Einführung in die Algebra

Wintersemester 2017/18

Luise Puhlmann

30. Oktober 2017

Inhaltsverzeichnis

[9. Oktober 2017]

`http://www.math.uni-bonn.de/people/palmer/A1.html`

Organisatorisches

- Assistent: Martin Palmer
- Abgabe der Übungsblätter Donnerstag vor der Vorlesung
- Übungsgruppen Beginn nächste Woche
- Literatur siehe Homepage

1 Gruppen

1.1 Grundlegendes

Definition 1. Eine Gruppe ist eine Menge G zusammen mit einer Abbildung

$$\begin{aligned} \circ\colon G \times G &\to G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

(genannt Gruppenoperation), sodass gilt:

(G1) $(a \circ b) \circ c = a \circ (b \circ c)\ \forall a, b, c \in G$ (Assoziativität)

(G2) $\exists e \in G$ mit $g \circ e = g = e \circ g\ \forall g \in G$ (Neutrales Element)

(G3) $\forall g \in G\ \exists g^{-1}$ sodass $g \circ g^{-1} = e = g^{-1} \circ g$ (Inverse Elemente)

Bemerkung.

- Neutrales Element e ist eindeutig
- Inverse Elemente g^{-1} sind eindeutig
- Es reicht sogar zu fordern: Existenz von Linksneutralem und Linksinversem oder Existenz von Rechtsneutralem und Rechtsinversem.
- Es gelten die Kürzungsregeln:

$$\begin{aligned} a \circ c = b \circ c &\Leftrightarrow a = b \qquad \forall a, b, c \in G \\ c \circ a = c \circ b &\Leftrightarrow a = b \qquad \forall a, b, c \in G \end{aligned}$$

Definition 2. $(G, \circ)$ heißt abelsch, falls $g \circ h = h \circ g$ für alle $g, h \in G$.

Beispiel.

- $(\mathbb{Z}, +)$
- $(K, +, \cdot)$ Körper $\Rightarrow (K, +)$ und $(K^* = K \setminus \{0\}, \cdot)$ sind Gruppen
- $(V, +, \cdot)$ K-Vektorraum, dann ist $(V, +)$ eine Gruppe
- K Körper, $n \in \mathbb{N}$; $G = \mathrm{GL}_n(K)$ ist Gruppe mit Matrixmultiplikation
- M nichtleere Menge; $S_M := \{f : M \to M | f \text{ invertierbar}\}$ mit $\circ =$ Komposition von Abbildungen ist eine Gruppe; Spezialfall: $M = \{1, \ldots n\}$, $n \in \mathbb{N}$ ergibt die symmetrische Gruppe S_n der Ordnung $n!$.
- Sei $(G, \circ)$ eine Gruppe und $a \in G$ fest gewählt. Dann ist $(G, \circ_a)$ eine Gruppe, wobei $g \circ_a h = g \circ a \circ h$.

Definition 3. $(G, \circ)$ Gruppe. Dann ist die Anzahl $|G|$ der Elemente von G die Ordnung von G.

Definition 4. Sei $(G, \circ)$ Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe (kurz UG), falls $H \neq \emptyset$ und $h_1, h_2 \in H \Rightarrow h_1 \circ h_2^{-1} \in H$. Wir schreiben dann: $H < (G, \circ)$ oder $H < G$.

Bemerkung. $H < (G, \circ)$ gilt genau dann, wenn gilt:

(UG0) $e \in H$

(UG1) $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$

(UG2) $h \in H \Rightarrow h^{-1} \in H$

Klar: Untergruppen sind Gruppen

Beispiel (selber nachprüfen!!!)**.**

- $2\mathbb{Z} < (\mathbb{Z}, +)$
- $n \in \mathbb{N}$; $O(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) | AA^T = \mathbb{1}_n\} < \mathrm{GL}_n(\mathbb{R})$ die orthogonale Gruppe
- $n \in \mathbb{N}$; $U(n) = \{A \in GL_n(\mathbb{C}) | A\overline{A}^T = \mathbb{1}_n\} < \mathrm{GL}_n(\mathbb{C})$ die unitäre Gruppe
- $SL_n(K) = \{A \in \mathrm{GL}_n(K) | \det(A) = 1\} < \mathrm{GL}_n(K)$
- $SO(n) = O(n) \cap SL_n(\mathbb{R}) < O(n)$
- Spezielle Unitäre Gruppe
- $H(3, \mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$: Obere Dreiecksmatrizen, nur 1en auf der Diagonalen (Heisenberggruppe)

Definition 5. Sei $(G, \circ)$ eine Gruppe. Sei $\emptyset \neq N \subseteq G$. Dann ist $\langle N \rangle$ die kleinste (bzgl. Inklusion) Untergruppe von G, die N enthält (also: $H < G$ mit $N \subseteq H \Rightarrow \langle N \rangle \subseteq H$). Wir nennen $\langle N \rangle$ die von N erzeugte Untergruppe von $(G, \circ)$.

Bemerkung. $\langle N \rangle$ ist wohldefiniert, denn seien $H_1, H_2 < G$ mit $N \subseteq H_1, N \subseteq H_2$, dann $N \subseteq H_1 \cap H_2$ und $H_1 \cap H_2 < G$. Also existiert kleinste Untergruppe, die N enthält; $\langle N \rangle$ ist wohldefiniert.

Definition 6. G Gruppe, $N \subseteq G$

1. N erzeugt die Gruppe G, falls $\langle N \rangle = G$. In diesem Fall heißt N Erzeugendensystem der Gruppe G

2. $(G, \circ)$ heißt endlich erzeugt als Gruppe, falls $\exists N \subseteq G$ mit $|N|$ endlich und $G = \langle N \rangle$.

Bemerkung. $(G, \circ)$ Gruppe, sei $N \subseteq G$. Dann gilt: N erzeugt G (also $G = \langle N \rangle$) genau dann, wenn $\forall g \in G : \exists n_1, \dots, n_r \in G$ (mit $r \in \mathbb{N}_0$), sodass $g = n_1 \circ \dots \circ n_r$ (mit $g = e$, falls $r = 0$) und $n_i \in N$ oder $n_i^{-1} \in N$ für alle $1 \leq i \leq r$ (*).

Beweis. „$\Leftarrow$“: Sei $g \in G$ und $g = n_1 \circ \dots \circ n_r$ wie in (*). Daraus folgt $g \in \langle N \rangle$, da $n_1, \dots, n_r \in \langle N \rangle$ und dann auch g, weil $\langle N \rangle$ Gruppe. Dadurch ist $G \subseteq \langle N \rangle$, also $G = \langle N \rangle$.
„$\Rightarrow$“: Sei $G = \langle N \rangle$. Behauptung: $H := \{g \in G | g \text{ von der Form (*)}\} < G$. (dkddiermsü)

Da $\langle N \rangle \subseteq H$ nach Definition von $\langle N \rangle$ gilt und $\langle N \rangle$ eine Gruppe ist, muss also $\langle N \rangle = H$ wegen Minimalität gelten, da $N \subseteq H$ gilt. Nach Voraussetzung folgt $G = H$. Also hat jedes $g \in G$ die Form (*). $\square$

Beispiel.

- $\{\text{Transpositionen}\} \subseteq S_n$, d.h. (i, j) mit $1 \leq i < j \leq n$ erzeugen die Gruppe S_n
- $\{\text{Einfache Transpositionen}\} \subseteq S_n$, d.h. (i, j) mit $1 \leq i < j = i + 1 \leq n$ erzeugt S_n

Definition 7. Eine Gruppe G heißt zyklisch, falls $\exists g \in G$, sodass $\langle \{g\} \rangle = G$ (d.h. falls G von einem Element erzeugt wird).

Beachte: $\langle \{g\} \rangle = \{e, g, g^{-1}, g^2, g^{-2}, \dots\} = \{g^i | i \in \mathbb{Z}\}$

Beispiel. $(\mathbb{Z}, +)$ ist zyklisch mit $\mathbb{Z} = \langle \{1\} \rangle = \langle \{-1\} \rangle$

Definition 8. $(G, \circ)$ und $(G', \circ')$ seien Gruppen. Ein Gruppenhomomorphismus (kurz: Gruppenhomo) von G nach G' ist eine Abbildung $f \colon G \to G'$ mit $f(g \circ h) = f(g) \circ' f(h) \ \forall g, h \in G$.

Er ist ein Gruppenisomorphismus (kurz: Gruppeniso), falls zusätzlich f invertierbar ist. Wir schreiben $(G, \circ) \simeq (G', \circ')$, falls ein Gruppenisomorphismus von G nach G' existiert und nennen die Gruppen isomorph.

