang der Höhenlinien.

- Im Dreieck $T := \{1, 2, 3\}$, die Permutationen $\sigma_1 := (2\ 3)$ und $\sigma_2 := (1\ 2)$ bestätigen $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$, denn $\sigma_1 \circ \sigma_2(3) = 2$, aber $\sigma_2 \circ \sigma_1(3) = 1$.
- Da $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$, ist die Verknüpfung $(\cdot \circ \cdot)$ auf $\mathrm{Abb}(T, T)$nicht kommutativ.

1.7. Grundlegende algebraische Strukturen

- Eine Verknüpfung $\star$ auf einer Menge A ist ein Beispiel für eine (algebraische) Struktur auf A.

- Ein Paar $(A, \star)$, bestehend aus einer Menge A und einer Verknüpfunng $(\cdot \ \star \ \cdot) : A \times A \to A$ heißt ein **Magma**.
- Falls die Verknüpfung eines Magmas kommutativ ist, sagt man, dass dieses Magma kommutativ ist.
- Ein Dreifach $(A, \star, \star\text{-komm})$, bestehend aus einer Menge A, einer Verknüpfung $v : A \times A \to A$, und einem Beweis $\star$-komm, dass die Verknüpfung v kommutativ ist, wird **kommutatives Magma** genannt.

1.8. Halbgruppen

- Falls die Verknüpfung eines Magmas $(A, \star)$ assoziativ ist, sagt man, dass das Magma $(A, \star)$ assoziativ ist.
- Ein Dreifach $(A, \star, \star\text{-assoz})$, bestehend aus einer Menge A, einer Verknüpfunng $(\cdot \star \cdot) : A \times A \to A$, und einem Beweis $\star$-assoz, dass die Verknüpfung $\star$ assoziativ ist, wird **Halbgruppe** genannt.
- Falls die Verknüpfung einer Halbgruppe kommutativ ist, sagt man, dass diese Halbgruppe kommutativ ist. Aus dieser Sicht ist eine **kommutative Halbgruppe** ein Vierfach $(A, \star, \star\text{-assoz}, \star\text{-komm})$.
- Beispiele und Gegenbeispiele:
  - Die Magmas $(\mathbb{Z}, +)$ und $(2\mathbb{Z}, *)$ sind assoziativ und kommutativ.
  - Das Magma $\mathrm{Abb}(X, X)$ ist assoziativ aber im allgemeinen nicht kommutativ.

1.9. Neutrales Element

- Sei $(A, \star)$ ein Magma und sei e ein Element in A. Man nennt das Element e ein **neutrales Element** (oder *Einselement*) bezüglich der Verknüpfung $\star$, falls die folgende Eigenschaft gilt:

$$\forall\ a : A,\ (e \star a = a)\ \wedge\ (a \star e = a).$$

- Falls e und e' beide neutrale Elemente für die Verknüpfung $\star$ sind, dann gilt $e = e'$. Der Beweis ergibt sich aus folgender Berechnung:

$$\begin{array}{rcll} e & = & (e \star e') & (a{=}a{\star}e' \text{ mit } a{:=}e) \\ & = & e' & (e{\star}a{=}a \text{ mit } a{:=}e') \end{array}$$

1.10. Beispiele für neutrale Elemente

- 0 ist ein neutrales Element für $(\mathbb{Z}, +)$.
- 1 ist ein neutrales Element für $(\mathbb{Z}, *)$.
- id_X ist ein neutrales Element für $(\mathrm{Abb}(X, X), \circ)$.
- Die Matrix I_2 ist ein neutrales Element für Matrix-multiplikation in $\mathrm{Mat}(2 \times 2, \mathbb{C})$.
- Da 1 nicht gerade ist, hat das Magma $(2\mathbb{Z}, *)$ *kein* neutrales Element.

1.11. Monoide

- Ein **Monoid** ist ein Tupel $M := (A, \star, e, \star\text{-assoz}, \text{e-neutral})$, bestehend aus:
  - einer Menge A.
  - einer Verknüpfung $(\cdot \star \cdot) : A \times A \to A$ auf A.
  - einem Element e in A.
  - einem Beweis $\star$-assoz, dass die Verknüpfung $\star$ assoziativ ist:

$$\forall\ a, b, c : A,\ \ (a \star b) \star c = a \star (b \star c).$$

  - einem Beweis e-neutral, dass e ein neutrales Element bezüglich $\star$ ist:

$$\forall\ a : A,\ \ (e \star a = a)\ \ \wedge\ \ (a \star e = a).$$

- Wir nennen A die **zugrunde liegende Menge** des Monoids M. Elemente von A werden auch Elemente von M genannt. In moderner Notation schreibt man auch $M.\mathrm{carrier}$ für diese Menge.

1.12. Kommutative Monoide

- Sei $M := (A, \star, e, \star\text{-assoz}, \text{e-neutral})$ ein Monoid. Das Tupel $(\star, e, \star\text{-assoz}, \text{e-neutral})$ wird eine **Monoidstruktur** auf der Menge A genannt.
- Falls die Verknüpfung $\star$ kommutativ ist, sagt man, dass das Monoid M kommutativ ist. Ein **kommutatives Monoid** ist deshalb ein Paar $kM := (M, \star\text{-komm})$, bestehend aus:
  - einem Monoid M.
  - einem Beweis $\star$-komm, dass die Verknüpfung $\star$ kommutativ ist.
- Äquivalent dazu ist ein kommutatives Monoid ein Tupel

$$kM := (A, \star, e, \star\text{-assoz}, \text{e-neutral}, \star\text{-komm}).$$

1.13. Daten und Eigenschaften

- Um die Notation zu vereinfachen, ist es hilfreich zu lernen, welche Daten tatsächlich Eigenschaften sind.
- Zum Beispiel, in der Definition eines Monoides:
  - A, $\star$ und e sind Daten.
  - $\star$-assoz und e-neutral sind Eigenschaften (weil sie durch Gleichheiten in der Menge A definiert werden).
- Üblicherweise schreibt man die Eigenschaften nicht. Das heißt, ein Monoid wird einfach als $M := (A, \star, e)$ geschrieben.
- Zum Beispiel, können wir an die Tupeln $(\mathbb{Z}, +, 0)$ und $(\mathrm{Abb}(X, X), \circ, \mathrm{id}_X)$ als Monoide denken. Auch an das Tupel $(\mathbb{N}_0, +, 0)$.

1.14. Existenz eines neutralen Elements

- Es stellt sich heraus, dass wir sogar das Element e aus den Daten löschen können, die ein Monoid definieren. Wir müssen nur annehmen, dass es ein neutrales Element gibt, das heißt, dass die folgende Eigenschaft gilt:

$$\exists\, e : A,\ \forall\, a : A,\ (e \star a = a)\ \wedge\ (a \star e = a).$$

  Beweis: Per Annahme ist die Menge $\{a : A \ / \ a \text{ ist neutral}\}$ nicht leer. Da solches Element a, falls es existiert, eindeutig ist, es handelt sich sogar um ein Singleton. Wir können also ein Element aus dieser Menge *auswählen*, und es e nennen.

- Deswegen können wir auch ein Monoid M als Tupel $(A, \star, \star\text{-assoz}, \text{exist-neutral})$ darstellen, in dem exist-neutral ein Beweis ist, dass es ein Element $e : A$ *existiert*, so dass gilt $\forall\, a : A, (e \star a = a)\ \wedge\ (a \star e = a)$.

1.15. Inverse Elemente

- Seien $M := (A, \star, e)$ ein Monoid und a ein Element in A. Ein Element b in A heißt **invers** zu a (bezüglich $\star$), falls die folgende Eigenchaft gilt:

$$(b \star a = e)\ \wedge\ (a \star b = e)\ .$$

- Das Element a heißt **invertierbar**, falls die folgende Eigenschaft gilt:

$$\exists\, b : A,\ (b \star a = e)\ \wedge\ (a \star b = e).$$

- Wenn $b \star a = e$ sagt man auch, dass b ein linksinverses Element zu a ist. Gleichfalls, wenn $a \star b = e$ sagt man auch, dass b ein rechtsinverses Element zu a ist.

1.16. Eindeutigkeit des inversen Elements

- Nehmen wir an, dass $a : A$ invertierbar ist. Wenn b und b' beide invers zu a sind, gilt $b = b'$. Der Beweis ergibt sich aus folgender Berechnung:

$$\begin{array}{rcll} b & = & b \star e & (e\text{-neutral}) \\ & = & b \star (a \star b') & (\text{inv}) \\ & = & (b \star a) \star b' & (\star\text{-assoz}) \\ & = & e \star b' & (\text{inv}) \\ & = & b' & (e\text{-neutral}) \end{array}$$

- Die Menge $\mathrm{Inv}(a) := \{b : A \mid b \text{ invers zu } a\}$ ist daher ein Singleton.
- Deshalb können wir dieses Element *auswählen* und es a^{-1} nennen:

$$\mathrm{Inv}(a) = \{a^{-1}\}.$$

1.17. Beispiele für invertierbare Elemente

- In einem Monoid $(A, \star, e)$ ist das neutrale Element invertierbar, mit $e^{-1} = e$.
- Wenn a invertierbar ist, dann ist a^{-1} auch invertierbar, mit $(a^{-1})^{-1} = a$.
- Wenn a und b invertierbar sind, dann ist das Element $a \star b$ auch invertierbar, da das Element $b^{-1} \star a^{-1}$ ein inverse Element dazu ist. Der Beweis ergibt sich aus folgender Berechnung:

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

- Wir haben die „*Regel von H.qmd und Jacke*“ bewiesen: $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

1.18. Konkrete Beispiele für invertierbare Elemente

- Im kommutativen Monoid $(\mathbb{Z}, +, 0)$, ist *jedes* Element invertierbar, da $\forall n : \mathbb{Z}, n + (-n) = 0$ gilt (das inverse Element von n ist $-n$).
- Im kommutativen Monoid $(\mathbb{N}_0, +, 0)$, ist hingegen das neutrale Element 0 *das einzige* invertierbare Element.
- Im Monoid $(\mathrm{Abb}(X), \circ, \mathrm{id}_X)$ sind die invertierbaren Elemente die Bijektionen $f : X \to X$, das heißt, die Abbildungen f, für die eine Umkehrfunktion $g : X \to X$ existiert (eine Abbildung g, so dass $g \circ f = \mathrm{id}_X \ \wedge \ f \circ g = \mathrm{id}_X$).

Anmerkung. Wenn es kein neutrales Element gibt, zum Beispiel im Magma $(2\mathbb{Z}, *)$, ist das Konzept „*invertierbares Element*“ sinnlos.

1.19. Die Menge invertierbaren Elemente eines Monoids

- Gegeben ein Monoid $M := (A, \star, e)$, können wir eine Menge $A^\times := \{a : A \ / \ a \text{ ist invertierbar}\}$ definieren. Auf dieser Menge können wir dann eine Abbildung $i : a \mapsto a^{-1}$ definieren. Wir haben bereits bewiesen, dass $e \in A^\times$, und dass die Verknüpfung von A eine Verknüpfung auf $A^\times$ induziert:

$$\forall\ a, b : A,\ a \in A^\times \wedge b \in A^\times \Rightarrow a \star b \in A^\times.$$

- Deswegen haben wir ein Monoid $M^\times := (A^\times, \star, e)$ gebaut, in dem jedes Element invertierbar ist. Dieses Monoid $M^\times$ wird die **Einheitgruppe von** M genannt. Es ist tatsächlich eine Gruppe (siehe unten).

1.20. Monoide, in denen alle Elemente invertierbar sind

- Betrachten wir ein Monoid $M := (A, \star, e)$, mit der Eigenschaft, dass jedes Element $a : A$ invertierbar ist.
- Aus formarler Sicht haben wir ein Paar $(M, \text{inv-exist})$, in dem M ein Monoid ist, und inv-exist ein Beweis für die folgende Eigenschaft ist:

$$\forall\ a : A,\ \exists\ b : A, b \star a = e \wedge a \star b = e.$$

- Wenn diese Eigenschaft gilt, impliziert die Eindeutigkeit eines inversen Elements, dass wir eine Abbildung $i : A \to A$ definieren können, die ein Element $a : A$ nach seinem inversen Element a^{-1} abbildet: $\forall\ a : A,\ i(a) := a^{-1}$.
- Diese Abbildung $i : A \to A$ überprüft die folgende Eigenschaft, dass für alles $a : A$, das Element $i(a)$ ein inverse Element zu a ist: $i(a) \star a = e \wedge a \star i(a) = e$.

1.21. Gruppen

- Die Idee ist, dass eine Gruppe, ein Monoid ist, in dem jedes Element invertierbar ist.
- Formal ist eine **Gruppe** ein Tupel $G := (A, \star, e, i, \star\text{-assoz}, \text{e-neutral}, \text{i-inv})$ bestehend aus:
  - einer Menge A.
  - einer Verknüpfung $(\cdot\ \star\ \cdot) : A \times A \to A$ auf A.
  - einem Element e in A.
  - einer Abbildung $i : A \to A$.
  - einem Beweis $\star$-assoz, dass $\forall\ a, b, c : A,\ (a \star b) \star c = a \star (b \star c)$ gilt.
  - einem Beweis e-neutral, dass $\forall\ a : A,\ (e \star a = a)\ \wedge\ (a \star e = a)$ gilt.
  - einem Beweis i-inv, dass $\forall\ a : A, i(a) \star a = e \wedge a \star i(a) = e$ gilt.

1.22. Eigenschaften und Notation

- Wie wir gesehen haben, können wir ein neutrales Element $e : A$ und eine Abbildung $i : A \to A$ konstruieren, wenn die folgende Eigenschaften gelten,:
  - Existenz von einem neutralen Element:
$$\exists\ e : A,\ \forall\ a : A,\ (e \star a = a)\ \wedge\ (a \star e = a).$$
  - Existenz von inversen Elementen:
$$\forall\ a : A,\ \exists\ b : A, b \star a = e \wedge a \star b = e.$$
- Deshalb können wir eine Gruppe auch als Tupel $(A, \star, \star\text{-assoz}, \text{neutral-exist}, \text{inv- exist})$ definieren.
- Wenn wir die Eigenschaften entfernen und nur die Daten behalten, können wir sogar eine Gruppe G mit $(A, \star, e, i)$, oder einfach $(A, \star)$, bezeichnen.

1.23. Kommutative Gruppen

- Sei $G = (A, \star, e, i)$ eine Grupppe.
- Falls die Verknüpfung $\star$ kommutativ ist, heißt die Gruppe G kommutativ (oder **abelsch**).
- Eine **kommutative Gruppe** ist deshalb ein Paar $kG := (G, \star\text{-komm})$, bestehend aus:
  - einer Gruppe G.
  - einem Beweis $\star$-komm, dass die Verknüpfung dieser Gruppe kommutativ ist.
- In der Praxis sagen wir jedoch einfach „*Sei G eine kommutative Gruppe*“ (die Eigenschaften entfernen und nur die Daten behalten).

1.24. Beispiele für Gruppen

- Sei $i : \mathbb{Z} \to \mathbb{Z}$ die Abbildung, die durch $i(n) := -n$ definiert wird. Das Tupel $(\mathbb{Z}, +, 0, i)$ ist eine abelsche Gruppe.
- Wenn $M := (A, \star, e)$ ein Monoid ist, gibt es auf der Menge $A^\times$ die Abbildung $i(a) := a^{-1}$. Dann ist das Tupel $M^\times := (A^\times, \star, e, i)$ eine Gruppe (die **Einhgeitgruppe** von M).
- Ein Monoid $(A, \star)$ ist genau dann eine Gruppe, wenn $\forall\ a : A, a \in A^\times$. Damit können wir beweisen, dass bestimmte Monoide *keine* Gruppenstruktur unterstützen.
- Zum Beispiel, das Monoid $(\mathbb{N}_0, +)$ *ist* keine Gruppe (da $\mathbb{N}_0^\times = \{0\}$).
- Beachten Sie, dass die Notation $A^\times$ mehrdeutig ist (da *invertierbar* nur Sinn macht, wenn eine Verknüpfung $\star$ angegeben wurde). Zum Beispiel, $(\mathbb{Z}, +)^\times = (\mathbb{Z}, +)$ und $(\mathbb{Z}, *)^\times = (\{1, -1\}, *)$. Hingegen ist die Notation $M^\times$ voll korrekt.

1.25. Hierarchie gruppenähnlicher Strukturen

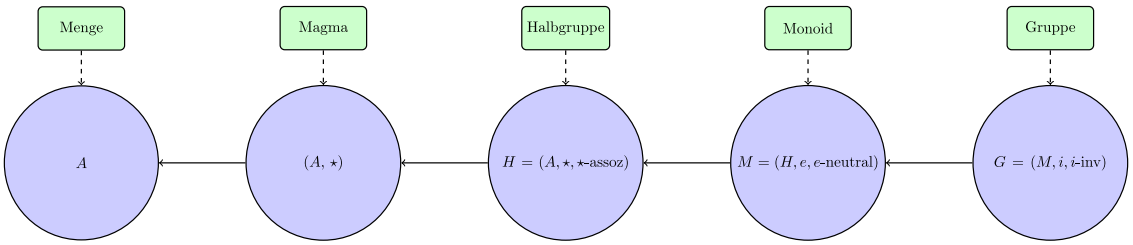

Abbildung 1.4.: Eine algebraische Hierarchie gruppenähnlicher Objekte, dargestellt als Git-Commit-Verlaufsdiagramm.

- Wir haben eine grundlegende „*Hierarchie*“ algebraischer Strukturen erstellt.
- Wir begannen mit einer Menge und fügten dann eine Operation und einige Eigenschaften hinzu.

1.26. Pause

Abbildung 1.5.: QR Code zur Zulip-channel.

- *Machen wir eine kurze Pause. Bisher war alles sehr abstrakt.*
- Wir benötigen weitere Beispiele.
- Wenn Sie Fragen haben, können Sie diese jetzt oder später auf Zulip stellen.

1.27. Symmetriegruppe eines Rechtecks

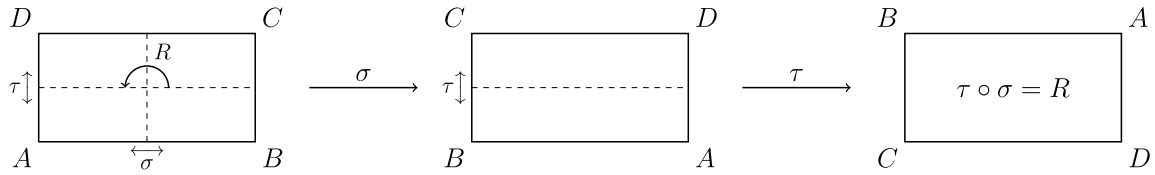

Abbildung 1.6.: Symmetriegruppe eines Rechtecks.

- Ein Rechteck hat zwei Reflexionachsen. Es besitzt außerdem eine Rotationssymmetrie (um den Winkel π).
- Nennen wir A, B, C, D die Eckpunkte eines Rechtecks.
- Wir können die Wirkung der Reflexionen σ und τ an diesen Eckpunkte betrachten.
- Wenn wir σ dann τ anwenden, ist die Wirkung dieselbe wie bei der Rotation R.

1.28. Verknüpfungstafel der Symmetriegruppe eines Rechtecks

- Mit den Transformationen id, σ, τ und R, können wir eine Gruppe bauen.
- Eine Verknüpfungstafel für diese Gruppe sieht wie folgt aus. Die Existenz inverser Elemente, so wie die Kommutativität dieser Verknüpfung, sind auf dieser Tafel sichtbar.
- Assoziativität ist *nicht* offensichtlich.

	id	σ	τ	R
id	id	σ	τ	R
σ	σ	id	R	τ
τ	τ	R	id	σ
R	R	τ	σ	id

Die Verknüpfungstafel hängt davon ab, wie die Gruppenelemente aufgelistet werden.

1.29. Symmetriegruppe eines Quadrats

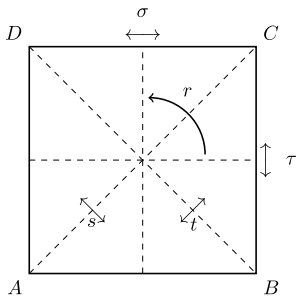

Abbildung 1.7.: Symmetriegruppe eines Quadrats.

- Ein Quadrat hat vier Reflexionachsen und eine Rotationssymmetrie (um den Winkel $\frac{\pi}{2}$).
- Wir können s und r verwenden, um jede andere dieser Symmetrien zu erhalten. Zum Beispiel, ist $r \circ s$ die Reflexion an der vertikalen Achse ($r \circ s = \sigma$).
- Wir schreiben r^2 statt $r \circ r$, und so weiter.

1.30. Eine Verknüpfungstafel für die Symmetriegruppe eines Quadrats

	id	r	r^2	r^3	s	t	σ	τ
id	id	r	r^2	r^3	s	t	σ	τ
r	r	r^2	r^3	id	σ	τ	t	s
r^2	r^2	r^3	id	r	t	s	τ	σ
r^3	r^3	id	r	r^2	τ	σ	s	t
s	s	τ	t	σ	id	r^2	r^3	r
t	t	σ	s	τ	r^2	id	r	r^3
σ	σ	s	τ	t	r	r^3	id	r^2
τ	τ	t	σ	s	r^3	r	r^2	id

Die Verknüpfungstafel hängt davon ab, wie die Gruppenelemente aufgelistet werden.

1.31. Die in einer Symmetriegruppe enthaltene Information

- Die Intuition ist: *Je mehr Symmetrien die Figur aufweist, desto komplizierter ist ihre Symmetriegruppe.*
- Beispielsweise ist ein Quadrat symmetrischer als ein Rechteck, und dies kann man in der Verknüpfungstafel sehen, die für das Quadrat komplizierter ist.
- In der Galois-Theorie ist die „*Figur*“ eine **Polynomgleichung**. Ihre „*Symmetriegruppe*“ wird als **Galois-Gruppe** bezeichnet.

- Die Eigenschaften der Galois-Gruppe spiegeln die Eigenschaften der Gleichung wider und liefern Informationen darüber. Dies zu verstehen, ist das Ziel dieses Kurses.
- Natürlich gibt es viel bessere Möglichkeiten, die interne Struktur einer Gruppe zu studieren, als einfach eine Verknüpfungstafel zu schreiben! Wir werden das hier lernen.

1.32. Übung 1

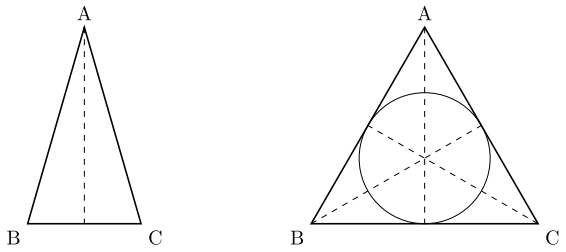

Abbildung 1.8.: Symmetrieachsen eines gleichschenkligen und eines gleichseitigen Dreiecks.

1. Bestimmen Sie eine Verknüpfungstafel für die Symmetriegruppe eines gleichschenkligen Dreiecks.
2. Machen Sie dann dasselbe für ein gleichseitiges Dreieck.
3. Welche Tafel ist komplizierter?

1.33. Übung 2

- Seien $G_1 = (A_1, \star_1, e_1, i_1)$ und $G_2 = (A_2, \star_2, e_2, i_2)$ Gruppen.
- Auf der Produktmenge $A := A_1 \times A_2$ können wir die folgende Verknüpfung definieren.

$$(a_1, a_2) \star (b_1, b_2) := (a_1 \star_1 b_1, a_2 \star_2 b_2)$$

- Zeigen Sie, dass das Magma $(A, \star)$ mit einer Gruppenstruktur ausgestattet werden kann.

1.34. Monoidhomomorphismus

- Seien $M := (A_M, \star_M, e_M)$ und $N := (A_N, \star_N, e_N)$ Monoiden.
- Man sagt, dass eine Abbildung $f : A_M \to A_N$ ein **Monoidhomomorphismus** ist, falls die folgenden Eigenschaften gelten:
  - $\forall\ a, b : A_M,\ f(a \star_M b) = f(a) \star_N f(b)$.
  - $f(e_M) = e_N$.

- Die Idee ist, dass die Abbildung f mit der Verknüpfung, und mit dem neutralen Element, kompatibel sein sollte.

  In der Praxis schreibt man oft $f(e) = e$ und $f(a \star b) = f(a) \star f(b)$ oder sogar $f(ab) = f(a)f(b)$.

1.35. Formale Definition

- Aus formaler Sicht ist ein **Monoidhomomorphismus zwischen den Monoiden** $M := (A_M, \star_M, e_M)$ **und** $N := (A_N, \star_N, e_N)$ ein Tupel

$$\varphi := (f, \star\text{-kompatibel}, e\text{-kompatibel}),$$

  wobei:

  - $f : A_M \to A_N$ eine Abbildung ist (oft die *zugrunde liegende Abbildung* des Homomorphismus φ genannt).
  - $\star$-kompatibel ein Beweis für die folgende Eigenschaft ist:

$$\forall\ a, b : A_M,\ \ f(a \star_M b) = f(a) \star_N f(b)$$

  - e-kompatibel ein Beweis für die folgende Eigenschaft ist:

$$f(e_M) = e_N.$$

1.36. Menge von Homomorphismen

- Seien $M := (A_M, \star_M, e_M)$ und $N := (A_N, \star_N, e_N)$ Monoide. Dann können wir die *Menge* $\mathrm{Hom}_{\mathrm{Mnd}}(M, N)$ aller Homomorphismen zwischen den Monoiden M und N betrachten.
- Die Elemente dieser Menge sind die zuvor definierten Tupel

$$\varphi := (f, \star\text{-kompatibel}, e\text{-kompatibel}).$$

- Oft wird $\varphi : \mathrm{Hom}_{\mathrm{Mnd}}(M, N)$ einfach als $\varphi : M \to N$ bezeichnet. Dies ist Notation für die Abbildung $f : A_M \to A_N$ (und, wie üblich, bleiben die Eigenschaften implizit).
- Zum Beispiel, falls $M = N$, ist $id_M : \mathrm{Hom}_{\mathrm{Mnd}}(M, N)$ der durch die Identitätsfunktion $id_{A_M} : A_M \to A_M$ induziert Monoidhomomorphismus. Das heißt, $id_M = (id_{A_M}, \star\text{-kompatibel}, e\text{-kompatibel})$.

1.37. Komposition von Homomorphismen

- Wenn M, N und P Monoide sind, können wir eine Verknüpfung definieren, das heißt, eine Abbildung

$$\circ_{\mathrm{Mnd}} : \mathrm{Hom}_{\mathrm{Mnd}}(M,N) \times \mathrm{Hom}_{\mathrm{Mnd}}(N,P) \to \mathrm{Hom}_{\mathrm{Mnd}}(M,P).$$

- Die Definition ergibt sich aus der folgenden Beobachtung: gegeben Abbildungen $f : M \to N$ und $g : N \to P$, die Monoidehomomorphismen sind, ist die Abbildung $g \circ f$ auch ein Monoidhomomorphismus.
- Um sicherzustellen, dass dies korrekt ist, müssen wir die folgenden Eigenschaften überprüfen, die von der Definition $(g \circ f)(a) := g(f(a))$ folgen:

$$\forall\ a, b : M,\ (g \circ f)(a \star_M b) = (g \circ f)(a) \star_P (g \circ f)(b) \text{ und } (g \circ f)(e_M) = e_P.$$

- Aus formaler Sicht, falls $\varphi := (f,\ \ldots\ )$ und $\psi := (g,\ \ldots\ )$, haben wir $\psi \circ_{\mathrm{Mnd}} \varphi := (g \circ f,\ \ldots\ )$.

1.38. Übung 3

Sei M, N, P und Q Monoide. Zeigen Sie die folgende Eigenschaften:

1. Wenn die Abbildungen $f : M \to N$ und $g : N \to P$ Monoidhomomorphismen sind, dann ist die Abbildung $g \circ f : M \to P$ ein Monoidhomomorphismus.
2. Für jeden Monoidhomomorphismus $\varphi : \mathrm{Hom}_{\mathrm{Mnd}}(M,N)$, gilt

$$\varphi \circ_{\mathrm{Mnd}} id_M = \varphi \text{ und } id_N \circ_{\mathrm{Mnd}} \varphi = \varphi.$$

3. Für alle Monoidhomomorphismen $\varphi : \mathrm{Hom}_{\mathrm{Mnd}}(M,N)$, $\psi : \mathrm{Hom}_{\mathrm{Mnd}}(N,P)$ und $\chi : \mathrm{Hom}_{\mathrm{Mnd}}(P,Q)$, gilt die Assoziativitäteigenschaft

$$\chi \circ_{\mathrm{Mnd}} (\psi \circ_{\mathrm{Mnd}} \varphi) = (\chi \circ_{\mathrm{Mnd}} \psi) \circ_{\mathrm{Mnd}} \varphi.$$

1.39. Beispiele für Monoidhomomorphismen

- Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}$ induziert ein Monoidhomomorphismus vom Monoid $(\mathbb{R}, +)$ zum Monoid $(\mathbb{R}_{>0}, *)$, wegen $\exp(a+b) = \exp(a) * \exp(b)$ und $\exp(0) = 1$.
- Sei $M := (A_M, \star_M, e_M)$ ein Monoid und $a : A_M$ ein Element. Dann gibt es genau einen Monoidhomomorphismus $\varphi_a : (\mathbb{N}_0, +) \to M$ mit $\varphi_a(1) = a$. Diese Eigenschaft ist als **universelle Eigenschaft des Monoids** $(\mathbb{N}_0, +)$ bekannt.

– Beachten Sie, dass ein solches Homomorphismus, falls er existiert, die Bedingungen $\varphi_a(0) = e_M$ und $\forall\ n : \mathbb{N}_{>0},\ \varphi_a(n) = \varphi_a(1 + ... + 1) = \varphi_a(1)^n = a^n$ erfüllen muss (letzteres beweist man durch Induktion).
– Es genügt dann zu beweisen, dass die so definierte Abbildung $\varphi_a(n) := a^n$, ein Monoidhomomorphismus ist, das außerdem die Eigenschaft $\varphi_a(1) = a$ erfüllt.

1.40. Kompatibilität mit dem neutralen Element

- Sei $M := (A_M, \star_M, e_M)$ und $N := (A_N, \star_N, e_N)$ Monoide.
- Wenn das Monoid N tatsächlich eine *Gruppenstruktur* besitzt , ist eine Abbildung $f : A_M \to A_N$ genau dann ein Gruppenhomorphismus, wenn die folgende Eigenschaft gilt:

$$\forall\ a, b : A_M,\ f(a \star_M b) = f(a) \star_N f(b)\ .$$

- Das heißt, die Eigenschaft $f(e_M) = e_N$ gilt in diesem Fall *automatisch.*

  Beweis. Zunächst haben wir

$$f(e_M) = f(e_M \star_M e_M) = f(e_M) \star_N f(e_M)\ .$$

  Danach, da $f(e_M)$ invertierbar ist, impliziert die vorherige Gleichheit, dass

$$f(e_M)^{-1} \star_N f(e_M) = f(e_M)^{-1} \star_N (f(e_M) \star f(e_M))\ ,$$

  somit $e_N = f(e_M)$.

