Einführung in die Algebra

Arthur Henninger

7. November 2024

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Grundbegriffe

Definition 1.1.1: (abelsche) Gruppe

Eine *Gruppe* ist eine Menge G zusammen mit einer Abbildung

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\mapsto a \cdot b = ab, \end{aligned}$$

sodass:

1) Assoziativität

$$\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

2) Existenz eines linksneutralen Elements:

$$\exists e \in G : \forall a \in G : e \cdot a = a.$$

3) Existenz von Linksinversen:

$$\forall a \in G \exists b \in G : b \cdot a = e.$$

Eine Gruppe G heißt *abelsch* oder *kommutativ*, wenn zusätzlich gilt:

4) Kommutativität:

$$\forall a, b \in G : a \cdot b = b \cdot a.$$

Notation 1.1.2

Wir schreiben $a \cdot b = ab$ und $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ mal}} \forall n \in \mathbb{N} \setminus \{0\}$ und falls G abelsch ist $a + b := a \cdot b, n \cdot a = a^n$

Lemma 1.1.3

Sei G eine Gruppe. Dann gilt

(1) $G \neq \emptyset$

(2) Linksinverse sind eindeutig und rechtsinvers, d.h.

$$\forall a, b, c \in G : ba = ca = e \implies b = c \text{ und } ab = e.$$

(3) Das linksneutrale Element ist eindeutig und rechtsneutral, d.h.

$$\forall e' \in G \text{ mit } e' \cdot a = a \forall a \in G \text{ gilt } e = e' \text{ und } a \cdot e = a \forall a \in G.$$

Beweis: (1) Da $e \in G$ ist $G \neq \emptyset$

(2) Seien $a, b \in G$ mit $ba = e$. Sei $a' \in G$ das Linksinverse zu b also $a'b = e$. Dann gilt

$$ab = eab = a' \underbrace{ba}_{e} b = a'eb = a'b = e.$$

Also ist b rechtsinvers zu a.
Sind $b, c \in G$ mit $ba = ca = e$. Dann gilt

$$c = ec = bac = be = bab = eb = b.$$

(3) Seien $a, b \in G$ mit $ba = ab = e$. Dann ist

$$ae = aba = ea = a.$$

Also ist e rechtsneutral.
Ist $e' \in G$ ein linksneutrales Element, dann gilt $e = e'e = e'$.

□

Notation 1.1.4

Für $a \in G$ schreiben wir a^{-1} für das Inverse (rechts- und links-) von a und $a^{-n} = (a^{-1})^n$. Wir nennen das (links- und rechts-) Neutrale Element $e \in G$ auch Einheit oder Eins.

Fakt 1.1.5

Analog zu 1.3:
Sei G eine Gruppe. Dann gilt

(1) $(a^{-1})^{-1} = a$

(2) $(ab)^{-1} = b^{-1}a^{-1}$

(3) Ist $ab = ac$, so ist $b = c$

(4) Ist $a^2 = a$, so ist $a = e$.

Definition 1.1.6: Untergruppe

Sei G eine Gruppe. Eine *Untergruppe* von G ist eine Teilmenge $H \subseteq G$ sodass

(1) $e \in H$

(2) $\forall a \in H$ ist $a^{-1} \in H$

(3) $\forall a, b \in H$ ist $ab \in H$.

Dann ist H mit $\cdot|_{H \times H}$ selbst eine Gruppe.

Bemerkung 1.1.7

Folgende Bedingung ist äquivalent zu denen der Definition: $\emptyset \neq H \subseteq G$ ist eine Untergruppe $\iff \forall a, b \in H : ab^{-1} \in H$.

Beweis: Offensichtlich erfüllen Untergruppen die Eigenschaft. Für die andere Implikation wähle $a \in H \implies e = aa^{-1} \in H$, also ist (1) erfüllt. Ist $a \in H$ beliebig, ist auch $a^{-1} = ea^{-1} \in H$, worduch (2) erfüllt ist. Schließlich ist für $a, b \in H$ auch $ab = a(b^{-1})^{-1} \in H$, wodurch (3) erfüllt ist. □

Definition 1.1.8: Gruppenhomomorphismus und Gruppenisomorphismus

Eine Abbildung $\varphi : G_1 \to G_2$ zwischen zwei Gruppen G_1 und G_2 heißt

1) *Gruppenhomomorphismus* (oder Homomorphismus oder Morphismus), falls

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in G_1.$$

2) *Gruppenisomorphismus* (oder Isomorphismus), falls φ ein bijektiver Homomorphismus ist.
G_1 und G_2 heißen dann isomorph und wir schreiben $G_1 \cong G_2$, falls ein Isomorphismus zwischen den Gruppen existiert.

Bemerkung 1.1.9

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(1) φ ist ein Isomorphismus

$$\iff \exists \psi : G_2 \to G_1 \text{ Hom.} \quad \text{mit } \varphi \circ \psi = \mathrm{Id}, \quad \varphi \circ \psi = \mathrm{Id}\,.$$

Denn: Die Existenz von ψ implziert, dass φ ein Isomorphismus ist. Umgekehrt kann man prüfen, dass für eine bijektive Abbildung φ auch die Umkehrabbildung $\psi := \varphi^{-1}$ ein Homomorphismus ist.

(2) $\varphi(e) = e$, denn mit Fakt 1.1.5 folgt:

$$\varphi(e)^2 = \varphi(e^2) = \varphi(e) \implies \varphi(e) = e.$$

(3) $\forall a \in G : \varphi(a^{-1}) = \varphi(a)^1$, denn

$$e = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}).$$

(4) φ ist injektiv $\iff \varphi^{-1}(e) = \{e\}$, denn:

$$\text{Für } a \neq b \in G_1 \text{ mit } \varphi(a) = \varphi(b) \text{ gilt } \varphi(\underbrace{ab^{-1}}_{\neq e}) = e \text{ aber } \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e.$$

Definition 1.1.10: Kern und Bild

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus.

(1) Der *Kern von* φ ist

$$\mathrm{Ker}(\varphi) = \{a \in G_1 : \varphi(a) = e\}\,.$$

(2) Das *Bild von* φ ist

$$\mathrm{Im}(\varphi) = \{b \in G_2 : \exists a \in G_1, \varphi(a) = b\}.$$

Aus Bemerkung 1.1.9 (4) folgt dann: φ injektiv $\iff \mathrm{Ker}(\varphi) = \{e\}$

Lemma 1.1.11

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann sind $\mathrm{Ker}(\varphi) \subseteq G_1, \mathrm{Im}(\varphi) \subseteq G_2$ Untergruppen.

Beweis: Klar ist $e \in \mathrm{Ker}(\varphi), e \in \mathrm{Im}(\varphi) \implies \mathrm{Ker}(\varphi), \mathrm{Im}(\varphi) \neq \emptyset$.
Für $a, b \in \mathrm{Ker}(\varphi)$ gilt:

$$\begin{aligned}\varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= ee^{-1} \\ &= e \\ &\implies ab^{-1} \in \mathrm{Ker}(\varphi).\end{aligned}$$

Für $c, d \in \mathrm{Im}(\varphi)$, wähle $a, b \in G_1$ mit $\varphi(a) = c, \varphi(b) = d$. Dann gilt

$$\begin{aligned}\varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= cd^{-1} \\ &\implies cd^{-1} \in \mathrm{Im}(\varphi).\end{aligned}$$

Folglich sind $\mathrm{Ker}(\varphi)$ und $\mathrm{Im}(\varphi)$ nach Bemerkung 1.1.7 Untergruppen. □

Beispiel 1.1.12

(1) Die triviale Gruppe ist $G = \{e\}$ mit der eindeutigen Abbildung

$$G \times G \to G.$$

Bis auf Isomorphie gibt es nur diese Gruppe mit einem Element.

(2) Sind G_1 und G_2 Gruppen, so ist $G = G_1 \times G_2$ mit komponentenweiser Gruppenstruktur

$$\begin{aligned}G \times G &\to G \\ (a_1, a_2), (b_1, b_2) &\mapsto (a_1 b_1, a_2 b_2)\end{aligned}$$

eine Gruppe. Sind G_1, G_2 abelsch, dann schreiben wir

$$G_1 \oplus G_2 := G_1 \times G_2.$$

(3) Ist K ein Körper, so sind

$$(K, +) \text{ und } (K \setminus \{0\}, \cdot)$$

Gruppen.

(4) Die Paare $(\mathbb{N}, +), (\mathbb{Z} \setminus \{0\}, \cdot)$ sind jeweils keine Gruppen, sondern sogenannte Monoide da lediglich Inverse fehlen.

(5) Für jede Menge M ist

$$\mathrm{Bij}(M) := \{f : M \to M | f \text{ bijektiv }\}$$

mit Komposition als Verknüpfung eine Gruppe.

(6) Die symmetrische Gruppe aus n Elementen ist

$$S_n := \mathcal{S}_n := \mathrm{Bij}(\{1, \dots, n\}).$$

.

(7) Die Abbildung

$$\mathrm{sgn} : S_n \to \{\pm 1\}$$

ist ein Homomorphismus. Die alternierende Gruppe auf n Elementen ist

$$A_n := \mathrm{Ker}(\mathrm{sgn}) \subseteq S_n.$$

(8) Die linearen Gruppen $GL_n(K), SL_n(K), O_n(K), SO_n(K), U_n(K)$, etc. sind Gruppen (wobei teilweise nicht jeder Körper die Grundlage für die Gruppen bilden kann oder Skalarprodukte existieren müssen).

(9) Ist K ein Körper, so ist die Automorphismengruppe von K

$$\mathrm{Aut}(K) = \{\varphi : K \to K : \varphi \in \mathrm{Bij}(K), \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in K\}$$

eine Gruppe. Die Abbildungen $\varphi : K \to K$ heißen Körperautomorphismen.

(10) Allgemeiner: Ist $\mathcal{C}$ eine Kategorie, sodass $\forall A, B \in \mathrm{Ob}(\mathcal{C})$ die Abbildungen zwischen A und B eine Menge $\mathrm{Hom}_{\mathcal{C}}(A, B)$ bilden. Dann ist für jedes $A \in \mathcal{C}$

$$\mathrm{Aut}_{\mathcal{C}}(A) = \{\varphi : A \to A : \varphi \text{ invertierbar}\} \subseteq \mathrm{Hom}(A, A)$$

eine Gruppe via Komposition. Spezialfälle sind

- $\mathrm{Bij}(M)$ mit $\mathcal{C}$ = Mengen
- $\mathrm{Gl}_n(M)$ mit $\mathcal{C}$ = endlich dimensionale Vektorräume
- $\mathrm{Aut}(M)$ mit $\mathcal{C}$ = Körper

(11) Sei M eine Menge

- Ein Wort w über M ist eine Sequenz

$$m_1^{n_1} \cdot \ldots \cdot m_k^{n_k} \text{ mit } m \in M \text{ und } n_i \in \mathbb{Z}.$$

- Das leere Wort ist die leere Sequenz.
- Ein Wort w heißt reduziert, falls $m_i = m_{i+1}$ für alle i.
- Jedes Wort w über M kann via $m^n m^{n'} \rightsquigarrow m^{n+n'}$ reduziert werden.

$$\begin{aligned} abba &\rightsquigarrow ab^2a \\ b^0 &\rightsquigarrow - \\ aa^{-1} &\rightsquigarrow -. \end{aligned}$$

Die Menge F_M aller reduzierten Wörter über M mit "Hintereinanderschreiben & reduzierenïst eine Gruppe, die freie Gruppe über M. Es ist $F_{\{1,\dots,n\}} =: F_n \cong \mathbb{Z}$ durch $a^n \mapsto n$.
Ist $M \subseteq G$ eine Teilmenge einer Gruppe G, so ist

$$\begin{aligned} \varphi_M : F_M &\to G \\ m_1^{n_1} \dots m_k^{n_k} &\mapsto m_1^{n_1} \cdot \ldots \cdot m_k^{n_k} \end{aligned}$$

ein Homomorphismus und wir können M zur Definition der Erzeuger nutzen.

Definition 1.1.13: erzeugte Untergruppe

Sei G eine Gruppe, $M \subseteq G$ Teilmenge. Die *von M erzeugte Untergruppe von G* ist

$$\langle M \rangle := \operatorname{Im} \varphi_M.$$

Ist $\langle M \rangle = G$, so sagen wir, dass M G erzeugt.