Eigenschaften von Gruppenhomomorphismen $f\colon G \to G'$ von G nach G' sei ein Gruppenhomomorphismus. Dann gilt:

(E1) f Gruppeniso $\Leftrightarrow$ f^{-1} Gruppeniso: Nach Definition existiert f^{-1}. Zu zeigen: $f^{-1}(g' \circ' h') = f^{-1}(g') \circ f^{-1}(h')$ für alle $g', h' \in G$. Sei $g', h' \in G'$. Daraus folgt $\exists g, h \in G : f(g) = g', f(h) = h'$. Also:

$$f^{-1}(g' \circ' h') = f^{-1}(f(g) \circ' f(h)) = f^{-1}(f(g \circ h)) = g \circ h = f^{-1}(g') \circ f^{-1}(h')$$

(E2) f bildet Neutrales auf Neutrales ab

[9. Oktober 2017]

[12. Oktober 2017]

(E3) f bildet Inverse auf Inverse ab

(E4) Sei $(G'', \circ'')$ eine weitere Gruppe; $f'\colon G' \to G''$ Gruppenhomo von $(G', \circ')$ nach $(G'', \circ'')$, dann ist $f' \circ f$ Gruppenhomo. Denn:

$$(f' \circ f)(g \circ h) = f'(f(g \circ h)) = f'(f(g) \circ' f(h)) = (f' \circ f)(g) \circ'' (f' \circ f)(h)$$

Beispiel (Gruppenhomos)**.**

1. $(G, \circ)$ mit $\mathrm{id}\colon G \to G,\ g \mapsto g$ Gruppenhomo von $(G, \circ)$ nach $(G, \circ)$

   Achtung $\mathrm{id}\colon G \to G,\ g \mapsto g$ ist kein Gruppenhomo von $(G, \circ)$ nach $(G, \circ_a)$, falls $a \neq e$

2. $\det\colon GL_n(K) \to K^*$ für einen Körper K ist ein Gruppenhomo

3. $f\colon \mathbb{R}^* \to \mathbb{R}_{\geq 0},\ x \mapsto |x|$ Gruppenhomo von $(\mathbb{R}^*, \cdot)$ nach $(\mathbb{R}_{\geq 0}, \cdot)$

4. $x \mapsto \exp(x)$ Gruppenhomo von $(\mathbb{Z}, +)$ nach $(\mathbb{R}^*, \cdot)$

5. Betrachte $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\} < GL_n(\mathbb{R}, \cdot)$ und $f\colon \mathbb{Z} \to G,\ a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ Gruppenhomo von $(\mathbb{Z}, +)$ nach $(G, \text{Matrixmultiplikation})$. Sogar Gruppeniso mit Inversem: $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mapsto a$

6. **Trivialer Gruppenhomo:** Schicke alles auf das neutrale Element

7. Gegeben $(G, \circ)$ Gruppe, $a \in G$. Dann ist $f\colon G \to G,\ g \mapsto g \circ a^{-1}$ ein Gruppenhomo von $(G, \circ)$ nach $(G, \circ_a)$

Lemma 1. *Sei $n \in \mathbb{Z}$.*

1. *Dann $\exists!$ Gruppenhomo $can\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}/n\mathbb{Z}, +)$ mit $can(1) = \overline{1}$*

2. *Falls $n \neq 0$, existiert kein nichttrivialer Gruppenhomo $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$*

Beweis.

1. **Eindeutigkeit:** Sei $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ Gruppenhomo. Dann $f(0) = \overline{0}$ nach (E2) und falls $f(1) = \overline{1}$, dann gilt $f(n) = f(1 + \ldots 1) = n \cdot f(1)$ für alle $n \in \mathbb{N}$ und damit auch $f(-n) = -nf(1)$ nach (E5) $\Rightarrow f$ eindeutig.

   Gruppenhomo: Es gilt dann $\mathrm{can}(x) = \overline{x}$ für alle $x \in \mathbb{Z}$ und da $\mathrm{can}(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \mathrm{can}(x) + \mathrm{can}(y)$ ist das auch ein Gruppenhomomorphismus

2. Sei $n \neq 0$. Sei $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ Gruppenhomo. Sei $f(\overline{1}) = x$. Dann: (ObdA $n \in \mathbb{N}$) $0 = f(0) = f(\overline{n}) = f(\overline{1} + \ldots \overline{1}) = nf(\overline{1}) = nx \Rightarrow x = 0 \Rightarrow f$ trivialer Gruppenhomomorphismus

□

Lemma 2. *Sei $(G, \circ)$ eine Gruppe.*

1. *Sei $Aut(G) = \{f\colon G \to G | f$ Gruppeniso von $(G, \circ)$ nach $(G, \circ)\}$. Dann ist $Aut(G)$ Gruppe, die Automorphismengruppen von G*

2. *Betrachte die Abbildung $Konj\colon G \to Aut(G)$, $g \mapsto Konj(g)$, wobei $Konj(g)(h) = g \circ h \circ g^{-1}$ für alle $h \in G$. Dann ist Konj ein Gruppenhomo von G nach $Aut(G)$. (Im Allgemeinen nicht injektiv.)*

Beweis. einfach nachrechnen □

Bemerkung.

1. Falls $(G, \circ)$ abelsch, dann ist jede Konjugation die Identität

2. $\mathrm{Konj}(g) = \mathrm{id}_G \Leftrightarrow g \in Z(G) := \{x \in G | x \circ y = y \circ x \ \ \forall y \in G\}$

Konvention: Von jetzt an schreiben wir meist gh statt $g \circ h$ und G statt $(G, \circ)$.

Satz 3. Sei $f\colon G \to G'$ Gruppenhomo. Dann gilt:

$$\begin{array}{llll} \ker(f) & := \{g \in G | f(g) = e\} & < G & \text{Kern von } f \\ \mathrm{Im}(f) & := \{g' \in G' | \exists g \in G \ f(g) = g'\} & < G' & \text{Bild von } f \end{array}$$

Beweis. einfach nachrechnen □

Beispiel.

1. $\mathrm{Ker}(\mathrm{can}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z} < \mathbb{Z}$

2. $\mathrm{Ker}(\mathrm{Konj}\colon G \to \mathrm{Aut}(G)) = Z(G) < G$

3. $\mathrm{Ker}(\det\colon GL_n(K) \to K^*) = SL_n(K)$

Übung: f Gruppenhomo; f ist injektiv genau dann, wenn $\mathrm{Ker}(f) = \{e\}$

Satz 4 (Satz von Cayley)**.** Sei G eine Gruppe. Dann ist

$$\begin{aligned} \Phi\colon G &\rightarrow S_G \\ g &\mapsto \Phi(g) \end{aligned}$$

mit $\Phi(g)(h) = gh$ für alle $h \in G$ ein injektiver Gruppenhomomorphismus. (Damit kann man G als Untergruppe einer Permutationsgruppe „realisieren".)

Beweis.
Wohldefiniert: $\Phi(g)$ ist invertierbar mit Inversem $h \mapsto g^{-1}h$.
Zu zeigen: $\Phi(g_1g_2) = \Phi(g_1) \circ \Phi(g_2)$, also $\Phi(g_1g_2)(h) = \Phi(g_1)(\Phi(g_2)(h))$ für alle $h \in G$. Es gilt aber $\Phi(g_1g_2)(h) = g_1g_2h$ und $\Phi(g_1)(\Phi(g_2)(h)) = \Phi(g_1)(g_2h) = g_1g_2h$ ✓
Injektiv: es reicht zu zeigen, dass der Kern trivial ist. Sei $g \in \mathrm{Ker}\Phi \Leftrightarrow \Phi(g) = e = \mathrm{id}_G \Leftrightarrow \Phi(g)(h) = h \ \forall h \in G \Leftrightarrow gh = h \forall h \in G \Leftrightarrow g = e$ ✓ □

1.2 Satz von Lagrange und Normalteiler

Definition 1. G Gruppe, $H < G$, $a \in G$. Dann ist:

$aH = \{ah | h \in H\} \subseteq G$ Linksnebenklasse von H zu a

$Ha = \{ha | h \in H\} \subseteq G$ Rechtsnebenklasse von H zu a

Meist arbeiten wir mit Linksnebenklassen und nennen sie einfach Nebenklassen.

