



WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER



FACHBEREICH 10
MATHEMATIK UND
INFORMATIK

Einführung in die Algebra

Aufarbeitung der Vorlesungsnotizen

Tobias Wedemeier

23. Oktober 2014

gelesen von

Prof. Dr. Kramer

Hierbei handelt es sich um eine Aufarbeitung der Vorlesungsmitschriften von **Prof. Dr. Kramer**, WWU Münster, aus der Vorlesung **Einführung in die Algebra** im Wintersemester 2014/15. Dies ist kein Skript der Vorlesung und keine eigene Arbeit des Autors.

Für Fehler in der Aufarbeitung wird keine Haftung übernommen. Hinweise auf Fehler sind gerne gesehen, hierfür kann man mich in der Uni ansprechen oder alternativ eine e-Mail an:

tobias.wedemeier@gmx.de

Auch ist eine Mitarbeit über Github möglich.

Wenn Teile aus der Vorlesung selber fehlen, können diese gerne an meine e-Mail versandt werden. Ich werde diese dann einarbeiten.

Inhaltsverzeichnis

Prolog	1
1 Elementare Gruppentheorie	1
1.1 Def. Gruppe	1
1.2 Beispiel 1	2
1.3 Beobachtungen	2
1.4 Lemma 1 (Sparsame Definition von Gruppen)	2
1.5 Beispiel 2	2
1.6 Def. zentralisieren	2
1.7 Beispiel 3	3
1.8 Def. Untergruppe	3
1.9 Lemma 2	3
1.10 Def. $\langle X \rangle$	3
1.11 Def. zyklische Gruppe	4
1.12 Zyklische Gruppen	4
1.13 Nebenklassen	4
1.14 Satz von Lagrange	5
1.15 Homomorphismen	6
1.16 Satz 1	7
Index	A
Abbildungsverzeichnis	B

Prolog

Geplante Inhalte

- Gruppentheorie, Untergruppen, Normalteiler, Quotienten, Permutationsgruppen
- Kommutative Ringe, Ideale, Faktorisierbarkeit
- Körper, Galois-theorie, Konstruierbarkeit mit Zirkel und Lineal

Algebra

: historisch das auflösen von Gleichungen. Moderne Algebra untersucht sog. algebraische Strukturen wie Gruppen, Ringe, Körper, Varietäten,...

Literatur:

- Cohn Basic Algebra
- Jacobsen Basic Algebra I
- Herstein Topics in Algebra
- Laug Algebra
- Bosch Algebra
- Lorenz Einführung in die Algebra

(die beiden letzten Bücher gehen vor allem auf die Körpertheorie ein)

Zur Vorlesung:

Regelmäßige Teilnahme + Mitschreiben. Meine eigenen Notizen gibt es dann immer im www eingescannt (kein Skript)

Übungen

Regelmäßige Teilnahme, vorrechnen. Zwei Namen auf Hausaufgaben, wenn beide alles vorrechnen können.

Regelmäßige Abgabe + min. eine Aufgabe erfolgreich vorrechnen + 50 + x% richtig \Rightarrow Klausurzulassung.

1 Elementare Gruppentheorie

Erinnerung: eine Verknüpfung auf einer nicht leeren Menge X ist eine Abbildung

$$X \times X \rightarrow X, (x, y) \mapsto m(x, y).$$

Häufig schreibt man $m(x, y) = xy$ oder $m(x, y) = x + y$, je nach Kontext. Die Schreibweise $m(x, y) = x + y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn $\forall x, y \in X$ gilt $m(x, y) = m(y, x)$.

1.1 Def. Gruppe

Eine Gruppe (G, \cdot) besteht aus einer Verknüpfung \cdot auf einer nicht leeren Menge G , mit folgenden Eigenschaften:

- (G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt $\forall x, y, z \in G$.
(Folglich darf man Klammern weglassen.)

(G2) Es gibt ein neutrales Element $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x \forall x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $xy = e = yx$.
man schreibt dann auch $y = x^{-1}$ für das Inverse zu x .

Fordert man von der Verknüpfung nur (G1) und (G2), so spricht man von einer Halbgruppe mit Eins oder einem **Monoid**. Fordert man nur (G1), so spricht man von einer Halbgruppe.

1.2 Beispiel 1

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind kommutative Gruppen.
- $(\mathbb{Z}, \cdot), (\mathbb{N}, \cdot), (\mathbb{N}, +)$ sind Monoide.