Definition 1.1.14: endlich erzeugte Gruppe, zyklische Gruppe

Sei G eine Gruppe.

(1) G heißt *endlich erzeugt*, wenn sie von einer endlichen Teilmenge erzeugt wird.

(2) G heißt *zyklisch*, wenn G von einem Element erzeugt wird.

Beispiel 1.1.15 (zyklische Gruppen)

Ist $|M| = 1$, dann ist $F_M \cong \mathbb{Z}$. $\rightsquigarrow$ Ist G zyklisch, so $\exists \varphi : \mathbb{Z} \to G$ surjektiver Homomorphismus.
$\implies$ G ist abelsch. Setze $1 = \varphi(1)$ (abhängig von φ, i.A. nicht das neutrale Element). Nun sind zwei Fälle zu unterscheiden:

(1)

$$\nexists 0 \neq m \in \mathbb{Z} \text{ mit } m \cdot 1 = 0 \in G \iff \varphi \text{ injektiv} \iff \varphi \text{ Isomorphismus und daher } G \cong \mathbb{Z}.$$

(2) $\exists 0 \neq m \in \mathbb{Z}$ mit $m \cdot 1 = 0$. Sei $m > 0$ minimal mit dieser Eigenschaft. Definiere:

$$C_m := \mathbb{Z}/m\mathbb{Z} := \{0, \dots, m-1\}.$$

mit der Verknüpfung

$$ab = a + b \mod m.$$

Dann ist

$$\begin{aligned} C_m &\to G \\ n &\mapsto n \cdot 1. \end{aligned}$$

Ein Isomorphismus $\implies \mathbb{Z}/m\mathbb{Z} \cong G$.

- Untergruppen: Ist $H \subseteq \mathbb{Z}$ eine Untergruppe, so $\exists n \in \mathbb{Z}$ mit $H = n\mathbb{Z}$ (Beweis via Division mit Rest).
- Ist $H \subseteq \mathbb{Z}/m\mathbb{Z}$, so ist auch $\varphi^{-1}(H) \subseteq \mathbb{Z}$ eine Untergruppe, also $\exists n \in \mathbb{Z}$ mit $H = n(\mathbb{Z}/m\mathbb{Z})$.
- kleine Übung: Für $n \neq 0$ gilt $n\mathbb{Z} \cong \mathbb{Z}$ und $(n(\mathbb{Z}/m\mathbb{Z})) \cong \mathbb{Z}/\left(\frac{m}{\operatorname{ggT}(n,m)}\right)\mathbb{Z}$.
  $\implies$ Untergruppen zyklischer Gruppen sind wieder zylkisch.

Definition 1.1.16: Ordnung von Gruppen und Elementen

Sei G eine Gruppe.

(1) Die *Ordnung von G* ist die Kardinalität der Menge G.

(2) Die *Ordnung von $a \in G$* ist

$$\operatorname{ord}(a) := |a| := \min\{n \in \mathbb{N} | a^n = e\}.$$

Wir können die Ordnung des Erzeugers nutzen, um $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ fundamental zu unterscheiden.

1.2 Normalteiler und Quotienten

Für Vektorräume betrachtet man Unterräume $W \subseteq V$ und Quotienten V/W. Hier wollen wir nun analog Quotienten von Gruppen definieren und studieren.

Definition 1.2.1: Nebenklassen

Sei $H \subseteq G$ eine Untergruppe.

(1) Die *Linksnebenklasse von H nach a* ist

$$aH := \{ab | b \in H\} \subseteq G.$$

Für $a \in H$ ist $aH = H$ wegen $aa^{-1}b = b$. (vgl. mit $v + W \subseteq V$ für UVR $W \subseteq V, v \in V$)

(2) Die *Rechtsnebenklasse von H nach a* ist

$$Ha = \{ba | b \in H\} \subseteq G.$$

(3) Die zu H via a *konjugierte Untergruppe* ist

$$aHa^{-1} = \left\{aba^{-1} | b \in H\right\} \subseteq G.$$

(4) Wir definieren G/H bzw. $H\backslash G$ als die Menge der Links- bzw. Rechtsnebenklassen von H

$$G/H = \{\text{Linksnebenklassen von } H \, \forall a \in G\}$$
$$H\backslash G = \{\text{Rechtsnebenklassen von } H \, \forall a \in G\}.$$

Der *Index* von H in G ist

$$(G : H) := |G/H|.$$

Naiv: $(aH, a'H) \mapsto aa'H$

Bemerkung 1.2.2

(1) Für jede Teilmenge $M \subseteq G$ und alle $a \in G$ sind

$$a\cdot : M \to aM$$
$$\cdot a : M \to Ma$$

Bijektionen, wobei aM analog zu aH definiert ist.

(2) Erinnerung: $aH = H$ für $a \in H \subseteq G$ Untergruppe. Allgemeiner:
Für $a, b \in G$ äquivalent:

(a) $aH = bH$
(b) $\exists c \in H$ mit $a = bc$
(c) $aH \cap bH \neq \emptyset$
(d) $b^{-1}a \in H$

Zwei Linksnebenklassen sind daher entweder gleich oder disjunkt.

(3) Analoge Kriterien gehlten für $Ha = Hb$.

(4) Nach (2) gilt (nach (1) ist $|aH| = |H|$)

$$G = \dot{\bigcup}_{aH \in G/H} aH.$$

Insbesondere: Ist G endlich, so ist $|G| = |H|\,(G : H) \implies |H| \mid |G|$ ($|H|$ teilt $|G|$)

Beweis von (2):

$$\begin{aligned} aH = bH &\implies \exists c \in H \text{ mit } a = ae = bc \\ &\implies aH \cap bH \neq \emptyset (\text{denn } a \in aH \cap bH) \\ &\implies \exists c, d \in H \text{ mit } ac = bd \\ &\implies b^{-1}a \in H (\text{denn } b^{-1}a = dc^{-1} \in H) \\ &\implies b^{-1}aH = H \\ &\implies bH = bb^{-1}aH = aH. \qquad \text{(Mult. ist Bijektion)} \end{aligned}$$

□

Nicht für jede Untergruppe $H \subseteq G$ trägt G/H eine offensichtliche Gruppenstruktur. Zu verstehen, wann dies der Fall ist, führt zum Begriff des Normalteilers.

Definition 1.2.3: Normalteiler

Eine Untergruppe $H \subseteq G$ heißt *Normalteiler* (*normale Untergruppe*, *normal* in G), wenn $aHa^{-1} = H \, \forall a \in G$. Wir schreiben $H \triangleleft G$.

Lemma 1.2.4

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann ist $\operatorname{Ker}(\varphi) \subseteq G_1$ normal.
Wir werden später sehen, dass dieses Beispiel für eine normale Untergruppe universell ist.

Beweis: $\operatorname{Ker}(\varphi) \subseteq G_1$ ist Untergruppe. Sei $b \in \operatorname{Ker}(\varphi), a \in G_1$. Dann ist

$$\begin{aligned} \varphi(aba^{-1}) = \varphi(a) \underbrace{\varphi(b)}_{=e} \varphi(a)^{-1} = e \\ \implies aba^{-1} \in \operatorname{Ker}(\varphi) \\ \implies a \operatorname{Ker}(\varphi) a^{-1} \subseteq \operatorname{Ker}(\varphi). \end{aligned}$$

Da $\operatorname{Ker}(\varphi) \supseteq a \operatorname{Ker}(\varphi) a^{-1}$ folgt die Gleichheit. □

Bemerkung 1.2.5

Im Gegensatz zum Kern ist das Bild eines Homomorphismus im Allgemeinen nicht normal. Für diese Feststellung genügt es, eine nicht-normale Untergruppe einer Gruppe zu finden (die Untergruppe ist dann das Bild der Inklusion). Beispielsweise ist

$$\langle (1 \quad 2) \rangle \subseteq S_3$$

nicht normal, denn

$$(1 \quad 2 \quad 3)(1 \quad 2)(3 \quad 2 \quad 1) = (2 \quad 3) \notin \langle (1 \quad 2) \rangle.$$

Lemma 1.2.6

Sei $H \subseteq G$ eine Untergruppe. Dann sind äquivalent:

(1) H ist normal in G

(2) $aH = Ha \, \forall a \in G$

(3) Die Abbildung

$$\begin{aligned} \cdot : G/H \times G/H &\to G/H \\ (aH, bH) &\mapsto abH \end{aligned}$$

ist wohldefiniert.

Beweis:

- (1) $\iff$ (2). Nach Bemerkung 1.2.2 (1) gilt

$$aHa^{-1} = H \iff aH = Ha.$$

- (1) $\iff$ (3). Die Abbildung in (3) ist nach 1.2.2 ist wohldefiniert

$$\iff \forall a, b \in G, \forall c, d \in H : \cdot(acH, bdH) = acbdH = abH = \cdot(aH, bH).$$

Das gilt nach 1.2.2 (2) genau dann, wenn

$$(ab)^{-1}acbd = b^{-1}a^{-1}acbd = b^{-1}cbd \in H.$$

Also genau dann, wenn

$$b^{-1}cb \in Hd^{-1} = H \iff H \text{ normal, da } b \in G, c \in H \text{ beliebig.}$$

□

Lemma 1.2.7

Sei $H \triangleleft G$ normale Untergruppe. Die Menge G/H mit

$$\begin{aligned} \cdot : G/H \times G/H &\to G/H \\ (aH, bH) &\mapsto abH \end{aligned}$$

ist eine Gruppe. Wir nennen diese Gruppe den Quotient von G nach H.

Beweis: Für $a, b, c \in G$ gilt

$$\begin{aligned} (aHbH)cH = (abH)cH = (ab)cH = a(bc)H = aH(bc)H = aH(bHcH) \\ aHa^{-1}H = aa^{-1}H = eH = H \\ eHaH = eaH = aH. \end{aligned}$$

□

Bemerkung 1.2.8

Sei $H \triangleleft G$ eine normale Untergruppe.

(1) Die Quotientenabbildung

$$\begin{aligned} \pi : G &\to G/H \\ a &\mapsto aH \end{aligned}$$

ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\pi) = H$ (nach Bemerkung 1.2.2 (2) bzw. weil $aH = H \iff a \in H$).

(2) Definieren wir analog eine Gruppenstruktur auf $H\backslash G$ via

$$\begin{aligned} H\backslash G \times H\backslash G &\to H\backslash G \\ (Ha, Hb) &\mapsto Hab, \end{aligned}$$

so ist

$$\begin{aligned} \varphi : G/H &\to H\backslash G \\ aH &\mapsto Ha \end{aligned}$$

ein Gruppenisomorphismus (es reicht, G/H zu betrachten). Nach Lemma 1.2.6 ist φ eine Bijektion und es gilt

$$\varphi(abH) = Hab = \varphi(aH)\varphi(bH).$$

Für Normalteiler müssen wir also, sogar für die Gruppenstruktur auf dem Quotienten nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

Theorem 1.2.9

Sei $H \subseteq G$ eine Untergruppe. Dann sind äquivalent

(1) H ist normal in G.

(2) Es existiert ein Gruppenhomomorphismus $\varphi : G \to G'$ mit $H = \mathrm{Ker}(\varphi)$.

Beweis: • (1) $\implies$ (2): Nach Bemerkung 1.2.8 (1) können wir für φ die Quotientenabbildung $G \to G/H$ nehmen. Dann ist $H = \mathrm{Ker}(G \to G/H = G')$

• (2) $\implies$ (1): Es reicht zu sehen, dass $\mathrm{Ker}(\varphi)$ normal ist. Das ist Lemma 1.2.4.

□

Theorem 1.2.10 Satz von Lagrange

Sei G endliche Gruppe.

(1) Für jede UG $H \subseteq G$ gilt $|H| \mid |G|$.

(2) Für alle $a \in G$ gilt $\mathrm{ord}(a) \mid |G|$.

(3) Für alle $a \in G$ gilt $a^{|G|} = e$.

Beweis: (1) Das Folgt direkt aus Bemerkung 1.2.2 (4).

(2) Folgt aus (1) angewendet auf $\langle a \rangle \subseteq G$.

(3) Folgt aus (2), da $a^{|G|} = (a^{\mathrm{ord}(a)})^{\frac{|G|}{\mathrm{ord}(a)}}$.