Aus der Linearen Algebra wissen wir folgendes:

1. Zwei Nebenklassen sind gleich oder disjunkt d.h. $aH \cap bH \neq \emptyset \Leftrightarrow aH = bH \Leftrightarrow b^{-1}a \in H$

2. Die Abbildung $aH \rightarrow H,\ ah \mapsto h$ ist bijektiv $\Rightarrow$ alle Nebenklassen haben dieselbe Kardinalität

3. $$G = \bigcup_{g \in G} gH = \dot{\bigcup_{b \in R}} bH$$
   , wobei $R \subseteq G$, sodass die bH mit $b \in R$ genau ein Repräsentantensystem für die verschiedenen Nebenklassen bilden.

4. $g \in aH \Leftrightarrow g^{-1} \in Ha^{-1}$ (dadurch ergibt sich eine Bijektion zwischen Links- und Rechtsnebenklassen)

Definition 2. Bezeichne mit G/H die Menge der Nebenklassen von G bezüglich H und mit $H\backslash G$ die Menge der Rechtsnebenklassen. Dann gilt $|G/H| = |H\backslash G|$ (nach (4)). Wir nennen diese Zahl den Index, auch $(G : H)$, von H in G

Satz 1 (Satz von Lagrange)**.** G Gruppe, $H < G$, $|G| < \infty$. Dann gilt

$$|G| = |H| \cdot (G : H) \ .$$

Insbesondere: $|G| = p$ Primzahl $\Rightarrow H = \{e\}$ oder $H = G$.

Beweis. Formel folgt direkt aus (3), (2) und Definition von Index. Falls nun $|G| = p \Rightarrow |H| = 1$ oder $|H| = p \Rightarrow H = \{e\}$ oder $H = G$. □

Noch mehr Wissen aus der Linearen Algebra: Falls G abelsch ist, dann ist G/H wieder eine Gruppe mit Gruppenoperation

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

Im Allgemeinen (falls G nicht abelsch ist) ist $\circ$ nicht wohldefiniert (siehe Übungsblatt 2).

Definition 3. G Gruppe, $H < G$ heißt Normalteiler falls gilt: $\forall g \in G, h \in H : \quad g \circ h \circ g^{-1} \in H$. Wir schreiben dann: $H \lhd G$.

Bemerkung. Falls G abelsch, dann ist jede Untergruppe Normalteiler.

Lemma 2. *Sei $f \colon G \to G'$ Gruppenhomomorphismus. Dann: Ker$(f) \lhd G$.*

Beweis. Sei $g \in G$ und $h \in \mathrm{Ker} f$. $\Rightarrow f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e \Rightarrow ghg^{-1} \in \mathrm{Ker} f \Rightarrow \mathrm{Ker} f \lhd G$. □

[9. Oktober 2017]

[16. Oktober 2017]

Satz 3. Sei G Gruppe, $N \lhd G$. Dann gilt:

1. G/N bilden Gruppe mit $\circ \colon G/N \times G/N \to G/N, \quad (aN, bN) \mapsto abN$.
2. Die Abbildung

$$\begin{aligned} \mathrm{can} \colon G &\to G/N \\ g &\mapsto gN \end{aligned}$$

ist ein surjektiver Gruppenhomo.

Beweis.

1. Es gilt $(aN \circ bN) \circ cN = abN \circ cN = abcN = aN \circ (bN \circ cN) \Rightarrow$ (G1) Offensichtlich $eN = N$ ist neutrales Element. (G2). $a^{-1}N$ ist offensichtlich Inverses zu aN (G3).

   noch zu zeigen: Das ist wohldefiniert. Sei also $a_1 N = a_2 N$ und $b_1 N = b_2 N$. Daraus sollte $a_1 b_1 N = a_2 b_2 N$ folgen.

   Tatsächlich gilt $a_1^{-1} a_2 \in N$ und $b_1^{-1} b_2 \in N$. Dann $(a_1 b_1)^{-1}(a_2 b_2) = b_1^{-1} a_1^{-1} a_2 b_2$, wobei $a_1^{-1} a_2 \in N$ und $b_1^{-1} a_1^{-1} a_2 b_2 = b_1^{-1} b_2 (b_2 a_1^{-1} a_2 b_2) \in N \Rightarrow (a_1 b_1)^{-1} a_2 b_2 \in N \Rightarrow a_1 b_1 N = a_2 b_2 N$.

2. surjektiv klar nach (3); um zu zeigen, dass das ein Gruppenhomomorphismus ist, muss man das einfach nachrechnen

$\square$

Bemerkung. Somit gilt: Normalteiler sind genau die Kerne von Gruppenhomomorphismen.

Satz 4 (Homomorphiesatz)**.** Sei $f\colon G \to H$ Gruppenhomo. Sei $N \lhd G$. Dann: $N \subseteq \mathrm{Ker}(f) \Leftrightarrow \exists!$ Gruppenhomo $\overline{f}\colon G/N \to H$, sodass $\overline{f} \circ \mathrm{can} = f$. Also

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "\mathrm{can}"'] & H \\ & G/N \arrow[u, "\exists!\overline{f}\text{ Gruppenhomo}"'] \end{tikzcd}$$

Beweis. „$\Leftarrow$“: $\mathrm{Ker}(\mathrm{can}) = \{g \in G | gN = N\} = \{g \in G | g \in N\} = N \Rightarrow f(N) = \overline{f}(\mathrm{can}(N)) = \overline{f}(e) = e \Rightarrow N \subseteq \mathrm{Ker}(f)$.
„$\Rightarrow$“: **Eindeutigkeit:** Es muss für $\overline{f}$ gelten: $\overline{f}(aN) = \overline{f}(\mathrm{can}(a)) = f(a) \ \ \forall aN \in G/N \Rightarrow \overline{f}$ eindeutig bestimmt durch f.

Existenz: Setzen $\overline{f}(aN) := f(a) \ \ \forall aN \in G/N$. Das ist wohldefiniert (klar). Zu zeigen: Das ist ein Gruppenhomo. (nachrechnen) $\square$

Korollar 5. *$f\colon G \to H$ Gruppenhomo. Dann gilt $G/\ker f \cong \mathrm{Im}\, f$.*

Beweis. $\mathrm{Ker}f \lhd G$ nach Lemma 2.2. $\Rightarrow G/\mathrm{Ker}f$ ist eine Gruppe nach Satz 2.3. $\mathrm{im}f$ ist eine Gruppe nach 1.3. Setze $N := \mathrm{Ker}f$. Klar: $N \subseteq \mathrm{Ker}f$. Also existiert nach Satz 2.4 ein $\overline{f}$, sodass

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "\mathrm{can}"'] & H \\ & G/\mathrm{Ker}f \arrow[u, "\exists!\overline{f}\text{ Gruppenhomo}"'] \end{tikzcd}.$$

Also haben wir $\overline{f}\colon G/\mathrm{Ker}f \to \mathrm{im}f$ ein Gruppenhomomorphismus. Er ist surjektiv, weil can surjektiv ist.
Behauptung: $\overline{f}$ ist injektiv.

Es gilt $\overline{f}(aN) = f(a) = e \Leftrightarrow a \in \mathrm{Ker}f = N$. Also $\mathrm{Ker}\overline{f} = \{N\} = \{\text{neutrales Element in } G/\mathrm{Ker}f\}$. Also ist $\overline{f}$ injektiv. $\Rightarrow \overline{f}$ ist Gruppenisomorphismus. $\square$

Satz 6 (1. Isomorphiesatz)**.** Sei G eine Gruppe, $H < G$, $N \lhd G$.

1. $HN := \{hn | h \in H, n \in N\} < G$

2. $N \lhd HN$, $(H \cap N) \lhd H$

3. Es gilt $H/(H \cap N) \cong HN/N$ mit dem Gruppenisomorphismus $h(H \cap N) \mapsto hN$.

Beweis.

1. $HN \neq \emptyset$, da $e = ee \in HN$. Seien $h_1 n_1, h_2 n_2 \in HN$ $(h_i \in H, n_i \in N)$. Dann ist $h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2 {-1} = h_1 h_2^{-1} h_2 n_1 n_2^{-1} h_2 {-1}$, wobei $n_1 n_2^{-1} \in N$, $h_2 n_1 n_2^{-1} h_2^{-1} \in N$, da $N \lhd G$ und $h_1 h_2^{-1} \in H$, also ist der gesamte Ausdruck Element von HN.

2. Zunächst zeigen wir, dass $N \lhd HN$: $N \subseteq HN$ (Klar, denn $n = en$). $\Rightarrow N < HN$, weil $N < G$; genauso $N \lhd HN$, weil $N \lhd G$.

