

Algebra Script

RWTH Aachen

Melkonian Dmytro

14 October 2018

Contents

Chapter 1

Gruppen, Ringe, Körper

Definition 1.1. (Gruppe) Eine **Gruppe** ist eine nicht-leere Menge G versehen mit einer inneren Verknüpfung $G \times G \rightarrow G, (a, b) \mapsto a \cdot b$, die folgende Axiomen genügt:

1. **Asoziativität** $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. **neutrales Element** $\exists e \in G : \forall a \in G : a \cdot e = e \cdot a$
3. **inverses Element** $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

Die Gruppe G heisst **kommutativ** (oder **abelsch**), falls

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

Beispiel 1.1.1. $(\mathbb{Z}, +)$

- G1: $(a + b) + c = a + (b + c)$
- G2: $e = 0 : 0 + a = a + 0 = a$
- G3: $a^{-1} = -a : (-a) + a = a + (-a) = 0$
- G4: $a + b = b + a$

$\forall a, b, c \in \mathbb{Z}$

Beispiel 1.1.2. $(S_m, \circ) \sigma_1 \circ \sigma_2 : \{1, \dots, m\} \rightarrow \{1, \dots, m\}$
 $S_m = \{\sigma : \{1, \dots, m\} \rightarrow \{1, \dots, m\} \mid \sigma - \text{Bijektiv}\}$

- G2: $e = id = \begin{pmatrix} 1, \dots, m \\ 1, \dots, m \end{pmatrix} = (1)(2), \dots, (m)$
- G3: Sei $\sigma \in S_m : \sigma \circ \sigma^{-1} = e = \sigma^{-1} \circ \sigma$
- G4: $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$

Satz 1.2. Eine Gruppe hat die folgenden Eigenschaften:

1. Das neutrale Element e ist eindeutig bestimmt.
2. Das inverse Element zu a in G ist eindeutig bestimmt.
3. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ für alle $a, b \in G$.
4. Für alle $a, b \in G$ hat die Gleichung $a \cdot x = b$ eine eindeutige Lösung in G . Die Gleichung $y \cdot a = b$ hat eindeutige Lösung in G . Es gilt $x = a^{-1} \cdot b$ und $y = b \cdot a^{-1}$.

Proof. Sei G - Gruppe

1. Angenommen $\exists e_1, e_2 \in G$ - Neutralelemente

$$\implies e_1 = e_1 \circ e_2 = e_2 \iff e_1 = e_2$$

2. Angenommen $\exists a_1, a_2$ sind inverse Elemente zu $a \in G$

$$\implies a_1 = a_1 \circ e = a_1 \circ (a \circ a_2) = (a_1 \circ a) \circ a_2 = e \circ a_2 = a_2 \iff a_1 = a_2$$

- 3.

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ ((a^{-1} \circ a) \circ b) = b^{-1} \circ (e \circ b) = b^{-1} \circ b = e$$

■

Definition 1.3. (Gruppenhomomorphismus) Sei $\phi : G_1 \rightarrow G_2$ eine Abbildung zwischen zwei Gruppen. Dann heisst ϕ **Gruppenhomomorphismus** falls für alle $g_1, g_2 \in G_1$:

$$\phi(g_1 \cdot_{G_1} g_2) = \phi(g_1) \cdot_{G_2} \phi(g_2)$$

Der **Kern** von ϕ ist die Menge

$$Ker(\phi) := \{g \in G_1 | \phi(g) = e_{G_2}\}$$

Ein bijektiver (resp. surjektiver bzw. injektiver) Gruppenhomomorphismus heisst **Isomorphismus** (resp. **Epimorphismus** bzw. **Monomorphismus**).

Beispiel 1.3.1. $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$

$$x \mapsto e^x = \exp(x)$$

$$\exp(x + y) = \exp(x)\exp(y)$$

Satz 1.4. Sei $\phi : G_1 \rightarrow G_2$ ein Gruppenhomomorphismus, dann gelten:

1. $\phi(e_1) = e_2$
2. $\phi(a^{-1}) = (\phi(a))^{-1}$ für alle $a \in G_1$.
3. Sei $\psi : G_2 \rightarrow G_3$ ein weiterer Gruppenhomomorphismus, dann ist auch $\psi \circ \phi : G_1 \rightarrow G_3$ ein Gruppenhomomorphismus.