1.41. Gruppenhomomorphismen

- Man nennt einen **Gruppenhomomorphismus zwischen den Gruppen** $G := (A_G, \star_G, e_G)$ **und** $H := (A_H, \star_H, e_H)$ ein Tupel $(f, \star\text{-kompatibel}, e\text{-kompatibel})$, wobei:
  – $f : A_G \to A_H$ eine Abbildung ist.
  – $\star$-kompatibel ein Beweis für die folgende Eigenschaft ist:

$$\forall\ a, b : A_G,\ f(a \star_G b) = f(a) \star_H f(b)$$

  – e-kompatibel ein Beweis für die folgende Eigenschaft ist:

$$f(e_G) = e_H.$$

- Aufgrund der vorherigen Bemerkung, reicht es jedoch eine Abbildung $f : A_G \to A_H$ zu definieren, die *einfach die erste Eigenschaft* oben erfüllt, um ein Gruppenhomomorphismus zwischen G und G zu bauen.

1.42. Beispiele für Gruppenhomomorphismen

- Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}$ induziert ein Gruppenhomomorphismus von der Gruppe $(\mathbb{R}, +)$ zur Gruppe $(\mathbb{R}_{>0}, *)$. Um dass zu zeigen genügt es, einfach die Bedingung $\exp(a + b) = \exp(a) * \exp(b)$ zu beweisen.
- Seien $G := (A_G, \star_G, e_G)$ eine Gruppe und $a : A_M$ ein Element. Dann gibt es genau einen Gruppenhomomorphismus $\varphi_a : (\mathbb{Z}, +) \to G$ mit $\varphi_a(1) = a$. Dies ist als **universelle Eigenschaft der Gruppe** $(\mathbb{Z}, +)$ bekannt.
  - Beachten Sie, dass ein solches Homomorphismus, falls er existiert, die Bedingungen $\varphi_a(0) = e_G$, $\forall\ n : \mathbb{Z}_{>0},\ \varphi_a(n) = \varphi_a(1 + ... + 1) = a^n$, und $\forall\ n : \mathbb{Z}_{<0},\ \varphi_a(n) = (a^n)^{-1}$ erfüllen muss (da $\varphi_a(n - n) = \varphi_a(0) = e_G$).
  - Es genügt entsprechend zu beweisen, dass die so definierte Abbildung $\varphi_a(n) := a^n$, ein Gruppenhomomorphismus ist, der $\varphi_a(1) = a$ erfüllt.

1.43. Ein konkretes Beispiel: Division mit Rest

- Sei $n : \mathbb{Z}_{>0}$. Betrachten wir die Abbildung

$$(\cdot \bmod n) : \mathbb{Z} \to \{0,\ 1,\ ...\ ,\ n - 1\}$$

  die eine ganze Zahl $m : \mathbb{Z}$ nach den Rest der Division mit Rest von m durch n abbildet ($m = q * n + r$ mit $0 \leqslant r \leqslant n - 1$).
- Dann gilt $(m_1 + m_2) \bmod n = (m_1 \bmod n) + (m_2 \bmod n)$.
- Wenn wir die Notation $\mathbb{Z}/n\mathbb{Z} := \{0,\ 1,\ ...\ ,\ n - 1\}$ und die Verknüpfung

$$(i \bmod n) +_{\mathbb{Z}/n\mathbb{Z}} (j \bmod n) := (i +_{\mathbb{Z}} j) \bmod n$$

  einführen, können wir eine Gruppenstruktur auf der Menge $\mathbb{Z}/n\mathbb{Z}$ konstruieren.
- Bezüglich dieser Gruppenstruktur ist die Abbildung $(\cdot \bmod n) : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ein Gruppenhomomorphismus.

1.44. Übung 4

- Seien M und N Monoide, und $f : M \to N$ ein Monoidhomomorphismus.
- Zeigen Sie die folgende Eigenschaften:
  1. $\forall\ a : M^\times, (f(a) \in N^\times) \wedge (f(a)^{-1} = f(a^{-1}))$.
  2. Der Monoidhomomorphismus $f : M \to N$ induziert (durch Einschränkung) einen Gruppenhomomorphismus $f|^{N^\times}_{M^\times} : M^\times \to N^\times$.

1.45. Übung 5

- Seien G, H, J und K Gruppen. Mit $\mathrm{Hom}_{\mathrm{Gpp}}(G,H)$ bezeichnen wir die Menge Gruppenhomomorphismen von G zu H.
- Definieren Sie eine Verknüpfung

$$\circ_{\mathrm{Gpp}} : \mathrm{Hom}_{\mathrm{Gpp}}(G,H) \times \mathrm{Hom}_{\mathrm{Gpp}}(H,J) \to \mathrm{Hom}_{\mathrm{Gpp}}(G,J)$$

und Gruppenhomomorphismen $id_G : \mathrm{Hom}_{\mathrm{Gpp}}(G,G)$, sodass die folgende Eigenschaften gelten:

1. $\forall\ \varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G,H),\ \varphi \circ_{\mathrm{Gpp}} id_G = \varphi \wedge id_H \circ_{\mathrm{Gpp}} \varphi = \varphi.$
2. $\forall\ \varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G,H),\ \psi : \mathrm{Hom}_{\mathrm{Gpp}}(H,J),\ \chi : \mathrm{Hom}_{\mathrm{Gpp}}(J,K),$

$$\chi \circ_{\mathrm{Gpp}} (\psi \circ_{\mathrm{Gpp}} \varphi) = (\chi \circ_{\mathrm{Gpp}} \psi) \circ_{\mathrm{Gpp}} \varphi.$$

1.46. Monoidisomorphismen

- Sei $\varphi : \mathrm{Hom}_{\mathrm{Mnd}}(M,N)$ ein Monoidhomomorphismus. Dann wird φ einen **Monoidisomorphismus** genannt, falls es ein Monoidhomorphismus $\psi : \mathrm{Hom}_{\mathrm{Mnd}}(N,M)$ existiert, so dass die folgende Eigenschaften gelten:

$$(\psi \circ_{\mathrm{Mnd}} \varphi = id_M)\ \wedge\ (\varphi \circ_{\mathrm{Mnd}} \psi = id_N).$$

- Die Menge Monoidisomorphismen von M nach N wird mit $\mathrm{Isom}_{\mathrm{Mnd}}(M,N)$ bezeichnet.
- Falls φ ein Isomorphismus ist, wird der Homomorphismus ψ einen **inversen Homomorphismus** zu φ genannt.

1.47. Gruppenisomorphismen

- Ebenso wird ein Gruppenhomorphismus $\varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G,H)$ einen **Gruppenisomorphismus** genannt, falls es ein Gruppenhomomorphismus $\psi : \mathrm{Hom}_{\mathrm{Gpp}}(H,G)$ existiert, sodass die folgende Eigenschaften gelten:

$$(\psi \circ_{\mathrm{Gpp}} \varphi = id_M)\ \wedge\ (\varphi \circ_{\mathrm{Gpp}} \psi = id_N).$$

- Die Menge Gruppenisomorphismen von G nach H wird mit $\mathrm{Isom}_{\mathrm{Gpp}}(M,N)$ bezeichnet.

1.48. Eindeutigkeit des inverses Homomorphismus

- Sei $\varphi := (f,\ \ldots\ )$ ein Homomorphismus zwischen Monoiden $M := (A_M, \star_M, e_M)$ und $N := (A_N, \star_N, e_N)$, oder zwischen Gruppen G und H. Nehmen wir an, dass es ein inverse Homomorphismus zu φ existiert. Dann ist solches Homomorphismus eindeutig.
- Um das zu beweisen, nehmen wir an, dass $\psi_1 := (g_1,\ \ldots\ )$ und $\psi_2 := (g_2,\ \ldots\ )$ beide inverse zu φ sind, und zeigen, dass $\psi_1 = \psi_2$ ist. Es genügt zu beweisen, dass die zugrunde liegende Abbildungen die Eigenschaft $g_1 = g_2$ erfüllen.
- Dies folgt von die Gleichheiten $g_1 \circ f = id_{A_N}$ und $g_2 \circ f = id_{A_N}$ und der Eindeutigkeit der Umkehrfunktion zu einer bijektive Funktion f.
- Es ist *entsprechend* möglich/erlaubt, die Notation φ^{-1} für den inversen Homomomorphismus zu φ zu benutzen.

1.49. Bijektive Homomorphismen

Satz. Ein Mondoidhomomorphismus $\varphi := (f, \star\text{-komp}, e\text{-komp})$ ist genau dann ein Monoidisomorphismus, wenn die Abbildung f eine Bijektion ist. Der analoge Satz gilt für Gruppenhomomorphismen.

- Es genügt, den Beweis entweder für Monoide oder Gruppen geben. Wir werden mit Monoiden arbeiten.
- Der entscheidende Punkt der Beweisführung ist, dass die Umkehrfunktion f^{-1} eines bijektives Monoidhomomorphismus $\varphi := (f, \star\text{-komp}, e\text{-komp})$ *automatisch* ein Homomorphismus ist. Das werden wir unten beweisen.

1.50. Monoidisomorphismen sind bijektiven („⇒“)

- Zunächst beweisen wir, dass, wenn ein Monoidhomomorphismus

$$\varphi := (f, \star\text{-komp}, e\text{-komp})$$

von $M = (A_M, \star_M, e_M)$ nach $N = (A_N, \star_N, e_N)$ ein Monoidisomorphismus ist, die Abbildung $f : A_M \to A_N$ eine Bijektion ist.

- Da φ ein Isomorphismus ist, gibt es einen inversen Homomorphismus $\psi = (g,\ \ldots\ )$, welcher die Eigenschaft $(\psi \circ_{\text{Mnd}} \varphi = id_M) \wedge (\varphi \circ_{\text{Mnd}} \psi = id_N)$ erfüllt.
- Per Definition der Komposition von Homomorphismen, gilt die Eigenschaft

$$(g \circ f = id_{A_M}) \wedge (f \circ g = id_{A_N})\ .$$

Das heißt, f ist eine Bijektion.

1.51. Bijektive Monoidhomomorphismen sind Isomorphismen („⇐“)

- Sei $\varphi = (f,\ \ldots\ )$ ein Monoidhomomorphismus zwischen Monoiden $M = (A_M, \star_M, e_M)$ und $N = (A_N, \star_N, e_N)$, so dass die Abbildung $f : A_M \to A_N$ bijektive ist. Wir wollen einen inversen Homomorphismus zu φ konstruieren. Dass heißt, einen Monoidhomomorphismus $\psi = (g,\ \ldots\ )$ zwischen N und M, sodass $(\psi \circ_{\text{Gpp}} \varphi = id_M) \wedge (\varphi \circ_{\text{Gpp}} \psi = id_N)$.
- Da $f : A_M \to A_N$ bijektiv ist, existiert ein $g : A_N \to A_M$, so dass $(g \circ f = id_{A_M}) \wedge (f \circ g = id_{A_N})$. Um einen inversen Homomorphismus ψ zu φ zu bauen, genügt es zu zeigen, dass g die folgende Eigenschaften erfüllt:

  $$(\forall\ c, d : A_N,\ g(c \star_N d) = g(c) \star_M g(d)) \wedge (g(e_N) = e_M)$$

  (die Eigenschaften, die einen Monoidhomomorphismus definieren). Das beweisen wir unten.

1.52. Kompatibilität mit der Verknüpfung

Zeigen wir zunächst, dass die Eigenschaft $\forall\ c, d : A_N,\ g(c \star_N d) = g(c) \star_M g(d)$ gilt.

- Da $f : A_M \to A_N$ bijektiv ist, gibt es eindeutige Elemente $a, b : A_M$, sodass $f(a) = c$ und $f(b) = d$.
- Da g eine Umkehrfunktion für f ist, gibt es auch $g(c) = g(f(a)) = a$ und $g(d) = g(f(b)) = b$.
- Da f ein Monoidhomorphismus ist, gilt

  $$c \star_N d = f(a) \star_N f(b) = f(a \star_M b).$$

- Da g eine Umkehrfunktion für f ist, haben wir dann

  $$g(c \star_N d) = g(f(a) \star_N f(b)) = g(f(a \star_M b)) = a \star_M b\ = g(c) \star_M g(d).$$

1.53. Kompatibilität mit den neutralen Element

Wir müssen noch überprüfen, dass $g(e_N) = e_M$ ist.

- Da f ein Monoidhomorphismus ist, gilt $f(e_M) = e_N$.
- Da g eine Umkehrfunktion für f ist, haben wir dann

  $$g(e_N) = g(f(e_M)) = e_M.$$

1.54. Übung 7

- Sei M ein Monoid. Betrachten wir die Menge $\mathrm{Hom}_{\mathrm{Mnd}}(M, M)$ von Homomorphismen von M nach sich selbst, mit der Verknüpfung $\circ_{\mathrm{Mnd}}$.
- Zeigen Sie, dass das folgende Tupel ein Monoid ist:

$$\mathrm{End}_{\mathrm{Mnd}}(M) := (\mathrm{Hom}_{\mathrm{Mnd}}(M, M)), \circ_{\mathrm{Mnd}}, id_M).$$

- Zeigen Sie, dass die Gruppe der invertiebaren Elemente des Monoids $\mathrm{End}_{\mathrm{Mnd}}(M)$ genau die Gruppe ist, deren Elemente die Monoidisomorphismen von M nach sich selbst sind:

$$\mathrm{Aut}_{\mathrm{Mnd}}(M) := \mathrm{End}_{\mathrm{Mnd}}(M)^{\times} = (\mathrm{Isom}(M, M), \circ_{\mathrm{Mnd}}, id_M).$$

  Es geht darum zu zeigen, dass die Komposition zweier Isomorphismen ein Isomorphismus ist.

1.55. Endomorphismen und Automorphismen

- Sei M ein Monoid. Die Elemente des Monoids $\mathrm{End}_{\mathrm{Mnd}}(M)$ werden **Monoidendomorphismen** von M gennant. Die Elemente der Gruppe $\mathrm{Aut}_{\mathrm{Mnd}}(M)$ werden **Monoidautomorphismen** von M gennant.
- Gegeben eine Gruppe G, können wir gleichfalls ein Monoid $\mathrm{End}_{\mathrm{Gpp}}(G)$ und eine Gruppe $\mathrm{Aut}_{\mathrm{Gpp}}(G)$ definieren. Die Elemente des Monoids $\mathrm{End}_{\mathrm{Gpp}}(G)$ werden **Gruppenendomorphismen** von G gennant. Die Elemente der Gruppe $\mathrm{Aut}_{\mathrm{Gpp}}(G)$ werden **Gruppenautomorphismen** von G gennant.

1.56. Beispiel: lineare Transformationen

- Sei V ein Vektorraum und sei $\mathrm{Hom}_{\mathrm{Lin}}(V, V)$ die Menge lineare Abbildungen von V nach sich selbst. Da die Komposition linearer Abbildungen noch linear ist, können wir auf dieser Menge eine Verknüpfung konstruieren.
- Auf diese Weise erhalten wir ein Monoid

$$\mathrm{End}_{\mathrm{Lin}}(V) := (\mathrm{Hom}_{\mathrm{Lin}}(V, V), \circ_{\mathrm{Lin}}, id_V).$$

- Die Gruppe invertierbarer Elemente dieser Gruppe ist die Gruppe, deren zugrundeliegende Menge aus bijektiven linearen Abbildungen besteht:

$$\mathrm{End}_{\mathrm{Lin}}(V)^{\times} = \mathrm{GL}(V).$$

2. Untergruppen und endlich erzeugte Gruppen

	id	σ	τ	R
id	id	σ	τ	R
σ	σ	id	R	τ
τ	τ	R	id	σ
R	R	τ	σ	id

	id	σ	τ	R
id	id	σ	τ	R
σ	σ	id	R	τ
τ	τ	R	id	σ
R	R	τ	σ	id

	id	σ	τ	R
id	id	σ	τ	R
σ	σ	id	R	τ
τ	τ	R	id	σ
R	R	τ	σ	id

2.1. Untermonoide

- Sei $M := (A, \star, e)$ ein Monoid.
- Die Idee ist, dass ein Untermonoid von M aus einer Teilmenge A' von A konstruiert werden kann, wenn die Verknüpfung von M eine Monoidstruktur auf A' *induziert*.
- Genauer gesagt, bitten wir um folgenden Eigenschaften für die Teilmenge $A' : \text{Teil}(A)$.
  - $e \in A'$.
  - $\forall\ a, b : A, a \in A' \wedge b \in A' \Rightarrow a \star b \in A'$.

2.2. Formaler Standpunkt und Notation

- Sei $M := (A, \star, e)$ ein Monoid.
- Ein **Untermonoid** von M ist ein Tupel $M' := (A', e\text{-dadrin}, \star\text{-stabil})$, wobei:
  - A' eine Teilmenge von A ist.
  - e-dadrin ein Beweis für $e \in A'$ ist.
  - $\star$-stabil ein Beweis ist, dass das Produkt zweier Elemente von A, die zu A' gehören, immer noch zu A' gehört:

$$\forall\ a, b : A, a \in A' \wedge b \in A' \Rightarrow a \star b \in A'.$$

- In diesem Fall, sagen wir auch einfach, dass *die Teilmenge A' ein Untermonoid von M ist.*

2.3. Begründung für die Definition

- Seien $M := (A, \star, e)$ ein Monoid und A' ein Untermonoid von M (normalerweise schreiben wir die Eigenschaften e-dadrin und $\star$-stabil nicht).
- Dann gibt es eine Verknüpfung $(\cdot \star' \cdot)$ auf A', die durch $(\cdot \star \cdot)$ induziert wird (siehe unten).
- Da die Verknüpfung $(\cdot \star \cdot) : A \times A \to A$ assoziativ ist, ist die Verknüpfung $(\cdot \star' \cdot) : A' \times A' \to A'$ auch assoziativ.
- Außerdem, da $e \in A'$ gilt, hat die Verknüpfung $(\cdot \star' \cdot)$ ein neutrales Element.
- Ein Submonoid kann daher *automatisch* als Monoid angesehen werden (siehe unten).

2.4. Eine Bemerkung über Teilmengen

- Sei A eine Menge. Aufgrund des Satzes vom ausgeschlossenen Dritten, wird eine Teilmenge $A' : \text{Teil}(A)$ durch eine Indikatorfunktion $\chi_{A'} : A \to \{0, 1\}$ definiert.
- Aus solcher Funktion $\chi_{A'} : A \to \{0, 1\}$ können wir die folgende *Menge* definieren:

$$A' := \{a : A \;/\; \chi_{A'}(a) = 1\}.$$

- Gegeben ein Element $a : A$, wenn wir $a \in A'$ schreiben, meinen wir $\chi_{A'}(a) = 1$. Das heißt, der Ausdruck $a \in A'$ ist eine Eigenschaft des Elements a von A, und A' ist die Menge, die aus den Elementen von A konstruiert wird, die diese Eigenschaft erfüllen.
- Wegen dieser Definitionen sollte ein Element a' der Teilmenge $A' : \text{Teil}(A)$ als Paar $a' := (a, p_a)$ geschrieben werden, wobei a ein Element von A ist, und p_a ein Beweis für die Eigenschaft $\chi_{A'}(a) = 1$ ist.

2.5. Die induzierte Verknüpfung

- Sei $(A, \star, e)$ ein Monoid und $(A', e\text{-dadrin}, \star\text{-stabil})$ ein Untermonoid davon. Insbesondere ist A' eine Teilmenge von A und $\star$-stabil ein Beweis für die folgende Eigenschaft:

$$\forall\ a, b : A, a \in A' \wedge b \in A' \Rightarrow a \star b \in A'$$

- Dann können wir eine Verknüpfung auf der Menge A' definieren:

$$(a, p_a) \star' (b, p_b) := (a \star b, p_{a \star b})$$

  wobei $p_{a \star b}$ der Beweis ist, dass $a \star b \in A'$.
- Dieser Beweis $p_{a \star b}$ wird aus p_a, p_b und $\star$-stabil abgeleitet.

2.6. Eigenschaften der induzierten Verknüpfung

- Da per Definition $(a, p_a) \star' (b, p_b) := (a \star b, p_{a\star b})$, und die Verknüpfung $\star$ assoziativ ist, ist die Verknüpfung $\star'$ auch assoziativ.
- Um ehrlicher zu sein, müssen wir, für alle $a, b, c : A$ die folgende Gleichheit beweisen:

$$((a \star b) \star c, p_{(a\star b)\star c}) = ((a \star (b \star c), p_{a\star(b\star c)})$$

- Dies ergibt sich aus dem Beweis für die Gleichheit $(a\star b)\star c = a\star(b\star c)$ und der Tatsache (die wir akzeptieren werden), dass wenn $(a \star b) \star c = a \star (b \star c)$, dann $p_{(a\star b)\star c} = p_{a\star(b\star c)}$ ist (dies ist der schwierige Teil).
- Außerdem ist das Element $e' := (e, e\text{-dadrin})$ ein neutrales Element für die Verknüpfung $\star'$. Der Beweis dafür geht um dieselben Ideen wie oben.
- Wenn Ihnen dieser formale Standpunkt nicht gefällt, können Sie die Beweise (in Blau) einfach nicht schreiben.

2.7. Untermonoide können als Monoide angesehen werden

- Sei $M := (A, \star, e)$ ein Monoid und $M' := (A', e\text{-dadrin}, \star\text{-stabil})$ ein Untermonoid davon. Insbesondere ist A' eine Teilmenge von A.
- Aus diesem Untermonoid können wir ein Monoid $\widehat{M'} := (A', \star', e')$ konstruieren, wobei:
  - die zugrundeliegende Menge von $\widehat{M'}$ die Menge A' ist,
  - die Verknüpfung von $\widehat{M'}$ die Verknüpfung $\star'$ ist,
  - das neutrales Element von $\widehat{M'}$ das Element $e' := (e, e\text{-dadrin})$ ist.
- Beachten Sie, dass M' und $\widehat{M'}$ sind unterschiedliche Konzepte: M' ist ein Untermonoid von M, während $\widehat{M'}$ ein Monoid ist, das aus M' konstruiert wurde.

2.8. Konventionen und Notation

- Wie gesagt, in der Praxis, schreibt man oft „*Sei* $(A, \star, e)$ *ein Monoid und* A' *ein Untermonoid*“, wobei A' eine Teilmenge von A ist.
- Das heißt, die *Eigenschaften*, dass e zu A' gehört und dass die Teilmenge A' unter der Verknüpfung $\star$ stabil bleibt, erscheinen nicht explizit.
- Es ist auch üblich, ein Untermonoid von $(A, \star, e)$ einfach als ein Monoid zu betrachten, dessen zugrunde liegende Menge eine Teilmenge A' von A ist. Das heißt, man identifiziert oft die Teilmenge A' mit dem Monoid $(A', \star', e)$.

2.9. Beispiele für Untermonoide

- Betrachten wir das Monoid $(\mathbb{Z}, +, 0)$ und eine ganze Zahl $n : \mathbb{Z}$. Die Teilmenge
$$n\mathbb{Z} := \{m \in \mathbb{Z} \ / \ \exists\ q : \mathbb{Z},\ m = q * n\}$$
von Vielfachen von n *ist* ein Untermonoid von $\mathbb{Z}$ (das heißt, diese Teilmenge erfüllt die Eigenschaften eines Untermonoids):
  - Da $n * 0 = 0$ ist, gilt $0 \in n\mathbb{Z}$.
  - Wenn $m_1 = q_1 * n$ ist und $m_2 = q_2 * n$ ist, gilt $m_1 + m_2 = (q_1 + q_2) * n$, somit $(m_1 + m_2) \in n\mathbb{Z}$.
- Die Teilmenge $\mathbb{Z}_{\geqslant 0} := \{n : \mathbb{Z} \ / \ n \geqslant 0\}$ ist ein Untermonoid von $\mathbb{Z}$.
- Die Teilmenge $\mathbb{Z}_{>0} := \{n : \mathbb{Z} \ / \ n > 0\}$ ist kein Untermonoid von $(\mathbb{Z}, +, 0)$. Grund dafür ist, dass das neutrales Element 0 nicht zu dieser Teilmenge gehört.

2.10. Untergruppen

- Sei $G := (A, \star, e)$ eine Gruppe und $A' : \text{Teil}(A)$ eine Teilmenge von A.
- Wir sagen, dass A' eine **Untergruppe** von G ist, wenn die folgende Eigenschaften gelten:
  - $e \in A'$.
  - $\forall\ a, b : A, a \in A' \wedge b \in A' \Rightarrow a \star b \in A'$.
  - $\forall\ a : A, a \in A' \Rightarrow a^{-1} \in A'$.
- Aus formaler Sicht, ist eine Untergruppe von $G := (A, \star, e)$ daher ein Tupel
$$U := (A', e\text{-dadrin}, \star\text{-stabil}, \text{inv-stabil}),$$
wobei $(A', e\text{-dadrin}, \star\text{-stabil})$ ein Untermonoid von $(A, \star, e)$ ist und inv-stabil ein Beweis ist, dass $\forall\ a : A, a \in A' \Rightarrow a^{-1} \in A'$.

2.11. Beispiele für Untergruppen

- Sei $G := (A, \star, e)$ eine Gruppe und A' die Teilmenge $\{e\}$ von A. Dann ist A' eine Untergruppe von G. Wenn wir A als eine Teilmenge seiner selbst betrachten, dann ist A auch eine Untergruppe von $(A, \star, e)$. Die leere Teilmenge ist keine Untergruppe.
- Betrachten wir die Gruppe $(\mathbb{Z}, +, 0)$ und eine ganze Zahl $n : \mathbb{Z}$. Die Teilmenge
$$n\mathbb{Z} := \{m : \mathbb{Z} \ / \ \exists\ q : \mathbb{Z},\ m = q * n\}$$
von Vielfachen von n ist eine Untergruppe von $\mathbb{Z}$:
  - Wir haben bereits bewiesen, dass $n\mathbb{Z}$ ein Untermonoid von $(\mathbb{Z}, +, 0)$ ist.
  - Wenn $m = q * n$, gilt $-m = -(q * n) = (-q) * n$, somit $(-m) \in n\mathbb{Z}$.
- Die Teilmenge $\{n : \mathbb{Z} \ / \ n \geqslant 0\}$ ist ein Untermonoid von $(\mathbb{Z}, +, 0)$, die keine Untergruppe ist. Grund dafür ist, dass (zum Beispiel) 1 zu dieser Teilmenge gehört, aber-1 nicht.

2.12. Untergruppen der Symmetriegruppe eines Quadrats

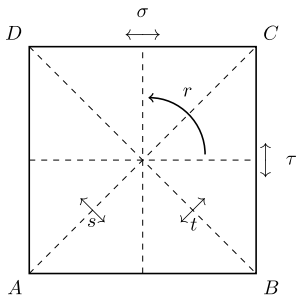

Abbildung 2.1.: Symmetriegruppe eines Quadrats.

- In der Symmetriegruppe eines Quadrats, ist die Teilmenge $\{id, r, r^2, r^3\}$ eine Untergruppe. Diese Untergruppe ist genau die Gruppe der *direkten* Symmetrien des Quadrats (die Reihenfolge der Punkte A, B, C, D ändert sich nach eine Rotation nicht).
- Die Teilmenge $\{id, s\}$, $\{id, t\}$,$\{id, \sigma\}$ und $\{id, \tau\}$ sind auch Untergruppe der Symmetrie gruppe des Quadrats.

2.13. Direkte Symmetrien des Quadrats

Die Verknüpfungstafel der Untergruppe $\{id, r, r^2, r^3\}$ ist unten sichtbar. Sie ist sozusagen in der Verknüpfungstafel der Umbgebungsgruppe abgeschlossen.

	id	r	r^2	r^3	s	t	σ	τ
id	id	r	r^2	r^3	s	t	σ	τ
r	r	r^2	r^3	id	σ	τ	t	s
r^2	r^2	r^3	id	r	t	s	τ	σ
r^3	r^3	id	r	r^2	τ	σ	s	t
s	s	τ	t	σ	id	r^2	r^3	r
t	t	σ	s	τ	r^2	id	r	r^3
σ	σ	s	τ	t	r	r^3	id	r^2
τ	τ	t	σ	s	r^3	r	r^2	id

2.14. Andere Untergruppen

Bei anderen Untergruppen kann es etwas komplizierter sein, die Verknüpfungstafel zu visualisieren, aber immer noch möglich.

	id	r	r^2	r^3	s	t	σ	τ
id	id	r	r^2	r^3	s	t	σ	τ
r	r	r^2	r^3	id	σ	τ	t	s
r^2	r^2	r^3	id	r	t	s	τ	σ
r^3	r^3	id	r	r^2	τ	σ	s	t
s	s	τ	t	σ	id	r^2	r^3	r
t	t	σ	s	τ	r^2	id	r	r^3
σ	σ	s	τ	t	r	r^3	id	r^2
τ	τ	t	σ	s	r^3	r	r^2	id

2.15. Untergruppen der Gruppe der ganzen Zahlen

Wir kommen endlich zu einem konkreten und nützlichen Satz .

Satz. Die nicht-trivialen Untergruppen von $(\mathbb{Z}, +, 0)$ sind genau die Teilmengen der Gestalt $n\mathbb{Z}$ für ein eindeutiges bestimmtes $n \in \mathbb{Z}_{>0}$.

- Mit nicht-trivialer Untergruppe einer Gruppe $G := (A, \star, e)$ meinen wir eine Untergruppe $U := A'$, die die folgende Eigenschaft erfüllt:

$$\exists\, a : A, (a \in A') \wedge (a \neq e).$$

- Dies wird normalerweise als $U \neq \{e\}$ geschrieben. Ob dies eine primitive Definition oder eine Konsequenz der Definition von $U = \{e\}$ ist, hängt davon ab, wie frei Sie das Prinzip des ausgeschlossenen Dritten anwenden.
- Es ist auch möglich, $\exists\, a : G, (a \in U) \wedge (a \neq e)$ zu schreiben.

2.16. Satz und Beweis

Satz. Sei U eine Untergruppe von $(\mathbb{Z}, +, 0)$. Wenn U nicht-trivial ist, dann existiert es eine eindeutige positive ganze Zahl $n \in \mathbb{Z}_{>0}$, so dass $U = n\mathbb{Z}$ ist.

Beweis. Beachten Sie, dass dieser Satz aus zwei Teilen besteht:

- Existenz:
$$\exists\, n \in \mathbb{Z}_{>0}, U = n\mathbb{Z}.$$
- Eindeutigkeit:
$$\forall\, m, n : \mathbb{Z}_{>0}, (U = m\mathbb{Z}) \wedge (U = n\mathbb{Z}) \Rightarrow m = n.$$

Wir können auch $\mathbb{N}$ statt $\mathbb{Z}_{>0}$ schreiben. So oder so, wenn wir $n\mathbb{Z}$ schreiben, müssen wir das Element n von $\mathbb{Z}_{>0}$ oder $\mathbb{N}$ als Element von $\mathbb{Z}$ interpretieren.