   Noch zu zeigen: $(H \cap N) \lhd H$. Klar: $(H \cap N) \subseteq H$, $(H \cap N) < H$, weil $(H \cap N) < G$. Sei $x \in H \cap N$, $h \in H$. Dann $hxh^{-1} \in H$, weil $H < G$; und $\in N$, weil $N \lhd G$. Also $hxh^{-1} \in (H \cap N) \Rightarrow H \cap N \lhd H$

3. Betrachte

   $$\begin{array}{rcl} f\colon H & \to & HN \xrightarrow{\text{can}} HN/N \\ h & \mapsto & he \end{array}$$

   Nachprüfen: f ist ein Gruppenhomo. Für $x \in H$ gilt $x \in \operatorname{Ker}(f) \Leftrightarrow xeN = N \Leftrightarrow x = xe \in \operatorname{Ker}(\text{can}) = N \Leftrightarrow x \in (H \cap N)$. Also existiert nach dem Homomorphiesatz ein Gruppenhomo $\overline{f}$:

   $$\overline{f}\colon H/(H \cap N) \to (HN)/N$$

   ist nach Konstruktion injektiv.

   Surjektiv: Sei $hnN \in (HN)/N$ mit $h \in H, n \in N$. Dann gilt aber: $hnN = hN$ und dann $f(h) = hN$ und damit $\overline{f} \circ \text{can}(h) = \overline{f}(\text{can}(h)) = hN \Rightarrow hN \in \operatorname{im} f \Rightarrow \overline{f}$ surjektiv. $\Rightarrow \overline{f}$ Gruppenisomorphismus.

□

Anmerkung zu Beweis des Homomorphiesatzes: Wo wird in „$\Rightarrow$“verwendet, dass $N \subseteq \operatorname{Ker} f$? Es wird benötigt für die Wohldefiniertheit von $\overline{f}$.

Satz 7 (2. Isomorphiesatz)**.** Sei G eine Gruppe; $N_1 \lhd G$, $N_2 \lhd G$, $N_1 \subseteq N_2$. Dann gilt $N_1 \lhd N_2$ und $N_2/N_1 \lhd G/N_1$ und es gilt:

$$(G/N_1)/(N_2/N_1) \cong G/N_2$$

durch den Isomorphismus $(gN_1)N_2/N_1 \mapsto gN_2$.

Beweis. G/N_1 ist Gruppe, weil $N_1 \lhd G$. $N_2/N_1 \subseteq G/N_1$ (Klar!); G/N_2 Gruppe, weil $N_2 \lhd G$. $N_1 \subseteq N_2$ und damit $N_1 \lhd N_2$, weil $N_1 \lhd G$. Sei

$$\begin{array}{rcl} f\colon G/N_1 & \to & G/N_2 \\ gN_1 & \mapsto & gN_2 \end{array}$$

Das ist wohldefiert: Seien $g, h \in G$, $gN_1 = hN_1 \Rightarrow g^{-1}h \in N_1 \subseteq N_2 \Rightarrow gN_2 = hN_2 \Rightarrow$ wohldefiniert.

Klar: f ist surjektiv und $gN_1 \in \mathrm{Ker}(f) \Leftrightarrow gN_2 = N_2 \Leftrightarrow g \in N_2$. Also $\mathrm{Ker}(f) = \{gN_1 | g \in N_2\} = N_2/N_1$. Also insbesondere $N_2/N_1 \lhd G/N_1$. Nach dem Korollar des Homomorphiesatzes erhalten wir einen Gruppenhomo

$$\overline{f} \colon (G/N_1)/\mathrm{Ker} f (= N_2/N_1) \to \mathrm{im} f = G/N_2 \text{ (da } f \text{ surjektiv)}$$

Nach Kosntruktion ist $\overline{f}$ injektiv, also erhalten wir den gewünschten Gruppenisomorphismus mit $\overline{f}(gN_1 \cdot (N_2/N_1)) = f(gN_1) = gN_2$. □

Anwendungen

1. **Anzahlformel:** G endliche Gruppe, $H < G$, $N \lhd G$. Dann $|HN| = \frac{|H||N|}{|H \cap N|}$. Denn nach Lagrange ist $|H| = |H \cap N|(H : H \cap N)$ und $|HN| = |N|(HN : N)$. Nach dem 1. Isomorphiesatz ist $(H : H \cap N) = (HN : N)$. Also $|HN| = \frac{|N||H|}{|H \cap N|}$ ✓
2. $(G, \circ) = (\mathbb{Z}, +)$, $m, n \in \mathbb{N}$ und $m|n$. Wir wissen: $m\mathbb{Z} < \mathbb{Z}$ und $n\mathbb{Z} < \mathbb{Z}$ (sogar Normalteiler, weil G abelsch ist). Klar ist: $n\mathbb{Z} \subseteq m\mathbb{Z}$ (insbesondere auch $n\mathbb{Z} \lhd m\mathbb{Z}$). Dann gilt
$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

1.3 Zyklische Gruppen

Wir schreiben kurz $\langle g \rangle$ statt $\langle \{g\} \rangle$.

Satz 1. Untergruppen von zyklischen Gruppen sind zyklisch.

Beweis. Sei G eine zyklische Gruppe; $G = \langle g \rangle$ mit $g \in G$. Sei $H < G$.

Fall 1 $H = \{e\} = \langle e \rangle$, also zyklisch

Fall 2 $H \neq \{e\} \Rightarrow \exists m \in \mathbb{Z} \setminus \{0\} : e \neq g^m \in H \Rightarrow \exists n \in \mathbb{N} : e \neq g^n \in H$ (weil $H < G$). Wähle $n := \min\{j \in \mathbb{N} | e \neq g^j \in H\}$. Behauptung: $H = \langle g^n \rangle$.

„$\supseteq$“: Klar, da $g^n \in H$

„=“: Angenommen, Gleichheit gilt nicht. Also $\exists s \in \mathbb{Z} : g^s \in H \setminus \langle g^n \rangle$ (beachte $G = \langle g \rangle$). Schreibe $s = an + r$ für $a, r \in \mathbb{Z}$ und $0 \leq r < n$. Falls $r = 0$, dann $s = an$ und $g^s = g^{an} = (g^n)^a \in \langle g^n \rangle$ Widerspruch!

Falls $r > 0$: Dann $g^r = (g^{an})^{-1} g^{an} g^r = ((g^n)^a)^{-1} g^s \in H$ (Widerspruch zur Minimalität)

Somit war die Annahme falsch und H ist zyklisch.

□

[16. Oktober 2017]

[19. Oktober 2017]

Lemma 2. *Bilder von zyklischen Gruppen und Gruppenhomomorphismen sind zyklisch.*

Beweis. Sei $f : G \to G'$ ein Gruppenhomomorphismus und sei G zyklisch, also $G = \langle g \rangle$ für ein $g \in G \Rightarrow G = \{g^i | i \in \mathbb{Z}\}$ also $f(G) = \{f(g^i) | i \in \mathbb{Z}\} = \{(f(g^i)) | i \in \mathbb{Z})\} = \langle f(g) \rangle \Rightarrow \operatorname{Im} f = \langle f(g) \rangle$ zyklisch. □

Lemma 3. *Sei G endliche Gruppe $|G| = n < \infty$. Sei $g \in G$ mit $G = \langle g \rangle$ (also G zyklisch). Sei* $\operatorname{ord}(g) = \min\{j \in \mathbb{N} | g^j = e\}$. *Dann gilt:* $\operatorname{ord}(g) = n$.

Definition 1. Allgemeiner: Sei G irgendeine Gruppe, $g \in G$. Dann definiere

$$\operatorname{ord}(g) := \begin{cases} \min\{j \in \mathbb{N} | g^j = e\} & \text{falls das existiert} \\ \infty & \text{sonst} \end{cases}$$

Wir nennen $ord(g)$ die Ordnung von $g \in G$.

Beweis von Lemma 3.

1. Behauptung: $\operatorname{ord}(g)$ existiert. Angenommen es existiert nicht, also $g^j \neq g \ \forall j \in \mathbb{N} \Rightarrow g^i \neq g^j$ falls $i \neq j$, $i, j \in \mathbb{N}$ (denn sonst gilt $g^{i-j} = e = g^{j-i}$ mit $i - j \in \mathbb{N}$ oder $j - i \in \mathbb{N}$). Also $|G| = \infty \Rightarrow$ Widerspruch.

   Jetzt ist noch zu zeigen, dass $n = \operatorname{ord}(g)$ gilt. Dazu sei $S := \left\{g, g^2, ..., g^{\operatorname{ord}(g)} = e\right\} \subset G$.