1.3 Beobachtungen

- a) Das Neutralelement (einer Verknüpfung) ist eindeutig bestimmt: sind e, e' beides Neutralelemente, so folgt: $e = ee' = e'$
- b) Das Inverse zu x ist eindeutig bestimmt:
 $xy = e = xy' = y'x \Rightarrow y' = y'e = y'xy = ey = y$

1.4 Lemma 1 (Sparsame Definition von Gruppen)

Sei $G \times G \rightarrow G$ eine assoziative Verknüpfung. Dann ist G schon eine Gruppe, wenn gilt:

- (i) es gibt $e \in G$ so, dass $ex = x \forall x \in G$ gilt.
- (ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$

Beweis

Sei $yx = e$, es folgt $xyx = y$. Wähle z mit $zy = e$, es folgt $\underbrace{zy}_{=e} xy = zy = e \Rightarrow xy = e$

Weiter gilt $xe = xyx = ex = x$. □

1.5 Beispiel 2

Sei X eine nicht leere Menge, sei $X^X = \{f : X \rightarrow X\}$ die Menge aller Abbildungen von X nach X . Als Verknüpfung auf X nehmen wir die Komposition von Abbildungen. Dann gilt wegen $f = id_X \circ f = f \circ id_X$, dass id_X ein Neutralelement ist.

Damit haben wir ein Monoid (X^X, \circ) .

Sei $Sym(X) = \{f : X \rightarrow X \mid f \text{ bijektiv}\}$. Zu jedem $f \in Sym(X)$ gibt es also eine Umkehrabbildung $g : X \rightarrow X$ mit $f \circ g = g \circ f = id_X$. Folglich ist $(Sym(X), \circ)$ eine Gruppe, die **Symmetrische Gruppe**. Wenn X endlich ist mit n Elementen, so gibt es genau $n! = n(n-1)(n-2) \cdots 2 \cdot 1$ Permutationen, also hat $Sym(X)$ dann genau $n!$ Elemente.

Für $X = \{1, 2, 3, \dots, n\}$ schreibt man auch $Sym(X) = Sym(n) \left(= S_n \right)$.

1.6 Def. zentralisieren

Sei $G \times G \rightarrow G$ eine Verknüpfung. Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder x **zentralisiert** y , wenn gilt $xy = yx$.

Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder **abelsch**.

1.7 Beispiel 3

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, (\mathbb{Q}^*, \cdot) sind abelsche Gruppen.

(b) K Körper, $G = GL_2(K) = \{X \in K^{2 \times 2} \mid \det(X) \neq 0\}$ Gruppe der invertierbaren 2×2 Matrizen.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

\Rightarrow nicht abelsch, genauso $GL_n(K)$ für $n \geq 2$.

(c) $Sym(2)$ ist abelsch, aber $Sym(3)$ nicht. Allgemein ist $Sym(X)$ nicht abelsch, falls $\#X \geq 3$ gilt.

1.8 Def. Untergruppe

Sei G eine Gruppe, sei $H \subseteq G$. Wir nennen H **Untergruppe** von G , wenn gilt:

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offensichtlich ist eine Untergruppe dann wieder eine Gruppe, mit der von G vererbten Verknüpfung.

Bsp

(a) $(\mathbb{Q}, +)$. \mathbb{Z} ist Untergruppe, denn $0 \in \mathbb{Z}$, $m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}$ und $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

(b) (\mathbb{Q}^*, \cdot) . \mathbb{Z}^* ist keine Untergruppe, kein Inverses.

1.9 Lemma 2

Sei G eine Gruppe und sei U eine nicht leere Menge von Untergruppen von G . Dann ist auch

$$\bigcap U = \{g \in G \mid \forall H \in U \text{ gilt } g \in H\}$$

eine Untergruppe von G .

Beweis

Für alle $H \in U$ gilt $e \in H$, also $e \in \bigcap U$. Angenommen $x, y \in \bigcap U$. Dann gilt für alle $H \in U$, dass $xy \in H$ sowie $x^{-1} \in H$. Es folgt $xy \in \bigcap U$ sowie $x^{-1} \in \bigcap U$. \square

1.10 Def. $\langle X \rangle$

Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Wir setzen:

$$\langle X \rangle = \bigcap \{H \subseteq G \mid H \text{ Untergruppe und } X \subseteq H\}$$

Ist nicht leer, da mindestens G enthalten ist.

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insb. also $\langle H \rangle = H$.

Satz

Sei $X \subseteq G$ und sei $W = \{x_1 \cdot x_2 \cdot \dots \cdot x_s \mid s \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \forall i = 1, \dots, s\}$.

Dann gilt: $\langle X \rangle = \{e\} \cup W$.