Proof. 1. $(\phi(e_1) = e_2)$ Sei $a \in G_1$, dann

$$\begin{aligned}\phi(a) &= \phi(a \cdot e_1) = \phi(a) \cdot \phi(e_1) \\ \phi(a)^{-1} \cdot \phi(a) &= \phi(a)^{-1} \cdot \phi(a) \cdot \phi(e_1) \\ e_2 &= e_2 \cdot \phi(e_1) = \phi(e_1)\end{aligned}$$

2. $(\phi(a^{-1}) = (\phi(a))^{-1})$ für alle $a \in G_1$

$$\begin{aligned}e_2 &= \phi(e_1) = \phi(a \cdot a^{-1}) = \phi(a) \cdot \phi(a^{-1}) \\ \implies \phi(a^{-1}) &\text{ ist das inverse zu } \phi(a)\end{aligned}$$

■

Definition 1.5. (Untergruppe) Eine Teilmenge H von G heisst **Untergruppe** von G , wenn folgende Axiome erfüllt sind:

1. $a, b \in H \implies a \cdot b \in H$ (abgeschlossen unter \cdot).
2. $e \in H$.
3. $a \in H \implies a^{-1} \in H$.

Beispiel 1.5.1. $(\mathbb{Z}, +)$

$$\begin{aligned}m\mathbb{Z} &= \{a \in \mathbb{Z} | a = lm : l \in \mathbb{Z}\} \\ 3\mathbb{Z} &= \{0, \pm 3, \pm 6, \dots\}\end{aligned}$$

Behauptung: $(m\mathbb{Z}, +) \subset (\mathbb{Z}, +)$ - Untergruppe

- u1: $a_1 = l_1 m = a_2 = l_2 m \implies a_1 + a_2 = l_1 m + l_2 m = (l_1 + l_2)m$
- u2: $0 \in m\mathbb{Z}$, da $0 = 0 \cdot m$
- u3: Sei $a = lm \in m\mathbb{Z} \implies -a = (-l)m \in \mathbb{Z}$

Beispiel 1.5.2.

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

$$(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$$

Beispiel 1.5.3.

$$(S_m, \circ) \supseteq (S_{m-1}, \circ)$$

Satz 1.6. Es sei $\phi : G_1 \rightarrow G_2$ ein Gruppenhomomorphismus.

1. $\ker(\phi)$ ist eine Untergruppe von G_1 .
2. $\text{Im}(\phi)$ ist eine Untergruppe von G_2 .
3. ϕ ist injektiv $\iff \ker(\phi) = \{e_1\}$.

Proof. 1. ($\ker(\phi)$ ist eine Untergruppe von G_1) Seien $a, b \in \ker(\phi)$

- u1: D.h. $\phi(a) = e_2 = \phi(b)$

$$\implies \phi(a \cdot b) = \phi(a) \cdot \phi(b) = e_2 \cdot e_2 = e_2$$

- u2: zz $e_1 \in \ker(\phi)$. Gilt $\phi(e_1) = e_2$.
- u3: Sei $a \in \ker(\phi)$. D.h. $\phi(a) = e_2$

$$\phi(a^{-1}) = (\phi(a))^{-1} = e_2^{-1} = e_2$$

2. ($\text{Im}(\phi)$ ist eine Untergruppe von G_2)

- u1: Das Bild von ϕ .

$$\text{Im}(\phi) = \{x \in G_2 \mid \exists a \in G_1 : \phi(a) = x\}$$

Seien $x, y \in \text{Im}(\phi)$. D.h.

$$\begin{aligned} & \exists a_1, a_2 \in G_1 : \phi(a_1) = x, \phi(a_2) = y \\ \implies & x \cdot y = \phi(a_1) \cdot \phi(a_2) = \phi(a_1 \cdot a_2) \\ \implies & x \cdot y \in \text{Im}(\phi) \end{aligned}$$