2.17. Existenz

- Zeigen wir zuerst, dass $U \cap \mathbb{N} \neq \emptyset$. Da per Annahme U nicht-trivial ist, existiert ein $n : \mathbb{Z}$, so dass $n \in U$ und $n \neq 0$. Diese n erfüllt $n > 0 \vee n < 0$. Wir können daher zwei Fälle unterscheiden.
  - Falls $n > 0$, dann haben wir es bewiesen, dass $U \cap \mathbb{N} \neq \emptyset$ ist.
  - Falls $n < 0$, dann ist $-n > 0$. Aber $-n \in U$ (da $n \in U$ ist und U eine Untergruppe ist). Dann gilt wieder $U \cap \mathbb{N} \neq \emptyset$.
- Da $U \cap \mathbb{N}$ eine nicht-leere Teilmenge von $\mathbb{N}$ ist, existiert es ein minimales Element n_0 in $U \cap \mathbb{N}$ (das heißt, $n_0 \in U \cap \mathbb{N}$ und $\forall\ m : \mathbb{N},\ m \in U \cap \mathbb{N} \Rightarrow n_0 \leqslant m$). Insbesondere $n_0 \in U$.
- Wir werden nun zeigen, dass $n_0\mathbb{Z} = U$ (für dieses n_0, deren Existenz wir bewiesen haben). Es reicht, $n_0\mathbb{Z} \subseteq U$ und $U \subseteq n_0\mathbb{Z}$ zu zeigen.

2.18. Direkte Inklusion

Zeigen wir zunächst, dass $n_0\mathbb{Z} \subseteq U$ ist. Das heißt, $\forall\ m : \mathbb{Z}, m \in n_0\mathbb{Z} \Rightarrow m \in U$. Gegeben $m : \mathbb{Z}$ sodass $m \in n_0\mathbb{Z}$ ist, existiert ein $q : \mathbb{Z}$, sodass $m = q * n$ ist. Dieses q erfüllt $(q \geqslant 0) \vee (q < 0)$. Durch Fallunterscheidung, erhalten wir Folgendes. - Falls $q \geqslant 0$ ist, gilt $m = q * n_0 = n_0 + \ ... \ + \ n_0$ (q mal). Da $0 \in U$ und $n_0 \in U$, können wir durch Induktion auf q zeigen, dass $q * n_0 \in U$ ist. Das heißt, $m_0 \in U$ ist. - Wenn $q < 0$, dann gibt es $-m = -(q * n_0) = (-q) * n_0$. Aus dem vorherigen Fall folgern wir, dass $-m \in U$. Da U eine Untergruppe ist, gilt auch $m \in U$.

2.19. Umgekehrte Inklusion und Ende des Existenzbeweises

- Zeigen wir danach, dass $U \subseteq n_0\mathbb{Z}$ ist.
- Gegeben $m : \mathbb{Z}$ sodass $m \in U$ ist, die Division mit Rest von m durch n_0 (die > 0 ist) ergibt ganze Zahlen q und r, so dass $m = q * n_0 + r$ und $0 \leqslant r < n_0$. Insbesondere, $r = m - q * n_0$ ist. Da U eine Untergruppe ist, impliziert die vorherige Gleichheit, dass $r \in U$ (denn $m \in U$ ist und $n_0 \in U$). Wenn $r \neq 0$ ist, widerspricht das der Minimalität von n_0 als Element von $U \cap \mathbb{Z}_{>0}$. Dann gilt $r = 0$ und $m = q * n_0$. Das heißt, $m \in n_0\mathbb{Z}$.
- Da $n_0\mathbb{Z} \subseteq U$ ist und $U \subseteq n_0\mathbb{Z}$ ist, haben wir bewiesen, dass $U = n_0\mathbb{Z}$ ist.

2.20. Eindeutigkeit

- Nehmen wir an, dass es $m : \mathbb{Z}$ und $n : \mathbb{Z}$ gibt, sodass $n > 0$, $m > 0$ und $n\mathbb{Z} = m\mathbb{Z}$ gelten. Wir werden es zeigen, dass dies $n = m$ impliziert.

- Von der Gleichheit $n\mathbb{Z} = m\mathbb{Z}$ folgern wir, dass die ganze Zahl m die ganze Zahl n teilt, und dass die ganze Zahl n die ganze Zahl m teilt. Das heißt, es existiert a sodass $n = a * m$ ist, und b sodass $m = b * n$ ist. Dann gilt $n = a * b * n$.
- Da $n \neq 0$, impliziert die vorherige Gleichheit, dass $a * b = 1$ ist, mit a eine ganze Zahl. Insbesondere gilt $a = 1$ oder $a = -1$.
- Da $n = a * m$ und $n, m > 0$, muss a auch positiv sein. Dann gilt $a = 1$, somit $n = m$.

2.21. Vergleich der Untergruppen einer Gruppe

- Sei $G = (A, \star, e)$ eine Gruppe und seien $U_1 = (A'_1, \ \dots\ )$ und $U_2 = (A'_2, \ \dots\ )$ Untergruppen von G, wobei A'_1 und A'_2 Teilmenge von A sind. Können wir U_1 und U_2 vergleichen?
- Betrachten wir die folgende Relation:
$$U_1 \preccurlyeq U_2 := A'_1 \subseteq A'_2.$$
- Da $\subseteq$ eine Ordnungsrelation auf Teil(A) ist, ist die Relation $\preccurlyeq$ eine Ordnungsrelation (zwischen Untergruppen von G).

2.22. Eine Bemerkung über binäre Relationen

- Denken wir zunächst daran, dass die Relation $A'_1 \subseteq A'_2$ Folgendes bedeutet:
$$\forall\ a : A, a \in A'_1 \Rightarrow a \in A'_2.$$
- So wie die Zugehörigkeit von einem Element $a : A$ zu einer Teilmenge A' durch ein unäres Prädikat $\chi_{A'} : A \to \{0, 1\}$ definiert wird, wird eine Relation auf einer Menge B durch ein binäres Prädikat $R : B \times B \to \{0, 1\}$ definiert.
- Zum Beispiel, für $B := Teil(A)$, wird das binäre Prädikat $\subseteq$ durch die Funktion $R_\subseteq$ definiert, die ein Paar Teilmengen (A'_1, A'_2) genau dann nach 1 abbildet, wenn $\forall\ a : A, a \in A'_1 \Rightarrow a \in A'_2$.
- Wenn wir versuchen, diese Funktion explizit zu berechnen, erhalten wir Folgendes:
$$R_\subseteq(A'_1, A'_2) := \inf_{a:A} \Big(\max\left(1 - \chi_{A'_1}(a), \chi_{A'_2}(a)\right)\Big).$$

2.23. Von einer Teilmenge erzeugte Untergruppe

- Sei $G := (A, \star, e)$ eine Gruppe. Gegebene eine Teilmenge $E : \text{Teil}(A)$, gibt es eine *kleinste* Untergruppe $U := (A', \ \dots\ )$ von G, sodass $E \subseteq A'$?
- Da wir Untegruppen von G vergleichen können, ist die Frage sinnvoll. Das heißt, das Konzept eines kleinsten Elements ist in diesem Zusammenhang sinnvoll.
- Beachten wir zunächst, dass es mindestens eine Untergruppe $U := (A', \ \dots\ )$ gibt, sodass $E \subseteq A'$ ist. Nämlich, die Untergruppe $G = (A, \ \dots\ )$.
- Wir werden nun auf zwei verschiedenen Arten zeigen, dass die Menge aller dieser Untergruppen ein minimales Element hat.

2.24. Durchschnitt von Untergruppen

- Seien $G = (A, \star, e)$ eine Gruppe und $(U_i)_{i:I}$ eine Familie Untergruppen von G. Das heißt, für jedes $i : I$, eine Untergruppe $U_i := (A'_i, e\text{-dadrin}, \star\text{-stabil}, \text{inv-stabil})$ von G.
- Wir möchten eine Untergruppe $\wedge_{i:I} U_i := (A',\ \dots\ )$ von G konstruieren, mit

$$A' := \cap_{i:I} A'_i.$$

- Es reicht dazu, die folgende Eigenschaften zu beweisen:
  - $e \in A'$ (das heißt, $\forall\ i : I, e \in A'_i$).
  - $\forall\ a, b : A, a \in A' \wedge b \in A' \Rightarrow \forall\ i : I, a \star b \in A'_i$.
  - $\forall\ a : A, a \in A' \Rightarrow \forall\ i : I, a^{-1} \in A'_i$.
- Alle drei Eigenschaften ergeben sich aus der Tatsache, dass für jedes $i : I$, $A' \subseteq A'_i$ ist.

2.25. Erzeugte Untergruppe: erste Konstruktion

- Seien $G := (A, \star, e)$ eine Gruppe und $E : \text{Teil}(A)$ eine Teilmenge von A.
- Betrachten wir die folgende Menge, die als Teilmenge von der Menge der Untergruppen von G definiert wird:

$$I := \{U := (A',\ \dots\ ) : \text{Untergruppe}(G)\ /\ E \subseteq A'\}$$

- Da es eine Projektion $\text{pr}_1 : I \to \text{Untergruppe}(G)$ gibt, können wir eine Familie $(U_i)_{i:I}$ definieren. Explizit ist $i : I$ aus der Form (U, p_U), wobei $U := (A',\ \dots\ )$ eine Untergruppe von G ist, und p_U ein Beweis für die Eigenschaft $E \subseteq A'$ ist. Dann wird $\text{pr}_1(U, p_U)$ als U definiert. Wir setzen dann, für jedes $i : I$, $U_i := \text{pr}_1(i)$.
- Es ist deshalb sinnvoll, die Untergruppe $\langle E \rangle_G := \wedge_{i:I} U_i$ einzuführen. Diese Untergruppe $\wedge_{i:I} U_i$ wird **die von der Teilmenge E erzeugte Untergruppe** gennant (und oft einfach als $\langle E \rangle$ bezeichnet).

2.26. Die kleinste Untergruppe, die eine Teilmenge enthält

- Seien $G := (A, \star, e)$ eine Gruppe und $E : \text{Teil}(A)$ eine Teilmenge von A. Sei $(U_i)_{i:I}$ die Familie aller Untergruppen von G, die die Eigenschaft $E \subseteq A'_i$ erfüllen, wobei A'_i die zugrundeliegende Menge der Untergruppe U_i ist. Wie zuvor gesehen, ist die zugrundeliegende Menge der Untergruppe $\langle E \rangle := \wedge_{i:I} U_i$ die Teilmenge $\cap_{i:I} A'_i$.
- Dann können wir überprüfen, dass die Untergruppe $\langle E \rangle$ die kleinste Untergruppe $U := (A',\ \dots\ )$ von G ist, die die Eigenschaft $E \subseteq A'$ erfüllt. Das heißt:

  - Die Untergruppe $\langle E \rangle$ erfüllt diese Eigenschaft.
  - Für jede Untergruppe U, die diese Eigenschaft erfüllt, gilt $\langle E \rangle \preccurlyeq U$.

- Die erste Eigenschaft folgt von der Tatsache, dass $E \subseteq \cap_{i:I} A_i$ ist (per Definition von A_i, gilt für jedes $i : I$, dass $E \subset A_i$ ist). Die zweite Eigenschaft folgt von der Tatsache, dass $\forall\ j : I, \cap_{i:I} A_i \subseteq A_j$ ist.

2.27. Induktive Definition

- Es gibt eine andere, explizitere Konstruktion der Untergruppe $\langle E \rangle$. Nämlich, durch die direkte Definition eines Prädikats $\chi_{\langle E \rangle} : A \to \{0, 1\}$.
- Gegeben $a : A$, setzen wir genau dann $\chi_{\langle E \rangle}(a) := 1$, wenn eine der folgenden Bedingungen gilt:
  - $a = e$.
  - $a \in E$.
  - $a = a_1 \star a_2$, mit $a_1, a_2 : A$, sodass $\chi_{\langle E \rangle}(a_1) = 1$ und $\chi_{\langle E \rangle}(a_2) = 1$.
  - $a = b^{-1}$, mit $b : A$, sodass $\chi_{\langle E \rangle}(b) = 1$.
- Dieses Prädikat definiert eine Teilmenge $\langle E \rangle : \mathrm{Teil}(A)$, nämlich:

$$\langle E \rangle := \{a : A \ / \ \chi_{\langle E \rangle}(a) = 1\}$$

2.28. Erzeugte Untergruppe: zweite Konstruktion

- Überprüfen wir, dass die Teilmenge $\langle E \rangle : \mathrm{Teil}(A)$ eine Untergruppe von G definiert.
- Es reicht dazu, die folgende Eigenschaften zu beweisen:
  - $\chi_{\langle E \rangle}(e) = 1$.
  - $\forall\ a_1, a_2 : A, \chi_{\langle E \rangle}(a_1) = 1 \wedge \chi_{\langle E \rangle}(a_2) = 1 \Rightarrow \chi_{\langle E \rangle}(a_1 \star a_2) = 1$.
  - $\forall\ b : A, \chi_{\langle E \rangle}(b) = 1 \Rightarrow \chi_{\langle E \rangle}(b^{-1}) = 1$.
- Alle drei Eigenschaften folgen unmittelbar aus der Definition des Prädikats $\chi_{\langle E \rangle}$. Es gibt fast nichts zu beweisen!

2.29. Induktiver Beweis

- Außerdem haben wir $\forall\ a : A, a \in E \Rightarrow \chi_{\langle E \rangle}(a) = 1$, auch per Definition des Prädikats $\chi_{\langle E \rangle}$. Das heißt, die Untergruppe $\langle E \rangle$ erfüllt die Bedingung $E \subset \langle E \rangle$ (als Teilmenge von A).
- Schließlich ist die induktiv definiert Untergruppe $\langle E \rangle$ die kleinste Untergruppe, die die vorherige Bedingung erfüllt.

- Um das zu zeigen, reicht es Folgendes zu bemerken: Wenn $U := (A',\ \dots\ )$ eine Untergruppe mit $E \subseteq A'$ ist, dann ist $\langle E\rangle \subseteq A'$. Das heißt, für jedes $g : G$,

$$g \in \langle E\rangle \Rightarrow g \in A'.$$

- Da die Eigenschaft $g \in \langle E\rangle$ induktiv definiert wurde, können wir die vorherige Implikation *durch Induktion auf* g beweisen. Dann folgt das Ergebnis aus der Definition von $g \in \langle E\rangle$ und der Tatsache, dass A' eine Untergruppe ist. Die Einzelheiten werden nun erklärt.

2.30. Einzelheiten zum induktiven Beweis

- **Induktionsanfang.** Zunächst müssen wir überprüfen, ob, wenn $a = e$ oder $a \in E$, dann $a \in A'$ ist. Dies folgt aus der Tatsache, dass A' eine Untergruppe von G ist, die E enthält.
- **Induktionsschritt.** Danach müssen wir überprüfen, ob, wenn $a = a_1 \star a_2$ mit $a_1, a_2 \in \langle E\rangle$ ist, dann $a \in A'$ ist. *Durch Induktion können wir annehmen*, dass $a_1 \in A'$ ist und $a_2 \in A'$ ist . Da A' eine Untergruppe ist, ergibt sich deshalb $a_1 \star a_2 \in A'$. Schließlich müssen wir überprüfen, ob, wenn $a = b^{-1}$ mit $b \in \langle E\rangle$ ist, dann $a \in A'$ ist. Durch Induktion können wir annehmen, dass $b \in A'$ ist. Dann folgt das Erggebnis erneut aus der Tatsache, dass A' eine Untergruppe ist.

  Diese Art von Beweis lässt sich mit einem Beweisassistenten einfacher schreiben!

2.31. Endlich erzeugte Gruppen und zyklische Gruppen

- Sei $G = (A,\ \dots,\ )$ eine Gruppe. Man sagt, dass die Gruppe G **endlich erzeugt** ist, wenn es eine *endliche* Teilmenge $E : \mathrm{Teil}(A)$ gibt, sodass $\langle E\rangle = A$ ist (als Teilmenge von A). Man schreibt oft:

$$\exists\ n : \mathbb{N}_{\geqslant 0},\ \exists\ g_0,\ \dots\ g_n : G,\ \langle g_0,\ \dots,\ g_n\rangle = G.$$

- In diesem Fall wird die Teilmenge $\{g_0,\ \dots,\ g_n\} : \mathrm{Teil}(A)$ als **Erzeugendensystem** für die Gruppe G bezeichnet.
- Wenn G durch ein einziges Element g_0 erzeugt werden kann (das heißt, wenn $E = \{g\}$ ist), wird die Gruppe G eine **zyklische Gruppe** gennant:

$$\exists\ g : G, \langle g\rangle = G \text{ (als Untergruppe von } G).$$

2.32. Übung 1

- Seien G eine Gruppe und E ein Erzeugendsystem für G. Zeigen Sie, dass die Elemente von G die folgende Beschreibung zulassen.

$$\forall\ g : G,\ \exists\ n : \mathbb{N}_{\geqslant 0},\ \exists\ g_0,\ ...,\ g_n \in E,\ \exists\ \varepsilon_0,\ ...,\ \varepsilon_n : \{\pm 1\},\ g = g_0^{\varepsilon_0}\ ...\ g_n^{\varepsilon_n}.$$

Hinweis. Die Annahme ist, dass $G = \langle E \rangle$ ist. Deshalb können Sie das Ergebnis durch Induktion über $g \in \langle E \rangle$ zeigen. Oder, benuzten Sie einen anderen Ansatz und zeigen Sie, dass die Teilmenge

$$T := \{g : G\ /\ \exists\ n : \mathbb{N}_{\geqslant 0},\ \exists\ g_0,\ ...,\ g_n \in E,\ \exists\ \varepsilon_0,\ ...,\ \varepsilon_n : \{\pm 1\},\ g = g_0^{\varepsilon_0}\ ...\ g_n^{\varepsilon_n}.\}$$

eine Untergruppe von G ist, die E enthält, und die in jeder Untergruppe U enthalten ist, die E enthält.

2.33. Übung 2

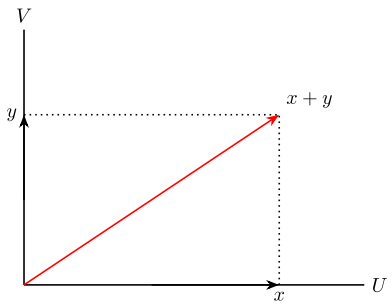

Abbildung 2.2.: Die von einer Vereinigung Untergruppen erzeugte Untergruppe

- Wie wir in der linearen Algebra gelernt haben, ist die Vereinigung zweier Untergruppen im Allgemeinen keine Untergruppe.
- Seien G eine Gruppe und U, V Untergruppen von G. Zeigen Sie, dass die Teilmenge

$$P(U, V) := \{g : G\ /\ \exists\ u : U,\ \exists\ v : V,\ g = u \star v\}$$

ein Erzeugendsystem für die Untergruppe $UV := \langle U \cup V \rangle$ ist.

2.34. Der Kern eines Gruppenhomomorphismus

- Seien $G := (A, \star_G, e_G)$ und $H := (B, \star_H, e_H)$ Gruppen und sei $\varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G, H)$ ein Gruppenhomomorphismus.
- Bezeichnen wir noch die zugrundeliegende Abbildung von φ mit $\varphi : A \to B$, und die davon induzierte Abbildung $\mathrm{Teil}(B) \to \mathrm{Teil}(A)$ mit φ^{-1}. Für jede $B' : \mathrm{Teil}(B)$, heißt die Teilmenge $\varphi^{-1}(B') := \{a : A \ / \ \varphi(a) \in B\}$ von A das **Urbild** von B'.

  Satz. Die Teilmenge

  $$\ker \varphi := \varphi^{-1}(\{e_H\}) = \{a : A \ / \ \varphi(a) = e_H\}$$

  ist eine Untergruppe von G.
- Die Untergruppe $\ker \varphi \preccurlyeq G$ wird als **Kern** des Homomorphismus φ bezeichnet.

2.35. Ein Beweis, dass der Kern eine Untergruppe ist

- Es reicht zu überprüfen:

  1. $e_G \in \ker \varphi$.
  2. $\forall\ g_1, g_2 : G,\ g \in \ker \varphi \Rightarrow (g_1 \star_G g_2) \in \ker \varphi$.
  3. $\forall\ g : G,\ g \in \ker \varphi \Rightarrow g^{-1} \in \ker \varphi$.
- Dazu berechnen wir:

  1. $\varphi(e_G) = e_H$ (per Definition eines Gruppenhomomorphismus).
  2. $\varphi(g_1 \star_G g_2) = \varphi(g_1) \star_H \varphi(g_2) = e_H \star_H e_H = e_H$.
  3. $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$.
- **Anmerkung.** Die Eigenschaft $\varphi(g^{-1}) = \varphi(g)^{-1}$ wurde im Vortrag 1.a, Übung 4 bewiesen.

2.36. Das Bild eines Gruppenhomomorphismus

- Seien $G := (A, \star_G, e_G)$ und $H := (B, \star_H, e_H)$ Gruppen und sei $\varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G, H)$ ein Gruppenhomomorphismus.
- Bezeichnen wir noch die zugrundeliegende Abbildung von φ mit $\varphi : A \to B$, und die davon induzierte Abbildung $\mathrm{Teil}(A) \to \mathrm{Teil}(B)$ *immer noch* mit φ. Für jede $A' : \mathrm{Teil}(A)$, heißt die Teilmenge $\varphi(A') := \{b : B \ / \ \exists\ a : A, \varphi(a) = b\}$ von A das Bild von B' unter φ. Wenn $A' = A$, schreiben wir auch $\varphi(G)$ statt $\varphi(A)$.

Satz. Die Teilmenge

$$\operatorname{im}\varphi := \varphi(G) = \{h : H \;/\; \exists\, g : G, \varphi(g) = h\}$$

ist eine Untergruppe von H.

- Die Untergruppe $\operatorname{im}\varphi \preccurlyeq H$ wird das **Bild** des Homomorphismus φ gennant.

2.37. Ein Beweis, dass das Bild eine Untergruppe ist

Wie zuvor:

1. Mit $g := e_G$ gibt es $\varphi(e_G) = e_H$. Somit $e_H \in \varphi(G)$.
2. Falls $h_1 = \varphi(g_1)$ ist und $h_2 = \varphi(g_2)$ ist, mit $g_1, g_2 : G$, dann ergibt sich

$$h_1 \star_H h_2 = \varphi(g_1) \star_H \varphi(g_2) = \varphi(g_1 \star_G g_2) \in \varphi(G).$$

3. Falls $h = \varphi(g)$ ist, mit $g : G$, dann ergibt sich $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$, somit $h^{-1} \in \varphi(G)$.

2.38. Injektive und surjektive Gruppenhomomorphismen

- Ein Gruppenhomorphismus φ wird injektiv/surjektiv genannt, wenn die zugrundeliegende Abbildung injektiv/surjektiv ist.
- Dann gelten die folgenden Eigenschaften, die zu der von linearen Algebra ähnlich sind.

  Satz. Seien G und H Gruppen und sei $\varphi : \operatorname{Hom}_{\mathrm{Gpp}}(G, H)$ ein Gruppenhomomorphismus.

  1. φ ist genau dann injektiv, wenn $\ker\varphi = \{e_G\}$.
  2. φ ist genau dann surjektiv, wenn $\operatorname{im}\varphi = H$.

- Die zweite Eigenschaft folgt von der Definition des Bildes. Zeigen wir die erste.

2.39. Erinnerung an die (Nicht-)Injektivität

- Eine Abbildung $f : A \to B$ heißt **nicht-injektiv**, falls gilt

$$\exists\, a_1, a_2 : A,\; a_1 \neq a_2 \wedge f(a_1) = f(a_2).$$

- Wenn dies *nicht passiert*, sagt man das f injektiv ist. Das heißt,

$$\begin{aligned} f \text{ injektiv} &:= \neg(\exists\ a_1, a_2 : A,\ a_1 \neq a_2 \wedge f(a_1) = f(a_2)) \\ &\Leftrightarrow \forall\ a_1, a_2 : A, f(a_1) = f(a_2) \Rightarrow \neg(a_1 \neq a_2) \\ &\Leftrightarrow \forall\ a_1, a_2 : A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \end{aligned}$$

  Die Eigenschaft $\neg(a_1 \neq a_2) \Leftrightarrow a_1 = a_2$ sollte als Eigenschaft der Unterscheidungsrelation $\neq$ betrachten werden.

- Der Punkt ist: Da per Definition (f injektiv) $:= \neg(f$ nicht-injektiv) ist, haben wir immer f nicht-injektiv $\Rightarrow \neg(f$ injektiv). Aber ohne LEM gilt die umgekehrte Implikation nicht, nur $\neg(f$ injektiv) $\Rightarrow \neg\neg(f$ nicht-injektiv), deren Schlussfolgerung schwächer ist.

2.40. Beweis für die Charakterisierung der Injektivität

- „$\Rightarrow$“ Nehmen wir zunächst an, dass φ injektiv ist, und zeigen wir, dass $\ker \varphi = \{e_G\}$. Da immer gilt $e_G \in \ker \varphi$, reicht es zu überprüfen, dass $\ker \varphi \subset \{e_G\}$. Das heißt, für alle $g : G,\ \varphi(g) = e_H \Rightarrow g = e_G$. Sei $g : G$ solches Element, mit $\varphi(g) = e_H$. Da $\varphi(e_G) = e_H$ auch gilt, und φ injektiv ist, ergibt sich $e_G = g$.
- „$\Leftarrow$“ Nehmen wir jetzt an, dass $\ker \varphi = \{e_G\}$ ist, und zeigen wir, dass φ injektiv ist. Es reicht zu überprüfen, ob, wenn $\varphi(g_1) = \varphi(g_2)$ in H ist, dann $g_1 = g_2$ in G ist. Seien $g_1, g_2 : G$, sodass $\varphi(g_1) = \varphi(g_2)$. Da φ ein Gruppenhomomorphismus ist, impliziert die vorherige Gleicheit, dass $\varphi(g_1 \star_G g_2^{-1}) = e_H$. Das heißt, $g_1 \star_G g_2^{-1} \in \ker \varphi$ ist. Da $\ker \varphi = \{e_G\}$ ist, folgt daraus, dass $g_1 \star_G g_2^{-1} = e_G$ ist, somit $g_1 = g_2$.

2.41. Übung 3

- Seien G, H Gruppen und $\varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G, H)$ ein Gruppenhomomorphismus. Zeigen Sie die folgende Eigenschaften:

  1. Wenn $U \preccurlyeq G$ (U eine Untergruppe von G) ist, ist $\varphi(U) \preccurlyeq H$.
  2. Wenn $V \preccurlyeq H$ ist, ist $\varphi^{-1}(V) \preccurlyeq G$.
  3. Wenn $E : \mathrm{Teil}(G)$ ist, gilt $\varphi(\langle E \rangle) = \langle \varphi(E) \rangle$ als Untergruppe von G.
  4. Wenn $F : \mathrm{Teil}(H)$ ist, gilt im Allgemeinem $\varphi^{-1}(\langle F \rangle) \neq \langle \varphi^{-1}(F) \rangle$.

  Hinweis. Für den letzten, betrachten Sie das Beispiel

$$G = (\mathbb{Z}, +),\ N = \{1\},\ \text{und } \forall\ n : \mathbb{Z},\ \varphi(n) := 0.$$

2.42. Übung 4

- Seien G, H Gruppen und sei $\varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G, H)$ ein Gruppenhomomorphismus. Gegeben $b : H$, die Menge $\varphi^{-1}(\{b\}) : \mathrm{Teil}(H)$ heißt die **Faser** von φ über b.
- Zum Beispiel, ist die Faser von φ über e_H genau der Kern von φ.

$$\varphi^{-1}(\{e_H\}) = \ker \varphi$$

- Zeigen Sie, dass die Fasern von F die folgende Beschreibung zulassen:

$$\forall\ b : H,\ \varphi^{-1}(b) \neq \emptyset\ \Rightarrow\ \forall\ a \in \varphi^{-1}(\{b\}), \varphi^{-1}(b) = a(\ker \varphi)$$

  wobei $a(\ker \varphi) \coloneqq \{g : G\ /\ \exists\ c : G,\ g = a \star_G c\}$.

  Dies ähnelt dem bekannten Ergebnis aus der linearen Algebra: wenn sie nicht leer ist, kann die Menge der Lösungen eines linearen Gleichungssystems $Ax = b$ als $a + kerA$ beschrieben werden, wobei a eine beliebige Lösung von $Ax = b$ ist.

2.43. Elemente endlicher Ordnung

- Sei G eine Gruppe und sei g ein Element von G. Per Definition:

$$g^0 \coloneqq e_G \text{ und } \forall\ m : \mathbb{N}_{\geqslant 0}, g^{m+1} \coloneqq g^m \star_G g.$$

- Dies ist tatsächlich eine Abbildung $G \times \mathbb{N}_{\geqslant 0} \to G$, die (g, n) nach g^n abbildet. Durch Induktion können Sie es beweisen, dass die folgende Eigenschaft gilt.

$$\forall\ m : \mathbb{N}_{\geqslant 0},\ g^{m+1} = g \star_G g^m.$$

- Man sagt, dass g **endliche Ordnung** hat, falls die folgende Eigenchaft gilt.

$$\exists\ n : \mathbb{N}_{>0},\ g^n = e_G.$$

2.44. Die Ordnung eines Elements

- Falls $g : G$ endliche Ordnung hat, kann man Folgendes festlegen:

$$\mathrm{Ord}_G(g) \coloneqq \min\{n : \mathbb{N}_{>0}\ /\ g^n = e_G\}$$

- Die natürliche Zahl $\mathrm{Ord}_G(g)$ heißt die **Ordnung** von g. Mittels euklidischer Division können wir die Struktur der Menge $\{n : \mathbb{N}_{>0}\ /\ g^n = e_G\}$ verdeutlichen. Man schreibt einfach $\mathrm{Ord}(g)$ statt $\mathrm{Ord}_G(g)$.
- Wenn g nicht endliche Ordnung hat, sagt man, dass g **unendliche Ordnung** hat, und setzt $\mathrm{Ord}(g) \coloneqq +\infty$.
- Da in diesem Fall die Menge $\{n : \mathbb{N}_{>0}\ /\ g^n = e_G\}$ leer ist, entspricht diese Definition der üblichen Konvention, dass $\inf \emptyset = +\infty$ ist.

2.45. Potenzen eines Elements

Satz. Sei $g : G$ und $n : \mathbb{N}_{>0}$. Dann gilt,

$$g^n = e_G \Leftrightarrow (g \text{ hat endliche Ordnung und } \mathrm{Ord}(g) \mid n) \ .$$

Als Konsequenz, zulässt die durch g erzeugte Untergruppe von G die folgende Beschreibung als Teilmenge von G:

$$\langle g \rangle = \{e_G, g, g^2, \ \ldots \ , \ g^{\mathrm{Ord}(g)-1}\}.$$

Beweis des Satzes.