Beweis

Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $fg \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von G , mit $X \subseteq H$. Es folgt $\langle X \rangle \subseteq H = \{e\} \cup W$. \square

1.11 Def. zyklische Gruppe

Sei G eine Gruppe und sei $g \in G$. Für $n \geq 1$ setze $g^n = \underbrace{g \cdot \dots \cdot g}_{n\text{-mal}}$ sowie $g^{-n} = \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{n\text{-mal}}$ und

$g^0 = e$.

Dann gilt $\forall k, l \in \mathbb{Z}$, dass $g^k \cdot g^l = g^{k+l}$.

Sei $\langle g \rangle = \langle \{g\} \rangle \stackrel{1.10}{=} \{g^n \mid n \in \mathbb{Z}\}$. Man nennt $\langle g \rangle$ die von g erzeugte **zyklische Gruppe**. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt n ein **Eponent** von g . Die **Ordnung** von g ist der kleinste Eponent von g ,

$$o(g) = \min(\{n \geq 1 \mid g^n = 1\} \cup \{\infty\})$$

$o(g) = \infty$ bedeutet: $g^n \neq e \forall n \geq 1$

$o(g) = 1$ bedeutet: $g^n = g = e$

1.12 Zyklische Gruppen

Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: zyklische Gruppen sind abelsch.

Satz

Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^1, g^2, g^3, \dots, g^n\}$. **Beweis**
Jedes $m \in \mathbb{Z}$ lässt sich schreiben als $m = kn + l$ mit $0 \leq l < n$ (Teilen mit Rest), also $g^m = \underbrace{g^{kn}}_{=e} \cdot g^l = g^l$.

Es folgt $G \subseteq \{g, g^2, \dots, g^n\}$, $g^n = g^0$. Ist $g^k = g^l$ für $0 \leq k \leq l < n$, so gilt $e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen $l < n$), also $\#\{g, g^2, \dots, g^n = g^0\} = n$. \square

Folgerung

Ist G endlich mit $\#G = n$ und ist $h \in G$ mit $O(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann G eine zyklische Gruppe. \square

1.13 Nebenklassen

Sei G eine Gruppe und sei H eine Untergruppe. Sei $a \in G$. Wir definieren:

$$aH = \{ah \mid h \in H\} \subseteq G$$

$$Ha = \{ha \mid h \in H\} \subseteq G$$

Man nennt aH die **Linksnebenklassen** von a bzgl. H (und Ha die **Rechtsnebenklassen**). In nicht abelschen Gruppen gilt im allgemeinen $aH \neq Ha$.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G und $a, b \in G$.
Dann sind äquivalent:

- (i) $b \in aH$
- (ii) $bH = aH$
- (iii) $bH \cap aH \neq \emptyset$

Beweis

(i) \Rightarrow (ii) : $b \in aH \Rightarrow b = ah$ für ein $h \in H \Rightarrow bH = \{ahh' | h' \in H\} \stackrel{H \text{ Untergruppe}}{=} \{ah'' | h'' \in H\} = aH$

(ii) \Rightarrow (iii) : klar

(iii) \Rightarrow (i) : Sei $g \in bH \cap aH$, $g = bh = ah' \Rightarrow b = ah'h^{-1} \in aH$, da H Untergruppe

□

Folgerung

Jedes $g \in G$ liegt in genau einer Linksnebenklasse bzgl. H , nämlich $g \in gH$. Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt:

$G/H = \{gH \mid g \in G\}$ Menge der Linksnebenklasse, Rechtsnebenklassen analog.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G , sei $a \in G$.
Dann ist die Abbildung $H \rightarrow gH, h \mapsto gH$ bijektiv.

Beweis

SSurjektiv ist klar nach Definition von gH . Angenommen, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$

□

1.14 Satz von Lagrange

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wenn zwei der drei Mengen $G, H, G/H$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt:

$$\#G = \#H \cdot \#G/H$$

Insbesondere ist dann $\#H$ eine **Teiler** von $\#G$.

Beweis

Wenn G endlich ist, dann sind auch H und G/H endlich.

Angenommen, G/H und H sind endlich. Dann ist auch $G = \bigcup G/H = \bigcup \{gH \mid gH \in G/H\}$ endlich, da $\#gH = \#H$ nach 1.13.

Jetzt zählen wir genauer: sei $\#G/H = m$; $\#H = n$ etwa $G/H = \{g_1H, g_2H, \dots, g_mH\}$.

$g_iH \stackrel{1.13}{=} n$ $g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach 1.13.