2. Behauptung: $S < G$. Klar: $e \in S$. Sei $g^a, g^b \in S$. Schreibe $a - b = k \cdot \operatorname{ord}(g) + r$, wobei $k, r \in \mathbb{Z}, 0 \leq r < \operatorname{ord}(g)$. Daraus folgt

   $$g^a \left(g^b\right)^{-1} = g^{a-b} = g^{k \cdot \operatorname{ord}(g) + r} = \left(g^{\operatorname{ord}(g)}\right)^k g^r = e^k g^r = e g^r = g^r \in S$$

   weil $0 \leq r < \operatorname{ord}(g)$. Da $g \in S$, gilt $\langle g \rangle \subset S$. Weil $S < G$ ist klar, dass $S \subset \langle g \rangle$, also $\langle g \rangle = S$.

3. Behauptung: $|S| = \operatorname{ord}(g)$. Seien $g^i, g^j \in S$ mit $1 \leq i, j \leq \operatorname{ord}(g)$ und $g^i = g^j$. Also $g^{i-j} = e = g^{j-i}$, was ein Widerspruch zur Minimaltität von $\operatorname{ord}(g)$ ist außer $i = j$. Folglich sind die $g^i (1 \leq i \leq \operatorname{ord}(g))$ paarweise verschieden, was die Behauptung zeigt.

□

Bemerkung. Sei G irgendeine Gruppe, $g \in G$. Dann gilt: $\operatorname{ord}(g) = |\langle g \rangle|$ und nach Satz von Lagrange dann $\operatorname{ord}(g)$ teilt $|G|$, falls $|G|$ endlich.

Satz 4 (Zyklische Gruppen)**.** Je zwei zyklische Gruppen der selben Ordnung sind isomorph. Genauer gilt für G zyklische Gruppe:

$$G \cong \begin{cases} \mathbb{Z} & \text{falls } |G| = \infty \\ \mathbb{Z}/n\mathbb{Z} & \text{falls } |G| = n \end{cases}$$

Beweis. Sei $G = \langle g \rangle$ mit $g \in G$. Sei $f : \mathbb{Z} \to G : j \mapsto g^j$. Dann ist f ein Gruppenhomomorphismus (nachrechnen) und surjektiv, da $G = \langle g \rangle$.

Fall 1 $|G| = \infty$. Dann muss f injektiv sein, damit f ein Isomorphismus ist und damit $\mathbb{Z} \cong G$. Falls f nicht injektiv ist, dann $\exists i, j \in \mathbb{Z}, i \neq j$ mit $g^i = g^j$, als $g^{i-j} = e = g^{j-i}$. Folglich ist $\operatorname{ord}(g) < \infty$. Damit wäre G nach 3 endlich, was ein Widerspruch ist.

Fall 2 $|G| = n$ endlich. Dann folgt aus 3:

$$\operatorname{ord}(g) = n \Rightarrow g^n = e \Rightarrow g^{nk} = (g^n)^k = e^k = e \ \forall k \in \mathbb{Z} \Rightarrow n\mathbb{Z} \subset \ker F$$

Nach dem Homotopiesatz gilt dann: TODO Diagramm. Also $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G$. Da $|\mathbb{Z}/n\mathbb{Z}| = n = |G|$ muss diese surjektive Abbildung schon ein Isomorphismus sein.

□

1.4 Auflösbare Gruppen

Definition 1. Eine Normalreihe eine Gruppe G ist eine Kette von Untergruppen der Form $\{e\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$. Man nennt die Quotientengruppe G_i/G_{i-1} die Faktoren der Normalreihe.

Definition 2. Eine Gruppe heißt auflösbar, falls eine Normalreihe mit abelschen Faktoren existiert.

Beispiel.

1. Abelsche Gruppen sind auflösbar: $\{e\} \lhd G$ und $G/\{e\} \cong G$, also abelsch
2. Sei $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$. Behauptung: G ist auflösbar. Dazu betrachtet man $G' = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(K) \right\} < \mathrm{GL}_2(K)$, wobei G' insbesondere eine Gruppe ist.

$$f : G \to G' : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

was ein Gruppenepimorphismus ist (nachrechnen). Es gilt:

$$\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} |b \in K \right\} \lhd G$$

Folglich gilt $\ker f \cong (K, +)$, sodass $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mapsto b$, weil $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}$ als Gruppenhomomorphismus offensichtlich bijektiv ist. Damit ist $\ker f$ abelsch und G' somit auch.

$$\Rightarrow \{e\} = G_0 \lhd \ker f = G_1 \lhd G_2 = G$$

und $kerf/\{e\}$ abelsch, sowie auch $G/\ker f \cong \operatorname{Im} f = G'$ abelsch. Somit ist G auflösbar.

3. S_4 ist auflösbar. Betrachte

$$S_4 > A_4 := \{\pi \in S_4 | \operatorname{sgn}(\pi) = 1\}$$

Nach LA 1 ist sgn ein Gruppenhomomorphismus und damit $A_4 = \ker(\operatorname{sgn}) < S_4$. Es gilt $S_4 \lhd A_4$, weil $A_4 = \ker(\operatorname{sgn})$ oder weil $(S_4 - A_4) = 2$, was dann nach Blatt 2 folgt. Betrachte nun

$$A_4 > V_4 := \left\{ e, \underbrace{(1,2)(3,4)}_{a}, \underbrace{(1,3)(2,4)}_{b}, \underbrace{(1,4)(2,3)}_{c} \right\}$$

Gruppentafel:

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

Dann gilt $A_4 \lhd V_4$, da folgendes gilt:

$$\forall \pi \in S_4 : \pi \circ \underbrace{(a_1, a_2)(a_3, a_4)}_{\tau} \circ \pi^{-1} = (\pi(a_1), \pi(a_2))(\pi(a_3), \pi(a_3))$$

weil

$$\begin{aligned}
\pi(a_1) &\xmapsto{\pi^{-1}} a_1 \overset{\tau}{\mapsto} a_2 \overset{\pi}{\mapsto} \pi(a_2) \\
\pi(a_2) &\longmapsto a_2 \mapsto a_1 \mapsto \pi(a_1) \\
\pi(a_3) &\longmapsto a_3 \mapsto a_4 \mapsto \pi(a_4) \\
\pi(a_4) &\longmapsto a_4 \mapsto a_3 \mapsto \pi(a_3)
\end{aligned}$$

also $V_4 \lhd A_4$. Folglich haben wir

$$\{e\} = G_0 \lhd V_4 = G_1 \lhd A_4 = G_2 \lhd S_4 = G_3 \tag{1}$$

G_1/G_0 $\cong V_4$ ablesch

G_2/G_1 $\cong \mathbb{Z}/2\mathbb{Z}$ also abelsch, da jede Gruppe H der Ordunung 2 zyklisch mit $H = \langle g \rangle (g \neq e)$ ist und dann nach Klassifikationssatz $H \cong \mathbb{Z}/2\mathbb{Z}$

G_3/G_2 Wir wissen, dass $|G_3/G_2| = 3$. Dann behaupten wir, dass $G_3/G_2 \cong \mathbb{Z}/3\mathbb{Z}$. Jede Gruppe H mit $|H| = 3$ ist zyklisch, denn $\langle g \rangle < H (g \neq e)$. Nach dem Satz von Lagrange gilt $\langle g \rangle = H$, weil $\langle g \rangle \neq e$ und 3 prim ist. Also folgt die Aussage aus dem Klassifikationssatz.

Daraus folgt, dass S_4 auflösbar ist.

Satz 1. Untergruppen und Bilder unter Gruppenhomomorphismen von auflösbaren Gruppen sind auflösbar.

Beweis. Sei G auflösbare Gruppe. Dann existiert eine Auflösung

$$\{e\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G \; G_i/G_{i-1} \text{ abelsch}$$

1. Sei $U < G$. Behauptung: $\{e\} = G_0 \cap U \lhd (G_1 \cap U) \lhd ... \lhd (G_n \cap U) = U$. Es ist klar, dass $(G_{i-1} \cap U) \subset (G_1 \cap U)$. Auch klar ist, dass $G_i \cap U$ eine Gruppe ist und $(G_{i-1}) < (G_1 \cap U)$. Jetzt ist noch zu zeigen, dass $(G_{i-1} \cap U) \lhd (G_i \cap U)$. Sei $x \in G_{i-1} \cap U$ und sei $y \in G_i \cap U$. Dann folgt, dass $\underbrace{yxy^{-1}}_{\in G_{i-1}} \in U$, weil $x, y \in U, U < G$, weil $x \in G_{i-1}, y \in G_i$ und $G_{i-1} \lhd G_i$. Daraus folgt, dass $yxy^{-1} \in U \cap G_{i-1}$, was zu zeigen war.