- „⇐“ Wenn es $k : \mathbb{N}_{>0}$ gibt, sodass $n = k * \mathrm{Ord}(g)$, dann gilt $g^n = (g^{\mathrm{Ord(g)}})^k = e_G^k = e_G$.
- „⇒“ Falls $g^n = e_G$ ist, schreibt man $n = k * \mathrm{Ord}(g) + r$ mit $0 \leqslant r < \mathrm{Ord}(g)$. Dann gilt $e_G = g^n = (g^{\mathrm{Ord}(g)})^k \star g^r = g^r$. Wenn $r > 0$ ist, widerspricht dies der Minimalität von $\mathrm{Ord}(g)$. Somit $r = 0$ und $n = k * \mathrm{Ord}(g)$.

2.46. Zyklische Gruppen

- Seien G eine Gruppe und $g : G$ ein Element von G.
- Durch die universelle Eigenschaft der Gruppe $(\mathbb{Z}, +)$, gibt es einen eindeutigen Gruppenhomomorphismus $\varphi_g : (\mathbb{Z}, +) \to G$, sodass $\varphi_g(1) = g$. Nämlich, der Homomorphismus, der durch $\forall\ n : \mathbb{Z}, \varphi_g(n) := g^n$ definiert wird.

  Satz. Die Gruppe G ist genau dann zyklisch, wenn es ein Element $g : G$ gibt, sodass der kanonische Gruppenhomomorphismus $\varphi_g : \mathbb{Z} \to G$ surjektiv ist.

  Beweis. Per Definition, ist die Gruppe G zyklisch, falls Folgendes gilt: $\exists\ g : G, \langle g \rangle = G$. Ausserdem, auch per Definition, ist im $\varphi_g = \{h : G \ / \ \exists\ n : \mathbb{N}_{\geqslant 0},\ h = g^n\}$. Es reicht deshalb zu überprüfen, dass die Teilmenge $\{h : G \ / \ \exists\ n : \mathbb{N}_{\geqslant 0},\ h = g^n\}$ von G die kleinste Untergruppe von G ist, die die Teilmenge $\{g\}$ enthält (Übung).

2.47. Endliche zyklische Gruppen

Eine Gruppe $G := (A, \star, e_G)$ wird **endlich** genannt, falls die Menge A endlich ist.

Satz. Die Gruppe $\langle g \rangle$ ist genau dann eine endliche Gruppe, wenn der kanonische Gruppenhomomorphismus $\varphi_g : (\mathbb{Z}, +) \to G$ nicht-injektiv ist.

Beweis. Beachten wir, dass $\langle g \rangle$ genau dann endlich ist, wenn g endliche Ordnung hat.

- „⇒“ Nehmen wir an, dass $\langle g \rangle$ endlich ist, und zeigen wir, dass φ_g nicht-injektiv ist. Dies folgt von der Tatsache, dass eine Abbildung f von $\mathbb{Z}$ nach $\{1, \ldots, n\}$ nicht-injektiv ist (Grund dafür ist, dass es zwei gleiche Elemente) in der Teilmenge $\{f(0), \ldots, f(n)\}$ gibt.
- „⇐“ Nehmen wir an, dass φ_g nicht-injektiv ist. Da φ_g ein Gruppenhomorphismus ist, impliziert dies, dass $\ker \varphi_g \neq \{e_G\}$ ist. Das heißt, es existiert $n : \mathbb{N}_{>0}$, sodass $g^n = e_G$. Was bedeutet, dass g endliche Ordnung hat, mit $\mathrm{Ord}(g) = \mathrm{Kard}(\langle g \rangle)$.

2.48. Eine Anmerkung zur Unterscheidung von Teilmengen

- Für $A_1, A_2 : \mathrm{Teil}(A)$ ist es wichtig, $A_1 \not\subseteq A_2$ als $\exists\, a : A, a \in A_2 \wedge a \notin A_1$ zu interpretieren.
- Angesichts der vorherigen Definition für $A_1 \not\subseteq A_2$, können wir setzen:

$$A_1 \neq A_2 := A_1 \not\subseteq A_2 \vee A_2 \not\subseteq A_1.$$

- Mit dieser Definition, wenn $\varphi : G \to H$ ein Gruppenhomomorphismus ist, gilt

$$\varphi \text{ nicht-injektiv} \Leftrightarrow \ker \varphi \neq \{e_G\}.$$

- Im vorherigen Satz über zyklische Gruppen, sind die für die Praxis relevanten Implikationen die folgenden:

$$\varphi_g \text{ nicht-injektiv} \Rightarrow g \text{ hat endliche Ordnung} \Rightarrow \neg(\varphi \text{ injektiv}).$$

2.49. Untergruppen einer zyklischen Gruppe

Beispiel. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch, denn $\mathbb{Z} = \langle 1 \rangle$ als Teilmenge von $\mathbb{Z}$. Wie zuvor gesehen, sind alle Untergruppen von $\mathbb{Z}$ von der Form $U = n\mathbb{Z}$. Da $n\mathbb{Z} = \langle n \rangle$ als Teilmenge von $\mathbb{Z}$, sind alle Untegruppen von $(\mathbb{Z}, +)$ zyklisch.

> **Satz.** Sei G eine zyklische Gruppe und sei U eine nicht-triviale Untergruppe von G. Dann ist U zyklisch.

Beweis. Sei $g : G$, sodass $G = \langle g \rangle$. Sei $U \preccurlyeq G$ eine nicht-triviale Untergruppe. Dann existiert es per Definition $a : G$, sodass $a \in U$ ist und $a \neq e_G$ ist.

- Da dieses a ein Element von G ist, gibt es $n : \mathbb{N}_{>0}$, sodass $a = g^n$ ist. Das heißt, $\{n : \mathbb{N}_{>0} \;/\; g^n \in U\} \neq \emptyset$ ist. Sei dann $n_0 := \min\{n : \mathbb{N}_{>0} \;/\; g^n \in U\}$ und $h := g^{n_0}$.
- Wir werden nun beweisen, dass $U = \langle h \rangle$ ist.

2.50. Ende des Beweises

- Da U eine Untergruppe ist, folgt aus $h \in U$, dass $\langle h \rangle \subseteq U$ ist.
- Umgekehrt, sei $a \in U$ und schreiben wir $a = g^k$ für ein bestimmtes $k : \mathbb{N}_{\geqslant 0}$. Es genügt zu zeigen, dass $a \in \langle g^{n_0} \rangle$.
  - Durch Division mit Rest ist $g^k = g^{qn_0+r}$, mit $0 \leqslant r < n$. Insbesondere ergibt sich $g^r = g^{k-qn_0} = g^k \star (g^{qn_0})^{-1} \in U$, als Produkt von Elementen von U.
  - Wenn $r \neq 0$ ist, widerspricht dies der Minimalität von n_0 als Element von $\{n : \mathbb{N}_{>0} \;/\; g^n \in U\}$. Somit $r = 0$ und $a = g^k = (g^{n_0})^q \in \langle g^{n_0} \rangle$.

3. Nebenklassen und der Satz von Lagrange

Abbildung 3.1.: Ein Porträt von Joseph-Louis Lagrange.

Joseph-Louis Lagrange (1736–1813) war ein französischer Mathematiker und Astronom italienischer Herkunft. Er begründete die analytische Mechanik in Physik und leistete auch Beiträge zur Gruppentheorie und zur Theorie der quadratischen Formen in der Zahlentheorie.

3.1. Links und Rechtsnebenklassen

- Seien G eine Gruppe und $U \preccurlyeq G$ (das heißt, U eine Untergruppe von G).
- Für alles Element $a : G$ (das heißt, ein Element a in der zugrundeliegende Menge von G), wird die Teilmenge (die auch durch $[a]_{L,U}$ bezeichnet werden kann)

$$aU := \{g : G \mid \exists\ u : U,\ g = au\}$$

  die **Linksnebenklasse** von U nach a genannt (au ist die übliche Abkürzung für $a \star u$).
- In analoger Weise, ist die **Rechtsnebenklasse** von U nach a die Teilmenge

$$Ua \text{ oder } [a]_{R,U} := \{g : G \mid \exists\ u : U,\ g = ua\}.$$

- Die **Linkstranslation** $L_a : G \to G$, die ein Element $g : G$ nach das Element ag abbildet, eine Bijektion von U nach aU induziert. Insbesondere sind U und aU gleichmächtig. In analoger Weise induziert die **Rechtstranslation** $R_a(g) := ga$ eine Bijektion von U nach Ua.

3.2. Beispiele für Nebenklassen

	id	r	r^2	r^3	s	t	σ	τ
id	id	r	r^2	r^3	s	t	σ	τ
r	r	r^2	r^3	id	σ	τ	t	s
r^2	r^2	r^3	id	r	t	s	τ	σ
r^3	r^3	id	r	r^2	τ	σ	s	t
s	s	τ	t	σ	id	r^2	r^3	r
t	t	σ	s	τ	r^2	id	r	r^3
σ	σ	s	τ	t	r	r^3	id	r^2
τ	τ	t	σ	s	r^3	r	r^2	id

Sei G die Symmetriegruppe eines Quadrats. Sei $U := \{id, r, r^2, r^3\}$ die (oben in blau dargestellt) Untergruppe von G, die aus direkten solchen Symmetrien besteht. Die Linksnebenklasse $sU = \{s, \tau, t, \sigma\}$ ist in Pink dargestellt. In Grün ist die Rechtsnebenklasse Ut.

3.3. Repräsentanten einer Linksnebenklasse

- Seien G eine Gruppe und U eine Unterguppe von G. Eine Teilmenge $T : \text{Teil}(G)$ wird eine Linksnebenklasse von U genannt, falls es ein Element $a : G$ gibt, sodass $T = aU$.
- Solches Element a wird als **Repräsentant** der Nebenklasse T bezeichnet. Gibt es weitere Repräsentaten? Falls ja, wie können wir diese charakterisieren?

Satz. Sei $a, b : G$. Dann sind äquivalent:

1. $aU = bU$.
2. $\exists\ g : G,\ g \in aU \cap bU$.
3. $b \in aU$.
4. $a^{-1}b \in U$.

- Da $a \in aU$ ist (denn $a = ae$ mit $e \in U$), sind Linksnebenklassen *nicht leer*.

3.4. Gleichheit zwischen Linksnebenklassen

Beweisen wir i ⇒ ii ⇒ iii ⇒ iv ⇒ i.

- „ i ⇒ ii “ : Nehmen wir an, dass $aU = bU$. Dann $aU \cap bU = aU$. Da $aU \neq \emptyset$ ist, folgt ii.
- „ ii ⇒ iii “ : Durch Annahme erhalten wir $g : G$ und $u, v \in U$, so dass $(g = au) \wedge (g = bv)$. Da U eine Untergruppe ist, gilt $b = gv^{-1} = auv^{-1}$ mit $uv^{-1} \in U$. Das heißt, $b \in aU$.
- „ iii ⇒ iv “ : Wenn $b \in aU$, gibt es $u \in U$, sodass $b = au$. Somit $a^{-1}b = u \in U$.
- „ iv ⇒ i “ : Da $a^{-1}b \in U$ ist, gibt es $u \in U$, sodass $b = au$ (nämlich, $u := a^{-1}b$). Zeigen wir dann, das $aU \subset bU$ und $bU \subset aU$.
  - Falls $g = av$ mit $v \in U$ gilt, dann gilt $g = av = a(uu^{-1})v = (au)u^{-1}v = bu^{-1}v$ mit $u^{-1}v \in U$. Somit $g \in bU$.
  - Gleichfalls, falls $g = bv$ mit $v \in U$ gilt, dann gilt $g = bv = (au)v = a(uv)$ mit $uv \in U$. Somit $g \in aU$.

3.5. Übung 1 - Unterscheidung zwischen Linksnebenklassen

- Da aU und bU Teilmengen von G sind, ist $aU = bU$ äquivalent zu $aU \subset bU \wedge bU \subset aU$.
- Per Definition, ist $aU \neq bU$ äquivalent zu $aU \not\subset bU \vee bU \not\subset aU$. Die Relation $aU \not\subset bU$ bedeutet:

$$\exists g : G, g \in aU \wedge g \notin bU$$

- Geben Sie für jede der folgenden Implikationen einen direkten Beweis:
  1. $aU \cap bU \neq \emptyset \Rightarrow aU = bU$. Das heißt, wenn $aU \cap bU$ nicht leer ist, gibt es $aU = bU$.
  2. $aU \neq bU \Rightarrow aU \cap bU = \emptyset$. Das heißt, wenn aU und bU unterschiedliche Teimengen von G sind, dann ist das Durchschnitt $aU \cap bU$ die leere Teilmenge von G.
- Beachten Sie, dass die Implikation $aU = bU \Rightarrow aU \cap bU \neq \emptyset$ bereits bewiesen wurde.

3.6. Übung 2

- Nehmen Sie die drei vorherigen Folien an und formulieren Sie analogen Sätze für Rechtsnebenklassen. Beweisen Sie danach diese Sätze.
- Sei U eine Untergruppe von G und $\sim_U$ die Relation, die durch die Bedingung $(a \sim_{L,U} b) := (a^{-1}b \in U)$ definiert wird. Zeigen Sie Folgende:
  1. Die Relation $\sim_U$ ist eine Äquivalenzrelation auf G (das heißt, auf der zugrundeliegende Menge von G).
  2. Die Äquivalenzklassen der Relation $\sim_{L,U}$ sind die Linksnebenklassen von U.
  3. Für Rechtsnebenklassen kann man in analoger Weise die Relation $a \sim_{R,U} b := ba^{-1} \in U$ betrachten.

3.7. Links Rechts

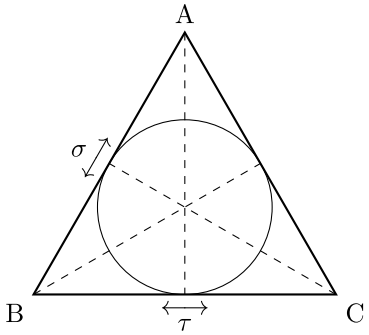

Abbildung 3.2.: Symmetrieachsen eines gleichseitigen Dreiecks.

- Es ist im Allgemeinen $aU \neq Ua$. Zum Beispiel, in der Symmetriegruppe eines gleichseitigen Dreiecks, betrachten wir die Untergruppe $U = \langle\tau\rangle = \{id, \tau\}$ und die Permutation σ. Dann ist die Linksnebenklasse $U\sigma = \{\sigma, \tau\sigma\}$ unterschiedlich von der Rechtsnebenklasse $\sigma U = \{\sigma, \sigma\tau\}$.
- Sichtbarer Grund dafür ist die Nichtkommutativität der Umgebungsgruppe ($\sigma\tau \neq \tau\sigma$).

3.8. Nebenklassen in kommutativen Gruppen

- Falls G eine kommutative Gruppe ist, dann für jede Untergruppe U und jedes Element $a : G$, gilt $aU = Ua$.
- Dies ergibt sich direkt aus der Definition von Links und Rechtsnebenklassen: Wenn $g = au$, gilt auch $g = ua$.

Anmerkung. Manchmal ist es hilfreich, informelle Berechnungen wie folgt durchzuführen:

$$(b \in aU) \Rightarrow (b = au \text{ mit } u \in U) \Rightarrow (bU = (au)U = a(uU) = aU).$$

3.9. Mengen Links und Rechstnebenklassen

- Wir werden eine Menge G/U konstruieren, deren Elemente die Linksnebenklassen von U sind. In ähnlicher Weise, werden wir auch eine Menge $U\backslash G$ konstruieren, deren Elemente die Rechtsnebenklassen von U sind.
- Der Kernpunkt der Konstruktion ist das Prädikat $\text{Neb}_{L,U} : \text{Teil}(G) \to \{0, 1\}$, das eine Teilmenge $A : \text{Teil}(G)$ genau dann nach 1 abbildet, wenn A eine Linksnebenklasse von U ist (das heißt, wenn es ein Element $a : G$ gibt, sodass $A = aU$ ist).
- Dann wird die Menge von Linksnebenklassen von U so konstruiert:

$$G/U \quad := \bigcup_{\{A:\text{Teil}(G) \ / \ \text{Neb}_{L,U}(A) \ = \ 1\}} \{A\} \ .$$

In dieser Schreibung, ist die Kardinalität von $\{A\}$ einfach 1 (da $\{A\}$ eine Menge mit einem einzigen Element ist, nämlich das Element A).

3.10. Beispiel für eine Menge Linksnebenklassen

	id	r	r^2	r^3	s	t	σ	τ
id	id	r	r^2	r^3	s	t	σ	τ
r	r	r^2	r^3	id	σ	τ	t	s
r^2	r^2	r^3	id	r	t	s	τ	σ
r^3	r^3	id	r	r^2	τ	σ	s	t
s	s	τ	t	σ	id	r^2	r^3	r
t	t	σ	s	τ	r^2	id	r	r^3
σ	σ	s	τ	t	r	r^3	id	r^2
τ	τ	t	σ	s	r^3	r	r^2	id

In der Symmetriegruppe eines Quadrats, hat die Untergruppe direkten Symmetrien zwei Linksnebenklassen: $U = \{id, r, r^2, r^3\}$ und $sU = \{s, \tau, t, \sigma\}$. Beachten Sie, dass $U = rU = r^2U = r^3U$ gilt (da $r \in U$ ist), und dass $sU = \tau U = tU = \sigma U$ auch gilt.

3.11. Die induzierte Partition

- Die Menge G/U von Linksnebenklassen von U in G ist mit einer Abbildung nach $\mathrm{Teil}(G)$ ausgestattet:

$$\mathrm{pr}_1 : G/U \to \mathrm{Teil}(G),\ \{A\} \mapsto A\ .$$

- In dieser Situation ist G die disjunkte Vereinigung der Linksnebenklassen von U.

$$G = \bigsqcup_{t\ :\ G/U} \mathrm{pr}_1(t)$$

- Dies bedeutet:

  1. $\forall\ g : G,\ \exists\ t : G/U, g \in \mathrm{pr}_1(t)$. Explizit existiert es eine Teilmenge A von G, die eine Linknebenklasse von U ist, sodass $g \in A$ (noch expliziter nehmen wir $A := gU$ an).
  2. $\forall t, t' : G,\ \mathrm{pr}_1(t) \cap \mathrm{pr}_1(t') \neq \emptyset \Leftrightarrow \mathrm{pr}_1(t) = \mathrm{pr}_1(t')$. Explizit ist $aU \neq bU \Leftrightarrow aU \cap bU = \emptyset$, wie aus dem Satz über Repräsentanten einer Linksnebenklasse folgt.

3.12. Eine Bemerkung zur Definition eine Linksnebenklasse

- Wir können das vorheriges Beispiel benötigen, um etwas über den formalen Standpunkt zu erklären. Zunächst möchte ich aber sagen, dass der Ausdruck $T : \mathrm{Teil}(G)$ eine Notation ist, für was Sie als $T \in \mathcal{P}(G)$ (die *Potenzmenge* von G) oder $T \subset G$ kennen.
- Wir haben zuvor ein Prädikat $\mathrm{Neb}_{L,U} : \mathrm{Teil}(G) \to \{0, 1\}$ definiert, sodass $\mathrm{Neb}_{L,U}(T) = 1$, genau dann wenn $\exists\ a : G,\ T = aU$ (das heißt, $\mathrm{Neb}_{L,U}(T)$ ist genau dann gleich 1, wenn ein $a : G$ existiert, sodass $T = aU$ ist). Dies gibt der Aussage „*T ist eine Linksnebenklasse von U*“ eine Bedeutung.
- Dann haben wir *die Menge von Linksnebenklassen von U* als Teilmenge von $\mathrm{Teil}(G)$ konstruiert:

$$\{T : \mathrm{Teil}(G)\ /\ T \text{ ist eine Linksnebenklasse von } U\}$$

  Diese Menge kann auch als $\mathrm{Neb}_{L,U}^{-1}(\{1\})$ charakterisiert werden.

3.13. Prädikaten und Teilmenge

- Formalerweise, sollten wir die Elemente einer Teilmenge als *Paaren* bezeichnen.
- Zum Beispiel, sollten die Elemente der Menge Linksnebenklassen nach U als Paaren (T, p_T) repräsentiert werden, wobei:
  - T eine Teilmenge von G ist (das heißt, eine Teilmenge von der zugrundeliegende Menge der Gruppe G…).
  - p_T ein Beweis ist, dass T eine Linksnebenklasse von U ist (im vorherigen Sinn).
- Zweck davon ist, Folgendes zu garantieren: Wenn wir ein Objekt haben, das wir eine Linksnebenklasse *nennen*, sollten wir in der Lage sein, nicht nur eine Teilmenge daraus zu erbringen, sondern auch einen Beweis, dass diese Teilmenge eine Linknebenklasse ist . Wir möchten diese Eigenschaft irgendwo *speichern*.

3.14. Natürliche Sprache und Formalisierung der Mathematik

- In der natürlichen Sprache betrachten wir die folgende Ausdrücke üblicherweise als das gleiche:
  - „T ist eine Linksnebenklasse von U“.
  - „T ist ein Element der Menge der Linksnebenklassen von U“.
- Formal ist das jedoch *nicht* der Fall:
  - Der erste ist ein *Satz*, nämlich der Satz $P_{L,U}(T) = 1$. Damit diese Notation korrekt ist, muss T eine Teilmenge von G sein (da $P_{L,U}$ ein Prädikat über Teilmengen von G ist).
  - Der zweite ist ein *Urteil*, der außerdem nur dann *wohltypisiert* ist, wenn T ein Paar $(T.\text{carrier}, p_T)$ ist, wobei $T.\text{carrier}$ eine Teilemenge von G ist und p_T ein Beweis ist, dass $T.\text{carrier}$ eine Linksnebenklasse von U ist.

3.15. Übung 3

- Sei G eine Gruppe und seien U, V Untergruppen von G, mit $V \preccurlyeq U$.
- Zeigen Sie, dass

$$[G :: V] = [G :: U][U :: V] \ .$$

3.16. Der Satz von Lagrange

- Sei G eine endliche Gruppe. Die Kardinalität von G wird auch die **Ordnung** von G gennant. Die Ordnung von G wird mit $|G|$ bezeichnet. Dies erstreckt sich auf Untergruppen von G.
- Da G endlich ist, so ist die Menge Teil(G). Daher ist für jede Untergruppe U von G die Menge G/U auch endlich. Die Kardinalität von G/U wird den **Index** von U genannt, und mit $[G :: U]$ bezeichnet (üblicherweise verwendet man die Notation $[G : U]$).

  Satz von Lagrange. Gegeben eine Endliche Gruppe G, gibt es, für jede Untergruppe U von G, die Gleichheit

  $$|G| = [G :: U]|U| \ .$$

  Insbesondere ist die Ordnung von U ein Teiler von der Ordnung von G.

3.17. Beweis des Satzes von Lagrange

- Da G die disjunkte Vereinigung der Linksnebenklassen von U ist, gilt

  $$|G| = \sum_{A \ : \ G/U} |A| \ .$$

- Hat aber jede Linksnebenklasse A von U die gleiche Kardinalität als U (weil es eine Bijektion von $A = aU$nach U existiert). Daher ergibt sich, per definition von $[G :: U]$ als die Kardinalität von G/U, die Gleichheit

  $$|G| = [G :: U]|U| \ .$$

3.18. Bemerkungen zum Satz von Lagrange

- Sei G eine endliche Gruppe und $U := \langle g \rangle$ die von einem Element $g : G$ erzeugte Untergruppe. Da $U = \{h : G \mid \exists \ n : \mathbb{N}, h = g^n\}$ endlich ist, muss g endliche Ordnung haben. Dann hat der Satz von Lagrange die folgende Konsequenz.

  Satz. Sei G eine endliche Gruppe und sei $g : G$. Dann hat g endliche Ordnung und ist Ord(g) ein Teiler von $|G|$. Insbesondere, falls d nicht ein Teiler der Ordnung von G ist, gibt es kein Element mit Ordnung n in G.

- In analoger Weise ist jede Gruppe G die disjunkte Vereinigung der Rechtsnebenklassen einer Untergruppe U, und gilt auch $|G| = |U\backslash G||U|$. Insbesondere ist die Kardinalität von $U\backslash G$ die gleiche von der von G/U.

  Also ist der Index von U in G auch die Anzahl von Rechtsnebenklassen.

3.19. Der Satz von Euler-Fermat

Sei G eine endliche Gruppe und $g : G$ ein Element von G. Dann gilt $g^{|G|} = e$.

Beweis. Da G endlich ist, hat g endliche Ordnung. Nach dem Satz von Lagrange, ist $\mathrm{Ord}(g)$ ein Teiler von $|G|$. Das heißt, es gibt $n : \mathbb{N}$, sodass $|G| = n\mathrm{Ord}(g)$. Dann gilt

$$g^{|G|} = g^{n\mathrm{Ord}(g)} = \left(g^{\mathrm{Ord}(g)}\right)^n = e^n = e \ .$$

Beispiel. Die Symmetriegruppe eines Quadrats hat 8 Elemente. Dann für jede Transformation T dieses Quadrats, gibt es $T^8 = id$. Explizit gibt es Transformationen mit Ordnung 2 und 4 (die Teiler von 8) aber nicht 3 oder 6.

3.20. Die Links oder Rechtsnebenklasse eines Elements

- Seien G eine Gruppe und U eine Untergruppe von G. Für alles Element $g : G$ können wir die Linksnebenklasse gU betrachten. Dies definiert eine Abbildung

$$\pi_U : G \to G/U, \ g \mapsto gU \ .$$

- Diese Abbildung besitzt die folgende Eigenschaften:

  1. π_U ist surjektiv (per Definition, für jede Linksnebenklasse A, gibt es $g : G$ sodass $A = gU$).
  2. $\pi_U(g_1) = \pi_U(g_2) \Leftrightarrow g_1^{-1}g_2 \in U$ (das heißt, $g_1 \sim_{L,U} g_2$).
  3. Für jede Linksnebenklasse $\{A\} : G/U$, ist die Faser $\pi_U^{-1}(\{A\}) = A$.

- In ähnlicher Weise können wir die Abibildung $G \to U\backslash G, \ g \mapsto Ug$ betrachten (die analoge Eigenschaften besitzt).

3.21. Faktorgruppe?

- Ist es möglich, die Abbildung $\pi_U : G \to G/U$ in einen Gruppenhomomorphismus zu verwandeln? Genauer gesagt, gibt es eine Gruppenstruktur auf der Menge G/U, so dass π_U ein Gruppenhomomorphismus ist?
- Wenn ja, würde die folgende Gleichheit gelten:

$$(g_1 \star_G g_2)U \stackrel{!}{=} (g_1U) \star_{G/U} (g_2U) \ .$$

- In diesem Fall, würden wir gerne wie folgt berechnen:

$$(g_1g_2)U \stackrel{!}{=} (g_1U)(g_2U) = (g_1g_2g_2^{-1}U)(g_2U) = (g_1g_2)(g_2^{-1}Ug_2)U \ .$$

- Nach naiver Betrachtung scheint es, dass wir dafür nur Folgendes benötigen:

$$\forall\ g_2 : G,\ g_2^{-1} U g_2 = U\ .$$

3.22. Normalteiler

- Seien G eine Gruppe und U eine Untergruppe von G.
- U heißt ein **Normalteiler** (oder **normale Untergruppe**) von G, wenn die folgende Eigenschaft gilt:

$$\forall\ g, u : G,\ u \in U \Rightarrow gug^{-1} \in U.$$

- In diesem Fall, schreibt man $U \lhd G$.

  Bemerkung. Falls G eine kommutative Gruppe ist, dann ist jede Untergruppe ein Normalteiler (denn $gug^{-1} = gg^{-1}u = u$).

3.23. Übung 4

- Sei gUg^{-1} die Teilmenge $\{h : G\ /\ \exists\ g : G,\ u : U,\ h = gug^{-1}\}$. Zeigen Sie, dass die folgende Eigenschaten äquivalent zu einander sind:

  1. U ist ein Normalteiler von G.
  2. $\forall\ g : G,\ gUg^{-1} \subseteq U$.
  3. $\forall\ g : G,\ gUg^{-1} = U$.
  4. $\forall\ g : G,\ gU = Ug$.

- Insbesondere, wenn U ein Normalteiler von G, stimmt die Linksnebenklasse von U nach g mit der Rechtsnebenklasse von U nach g überein.

3.24. Beispiele für Normalteiler

- Da $(\mathbb{Z}, +)$ eine kommutative Gruppe ist, ist jede Untergruppe $n\mathbb{Z}$ ein Normalteiler.
- Wenn $\varphi : G \to H$ ein Gruppenhomomorphismus ist, dann ist Ker φ ein Normalteiler von G. Grund dafür ist, dass $\forall\ g, u : G, u \in \text{Ker}\ \varphi \Rightarrow gug^{-1} \in \text{Ker}\ \varphi$, weil für alle g, u

$$\varphi(gug^{-1}) = \varphi(g)\varphi(u)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g)^{-1} = e_H\ .$$

- In der Symmetriegruppe eines Quadrats (oder eines Dreiecks, *etc*), ist die Untergruppe der *direkten* Symmetrien ein Normalteiler. Grund dafür ist, wenn u eine direkte Transformation ist, so ist gug^{-1} (falls g nicht direkt ist, dann ist g^{-1} auch nicht direkt, aber die Verknüpfung zwei nicht direkte Transformationen ist wieder direkt!).
- Dieses letztes Beispiel kann auch wie folgt behandelt werden.

3.25. Untergruppen mit Index zwei

Satz. Seien G eine Gruppe und U eine Untergruppe von G mit Index 2. Dann ist U ein Normalteiler von G.

Beweis.

- Erinnern wir uns daran, dass der Index von U in G sowohl die Anzahl der Linksnebenklassen als auch die Anzahl der Rechtsnebenklassen von U in G ist.
- Sei $g : G$. Falls $g \in U$, dann ist $gU = U = Ug$. Falls $g \notin U$, dann ist die Partition von G wegen Linksnebenklasse von U die folgende: $G = U \sqcup gU$. In analoger Weise, ist die Partition wegen Rechtsnebenklasse $G = U \sqcup Ug$. Da $U = U$ ist, muss $gU = Ug$ sein.
- Also gilt in jedem Fall $gU = Ug$. Beachten Sie jedoch, dass dieser Beweis nur dann korrekt ist, wenn man die folgende Eigenschaft ohne Beweis akzeptiert: $g \in U \vee g \notin U$.

3.26. Eine Verknüpfung für die Faktorgruppe

- Wenn U ein Normalteiler von G ist, möchten wir eine Verknüpfung auf der Menge der Linksnebenklassen von U definieren.

$$? \ : \ G/U \times G/U \to G/U$$

- Da jede Linksnebenklasse $t : G/U$ von der Form gU für ein bestimmtes Element $g : G$ ist, ist die Idee gerade

$$(g_1U)(g_2U) := (g_1g_2)U$$

  zu setzen.

- Die Schwierigkeit bei dieser Definition besteht darin, dass wir sicherstellen müssen, dass das Ergebnis nicht von der Wahl der Repräsentanten g_1 und g_2 abhängt:

  Problem. Wenn $g_1U = g_1'U$ und $g_2U = g_2'U$, gibt es $(g_1g_2)U = (g_1'g_2'U)$?