3. (ϕ ist injektiv $\iff \ker(\phi) = \{e_1\}$) Sei ϕ -injektiv

$$\implies (\phi(a) = \phi(b) \implies a = b)$$

$$\text{Sei } a \in \ker(\phi) \implies \phi(a) = e_2 = \phi(e_1) \implies a = e_1$$

$$\text{Sei } \ker(\phi) = \{e_1\}$$

Angenommen $\phi(a) = \phi(b)$

$$\implies \phi(a) \cdot \phi(b)^{-1} = e_2 \iff \phi(a \cdot b^{-1}) = e_2$$

$$\implies a \cdot b^{-1} = e_1 \iff a = b$$

■

Remark. Sei G eine Gruppe, H eine Untergruppe von G . Für $g_1, g_2 \in G$ definieren wir

$$g_1 \equiv g_2 \pmod{H} : \iff g_1(g_2)^{-1} \in H$$

Wir sagen, dass g_1 **kongruent zu g_2 modulo H** ist.

Satz 1.7. Die Kongruenz modulo H ist eine Äquivalenzrelation. Wir schreiben $G \setminus H$ für Menge der Äquivalenzklassen.

Satz 1.8. Sei G eine abelsche Gruppe. Dann ist $G \setminus H$ eine abelsche Gruppe mit der Verknüpfung

$$+ : G \setminus H \times G \setminus H, ([g_1], [g_2]) \mapsto [g_1] + [g_2] := [g_1 + g_2]$$

Lemma 1.9. Sei G eine abelsche Gruppe, $H \subseteq G$ eine Untergruppe. Die Abbildung

$$\pi : G \rightarrow G \setminus H, g \mapsto [g]$$

ist ein surjektiver Gruppenhomomorphismus mit $\ker(\pi) = H$

Folgerung 1.9.1. $\mathbb{Z} \setminus m\mathbb{Z}$ ist eine abelsche Gruppe für jedes $m \in \mathbb{Z}$ und besteht aus m paarweise verschiedene Restklassen.

Definition 1.10. (Normalteiler) Eine Untergruppe $N \subseteq G$ heisst **Normalteiler** von G falls für alle $g \in G$ gilt:

$$\{g \cdot n | n \in N\} =: gN = Ng := \{n \cdot g | n \in N\}$$

Satz 1.11. Sei N ein Normalteiler von G , dann ist $G \setminus N$ mit obiger Verknüpfung eine Gruppe.

Satz 1.12. Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus, dann gilt

1. $\ker \varphi$ ist ein Normalteiler von G
2. φ induziert einen Isomorphismus von Gruppen $\bar{\varphi} : G \setminus \ker \varphi \rightarrow \text{Im}(\varphi), [g] \mapsto \varphi(g)$

Definition 1.13. (Ring) Ein **Ring** ist eine Menge R mit zwei inneren Verknüpfungen $+, \cdot$ so, dass $(R, +)$ eine abelsche Gruppe ist und \cdot eine assoziative Verknüpfung für R mit einem neutrales Element (**Einselement**) ist. Es sollen für alle $a, b, c \in R$ gelten:

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(b + c) \cdot a = b \cdot a + c \cdot a$

Remark. Ein Ring R heisst **kommutativ**, falls $\forall a, b \in R$ gilt: $a \cdot b = b \cdot a$. Das neutrale Element bezüglich der Addition $+$ bezeichnen wir mit 0 und das Inverse von a mit $-a$. Wir schreiben $a - b$ für $a + (-b)$. Der Einselement der Multiplikation bezeichnen wir mit 1 .

Definition 1.14. (Körper) Ein **Körper** ist ein kommutativer Ring K so, dass $K \setminus \{0\}$ mit der Multiplikation als Verknüpfung eine Gruppe ist. Insbesondere ist $0 \neq 1$.