□

Korollar 1.2.11

Sei G eine Gruppe mit $|G| = p$ prim. Dann ist G zyklisch.

Beweis: Wähle $a \in G, a \neq e \implies \mathrm{ord}(a) > 1$. Mit Lagrange folgt: $\mathrm{ord}(a) = p \implies \langle a \rangle = G$ □

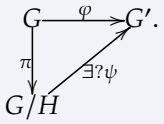
Theorem 1.2.12 Homomorphiesatz

Sei $H \triangleleft G$ normale UG. Sei $\pi : G \to G/H$ die Quotientenabbildung. Sei $\varphi : G \to G'$ ein Homomorphismus. Dann sind äquivalent

(1) φ faktorisiert durch π, d.h.. $\exists$ Homomorphismus $\psi : G/H \to G'$ mit $\varphi = \psi \circ \pi$

(2) $H \subseteq \mathrm{Ker}(\varphi)$

Wir nennen diese Äquivalenz die universelle Eigenschaft Wir fragten uns:



Wann gibt es ψ?

Beweis: • (1) $\implies$ (2): $\forall a \in H$:

$$\begin{aligned} a \in H &\implies \varphi(a) = (\psi \circ \pi)(a) = \psi(\pi(a)) = \psi(e) = e \\ &\implies a \in \mathrm{Ker}(\rho). \end{aligned}$$

- (2) $\implies$ (1): Definiere:

$$\begin{aligned}\psi : G/H &\to G' \\ aH &\mapsto \varphi(a).\end{aligned}$$

Wir müssen zeigen: ψ ist wohldefiniert (falls ja, dann offensichtlich ein Homomorphismus). Sei also $b \in G$ mit $aH = bH$. Dann ist $b^{-1}a \in H$ und $a^{-1}b \in H \subseteq \mathrm{Ker}(\rho)$ (Bemerkung 1.2.2). Also gilt

$$\varphi(a) = \varphi(a) \cdot \varphi(a^{-1}b) = \varphi(aa^{-1}b) = \varphi(b).$$

Es folgt nach Definition $\implies \psi(aH) = \psi(bH)$

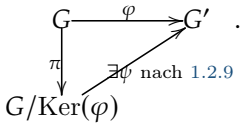
□

Korollar 1.2.13

Jeder surjektive Homomorphismus $\varphi : G \to G'$ induziert einen Isomorphismus

$$\psi : G/\mathrm{Ker}(\varphi) \xrightarrow{\sim} G'.$$

Beweis: In 1.2.9 setze $H = \mathrm{Ker}(\varphi)$.



φ surjektiv $\implies \psi$ surjektiv, φ injektiv: Es gilt

$$\psi(aH) = e \iff \varphi(a) = e \iff a \in \mathrm{Ker}(\rho) = H \iff aH = H.$$

□

Korollar 1.2.14 Erster Isomorphiesatz

G Gruppe, $H \subseteq G$ Untergruppe, $N \triangleleft G$ normale Untergruppe. Dann

(1) $HN := \langle H, N\rangle = \{ab | a \in H, b \in N\} \subseteq G$

(2) $N \triangleleft HN$

(3) $H \cap N \triangleleft H$

(4) Der Homomorphismus

$$\varphi : H \xrightarrow{\varphi_1} HN \xrightarrow{\varphi_2} HN/N$$

induziert einen Isomorphismus

$$H/H \cap N \cong HN/N.$$

Dabei ist φ_1 die Inklusion und φ_2 die Projektion/Quotientenabbildung.

Bemerkung 1.2.15

Vergleiche: Sind $V_1, V_2 \subseteq V$ Untervektorräume, so gilt $V_1/V_1 \cap V_2 \cong (V_1 + V_2)/V_2$

Beweis von 1.2.14: (1) Nach Definition gilt

$$\langle H, N\rangle = \left\{a_1^{m_1} b_1^{n_1} \dots a_k^{m_k} b_k^{n_k} | a_i \in H, b_i \in N, m_i, n_i \in \mathbb{Z}\right\}.$$

Da $N \triangleleft G$ normal ist, gilt

$$a_i b_i = b_i' a_i' \qquad (a_i b_i a_i^{-1} \in N)$$

.

$\implies \exists a \in H, b \in N$

$$a_1^{m_1} b_1^{n_1} \dots a_k^{m_k} b_k^{n_k} = ab.$$

(2) Klar, da $N \triangleleft G$

(3)+(4) Nach 1.2.13 reicht es zu zeigen: φ surjektiv mit $\operatorname{Ker}(\varphi) = H \cap N$.
Da $H \overset{\varphi_1}{\subseteq} HN$ gilt

$$\operatorname{Ker}(\varphi) = H \cap \underbrace{\operatorname{Ker}(HN \to HN/N)}_{=N \text{ nach } 1.2.8} = H \cap N.$$

Jedes Element in HN/N lässt sich schreiben als abN mit $a \in H, b \in N$. Es ist $abN = aN = \varphi(a)$ (da $b \in N$)
$\implies \varphi$ surjektiv.

□

Korollar 1.2.16 zweiter Isomorphiesatz

G Gruppe, $H, N \triangleleft G$ normale Untergruppe, $N \subseteq H$. Dann gilt

(1) $H/N \triangleleft G/N$

(2) Die Abbildung

$$\varphi : G \overset{\pi}{\to} G/N \overset{\pi'}{\to} (G/H)/(H/N)$$

induziert einen Isomorphismus

$$G/H \cong (G/N)/(H/N).$$

Beweis: (1) Nach Definition: $H/N \subseteq G/N$. Sei $aN \in H/N, bN \in G/N$

$$(bN) \cdot (aN) \cdot (bN)^{-1} = bab^{-1}N \in H/N \implies H/N \triangleleft G/N.$$

(2) φ surjektiv, da π und π' surjektiv

$$\begin{aligned} \operatorname{Ker}(\varphi) &= \pi^{-1}(\operatorname{Ker}(\pi')) \\ &= \pi^{-1}(H/N) \\ &= H. \end{aligned}$$

□

Bemerkung 1.2.17

Vergleiche: Sind $V_1, V_2 \subseteq V$ UVR mit $V_2 \subseteq V_1$, dann gilt

$$V/V_1 = (V/V_2)/(V_1/V_2).$$

Korollar 1.2.18

Für jede Gruppe G gibt es Mengen M und M' und einen Homomorphismus

$$\varphi \to F_{M'}, \text{ sodass } \operatorname{Im}(\varphi) \subseteq F_{M'} \text{ normal und } G \cong F_{M'}/\operatorname{Im}(\varphi).$$

Beweis: Wähle Erzeuger $M' \subseteq G \rightsquigarrow \exists$ Surjektion $\varphi_{M'} : F_{M'} \to G$. Wähle Erzeuger $M \subseteq \operatorname{Ker}(\varphi_{M'}) \rightsquigarrow \exists$ Homomorphismus $\varphi : F_M \to \operatorname{Ker}(\varphi_{M'}) \to F_{M'}$ mit erster Abbildung surjektiv. Nach Konstruktion gilt

$$\operatorname{Im}(\varphi) = \operatorname{Ker}(\varphi_{M'}).$$

Nach 1.2.13

$$F_{M'}/\operatorname{Im}(\varphi) = F_{M'}/\operatorname{Ker}(\varphi_{M'}) \cong G.$$

□

Lemma 1.2.19

Sei $M \subseteq G$ eine Teilmenge einer Gruppe G. Dann $\exists$ eine kleineste normale Untergruppe $N \subseteq G$ mit $M \subseteq N$. N heißt *normaler Abschluss von* M.

Beweis: Man setzt

$$N := \bigcap_{M \subseteq N' \trianglelefteq G} N'.$$

N ist dann normal als Schnitt normaler Untergruppen. □

Definition 1.2.20: Gruppe aus Erzeugern und Relationen

Sei M eine Menge und $M' \subseteq F_M$ eine Teilmenge. *Die Gruppe mit Erzeugern M und Relationen M'.* ist definiert als

$$\langle M | M' \rangle = F_M/N,$$

wobei N der normale Abschluss von M' in N ist.

Korollar 1.2.21

Jede Gruppe ist isomorph zu einer Gruppe der Form

$$\langle M | M' \rangle .$$

Beispiel 1.2.22

1) Zyklische Gruppen sind von der Form

$$\langle a | a^m \rangle .$$

   i) $\mathbb{Z} \cong \langle a | \emptyset \rangle$
   ii) $\mathbb{Z}/m\mathbb{Z} \cong \langle a | a^m \rangle$.

   Man schreibt auch $\langle a | a^m = e \rangle$

2) Dyadische Symmsteriegruppe von dyadischen Quadern. Sie wird erzeugt durch

   - Rotation R um $90°$
   - Spiegelung S

Also ist

$$\rightsquigarrow D_4 = \left\langle R, S | R^4 = S^2 = \mathrm{Id}, SRS = R^{-1} \right\rangle.$$

Hier ist $m' = \left\{R^4, S^2, SRSR\right\}$

3)

$$\langle a | \emptyset \rangle := F_1 / \langle e \rangle \cong F_1 \cong \mathbb{Z} \quad (a^n \mapsto n).$$

1.3 Gruppenoperationen

Definition 1.3.1: Gruppenoperation

Sei G eine Gruppe und X eine Menge. Eine *Operation* (oder *Aktion* oder *Wirkung*) von G auf X ist eine Abbildung

$$\begin{aligned} \rho : G \times X &\to X \\ (a, x) &\mapsto ax =: \rho(a, x), \end{aligned}$$

sodass

(1) $ex = x \; \forall x \in X$

(2) $a(bx)) = (ab)x \; \forall a, b \in G, x \in X$

Bemerkung 1.3.2

$\rho : G \times X \to X$ ist eine Operation $\iff G \to \mathrm{Bij}(X), a \mapsto (x \mapsto ax)$ ist ein Homomorphismus

Standardbeispuel: S_n-Operationen auf $\{1, \ldots, n\} \hat{=} \mathrm{Id} : S_n \to S_n = \mathrm{Bij}(\{1, \ldots, n\})$

$$\rho(\begin{pmatrix} i & j \end{pmatrix}, i) = j.$$

- $S_n 1 = \{1, \ldots, n\}$
- $\mathrm{Stab}(1) \cong S_{n-1}$

Frage 1

Wie operiert die Dyedergruppe auf den Ecken $\{1, 2, 3, 4\}$ des Quadrats? (Untergruppe von S_4???)

Definition 1.3.3: Orbit, Stabilisator

Sei $\rho : G \times X \to X$ eine Operation einer Gruppe G auf einer Menge X. Sei $x \in X$

(1) Der *Orbit* (oder die *Bahn*) von x (unter ρ) ist

$$G \cdot x = \{ax | a \in G\} \subseteq X.$$

(2) Der *Stabilisator* von x (unter ρ) ist

$$G_x := \mathrm{Stab}_G(x) := \mathrm{Stab}(x) = \{a \in G | ax = x\} \subseteq G.$$

Intuitiv ist, dass Gx ist nicht größer als G sein kann.

