Algebra für LAK

Sommersemester 2015

Mitschrift von:
Sarah Zloklikovits

Vorlesung von:
Günther Hörmann

Inhaltsverzeichnis

Einleitung

Algebraische Strukturen, die wir schon kennen (sollten)

Halbgruppe $(\mathbb{N}, +)$: $\mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto m + n \in \mathbb{N}$

Eigenschaften:

- assoziativ: $(k + l) + m = k + (l + m)$
- kommutativ: $m + n = n + m$

Gruppe $(\mathbb{Z}, +)$: $\mathbb{N} \subseteq \mathbb{Z}$, neutrales Element 0: $m + 0 = 0 + m = m$.

Zu $m \in \mathbb{Z}$ gibt es ein additives Inverses $-m \in \mathbb{Z}$, $\underbrace{m + (-m)}_{\text{Schreibeweise } m-m} = (-m) + m = 0$

$+$ ist auch kommutativ: $m + n = n + m$

Ring $(\mathbb{Z}, +, \cdot)$:
Distributivgesetz: $k \cdot (l + m) = k \cdot l + k \cdot m$
multiplikativ neutrales Element: $1 : 1 \cdot k = k \cdot 1 = k$
Multiplikation ist auch kommutativ: $k \cdot l = l \cdot k$

Restklassenringe $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\} = \mathbb{Z}/m \cdot \mathbb{Z}$
$\overline{k} = \{k + m \cdot z | z \in \mathbb{Z}\} = k + m \cdot \mathbb{Z}$
$\overline{k} + \overline{l} := \overline{k + l}$, $\overline{k} \cdot \overline{l} := \overline{k \cdot l}$, $\overline{0}$...neutrales Element bzgl. $+$, $\overline{1}$...neutrales Element bzgl. $\cdot$

Bemerkung: Sei p eine Primzahl $\Rightarrow \mathbb{Z}_p$ ist Körper, $\forall\, \overline{l} \in \mathbb{Z}_p : \exists!\, \overline{k} \in \mathbb{Z}_p : \overline{l} \cdot \overline{k} = \overline{k} \cdot \overline{l} = \overline{1}$

Körper: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
$\mathbb{Q}$ erweitert $\mathbb{Z}$ so, dass jedes $z \in \mathbb{Z}, z \neq 0$, ein multiplikatives Inverses $\frac{1}{z} \in \mathbb{Q}$ hat.

$\mathbb{R}$ erweitert $\mathbb{Q}$ so, dass „keine Lücken auf der Zahlengeraden bleiben“; bedeutet: $\mathbb{R}$ ist vollständig.

$\mathbb{C}$ erweitert $\mathbb{R}$ so, dass jedes Polynom mit reellen (oder komplexen) Koeffizienten eine Nullstelle besitzt, z.B. x^2+1 hat Nullstelle bei $\pm i \in \mathbb{C}/\mathbb{R}$

Permutationsgruppen: $M = \{1, ..., n\}$
$S_n := \{f : M \to M | f \text{ bijektiv}\}$
$f \circ g \in S_n$ für $f, g \in S_n$ (Verknüpfung bijektiver Abbildungen sind bijektiv).

Diese Verknüpfung ist assoziativ, auch die Inverse f^{-1} ist bijektiv und
$f \circ f^{-1} = f^{-1} \circ f = id$. $(S_n, \circ)$ ist eine Gruppe mit $n!$ Elementen.

Notation:

$$f \hat{=} \begin{pmatrix} 1 & . & . & . & n \\ f(1) & . & . & . & f(n) \end{pmatrix}$$

Verknüpfung „von rechts nach links“.

Beispiel:

$$\begin{pmatrix} 1 & 2 & 3 \\ & \downarrow & \\ 3 & \underline{1} & 2 \end{pmatrix} \circ \begin{pmatrix} \underline{1} & 2 & 3 \\ \downarrow & & \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \underline{1} & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ & & \downarrow \\ 2 & 1 & \underline{3} \end{pmatrix} \circ \begin{pmatrix} \underline{1} & 2 & 3 \\ \downarrow & & \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \underline{3} & 2 & 1 \end{pmatrix}$$

$\rightarrow$ stimmen nicht überein weil nicht kommutativ!

Ringe von Matrizen/ lineare Abbildungen:
$(M(n, \mathbb{R}), +, \cdot)$ für $n \geq 2$ nichtkommutativer Ring; I_n...multiplikatives neutrales Element.