Remark. Es gelten folgende Rechenregeln für alle $a, b, c \in R$:

1. $a \cdot 0 = 0 \cdot a = 0$
2. Das Einselement ist eindeutig. Wenn $1 = 0$, dann ist $R = \{0\}$
3. $-a = (-1) \cdot a$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$ und $(b - c) \cdot a = b \cdot a - c \cdot a$

Definition 1.15. (Ringhomomorphismus) Es seien R und S zwei Ringe und $\varphi : R \rightarrow S$ eine Abbildung. Dann heisst φ ein **Ringhomomorphismus** falls für alle $a, b, c \in R$ gilt

$$\varphi(a \cdot b + c) = \varphi(a) \cdot \varphi(b) + \varphi(c) \text{ und } \varphi(1_R) = \varphi(1_S)$$

Satz 1.16. $\mathbb{Z} \setminus m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Definition 1.17. (Polynom) Ein **Polynom** ist eine Folge $(a_i)_{i \in \mathbb{N}_0}$ von Elementen aus K , so dass nur endlich viele $a_i \neq 0$. Wir definieren $x := (\delta_{i,1})_{i \in \mathbb{N}_0}$. Die Menge aller Polynome mit Koeffizienten in K bezeichnen wir als $K[x]$.

Remark. Zwei Polynome $(a_i)_{i \in \mathbb{N}_0}$ und $(b_i)_{i \in \mathbb{N}_0}$ sind per Definition gleich, wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$.

Satz 1.18. Mit den Operation $+$ und \cdot wird $K[x]$ zu einem kommutativen Ring.

Proof. Für ein Polynom $(a_i)_{i \in \mathbb{N}_0} \in K[x]$ gilt

$$(a_i)_{i \in \mathbb{N}_0} = \sum_{i \in \mathbb{N}_0} a_i x^i$$

Dann ist $+$ (bzw. \cdot) die übliche Addition (bzw. Multiplikation) von Polynomen. ■

Definition 1.19. (Leitkoeffizienten und Grad) Es sei $p = \sum_{i \in \mathbb{N}_0} a_i x^i \in K[x]$ und m maximal mit $a_m \neq 0$. Dann heisst a_m der **Leitkoeffizient** von p . In diesem Fall definieren wir den **Grad** von p als $\deg p = m$. Konvention: $\deg(0)_{i \in \mathbb{N}_0} = -\infty$.

Satz 1.20. Sei $\alpha \in K$ gegeben, dann ist die Abbildung

$$\pi_\alpha : K[x] \rightarrow K; p \mapsto p(\alpha) := \sum_{i \in \mathbb{N}_0} a_i \alpha^i$$

ein Ringhomomorphismus, der **Einsetzungshomomorphismus**.

Definition 1.21. (Nullstelle von Polynome) Sei $\alpha \in K$ gegeben. Dann heisst α eine **Nullstelle** von $p \in K[x]$ falls $\pi_\alpha(p) = p(\alpha) = 0$.

Satz 1.22. Für Polynome $p, q \in K[x]$ gilt:

1. $\deg(p + q) \leq \max \deg p, \deg q$. Falls $\deg p \neq \deg q$, dann gilt $=$.
2. $\deg(p \cdot q) = \deg p + \deg q$.

Folgerung 1.22.1. Im Ring $K[x]$ gilt die Kürzungsregel

$$p \cdot q = p \cdot r \wedge p \neq 0 \implies q = r$$

und er ist **nullteilerfrei**

$$p \cdot q = 0 \implies p = 0 \vee q = 0$$

Theorem 1.23. (Polynomdivision) Für $p, q \in K[x]$ mit $q \neq 0$ gibt es eindeutige $a, b \in K[x]$ mit

$$p = a \cdot q + b \wedge \deg b < \deg q$$

Folgerung 1.23.1. Sei $\alpha \in K$ eine Nullstelle von $p \in K[x]$. Dann $\exists! q \in K[x]$ mit $\deg q = \deg p - 1$ und

$$p = (x - \alpha) \cdot q$$

Folgerung 1.23.2. Sei $p \in K[x]$ ein Polynom vom Grad m . Dann hat p höchstens m paarweise verschiedene Nullstellen.