2. Behauptung: $G_i \cap U/G_{i-1} \cap U$ abelsch. Es gilt $G_i \cap U/G_{i-1} \cap U \overset{1.\text{ Iso}}{\cong} (U \cap G_i)G_i/G_i \lhd G_i/G_{i-1}$ abelsch. Daraus folgt die Behauptung.

□

[19. Oktober 2017]

[23. Oktober 2017]

1.5 title

[23. Oktober 2017]

[26. Oktober 2017]

Satz 1 (Satz 5.2)**.** G irgendein weirdes Zeichen X; X endlich: $|X| = \sum_{i \in I}(G : G_{x_i}) = |X^G| + \sum_{x_i \notin X^G}(G : G_{x_i})$

Satz 2 (Satz 5.3)**.** G endliche Gruppe, G weirdes Zeichen G durch Konjugation; $|G| = |Z(G)| + \sum_{i \in I, x_i \notin Z(G)}(G : C_G(x_i))$.

1.6 p-Gruppen und Sylow-Sätze

Definition 1. Sei p Primzahl (insbesondere ≥ 2). Eine p-Gruppe ist eine Gruppe G mit $|G| = p^r$ für ein $r \in \mathbb{N}_0$. Insbesondere ist $|G|$ endlich.

Satz 1. $G \neq \{e\}$ p-Gruppe $\Rightarrow Z(G) \neq \{e\}$

Beweis. Nach 5.3 (mit Notation von dort) $|G| = Z(G) + \sum_{i \in I, x_i \notin Z(G)}(G : G_{x_i})$. Nach Lagrange ist das durch p teilbar oder $= 1$. (Weil G eine p-Gruppe ist). $(G : G_{x_i}) = 1 \Leftrightarrow G = G_{x_i} \Leftrightarrow x_i \in Z(G)$. Das ist ein Widerspruch. Also sind die Summanden $(G : G_{x_i})$ durch p teilbar. Damit teilt p auch $|Z(G)| \Rightarrow |Z(G)| \geq 2 \Rightarrow Z(G) \neq \{e\}$. □

Satz 2. G p-Gruppe. Dann existiert Normalreiche der Form

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

für ein $n \in \mathbb{N}$, sodass $G : i/G_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$ $(1 \neq i \neq n)$. Insbesondere ist G auflösbar.

Beweis. Übungsblatt 3. $\square$

Definition 2. G endliche Gruppe, p Primzahl. Sei $|G| = p^r m$ mit $p \not| m$. $H < G$ heißt p-Sylowgruppe, falls $|H| = p^r$. Wir definieren $Syl_p(G) := \{H < G | H \text{ ist Sylowgruppe}\}$

Satz 3 (Sylowsätze)**.** p Primzahl, G endliche Gruppe, $|G| = p^r m$ mit $p \not| m$.

1. $\forall 0 \neq k \neq r \exists H < G$ mit $|H| = p^k$
2. Sei $U < G$ p-Gruppe. Dann $\exists g \in G$ und $S \in Syl_p(G)$, sodass $U < gSg^{-1}$.
3. Sei $n_p = |Syl_p(G)|$. Dann gilt
   - $n_p \equiv 1 \pmod p$
   - $n_p | m$

Beweis.

1. Sei $1 \leq k \leq r$. Fall $k = 0$ klar mit $H = \{e\}$. Sei $X = \{A \subseteq G || A| = p^k\}$, wobei $\frac{|X| = p^r m}{p^k}$; Übungsballt 3: $p^{r-k+1} \not| |X|$.

   Nun G weirdes Zeichen X durch $g.A = gA := \{ga | a \in A\}$ für $g \in G, A \in X$. (klar: $|gA| = p^k$ also $gA \in X$). Nachrechnen: (O1), (O2) gilt (offensichtlich).

   Nach Satz 5.2 folgt $|X| = \sum_{i \in I} (G : G_{x_i})$, wobei $\exists i \in I$, sodass $p^{r-k+1} \not| (G : G_{x_i})$, weil $p^{r-k+1} \not| |X|$. Wähle solch ein $x_i =: A' \in X$.

   Behauptung: $G_{A'} < G$ mit $|G_{A'} = p^k$. Dann folgt 1) mit $H = G_{A'}.Klar : G_{A'} < G$. Nach Lagrange: $|G| = |G_{A'}|(G : G_{A'})$, wobei p^r die linke Seite der Gleichung teilt, und im Index auf der rechten Seite p höchstens $r - k$-mal vorkommt.

   $\Rightarrow p^k$ teilt $|G_{A'}| \Rightarrow p^k \leq |G_{A'}|$. Sei $a \in A'$. Dann $G_{A'}.a := \{g.a | g \in G_{A'}\} \subseteq G_{A'}.A' \subseteq A'$ nach Definition von $G_{A'}$.

   Also: $|G_{A'}| = |G_{A'}.a| \leq |A'| = p^k$. (Def. von $G_{A'.a}$ und $A' \in X$). Also: $|G_{A'}| = p^k \Rightarrow$ Behauptung $\Rightarrow$ 1).

2. Sei $U < G$ mit $|U| = p^s$ für ein $s \in \mathbb{N}$. Sei $S \in Syl_p(G)$. U weirdes Zeichen G/S nach (B3) durch Linksmultiplikation.

   $$u.(gS) = ugS \qquad u \in U, g \in G$$

   $m = |G/S| = \sum_{i \in I} (U : U_{x_i})$ (nach Definition ist $S \in Syl_p(G)$; wende Lagrange an; die zweite Gleichheit folgt aus Satz 5.2).

   Weil $p \not| m$, existiert ein $i \in I$ sodass $p \not| (U : U_{x_i})$. Wähle ein solches $x_i =: aS$. Nach Lagrange ist

   $$p^s = |U| = |U_{aS}|(U : U_{aS})$$

   . Also $(U : U_{as}) = 1$. Also $U = U_{aS}$. Damit

$$\begin{array}{rrcll} & u.aS & = & aS & \forall a \in U \\ \Leftrightarrow & (ua)S & = & as & \forall u \in U \\ \Leftrightarrow & a^{-1}uaS & = & S & \forall u \in U \\ \Leftrightarrow & a^{-1}ua & \in & S & \forall u \in U \\ \Leftrightarrow & u & \in & aSa^{-1} & \forall u \in U \end{array}$$

Setze $g := a$ und erhalte $U < gSg^{-1}$.

3. Übungsaufgabe

□

Konsequenzen G endliche Gruppe, p Primzahl.

1. Je zwei p-Sylowuntergruppen in G sind zueinander konjugiert (d.h. $S, S' \in Syl_p(G) \Rightarrow \exists g \in G : S' = gSg^{-1}$)

   Beweis. Nach Sylowsatz 2 folgt $\exists g \in G$ mit $S' < gSg^{-1}$. Da $|S'| = |gSg'|$ nach Definition von p-Sylow gilt $S' = gSg^{-1}$. □

   Beachte: Falls $n_p = |Syl_p(G)| = 1$, also $\exists!$ p-Sylowgruppe S, dann ist $S \lhd G$. Denn $\forall g \in G$ ist gSg^{-1} wieder p-Sylow, also $gSg^-1 = S$.

2. (Cauchy) $p||G| \Rightarrow \exists g \in G$ mit $ord(g) = p$.

   Beweis. Nach Sylowsatz 1 existiert $H < G$ mit $|H| = p$. Wähle $g \in H$, $g \neq e$. Dann ist $\langle g \rangle < H$ und $\langle g \rangle \neq \{e\}$, also $\langle g \rangle = H$ nach Lagrange. Aus Kapitel 3 folgt $ord(g) = |H| = p$. □

3. G ist p-Gruppe $\Leftrightarrow$ Jedes Element $g \in G$ hat Ordnung p^s für geeignetes $s \in \mathbb{N}_0$ (abhängig von g).

   Beweis. „$\Rightarrow$ “: Sei $g \in G$. Sei $ord(g) = n$. Aus Satz 3.3 folgt $|\langle g \rangle| = n$. $\Rightarrow n||G|$ nach Lagrange. $\Rightarrow$ (da G p-Gruppe) $n = p^s$ für ein s.

   “$\Leftarrow$“: zu zeigen: $|G| = p^r$ für ein $r \in \mathbb{N}_0$.

   Annahme: $q||G|$ für q Primzahl $p \neq q$. Nach dem Satz von Cauchy existiert $g \in G$ mit $ord(g) = q$. Das ist ein Widerspruch. □

   Bemerkung. p-Gruppen mit unendlicher Ordnung kann man definieren als Gruppen mit $ord(g) =$ Potenz von p für alle $g \in G$.