3.27. Die vorherige Verknüpfung ist wohldefiniert

- Zunächst untersuchen wir den Fall wenn $g_2' = g_2 u$ für ein bestimmtes $u \in U$. Dann gilt

$$(g_1 g_2')U = (g_1 g_2 u)U = (g_1 g_2)(uU) = (g_1 g_2)U \ .$$

- Danach untersuchen wir den Fall wenn $g_1' = g_1 u$ für ein bestimmtes $u \in U$. Dann gilt

$$(g_1' g_2)U = (g_1 u g_2)U = (g_1 (g_2 g_2^{-1}) u g_2)U = (g_1 g_2)\underbrace{(g_2^{-1} u g_2)}_{\in U}(U) = (g_1 g_2)U \ .$$

- Dieser Beweis gilt in der Mathematik allgemein als überzeugend. Sollte aber man zeigen:

$$\forall\, t_1, t_2 : G/U,\ \exists!\, t : G/U,\ \forall\, g_1, g_2 : G,\ (g_1 \in \mathrm{pr}_1(t_1)) \wedge (g_2 \in \mathrm{pr}_1(t_2)) \Rightarrow (g_1 g_2) \in \mathrm{pr}_1(t)$$

  wobei $\mathrm{pr}_1 : G/U \to \mathrm{Teil}(G)$ die kanonische Abbildung ist, die früher gebaut wurde. Dann als Anwendung dieses Satzes und einer swachen Form des Auswahlaxioms könnte man $t_1 \star_{G/U} t_2 := t$ setzen, wobei t das Element ist, das im Beweis konstruiert wurde.

3.28. Eigenschaften dieser Verknüpfung

- Nun wollen wir beweisen, dass das Paar $(G/U, \star_{G/U})$ eine Gruppe ist. Das heißt, wir müssen Folgendes überprüfen:

  1. Die Assoziativität der Verknüpfung $\star_{G/U}$.
  2. Die Existenz eines neutralen Elements für $\star_{G/U}$.
  3. Die Existenz, für alles $g : G$, eines inversen Element zu g.

- Für die Assoziativität können wir einfach schreiben:

$$\begin{array}{rcccl} \forall\, g_1, g_2, g_3 : G,\ ((g_1U)(g_2U))(g_3U) & = & ((g_1 g_2)U)(g_3U) & = & ((g_1 g_2)g_3)U \\ & & & = & (g_1(g_2 g_3))U \\ & & & = & (g_1U)((g_2 g_3)U) \\ & & & = & (g_1U)((g_2U)(g_3U)). \end{array}$$

3.29. Neutrale und inverse Elemente

- Sei $e : G$ das neutrales Element für $\star_G$. Wir behaupten, dass das Element $eU : G/U$ ein neutrales Element für $\star_{G/U}$ ist.
  - $\forall\ g : G,\ (eU) \star_{G/U} (gU) = (e \star_G g)U = gU.$
  - $\forall\ g : G,\ (gU) \star_{G/U} (eU) = (g \star_G e)U = gU.$
- Als Konsequenz, für jedes Element $g : G$, ist $g^{-1}U$ ein inverse Element für gU (bezüglich $\star_{G/U}$).
  - $(g^{-1}U) \star_{G/U} (gU) = (g^{-1} \star_G g)U = eU.$
  - $(gU) \star_{G/U} (g^{-1}U) = (g \star_G g^{-1})U = eU.$
- Dies beendet den Beweis, dass, wenn U ein Normalteiler von der Gruppe G ist, $(G/U, \star_{G/U})$ eine Gruppe ist.

3.30. Die kanonische Projektion ist ein Gruppenhomomorphismus

- Wenn U ein Normalteiler von der Gruppe G ist, wird die Gruppe $(G/U, \star_{G/U})$ eine **Faktorgruppe** (oder **Quotientgruppe**) genannt.
- Die **kanonische Projektion** zu dieser Faktorguppe, die wir zuvor eingeführt haben, ist die Abbildung

$$\pi_U : G \to G/U,\ g \mapsto gU\ ,$$

  die ein Element $g : G$ nach die Linksnebenklasse von U nach g abbildet.
- Es ist nun unmittelbar, dass diese Abbildung einen Gruppenhomomorphismus induziert, weil Folgendes gilt:

$$\forall\ g_1, g_2 : G, \pi_U(g_1 \star_G g_2) = (g_1 g_2)U = (g_1 U)(g_2 U) = \pi_U(g_1) \star_{G/U} \pi_U(g_2)\ .$$

  Da $\pi_U(g) = eU \Leftrightarrow gU = eU \Leftrightarrow g \in U$ ist, gilt außerdem $\operatorname{Ker} \pi_U = U$.

3.31. Division mit Rest und Faktorgruppen

- Betrachten wir $n : \mathbb{Z}$ mit $n > 0$ und die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ der Gruppe $(\mathbb{Z}, +)$. Für alles Element $a : \mathbb{Z}$, ist die Nebenklasse von $n\mathbb{Z}$ nach a die Teilmenge

$$a + n\mathbb{Z} := \{b : \mathbb{Z} \mid b - a \in n\mathbb{Z}\} \ .$$

- Eine solche Nebenklasse hat ein eindeutiger Repräsentant $r : \mathbb{Z}$, sodass $0 \leqslant r < n$. Nämlich, r ist das Rest der Divsion mit Rest von a durch n. Daher können wir $\mathbb{Z}/n\mathbb{Z}$ mit $\{0,\ 1,\ \ldots\ ,\ n-1\}$ als Menge identifizieren. Durch dieser Identifikation, sehen wir die kanonische Projektion an, als die Abbildung $\mathrm{mod}\ n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, die eine ganze Zahl a nach das Rest $a \bmod n$ der Division mit Rest von a durch n abbildet.
- Die Tatsache, dass diese kanonische Projektion ein Gruppenhomomorphismus ist, wird auf eine bereits bekannte Eigenschaft reduziert:

$$(a + a') \bmod n = (a \bmod n) + (a' \bmod n) \ .$$

3.32. Übung 5

1. Seien G eine endliche Gruppe und N eine normale Untergruppe von G. Zeigen Sie, dass die Kardinalität von G/U gleich dem Index von N ist: $|G/N| = [G :: N]$.
2. Sei G die Symmetriegruppe eines Quadrats (oder eines Dreiecks *etc*). Zeigen Sie, dass die Untergruppe direkten Symmetrien Index 2 hat.
3. Seien G eine Gruppe und U eine Untergruppe von G. Zeigen Sie, dass U genau dann ein Normalteiler ist, wenn es eine Gruppe H und ein Gruppenhomomorphismus $\varphi : G \to H$ existiert, sodass $U = \mathrm{Ker}\ \varphi$.
4. Sei G eine Gruppe. Zeigen Sie, dass die triviale Untergruppe $\{e_G\}$ ein Normalteiler von G ist, und dass die kanonische Prokjektion $\pi_{\{e_G\}} : G \to G/\{e_G\}$ ein Gruppenisomorphismus ist.

3.33. Die universelle Eigenschaft der Faktorgruppen

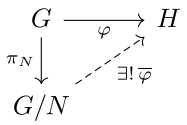

Abbildung 3.3.: Der Gruppenhomomorphismus φ *faktorisiert* durch N.

- Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Sei N ein Normateiler von G, sodass $N \preccurlyeq \operatorname{Ker} \varphi$ (das heißt, $\forall\ n : G, n \in N \Rightarrow \varphi(n) = e_H$). Zum Beispiel, kann N die volle Untergruppe Ker φ sein.
- Wie immer, wird die kanonische Projektion $G \to G/N$ als π_N bezeichnet.

  Satz. Existiert ein eindeutige Gruppenhomomorphismus $\overline{\varphi} : G/N \to H$, sodass $\varphi = \overline{\varphi} \circ \pi_N$.

3.34. Beweis der universelle Eigenschaft

- Nehmen wir an, dass ein Gruppenhomomorphismus $\overline{\varphi} : G/N \to H$ existiert, mit der Eigenschaft $\varphi = \overline{\varphi} \circ \pi_N$. Dann, für jedes Element $g : G$, gilt

$$\overline{\varphi}(gN) = \overline{\varphi}(\pi_N(g)) = \varphi(g)\ .$$

  Da π_N surjektiv, ist ein solcher Homomorphismus $\overline{\varphi}$ insbesondere eindeutig.
- Wir müssen nun beweisen, dass $\overline{\varphi}(gN) := \varphi(g)$ wohldefiniert und ein Gruppenhomomorphismus ist. Genauer gesagt, müssen wir zunächst Folgendes beweisen:

$$\forall\ t : G/N, \exists!\ h : H, \forall\ g : G,\ g \in \mathrm{pr}_1(t) \Rightarrow \varphi(g) = h\ ,$$

  wobei pr_1 die kanonische Abbildung $\mathrm{pr}_1 : G/N \to \mathrm{Teil}(G)$ ist.

3.35. Die Abbildung ist wohldefiniert

- Sei $t : G/N$. Da die kanonische Projektion $\pi_N : G \to G/N$ surjektiv ist, gibt es $g_0 : G$, sodass $t = \pi_N(g_0)$. Setzen wir dann $h_0 := \varphi(g_0)$, für *dieses* g_0.
- Dann müssen wir noch die folgende Eigenschaft beweisen:

$$\forall\ g : G,\ g \in (g_0 N) \Rightarrow \varphi(g) = \varphi(g_0)\ .$$

  Dies folgt von der Tatsache, dass $g_0^{-1} g \in N$ und $N \preccurlyeq \operatorname{Ker} \varphi$, also

$$\varphi(g) = \varphi(g_0 g_0^{-1} g) = \varphi(g_0)\varphi(g_0^{-1} g) = \varphi(g_0) e_H = \varphi(g_0)\ .$$

- Insbesondere hängt das Element h_0 nicht von der Wahl des Elements g_0 ab, und ist durch die Eigenschaft $\forall\ g : G,\ g \in \mathrm{pr}_1(t) \Rightarrow \varphi(g) = h_0$ eindeutig definiert: Wenn h_1 auch diese Eigenchaft hat, dann gilt $h_1 = \varphi(g) = h_0$.
- In der Praxis genügt es, die Eigenschaft $\forall\ g : G,\ g \in (g_0 N) \Rightarrow \varphi(g) = \varphi(g_0)$ gilt zu zeigen.

3.36. Die Abbildung ist ein Gruppenhomomorphismus

- Der letzte Schritt im Beweis besteht darin, Folgendes zu beweisen:

$$\forall\ t_1, t_2 : G/N,\ \overline{\varphi}(t_1 \star_{G/U} t_2) = \overline{\varphi}(t_1) \star_H \overline{\varphi}(t_2)\ .$$

- Da π_N surjektiv ist, können wir annehmen, dass $t_1 = g_1 N$ und $t_2 = g_2 N$ sind, für bestimmte $g_1, g_2 : G$. Dann gilt, durch direkte Berechnung:

$$\begin{array}{rcccl} \overline{\varphi}(t_1 t_2) & = & \overline{\varphi}((g_1 N)(g_2 N)) & = & \overline{\varphi}((g_1 g_2)N) \\ & & & & = \varphi(g_1 g_2) \\ & & & & = \varphi(g_1)\varphi(g_2) \\ & & & & = \overline{\varphi}(g_1 N)\overline{\varphi}(g_2 N) \\ & & & & = \overline{\varphi}(t_1)\overline{\varphi}(t_2)\ . \end{array}$$

3.37. Bild und Kern des induzierten Homomorphismus

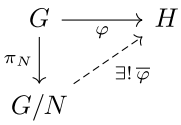

Abbildung 3.4.: Der Gruppenhomomorphismus φ *faktorisiert* durch N.

- In dieser Situation (die auftritt, wenn $N \preccurlyeq \operatorname{Ker} \varphi$ ist), gilt Folgendes:

  1. $\operatorname{Im} \overline{\varphi} = \operatorname{Im} \varphi$ als Untergruppe von H.
  2. $\pi_N(\operatorname{Ker} \varphi) \preccurlyeq \operatorname{Ker} \overline{\varphi}$ und die Abbildung $\pi_N|_{\operatorname{Ker} \varphi} : \operatorname{Ker} \varphi \to \operatorname{Ker} \overline{\varphi}$ induziert ein Gruppenisomorphismus

$$(\operatorname{Ker} \varphi)/N \ \simeq\ \operatorname{Ker} \overline{\varphi}\ .$$

- Insbesondere, wenn $N = \operatorname{Ker} \varphi$ ist, dann ist $\overline{\varphi}$ injektiv! Oben ist es implizit, dass $N \lhd (\operatorname{Ker} \varphi)$. Dies folgt unmittelbar von der Tatsache, dass $N \lhd G$ ist (Übung).

3.38. Bestimmung des Bildes und des Kerns

- Das $\operatorname{Im} \overline{\varphi} = \operatorname{Im} \varphi$, folgt von der Definition des Homomorphismus $\overline{\varphi}(gN) := \varphi(g)$.
- Von der Eigenschaft $\varphi = \overline{\varphi} \circ \pi_N$, folgt außerdem, dass $\pi_N(\operatorname{Ker} \varphi) \preccurlyeq \operatorname{Ker} \overline{\varphi}$ ist.

- Betrachten wir nun den Gruppenhomomorphismus $\pi_N|_{\text{Ker }\varphi} : \text{Ker } \varphi \to \text{Ker } \overline{\varphi}$, und wenden den Satz darauf an. Da $N = \text{Ker } (\pi_N|_{\text{Ker }\varphi})$, gibt es einen induzierten Gruppenhomomorphismus $\overline{\pi_N|_{\text{Ker }\varphi}} : (\text{Ker } \varphi)/N \to \text{Ker } \overline{\varphi}$.
- Beweisen wir nun, dass dieser Gruppenhomomorphismus ein Gruppenisomorphismus ist:

  1. Sei $g : G$, sodass $\overline{\varphi}(gN) = e_H$ ist. Dann ist $\varphi(g) = e_H$. Das heißt, $g \in \text{Ker } \varphi$. Dies impliziert, dass $\overline{\pi_N|_{\text{Ker }\varphi}}$ surjektiv ist.
  2. Sei $g : G$, sodass $\overline{\pi_N|_{\text{Ker }\varphi}}(gN) = e_{\text{Ker }\overline{\varphi}}$. Das heißt, $gN = eN$. Dies zeigt, dass $\overline{\pi_N|_{\text{Ker }\varphi}}$ injektiv ist.

3.39. Homomorphiesatz

- Der vorherige Beweis war ziemlich kompliziert. Es braucht Zeit, um ihn voll zu verstanden .
- Wichtig in der Praxis ist der folgende Sonderfall:

  Satz. Sei $\varphi : G \to H$ ein Gruppenhomorphismus. Dann induziert der Gruppenhomomorphismus $\overline{\varphi} : G/\text{Ker } \varphi \to H$ einen Gruppenisomomorphismus

  $$G/\text{Ker } \varphi \simeq \text{Im } \varphi \ .$$

  Insbesondere, wenn φ surjektiv ist, dann ist $\overline{\varphi}$ ein Gruppenisomorphismus

  $$G/\text{Ker } \varphi \simeq H \ .$$

3.40. Übung 6

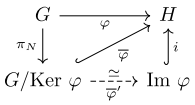

Abbildung 3.5.: Die kanonische Faktorisierung eines Gruppenhomomorphismus.

- Es ist eine gute Übung, einen direkten Beweis des vorherigen Satzes zu geben.
- Im obigen Diagramm wurde der Gruppenhomomorphismus $\overline{\varphi}$, der in der universelle Eigenschaft der Faktorgruppen erscheint, durch $i \circ \overline{\varphi}'$ ersetzt.

3.41. Übung 7

- Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.
- Zeigen Sie die folgende Eigenschaften:

  1. Wenn $N \lhd H$, dann ist $\varphi^{-1}(N) \lhd G$.
  2. Wenn $N \lhd G$, dann ist $\varphi(N) \lhd \text{Im } \varphi$.
  3. Wenn $N \lhd G$, und φ surjektiv ist, dann ist $\varphi(N) \lhd H$.

3.42. Durchschnitt normaler Untergruppen

- Seien G eine Gruppe und $(N_i)_{i:I}$ eine Familie normaler Untergruppen von G. Das heißt, für jedes $i : I$, die Untergruppe N_i von G ist eine normale Untergruppe.

  Satz. Die (bereits definierte) Untergruppe $\wedge_{i:I} N_i$ ist eine normale Untergruppe.

  Beweis. Bezeichnen wir mit A_i die zugrundeliegende Menge der Untergruppe U_i. Per Konstruktion ist die zugrundeliegende Menge der Untergruppe $\wedge_{i:I} N_i$ das Durschschnitt $A := \cap_{i:I} A_i$. Es reicht deshalb zu beweisen, dass für alle $a, g : G$,

  $$a \in A \Rightarrow gag^{-1} \in A \ .$$

  Aber für alles $h : G$, ist $h \in A$ äquivalent zu $\forall, i : I,\ h \in A_i$, und, da N_i eine normale Untergruppe ist, gibt es $\forall\ i : I,\ gag^{-1} \in A_i$. Damit ist der Beweis fertig .

3.43. Erzeugte normale Untergruppe: erste Konstruktion

- Seien G eine Gruppe und $E : \text{Teil}(A)$ eine Teilmenge von A.
- Betrachten wir die folgende Menge, die als Teilmenge von der Menge der Untergruppen von G definiert wird:

  $$I := \{N : \text{Untergruppe}(G) \ / \ N \lhd G \ \wedge \ E \subseteq U\}$$

- Dann können wir eine Familie $(N_i)_{i:I}$ wie zuvor definieren.
- Nach dem vorherigen Satz, ist die Untergruppe

  $$\langle E \rangle_N := \wedge_{i:I} N_i$$

  eine *normale* Untergruppe. Diese Untergruppe wird **die von der Teilmenge E erzeugte normale Untergruppe** (oder **erzeugte Normalteiler**) gennant.

3.44. Übung 8

- Sei G eine Gruppe und sei E eine Teilmenge von G (das heißt, eine Teilmenge von der zugrundeliegendemenge von G).
- Zeigen Sie die folgende Eigenchaften:

  1. $\langle E\rangle \preccurlyeq \langle E\rangle_N$. Das heißt, die von E erzeugte Untergruppe ist eine Untergruppe der von E erzeugten normalen Untergruppe.
  2. $\langle E\rangle_N$ ist die kleinste normale Untergruppe, die die Teilmenge E enthält.

3.45. Induktive Definition

- Es gibt eine andere, explizitere Konstruktion der normalen Untergruppe $\langle E\rangle_N$. Nämlich, eine *induktive* Definition.
- Die Definition ist Folgende. Für alle $a : G$, um $a \in \langle E\rangle_N$ zu beweisen, genügt es eine der folgender Bedingungen zu überprüfen:

  - $a = e$
  - $a \in E$.
  - $a = a_1a_2$, mit $a_1 \in \langle E\rangle_N$ und $a_2 \in \langle E\rangle_N$.
  - $a = b^{-1}$, mit $b \in \langle E\rangle_N$.
  - $a = gbg^{-1}$, mit $b \in \langle E\rangle_N$ und $g : G$.

3.46. Erzeugte normale Untergruppe: zweite Konstruktion

- Überprüfen wir, dass die Teilmenge $\langle E\rangle_N : \mathrm{Teil}(G)$ eine normale Untergruppe von G ist.
- Es reicht dazu, die folgende Eigenschaften zu beweisen:

  - $e \in \langle E\rangle_N$.
  - $\forall\ a_1, a_2 : G, a_1 \in \langle E\rangle_N \wedge a_2 \in \langle E\rangle_N \Rightarrow (a_1a_2) \in \langle E\rangle_N$.
  - $\forall\ b : G, b \in \langle E\rangle_N \Rightarrow b^{-1} \in \langle E\rangle_N$.
  - $\forall\ b : G,\ b \in \langle E\rangle_N \Rightarrow \forall\ g : G,\ gbg^{-1} \in \langle E\rangle_N$.

- Alle vier Eigenschaften folgen unmittelbar aus der Definition der Teilmenge $\langle E\rangle_N$.
- Außerdem haben wir $\forall\ a : G, a \in E \Rightarrow a \in \langle E\rangle_N$, auch per Definition der Teilmenge $\langle E\rangle_N$.

3.47. Übung 9

- Zeigen Sie, dass $\langle E\rangle_N$ die kleinste normale Untergruppe von G ist, die die Teilmenge E enthält.

- **Hinweis.**
  - Um den Satz zu beweisen, reicht es Folgendes zu zeigen: Wenn N eine normale Untergruppe von G ist, die E enthält, dann ist $\langle E \rangle_N \subseteq N$. Das heißt, für jedes $g : G$,
$$a \in \langle E \rangle_N \Rightarrow a \in N.$$
  - Da die Eigenschaft $a \in \langle E \rangle_N$ induktiv definiert wurde, können wir die vorherige Implikation durch Induktion auf a beweisen.

3.48. Übung 10

- Sei G eine Gruppe und seien U, V Untergruppen von G. Wir haben bereits gesehen, dass die Vereinigung $U \cup V$ im Allgemeinen keine Untergruppe von G ist, und dass die Teilmenge
$$P(U,V) := \{g : G \ / \ \exists\ u : U,\ \exists\ v : V,\ g = u \star v\}$$
ein Erzeugendsystem für die Untergruppe $UV := \langle U \cup V \rangle$ ist. Das heißt, $UV = \langle P(U,V) \rangle$.
- Zeigen Sie Folgendes:
  1. Wenn $U \lhd G$ *oder* $V \lhd G$, dann ist $UV = P(U,V)$. Vergleichen Sie dies mit der Summe zweier Vektorunterräume in einem Vektorraum.
  2. Wenn $U \lhd G$ *und* $V \lhd G$, dann ist $UV \lhd G$.

4. Faktorgruppen und Isomorphiesätze

Abbildung 4.1.: Ein Porträt von Leopold Kronecker.

Leopold Kronecker (1823-1891) war ein deutscher Mathematiker. Seine Forschungen lieferten grundlegende Beiträge zur Algebra und Zahlentheorie, aber auch zur Analysis und Funktionentheorie.

4.1. Untergruppen von Faktorgruppen

- Seien G eine Gruppe und N ein Normalteiler von G. Die Elemente der Faktorgruppe G/N sind die Linknebenklassen von N. Da die Untergruppe N normal ist, ist jede Linksnebenklasse von N auch eine Rechtsnebenklasse: $\forall\ g : G,\ gN = Ng$.
- Die kanonische Projektion von G nach G/N, die ein Element $g : N$ nach die Linknebenklasse gN abbildet, wird als $\pi_N : G \to G/N$ bezeichnet. Diese Abbildung ist ein Gruppenhomomorphismus, der die Eigenschaft Ker $\pi_N = N$ erfüllt.

  Satz. Falls $V \subset (G/N)$ eine Untergruppe ist, dann ist $\pi_N^{-1}(V)$ eine Untergruppe von G, die N enthält. Die Abbildung $V \mapsto \pi_N^{-1}(V)$ induziert eine Bijektion zwischen Untergruppen von G/N und Untergruppen von G, die N enthalten.

4.2. Konstruktion einer inversen Abbildung

- Zunächst überprüfen wir den ersten Teil des Satzes. Das Urbild einer Untergruppe durch einen Gruppenhomomorphismus ist immer eine Untergruppe. Daher ist $\pi_N^{-1}(V)$ eine Untergruppe von G. Da $\{e_{G/N}\} \subset V$ enthalten ist, gibt es außerdem $\pi_N^{-1}(\{e_{G/N}\}) \subset \pi_N^{-1}(V$. Das heißt, $N =$ Ker $\pi_N \subset \pi_N^{-1}(V)$.
- Jetzt möchten wir eine Abbildung konstruieren, die eine Untergruppe U von G, die N enthält, nach eine Untergruppe von G/N abbildet. Wir setzen einfach $V := \pi_N(U)$.
- Es bleibt zu beweisen, dass $\pi_N(\pi_N^{-1}(V)) = V$ und $\pi_N^{-1}(\pi_N(U)) = U$. Die erste Gleichheit folgt von der Tatsache, dass π_N surjektiv ist. Für die zweite, folgt die Inklusion $U \subset \pi_N^{-1}(\pi_N(U))$ von der Definition des Urbilds. Für die umgekehrte Inklusion, müssen wir beweisen, dass, für jedes $g : G$ gilt $g \in U$, wenn $\pi_N(g) \in \pi_N(U)$ (siehe unten).

4.3. Ende des Beweises

- Der Satz $\pi_N(g) \in \pi_N U)$ bedeutet, dass ein Element u in U existiert, mit $\pi_N(g) = \pi_N(u)$.
- Per Definition von π_N, ist $\pi_N(g) = \pi_N(u)$ äquivalent zu $gN = uN$ als Teilmenge von G. Inbesondere, $g \in uN$. Das heißt, es existiert $h : G$, sodass $h \in N$ und $g = uh$.
- Da N eine Untergruppe von U ist, impliziert die vorherige Gleichheit, dass $g \in U$.

Bemerkung. Nach dem Homomorphiesatz, können wir $\pi_N(U)$ mit der Faktorgruppe U/N identifizieren. Durch dieser Identifikation sind die Untergruppen von G/N die Gruppen der Gestalt U/N, wobei U eine Untergruppe von G ist, die N enthält.

$$\begin{array}{ccc} \{U \preccurlyeq G \text{ sodass } N \subset U\} & \xrightarrow{\simeq} & \{V \preccurlyeq (G/N)\} \\ U & \longmapsto & U\big/N \end{array}$$

4.4. Erster Isomorphiesatz

- Sei U eine Untergruppe von G. Auch wenn U nicht N enthält, ist $\pi_N(U)$ eine Untergruppe von G/N. Deshalb existiert eine Untergruppe U' von G, die N enthält, sodass $\pi_N(U) = \pi_N(U')$. Wie können wir die Untergruppen $\pi_N(U)$ und U' besser beschreiben?

  Satz. Der Gruppenhomomorphismus $\pi_N|_U : U \to G/N$ induziert einen Gruppenisomorphismus

  $$\pi_N(U) \simeq U\big/(U \cap N) \ .$$

  Außerdem gibt es eine Gleichheit $\pi_N^{-1}(\pi_N(U)) = UN$ (die von $U \cup N$ erzeugte Untergruppe von G) und einen Gruppenisomorphismus

  $$UN/N \simeq U\big/(U \cap N) \ .$$

- Für abelsche Gruppen, schreibt man oft $(U + N)/N \simeq U/(U \cap N)$.

4.5. Beweis des ersten Isomorphiesatzes

- Nach dem Homomorphiesatz, induziert $\pi_N|_U$ einen Gruppenisomorphimus

  $$U\big/(\text{Ker } (\pi_N|_U)) \simeq (\text{Im } \pi_N) = \pi_N(U)$$

- Es bleibt daher zu beweisen, dass Ker $(\pi_N|_U) = U \cap N$. Dies folgt von der Tatsachen, dass Ker $(\pi_N|_U) = U \cap (\text{Ker } \pi_N)$, und Ker $\pi_N = N$.
- Danach müssen wir noch beweisen, dass $\pi_N^{-1}(\pi_N(U)) = UN$. Da für alle $V \preccurlyeq (G/N)$, gilt $N = \text{Ker } \pi_N = \pi_N^{-1}(\{e_{G/N}\}) \subset \pi_N^{-1}(V)$. Da per Definition des Urbilds $U \subset \pi_N^{-1}(\pi_N(U))$ auch gilt, gibt es tatsächlich $(U \cup N) \subset \pi_N^{-1}(\pi_N(U))$. Da $\pi_N^{-1}(\pi_N(U))$ eine Untergruppe von G ist, impliziert die vorherige Inklusion, dass $\langle U \cup N \rangle \subset \pi_N^{-1}(\pi_N(U))$.
- Für die umgekehrte Inklusion, betrachten wir ein $g : G$, sodass $g \in \pi_N^{-1}(\pi_N(U))$. Dann existiert ein $u \in U$, sodass $gN = uN$. Insbesondere $g \in uN \subset UN$.

4.6. Zweiter Isomorphiesatz

Alle Untergruppen von G/N von der Form U/N sind. Aber für welche U sind diese Untergruppen Normalteiler von G/N?

> **Satz.** Sei U eine Untergruppe von G, die Nenthält. Dann ist U/N genau dann ein Normalteiler von G/N, wenn U ein Normalteiler von G ist. Dann gibt es außerdem ein Gruppenisomorphismus
>
> $$(G/N)\big/(U/N) \simeq G/U \ ,$$
>
> der von dem kanonischen Gruppenhomomorphismus
>
> $$G \underset{\pi_N}{\longrightarrow} G/N \underset{\pi_{U/N}}{\longrightarrow} (G/N)/(U/N)$$
>
> induziert wird.

4.7. Beweis des zweiten Isomorphiesatzes

- Wir haben schon gesehen, dass das Urbild eines Normalteilers durch einen Gruppenhomomorphismus ein Normalteiler ist.
- Wenn der Gruppenhomomorphismus außerdem surjektiv ist, ist das Bild eines Normalteilers auch ein Normalteiler.
- Da der Gruppenhomomorphismus $\pi_N : G \to G/N$ surjektiv ist, ist eine Untergruppe U von G, die N enthält, genau dann ein Normalteiler von G, wenn $\pi_N(U)$ (das isomorph zu U/N ist) ein Normalteiler von G/N ist.
- In diesem Fall, ist der kanonische Gruppenhomomorphismus $\varphi : G \to (G/N)/(U/N)$ surjektiv (als Komposition von surjektiven Homomorphismus) und wir müssen nur den Kern bestimmen. Da $\varphi := \pi_{U/N} \circ \pi_N$ ist, ist $\varphi(g) = e$ äquivalent zu $\pi_N(g) \in \operatorname{Ker} \pi_{U/N} = U/N$, was zu $g \in \pi^{-1}(U/N) = U$ äquivalent ist. Also $\operatorname{Ker} \varphi = U$.

4.8. Endliche zyklische Gruppen

- Denken Sie daran, dass eine zyklische Gruppe, eine Gruppe G ist, die von einem einzigen Element erzeugt wird: $\exists\, g : G, \langle g \rangle = G$ als Untergruppen von G. Äquivalent dazu, existiert $g : G$, sodass der kanonische Gruppenhomomorphismus $\varphi_g : \mathbb{Z} \to G$ surjektiv ist. Außerdem wissen wir bereits, dass, in diesem Fall, die Gruppe G genau dann endlich ist, wenn φ_g nicht-injecktiv ist.
- Dann ergibt sich Folgendes unmittelbar vom Homomorphiesatz.

Satz. Sei G eine **endliche zyklische Gruppe** und sei $n := |G|$ die Ordnung von G (insbesondere $n > 0$). Dann gibt es einen Gruppenisomorphismus $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Beweis. Per Annahme, und durch eine Anwendung des Homomorphiesatzes, existiert $g : G$ mit $\mathbb{Z} \;/\; \text{Ker}\ \varphi_g \simeq G$. Da Ker φ_g eine Untergruppe von $\mathbb{Z}$ ist, ist Ker $\varphi_g = m\mathbb{Z}$ für ein bestimmtes $m > 0$. Da die Ordnung von $\mathbb{Z}/m\mathbb{Z} = m$ ist, gibt es unbedingt $m = n$.