Theorem 1.3.4 Orbit-Stabilisator-Theorem

Sei $\rho : G \times X \to X$ eine Operation, $x \in X$

(1) $\mathrm{Stab}(x) \subseteq G$ ist eine UG

(2) Die *Orbitabbildung*

$$\begin{aligned} o_x : G &\to Gx \\ a &\mapsto ax \end{aligned}$$

induziert eine Bijektion zwischen den Linksnebenklassen

$$G/\mathrm{Stab}(x) \cong Gx.$$

(3) Ist $|G| < \infty$, so gilt

$$|G| = |Gx| \cdot |\mathrm{Stab}(x)|\,.$$

(4) Für $x \in X$ gilt

$$Gx \cap Gy \neq \emptyset \iff Gx = Gy \quad \rightsquigarrow X = \dot{\bigcup_{o \text{ Orbits}}} o = \dot{\bigcup_{o \in \{G\cdot x \mid x \in X\}}} o.$$

(5) Ist $Gx = Gy$, dann sind $\mathrm{Stab}(x)$ und $\mathrm{Stab}(y)$ konjugiert. ($H, H' \subset G$ UG heißen konjugiert, falls $\exists\, a \in G : aHa^{-1} = H'$)

Beweis: (1) $e \in \mathrm{Stab}(x)$. Sind $a, b \in \mathrm{Stab}(x)$, so gilt

$$ab^{-1}x = ab^{-1}ab^{-1}bx = ax = x \implies ab^{-1} \in \mathrm{Stab}(x) \implies \mathrm{Stab}(x) \text{ ist UG.}$$

(2) Für $a, b \in G$ gilt

$$\begin{aligned} ax = bx &\iff b^{-1}ax = x \\ &\iff b^{-1}a \in \mathrm{Stab}(a) \\ &\overset{??}{\iff} a\,\mathrm{Stab}(x) = b\,\mathrm{Stab}(x) \\ &\implies o_x^{-1}(ax) = a\,\mathrm{Stab}(x). \end{aligned}$$

Da o_x surjektiv ist, gilt (2)

(3) Nach 1.2.2 gilt:

$$|G| = |\mathrm{Stab}(x)| \cdot \underbrace{(G : \mathrm{Stab}(x))}_{=|G/\mathrm{Stab}(x)|=|Gx|}.$$

(4) $Gy = Gx \iff Gx \cap Gy \neq \emptyset$ Umgekehrt: Sei

$$\begin{aligned} z \in Gx \cap Gy &\implies \exists\, a, b \in G : ax = z = by \\ &\implies y = b^{-1}ax \in Gx \implies Gy \subseteq Gx. \end{aligned}$$

Analog: $Gx \subseteq Gy$.

(5) Ist $Gx = Gy$ so $\exists\, a \in G$ mit $y = ax$. Sei $b \in \mathrm{Stab}(x)$. Dann gilt

$$aba^{-1}y = abx = ax = y.$$

Also $\implies a\,\mathrm{Stab}(x)a^{-1} \subseteq \mathrm{Stab}(y)$. Analog $a^{-1}\,\mathrm{Stab}(y)a \subseteq \mathrm{Stab}(x) \implies \mathrm{Stab}(y) = a\,\mathrm{Stab}(x)a^{-1}$.

□

Theorem 1.3.5 Bahngleichung

Sei $\rho : G \times X \to X$ eine Operation einer endlichen Gruppe G auf einer endlichen Menge X. Sei $x_1, \dots, x_n \in X$ ein Repräsentantensystem der Orbits (d.h. $\forall$ Orbits $o \exists! \, x_i \in \{x_1, \dots, x_n\}$, sodass $x_i \in o$). Dann gilt

$$\begin{aligned} |X| &= \sum_{i=1}^{n} |Gx_i| \\ &= \sum_{i=1}^{n} |G : \mathrm{Stab}(x_i)| \, . \end{aligned}$$

Definition 1.3.6: frei, transitiv, treu

Sei $\rho : G \times X \to X$ eine Operation

(1) ρ heißt *frei*, falls $\mathrm{Stab}(x) = \{e\}$ $\forall x \in X$

(2) ρ heißt *transitiv*, falls $Gx = X \, \forall x \in X$

(3) Der *Kern* von ρ ist

$$\mathrm{Ker}(\rho) = \bigcap_{x \in X} \mathrm{Stab}(x) = \{a \in G | ax = x \, \forall x \in X\} \, .$$

(4) ρ heißt *treu*, wenn $\mathrm{Ker}(\rho) = \{e\}$.

Beispiel 1.3.7

Zu einer Gruppe G gibt es (mindestens) drei natürliche assoziierte Operationen

(1) Die Gruppenstruktur $\cdot : G \times G \to G$ definiert eine Operation von G auf sich selbst.

- $\cdot$ ist transitiv, denn $(ba^{-1})a = b$, frei denn $ab = b \implies a = e$ und damit auch treu (es ist stets $a, b \in G$)
- Beobachtung: Ist $|G| < \infty$, so ist G eine "transitive" UG von $S_{|G|}$.

(2) Die Abbildung

$$\begin{aligned} G \times G &\to G \\ (a, b) &\mapsto ba^{-1} \end{aligned}$$

ist auch eine freie, transitive und treue Operation. Achtung: $(a, b) \mapsto ba$ ist im Allgemeinen keine Operation.

(3) Die Konjugationsabbildung

$$\begin{aligned} \rho : G \times G &\to G \\ (a, b) &\mapsto aba^{-1} \end{aligned}$$

ist eine Operation. Für $b \in G$:

$$\mathrm{Stab}_G(b) = \left\{a \in G | aba^{-1} = b\right\} = Z(b) \text{ und } \mathrm{Ker}(\rho) = Z(G).$$

(4) Ist S die Menge der Untergruppen von G, so ist

$$\begin{aligned} \rho : G \times S &\to S \\ (a, H) &\mapsto aHa^{-1} \end{aligned}$$

eine Operation.

$$N(H) := \mathrm{Stab}(H) = \left\{a \in G | aHa^{-1} = H\right\}.$$

Normalisator von H in G.

Beobachtung: $N(H) \subseteq G$ ist die größte UG mit $H \triangleleft N(H) \rightsquigarrow H \subseteq G$ ist normal $\iff N(H) = G$

Beispiel 1.3.8

Ist $H \subseteq G$ eine UG, so ist

$$\begin{aligned} H \times G &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

eine H-Operation. Die ρ-Orbits sind genau die Rechtsnebenklassen von H in G.

Notation 1.3.9

Sei $\rho : G \times X \to X$ eine Operation. Wir schreiben $G\backslash X$ für die Menge der G-Orbits.

Korollar 1.3.10

Sei G eine endliche Gruppe, $a_1, \ldots, a_n \in G - Z(G)$ ein Repreäsentantensystem der Konjugationsoperation auf $G - Z(G)$. Dann gilt

$$|G| = \underbrace{|Z(G)|}_{1-\text{elementige Orbits}} + \sum_{i=1}^{n} (G : Z(a_i)).$$

Beweis: Bahnengleichung angewendet auf Konjugation. □

1.4 Sylow-Sätze

Definition 1.4.1: p-Gruppen, p-Sylow-Untergruppe

Sei G eine endliche Gruppe, p Primzahl, $|G| = p^n m$ mit $p \nmid m$

(1) G heißt *p-Gruppe*, wenn $m = 1$

(2) Eine UG $H \subseteq G$ heißt *p-Sylow-Untergruppe*, wenn $|H| = p^n$

Theorem 1.4.2 Sylow-Sätze

Sei G wie oben. Dann gilt

(1) G hat eine p-Sylow-UG

(2) Je zwei p-Sylow-UG sind konjugiert.

(3) Ist s_p die Anzahl der p-Sylow UGs. Dann gilt

  (a) $s_p = (G : N(H))$, wobei $H \subseteq G$ p-Sylow UG ist

  (b) $s_p \mid m$

  (c) $s_p \equiv 1 \mod p$

Korollar 1.4.3 Satz von Cauchy

Sei G eine endliche Gruppe und p prim mit $p \mid |G|$. Dann $\exists\, a \in G$ mit $\operatorname{ord}(a) = p$.

Beweis: Sylow: $\exists$ UG $H \subseteq G$ mit $|H| = p^n$ für $n \geq 1$. Sei $e \neq b \in H \implies \operatorname{ord}(b) = p^s$ für ein $1 \leq s \leq n$. Setze $a = b^{p^{s-1}} \implies \operatorname{ord}(a) = p$. □

Beispiel 1.4.4

Sei G eine Gruppe mit

$$|G| = 12 = 2^2 \cdot 3$$

und ohne Normalteiler von Ordnung 3. Dann gilt

$$G \cong A_4.$$

Ansonsten würde G "zerfallen" in $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ bzw. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

---

4. Vorlesung - 21.10.2024

Beweis: Sei s_3 die Anzahl der 3-Sylow-UG. Nach Annahme gilt $s_3 > 1$ (da 3-Sylow nicht normal). Nach sylow $s_3 \mid 4$ und $s_3 = 1 \mod 3$. Also ist $s_3 = 4$.
Sei S die Menge der 3-Sylow-UG von G. Betrachte Konjugationsoperation $\rho : G \times S \to S$. Nach Sylow ist ρ transitiv.
Für $H \in S$ gilt daher $\operatorname{Stab}(H) = H$ (benutzen: Orbit-Stabilisator, ρ transitiv) $\implies$ ρ ist treu. (denn $H \cap H' = \{e\}$ für 3-Sylow-UGs $H \neq H'$)
$\implies$ ρ induziert einen injektiven Homomorphismus $G \to \operatorname{Bij}(S) \cong S_4$
$\implies$ mit Blatt 1 Aufgabe 2 folgt $G \cong A_4$ □

Beweis von Theorem 1.4.2: (1) Sei S die Menge aller Teilmengen $M \subseteq G$ mit $|M| = p^n$. Betrachte Operation

$$\begin{aligned} \rho : G \times S &\to S \\ (a, M) &\mapsto aM. \end{aligned}$$

Nach Theorem 1.3.4 ist

$$N := |S| = \sum_{\text{orbits}} |O|$$

$$N = \binom{p^n m}{p^n} = \binom{m}{1} = m \mod p.$$

Skizze: $(1+x)^{p^m} = (1+x^p)^m \mod p$ (beides ausschreiben).

$$\begin{aligned} &\implies p \nmid N \\ &\implies \exists \text{Orbit } O \text{ mit } p \nmid |O|. \end{aligned}$$

Sei $H \subseteq G$ der Stabilisator eines Elements $M \in O$. Beobachte: H operiert frei (1) auf M, denn

$$ab = a'b \implies a = a' \; \forall a, a' \in H, b \in M \subseteq G.$$

Mit der Bahngleichung und dem Orbit-Stabilisator-Theorem

$$|M| = \sum_{\text{Orbits } O' \text{ der } H\text{-Operation}} |O'|$$
$$|H| = \underbrace{|\mathrm{Stab}(m)|}_{1, \text{ da } H \text{ frei operiert}} \cdot |Hm|$$
$$\implies |M| = (\#H\text{-Orbits auf } M)\,|H|\,.$$

folgt $\implies |H| \mid |M| = p^n$.
Andererseits gilt:

$$|G| = |H| \cdot |O|\,.$$

Da $p \nmid |O|$ muss also $p^n \mid |H|$. Damit ist $|H| = p^n$.

(2) Sei $H \subseteq G$ eine p-Sylow-UG (maximale Ordnung). Sei $K \subseteq G$ eine p-Untergreuppe. Wir zeigen $\exists H' \subseteq G$ UG konjugiert zu H mit $K \subseteq H'$
$\implies$ (2), denn falls $|K| = |H|$ gilt $K = H'$.
Sei $\rho : G \times S \to S$ eine Operation auf einer endlichen Menge S, sodass

(1) $p \nmid |S|$
(2) p ist transitiv
(3) $\exists s \in S$ mit $\mathrm{Stab}(s) = H$

z.B. $S = G/H$ ($|S| = m$) und ρ Linksmultiplikation ($\mathrm{Stab}(H) = H$).
Wir betrachten

$$\rho|_K : K \times S \to S.$$

Es gilt $|K| = p^i$ für ein $i \leq n$ und $p \nmid |S|$. Mit der Bahnengleichung und der Definition vom Übungsblatt folgt $\implies \exists$ Fixpunkt $s \in S$ von $\rho|_K \implies K \subseteq \mathrm{Stab}_G(s')$. Da ρ transitiv ist, sind $H = \mathrm{Stab}_G(s)$ und $\mathrm{Stab}_G(s')$ konjugiert.

(3) Sei S die Menge aller p-Sylow-UG von G und $s_p = |S|$. Wir betrachten die Konjugationsoperation

$$\rho : G \times S \to S.$$

Nach (2) ist ρ transitiv. Sei $H \in S$. Nach dem Orbit-Stabilisator-theorem ist

$$|G| = \left|\underbrace{N(H)}_{\mathrm{Stab}(H)}\right| \cdot s_p \implies s_p = (G : N(H)) \implies 3(\mathrm{a}).$$

Da $H \subseteq N(H)$ gilt, gilt auch $p^n = |H| \mid |N(H)| \implies s_p = (G : N(H)) \mid m$. Für (c) betrachten wir die Konjugationsoperation

$$\rho : H \times S \to S.$$

Da $|H| = p^n$ hat jeder Orbit p^s für ien $s \leq n$. Für $H' \in S$ hat Orbit von Ordnung 1 genau dann, wenn $H \subseteq N(H')$. Dann sind $H, H' \subseteq N(H')$ p-Sylow-UG also konjugiert nach Sylow (2), also $H = H'$ da $H' \triangleleft N(H')$

$$\implies \exists!\, H' \in S \text{ mit Orbit von Ordnung 1 (nämlich } H)$$
$$\implies s_p = |S| = \sum_{\rho\text{-Orbis } O} |O| = 1 \mod p.$$

□

1.5 Exakte Sequenz

Ziel: Formalisiere für $N \triangleleft G$ das Zerlegen in N und G/N und insbesondere die Existenz.