Anwendungen Vorbemerkung: G Gruppe, $|G| = p$ Primzahl $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$. (Denn wähle $g \in G$, $g \neq e$. Dann $\langle g \rangle < G$ und nach Lagrange ist $|\langle g \rangle| = p = |G|$, also $G = \langle g \rangle$ zyklisch, also $G \cong \mathbb{Z}/p\mathbb{Z}$ nach Klassifikation von zyklischen Gruppen.)

Satz 4. *G Gruppe, $|G| = pq$ mit $p \neq q$ Primzahl. Dann ist G auflösbar.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $p > q$. Nach Sylowsatz 3 gilt: $n_p|q$, also $n_p \in \{1, q\}$ und $n_p \equiv 1 \pmod p$.

$\Rightarrow n_p = 1$, weil $p > q$. Nach Bemerkung in 1 gilt $\exists!$ p-Sylowgruppe S und $S \lhd G$. Nach Definition von p-Sylow und weil $|G| = pq$ gilt $|S| = p$. Also erhalten wir eine Normalreihe

$$\{e\} \lhd S \lhd G$$

mit $S/\{e\} \cong S \cong \mathbb{Z}/p\mathbb{Z}$ und $|G/S| = q$, also $G/S \cong \mathbb{Z}/q\mathbb{Z}$.

$\Rightarrow$ Faktoren sind abelsch $\Rightarrow G$ ist auflösbar. □

Satz 5. G Gruppe, $|G| = pq, p, q$ Primzahlen, $p < q$ und $p \not| q-1$. Dann $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z} \times q\mathbb{Z}$

Beweis. Nach Sylowsatz 3 gilt $n_p \in \{1, q\}, n_q \in \{1, p\}$ und $n_p \equiv 1 \pmod p$, $n_q \equiv 1 \pmod q$. Da $p < q$ ist, gilt $n_q = 1$. Also existiert genau eine q-Sylowgruppe $Q \lhd G$. Falls $n_p = q \Rightarrow q \equiv 1 \pmod p$. Daraus folt $p|(q-1)$ im Widerspruch zur Voraussetzung. Also ist $n_p = 1 \Rightarrow \exists!$ p-Sylowgruppe $P \lhd G$.

1. Behauptung: $x \in P, y \in Q$. Dann $xy = yx$. Denn $xyx^{-1}y^{-1} \in Q$, da $xyx^{-1} \in Q$ (Q Normalteiler) und $y^{-1} \in Q$, $xyx^{-1}y^{-1} \in P$, da $x \in P und yx^{-1}y^{-1} \in P$ (P Normalteiler).

$\Rightarrow xyx^{-1}y^{-1} \in P \cap Q$. Aber $P \cap Q = \{e\}$, da $|P \cap Q||p = |P|$ und $|P \cap Q||q = |Q|$.

$\Rightarrow$ 1. Behauptung.

Betrachte nun $\Phi\colon P \times Q \to G, (x, y) \mapsto xy$. Φ ist ein wohldefinierter Gruppenhomomorphismus. Denn $\Phi((x, y) \circ (x', y')) = \Phi((xx', yy')) = xx'yy'$; $\Phi((x, y)) \circ \Phi((x', y')) = xyx'y' = xx'yy'$ (nach der 1. Behauptung).

Außerdem ist Φ injektiv, denn $\Phi((x, y)) = e \Leftrightarrow xy = e \Leftrightarrow x = y^{-1} = e$, weil $P \cap Q = \{e\}$.

Φ ist surjektiv, weil $|P \times Q| = |P||Q| = pq = |G|$. $\Rightarrow \Phi$ liefert Gruppenisomorphismus $P \times Q \cong G$, also $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong G$ □

Korollar 6. *G Gruppe, $|G| = 15$. Dann $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und G ist zyklisch.*

Beweis. Wir wissen $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Behauptung: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$. Sei nämlich $g = (\bar{1}, \bar{1}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Dann gilt: $ord(g) = \min\{j|(\bar{1}, \bar{1}) + \ldots (\bar{1}, \bar{1}) = (\bar{0}, \bar{0} \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})\} = 15$

$\Rightarrow |\langle g\rangle| = 15 \Rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ist zyklisch.

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}, g \mapsto \bar{1}$ gibt den Isomorphismus. □

[26. Oktober 2017]

[30. Oktober 2017]

1.7 Ringe

Definition 1. Ein Ring (mit 1) ist eine Menge R zusammen mit zwei Abbildungen

$$\begin{array}{rcll} +, \cdot\colon R \times R & \to & R & \\ (a, b) & \mapsto & a + b & \text{Addition} \\ \text{bzw. } (a, b) & \mapsto & a \cdot b & \text{Multiplikation,} \end{array}$$

sodass gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $\forall a, b, c \in R$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (also $\cdot$ ist assoziativ)

(R3) $\forall a, b, c \in R$ gilt:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

(Distributivität)

(R4) $\exists 1 = 1_R \in R$, sodass $a \cdot 1 = a = 1 \cdot a$ für alle $a \in R$ (Neutrales bezüglich $\cdot$)

Bemerkung.

1. Wir bezeichnen mit 0 oder 0_R das neutrale Element bezüglich + und mit $(-a)$ das Inverse zu $a \in R$ bzgl $+$.

2. Das Element $1 \in R$ ist eindeutig (denn sei $1'$ ein anderes, dann ist $1 = 1 \cdot 1' = 1'$).

3. In einem Ring gilt: $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$, denn $a \cdot 0 = a \cdot (0 + 0 = (a \cdot 0) + (a \cdot 0) \Rightarrow 0 = a \cdot 0$; analog für $0 \cdot a$.

Definition 2. Ein Ring $(R, +, \cdot)$ heißt kommutativ, falls $a \cdot b = b \cdot a$ für alle $a, b \in R$

Beispiel.

1. Jeder Körper $(K, +, \cdot)$ ist ein kommutativer Ring (aber Ringe haben im Allgemeinen keine multiplikativ Inversen)

2. (aus LA) Sei V ein K-Vektorraum, K ein Körper, dann ist $(\mathrm{End}_K(V), +, \cdot)$ ein Ring mit $(f + g)(v) = f(v) + g(v)$ und $(f \cdot g)(v) = (f \circ g)(v)$ (Hintereinanderausführung) mit $f, g \in \mathrm{End}_K(V), v \in V$ mit $0_{\mathrm{End}_K(V)} =$ Nullabbildung; $1_{\mathrm{End}_K(V)} = \mathrm{id}_V$.

3. Nullring: $R = \{0 = 1\}$ mit $0 + 0 = 0$ und $0 \cdot 0 = 0$.

4. Es gilt folgende Umkehrung von 1.: wenn $(R, +, \cdot)$ ein kommutativer Ring ist, $R \neq \{0\}$, jedes $x \in R$ mit $x \neq 0$ besitzt Inverses x^{-1} bezüglich $\cdot$; dann ist $(R, +, \cdot)$ Körper

5. $(R, +, \cdot)$ Ring. Betrachte

$$R[t] = \left\{ \sum_{i=0}^{\infty} a_i t^i | a_i \in R, \text{ nur endlich viele } a_i \neq 0 \right\} = \left\{ \sum_{i=0}^{n} a_i t^i | a_i \in R, n \in \mathbb{N}_0 \right\}$$

Polynome mit Koeffizienten in R. Dann ist $(R[t], +, \cdot)$ ein Ring mit $0_{R[t]} =$ Nullpolynom, d.h. $a_i = 0$ für alle i. $1_{R[t]}$ ist das Polynom $p(t) = \sum_{i=0}^{\infty} a_i t^i$ mit $a_0 = 1$ und $a_i = 0$ für $i \geq 1$. Es gilt: $(R[t], +, \cdot)$ ist kommutativ $\Leftrightarrow$ $(R, +, \cdot)$ ist kommutativ.

Definition 3. $(R, +, \cdot)$ Ring. $R' \subseteq R$ heißt Unterring, falls

(UR1) $1_R \in R'$

(UR2) $\forall a, b \in R' : a + (-b) \in R', a \cdot b \in R'$

Beispiel. $(R, +, \cdot)$ Ring. $Z(R) = \{a \in R | a \cdot x = x \cdot a \ \ \forall x \in R\}$ Zentrum des Ringes ist ein Unterring.

Warnung: $Z(R) \neq Z((R, +))$ im Allgemeinen

Definition 4. Seien $(R, +, \cdot)$ und $(S, +, \cdot)$ Ringe. Eine Abbildung $\varphi\colon R \to S$ ist Ringhomomorphismus (kurz Ringhomo), falls gilt:

(RH1) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(RH2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

(RH3) $\varphi(1_R) = \varphi(1_S)$

für alle $a, b \in R$.