4.9. Faktorgruppen einer zyklischen Gruppen

- Wir wissen bereits, dass die Untergruppen einer zyklische Gruppe zyklische Gruppen sind. Der analoge Satz gilt für Faktorgruppen einer zyklischen Gruppe.
- Beachten Sie dass eine zyklische Gruppe ist unbedingt abelsche. Daher ist jede Untergruppe einer zyklischen Gruppe ein Normalteiler.

Satz. Sei G eine zyklische Gruppe und sei U eine Untergruppe von G. Dann ist G/U zyklisch. Wenn U nicht-trivial ist, gilt außerdem, dass G/U endlich ist.

Beweis. Da G zyklische ist, gibt es ein surjektiv Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$. Da der kanonische Gruppenhomomorphismus $\pi_U : G \to G/U$ auch surjektiv ist, ist der Gruppenhomomorphismus $\pi_U \circ \varphi : \mathbb{Z} \to G/U$ wiederum surjektiv. Dies impliziert, dass die Gruppe G/U zyklisch ist. Falls G endlich ist, ist G/U auch endlich. Ansonsten, ist $G \simeq \mathbb{Z}$ und $G/U \simeq \mathbb{Z}/n\mathbb{Z}$ für ein bestimmtes $n > 0$. Also ist G/U auch in diesem Fall endlich.

4.10. Übung 1

- Sei G eine endliche zyklische Gruppe, mit Ordnung n.
- Zeigen Sie, dass, für jeden Teiler d von n, eine Untergruppe U von G existiert, mit $|U| = d$.
- Sei U eine Untergruppe von G, mot Ordnung d. Finden Sie $k : \mathbb{N}_{>0}$, sodass $G/U \simeq \mathbb{Z}/k\mathbb{Z}$.

4.11. Struktur endlich erzeugter abelscher Gruppen

- Die Struktur einer Gruppe G zu bestimmen bedeutet, eine Liste von Gruppen anzugeben, zu denen G isomorph sein kann. Dies wird auch als *Klassifizierungsproblem* bezeichnet.
- Das allgemeneine Klassifizierungsproblem für Gruppen ist, sogar für sogenannte endliche *einfache* Gruppen, eine schwierige Frage.

- Aber für *endlich erzeugte abelsche Gruppen* haben wir zwei relativ zugänglich Klassifizierungssätze, die wir unten vorstellen werden.
- Wir werden insbesondere sehen, dass die Struktur einer endlichen abelschen Gruppe der Ordnung n vollständig durch die „arithmetische Komplexität“ von n bestimmt wird.

4.12. Gruppen mit Primzahlordnung

- Manchmal ist die Annahme, dass G abelsch ist, nicht notwendig, um G zu charakterisieren. Zum Beispiel ist jede zyklische Gruppe isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$.
- Als Nächstes, können wir nach Verwendung des Satzes von Lagrange beweisen, dass alle Gruppen mit Primzahlordnung zyklisch sind. Insbesondere ist eine solche Gruppe abelsch.

> **Satz.** Sei p eine Primzahl und sei G eine endliche Gruppe mit Ordnung p. Dann ist G eine zyklische Gruppe. Das heißt, es gibt ein Gruppenisomorphismus $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Beweis. Da die Ordnung von G eine Primzahl ist, ist $|G| > 1$. Das heißt, es gibt ein $g : G$, sodass $g \neq e$. Sei $n \geqslant 1$ die Ordnung des Elements g. Da $g \neq e$ ist, ist $n > 1$. Nach dem Satz von Lagrange, ist n ein Teiler von p. Da p eine Primzahl ist, impliziert dies, dass $n = p$. Die Untergruppe $\langle g \rangle$ von G hat deshalb Ordnung $p = |G|$. Somit $G = \langle g \rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

4.13. Klassifizierung endlicher abelscher Gruppen

- Endliche Gruppen sind endlich erzeugt. Als ersten Schritt zur Klassifizierung der endlich erzeugten abelschen Gruppen werden wir endliche abelsche Gruppen klassifizieren.
- Das wichtigste Begriff für den Beweis ist das von p-primären Anteile, für jede Primzahl p, die wir unten studieren werden.
- Der folgende Satz gibt eine komplette Klassifikation endlicher abelscher Gruppen.

> **Satz.** Sei G eine endliche abelsche Gruppe. Sei $n := |G|$ die Ordnung von G und sei $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ die Primfaktorzerlegung von n. Dann existieren eindeutige Partitionen $m_{i,1} + \dots + m_{i,s_i} = \alpha_i$, sodass
>
> $$G \simeq \prod_{i=1}^{k} \left(\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}\right) \times \ \dots \ \times \left(\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z}\right) .$$

4.14. Anmerkungen zu der Klassifikationssatz endlicher abelscher Gruppen

- Per Definition einer Partition, haben wir $s_i \geqslant 1$ und $m_{i,1} \geqslant ... \geqslant m_{i,s_i}$. Wenn wir einen Gruppenisomorphismus $G \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z})$ haben, dann ist $|G| = \prod_{i=1}^{k} p_i^{m_{i,1}+...+m_{i,s_i}}$. Da die Primfaktorzerlegung einer natürtlichen Zahl eindeutig ist, können wir auch den Klassifikationssatz wie folgt formulieren.

  Satz. Sei G eine endliche abelsche Gruppe. Dann exisitieren eine eindeutige natürliche Zahl k, eindeutige Primzahlen $p_1, \ ..., p_k$ und, für alles $i \in \{1, \ ... \ , \ k\}$, eine eindeutige endliche Folge $m_{i,1} \geqslant ... \geqslant m_{i,s_i}$, sodass G isomorph zu die Gruppe $\prod_{i=1}^{k} (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z})$ ist.

- Die natürlichen Zahlen $(p_i^{m_{i,1}}, \ ... \ , \ p_i^{m_{i,s_i}})_{1 \leqslant i \leqslant k}$ werden die **elementaren Teiler von** G gennant. Der Klassifikationssatz besagt, dass *jede endliche abelsche Gruppe isomorph zu einem Produkt zyklischer Gruppen ist.*

4.15. Primären Anteile

- Sei G eine endliche Gruppe und sei $n := |G|$. Nach dem Satz von Euler-Fermat, gibt es, für alles $g : G$, $g^n = e$.
- Sei $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ die Primfaktorzerlegung von n und sei $g : G$. Nach dem Satz von Lagrange, ist die Ordnung von g ein Teiler von n. Dann ist $\mathrm{Ord}_G(g)$ unbedingt von der Form $p_1^{\beta_1} ... p_k^{\beta_k}$, für einige natürliche Zahlen $(\beta_i)_{1 \leqslant i \leqslant k}$, mit $0 \leqslant \beta_i \leqslant \alpha_i$.
- Die Idee für p-primären Anteile besteht darin, alle Elemente von eine endliche G zusammenzufassen, *deren Ordnung eine Potenz der Primzahl p ist.*

  Definition. Sei G eine abelsche Gruppe, nicht unbedingt endlich. Für jede Primzahl p, wird der p-**primär Anteil**, als Teilmenge von G, wie folgt definiert:

$$G(p) := \{g : G \ / \ \exists \ k : \mathbb{N}_{>0}, \ g^{p^k} = e\} \ .$$

4.16. Primären Anteile sind Untergruppen

- Für abelsche Gruppe ist es oft praktisch, additive Notation zu verwenden. Das heißt, $g_1 +_G g_2$ statt $g_1 \star_G g_2$ und, wenn m eine natürliche Zahl ist, $m \cdot g$ statt g^m zu schreiben. Das neutrale Element e_G wird als 0_G bezeichnet und g^{-1}, das inverse Element zu g, als $-g$.

Satz. Der p-primär Anteil $G(p) = \{g : G \mid \exists\ k : \mathbb{N}_{>0},\ p^k \cdot g = 0\}$ ist eine Untergruppe von G. Wenn $G(p) \neq \{0_G\}$, ist p ein Teiler von $|G|$.

Beweis. Aus $p \cdot 0_G = 0_G$ folgt, dass 0_G ein Element von $G(p)$ ist. Danach:

- Wenn $g_1, g_2 \in G(p)$, dann gibt es k_1, k_2 mit $p^{k_1} \cdot g_1 = 0$ und $p^{k_2} \cdot g_2 = 0$. Somit $p^{\max(k_1,k_2)} \cdot (g_1 + g_2) = p^{\max(k_1,k_2)} \cdot g_1 + p^{\max(k_1,k_2)} \cdot g_2 = 0 + 0 = 0$.
- Wenn $g \in G(p)$, dann $p^k \cdot g = 0$ für einiges k. Somit $p^k \cdot (-g) = -(p^k \cdot g) = -0 = 0$.
- Wenn $g \neq 0_G$ und $p^k \cdot g = 0_G$, gilt $\mathrm{Ord}_G(g) \mid p^k$. Da p eine Primzahl ist, muss $p \mid |G|$.

4.17. Bemerkungen zu primären Anteile

- $p^k \cdot g = 0$ bedeutet, dass g endliche Ordung hat und dass die Ordnung von g *ein Teiler* von p^k ist. Da p eine Primzahl ist, muss $\mathrm{Ord}(g) = p^\alpha$ für einiges $\alpha \leqslant k$ gelten.
- Die hier betrachteten Konzepte sind Teil eines umfassenderen Zusammenhangs, nämlich dem der **Torsion** in einem Modul (eine abelsche Gruppe G kann auch als Modul über $\mathbb{Z}$ angesehen werden). In diesem Zusammenhang sind die p-primären Komponente Beispiele für abelsche Torsionsgruppen.
  - Für jedes $m : \mathbb{Z}$, ist die Teilmenge $G[a] := \{g : G \ /\ a \cdot g = 0\}$ eine Untergruppe von G, die als die a-Torsion von G bezeichnet wird.
  - Wenn $g : G$ die Eigenschaft $\exists\ a : \mathbb{Z}$ sodass $a \cdot g = 0$ erfüllt, heißt g ein Torsionselement von G. Die Teilmenge aller Torsionselemente einer abelschen Gruppe G ist eine Untergruppe $\mathrm{Tor}(G) \preccurlyeq G$, die die *Torsionsuntergruppe* von G genannt wird.

4.18. Abelsche Torsionsgruppen

- Eine abelsche Gruppe G wird eine Torsionsgruppe genannt, wenn jedes Element $g : G$ ein Torsionselement ist. Das heißt, falls $G = \cup_{a:\mathbb{Z}}\ G[a] = \mathrm{Tor}(G)$. Zum Beispiel, die Torsionsuntergruppe ist eine Torsionsgruppe. Das heißt, $\mathrm{Tor}(\mathrm{Tor}(G)) = \mathrm{Tor}(G)$.
- Jede endliche Gruppe ist eine Torsionsgruppe. Die Gruppe $\mathbb{Q}/\mathbb{Z}$, deren Elemente als Einheitswurzeln in $\mathbb{C}$ angesehen werden können, ist eine unendliche Torsionsgruppe.
- Die Teilmenge

$$G[a^\infty] := \bigcup_{k:\mathbb{N}_{>0}} G[a^k] \ = \ \{g : G \ /\ \exists\ k : \mathbb{N}_{>0},\ a^k \cdot g = 0\}$$

  ist auch eine Untergruppe von G, die als a^∞-Torsion von G bezeichnet wird.
- Für eine Primzahl p, wird die Notation $G(p) := G[p^\infty]$ verwendet.

4.19. Elemente mit Primzahlordnung

- Der Satz von Lagrange lässt die folgende partielle Umkehrung zu.

  > **Satz von Cauchy (kommutativer Fall).** Sei G eine endliche abelsche Gruppe und sei p ein Primteiler von $|G|$. Dann existiert ein element $g : G$ mit $\mathrm{Ord}_G(g) = p$.

- Als Konsequenz dieses Satzes ist der p-primär Anteil einer abelsche Gruppe, deren Ordnung durch p Teilbar ist, nicht trivial:

$$p \mid |G| \Rightarrow G(p) \neq \{0_G\} \ .$$

- Die Annahme, dass p eine Primzahl ist, ist wesentlich. Zum Beispiel, hat die Kleinsche Viergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ Ordnung 4 aber besitzt kein Element mit Ordnung 4.
- Die Annahme, dass G abelsch ist, ist *nicht* wesentlich (siehe den *Satz von Cauchy* später im Kurs).

4.20. Bemerkung zum Beweis

- Es reicht zu beweisen, dass ein Element $g : G$ existiert, sodass $p \mid \mathrm{Ord}_G(g)$.
- Grund dafür ist, wenn $\mathrm{Ord}_G(g) = pk$, dann $(pk) \cdot g = 0_G$. Das heißt, $p \cdot (k \cdot g) = 0_G$. Außerdem ist $g' := k \cdot g \neq 0_G$, weil $k < \mathrm{Ord}_G(g)$. Somit $\mathrm{Ord}_G(g') > 1$ und $\mathrm{Ord}_G(g') \mid p$. Da p eine Primzahl ist, gilt $\mathrm{Ord}_G(g') = p$.
- Sei $n : \mathbb{N}_{\geqslant 0}$ die natürliche Zahl sodass $|G| = n + 1$. Der Beweis des vorherigen Satzes läuft dann durch vollständige Induktion auf n.
- Genauer gesagt, werden wir beweisen, für jede Primzahl p, dass $\forall\ n \in \mathbb{N}_{\geqslant 0},\ P(n)$ gilt, wobei $P(n)$ der folgende Satz ist:

  > Für jede endliche abelsche Gruppe G sodass $|G| = n + 1$ und $p \mid |G|$, gibt es ein Element $g : G$, sodass $p \mid \mathrm{Ord}_G(g)$.

4.21. Induktion

- Wenn $n = 0$, sei G eine endliche Gruppe sodass $|G| = 1$ und $p \mid |G|$. Dann muss $p = 1$ gelten. Aber, per Definition ener Primzahl, gilt $p > 1$ und erreichen wir einen Widerspruch. Durch die *Ex falso quod libet* Regel, reicht das, um den Fall $n = 0$ zu beweisen.
- Wir müssen noch den Induktionsschritt beweisen ($n \geqslant 1$).

- Da $|G| = n + 1 \geqslant 2$, ist die Gruppe G nicht-trivial: $\exists\ g : G, g \neq 0_G$. Sei g ein solches Element und sei $U := \langle g \rangle$ die durch g erzeugte Untergruppe von G. Dann $p \mid |U| \vee p \nmid |U|$.
  - Wenn $p \mid |U|$, haben wir unmittelbar $p \mid \mathrm{Ord}_G(g)$. Genau, da $U = \langle g \rangle$, gilt $|U| = \mathrm{Ord}_G(g)$.
  - Wenn $p \nmid |U|$, da $|G| = |U||G/U|$ und p eine Primzahl ist, muss $p \mid |G/U|$ (Lemma von Euklid). Da $|G/U| < |G|$, können wir die Induktionsannahme anwenden.

4.22. Induktionsschritt

- Per Induktion, gibt es eine Nebenklasse $a+U$ in G/U (mit additiven Notation), sodass $p \mid \mathrm{Ord}_{G/U}(a + U)$.
- Setzen wir $m := \mathrm{Ord}_G(a)$ und $m_U := \mathrm{Ord}_{G/U}(a + U)$. Da $m \cdot a = 0_G$, gilt auch

$$m \cdot (a + U) = m \cdot \pi_U(a) = \pi_U(m \cdot a) = \pi_U(0_G) = 0_{G/U}.$$

- Daher muss m_U ein Teiler von m sein. Da $p \mid m_U$ gilt, muss auch $p \mid m$ gelten.
- Das heißt, wir haben ein Element a in G gefunden, so dass $p \mid \mathrm{Ord}_G(a)$ und dies beendet die Induktion.

4.23. Übung 2

- Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, wobei G und H nicht unbedingt abelsch sind.
- Sei $g : G$ und nehmen Sie an, dass g endliche Ordnung in G hat.

  1. Zeigen Sie, dass $\varphi(g)$ endliche Ordnung in H hat.
  2. Zeigen Sie, dass $\mathrm{Ord}_{G/U}(gU) \mid \mathrm{Ord}_G(g)$.

4.24. Zerlegung in primäre Anteile

- Wir wissen nun, nach diesem Satz und diesem Satz, dass $G(p) \neq \{0_G\} \Leftrightarrow p \mid |G|$. Daher ist die Menge aller Primzahlen p sodass $G(p) \neq \{0_G\}$, genau die Menge von Primfaktoren von $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$.
- Das folgende Ergebnis erklärt die Nützlichkeit von p-primären Anteile.

Satz. Sei G eine endliche abelsche Gruppe und sei $n := |G|$, mit Primfaktorzerlegung $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$. Dann gibt es einen Gruppenisomorphismus

$$G \simeq G(p_1) \times \ ... \ \times G(p_k)$$

wobei $G(p) := \{g : G \ / \ \exists \ k : \mathbb{N}_{\geqslant 0},\ p^k \cdot g = 0\}$ der p-primäre Anteil von G ist.

- Explizit werden wir einen solchen Isomorphismus φ so definieren: für jedes $(g_1, \ ... \ , \ g_k) : \prod_{i=1}^{k} G(p_i)$, setzt man $\varphi(g_1, \ ... \ , \ g_k) = g_1 + \ ... \ + g_k$.

4.25. Beweis für die Zerlegung in primäre Anteile

- Wir betrachten die folgende Abbildung.

$$\begin{array}{rcl} \varphi : G(p_1) \times \ ... \ \times G(p_k) & \longrightarrow & G \\ (g_1, \ ... \ , \ g_k) & \longmapsto & g_1 + \ ... \ + g_k \end{array}$$

- Diese Abbildung ist ein Gruppenhomomorphismus (Übung).
- Wir werden beweisen:
  1. Ker $\varphi = \{0_{G(p_1)\times \ ... \ \times G(p_k)}\} = \{(0_{G(p_1)}, \ ... \ , 0_{G(p_k)})\}$. Das heißt, dass φ injektiv ist.
  2. Im $\varphi = G$. Das heißt, dass φ surjektiv ist.

4.26. Injektivität

- Dass φ injektiv ist, bedeutet:

$$\forall \ (g_1, \ ... \ , g_k) \in \prod_{i=1}^{k} G(p_i) \ , \quad g_1 + \ ... \ + g_k = 0_G \Rightarrow \forall \ i \in \{1, \ ... \ , k\}, \ g_i = 0_G \ .$$

- Wir werden das durch endliche Induktion auf k zeigen. Das heißt, wir betrachten den folgenden Satz:

$$\forall \ j \in \{1, \ ... \ , k\}, \forall \ (g_1, \ ... \ , g_j) \in \prod_{i=1}^{j} G(p_i) \ , \ \ g_1 + ... + g_j = 0_G \Rightarrow \forall \ i \in \{1, \ ... \ , j\}, \ g_i = 0_G \ .$$

- Der Fall $j = 1$ ist klar: $\forall \ g_1 \in G(p_1)$, wenn $g = 0_G$, dann $g = 0_G$.

4.27. Ende vom Beweis der Injektivität

- Betrachten wir jetzt $(g_1, \ ... \ , g_{j+1}) \in \prod_{i=1}^{j+1} G(p_i)$ sodass $g_1 + \ ... \ + g_j + g_{j+1} = 0_G$.
- Da $g_i \in G(p_i)$, gibt es $m_i : \mathbb{N}_{>0}$ sodass $p_i^{m_i} \cdot g_i = 0_G$. Setzen wir $a := p_1^{m_1} ... p_j^{m_j}$ und $b := p_{j+1}^{m_{j+1}}$. Dann gilt $a \cdot (g_1 + \ ... \ + g_j) = 0_G$ und $b \cdot g_{j+1} = 0_G$.

  Aus diesen Gleichungen können wir *nicht* direkt ableiten, dass $(g_1 + \ ... \ + g_j) = 0_G$ und $g_{j+1} = 0_G$. Weil a und b *nicht* invertierbar in $\mathbb{Z}$ sind.
- Außerdem sind a und b teilerfr.qmd. Nach dem Lemma von Bézout existieren daher $u, v : \mathbb{Z}$, sodass $ua + vb = 1_{\mathbb{Z}}$. Dann gilt

$$g_{j+1} = 1_{\mathbb{Z}} \cdot g_{j+1} = (ua + vb) \cdot g_{j+1} = (ua) \cdot g_{j+1} + 0_G = -(ua) \cdot (g_1 + \ ... \ + g_j) = 0_G \ .$$

- Da $g_{j+1} = 0_G$, reduziert die oben Annahme zu $g_1 + \ ... \ + g_j = 0_G$. Dann impliziert die Induktionsannahme, dass $\forall \ i \ \in \{1, \ ... \ , j\}, \ g_i = 0$.

4.28. Surjektivität

- Für die Surjektivität müssen wir beweisen, dass

$$\forall \ g : G, \ \exists \ (g_1, \ ... \ , g_k) : \prod_{i=1}^{k} G(p_i), \ g = g_1 + ... + g_k \ .$$

- Erinnern Sie daran, dass $n := |G|$ mit Primfaktorzerlegung $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$, und dass $\forall \ g : G, \ n \cdot g = 0_G$ (Satz von Euler-Fermat).
- Für die Surjektivität reicht es daher zu beweisen, dass, für alle $k : \mathbb{N}_{>0}$, alle Primzahlen $(p_1, \ ... \ , p_k)$, alle natürliche Zahlen $(\alpha_1, \ ... \ , \alpha_k) : \mathbb{N}_{>0}^k$, und alles Element $g : G$,

$$(p_1^{\alpha_1} ... p_k^{\alpha_k}) \cdot g = 0_G \Rightarrow \exists \ (g_1, \ ... \ , g_k) : \prod_{i=1}^{k} G(p_i), \ g = g_1 + \ ... \ + g_k \ .$$

- Dies wird durch vollständige Induktion auf k bewiesen.

4.29. Folge vom Beweis der Surjektivität

- Wenn $k = 1$, dann müssen wir beweisen, dass

$$\forall \text{ Primzahl } p,\ \forall\ \alpha : \mathbb{N}_{>0},\ \forall\ g : G,\ (p^\alpha \cdot g = 0_G \Rightarrow g \in G(p))\ .$$

  Dies folgt aber von der Definition von $G(p) = \{g : G\ /\ \exists\ k : \mathbb{N}_{>0},\ p^k \cdot g = 0_G\}$.

- Für den Induktionsschritt, nehmen wir Primzahlen $(p_1,\ \ldots\ , p_{k+1})$, natürliche Zahlen $(\alpha_1,\ \ldots\ , \alpha_{k+1})$ und g in G sodass $(p_1^{\alpha_1} \ldots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}) \cdot g = 0_G$ und setzen wir $a := p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ und $b := p_{k+1}^{\alpha_{k+1}}$. Dann gilt $(ab) \cdot g = 0_G$.
- Da b und a teilerfr.qmd sind, existieren $u, v : \mathbb{Z}$, sodass $ub + va = 1$. Dann gilt $g = 1_{\mathbb{Z}} \cdot g = (ub) \cdot g + (va) \cdot g$. Setzen wir $h_1 := (ub) \cdot g$ und $h_2 := (va) \cdot g$.
- Dann gilt $g = h_1 + h_2$ mit $a \cdot h_1 = a \cdot ((ub) \cdot g) = (aub) \cdot g = u \cdot ((ab) \cdot g) = u \cdot 0_G = 0_G$ und $b \cdot h_2 = v \cdot ((ab) \cdot g) = v \cdot 0_G = 0_G$.

4.30. Ende vom Beweis der Surjektivität

- Da $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, aus $a \cdot h_1 = 0_G$ und der Induktionsannahme, folgt die Existenz von $(g_1,\ \ldots\ , g_k) : \prod_{j=1}^{k} G(p_j)$, sodass $h_1 = g_1 + \ \ldots\ + g_k$.
- Da $b = p_{k+1}^{\alpha_{k+1}}$, aus $b \cdot h_2 = 0_G$ folgt $h_2 \in G(p_{k+1})$. Setzen wir dann $g_{k+1} := h_2$.
- Dann gilt $g = h_1 + h_2 = (g_1 + \ \ldots\ + g_k) + g_{k+1}$, mit $\forall\ j \in \{1,\ \ldots\ , k+1\},\ g_j \in G(p_j)$ und dies beendet die Induktion.

  Bemerkung. Man kann die Zerlegung in primäre Anteile $G \simeq G(p_1) \times \ \ldots\ \times G(p_k)$ auch als direkte Summe von Untergruppen schreiben:

$$G = G(p_1) \oplus\ \ldots\ \oplus G(p_k)\ .$$

  Dies bedeutet, dass jedes $g : G$ eindeutig als $g = g_1 + \ \ldots + g_k$ mit $g_i \in G(p_i)$ geschrieben werden kann.

5. Struktur endlicher abelscher Gruppen

Abbildung 5.1.: Ein Porträt von Camille Jordan.

Camille Jordan (1838-1922) war ein französischer Mathematiker. Er hat fundamentale Beiträge zur Analysis, Gruppentheorie und Topologie geleistet. Sein Lehrbuch *Traité des substitutions et des équations algébriques* (1870) war das erste Buch über Gruppentheorie.

5.1. p-Gruppen

Definition. Für eine Primzahl p ist eine p-Gruppe eine nicht-triviale Gruppe G in der die Ordnung jedes Elements eine Potenz von p ist: $\forall\ g : G,\ \exists\ k : \mathbb{N}_{\geqslant 0},\ g^{p^k} = e_G$.

- Eine p-Gruppe ist nicht unbedingt endlich. Sie ist auch nicht unbedingt abelsch.
- Eine nicht-triviale *endliche* Gruppe G ist genau dann eine p-Gruppe wenn ihre Ordnung eine Potenz von p ist. Das heißt, wenn $\exists\ n : \mathbb{N}_{>0},\ |G| = p^n$.
  - „$\Rightarrow$“ Sei q eine Primzahl, die ein Teiler von $|G|$ ist. Nach dem Satz von Cauchy (den wir derzeit nur im abelschen Fall bewiesen haben), gibt es $g : G$ mit $\mathrm{Ord}(g) = q$. Dann muss $q = p$ und $|G| = p^n$ für einziges $n : \mathbb{N}_{>0}$.
  - „$\Leftarrow$“ Nehmen wir an, dass $|G| = p^n$. Nach dem Satz von Lagrange, muss $\mathrm{Ord}(g)$ für jedes $g : G$ ein Teiler von p sein. Da p eine Primzahl ist, muss $\mathrm{Ord}(g) = p^k$ gelten.

5.2. Beispiele für p-Gruppen

- Eine zyklische Gruppe der Gestalt $\mathbb{Z}/p^n\mathbb{Z}$ ist eine (endliche abelsche) p-Gruppe. Eine zyklische Gruppe der Gestalt $\mathbb{Z}/(pq)\mathbb{Z}$ mit p, q unterschiedliche Primzahlen ist keine p-Gruppe: nach dem Satz von Cauchy besitzt diese Gruppe ein Element mit Ordnung q.
- Produkten der Gestalt $\mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z}$ sind p-Gruppen. Die Gruppen $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind p-Gruppen, aber das Produkt $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ ist keine p-Gruppe (das Element $(1, 1)$ hat Ordnung 6, die keine Potenz einer Primzahl ist).
- Die Symmetriegruppe eines Quadrats ist eine nicht-abelsche endliche 2-Gruppe mit Ordnung $8 = 2^3$ (die Elemente r und r^3 haben Ordnung 4 und die andere nicht-triviale Elemente haben Ordnung 2).
- Die Gruppe $\{z : \mathbb{C}\ /\ \exists\ k : \mathbb{N}_{>0},\ z^{p^k} = 1\}$, bestehend aus der Elemente in $\mathbb{C}$, *mit Ordnung eine Potenz von* p, ist eine **unendliche** abelsche p-Gruppe.

5.3. Primäre Anteile

- Denken Sie daran, dass jede endliche abelsche Gruppe G isomorph zum Produkt ihrer primären Anteile ist.
- Das heißt, wenn $n := |G|$, mit Primfaktorzerlegung $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, dann gibt es einen Gruppenisomorphismus

$$\varphi : \begin{array}{ccc} G(p_1) \times \ \ldots\ \times G(p_k) & \longrightarrow & G \\ (g_1,\ \ldots\ , g_k) & \longmapsto & g_1 + \ \ldots\ + g_k \end{array}$$

  (das heißt, eine Zerlegung $G = G(p_1) \oplus \ \ldots\ \oplus G(p_k)$) wobei

$$G(p) := \{g : G\ /\ \exists\ k : \mathbb{N}_{\geqslant 0},\ p^k \cdot g = 0\}$$

  der p-primäre Anteil von G ist.
- Insbesondere ist der p-primäre Anteil $G(p)$ per Definition eine p-Gruppe.

5.4. Die Ordnung eines primären Anteils

- Wir möchten als nächsten die Struktur von der p-primären Anteile $G(p_i)$ erklären.
- Aber zunächst geben wir wieder einen formalen Beweis, dass die Ordung einer solchen Untergruppe $G(p)$ eine Potenz der Primzahl p ist.

> **Satz.** Sei G eine nicht-triviale endliche abelsche Gruppe und sei p ein Primfaktor von $|G|$. Dann existiert eine natürliche Zahl $\alpha : \mathbb{N}_{>0}$, sodass $|G(p)| = p^\alpha$.

Beweis. Sei $g \in G(p)$ sodass $g \neq 0_G$. Sei q eine Primzahl, mit $q \mid |G(p)$. Nach dem Satz von Cauchy, existiert ein $g : G(p)$ mit $\mathrm{Ord}_{G(p)}(g) = q$. Da g ein Element von $G(p)$ ist, muss $q = p^k$ für ein bestimmtes $k : \mathbb{N}_{>0}$. Da q ein Primzahl ist, impliziert dies, dass $k = 1$ und $q = p$. Dann haben wir bewiesen, dass die eindeutige Primzahl, die $|G(p)|$ teilt, p ist. Daher gilt $|G(p)| = p^\alpha$ für einziges $\alpha : \mathbb{N}_{>0}$.

5.5. Klassifikationssatz für endliche abelsche p-Gruppen

> **Satz.** Sei H eine endliche abelsche p-Gruppe mit Ordnung $|H| = p^\alpha$ für ein bestimmtes $\alpha : \mathbb{N}_{>0}$. Dann existiert eine eindeutige Partition $m_1 + ... + m_s = \alpha$, sodass
>
> $$H \simeq (\mathbb{Z}/p^{m_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z}) \ .$$

- Um diesen Satz besser zu verstanden, betrachten wir zunächst die Produktgruppe

$$G := (\mathbb{Z}/p^{m_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z})$$

mit $m_1 \geqslant \ ... \ \geqslant m_s$.

- Dann gilt $\forall\ i,\ p^{m_{i+1}} \mid p^{m_i}$ und, als Konsequenz davon, $\forall\ g : G,\ p^{m_1} \cdot g = 0_G$.
- Da das Element $g := (1, 0, \ ... \ , 0)$ Ordnung p^{m_1} hat, ist außerdem m_1 die *größte natürliche Zahl m sodass ein $g : G$ mit $Ord(g) = p^m$ existiert.* Beachten Sie, dass $(1, 1, 0, \ ... \ , 0)$ auch Ordnung p^{m_1} hat.