Definition 1.5.1

(1) Eine *exakte Sequenz von Gruppen* ist eine Sequenz

$$\ldots \to G_{i-1} \xrightarrow[\text{Hom}]{\varphi_{i-1}} G_i \xrightarrow[\text{Hom}]{\varphi_i} G_{i+1} \to \ldots$$

mit $\operatorname{Im}(\varphi_{i-1}) = \operatorname{Ker}(\varphi_i)\ \forall i$.

(2) Eine *kurze exakte Sequenz* von Gruppen ist eine exakte Sequenz

$$1 \to G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \to 1,$$

wobei 1 die Gruppe mit einem Element ist.
Insbesondere ist

- φ_1 injektiv
- φ_2 surjektiv
- $\operatorname{Im}(\varphi_1) = \operatorname{Ker}(\varphi_2)$

Die Sequenz wird auch *Extension von G_3 durch G_1* genannt.

(3) Ein *Morphismus kurzer exakter Sequenzen* ist ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \to & G_1 & \to & G_2 & \to & G_3 & \to & 1 \\ & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_3} & & \\ 1 & \to & G_1' & \to & G_2' & \to & G_3' & \to & 1 \end{array}$$

Ein solcher Morphismus heißt *Isomorphismus*, wenn alle ψ Isomorphismpen sind.

Beispiel 1.5.2

(1) Ist $N \triangleleft G$ eine normale UG, so ist

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \to 1$$

nach 1.2.8 eine kurze exakte Sequenz (ι Inklusion, π Quotientenabbildung)
Nach 1.2.13 ist jede kurze exakte Sequenz von Gruppen isomorph zu einer der Form

$$\begin{array}{ccccccccc} 1 & \to & G_1 & \xrightarrow{\iota} & G_2 & \xrightarrow{\varphi} & G_3 & \to & 1 \\ & & \downarrow{\scriptstyle \iota|_{G_1}} & & \downarrow{\scriptstyle =} & & \uparrow{\scriptstyle \exists \text{ isom.}} & & \\ 1 & \to & \operatorname{Ker}(\varphi) & \to & G_2 & \to & G_2/\operatorname{Ker}(\varphi) & \to & 1 \end{array}$$

(2) Für jede Gruppe G gibt es Mengen M, M' und eine exakte Sequenz

$$\begin{array}{ccccccc} F_{M'} & \to & F_M & \xrightarrow{\pi} & G & \to & 1. \\ & \searrow & \uparrow & & & & \\ & & \operatorname{Ker}(\pi) & & & & \\ & & \uparrow & & & & \\ & & T & & & & \end{array}$$

Definition 1.5.3: kurze exakte Sequenz

Wir sagen, dass eine kurze exakte Sequenz

$$1 \to G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \to 1$$

spaltet, wenn es einen Homomorphismus

$$\psi : G_3 \to G_2$$

mit $\varphi_2 \circ \psi = \mathrm{Id}_{G_3}$ gibt.

Beobachtung:

$$1 \to G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \to 1$$

spaltet $\iff \exists H \subseteq G_2$ UG mit $\varphi_2|H$ Isomorphismus.
Wir werden sehen: Die exakte Sequenz spaltet $\iff G_2 \cong G_1 \rtimes_\rho G_3$

---

6. Vorlesung - 25.10.2024

Beispiel 1.5.4

$$1 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{N:=} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \to 1$$

spaltet nicht. Wenn ψ existieren würde, dann müsste

$$\psi(\mathbb{Z}/2\mathbb{Z}) = N \quad \lightning .$$

Definition 1.5.4: semi-direktes Produkt

Seien G_1 und G_2 Gruppen und $\rho : G_2 \times G_1 \to G_1$ Operation, sodass $\forall a \in G_2 : \rho(a_2, -) : G_1 \to G_1$ ein Homomorphismus ist.
Das *(externe) semi-direkte Produkt von G_2 und G_1 bezüglich ρ* ist die Gruppe $G_1 \rtimes_\rho G_2$ mit zugrunde liegender Menge $G_1 \times G_2$ und Gruppenstruktur

$$(a_1, a_2) \cdot (a_1', a_2') = (a_1 \cdot \rho(a_2, a_1'), a_2 \cdot a_2').$$

Bemerkung 1.5.5

(1) Die Bedingung "$\rho(a_2, -)$ ist ein Homomorphismus" ist äquivalent dazu, dass der durch ρ induzierte Homomorphismus

$$\Phi : G_2 \to \mathrm{Bij}(G_{11})$$

durch die Untergruppe

$$\mathrm{Aut}(G_1) \subseteq \mathrm{Bij}(G_1)$$

aller Gruppenautomorphismen faktorisiert

$$\begin{array}{ccc} G_2 & \longrightarrow & \mathrm{Bij}(G_1)\,. \\ & \searrow & \cup| \\ & & \mathrm{Aut}(G_1) \end{array}$$

(d.h. $\Phi(G_2) \subseteq \mathrm{Aut}(G_1)$)

(2) $G_1 \rtimes_\rho G_2$ ist tatsächlich eine Gruppe. Das neutrale Element ist (e,e). Das Inverse von (a_1,a_2) ist

$$(a_1,a_2)^{-1} = (\rho(a_2^{-1},a_1^{-1}),a_2^{-1}).$$

(3) Ist ρ trivial, so ist $G_1 \rtimes_\rho G_2 = G_1 \times G_2$

(4) Wir schreiben oft

$$G_1 \rtimes G_2 \text{ statt } G_1 \rtimes_\rho G_2,$$

wenn ρ aus dem Kontext klar ist.

(5) Via

$$\begin{aligned} G_1 &\to G_2 \rtimes_\rho G_2 \\ a &\mapsto (a,e) \\ \text{und } G_2 &\to G_1 \rtimes_\rho G_2 \\ a &\mapsto (e,a) \end{aligned}$$

sind G_1 und G_2 UG von $G_1 \rtimes_\rho G_2$. $G_1 \subseteq G_1 \rtimes_\rho G_2$ ist sogar normal, denn

$$\begin{aligned} (a_1,a_2)\cdot(a,e)\cdot(\rho(a_2^{-1},a_1^{-2}),a_2^{-1}) &= (a_1\rho(a_2,a),a_2)(\rho(a_2^{-1}.a_1^{-1}),a_2^{-1}) \\ &= (\dots,a_2a_2^{-1}) \\ &= (\dots,e) \in G_1. \end{aligned}$$

(6) Die Untergruppe $G_2 \subseteq G_1 \rtimes_\rho G_2$ ist normal $\iff$ ρ trivial ist.
Klar ist $G_2 \triangleleft G_1 \times G_2$. Umgekehrt ist für $\forall a \in G_2, a_1 \in G_1$ auch

$$\begin{aligned} &(a_1,e)(e,a)(a_1^{-1},e) = (a_1\rho(a,a_1^{-1}),a) \in G_2 \\ \implies\ &a_1\rho(a,a_1^{-1}) = e\ \forall a \in G_2, a_1 \in G_1 \\ \iff\ &\rho(a,a_1^{-1}) = a_1^{-1} \\ \iff\ &\rho \text{ trivial}\,. \end{aligned}$$

(7) Aus (5) + (6) folgt: $G_1 \rtimes_\rho G_2$ ist abelsch $\iff$ G_1, G_2 abelsch und ρ trivial

Proposition 1.5.6

Sei

$$1 \to N \to G \to G/N \to 1 \qquad (*)$$

eine kurze exakte Sequenz. Dann sind äquivalent

(1) (*) spaltet

(2) $\exists$ Operation $\rho : G/N \times N \to N$ (via Homs) und ein Isomorphismus

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle \mathrm{Id}} & & \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & N & \longrightarrow & N \rtimes_\rho G/N & \longrightarrow & G/N & \longrightarrow & 1 \end{array} \qquad (* *)$$

mit $N \rtimes_\rho G/N \ni (e, a) \longleftarrow a \in G/N$

Beweis:

- (2) $\implies$ (2): Die Spaltung ist gegeben durch die Inklusion $G/N \to G \rtimes_\rho G/N$ verkettet mit ψ.
- (1) $\implies$ (2):
  Gegeben ein Rechtsinverses

  $$\iota : G/N \to G \text{ von } G \to G/N$$

  definieren wir

  $$\begin{aligned} \psi : N \times G/N &\to G \\ (a, BN) &\mapsto a\iota(bN). \end{aligned}$$

  Beobachtung:

  - ψ ist eventuell kein Homomorphismus, da für $(a, bN), (a', b'N) \in N \times G/N$

    $$a\iota(bN)a'\iota(b'N) \stackrel{?}{=} aa'\iota(bN)\iota(b'N)$$

    unklar ist.
  - ψ ist aber bijektiv, denn $\iota(G/N)$ ist ein Repräsentantensystem der Nebenklassen von N in G und jedes Element liegt in einer eindeutigen Nebenklasse
  - ψ macht (**) kommutativ (als Diagramm von Mengen)

  Todo: Definiere Gruppenstruktur auf $G \times N$ so, dass ψ ein Homomorphismus ist.
  Nun wollen wir auf $N \times G/N$ eine Gruppenstruktur $\cdot$ defineiren, sodass ψ ein Gruppenhomomorphismus ist. Dafür sei

  $$\begin{aligned} \rho : G/N &\to N \\ (bN, a) &\mapsto \iota(bN)a\iota(bN)^{-1}. \end{aligned}$$

  Da N normal in G ist, folgt die Wohldefiniertheit. Man prüft des Weiteren:

  - ρ ist Operation
  - $\forall bN \in G/N$ ist $\rho(bN, -) : N \to N$ ein Homomorphismus
  - $\psi : N \rtimes_\rho G/N \to G$ ist ein Homomorphismus mit der Gruppenstruktur

    $$\begin{aligned} (a, bN) \cdot (a', b'N) &= \psi^{-1}(\psi(a, bN)\psi(a', b'N)) = \psi^{-1}(a\iota(bN)a'\iota(b'N)) \\ &= \psi^{-1}(a\rho(bN, a')\iota(bN)\iota(b'N)) = (a\rho(bN, a'), bb'N). \end{aligned}$$

    Dies entspricht exakt der Gruppenstruktur auf $N \rtimes_\rho G/N$.

□

Proposition 1.5.7

Seien $p < q$ zwei Primzahlen und sei G eine endliche Gruppe der Ordnung $|G| = pq$. Dann gilt

$$G = \mathbb{Z}/q\mathbb{Z} \rtimes_\rho \mathbb{Z}/p\mathbb{Z}$$

für eine Operation ρ. Ist $q \neq 1 \mod p$, so gilt $G \cong \mathbb{Z}/pq\mathbb{Z}$

Beweis: Sei s_q die Anzahl der q-Sylowuntergruppen von G. Nach 1.4.2 gilt $s_q \mid p$ und $s_q = 1 \mod q$, also $s_q = 1$ und damit ist die einzige q-Sylowuntergruppe H von G normal. Da $|H| = q$ und $|G/H| = p$ prim sind, sind beide Gruppen zyklisch und wir erhalten eine exakte Sequenz

$$1 \to \mathbb{Z}/q\mathbb{Z} \to G \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 1.$$

Ist nun $H' \subseteq G$ eine p-Sylowuntergruppe, so ist $\pi|_{H'}$ ein Isomorphismus (die Ordnung des Kerns zeilt p und q), daher spaltet $\pi|_{H'}^{-1}$ verkettet mit der Inklusion $H' \to G$ die Sequenz und es ist

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\rho \mathbb{Z}/p\mathbb{Z}$$

nach Proposition 1.5.6.
Nach Theorem 1.4.2 gilt $s_q \mid q$ und $s_p = 1 \mod p$. Ist also $q \neq 1 \mod p$, so ist $H' \cong \mathbb{Z}/p\mathbb{Z}$ normal in G, also gilt $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ nach Bemerkung 1.5.5. Das Element $(1,1) \in G$ hat Ordnung pq und G ist sogar zyklisch. □

1.6 Endlich erzeugte abelsche Gruppen

Theorem 1.6.1 Hauptsatz über endlich erzeugte abelsche Gruppen

Sei G endlich erzeugte abelsche Gruppe. Dann $\exists r, N, n_1, \dots, n_s \in \mathbb{N}$ und Primzahlen $p_1, \dots, p_s$ und ein Isomorphismus

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{N} (\mathbb{Z}/p_i^{n_i}\mathbb{Z}).$$

Diese Zerlegung ist eindeutig bis auf Permutation. Die Zahl r heißt *Rang von* G.