Chapter 2

Matrizen und Lineare Gleichungen

Definition 2.1. (Lineares Gleichungssystem) Es sei K ein Körper, $m, n \in \mathbb{N}$, $a_{ij}, b_i \in K$. Dann nennt man

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \dots & + & a_{m,n}x_n & = & b_m \end{array}$$

ein **lineares Gleichungssystem (LGS)**, wobei die Menge aller $(x_1, \dots, x_n) \in K^n$ gesucht ist, die alle Gleichungen erfüllen.

Definition 2.2. (Matrix) Etwas kompakter: Für $n, m \in \mathbb{N}$ und $a_{ij} \in K$, nennt man

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

eine $m \times n$ -**Matrix**, die Zahlen a_{ij} heissen **Einträge** oder **Elemente** der Matrix.

Definition 2.3. (Operationen mit Matrizen) Die Menge aller $m \times n$ -Matrizen mit Einträgen in K bezeichnen wir mit $M_{m,n}(K)$.

1. Es seien $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}, B = (b_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in M_{m,n}(K)$. Dann definieren wir $A + B \in M_{m,n}(K)$ durch

$$(A + B) := C = (c_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \text{ wobei } c_{ij} := a_{ij} + b_{ij}.$$

2. Es seien $A \in M_{m,n}(K)$ und $B \in M_{n,\ell}(K)$. Dann definieren wir $A \cdot B \in M_{m,\ell}(K)$ durch

$$(A \cdot B) := C = (c_{ij})_{1 \leq i \leq m, 1 \leq j \leq \ell} \text{ wobei } c_{ij} := \sum_{k=1}^n a_{ik} b_{kj}.$$

Definition 2.4. Das lineare Gleichungssystem $Ax = b$ heisst **homogen**, falls $b = 0$, ansonsten heisst es **inhomogen**

Remark. Jedes homogene LGS besitzt immer die **triviale Lösung** $x = 0$. Wir suchen also vor allem Lösungen $x \neq 0$.

Für ein LGS $Ax = b$ betrachten wir die **erweiterte Koeffizientenmatrix** $(A|b)$:

$$(A|b) = \left(\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{array} \right)$$

Definition 2.5. (Gaussalgorithmus) **Bestandteil des Gaussalgorithmus:**

1. Vorwärtselimination (\rightarrow erreiche **Zeilenstufenform**)
2. Lösbarkeitsentscheidung
3. Rückwärtssubstitution (\rightarrow Unterscheidung **freie und abhängige Variable**)

Zeilenstufenform: Eine Matrix $A \in M_{m,n}(K)$ ist in Zeilenstufenform, wenn es eine Zahl $0 \leq r \leq m$ gibt, so dass

- in den ersten r -Zeilen jeweils nicht nur Nullen stehen und in den Zeilen $r + 1$ bis m nur Nullen stehen
- $j_1 < j_2 < \dots < j_r$ wobei für $1 \leq i \leq r, j_i$ den minimale Index, so dass $a_{i,j_i} \neq 0$ ist.

Satz 2.6. Der Gaußalgorithm liefert nach endlich vielen Schritten entweder alle Lösungen des inhomogenen LGS oder endet mit einer negativen Entscheidung über Lösbarkeit des LGS.

Es sei G eine abelsche Gruppe, dann ist G^n auch eine abelsche Gruppe.

Definition 2.7. Es sei $\text{End}(G^n) = \{f : G^n \rightarrow G^n \mid f \text{ ist Gruppenhomomorphismus} \}$. Wir definieren

$$+ : \text{End}(G^n) \times \text{End}(G^n) \rightarrow \text{End}(G^n), (f_1, f_2) \mapsto (\underline{g} \mapsto f_1(\underline{g}) + f_2(\underline{g}))$$

und

$$\circ : \text{End}(G^n) \times \text{End}(G^n) \rightarrow \text{End}(G^n), (f_1, f_2) \mapsto (\underline{g} \mapsto f_1(\underline{g})f_2(\underline{g}))$$

Satz 2.8. $\text{End}(G^n)$ ist ein Ring.

Satz 2.9. Die Menge $M_{n,n}(K)$ mit Addition und Multiplikation bildet einen Ring.