5.6. Eindeutigkeit der Partition

- Nehmen wir an, dass ein Gruppenisomorphismus

$$H \simeq (\mathbb{Z}/p^{m_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z})$$

existiert, mit $m_1 \geqslant \ ... \ \geqslant m_s \geqslant 1$. Dann ist

$$m_1 = \max\left\{m : \mathbb{N}_{>0} \ / \ \exists \ h : H, \ \mathrm{Ord}(h) = p^m\right\} .$$

- Betrachten wir danach die Faktorgruppe

$$H\Big/(\mathbb{Z}/p^{m_1}\mathbb{Z}) \simeq (\mathbb{Z}/p^{m_2}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z}) \ .$$

Dann ist m_2 die größte $m : \mathbb{N}_{>0}$ sodass ein $h : H/(\mathbb{Z}/p^{m_1}\mathbb{Z})$ existiert, mit $\mathrm{Ord}(h) = p^m$.

- Dies zeigt, dass die Folge $m_1, m_2, \ ... \ , m_s$ von H eindeutig bestimmt ist.

5.7. Formales Argument für den Beweis der Eindeutigkeit

- Wenn $m_1 + ... + m_s = |H| = n_1 + ... + n_t$ die beide Partionen von $|H|$ sind, so dass

$$(\mathbb{Z}/p^{m_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z}) \ \simeq \ H \ \simeq \ (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{n_t}\mathbb{Z})$$

gilt, dann ist $m_1 = n_1 = \max\{m : \mathbb{N}_{>0} \ / \ \exists \ h : H, \ \mathrm{Ord}(h) = p^m\}$.

- Dann ist die Faktorgruppe $H/(\mathbb{Z}/p^{m_1}\mathbb{Z})$ eine endliche abelsche p-Gruppe und erhalten wir einen Gruppenisomorphismus:

$$(\mathbb{Z}/p^{m_2}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z}) \ \simeq (\mathbb{Z}/p^{n_2}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{n_t}\mathbb{Z}) \ .$$

- Durch Induktion auf der Ordnung der p-Gruppe H, gilt $s = t$ und $\forall \ i \in \{1, \ ... \ , s\}$, $m_i = n_i$.

5.8. Beispiel: abelsche p-Gruppen mit Ordnung 8

- Ist G eine *abelsche* Gruppen mit Ordnung $8 = 2^3$, dann ist G eine endliche abelsche p-Gruppe. Die Möglichkeiten für Partitionen von 3 sind: $(1+1+1)$, $(2+1)$ und 3.
- Es gibt dann, bis auf Gruppenisomorphismus, die folgende drei Möglichkeiten für eine endliche ***abelsche*** Gruppe mit Ordnung 8:

  1. $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  2. $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  3. $G \simeq \mathbb{Z}/8\mathbb{Z}$.

- In diesem Beispiel sehen wir klar, dass die drei Möglichkeiten schließen sich gegenseitig aus (zum Beispiel gibt es kein Element mit Ordnung 4 oder 8 in dem ersten Produkt).
- Es gibt auch *nicht-abelsche* p-Gruppen mit Ordnung 8.

5.9. Beweis des Klassifikationssatzes für endliche abelsche p-Gruppen

Satz. Sei H eine endliche abelsche p-Gruppe mit Ordnung $|H| = p^\alpha$ für einziges $\alpha : \mathbb{N}_{>0}$. Dann existieren eine Partition $m_1 + ... + m_s = \alpha$ und ein Gruppenisomorphismus

$$H \simeq (\mathbb{Z}/p^{m_1}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p^{m_s}\mathbb{Z}) \ .$$

- Wir müssen noch diesen Existenzsatz beweisen. Die Idee ist

$$m_1 := \max\left\{m : \mathbb{N}_{>0} \ / \ \exists \ h : H, \ \mathrm{Ord}(h) = p^m\right\}$$

  zu *setzen*. Da H endlich ist, ist m_1 wohldefiniert.
- Sei $h_1 : H$ mit $\mathrm{Ord}(h_1) = m_1$ und $H_1 := \langle h_1 \rangle$ die durch h_1 erzeugte Untergruppe von H. Dann gilt $(H = H_1) \vee (H \neq H_1)$.
  - Falls $H = H_1$, dann gilt $m_1 = \alpha$ und $H \simeq \mathbb{Z}/p^\alpha\mathbb{Z}$. Der Satz wird daher bewiesen.
  - Falls $H \neq H_1$ werden wir H/H_1 betrachten und durch Induktion argumentieren.

5.10. Induktionsschritt

- Da $\langle h_1 \rangle = H_1 \neq H$ und $|H_1| = p^{m_1}$, ist die Gruppe H/H_1 eine endliche abelsche p-Gruppe mit Ordnung $p^{\alpha - m_1} < p^\alpha$. Per die Induktionsannahme existieren eine Partition $m_2 + ... + m_s = \alpha - m_1$ und ein Gruppenisomorphismus

$$H/H_1 \simeq \underbrace{(\mathbb{Z}/p^{m_2}\mathbb{Z})}_{=:H_2'} \times \ ... \ \times \underbrace{(\mathbb{Z}/p^{m_s}\mathbb{Z})}_{=:H_s'} \ .$$

- Wir können jede Gruppe H_i' als Untergruppe von H/H_1 ansehen. Da H_i' zyklisch ist, gibt es ein Element $h_i' : H/H_1$ mit $H_i' = \langle h_i' \rangle_{H/H_1}$. Inbesondere ist $\mathrm{Ord}_{H/H_1}(h_i') = p^{m_i}$.
- Von hier aus, möchten wir Folgendes beweisen:

  1. Es gibt $h_i : H$, sodass $\pi_{H/H_1}(h_i) = h_i'$ und $\mathrm{Ord}_H(h_i) = p^{m_i}$.
  2. Es gibt ein Gruppenisomorphismus $H \simeq H_1 \times H_2 \times \ ... \ \times H_s$, wobei $H_i := \langle h_i \rangle$.

5.11. Lifting-Lemma

Lemma. Sei $h' : H/H_1$, wobei H_1 wird wie zuvor definiert (m_1 maximal, sodass H_1 zyklisch mit Ordnung p^{m_1} ist). Dann existiert $h : H$ mit $\mathrm{Ord}_H(h) = \mathrm{Ord}_{H/H_1}(h')$.

Bemerkungen.

- Da $\pi_{H/H_1} : H \to H/H_1$ surjektiv ist, existiert $g : H$ mit $\pi_{H/H_1}(g) = h'$. Da π_{H/H_1} ein Gruppenhomomorphismus ist, gibt es (in multiplikative Notation)

$$(h')^{\mathrm{Ord}_H(g)} = \pi_{H/H_1}(g)^{\mathrm{Ord}_H(g)} = \pi_{H/H_1}(g^{\mathrm{Ord}_H(g)}) = \pi_{H/H_1}(e_H) = e_{H/H_1}$$

  somit $\mathrm{Ord}_{H/H_1}(h') \mid \mathrm{Ord}_H(g)$. Das Lemma besagt, dass wir ein Repräsentant $g' \sim g$ von h' finden können, sodass $\mathrm{Ord}_H(g')$ *genau das Gleiche* als $\mathrm{Ord}_{H/H_1}(h')$ ist.
- Da H/H_1 eine p-Gruppe ist, ist $\mathrm{Ord}_{H/H_1}(h')$ eine Potenz von p.

5.12. Beweis vom Lifting-Lemma

- Setzen wir $p^m := \mathrm{Ord}_{H/H_1}(h')$ und nehmen wir $g : H$ sodass $\pi_{H/H_1}(g) = h'$. Wir werden π_{H/H_1} einfach als $\pi_1 : H \to H/H_1$ schreiben. Dann gilt (in additive Notation)

$$\pi_1(p^m \cdot g) = p^m \cdot \pi_1(g) = p^m \cdot h' = 0_{H/H_1} \ ,$$

  das heißt, $p^m \cdot g \in \mathrm{Ker}\ \pi_1 = H_1$.

- Da $H_1 = \langle h_1 \rangle_H$, können wir $p^m \cdot g = r \cdot h_1$ für ein bestimmtes $r : \mathbb{N}_{>0}$ schreiben. Außerdem können wir $r = p^\ell u$ schreiben, für ein bestimmtes $\ell : \mathbb{N}_{\geqslant 0}$ und ein bestimmtes $u : \mathbb{N}_{>0}$ mit $p \nmid u$.
- Dann haben wir $p^m \cdot g = p^\ell \cdot (u \cdot h_1)$. Da $|H_1| = p^{m_1}$ und $p \nmid u$, muss $\mathrm{Ord}_{H_1}(u \cdot h_1) = p^{m_1}$ (**Übung**). Falls $\ell \geqslant m_1$, gilt daher $p^m \cdot g = p^{\ell - m_1} \cdot (p^{m_1} \cdot (u \cdot h_1)) = 0_H$. Falls $\ell < m_1$, gilt $\mathrm{Ord}_H(p^\ell \cdot (u \cdot h_1)) = p^{m_1 - l}$, somit $\mathrm{Ord}_H(p^m \cdot g) = p^{m_1 - \ell}$.

5.13. Ende vom Beweis des Lifting-Lemmas

- Wir sind noch im Fall wobei $\ell < m_1$ und $p^{m_1 - \ell} \cdot (p^m \cdot g) = 0_H$. Außerdem folgt aus der Konstruktion, dass $\mathrm{Ord}_H(g) = p^{m_1 - \ell + m}$ (**Übung**).
- Aus der Maximalität von m_1 folgt $m_1 - \ell + m \leqslant m_1$, somit $m \leqslant \ell$. Dann gilt $p^m \cdot (g - p^{\ell - m} u \cdot h_1)) = 0_H$. Setzen wir dann $h := g - p^{\ell - m} u \cdot h_1$. Dieses h ist ein Element von H, das $p^m \cdot h = 0$ erfüllt. Das heißt, $\mathrm{Ord}_H(h) \mid p^m = \mathrm{Ord}_{H/H_1}(h')$.
- Außerdem gilt $\pi_1(h) = \pi_1(g - p^{\ell - m} u \cdot h_1) = \pi_1(g) - p^{\ell - m} \cdot \pi_1(h_1) = \pi_1(g) = h'$. Daher gilt auch $\mathrm{Ord}_{H/H_1}(h') \mid \mathrm{Ord}_H(h)$.
- Da $\mathrm{Ord}_H(h) \mid p^m = \mathrm{Ord}_{H/H_1}(h')$ und $\mathrm{Ord}_{H/H_1}(h') \mid \mathrm{Ord}_H(h)$, gilt $\mathrm{Ord}_H(h) = \mathrm{Ord}_{H/H_1}(h')$.
- Dann haben wir ein Element $h : H$ aufgebaut, sodass $\pi_{H/H_1}(h) = h'$ und $\mathrm{Ord}_H(h) = \mathrm{Ord}_{H/H_1}(h')$. Dies beendet den Beweis des Lifting-Lemmas.

5.14. Zerlegung als Produkt

- Dann gehen wir zurück zum Induktionsschritt. Es gibt ein eine Partition $m_2 + \ \ldots \ + m_s = m - m_1$ und eine Zerlegung als direkte Summe von Untergruppen

$$H/H_1 \simeq H_2' \oplus \ \ldots \ \oplus H_s'$$

  wobei $H_i' := \langle h_i' \rangle_{H/H_1}$ mit $\mathrm{Ord}_{H/H_1}(h_i') = p^{m_i}$.
- Nach dem Lifting-Lemma existiert, für jedes $i \in \{2, \ \ldots \ , s\}$, ein Element $h_i : H$ mit $\mathrm{Ord}_H(h_i) = p^{m_i}$. Außerdem haben wir, per Definition von $H_1 = \langle h_1 \rangle_H$, $\mathrm{Ord}_H(h_1) = p^{m_1}$.
- Dann setzen wir $H_i := \langle h_i \rangle_H$ und betrachten wir die folgende Abbildung

$$\begin{array}{rcl} \varphi : H_1 \times H_2 \times \ \ldots \ \times H_s & \longrightarrow & H \\ (x_1, x_2, \ \ldots \ , x_s) & \longmapsto & x_1 + x_2 + \ \ldots \ + x_s \end{array}$$

  die ein Gruppenhomomorphismus ist. Am Nächsten zeigen wir, dass φ bijektiv ist.

5.15. Injektivität

- Zeigen wir zunäscht, dass φ injektiv ist. Das heißt, Ker $\varphi = \{(0_H, \ ... \ , 0_H)\}$.
- Sei $(x_1, x_2, \ ... \ , x_s) : H_1 \times H_2 \times \ ... \ \times H_s$, mit $x_1 + x_2 + \ ... \ + x_s = 0_H$. Da $H_i = \langle h_i \rangle$ mit $\mathrm{Ord}_H(h_i) = p^{m_i}$ gilt, existiert für jedes i ein $\lambda_i \in \{0_{\mathbb{Z}}, \ ... \ , \ p^{m_i} - 1_{\mathbb{Z}}\}$ mit $x_i = \lambda_i \cdot h_i$.
- Durch Abbildung der kanonischen Projektion $\pi_1 : H \to H/H_1 \simeq H_2' \times \ ... \ \times H_s'$, gilt $\pi_1(x_1 + x_2 + \ ... \ + x_s) = \pi_1(0_H) = 0_{H/H_1}$ und

$$\begin{aligned} \pi_1(x_1 + x_2 + \ ... \ + x_s) &= \lambda_1 \cdot \pi_1(h_1) + \lambda_2 \cdot \pi_1(h_2) + \ ... \ + \lambda_s \cdot \pi_1(x_s) \\ &= 0_{H/H_1} + \lambda_2 \cdot h_2' + \ ... \ + \lambda_s \cdot h_s' \end{aligned}$$

- Da $H/H_1 = \langle h_2' \rangle \oplus \ ... \ \oplus \langle h_s' \rangle$, impliziert die Gleichung $\lambda_2 \cdot h_2' + \ ... \ + \lambda_s \cdot h_s' = 0_{H/H_1}$, dass, für jedes $i \in \{2, \ ... \ , s\}$, $\lambda_i \cdot h_i' = 0_{H_i'}$, das heißt, $p^{m_i} = \mathrm{Ord}(h_i') \mid \lambda_i$, somit $\lambda_i = 0_{\mathbb{Z}}$.
- Aus $x_1 + x_2 + \ ... \ + x_s = 0_H$ folgt dann $\lambda_1 \cdot h_1 = 0_H$ und, wie zuvor, $\lambda_1 = 0_{\mathbb{Z}}$.

5.16. Surjektivität

- Sei $x : H$. Da $H/H_1 = \langle h_2' \rangle \oplus \ ... \ \oplus \langle h_s' \rangle$, können wir $\pi_1(x) = x_2' + \ ... \ + x_s'$ mit $x_i' \in \langle h_i' \rangle_{H/H_1}$ schreiben. Dann existiert, für jedes $i \in \{2, \ ... \ , n\}$, ein Element $\lambda_i \in \{0_{\mathbb{Z}}, \ ... \ , p^{m_i} - 1\}$, sodass $x_i' = \lambda_i \cdot h_i'$.
- Setzen wir danach $x_i := \lambda_i \cdot h_i \in \langle h_i \rangle = H_i \preccurlyeq H$ und $x_1 := x - (x_2 + \ ... \ + x_s)$. Dann gilt

$$\pi_1(x_1) = \pi_1(x) - (\lambda_2 \cdot \pi_1(h_2) + \ ... \ + \lambda_s \cdot \pi_1(h_s)) = \pi_1(x) - (x_2' + \ ... \ + x_s') = 0_{H/H_1}$$

  das heißt, $x_1 \in$ Ker $\pi_1 = H_1$.
- Dann gilt $x = x_1 + x_2 + \ ... \ + x_s$ mit, für jedes $i \in \{1, \ ... \ , s\}$, $x_i \in H_i$.
- Dies beendet den Beweis des Klassifikationssatzes für endliche abelsche p-Gruppen.

5.17. Klassifikationssatz für endliche abelsche Gruppen

Aus der vorherigen Klassifikationssatz für endliche abelsche p-Gruppen und die Zerlegung einer endliche abelsche p-Gruppe als Produkt/direkte Summe ihrer primären Anteile, folgt der folgende Klassifikationssatz für endliche abelsche Gruppe, den wir bereits vorgestellt haben.

> **Satz.** Sei G eine endliche abelsche Gruppe. Sei $n := |G|$ die Ordnung von G und sei $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ die Primfaktorzerlegung von n. Dann existieren eindeutige Partitionen $m_{i,1} + ... + m_{i,s_i} = \alpha_i$, sodass
>
> $$G \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z}) \ .$$

Beweis. Gilt die Zerlegung $G = G(p_1) \oplus ... \oplus G(p_k)$. Dann für jedes i existiert eine eindutige Partition $m_{i,1} + ... + m_{i,s_i} = \alpha_i$ sodass $G(p_i) \simeq (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z})$.

5.18. Bemerkungen zum Klassifikationssatz für endliche abelsche Gruppen

- In einer Partition $m_{i,1} + \ ... \ + m_{i,s_i}$, gilt $m_{i,1} \geqslant \ ... \ \geqslant m_{i,s_i}$. Es kann sein, dass $m_{i,j} = m_{i,j+1} = ... = m_{i,j+q_i}$ gilt. Daher schreibt man manchmal $n_{i,1} > \ ... \ > n_{i,\ell_i}$ mit $q_1 n_{i,1} + \ ... \ + q_{\ell_i} n_{i,\ell_i} = \alpha_i$ (statt $m_{i,1} + \ ... \ + m_{i,s_i} \alpha_i$) und

  $$G \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{n_{i,1}}\mathbb{Z})^{q_1} \times \ ... \ (\mathbb{Z}/p_i^{n_{i,\ell_i}}\mathbb{Z})^{q_{\ell_i}}$$

  statt $G \simeq (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z})$.
- Wie zuvor gesagt, die hier betrachteten Konzepte sind Teil eines breiteren Zusammenhangs, nämlich *Modulntheorie über einem Haupidealring* (wie zum Beispiel $\mathbb{Z}$), wobei jeder endlich erzeugte *Torsionsmodul* eine primäre Zerlegung hat, und jeder primäre Anteil eine Zerlegung in direkte Summe von zyklischen Untermoduln hat. Wir werden diese Konzepte später im Kurs wieder antreffen.

5.19. Die Elementareteiler einer endlichen abelschen Gruppen

- Die wichtigste Information im Klassifikationssatz für endliche abelsche Gruppen ist die endliche Folge $(p_i^{m_{i,j}})_{1 \leqslant i \leqslant k, \ 1 \leqslant j \leqslant s_i}$. Diese Folge bestimmt vollständig die Isomorphieklasse der Gruppe G. im folgenden Sinne:

$$G \simeq \prod_{i=1}^{k} \left(\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}\right) \times \ \ldots \ \times \left(\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z}\right) \ .$$

- Insbesondere bestimmt diese Folge die Ordnung von G ($|G| = \prod_{i=1}^{k} p_i^{m_{i,1}+ \ \ldots \ +m_{i,s_i}}$).

  Definition. Die endliche Folge $(p_i^{m_{i,j}})_{1 \leqslant i \leqslant k, \ 1 \leqslant j \leqslant s_i}$ heißt die Folge von **Elementarteiler** der Gruppe G.

  Zum Beispiel, ist die Folge der Elementarteiler der Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ die endliche Folge $(2, 2, 2)$.

5.20. Die aus den Elementarteilern aufgebaut Matrix

Mit den Konventionen $p_1 < \ \ldots < p_k$ und $m_{i,1} \geqslant \ \ldots \ \geqslant m_{i,s_i}$, können wir die folgende $k \times s$ Matrix $(\beta_{i,j})_{1 \leqslant i \leqslant k, \ 1 \leqslant j \leqslant s}$ konstruieren, wobei $s := \max_{1 \leqslant i \leqslant k} \ s_i$.

$$\beta := \begin{bmatrix} p_1^{m_{1,1}} & p_1^{m_{1,2}} & \ldots & \ldots & p_1^{m_{1,s_1}} & 1 & 1 \\ p_2^{m_{2,1}} & p_1^{m_{2,2}} & \ldots & \ldots & \ldots & \ldots & p_2^{m_{2,s_2}} \\ \vdots & & & & & & \\ p_k^{m_{k,1}} & p_k^{m_{k,2}} & \ldots & p_k^{m_{k,s_k}} & 1 & \ldots & 1 \end{bmatrix}$$

Das heißt:

$$\beta_{i,j} := \begin{cases} p_i^{m_{i,j}} & \text{if } j \leqslant s_i \ , \\ 1 & \text{if } s_i < j \leqslant s \ . \end{cases}$$

Wenn $\beta_{i,j} = 1$, dann ist $\mathbb{Z}/\beta_{i,j}\mathbb{Z}$ die triviale Gruppe. Daher gilt $G \simeq \prod_{i=1}^{k} \prod_{j=1}^{s} \mathbb{Z}/\beta_{i,j}\mathbb{Z}$. Wir können auch $m_{i,j} = 0$ für alles j mit $s_i < j \leqslant s$ setzen.

5.21. Invarianten Faktoren

- Setzen wir, für alles $j \in \{1, \ \ldots \ , s\}$, $d_j := \prod_{i=1}^{k} \beta_{i,j}$ (das Produkt der Elemente der j-ten Spalte). Die $(d_j)_{1 \leqslant j \leqslant s}$ werden die **invarianten Faktoren** von G genannt.
- Dann gelten die folgende Eigenschaften:
  - Da $\forall \ i, \ m_{i,j+1} \leqslant m_{i,j}$, ist $d_{j+1} = \prod_{i=1}^{k} p_i^{m_{i,j+1}}$ ein Teiler von $d_j = \prod_{i=1}^{k} p_i^{m_{i,j}}$.

– In der j-ten Spalte, sind Elemente $\beta_{i_1,j}$ und $\beta_{i_2,j}$ in verschiedenen Zeilen teilerfr.qmd. Nach dem chinesischen Restsatz, gibt es daher ein Gruppenisomorphismus

$$\prod_{i=1}^{k} (\mathbb{Z}/\beta_{i,j}\mathbb{Z}) \quad \simeq \quad \mathbb{Z}/\left(\prod_{i=1}^{k} \beta_{i,j}\right)\mathbb{Z} \quad = \quad \mathbb{Z}/d_j\mathbb{Z}$$

– Die Primfaktorzerlegung von d_j ist genau $\prod_{i\in\{1\leqslant i\leqslant k \ / \ m_{i,j}>0\}} p_i^{m_{i,j}}$. Wir können daher die Elementarteiler $(p_i^{m_{i,j}})_{i,j}$ von den invarianten Faktoren $(d_j)_{1\leqslant j\leqslant s}$ erneut finden.

5.22. Der Satz über invariante Faktoren

- Als Konsequenz der vorherigen Bemerkungen, gilt der folgende Satz.

  Satz. Sei G eine endliche abelsche Gruppe. Dann existiert eine eindeutige endliche Folge $(d_1, \ \dots \ , d_s)$ mit:

  1. $\forall\ j \in \{1, \ \dots \ , s-1\},\ d_{j+1} \mid d_j$.
  2. $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \ \dots \ \times (\mathbb{Z}/d_s\mathbb{Z})$.

- Dies gibt eine andere Zerlegung von G als Produkt zyklischer Gruppen. Das heißt, es gibt einen anderen Klassifikationssatz. Natürlich ist $|G| = d_1 \ \dots \ d_s$.
- Die Eindutigkeit der invarianten Faktoren folgt aus der Eindeutigkeit der Elementarteiler.
- Eine abstrakte Version dieses Ergebnisses hat Anwendungen in der linearen Algebra (Frobenius-Normalform).

5.23. Abelsche Gruppen mit Ordnung 600

- Sei G eine abelsche Gruppe mit Ordnung $600 = 2^3 \times 3^1 \times 5^2$. Dann haben drei Primzahlen $p_1 = 2$, $p_2 = 3$ und $p_3 = 5$, mit Exponente $\alpha_1 = 3$, $\alpha_2 = 1$ und $\alpha_3 = 2$.
- Die Möglichkeiten für die Partionen für α_1, α_2, α_3 sind:
  - $3 = 1 + 1 + 1$, $3 = 2 + 1$, und $3 = 3$ (drei Möglichkeiten).
  - $1 = 1$ (eine einzige Möglichkeit).
  - $2 = 1 + 1$ und $2 = 2$ (zwei Möglichkeiten).
- Das heißt, wir haben $3 \times 1 \times 2 = 6$ Möglichkeiten für die Isomorphieklasse von G.

5.24. Erster Fall

- Falls $3 = 1 + 1 + 1$, $1 = 1$ und $2 = 1 + 1$ die Partinionen von 3, 1 und 2 sind, dann sind die Elementarteiler von G die natürliche Zahlen $(2, 2, 2, 3, 5, 5)$ und gilt

$$G \simeq \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}_{\text{2-primaere Anteil von } G} \times \underbrace{\mathbb{Z}/3\mathbb{Z}}_{\text{3-primaere Anteil von } G} \times \underbrace{\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}}_{\text{5-primaere Anteil von } G} .$$

- Dann betrachten wir die Matrix

$$\begin{bmatrix} 2 & 2 & 2 \\ 3 & 1 & 1 \\ 5 & 5 & 1 \end{bmatrix}$$

und die invarianten Faktoren $d_1 = 2 \times 3 \times 5 = 30$, $d_2 = 2 \times 1 \times 5 = 10$ und $d_3 = 2 \times 1 \times 1 = 2$. Dann gilt $d_3 \mid d_2 \mid d_1$ und existiert ein Gruppenisomorphismus

$$G \simeq \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} .$$

5.25. Zweiter Fall

- Falls $3 = 1 + 1 + 1$, $1 = 1$ und $2 = 2$, gibt es $(2, 2, 2, 3, 25)$ für die Elementarteiler und

$$G \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} .$$

- Dann ist die Matrix von Elementarteiler

$$\begin{bmatrix} 2 & 2 & 2 \\ 3 & 1 & 1 \\ 25 & 1 & 1 \end{bmatrix}$$

und sind die invarianten Faktoren $d_1 = 2 \times 3 \times 25 = 150$, $d_2 = 2$ und $d_3 = 2$, sodass $d_3 \mid d_2 \mid d_1$ und

$$G \simeq \mathbb{Z}/150\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} .$$

5.26. Übung 1

- Berechnen Sie die Elementarteiler und die invarianten Faktoren in den verbleibenden vier Fällen.
- Es wird Fälle geben, in denen es nur 2 oder wenig invariaten Faktoren gibt. Zum Beispiel, $G \simeq \mathbb{Z}/600\mathbb{Z}$.
- Im Allgemeinem ist die „Normalform“ einer endlichen abelschen Gruppe mit den invarianten Faktoren praktischer und kürzer zu schreiben als die Normalform mit den Elementarteilern.

5.27. Übung 2

Sei $m, n : \mathbb{N}_{>0}$.

- Zeigen Sie, dass die Gruppen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ genau dann isomorph sind, wenn m und n teilerfr.qmd sind.
- Zeigen Sie danach, dass ein Produkt zweier zyklischer Gruppen mit teilerfr.qmden Ordnungen wieder zyklisch ist.

5.28. Übung 3

- Sei G eine (nicht unbedingt abelsche) endliche Gruppe. Sei

$$\omega(G) := \min\{n : \mathbb{N}_{>0} \ / \ \forall \ g : G, \ g^n = e_G\} \ .$$

  Zeigen Sie, dass $\omega(G)$ wohldefiniert ist.

- Jetzt nehmen wir außerdem G abelsch an.
  - Zeigen Sie, dass $\omega(G)$ das kleinstes gemeinsames Vielfaches der Ordnungen der Elemente von G ist.
  - Zeigen Sie, dass $\exists \ \alpha : \mathbb{N}_{>0}, \ |G| \mid \omega(G)^\alpha$. **Hinweis:** Zeigen Sie zunächst, dass $|G|$ und $\omega(G)$ die gleichen Primteiler haben.

6. Struktur endlich erzeugter abelscher Gruppen

Abbildung 6.1.: Ein Porträt von Felix Klein.

Felix Klein (1849-1925) war ein deutscher Mathematiker. Seine Forschungen lieferten grundlegende Beiträge zur Geometrie, Gruppentheorie, Funktionentheorie und Anwendugen der Mathematik.

6.1. Endlich erzeugte abelsche Gruppen

- Denken Sie daran, dass eine Gruppe G endlich erzeugt gennant wird, wenn es ein endlich Erzeugendensystem $(g_1, \ \dots \ , g_k)$ gibt, sodass $\langle g_1, \ \dots \ , g_k \rangle_G = G$.
- Im abelschen Fall bedeutet das, dass jedes Element $g : G$ als lineare Kombination der $(g_i)_{1 \leqslant i \leqslant k}$ geschrieben werden kann:

$$g = \lambda_1 \cdot g_1 + \ \dots \ + \lambda_k \cdot g_k, \ \text{mit } \lambda_i : \mathbb{Z} \ .$$

- Zum Beispiel ist jede Gruppe $\mathbb{Z}^r$ endlich erzeugt.
- Jede endliche Gruppe ist endlich erzeugt (nehmen Sie für ein Erzeugendensystem die ganze zugrundeliegende Menge von G).

- Wenn G_1 und G_2 endlich erzeugt sind, so ist das Produkt $G_1 \times G_2$. Zum Beispiel ist $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ endlich erzeugt.

6.2. Klassifikationssatz für endlich erzeugte abelsche Gruppen

- In gewisser Weise kennen wir bereits *alle* endlich erzeugten abelschen Gruppen.

  Satz. Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutige natürliche Zahlen $n : \mathbb{N}_{\geqslant 0}$ und $s : \mathbb{N}_{\geqslant 0}$ und eine eindeutige Folge natürlichen Zahlen $(d_1, \ ... \ , d_s) : \mathbb{N}_{>0}^{s}$, so dass die folgende Eigenschaften gelten:

  1. $\forall\ j \in \{1, \ ... \ s-1\},\ d_{j+1} \mid d_j$.
  2. Es gibt einen Gruppenisomorphismus

  $$G \simeq \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/d_s\mathbb{Z}) \ .$$

- Beachten Sie, dass der Teil $(\mathbb{Z}/d_1\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/d_s\mathbb{Z})$ eine endliche abelsche Gruppe ist.
- Dieser Satz hat viele Anwendungen, zum Beispiel in der algebraischen Topologie (Homologietheorie von Mannigfaltigkeiten *usw*).

6.3. Torsionsuntergruppe

- Wir werden den Beweis des vorherigen Satzes in mehrere Schritte unterteilen.
- Die erste Frage ist: Wenn $G := \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/d_s\mathbb{Z})$, wie kann man die endliche Gruppe $(\mathbb{Z}/d_1\mathbb{Z}) \times \ ... \ \times (\mathbb{Z}/d_s\mathbb{Z})$ als Untergruppe von G charakterisieren?