Definition 1.6.2: Kommutatoruntergruppe

Sei G eine Gruppe. Die *Kommutatoruntergruppe* von G ist

$$[G,G] = \left\langle \left\{ aba^{-1}b^{-1} | a, b \in G \right\} \right\rangle.$$

Lemma 1.6.3

$$[G,G] \triangleleft G.$$

Beweis: Sei $b \in [G,G], a \in G$

$$\begin{aligned} &\implies aba^{-1}b^{-1} \in [G,G] \\ &\implies aba^{-1} = \underbrace{(aba^{-1}b^{-1})}_{\in [G,G]} \underbrace{b}_{\in [G,G]} \in [G,G]. \end{aligned}$$

□

Definition 1.6.4: Abelisierung

Sei G eine Gruppe. Die *Abelisierung* (oder *Abelianisierung*) von G ist

$$G_{ab} = G/[G,G]$$

(zusmamen mit $\pi : G \to G_{ab}$)

Lemma 1.6.5

Sei G eine Gruppe. Dann gilt

(1) G_{ab} ist abelsch.

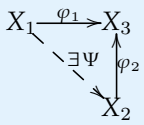
(2) Ist $\varphi : G \to H$ ein Homomorphismus zu einer abelschen Gruppe H, so faktorisiert φ eindeutig durch $G \xrightarrow{\pi} G_{ab}$.
Faktorisierung:

Gegeben: $\varphi_1 : X_1 \to X_3$
$\varphi_2 : X_2 \to X_3$

sagen wir, dass "φ_1 über φ_2 faktorisiert", wenn

$$\exists \Psi : X_1 \to X_2 \text{ mit } \varphi_2 \circ \Psi = \varphi_1$$

mit



kommutiert.

(3) Ist $N \triangleleft G$ mit G/N abelsch, so ist

$$[G,G] \subseteq N.$$

Beweis: (1) Für $a, b \in G$ ist

$$a[G,G] \cdot b[G,G] = ab[G,G] = abb^{-1}a^{-1}ba[G,G] = ba[G,G].$$

(2) Nach Homomorphiesatz 1.2.12 recht es zu zeigen:

$$[G,G] \subseteq \mathrm{Ker}(\varphi).$$

Für $a, b \in G$ gilt

$$\varphi(aba^{-1}b^{-1}) - \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b^{-1}) \overset{H\text{abelsch}}{=} \varphi(a) \cdot \varphi(a)^{-1}\varphi(b)\varphi(b)^{-1} = 1,$$

da H abelsch ist.

(3) Folgt aus (2) angewendet auf $G \to G/N$.

□

Lemma 1.6.6

Sei M eine endliche Menge. Dann ist

$$(F_M)_{ab} \cong \mathbb{Z}^{|M|}.$$

Beweis: Folgt aus direkter Rechnung □

Korollar 1.6.7

Sei G eine endlich erzeugte abelsche Gruppe. Dann $\exists\, r \in \mathbb{N}$ und ein surjektiver Homomorphismus

$$\mathbb{Z}^r \to G.$$

Beweis: Da G endlich erzeugt ist, existiert $r \in \mathbb{N}$ und ein surjektiver Homomorphismus $\varphi : F_n \to G$. Da G abelsch ist, faktorisiert φ über einen surjektiven Homomorphismus $\mathbb{Z}^r \to G$. □

---

7. Vorlesung - 28.10.2024

Lemma 1.6.8

Sei G eine abelsche Gruppe und sei n die minimale Anzahl der Erzeuger von G. Sei $H \subseteq G$ eine Untergruppe. Dann ist H endlich erzeugt und die minimale Anzahl der Erzeuger von H ist höchstens n.

Beweis: Induktion über n. Für $n = 0$ ist $G = 1 \implies H = 1$. Ist $n = 1$, so ist G zyklishc und die Aussage folgt aus Beispiel 1.1.15.
Sei nun $G = \langle a_1, \dots, a_n \rangle$. Wir setzen $\overline{G} = G/\langle a_n \rangle$ mit Quotientenabbildung $\pi : G \to \overline{G}$ und $\overline{H} = \pi(H)$. Dann wird $\overline{G}$ von $\pi(a_1), \dots, \pi(a_{n-1})$ erzeugt, also ist $\overline{H}$ nach Induktionsannahme endlich erzeugt durch höchstens $(n-1)$ Elemente, also $\overline{H} = \left\langle \overline{b}_1, \dots, \overline{b}_{n-1} \right\rangle$. Seien $b_1, \dots, b_{n-1} \in H$ mit $\pi(b_i) = \overline{b}_i$. Dann ist

$$\langle b_1, \dots, b_{n-1} \rangle \subseteq H \subseteq \langle b_1, \dots, b_{n-1}, a_n \rangle .$$

Wir folgern, dass $H = \langle b_1, \dots, b_{n-1}, H \cap \langle a_n \rangle \rangle$. Nun ist aber $H \cap \langle a_n \rangle \subseteq \langle a_n \rangle$ eine Untergruppe und damit nach IA durch höchstens ein Element b_n erzeugt, also ist $H = \langle b_1, \dots, b_{n-1}, b_n \rangle$, w.z.b.w. □

Bemerkung 1.6.9

Die Aussage von Lemma 1.6.8 stimmt im Allgemeinen nicht für endlich erzeugt nicht-abelsche Gruppen. Beispielsweise kann man zeigen, dass die Kommutatoruntergruppe von F_2 nicht endlich erzeugt ist (wir geben hier keinen Beweis dafür an).

Korollar 1.6.10

Sei G endlich erzeugt und abelsch. Dann existiert eine exakte Sequenz $n \leq m$

$$\mathbb{Z}^n \xrightarrow{\psi} \mathbb{Z}^m \to G \to 1.$$

Wir nennen eine solche exakte Sequenz Präsentation der Gruppe G.

Beweis: wir wissen aus Korrolar 1.6.7, dass es $\mathbb{Z}^m \xrightarrow{\phi} G \to 1$ gibt. Wir betrachten nun $\mathrm{Ker}(\varphi) \subseteq \mathbb{Z}^m$. Dieser ist endlich erzeugt von $n \leq m$ Elementen und wir erhalten durch Korollar 1.6.7 $\mathbb{Z}^n \to \mathrm{Ker}(\varphi)$. Wir erhalten nun die exakte Sequenz durch

$$\psi : \mathbb{Z}^n \to \mathrm{Ker}(\varphi) \hookrightarrow \mathbb{Z}^m.$$

□

Jeder Gruppenhomomorphismus $\mathbb{Z}^n \to \mathbb{Z}^m$ ist durch $A \in M(m \times n, \mathbb{Z})$ gegeben. Ersetzen wir

$$\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^m \to G \to 1$$

durch eine isomorphe kurze exakte Sequenz, so ersetzen wir A durch SAT, wobei $T \in \mathrm{Gl}_n(\mathbb{Z})$ und $S \in \mathrm{Gl}_m(\mathbb{Z})$ ist:

$$\begin{array}{ccccccc} \mathbb{Z}^n & \xrightarrow{A} & \mathbb{Z}^m & \longrightarrow & G & \longrightarrow & 1 \\ \cong\uparrow T & & S\downarrow\cong & & \uparrow \mathrm{id} & & \\ \mathbb{Z}^n & \xrightarrow{SAT} & \mathbb{Z}^m & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Der schwierigste Teil des Hauptsatzes ist dann die folgende Aussage über gannzahlige Matrizen: Wir wollen Matrizen

$$A \in M(m \times n, \mathbb{Z})$$

bis auf Multiplikation mit Elementen von $\mathrm{Gl}_n(\mathbb{Z}), \mathrm{Gl}_m(\mathbb{Z})$ verstehen.

Theorem 1.6.11 Elementarteilersatz /Smith-Normalform

Für jedes $a \in M(m \times n, \mathbb{Z})$ existiert $T \in \mathrm{Gl}_n(\mathbb{Z}), S \in \mathrm{Gl}_m(\mathbb{Z})$ mit

$$SAT = \left(\begin{array}{c|c} \mathrm{diag}(\alpha_1, \dots, \alpha_r) & 0 \\ \hline 0 & 0 \end{array} \right)$$

mit $\alpha_i \mid \alpha_{i+1} \, \forall i$. Die zahlen $r, \alpha_1, \dots, \alpha_r$ sind eindeutig bis auf Vorzeichen.

Beweis der Existenz: Wir müssen zeigen, dass wir A mittels elementarer Zeilen- und Spaltenoperationen auf die gewünschte Form bringen können. Folgende Operationen können genutzt werden:

- Multiplikation einer Zeile/Spalte mit -1
- Vertauschen zweier Spalten/Zeilen
- Addieren eines Vielfachen einer Zeile/Spalte zu einer anderen

Wir zeigen nun folgende Aussage per Induktion über n und m: Sei $0 \neq A \in M_{m\times n}(\mathbb{Z})$. Dann kann A mittels elementarer Zeilen- und Spaltenoperationen auf die Form

$$\left(\begin{array}{c|c} a & 0 \\ \hline 0 & B \end{array}\right)$$

gebracht werden, wobei $a \in \mathbb{Z}$ jeden Eintrage von B teilt. Dies erreichen wir wie folgt:

- Schritt 1: Wähle $a_{ij} \neq 0$ mit $|a_{ij}|$ minimal. Nach vertaischen können wir $(i,j) = (1,1)$ annehmen.
- Schritt 2: Durch addieren geeigneter Vielfache auf die erste Zeile/Spalte können wir erreichen, dass

  $$|a_{i1}|, |a_{1j}| < |a_{11}| \ \forall i,j \neq 1.$$

  Sind a_{i1}, a_{1j} mit $i,j \neq 1$ alle 0, so gehen wir weiter zu Schritt 3, sonst zu Schritt 1. In jeder Iteration der Schritte 1 und 2 wird $|a_{11}|$ strikt kleiner, weshlab der Prozess terminiert und Schritt 3 erreicht wird.
- Schritt 3: Existiert kein a_{ij} mit $a_{11} \nmid a_{ij}$, sind wir fertig. Sonst Addieren wir die erste Spalte auf die j-te und dann ein geeignetes Vielfaches der ersten auf die i-te Zeile, sodass $|a_{ij}| < |a_{11}|$. Dann gehen wir zurück zu Schritt 1.

Da in jeder Iteration von Schritt 1 oder 3 $|a_{11}|$ strikt kleiner wird, terminiert der Algorithmus. Das Endresultat ist eine Matrix wie in der Behauptung. □

Beispiel

$$\begin{pmatrix} 30 & 42 & 42 \\ 30 & 38 & 30 \\ 60 & 84 & 54 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 30 & 42 & 42 \\ 0 & -4 & -12 \\ 0 & 0 & -30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 30 & 12 & 12 \\ 0 & -4 & -12 \\ 0 & 0 & -30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -4 & -12 & 0 \\ 0 & -30 & 0 \\ 12 & 12 & 30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -4 & 0 & 0 \\ 0 & -30 & 0 \\ 0 & -24 & 30 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & -4 \\ -24 & 30 & 0 \\ -28 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ -24 & 30 & -48 \\ -28 & 0 & -60 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 30 & -48 \\ 0 & 0 & -60 \end{pmatrix}$$

.