V Vektorraum über $\mathbb{R}, L(V) := \{f : V \to V | f \ \mathbb{R}-\text{linear}\}$
dim $V \geq 2$: Multiplikation (=Verknüpfung von Abbildungen) nicht kommutativ.
id_V...multiplikativ neutral

Klassische Fragen der Algebra (und Geometrie)

(A) Auflösung von Polynomgleichungen, Nullstellen

$p, q \in \mathbb{R} : x^2 + p \cdot c + q = 0$
Formel für Nullstellen: $x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \quad \in \mathbb{C}$.
(geometrisch bekannt schon seit ca. 1700 v. Chr., algebraisch seit ca. 800 n.Chr.)

16. Jahrhundert: Formel für Polynome von Grad 3 und 4

Abel 1826: für allgemeine Polynome vom Grad ≥ 5 gibt es keine solcher Auflösungsformel mit Wurzeln - es gibt Mehtoden mittels Strukturen von Gruppen, Ringen und Körpern.

(B) Konstruierbarkeit mit Zirkel und Lineal

Folgende Fragestellungen sind mit Theorie der Körpererweiterung negativ entschieden worden:

1. Deli'sches Problem der Würfelverdopplung
2. Winkeldreiteilung
3. Quadratur des Kreises: beruht auf der Transzendenz von π (Lindemann 1882), d.h. es gibt kein Polynom $p(x) = a_m x^m + a_{m-1} x^{m-1} + ... + a_0$ mit rationalen Koeffizienten $a_0, a_1, ..., a_m$, sodass $p(\pi) = 0$ gelten kann.

„Moderne Algebra“ - Studium der algebraischen Strukturen und deren Anwendungen - axiomatisches Gerüst, daher Musterbeispiel einer (mathematischen) Theorie.

Teil I

Gruppen

Kapitel 1

Gruppenaxiome, Untergruppen, Beispiele

1.1 Halbgruppen

Sei M eine Menge - eine **(innere) Verknüpfung** auf der Menge M ist eine Abbildung $* : M \times M \to M, \quad (a, b) \mapsto a * b$

$*$ heißt **assoziativ**, wenn $(a * b) * c = a * (b * c) \quad \forall a, b, c \in M$
$*$ heißt **kommutativ**, falls $a * b = b * a \quad \forall a, b \in M$

Definition:

1. Eine Menge H zusammen mit einer assoziativen Verknüfpung $*$ darauf heißt **Halbgruppe** $(H, *)$
2. Sei $(H, *)$ Halbgruppe. Ein Element $e \in H$ heißt **neutral** (bzgl. $*$), falls

$$a = a * e = e * a \quad \forall a \in H$$

.
(e heißt **linksneutral**, falls $e*a = a \; \forall a \in H$ gilt; analog **rechtsneutral**, falls $a*e = a$ gilt.)

„Sätzchen“: Ein neutrales Element ist eindeutig.

„Beweischen“: Seien e und e' neutral in $(H, *)$, dann folgt $e = e * e' = e' \; \square$

Beispiele:

1. $\mathbb{N} = \{0, 1, 2, ...\}$.
   $(\mathbb{N}, +)$ kommutative Halbgruppe, 0 neutral
   $(\mathbb{N}, \cdot)$ kommutative Halbgruppe, 1 neutral

2. M $\neq \emptyset$, $H := \{f : M \to M\}$ mit Verknüpfung von Abbildung:

$$(f \circ g)(x) = f(g(x)), \quad f, g \in H, x \in M$$

   $f \circ (g \circ h) = (f \circ g) \circ h$
   $id_M : M \to M, x \mapsto x$...identische Abbildung. Diese ist neutral, denn
   $(f \circ id_M)(x) = f(id_M(x)) = f(x)$ und $(id_M \circ f)(x) = id_m(f(x)) = f(x)\ \forall x \in M$
   Bemerkung: $|M| \geq 2 \Rightarrow (H, \circ)$ nicht kommutativ

3. $(M(n, \mathbb{R}), +)$ kommutative Halbgruppe; $(M(n, \mathbb{R}), \cdot)$ Halbgruppe, nicht kommutativ falls $n \geq 2$

1.2 Gruppen

Definition:

Eine Menge G mit Verknüpfung $* : G \times G \to G$ heißt **Gruppe**, wenn gilt:

(G1) $*$ ist assoziativ

(G2) a.) $\exists$ (eindeutiges) neutrales Element $e \in G$
b.) $\forall a \in G \quad \exists! b \in G : b * a = a * b = e$. b heißt **Inverses** zu a; wir schreiben $b = a^{-1}$.

(Falls (G1) und (G2.a) erfüllt sind, ist $(G, *)$ Halbgruppe mit neutralem Element e.)

G heißt **kommutative Gruppe** oder **abelsche Gruppe**, wenn $*$ kommutativ ist.