  Definition. Sei G eine abelsche Gruppe. Ein Element von G mit endlicher Ordnung wird als **Torsionselement** bezeichnet.

  $$\mathrm{Tor}(G) := \{g : G \mid \exists\ n : \mathbb{N}_{>0},\ n \cdot g = 0_G\} \ .$$

- Da G abelsch ist, ist die Teilmenge $\mathrm{Tor}(G)$ eine Untergruppe von G. **Beweis.** $0_G \in \mathrm{Tor}(G)$ und, wenn $g_1, g_2 \in \mathrm{Tor}(G)$, dann gibt es $n_1 \cdot g_1 = 0_G$ und $n_2 \cdot g_2 = 0_G$ für einigen n_1, n_2, somit auch $n \cdot (g_1 + g_2) = 0_G$ für $n := \max(n_1, n_2)$. Schließlich gilt auch $n_1 \cdot (-g_1) = -(n_1 \cdot g_1) = -0_G = 0_G$. Das heißt, $-g_1$ ist auch Torsion.

6.4. Beispiel für Torsionsuntergruppen

- Wenn G eine endliche Gruppe ist, ist $\mathrm{Tor}(G) = G$. Die Faktorgruppe $\mathbb{Q}/\mathbb{Z}$ (die isomorph zu die Gruppe der Einheitswurzeln $\mu := \{z : \mathbb{C} \mid \exists\, n : \mathbb{N}_{>0},\ z^n = 1\}$ ist) ist ein Beispiel für eine unendliche abelsche Gruppe G mit $\mathrm{Tor}(G) = G$.
- Die Torsionsuntergruppe von $G := \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \ \ldots\ \times (\mathbb{Z}/d_s\mathbb{Z})$ ist genau die Untergruppe $T := (\mathbb{Z}/d_1\mathbb{Z}) \times \ \ldots\ \times (\mathbb{Z}/d_s\mathbb{Z})$. **Beweis.** Sei $g = (x_1, \ \ldots\ , x_r, h_1, \ \ldots\ , h_s)$ ein Element von G und sei n eine natürliche Zahl mit $n \geqslant d_j$ für alles j. Dann gilt $n \cdot g = (nx_1, \ \ldots\ , nx_s, 0, \ \ldots\ , 0)$. Insbesondere, wenn $\forall\ j \in \{1, \ \ldots\ , r\}, x_i = 0_{\mathbb{Z}}$ gilt, dann ist $n \cdot g = 0_G$. Das heißt, $T \subset \mathrm{Tor}(G)$. Umgekehrt, wenn $n \cdot g = 0_G$ für einige $n > 0$, dann gibt es, für alles $i \in \{1, \ \ldots\ , r\}$, $n \cdot x_i = 0_{\mathbb{Z}}$. Da $n \neq 0_{\mathbb{Z}}$, impliziert das, dass $x_i = 0_{\mathbb{Z}}$. Das heißt, $\mathrm{Tor}(G) \subset T$.

6.5. Quotient durch die Torsionsuntergruppe

- Im Beispiel $G := \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \ \ldots\ \times (\mathbb{Z}/d_s\mathbb{Z})$ gilt $G/\mathrm{Tor}(G) \simeq \mathbb{Z}^r$ und $\mathbb{Z}^r$ ist **torsionsfrei / ohne Torsion** (das heißt, $\mathrm{Tor}(\mathbb{Z}^r) = \{0_{\mathbb{Z}^r}\}$).
- Dies ist eine allgemeine Tatsache.

  Satz. Sei G eine abelsche Gruppe. Die Faktorgruppe $G/\mathrm{Tor}(G)$ hat keine Torsion:

  $$\mathrm{Tor}(G/\mathrm{Tor}(G)) = \{0_G\}\ .$$

  Beweis. Sei $[g]$ ein Element von $G/\mathrm{Tor}(G)$ (das heißt, $[g] := g + \mathrm{Tor}(G)$ ist die Nebenklasse, modulo die Untergruppe $\mathrm{Tor}(G)$, des Elements g von G) und nehmen wir an, dass es ein $n : \mathbb{N}_{>0}$ gibt, mit $n \cdot [g] = 0_{G/\mathrm{Tor}(G)}$. Dann gilt $[n \cdot g] = 0_{G/\mathrm{Tor}(G)}$. Das heißt, $n \cdot g \in \mathrm{Tor}(G)$. Existiert dann $k : \mathbb{N}_{>0}$, so dass $k \cdot (n \cdot g) = 0_G$. Das heißt, $(kn) \cdot g = 0_G$, mit $kn : \mathbb{N}_{>0}$. Somit $g \in \mathrm{Tor}(G)$ und $[g] = 0_{G/\mathrm{Tor}(G)}$. Dies genügt, um $\mathrm{Tor}(G/\mathrm{Tor}(G)) = \{0_G\}$ zu beweisen.

6.6. Übung 1

Seien G und H abelsche Gruppen.

- Zeigen Sie die folgende universelle Eigenschaft:

  $$\forall\ \varphi : \mathrm{Hom}_{\mathrm{Gpp}}(G, H),\ \exists!\ \overline{\varphi} : \mathrm{Hom}_{\mathrm{Gpp}}(G/\mathrm{Tor}(G), H/\mathrm{Tor}(H)),\ \pi_{H/\mathrm{Tor}(H)} \circ \varphi = \overline{\varphi} \circ \pi_{G/\mathrm{Tor}(G)}\ .$$

- Inbesondere, wenn H torsionsfrei ist, gibt es eine eindeutige Faktorisation $\overline{\varphi} : G/\mathrm{Tor}(G) \to H$, sodass $\varphi = \overline{\varphi} \circ \pi_{G/\mathrm{Tor}(G)}$.

6.7. Endlich erzeugte Torsionsgruppen

Wir haben bereits gesehen, dass eine endliche Gruppe endlich erzeugt ist, und eine Torsionsgruppe. Das Umgekehrte gilt ebenfalls.

Satz. Eine endlich erzeugte Torsionsgruppe ist endlich.

Beweis. Sei G eine abelsche Gruppe, die endlich erzeugt und eine Torsionsgruppe ist. Sei $(g_1, \ \dots \ , g_k)$ ein Erzeugendensystem für G. Dies bedeutet, dass der folgende Gruppenhomorphismus surjektiv ist.

$$\varphi : \mathbb{Z} \times \dots \times \mathbb{Z} \longrightarrow G, \quad (\lambda_1, \ \dots \ , \lambda_k) \longmapsto \lambda_1 \cdot g_1 + \ \dots \ + \lambda_k \cdot g_k$$

Da G eine Torsionsgruppe ist, hat jedes g_i endlich Ordnung. Sei $n_i := \mathrm{Ord}_G(g_i)$. Dann gilt $\mathrm{Ker}\ \varphi = n_1\mathbb{Z} \times \ \dots \ \times n_k\mathbb{Z}$ und gibt es einen surjektiven Gruppenhomomorphismus von einer endlichen Gruppe nach G. Insbesondere ist G eine endliche Gruppe.

$$\overline{\varphi} : G/\mathrm{Ker}\ \varphi \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times \ \dots \ \times (\mathbb{Z}/n_k\mathbb{Z}) \longrightarrow G$$

6.8. Freie abelsche Gruppen

- Eine endlich erzeugte abelsche Gruppe ist analog zu einem endlichdimensionalen Vektorraum: das heißt, *es gibt ein endliches Erzeugendensystem*. Der Unterschied besteht darin, dass ein endlichdimensionaler Vektorraum unbedingt eine endliche Basis besitzt.

  Definition. Sei G eine abelsche Gruppe. Eine Familie $(g_i)_{i \ : \ I}$ von Elementen aus G wird als $\mathbb{Z}$-**Basis** bezeichnet, wenn es, für alles $g : G$, eine eindeutige Familie von ganzen Zahlen $(\lambda_i)_{i \ : \ I}$ gibt, sodass:

  1. Die Menge $\{j : I \ / \ \lambda_j \neq 0_{\mathbb{Z}}\}$ endlich ist. In diesem Fall ist $(\lambda_i)_{i:I}$ ein Element aus der Menge $\mathbb{Z}^{(I)}$, bestehend aus Abbildungen mit endlichen Träger.
  2. $g = \sum_{i:I} \lambda_i \cdot g_i$ (Im Hinblick auf Bedingung (i), ist diese Summe wohldefiniert).

- Wenn G eine $\mathbb{Z}$-basis besitzt, wird G eine $\mathbb{Z}$-**freie abelsche Gruppe** genannt. Man sagt auch *Basis* und *freie abelsche Gruppe*, statt $\mathbb{Z}$-Basis und $\mathbb{Z}$-freie abelsche Gruppe.

6.9. Endliche Basen und Rang

- Eine endliche Familie $(g_1, \ \dots \ , g_k)$ ist genau dann eine Basis, wenn, für jedes $g : G$, $\exists!$ $(\lambda_1, \ \dots \ , \lambda_k) : \mathbb{Z}^k$, sodass $g = \lambda_1 \cdot g_1 + \ \dots \ + \lambda_k \cdot g_k$.

  Satz. Sei G eine abelsche Gruppe, die eine Basis $(g_1, \ \dots \ , g_n)$ mit n Elementen besitzt. Dann hat jede Basis für G genau n Elemente.

  Beweis. Nehmen wir an, dass $(g_1, \ \dots \ , g_k)$ und $(h_1, \ \dots \ , h_\ell)$ beide Basen von G sind.

  - Dann ist, per Definition einer Basis, die Abbildung $\varphi : \mathbb{Z}^k \to G$, die durch $\varphi(\lambda_1, \ \dots \ , \lambda_k) := \lambda_1 \cdot g_1 + \ \dots \ + \lambda_k \cdot g_k$ definiert wird, ein Gruppenisomorphismus. Das heißt, durch die Wahl von $(g_1, \ \dots \ , g_k)$ ist $G \simeq \mathbb{Z}^k$.
  - In analoger Weise, ist G durch die Wahl von $(h_1, \ \dots \ , h_\ell)$ isomorph zu $\mathbb{Z}^\ell$.
  - Aber wenn $\mathbb{Z}^k \simeq \mathbb{Z}^\ell$, muss $(\mathbb{Z}/2\mathbb{Z})^k \simeq \mathbb{Z}^k/2\mathbb{Z}^k \simeq \mathbb{Z}^\ell/2\mathbb{Z}^\ell \simeq (\mathbb{Z}/2\mathbb{Z})^\ell$ auch gelten. Durch Vergleichung die Kardinalität dieser Mengen, gibt es $2^k = 2^\ell$, somit $k = \ell$.

6.10. Der Rang einer freien Gruppe mit endlicher Basis

- Wenn G eine endliche Basis besitzt, kann man den **Rang** von G definieren.

  Definition. Die Kardinalität einer beliebigen Basis für G wird **Rang** von G genannt, und als $\mathrm{Rg}(G)$ bezeichnet.

- Zum Beispiel hat $\mathbb{Z}^n$ Rang n. Um es zu beweisen, reicht es *eine* Basis zu finden! Die sogenannte *kanonische Basis* von $\mathbb{Z}^n$ ist:

$$e_1 = (1, 0, 0 \ \dots \ , 0), \ e_2 = (0, 1, 0 \ \dots \ , 0), \ e_n = (0, , \ \dots \ , 0, 1)$$

- Der Fall $\mathrm{Rg}(G) = 0$ ist äquivalent zu $G = \{0_G\}$. In diesem Fall ist die leere Familie eine Basis für G (nehmen Sie $I = \emptyset$ in der Definition einer Basis). ## Untergruppen einer endlich erzeugten freien abelschen Gruppe

  Satz. Sei G eine endlich erzeugte freie abelsche Gruppe (das heißt, eine abelsche Gruppe mit einer endlichen Basis). Sei $n := \mathrm{Rg}(G)$. Dann ist jede Untergruppe $U \preccurlyeq G$ eine endlich erzeugte freie abelsche Gruppe, mit $\mathrm{Rg}(U) \leqslant n$.

Beweis. Der Beweis erfolgt durch Induktion über n.

- Wenn $n = 0$, gilt $U = G = \{e_G\}$, die eine endlich erzeugte freie Gruppe mit Rang 0 ist.
- Nehmen wir an, dass $n = k + 1$ und dass die Eigenschaft gilt, für Untergruppen von endlich erzeugten Gruppen mit Rang k. Dann können wir G als $\mathbb{Z}g_1 \oplus \ \dots \ \oplus \mathbb{Z}g_k \oplus \mathbb{Z}g_{k+1}$, für einige $\mathbb{Z}$-Basis $(g_1, \ \dots \ , g_k, g_{k+1})$ von G schreiben. Sei $\pi : G \to \mathbb{Z}g_{k+1}$ die durch $(x_1, \ \dots \ , x_k, x_{k+1}) \mapsto x_{k+1}$ definierte Projektion.
- Dann ist $\pi(U)$ eine Untergruppe von $\mathbb{Z}g_{k+1} \simeq \mathbb{Z}$. Aber eine Untergruppe von $\mathbb{Z}$ muss von der Form $m\mathbb{Z}$ sein. Dann gilt $\pi(U) \simeq m(\mathbb{Z}g_{k+1}) \simeq \mathbb{Z}(m \cdot g_{k+1})$, die $\mathbb{Z}$-frei ist.

6.11. Folge vom Beweis der Existenz einer Basis

- Das heißt, $\pi(U)$ besitzt eine Basis, mit einem einzigen Element $h_{k+1} \coloneqq m \cdot g_{k+1}$.
- Danach, per die Induktionsannahme, besitzt die Untergruppe

$$\text{Ker } \pi|_U = U \cap \text{Ker } \pi \subseteq \text{Ker } \pi = \mathbb{Z}g_1 \oplus \ \ldots \ \oplus \mathbb{Z}g_k \simeq \mathbb{Z}^k$$

  eine Basis, mit Kardinalität $\ell \leqslant k$. Sei $(h_1, \ \ldots \ , h_\ell)$ eine solche Basis für Ker $\pi|_U$.
- Sei u ein Element von U. Da $\pi(u - \pi(u)) = \pi(u) - \pi(\pi(u)) = \pi(u) - \pi(u) = 0_G$, ist $u - \pi(u)$ ein Element von Ker π. Außerdem ist $\pi(u)$ ein Element aus $\pi(U) = \mathbb{Z}h_{k+1}$. Daher können wir $u - \pi(u) = \lambda_1 h_1 + \ \ldots \ + \lambda_k h_k$ und $\pi(u) = \lambda_{k+1} h_{k+1}$ schreiben.
- Dann gilt $u = (u - \pi(u)) + \pi(u) \in \langle h_1, \ \ldots \ , h_k, h_{k+1} \rangle_G$. Dies bewiest, dass $U = \langle h_1, \ \ldots \ , h_k, h_{k+1} \rangle_G$. Insbesondere ist U endlich erzeugt.

6.12. Ende vom Beweis der Existenz einer Basis

- Es bleibt zu beweisen, dass das Erzeugendensytem $(h_1, \ \ldots \ , h_k, h_{k+1})$ eine Basis für U ist. Das heißt, dass die Familie $(h_1, \ \ldots \ , h_k, h_{k+1})$ auch eine **freie Familie** ist:

$$(\lambda_1 \cdot h_1 + \ \ldots \ + \lambda_k \cdot h_k + \lambda_{k+1} \cdot h_{k+1} = 0_G) \Longrightarrow (\lambda_1 = \ \ldots \ = \lambda_k = \lambda_{k+1} = 0_{\mathbb{Z}}) \ .$$

- Setzen wir $x \coloneqq \lambda_1 \cdot h_1 + \ \ldots \ + \lambda_k \cdot h_k \in \text{Ker } \pi|_U$ und $y \coloneqq \lambda_{k+1} \cdot h_{k+1} \in \pi(U)$ und nehmen wir an, dass $x + y = 0_G$. Dann gilt $0_G = \pi(0_G) = \pi(x) + \pi(y) = 0_G + y = y$. Daher auch $x = 0_G$.
- Aus $x = 0_G$ und der Tatsache, dass die Familie $(h_1, \ \ldots \ , h_k)$ eine Basis für Ker $\pi|_U$ ist, folgt $\forall \ i \in \{1, \ \ldots \ , k\}, \ \lambda_i = 0_{\mathbb{Z}}$.
- Und aus $y = 0_G$ und der Tatsache, dass h_{k+1} eine Basis für $\pi(U)$ ist, folgt $\lambda_{k+1} = 0_{\mathbb{Z}}$. Dies beendet den Beweis.

6.13. Unterschiede zu Vektorräume

- In einer endlich erzeugten freien abelschen Gruppe mit Rang n, ist eine freie Familie mit n Elemente nicht unbedingt eine Basis. Zum Beispiel, in $G = \mathbb{Z}$, die Familie mit dem einzigen Element $h \coloneqq 2$ ist $\mathbb{Z}$-frei ($n \cdot 2 = 0_{\mathbb{Z}} \Rightarrow 2n = 0_{\mathbb{Z}} \Rightarrow n = 0_{\mathbb{Z}}$) aber kein Erzeugendensystem für $\mathbb{Z}$.
- Aus dem gleichen Grund, ist eine Untergruppe U von G mit $\text{Rg}(U) = \text{Rg}(G)$ nicht unbedingt die ganze G. Zum Beispiel, $2\mathbb{Z} \neq \mathbb{Z}$.

- Es ist im Allgemeinen nicht möglich, in einem Erzeugendensystem, eine Unterfamilie zu finden, die eine Basis für G ist. Zum Beispiel, in $G = \mathbb{Z}$, ist die Familie $(h_1, h_2) := (2, 3)$ ein Erzeugendensystem (da $3 - 2 = 1$ und $\langle 1 \rangle_{\mathbb{Z}} = \mathbb{Z}$) aber weder $h_1 = 2$ noch $h_2 = 3$ sind Basen für $\mathbb{Z}$.

6.14. Freie abelsche Gruppe sind torsionsfrei

- Das folgende Ergebnis gilt für alle freie abelsche Gruppe (*keine* Annnahme, dass G endlich erzeugt ist).

  Satz. Sei G eine freie abelsche Gruppe. Dann ist G torsionsfrei.

  Beweis. Sei $(g_i)_{i \,:\, I}$ eine Basis für G und sei g ein Torsionselement. Dann existiert $n : \mathbb{N}_{>0}$ mit $n \cdot g = 0_G$ und eine Familie $\lambda : \mathbb{Z}^{(I)}$, sodass $g = \sum_{i:I} \lambda_i \cdot g_i$. Gilt deshalb

  $$0_G = n \cdot g = n \cdot \sum_{i:I} \lambda_i \cdot g_i = \sum_{i:I} (n\lambda_i) \cdot g_i.$$

  Da die Familie $(g_i)_i$ frei ist, impliziert dies, dass $\forall\ i : I, n\lambda_i = 0_{\mathbb{Z}}$, somit $\lambda_i = 0_{\mathbb{Z}}$.

- Die umgekehrte Implikation gilt im Allgemeinen nicht. Zum Beispiel, die abelsche Gruppe $\mathbb{Q}$ ist torsionsfrei ($(n \cdot \frac{a}{b} = 0_{\mathbb{Q}}) \wedge \frac{a}{b} \neq 0_{\mathbb{Q}} \Rightarrow n = 0_{\mathbb{Z}}$) aber nicht $\mathbb{Z}$-frei (siehe unten).

6.15. Übung 2

- Zeigen Sie, dass Elemente $\frac{p}{q}$ und $\frac{p'}{q'}$ in $\mathbb{Q}$ immer linear abhängig über $\mathbb{Z}$ sind. Das heißt, finden Sie $n, m : \mathbb{Z}$, so dass $n \cdot \frac{p}{q} + m \cdot \frac{p'}{q'} = 0_{\mathbb{Q}}$.
- Folgern Sie daraus, dass wenn die abelsche Gruppe $\mathbb{Q}$ endlich erzeugt ist, dann jedes Erzeugendensystem für $\mathbb{Q}$ genau ein Element besitzt.
- Nehmen Sie an, dass ein $\frac{p}{q} : \mathbb{Q}$ existiert, mit $\mathbb{Z}\frac{p}{q} = \mathbb{Q}$ und erreichen Sie einen Widerspruch.

6.16. Übung 3

Sei G eine abelsche Gruppe. Zeigen Sie, dass für jedes $g : G$, die Familie $\{g\}$ genau dann frei ist, wenn g nicht ein Torsionselement von G ist.

6.17. Endlich erzeugte und torsionsfreie abelsche Gruppen

- Wir haben gerade gesehen, dass torsionsfreie abelsche Gruppen im Allgemeinen *nicht* frei sind.
- Allerdings gibt es für *endlich erzeugte* abelsche Gruppe das folgende Ergebnis.

> **Satz.** Sei G eine endliche erzeugte abelsche Gruppe, die außerdem torsionsfrei ist. Dann besitzt G eine endliche $\mathbb{Z}$-basis.

Beweis. Man startet mit einem Erzeugendensystem $(g_1, \ \dots \ , g_n)$ für G. Da G torsionsfrei ist, ist die Familie $\{g_1\}$ eine freie Familie. Es gibt deshalb eine wohldefinierte natürliche Zahl $k : \mathbb{N}_{>0}$ mit

$$k = \max\{1 \leqslant j \leqslant n \ / \ (g_1, \ \dots \ g_j) \text{ frei}\} \ .$$

Wir werden zeigen, dass $(g_1, \ \dots \ , g_k)$ eine $\mathbb{Z}$-Basis für G ist.

6.18. Folge vom Beweis, dass G eine Basis besitzt

- Sei $U := \langle g_1, \ \dots \ , g_k\rangle$. Per Konstruktion ist $(g_1, \ \dots \ , g_k)$ eine Basis für U. Wenn $k = n$, ist $(g_1, \ \dots \ , g_k)$ auch eine Basis für G.
- Nehmen wir jetzt an, dass $k < n$. Per Maximalität von k, ist, für jedes $i \in \{k + 1, \ \dots \ , n\}$, die Familie $(g_1, \ \dots \ , g_k, g_i)$ nicht frei. Das heißt, es gibt ganze Zahlen $\lambda_{i,1}$, $\dots$, $\lambda_{i,k}$, μ_i, nicht alle von ihnen null, so dass $\lambda_{i,1} \cdot g_1 + \ \dots \ + \lambda_{i,k} \cdot g_k + \mu_i \cdot g_i = 0_G$.
- Dann gilt $\mu_i \neq 0_{\mathbb{Z}}$. Weil, wenn $\mu_i = 0_{\mathbb{Z}}$, dann $\forall \ j \in \{1, \ \dots \ , k\}, \ \lambda_{i,j} = 0_{\mathbb{Z}}$.
- Sei $\mu := \mu_{k+1} \dots \mu_n$ und sie $\varphi : G \to G$ die durch $g \mapsto \mu \cdot g$ definierte Abbildung. Dann ist φ einen Gruppenhomomorphismus und setzen wir $\mu G := \text{Im } \varphi$.
- Beachten Sie, dass $\mu \cdot g_i = (\prod_{\ell \neq i} \mu_\ell) \cdot (\mu_i \cdot g_i) = -(\prod_{\ell \neq i} \mu_\ell) \cdot (\lambda_{i,1} \cdot g_1 + \ \dots \ + \lambda_{i,k} \cdot g_k)$ eine lineare Kombination von $(g_1, \ \dots \ , g_k)$ ist.

6.19. Ende vom Beweis, dass G eine Basis besitzt

- Da für alles $i \in \{s + 1, \ \dots \ , n\}$, $\mu \cdot g_i \in \langle g_1, \ \dots \ , g_k\rangle = U$ und $G = \langle g_1, \ \dots \ , g_n\rangle$, gilt $\mu G \subset U$.
- Da U endlich erzeugt und frei ist, ist μG auch endlich erzeugt und frei, als Untergruppe einer endlich erzeugten freien abelschen Gruppe.
- Da G torsionsfrei ist, ist die Abbildung $\varphi : g \mapsto \mu \cdot g$ injektiv. Sie induziert daher ein Gruppenisomorphismus $G \simeq \mu G$.
- Da μG eine endliche $\mathbb{Z}$-Basis hat, hat G auch eine endliche $\mathbb{Z}$-Basis. Dies beendet den Beweis.

6.20. Zerlegungssatz für endlich erzeugte abelsche Gruppen

- Der folgende Zerlegungssatz ist der letzte Schritt in der Klassifiezierung endlich erzeugter abelscher Gruppen.

  Satz. Sei G eine endlich erzeugte abelsche Gruppe und sei $\mathrm{Tor}(G)$ die Torsionsuntergruppe von G. Dann ist die Faktorgruppe $G/\mathrm{Tor}(G)$ eine endlich erzeugte freie abelsche Gruppe. Außerdem gibt es eine Untergruppe $F \preccurlyeq G$, sodass $F \simeq G/\mathrm{Tor}(G)$ und

  $$G = F \oplus \mathrm{Tor}(G) \ .$$

- Insbesondere „hat jede endlich erzeugte abelsche Gruppe G einen freien Teilen (mit endlichen Rang) $F \simeq \mathbb{Z}^r$ und einen Torsionsteilen $\mathrm{Tor}(G)$ (die endliche ist)".
- Aus diesem Satz und dem Satz über invariante Faktoren, folgt der Klassifikationssatz für endlich erzeugte abelsche Gruppen (siehe unten).

6.21. Beweis des Zerlegunssatzes

- Sei $\pi : G \to G/\mathrm{Tor}(G)$ die kanonische Projektion und sei $(g_1, \ \ldots \ , g_n)$ ein Erzeugendensystem für G. Da π surjektiv ist und $G = \langle g_1, \ \ldots \ , g_n \rangle$, gilt $G/\mathrm{Tor}(G) = \langle \pi(g_1), \ \ldots \ , \pi(g_n) \rangle$. Das heißt, die Gruppe $G/\mathrm{Tor}(G)$ ist endlich erzeugt.
- Da $G/\mathrm{Tor}(G)$ torsionsfrei ist, muss dann $G/\mathrm{Tor}(G)$ eine $\mathbb{Z}$-Basis $(h_1, \ \ldots \ , h_r)$ besitzen.
- Da π surjektiv ist, existiert, für jedes i, ein Element $g_i : G$ mit $\pi(g_i) = h_i$. Sei dann $\varphi : G/\mathrm{Tor}(G) \to G$ der eindeutige Gruppenhomomorphismus, die h_i nach g_i abbildet. **Übung:** ein solcher Gruppenhomomorphismus existiert und erfüllt $\pi \circ \varphi = id_{G/\mathrm{Tor(G)}}$.
- Sei $F := \langle g_1, \ \ldots \ , g_r \rangle \preccurlyeq G$. Wir werden beweisen, dass $F \simeq \mathbb{Z}^r$ ist und dass $F \oplus \mathrm{Tor}(G) = G$ gilt.

6.22. Ende vom Beweis des Zerlegunssatzes

- Da $\varphi : G/\mathrm{Tor}(G) \to G$ die Bedingung $\pi \circ \varphi = id_{G/\mathrm{Tor}(G)}$ erfüllt, ist φ injektiv. Da per Definition $F = \mathrm{Im}\ \varphi$, gilt $F \simeq G/\mathrm{Tor}(G) \simeq \mathbb{Z}^r$.
- Um $F \oplus \mathrm{Tor}(G) = G$ zu beweisen, reicht es $F \cap \mathrm{Tor}(G) = \{0_G\}$ und $F + \mathrm{Tor}(G) = G$ zu zeigen.
  - Sei $x \in F \cap \mathrm{Tor}(G)$. Dann gilt $x = \lambda_1 \cdot g_1 + \ \ldots \ + \lambda_r \cdot g_r$ für einzige $\lambda_1, \ldots, \lambda_r$ in $\mathbb{Z}$ und auch $\pi(x) = 0_{G/\mathrm{Tor}(G)}$. Daher gilt $\lambda_1 \cdot \pi(g_1) + \ \ldots \ + \lambda_r \cdot \pi(g_r) = 0_{G/\mathrm{Tor}(G)}$. Da $(\pi(g_i))_{1 \leqslant i \leqslant r} = (h_i)_{1 \leq i \leq r}$ eine freie Familie ist, muss jedes $\lambda_i = 0_{\mathbb{Z}}$. Somit $x = 0_G$.
  - Sei $x : G$. Schreiben wir $x = (x - \varphi(\pi(x))) + \varphi(\pi(x))$. Dann gilt $\varphi(\pi(x)) \in \mathrm{Im}\ \varphi = F$. Außerdem gilt $\pi(x - \varphi(\pi(x))) = \pi(x) - \underbrace{(\pi \circ \varphi)}_{= id_{G/\mathrm{Tor}(G)}}(\pi(x)) = 0_{G/\mathrm{Tor}(G)}$. Somit $(x - \varphi(\pi(x))) \in \mathrm{Ker}\ (\pi) = \mathrm{Tor}(G)$ und $x \in \mathrm{Tor}(G) + F$.

6.23. Normalform für endlich erzeugte abelsche Gruppen

- Der Zerlegungssatz für endlich erzeugte abelsche Gruppen wird oft wie folgt geschrieben: es gibt ein eindeutiges $r : \mathbb{N}_{\geq 0}$ und einen Gruppenisomorphismus

$$G \simeq \mathbb{Z}^r \times \mathrm{Tor}(G) \ .$$

- Die Gruppe $\mathrm{Tor}(G)$ ist eine endliche abelsche Gruppe. Nach dem Satz über invariante Faktoren, gibt es eine eindeutige endliche Folge natürlichen Zahlen $(d_1, \ \ldots \ , d_s)$, so dass die folgende Eigenschaften gelten:

  1. $\forall \ j \in \{1, \ \ldots \ s-1\}, \ d_{j+1} \mid d_j$.
  2. Es gibt einen Gruppenisomorphismus $\mathrm{Tor}(G) \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \ \ldots \ \times (\mathbb{Z}/d_s\mathbb{Z})$.

- Dann gibt einen Gruppensisomorphismus

$$G \simeq \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \ \ldots \ \times (\mathbb{Z}/d_s\mathbb{Z}).$$

6.24. Bemerkungen

- Sei G eine endlich erzeugte abelsche Gruppe und sei r die eindeutige natürliche Zahl mit $G \simeq \mathbb{Z}^r \times \mathrm{Tor}(G)$. Obwohl G im Allgemeinem nicht frei ist, wird die (wohldefiniert) natürliche Zahl r den Rang von G genannt.
- Anstelle von invarianten Faktoren kann man auch die Elementarteiler von G verwenden. In diesem Fall, schreibt man die endliche Gruppe $\mathrm{Tor}(G)$ als Produkt ihrer primären Anteile. Dann gibt es einen Gruppenisomorphismus

$$G \simeq \mathbb{Z}^r \times \prod_{i=1}^{k} (\mathbb{Z}/p_i^{m_{i,1}}\mathbb{Z}) \times \ \ldots \ \times (\mathbb{Z}/p_i^{m_{i,s_i}}\mathbb{Z})$$

  wobei $\prod_{i=1}^{k} p_i^{\alpha_i}$ die Primfaktorzerlegung von $|\mathrm{Tor}(G)|$ ist, und $m_{i,1} + \ \ldots \ + m_{i,s_i} = \alpha_i$ eine Partition von α_i ist.

6.25. Übung 4

Sei G eine Torsionsgruppe und sei H eine torsionsfreie abelsche Gruppe. Zeigen Sie, dass jeder Gruppenhomomorphismus $\varphi : G \to H$ ist null.