Einführung in die Algebra

Arthur Henninger

21. Oktober 2024

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Grundbegriffe

Definition 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 1.2

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 1.3

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 1.4

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 1.5

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 1.6: 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 1.7

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 1.8: 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 1.9

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

(1) φ ist ein Isomorphismus

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

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 1.5 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 1.10: 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 1.9 (4) folgt dann: φ injektiv $\iff \mathrm{Ker}(\varphi) = \{e\}$

Lemma 1.11

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

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

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

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

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

Folglich sind $\operatorname{Ker}(\varphi)$ und $\operatorname{Im}(\varphi)$ nach Bemerkung 1.7 Untergruppen. □

Beispiel 1.12

(1) Die <u>triviale</u> 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

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

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 <u>Monoide</u> da lediglich Inverse fehlen.

(5) Für jede Menge M ist

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

mit Komposition als Verknüpfung eine Gruppe.

(6) Die symmetrische Gruppe aus n Elementen ist

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

.

(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 $F_{\{1,\ldots,n\}} =: F_n \cong \mathbb{Z}$ durch $a^n \mapsto n$.
Ist $M \subseteq G$ eine Teilmenge einer Gruppe G, so ist

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

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

Definition 1.13: 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 1.14: 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 1.15 (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 1.16: 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 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 Untegruppe* 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

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

Der *Index* von H in G ist

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

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

Bemerkung 2.2

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

$$\begin{aligned} a\cdot : M &\to aM \\ \cdot a : M &\to Ma \end{aligned}$$

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 fpr $Ha = Hb$.

(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 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 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 diese Beispiel für eine normale Untegruppe 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 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 2.6

Sei $H \subseteq G$ eine Ungergruppe. 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 2.2 (1) gilt

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

- (1) $\iff$ (3). Die Abbildung in (3) ist nach 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 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 2.7

Sei $H \triangleleft G$ normale Untegruppe. 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 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 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 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 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 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 2.4.

□

Theorem 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 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 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 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:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G'. \\ G/H \arrow[ur, "\exists ? \psi"'] & \end{tikzcd}$$

Wann gibt es ψ.

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

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

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

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

z.z.: 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 $a^{-1}b \in H \subseteq \mathrm{Ker}(\varrho)$ (Bemerkung 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 2.13

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

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

Beweis: In 2.9 setze $H = \mathrm{Ker}(\varphi)$.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/\mathrm{Ker}(\varphi) \arrow[ur, "\exists\psi \text{ nach } 2.9"'] & \end{tikzcd} .$$

φ surjektiv $\implies$ ψ surjektiv. φ injektiv: Es gilt

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

□

Korollar 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 2.15

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

Beweis von 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 2.13 reicht es zu zeigen: φ surjektiv mit $\operatorname{Ker}(\varphi) = H \cap N$.
Da $H \overset{\varphi_1}{\subseteq} HN$ gilt

$$\operatorname{Ker}(\varphi) = H \cap \underbrace{\operatorname{Ker}(HN \to HN/N)}_{=N \text{ nach } 2.8} = H \cap N.$$

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

□

Korollar 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

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

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 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 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 $M \subseteq \mathrm{Ker}(\varphi_{M'}) \rightsquigarrow \exists$ Homomorphismus $\varphi : F_M \to \mathrm{Ker}(\varphi_{M'}) \to F_{M'}$ mit erster Abbildung surjektiv. Nach Konstruktion gilt

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

Nach 2.13

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

□

Lemma 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

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

Man prüft: N ist normal. □

Definition 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 2.21

Jede Gruppe ist isomorph zu einer Gruppe der Form

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

Beispiel 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 3.1: Gruppenoperation

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

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

sodass

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

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

Bemerkung 3.2

$$\varrho : G \times X \longrightarrow X \text{ ist eine Operation} \quad \Longleftrightarrow \quad G \longrightarrow \mathrm{Bij}(X), a \mapsto (x \mapsto ax) \text{ ist ein Homomorphismus}$$

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

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

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

Frage 1

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

Definition 3.3: Orbit, Stabilisator

Sei $\varrho : G \times X \longrightarrow X$ 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 p) 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 3.4 Orbit-Stabilisator-Theorem