Korollar 1.6.12

Sei G endlich erzeugt und abelsch.. Dann existiert $n \geq 0$ und $\alpha_1, \dots, \alpha_r$ mit $\alpha_i \mid \alpha_{i+1}$ und

$$G \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/\alpha_i\mathbb{Z}.$$

Beweis: Wir wählen eine Präsentation $\mathbb{Z}^n \xrightarrow{A\cdot} \mathbb{Z}^m \to G \to 1$ von G. Indem wir A mit Isomorphismus komponieren, können wir nach 1.6.11 annehmen, dass A in Smith-Normalform. Sind dann $\alpha_1, \dots, \alpha_r$ die (positiven) Elementarteiler von A und $N = m - r$, so ist

$$G \cong \mathbb{Z}^m/(A \cdot \mathbb{Z}^n) \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/\alpha_i\mathbb{Z}.$$

□

Bemerkung 1.6.13

Die Zahlen N und α_i in Korollar 1.6.12 sind, bis auf Reihenfolge, eindeutig durch G festgelet. Für die α_i zählt man dafür Elemente endlicher Ordnung in G. Dann wählt man eine Primzal p mit $p \nmid a_i$ für alle i und stellt fest, dass

$$G/pG \cong (\mathbb{Z}/p\mathbb{Z})^N.$$

Also ist N eindeutig festgelegt durch $|G/pG|$

Für den Beweis von Theorem 1.6.1 fehlr nur noch, dass wir jede zyklische Gruppe eindeutig in p-Gruppen zerlegen können.

Definition 1.6.14: Torsionsgruppen

Sei G eine abelsche Gruppe

(1) Die *Torsionsgruppe* von G ist definiert als

$$G_{\text{tor}} := \{a \in G \mid \operatorname{ord}(a) < \infty\}.$$

(2) Für eine Primzahl p ist di *p-Torsionsgruppe* von G definiert als

$$G[p] := \{a \in G \mid \operatorname{ord}(a) = p^n \text{ für ein } n \in \mathbb{N}\}.$$

Lemma 1.6.15

Sei G eine abelsche Gruppe. Dann sind G_{tor} und $G[p]$ Untergruppen von G.

Beweis: Es ist $\operatorname{ord}(g^{-1}) = \operatorname{ord}(g)$. Da G abelsch ist, folgt außerdem

$$(ab)^{\operatorname{ord}(a)\operatorname{ord}(b)} = \underbrace{a^{\operatorname{ord}(a)\operatorname{ord}(b)}}_{l} \cdot \underbrace{b^{\operatorname{ord}(a)\operatorname{ord}(b)}}_{l} = e.$$

Also gilt $\operatorname{ord}(ab) \mid \operatorname{ord}(a)\operatorname{ord}(b)$. Daraus folgen die Aussagen. □

Die Proposition und der Satz finden sich nicht im offiziellen Skript. Sie wurden lediglich von Tobias Lenz in der Vorlesung behandelt.

Proposition

Aus

$$\mathbb{Z}^m \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/\alpha_i\mathbb{Z} \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/\beta_i\mathbb{Z}$$

mit $\alpha_i \mid \alpha_{i+1}$ und $\beta_i \mid \beta_{i+1}$ folgt $m = n$ und $\alpha_i = \beta_i \, \forall i$

Beweis der Proposition: Betrachte den Fall $m = n = 0$.

$$G := \bigoplus_{i=1}^{r} \mathbb{Z}/\alpha_i \cong \bigoplus_{i=1}^{r} \mathbb{Z}/\beta_i.$$

Induktion über r. Behauptung: $\alpha_i = \beta_i$. Beweis:

$$G/\beta_1 G \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/\beta_i)/\beta_1 = \bigoplus_{i=1}^{r} \mathbb{Z}/\beta_1 \text{ der Ordnung } \beta_1^r.$$

Es ist

$$G/\beta_1 G \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/\alpha_i)/\beta_1 \rightsquigarrow \text{ Ordnung } \leq \alpha_1 \beta_1^{r-1} \implies \beta_1^r \leq \alpha_1 \beta_1^{r-1} \text{ und } \beta_1 \leq \alpha_1.$$

Symmetrisch: $\alpha_i \leq \beta_i$, also $\alpha_1 = \beta_1$. Nun ist

$$\alpha_1 G = \bigoplus_{i=1}^{r} \alpha(\mathbb{Z}/\alpha_i) \cong \bigoplus_{i=2}^{r} \mathbb{Z}/(\alpha_i/\alpha_1).$$

Genauso wegen $\alpha_i - \beta_i$:

$$\alpha_i G \cong \bigoplus_{i=2}^{r} \mathbb{Z}/(\beta_i/\alpha_1).$$

Nach Induktion folgt

$$\beta_i/\alpha_i = \alpha_i/\alpha_1 \, \forall i \text{ also } \beta_i = \alpha_i.$$

Das schließt den Beweis für $m = n = 0$ ab.
Allgemeiner Fall:

$$G_{\text{tor}} = \bigoplus \mathbb{Z}/\alpha_i \cong \bigoplus \mathbb{Z}/\beta_i.$$

Also $\alpha_i = \beta_i$. Ist jetzt $p > \alpha_n$, dann ist

$$p- : \mathbb{Z}/\alpha_i \to \mathbb{Z}/\alpha_i$$

bijektiv. Also

$$G/pG \cong \underbrace{\mathbb{Z}^n/p\mathbb{Z}^n}_{(\mathbb{Z}/p)^k} \oplus 0 \cong (\mathbb{Z}/p)^m.$$

Folgt aus Kardinalitätsgruünden: $p^n = p^m$, also $m = n$. □

Theorem 1.6.16 Chinesischer Restsatz

Sei G eine abelsche Gruppe, $|G| < \infty$. Sind $p_1, \ldots, p_n$ die Primteiler von $|G|$. Dann ist die Abbildung

$$\begin{aligned} \Phi : G[p_1] \times \ldots \times G[p_n] &\to G \\ a_1, \ldots, a_n &\mapsto \sum_{i=1}^{m} a_i \end{aligned}$$

ein Isomorphismus von Gruppen.

Beweis: Wir schreiben $|G| = p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}$ für paarweise unterschiedliche Primzahlen p_i und natürliche Zahlen n_i. Nach Theorem 1.4.2 ist $G[p_i]$ gleich der eindeutigen p_i-Sylowuntergruppe von G. Insbesondere gilt $|G[p_i]| = p_i^{n_i}$ und daher $|G[p_1] \times \ldots \times G[p_m]| = |G|$. Da Φ offensichtlich ein Homomorphismus ist, reicht es also zu zeigen, dass Φ injektiv ist.
Seien $(a_1, \ldots, a_m) \in G[p_1] \times \ldots \times G[p_m]$ mit $\sum_{i=1}^{m} a_i = 0$ und $N_j = \prod_{i \neq j} p_i^{n_i}$. Dann gilt

$$0 = \sum_{i=1}^{m} a_i = N_j \cdot \sum_{i=1}^{m} a_i = N_j a_j.$$

Da $p_j \nmid N_j$ gilt, ist $N_j a_j = 0 \in G$ genau dann, wenn $a_j = 0$. Wir folgern also $a_i = 0$ für alle $i = 1, \ldots, m$, also ist Φ injektiv. □

Angewendet auf zyklische Gruppen ergibt der chinesische Restsatz den letzten Teil von Theorem 1.6.1:

Korollar 1.6.17

Sei N eine natürliche Zahl mit $N = p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}$, wobei die p_i paarweise verscheidene Primzahlen sind. Dann existiert ein Isomorphismus

$$\mathbb{Z}/N\mathbb{Z} \cong \bigoplus_{i=1}^{m} \mathbb{Z}/p_i^{n_i}\mathbb{Z}.$$

Bemerkung 1.6.18

Die klassische Form des chinesischen Restsatzes ist Korollar 1.6.17 in folgender Form:
Sind $q_1, \ldots, q_m$ Primpotenzen und $a_1, \ldots, a_m \in \mathbb{Z}$, so sind die Kongruenzen

$$\begin{aligned} a &\equiv a_1 \mod q_1 \\ &\vdots \\ a &\equiv a_m \mod q_m \end{aligned}$$

eindeutig lösbar modulo $\prod_{i=1}^{m} q_i$.

1.7 Einfache und auflösbare Gruppen

Wir untersuchen endliche Gruppen G mit Normalteiler $N \triangleleft G$. Dann existiert eine kurze exakte Sequenz

$$1 \to N \to G \to G/N \to 1.$$

Ist N nicht-trivial, so sind N und G/N beide echt kleiner als G und daher leichter zu handhaben als G selbst. Will man Gruppen also klassifizieren, so ist ein natürlicher Ansatz, zuerst Grupen ohne nicht-triviale Normalteiler und dann deren Extensionen zu klassifizieren.

Definition 1.7.1

G heißt *einfach*, wenn G genau zwei Normalteiler hat.

Bemerkung 1.7.2

Die zwei Normalteiler einer einfachen Gruppe sind dann automatisch $\{e\}$ und G selbst. Insbesondere ist die triviale Gruppe nicht einfach.

Bemerkung 1.7.3

Eine einfache Gruppe kann durch aus nicht-triviale Untergruppen enthalten. Diese sind dann aber nicht normal.

Definition 1.7.4

Für eine Gruppe G definieren wir:

(1) Die *Normalreihe* von G ist eine Folge

$$\{e\} \triangleleft G_n \triangleleft \ldots \triangleleft G_0 = G.$$

Die *Faktorgruppen* der Normalreihe sind die Quotientengruppen G_i/G_{i+1}.

(2) Eine *Zerlegungsreihe* von G ist eine Normalreihe, bei der alle Faktorgruppen einfach sind.

(3) G heißt *auflösbar*, wenn sie eine Normalreihe besitzt, bei der alle Faktorgruppen abelsch sind.

Es stellt sich heraus, dass man zu jeder auflösbaren Gruppe eine natürliche Normalreihe mit abelschen Faktorgruppen findet. Dieser Weg führt über abgeleitete Untergruppen:

Definition 1.7.5

Sei G iene Gruppe. Die *i-te abgeleitete Untergruppe* D^iG von G ist rekursiv definiert als

$$D^0G := G$$
$$D^{i+1}G := [D^iG, D^iG].$$

Theorem 1.7.6

Eine Gruppe G ist genau dann auflösbar, wenn ein $n \geq 0$ mit $D^nG = \{e\}$ existiert.

Beweis: Existiert solch ein n, dann ist

$$\{e\} = D^nG \triangleleft \ldots \triangleleft D^0G = G$$

eine Normalreihe, deren Faktorgruppen nach Lemma 1.6.5 abelsch sind. Also ist G auflösbar.
Nun nehmen wir umgekehrt an, dass eine Normalreihe

$$\{e\} \triangleleft G_n \triangleleft \ldots \triangleleft G_0 = G$$

mit abelschen Faktorgruppen existiert. Wir behaupten, dass $D^iG \subseteq G_i$ gilt. Für $i = n$ liefert das die Behauptung. Dazu führen wir Induktion über i. Der Induktionsanfang ist klar, da $D^0G = G_0$. Für den Schritt beobachten wirmit Lemma 1.6.5, dass

$$D^{i+1}G = [D^iG, D^iG] \subseteq [G_i, G_i] \subseteq G_{i+1}.$$

Genau das war zu beweisen. □

---

8. Vorlesung - 04.11.2024

Korollar 1.7.7
Sei $H \subseteq G$ UG

1) Ist G auflösbar, so ist H auflösbar
2) Ist $H \triangleleft G$, so gilt

$$G \text{ auflösbar} \iff H \text{ und } G/H \text{ auflösbar.}$$

Beweis: 1) Nach Induktion gilt

$$D^{i+1}H = [D^iH, D^iH] \subseteq [D^iG, D^iG] = D^{i+1}G.$$

Dies gilt, da $D^0H = H \subseteq G = D^0G$ und

$$D^{i-1}H \subseteq D^{i-1}G \implies D^iH = [D^{i-1}H, D^{i-1}H] \subseteq [D^{i-1}G, D^{i-1}G] = D^iG.$$

Die Teilmengeneigenschaft folgt daraus, dass jedes Element von D^iH in D^iG enthalten ist.
Also

$$\begin{aligned} G \text{ auflösbar} &\implies D^iG = 1 \quad i \gg 0 \\ &\implies D^iH = 1 \quad i \gg 0 \\ &\implies H \text{ auflösbar.} \end{aligned}$$

2) Wir zeigen: Ist

$$1 \to G_1 \xrightarrow{\iota} G_2 \xrightarrow{\pi} G_3 \to 1$$

eine kurze exakte Sequenz, so ist für alle $i \geq 0$ auch

$$1 \to D^iG_2 \cap G_1 \xrightarrow{\iota_i} D^iG_2 \xrightarrow{\pi_i} D^iG_3 \to 1$$

mit

$$\begin{aligned} \iota_i &= \iota|_{D^iG_2 \cap G_1} \\ \pi_i &= \pi|_{D^iG_2} \end{aligned}$$

exakt. Daraus folgt das Korollar, denn

$\implies$ Ist $D^iG_2 = 1$, so folgt aus der Exaktheit, dass $D^iG_3 = 1$ und

$$D^iG_1 \subseteq D^iG_2 \cap G_1 = 1 \implies D^iG_1 = 1.$$

$\impliedby$ Ist $D^iG_1 = D^iG_3 = 1$, so gilt aufgrund des Diagramms, dass $D^iG_2 = G_1$ also $D^{2i}G_2 = D^i(D^iG_2) \subseteq D^iG_1 = 1$

Beweis der Behauptung:

- ι_i injektiv ist klar
- $\mathrm{Ker}(\pi_i) = \underbrace{\mathrm{Ker}(\pi)}_{G_1} \cap D^i G_2 = \mathfrak{I}(\iota_i)$
- zu zeigen: π_i ist surjektiv. Nach Induktion reicht es zu zeigen, dass π_1 surjektiv ist.
  Da $\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}\ \forall a, b \in G_2$ gilt $\mathrm{Im}(\pi_1) \subseteq [G_3, G_3]$. Seien umgekehrt $a, b \in G_3$. Wähle $c, d \in G_2$ mit $\pi(c) = a, \pi(d) = b$. Dann ist

$$\pi(cdc^{-1}d^{-1}) = aba^{-1}b^{-1}.$$

$\Longrightarrow$ Alle Kommutatoren von G_3 sind in $\mathrm{Im}(\pi_1)$ $\Longrightarrow$ $\mathrm{Im}(\pi_1) = [G_3, G_3]$.