$G = g_1H \cup g_2H \cup \dots \cup g_mH \Rightarrow \#G = m \cdot n$

□

Bem

- (1) Eine entsprechende Aussage gilt für Rechtsnebenklassen.
- (2) Die Abbildung $G \rightarrow G, g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} \stackrel{\text{Achtung!}}{=} \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1} \quad (\text{ÜA})$$

Korollar A (Lagrange)

Sei G eine endliche Gruppe und sei $g \in G$. Dann teilt $o(g)$ die Zahl $\#G$.

Beweis

Da G endlich ist, folgt $o(g) < \infty$. Nach dem Satz von Lagrange ist $\# \langle g \rangle = o(g)$ ein Teiler von $\#G$. \square

Korollar B

Sei G eine endliche Gruppe, sei p eine **Primzahl** (d.h. die einzigen Teiler von p sind 1 und p) und $p > 1$. Wenn gilt $\#G = p$, dann ist G zyklisch. Für jedes $g \in G \setminus \{e\}$ gilt $\langle g \rangle = G$.

Beweis

Sei $g \in G \setminus \{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt p . Es folgt $o(g) = p$, also $G = \langle g \rangle$ vgl. 1.12. \square

Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.

Die Zahl $\#G/H := [G : H]$ nennt man auch den **Index von H in G**.

Wichtige Rechenregeln in Gruppen

- (a) Man darf kürzen

$$ax = ay \Rightarrow x = y$$

$$xa = ya \Rightarrow x = y$$

(multipliziere beide Seiten von links/rechts mit a^{-1})

- (b) Es gilt $(x^{-1})^{-1} = x$ ($x^{-1}x = e = xx^{-1} \Rightarrow (x^{-1})^{-1} = x$)

- (c) Beim Invertieren darf die Reihenfolge umgedreht werden:

$$(ab)^{-1} = b^{-1}a^{-1} \quad (ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab \Rightarrow (ab)^{-1} = b^{-1}a^{-1}) \quad (\text{in abelschen Gruppen gilt natürlich damit } (ab)^{-1} = a^{-1}b^{-1})$$

1.15 Homomorphismen

Seien G, K Gruppen. Eine Abbildung $\varphi : G \rightarrow K$ heißt **(Gruppen-)Homomorphismus**, wenn $\forall x, y \in G$ gilt

$$\varphi \underbrace{(x \cdot y)}_{\text{Verknüpfung in } G} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verknüpfung in } K}$$

Bsp

- (a) $\text{id}_G : G \rightarrow G$ ist Homomorphismus
- (b) $H \subseteq G$ Untergruppe $i : H \hookrightarrow G, h \mapsto h$ Inklusion, ist Homomorphismus.
- (c) $(G, \cdot) = (\mathbb{Z}, +)$ $m \in \mathbb{Z}$ $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto mx$ ist Homomorphismus, denn $\phi(x + y) = m(x + y) = mx + my = \varphi(x) + \varphi(y)$
- (d) G Gruppe, $a \in G, a \neq e, \lambda_a(x) = ax$.
 $\lambda : G \rightarrow G$ ist kein Homomorphismus, denn $\lambda_a(e) = a, \lambda(ee) = a$, aber $\lambda_a(e)\lambda_a(e) = aa \neq a$

Lemma

Sei $\varphi : G \rightarrow K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1} \forall x \in G$. (e_G Neutralelement in G und e_K Neutralelement in K)

Beweis

$$\begin{aligned}\varphi(e_G) &= \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \xrightarrow{\text{kürzen}} e_K = \varphi(e_G) \\ e_K &= \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})\end{aligned}$$

□

Achtung: $\varphi(x)^{-1}$ ist das Inverse in K von $\varphi(x)$ nicht die Umkehrabbildung!

Das **Bild** eines Homomorphismus $\varphi : G \rightarrow K$ ist $\varphi(G) \subseteq K$,
der **Kern** ist $\ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\} \subseteq G$

1.16 Satz 1

Bild und Kern von Gruppenhomomorphismen sind Untergruppen.

Beweis

Setze $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ gilt $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist H Untergruppe.

Index

Die Seitenzahlen sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar!

abelsch, 2

Bild, 7

Eponent, 4

Gruppe, 1

Unter-, 3

symmetrische , 2

zyklische , 4

Homomorphismus

Gruppen-, 6

Index von H in G , 6

Kern, 7

Monoid, 2

Nebenklassen

Links-, 4

Rechts-, 4

Ordnung, 4

Primzahl, 6

Satz von Lagrange, 5

Teiler, 5

Verknüpfung, 1

zentralisiert, 2

zyklisch, 4

Abbildungsverzeichnis