Einführung in die Algebra

Arthur Henninger

October 13, 2024

Contents

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.

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

Proof: (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 $\iff \forall a, b \in H : ab^{-1} \in H$.

Proof: 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 $\varphi : G_1 \longrightarrow G_2$ 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 $\varphi : G_1 \longrightarrow G_2$ ein Homomorphismus. Dann gilt:

(1) φ ist ein Isomorphismus

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

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 $\varphi : G_1 \longrightarrow G_2$ 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 $\mathrm{Ker}(\varphi) \subseteq G_1, \mathrm{Im}(\varphi) \subseteq G_2$ Untergruppen.

Proof: 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 1.7 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

$$\begin{gathered}G \times G \to G\\ (a_1, a_2), (b_1, b_2) \mapsto (a_1b_1, a_2b_2)\end{gathered}$$

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

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

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 & reduzieren" ist 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

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

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

Definition 1.13

Sei G eine Gruppe, $M \subseteq G$ Teilmenge. Die von M erzeugte Untegruppe 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

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)

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

(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

Sei G eine Gruppe.

(1) Die <u>Ordnung von G</u> ist die Kardinalität der Menge G.

(2) Die <u>Ordnung von $a \in G$</u> 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

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

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

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 $|G| = |H| \, (G : H) \implies |H| \,|\, |G|$ ($|H|$ teilt $|G|$)

Beweis von (2):

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

□

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

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.

Proof: $\operatorname{Ker}(\varphi) \subseteq G_1$ 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.

Proof:

- (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 $H \lhd G$ 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.

Proof: 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 $H \lhd G$ eine normale Untergruppe.

(1) Die Quotientenabbildung

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

ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\varphi) = H$ (nach Bemerkung 2.2 (2)).

(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. 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 $H = \mathrm{Ker}(\varphi)$.

Proof:

- (1) $\implies$ (2): Nach Bemerkung 2.8 (1) können wir für φ die Quotientenabbildung $G \to G/H$ nehmen.
- (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 $H \subseteq G$ mit $H = \langle a \rangle$ gilt $|H| \mid |G|$.

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

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

Proof:

(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 $a^{|G|} = (a^{\mathrm{ord}(a)})^{\frac{|G|}{\mathrm{ord}(a)}}$.

□

Kapitel 3

Ringe

Kapitel 4

Körper

Kapitel 5

Galoistheorie