Sei $\varrho : G \times X \longrightarrow X$ eine Operation, $x \in X$

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

(2) Die *Orbitabbildung*

$$\begin{aligned} o_x : G &\longrightarrow Gx \\ a &\longmapsto ax \end{aligned}$$

induziert eine Bijektion zwischen den Linksnebenklassen

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

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

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

(4) Für $y \in Y$ gilt

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

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

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

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

(2) Für $a, b \in G$ gilt

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

Da o_x surjektiv ist, gilt (2)

(3) Nach 2.2 gilt:

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

(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 $b \in \operatorname{Stab}(x)$. Dann gilt

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

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

□

Theorem 3.5 Bahngleichung

Sei $\varrho : G \times X \to X$ eine Operation einer endlichen Gruppe G auf einer endlichen Menge X. Sei $x_1, \ldots, x_n \in X$

ein Repräsentantensystem der Orbits (d.h. ∀ 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 3.6: frei, transitiv, treu

Sei $\varrho : G \times X \to X$ 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

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

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

Beispiel 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

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

ist eine Operation. Für $b \in G$:

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

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

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

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 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 3.9
Sei $\varrho : G \times X \longrightarrow X$ eine Operation. Wir schreiben $G \backslash X$ für die Menge der G-Orbits.

Korollar 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 4.7: 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 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 4.3 Satz von Cauchy
Sei G eine endliche Gruppe und p prim mit $p \mid |G|$. Dann $\exists\, a \in G$ mit $\mathrm{ord}(a) = p$.

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

Beispiel 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. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Vorlesung vom 21.10.2024

Denn: 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 $\mathrm{Stab}(H) = H$ (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 $G \to \mathrm{Bij}(S) \cong S_4$
$\implies$ mit Blatt 1 Aufgabe 2 folgt $G \cong A_4$ □

Beweis von Theorem 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 3.4 ist

$$N := |S| = \sum_{\text{orbits}} |O|$$
$$N = \binom{p^n m}{p^n} = \binom{m}{1} = m \mod p.$$

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

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

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 $H' \triangleleft N(H')$

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

□

1.5 Exakte Sequenz

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

Definition 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 $\mathrm{Im}(\varphi_{i-1}) = \mathrm{Ker}(\varphi_i)\, \forall i$.

(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
- $\mathrm{Im}(\varphi_1) = \mathrm{Ker}(\varphi_2)$

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

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

$$\begin{tikzcd}
1 \arrow[r] & G_1 \arrow[r] \arrow[d, "\psi_1"] & G_2 \arrow[r] \arrow[d, "\psi_2"] & G_3 \arrow[r] \arrow[d, "\psi_3"] & 1 \\
1 \arrow[r] & G_1' \arrow[r] & G_2' \arrow[r] & G_3' \arrow[r] & 1
\end{tikzcd}$$

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

Beispiel 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 2.8 eine kurze exakte Sequenz (ι Inklusion, π Quotientenabbildung)
Nach 2.13 ist jede kurze exakte Sequenz von Gruppen isomorph zu einer der Form

$$\begin{tikzcd}
1 \arrow[r] & G_1 \arrow[r, "\iota"] \arrow[d, "\iota|_{G_1}"] & G_2 \arrow[r, "\varphi"] \arrow[d, "="] & G_3 \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Ker}(\varphi) \arrow[r] & G_2 \arrow[r] & G_2/\mathrm{Ker}(\varphi) \arrow[r] \arrow[u, dashed, "\exists\,\text{isom.}"] & 1
\end{tikzcd}$$

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

$$\begin{tikzcd}
F_{M'} \arrow[r] \arrow[dr] & F_M \arrow[r, "\pi"] & G \arrow[r] & 1. \\
 & \mathrm{Ker}(\pi) \arrow[u] & & \\
 & T \arrow[u] & &
\end{tikzcd}$$

Definition 5.3

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 $\iff G_2 \cong G_1 \rtimes_p G_3$

Kapitel 2

Ringe

Kapitel 3

Körper

Kapitel 4

Galoistheorie