□

Nun untersuchen wir die Auflösbarkeit von $\mathfrak{S}_n$.

Lemma 1.7.8

Für die alternierende Gruppe gilt:

(1) Ist $n \geq 3$, so wir A_n erzeugt durch 3-Zykel

(2) Ist $n \geq 5$, so sind alle Zyklen der Form $\begin{pmatrix} i & j & k \end{pmatrix}$ in A_n konjugiert.

Beweis: (1) Wir erinnern uns: $\mathfrak{S}_n$ wird von Transpositionen erzeugt.
$\Longrightarrow$ Die Elemente der $A_n \subseteq \mathfrak{S}_n$ sind genau die, die wir als Verkettung einer geraden Anzahl an Transpositionen schreiben können. Für paarweise verschiedene i, j, k, l gilt

$$\begin{aligned} \begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} i & j \end{pmatrix} &= \mathrm{Id} \\ \begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} j & k \end{pmatrix} &= \begin{pmatrix} i & j & k \end{pmatrix} \\ \begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & l \end{pmatrix} &= \begin{pmatrix} i & k & j \end{pmatrix}\begin{pmatrix} i & k & l \end{pmatrix}. \end{aligned}$$

Nun folgt bereits die Aussage, da wir immer zwei aufeinanderfolgende Transpositionen durch 3-Zykel darstellen können.

(2) Es genügt zu zeigen, dass $\begin{pmatrix} i & j & k \end{pmatrix}$ und $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ konjugiert sind. In $\mathfrak{S}_n$ sind alle Permutationen vom selben Zykeltyp konjugiert.

$$\Longrightarrow \exists \pi \in \mathfrak{S}_n \text{ mit } \pi \circ \begin{pmatrix} i & j & k \end{pmatrix} \circ \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}.$$

Wir unterscheiden zwei Fälle:

- Fall 1: $\pi \in A_k$. In diesem Fall sind wir fertig
- Fall 2: $\pi \notin A_n \Longrightarrow \begin{pmatrix} 4 & 5 \end{pmatrix} \circ \pi \in A_n$ und

$$\begin{pmatrix} 4 & 5 \end{pmatrix}\pi\begin{pmatrix} i & j & k \end{pmatrix}\pi^{-1}\begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}.$$

□

Theorem 1.7.9

Für $n \geq 1$ gilt:

1) $[\mathfrak{S}_n, \mathfrak{S}_n] = A_n$

2)

$$[A_n, A_n] = \begin{cases} 1 & \text{für } n = 1, 2, 3 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{für } n = 4 \\ A_n & \text{für } n \geq 5 \end{cases}.$$

Beweis: 1) $n = 1$ ist klar. Für $n = 2$ ist $\mathfrak{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$ also $[\mathfrak{S}_2, \mathfrak{S}_2] = 1 = A_2$. Für $n \geq 3$ ist

$$\text{sgn} : \mathfrak{S}_n \to \mathbb{Z}/2\mathbb{Z} \text{ ist surjektiv mit } \text{Ker}(\text{sgn}) = A_n.$$

Also

$$\implies \mathfrak{S}_n/A_n \cong \mathbb{Z}/2\mathbb{Z} \| \qquad \overset{1.6.5}{\implies} [\mathfrak{S}_n, \mathfrak{S}_n] \subseteq A_n.$$

Umgekehrt ist

$$(i \quad j \quad k) = (i \quad k)(j \quad k)(i \quad k)(j \quad k) = [(i \quad k), (j \quad k)].$$

Nun

$$\overset{1.7.8}{\implies} A_n \subseteq [\mathfrak{S}_n, \mathfrak{S}_n].$$

Hieraus folgt die erste Aussage.

2) Für $n = 3$ ist

$$|A_3| = 3 \implies A_3 \cong \mathbb{Z}/3\mathbb{Z} \overset{\mathbb{Z}/3\mathbb{Z} \text{ abelsch}}{\implies} [A_3, A_3] = 1.$$

Für $n = 4$ zeigt eine direkte Rechnung

$$\begin{gathered} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to [A_4, A_4] \\ l \mapsto l \\ (1 \quad 0) \mapsto (1 \quad 2)(3 \quad 4) \\ (0 \quad 1) \mapsto (1 \quad 4)(2 \quad 3) \\ (1 \quad 1) \mapsto (1 \quad 3)(2 \quad 4). \end{gathered}$$

Dies ist ein Isomorphismus.
Für $n \geq 5$ müssen wir noch zeigen, dass $A_n \subseteq [A_n, A_n]$. Nach 1.7.8 genügt es zu zeigen, dass

$$(1 \quad 2 \quad 3) \in [A_n, A_n],$$

denn alle 3-Zykel in $[A_n, A_n]$ (da $[A_n, A_n] \trianglelefteq A_n$) $\overset{1.7.8\ (2)}{\implies} A_n \subseteq [A_n, A_n]$. Wir beibachten

$$(1 \quad 2 \quad 4)(1 \quad 3 \quad 5)(4 \quad 2 \quad 1)(5 \quad 3 \quad 1) = (1 \quad 2 \quad 3).$$

□

Korollar 1.7.10

Für $n \geq 5$ sind A_n und $\mathfrak{S}_n$ nicht auflösbar.

Korollar 1.7.11

A_5 ist einfach

Beweis: Angenommen $\exists 1 \neq N \trianglelefteq A_5$ bzw. eine kurze exakte Sequenz

$$1 \to N \to A_3 \to A_5/N \to 1$$

mit $|N| < 60$ und $|A_5/N| < 60$. $\implies$ $N, A_5/N$ sind auflösbar nach Blatt 5 Aufgabe 1 $\implies$ A_5 auflösbar (Widerspruch zu 1.7.10) □

Bemerkung 1.7.12

Allgemeiner: A_n ist einfach für $n \geq 5$.
Es gibt eine Klassifikation *aller* endlicher einfacher Gruppen:

- 3 Serien:
  - $\mathbb{Z}/p\mathbb{Z}, p$ prim
  - $A_n, n \geq 5$
  - endliche Gruppen vom Lie-Typ (z.B. $\mathrm{PSL}_n(\mathbb{F}_q)$)
- 26 "sporadische" Gruppen
  Die größte dieser 26 ist die *Monstergruppe* M von Ordnung

$$|M| \approx 10^{54}.$$

Kapitel 2

Ringe

2.1 Grundbegriffe

Definition 2.1.1: (kommutativer) Ring

Ein *Ring* ist eine Menge R mit zwei Verknüpfungen:

- "Addition":

$$\begin{aligned} + : R \times R &\to R \\ (a, b) &\mapsto a + b \end{aligned}$$

- "Multiplikation":

$$\begin{aligned} + : R \times R &\to R \\ (a, b) &\mapsto a \cdot b = ab, \end{aligned}$$

sodass:

(1) $(R, +)$ ist eine abelsche Gruppe (neutrales Element 0)

(2) *Assoziativität der Multiplikation*

$$\forall a, b, c \in R : a(bc) = (ab)c.$$

(3) *Existenz der Eins*:

$$\exists 1 \in R \text{ mit } 1 \cdot a = a \cdot 1 = a \, \forall a \in R.$$

(4) *Distributivität*:

$$\forall a, b, c \in R : a \cdot (b + c) = (ab) + (ac) \text{ und } (a + b) \cdot c = (ac) + (bc).$$

Ein Ring heißt *kommutativ*, wenn $\cdot$ kommutativ ist.

Bemerkung 2.1.2

Sei R ein Ring.

(1) Wir schreiben $ab + c$ für $(ab) + c$ ("Punkt vor Strich")

(2) $1 \in R$ ist eindeutig. Ist $a \in R$ mit $ab = ba = b \, \forall b \in R$, so ist $1 = 1 \cdot a = a$.

(3) Hat $a \in R$ ein beidseitiges Inverses b bzgl. $\cdot$, so ist b eindeutig. Wir schreiben $a^{-1} := b$

(4) $\forall a \in R$ gilt:

$$0 \cdot a = (0+0) \cdot a = 0a + 0a \implies 0 \cdot a = 0.$$

Analog $a0 = 0$

(5) Für $a \in R$ schreiben wir $-a$ für das Inverse von a bzgl. $+$.
$\forall a, b \in R$ gilt:

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

Also: $(-a)b = -(ab)$

(6) In der Literatur wird manchmal $0 \neq 1$ gefordert. Für uns gilt das nicht. Ist aber $0 = 1$, so gilt $\forall a \in R$, dass

$$a = 1 \cdot a = 0 \cdot a = 0.$$

Also ist $R = \{0\}$. Dieser Ring heißt *Nullring* und wir schreiben $R = 0$.

Bemerkung

Man kann zeigen, dass die Kommmutatitiviät der Addition aus den übrigen Axiomen folgt.

Beispiel 2.1.3

1) • $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring
   • $\forall n \in Z$ ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/-n\mathbb{Z}$ (da $n\mathbb{Z} = -n\mathbb{Z}$) mit $+$ und $\cdot$ modulo n ein kommutativer Ring.

2) Ist R ein Ring, so ist die Menge

$$M_n(R) := M_{n\times n}(R)$$

der $(n \times n)$-Matrizen über R mit Matrixaddition/Multiplikation ein im Allgemeinen nicht kommutativer Ring.

3) Ist A eine abelsche Gruppe, so wird

$$\mathrm{End}(A) := \{\varphi : A \to A | \varphi \text{ Homomorphismus}\}.$$

mit

$$\varphi_1 + \varphi_2 : a \mapsto \varphi_1(a) + \varphi_2(a) \text{ und } \varphi_1 \cdot \varphi_2 := \varphi_1 \circ \varphi_2$$

ein im Allgemeinen nicht kommutativer Ring genannt *Endomorphismenring von A*.

Bemerkung 2.1.4

Wir fordern nicht, dass $(R, \cdot)$ eine Gruppe ist. $\implies$ Beweis von Lemma 1.1.3 funktioniert nicht

(1) Wir müssen explizit fordern, dass 1 beidseitig neutral ist. z.B. erfüllt die Menge

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$$

mit Matrixaddition und Multiplikation die Axioma (1),(2) und (4) in 2.1.1.

Alle $\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ sind linksneutral bzgl.

$$\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}.$$

Es gibt kein Rechtsneutrales

(2) Einseitige Inverse sind im Allgemeinen nicht eindeutig und nicht beidseitig.

Konvention 1.5: Von jetzt an schreiben wir "Ring" für kommutativer Ring.

Kapitel 3

Körper

Kapitel 4

Galoistheorie