Falls φ zusätzlich bijektiv ist, ist es ein Ringisomorphismus (kurz Ringiso)

Bemerkung. $\varphi\colon R \to S$ Ringhomo $\Rightarrow R \to S$ ist Gruppenhomo von $(R, +)$ nach $(S, +)$ wegen (RH1).

Lemma 1.

1. *$\varphi\colon R \to S$ Ringiso $\Rightarrow \varphi^{-1}\colon S \to R$ Ringiso*

2. *$\varphi_1\colon R \to S, \varphi_2\colon S \to T$ Ringhomos $\Rightarrow \varphi_2 \circ \varphi_1\colon R \to T$ ist ein Ringhomo*

Beweis. Nachrechnen. ☐

Lemma 2. *Sei $\varphi\colon R \to S$ Ringhomomorphismus. Dann ist im$\varphi \subseteq S$ ein Unterring.*

Beweis. Es gilt $\varphi(1_R) = 1_S \in \mathrm{im}\varphi \Rightarrow$ UR1.

Seien $s_1, s_2 \in \mathrm{im}\varphi \Rightarrow \exists r_1, r_2 \in R : \ \ \varphi(r_1) = s_1, \varphi(r_2) = s_2 \Rightarrow s_1 \cdot s_2 = \varphi(r_1) \cdot \varphi(r_2) = \varphi(r_1 \cdot r_2) \in \mathrm{im}\varphi \Rightarrow s_1 \cdot s_2 \in \mathrm{im}\varphi$.

Außerdem ist $s_1 + (-s_2) = \varphi(r_1) + (-\varphi(r_2)) = \varphi(r_1) + \varphi(-r_2) = \varphi(r_1 + (-r_2)) \in \mathrm{im}\varphi \Rightarrow s_1 + (-s_2) \in \mathrm{im}\varphi \Rightarrow$ UR2. ☐

Warnung: Wir setzen für $\varphi\colon R \to S$ Ringhomo

$$\mathrm{Ker}\varphi := \{r \in R | \varphi(r) = 0_S\} \ .$$

Dann ist Ker $\subseteq R$ genau dann Unterring, falls S der Nullring ist. Denn:

„$\Rightarrow$“: Kerφ Unterring $\Rightarrow 1_R \in \mathrm{Ker}\varphi \Rightarrow 0_S = \varphi(1_R) = 1_S \Rightarrow \forall s \in S : \ \ s = s \cdot 1_S = s \cdot 0_S = 0_S$.

“$\Leftarrow$“: $S = \{0\} \Rightarrow \mathrm{Ker}\varphi = R$ offensichtlich Unterring.

Definition 5. Sei $(R, +, \cdot)$ ein Ring. $I \subseteq R$ heißt Ideal, falls gilt:

(I1) $I < (R, +)$

(I2) a) $a \cdot x \in I$ für alle $x \in I, a \in R$

b) $x \cdot a \in I$ für alle $x \in I, a \in R$

Falls nur (I1), (I2a) erfüllt sind, heißt I Linksideal; falls nur (I1) und (I2b) erfüllt sind, heißt I Rechtsideal.

Beispiel.

1. $(\mathbb{Z}, +, \cdot)$ ist Ring. Sei nun $n \in \mathbb{Z}$ und $I = n\mathbb{Z} = \{nk | k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ ist Ideal, denn: $n\mathbb{Z} < (\mathbb{Z}, +)$, also folgt (I1); und für $a \in \mathbb{Z}$ und $x = nk \in n\mathbb{Z}$ gilt: $ax = ank = nak \in I$; $xa = nka = nak \in I$ und damit folgt (I2).

2. $(R, +, \cdot)$ Ring; $(R[t], +, \cdot)$ wie in Beispiel oben; $I = \{p(t) \in R[t] | p(t) = \sum_{i=0}^{\infty} a_i t^i \;\; a_0 = 0\}$ Polynome ohne konstanten Term. Dann ist $I \subseteq R[t]$ ein Ideal (kurz selbst überlegen).

Lemma 3. *$\varphi\colon R \to S$ Ringhomo $\Rightarrow$ $Ker\varphi \subseteq R$ ist Ideal.*

Beweis. $\mathrm{Ker}\varphi < (R, +)$ nach 1.3 $\Rightarrow$ (I1). Sei nun $a \in R, x \in \mathrm{Ker}\varphi \Rightarrow \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0_S = 0_S \Rightarrow ax \in \mathrm{Ker}\varphi$. Genauso $xa \in \mathrm{Ker}\varphi \Rightarrow$ (I2). □

Beispiel. $(R[t], +, \cdot)$ wie in Beispiel 3. Sei $a \in R$.

$$\begin{array}{rcl} \mathrm{ev}_a\colon R[t] & \to & R \\ p(t) = \sum_{i=0}^{\infty} b_i t^i & \mapsto & p(a) = \sum_{i=0}^{\infty} b_i a^i \\ (b_i \in R;\ \text{fast alle } b_i = 0) & & (\text{mit } a^i = a \cdot \dots \cdot a (n\text{-mal})) \end{array}$$

Auswertungsabbildung

Nachrechnen: ev_a ist Ringhomo.

$\mathrm{Ker}(\mathrm{ev}_a) = \{p(t) \in R[t] | p(a) = 0_R\}$. Also: das sind genau die Polynome, die a als Nullstelle haben. Wir wissen: $\mathrm{Ker}(\mathrm{ev}_a) \subseteq R[t]$ Ideal nach 7.3.

Spezialfall: $a = 0_R$. Dann gilt $\mathrm{Ker}(\mathrm{ev}_0) = I$ wie in Bsp. 3 Teil 2); (insbesondere I Ideal).

Seien nun ein Ring $(R, +, \cdot)$ und ein Ideal $I \subseteq R$ gegeben. Insbesondere, nach ($I1$), ist $I < (R, +)$, sogar $I \lhd (R, +)$, weil $(R, +)$ abelsch.

$\to$ R/I ist wieder Gruppe mit den Nebenklassen in $(R, +)$ bezüglich I als Elemente. Nebenklassen sind von der Form $\overline{a} = \{a + x | x \in I\}$ $a \in R$ und die Gruppenoperation auf G/I ist $\overline{a} \circ \overline{b} = \overline{a + b}$

Satz 4. Voraussetzungen: R, I wie oben. Dann wird $(R/I, \circ)$ zu einem Ring $(R/I, +, \cdot)$, wobei $+ = \circ$ und Multiplikation $\cdot = \odot$ gegeben ist durch $\overline{a} \odot \overline{b} = \overline{a \cdot b}$, wobei letzteres die Multiplikation in R ist.

Beweis.

(R1) $(R/I, +)$ ist abelsche Gruppe (nach Kapitel 1.1)

(R2) Seien $\overline{a}, \overline{b}, \overline{c} \in R/I$. $(\overline{a} \odot \overline{b}) \odot \overline{c} = (\overline{ab}) \odot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \odot \overline{bc} = \overline{a} \odot (\overline{b} \odot \overline{c})$.

(R3) Seien $\overline{a}, \overline{b}, \overline{c} \in R/I$. Dann $\overline{a} \odot (\overline{b} \circ \overline{c}) = \overline{a} \odot \overline{b + c} = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{ab} \circ \overline{ac} = \overline{a} \odot \overline{b} \circ \overline{a} \odot \overline{c}$. Analog für den zweiten Teil von (R3).

(R4) Sei $\overline{a} \in R/I$. Dann gilt $\overline{a} \odot \overline{1_R} = \overline{a1_R} = \overline{a} = \overline{1_R \cdot a} = \overline{1_R} \odot \overline{a}$

$\Rightarrow \overline{1_R}$ ist neutrales Element für $\odot$.

Noch zu prüfen: $\odot$ ist wohldefiniert! Also zu zeigen: für $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$ folgt $\overline{a} \odot \overline{b} = \overline{a'} \odot \overline{b'}$ mit $\overline{a}, \overline{b}, \overline{a'}, \overline{b'} \in R/I$. Sei also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$.

$\boxed{\text{Dann existieren } x, y \in I \text{ mit } a + (-a') = x \text{ und } b + (-b') = y \ (1)}$.

Zu zeigen ist nun $\overline{ab} = \overline{a'b'}$. Es gilt $a \cdot b = (a' + x) \cdot (b' + y) = (a'b') + (a'y) + (xb') + (xy)$, wobei $(a'y) + (xb') + (xy) \in I$, weil I Ideal ist. $\Rightarrow (ab) + (-a'b') \in I \Rightarrow \overline{ab} = \overline{a'b'}$.

□