Schreibweisen oft $a \cdot b$ oder ab statt $a * b$; bei abelschen Gruppen $a + b$ statt $a * b$; neutrales Element bzgl. + wird meist mit 0 bezeichnet, bzgl. Multiplikation mit 1. Additiv Inverses zu a wird meist mit -a notiert.

Bemerkung:

(i) durch Induktion: Assoziativität für endlich viele Faktoren, d.h. $a_1 * a_2 * ... * a_n$ sinnvoll definiert und unabhängig von Klammerung.

(ii) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, denn: $(a \cdot b)(b^{-1} \cdot a^{-1}) = a(\underbrace{b \cdot b^{-1}}_{=e})a^{-1} = a \cdot a^{-1} = e$ und
$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$

Lemma: Beim Nachweis der Gruppeneigenschaften genügt es, statt **(G2)** die folgende Version zu zeigen:

(G2') $\exists e \in G$ mit Eigenschaften:

(a) $e * a = a \quad \forall a \in G$ (e linksneutral)

(b) $\forall a \in G \quad \exists b \in G : b * a = e$ (Linksinverses)

d.h. aus (G1) und (G2') folgt (G2).

Beweis:

1. Schritt: Jedes Linksinverses ist auch Rechtsinverses:
Sei b linksinvers zu a, d.h. $b \cdot a = e$, und sei c linksinvers zu b, d.h. $c \cdot b = e$, dann folgt

$$\underline{a \cdot b} = (ea)b = ((cb)a)b = (c(ba))b = (ce)b = cb = \underline{e}$$

2. Schritt e linksneutral $\Rightarrow$ e rechtsneutral; insbesondere ist dann e wegen Sätzchen in 1.1. eindeutig. Sei $a \in G$ mit Linksinversem $b \in G$, d.h. $ba = e$; wegen 1. Schritt istauch $ab = e$; daher

$$\underline{ae} = a(ba) = (ab)a = ea = \underline{a}$$

3. Schritt: Linksinverses ist eindeutig (somit ebenso Rechtsinverses eindeutig):
Seien b, b' linksinvers zu a, dann gilt

$$b = eb = (b'a)b = b'(ab) = b'e = b'$$

□

Beispiele:

1. $(\mathbb{Z}, +)$ abelsche Gruppe
2. $(\mathbb{Z}_m, +)$ abelsche Gruppe mit m Elementen
3. $(S_3, \circ)$ nichtabelsche Gruppe mit $3! = 6$ Elementen (-siehe Einleitung zur VO)

Satz: In einer Gruppe G sind für jedes $a \in G$ die Abbildungen $l_a : G \to G, x \mapsto a \cdot x$ (**Linkstranslation**) und $r_a : G \to G, x \mapsto x \cdot a$ (**Rechtstranslation**) bijektiv.
Insbesondere gelten die **Kürzungsregeln**:

$$\begin{aligned} ax &= ay \Rightarrow x = y, \\ xa &= ya \Rightarrow x = y. \end{aligned}$$

Beweis:

$$l_a(x) = b \Leftrightarrow ax = b \Leftrightarrow x = a^{-1}b$$

somit l_a injektiv ($\leftrightarrow$ x ist eindeutig) und surjektiv ($\leftrightarrow$ für jedes b lösbar).
Ebenso

$$r_a(x) = b \Leftrightarrow x \cdot a = b \Leftrightarrow x = ba^{-1}$$

$ax = ay$ bedeutet $l_a(x) = l_a(y)$, also $x = y$, weil l_a injektiv.
$xa = ya$ heißt $r_a(x) = r_a(y)$, also $x = y$.

□

1.3 Untergruppen

Definition:
Sei G eine Gruppe und $H \subseteq G$. Dann heißt H **Untergruppe** von G (wir schreiben $H < G$), falls gilt:

(U1) $a, b \in H \Rightarrow a \cdot b \in H$
(d.h. $(a, b) \mapsto a \cdot b$ ist eine Verknüpfung auf H, H ist „abgeschlossen“ unter $\cdot$).

(U2) $(H, \cdot)$ ist eine Grupe

Lemma: $H \subseteq G$ ist Untergruppe genau dann, wenn $H \neq \emptyset$ und $\forall a, b \in H : a \cdot b^{-1} \in H$.

Beweis:

$\boxed{\Rightarrow}$ Wenn H Untergruppe $\Rightarrow \exists e \in H \Rightarrow H \neq \emptyset$;
weiters $b^{-1} \in H$ und $ab^{-1} \in H$, weil $(H, \cdot)$ selbst Gruppe ist.

$\boxed{\Leftarrow}$
- Assoziativgesetz gilt in G, daher auch für alle Elemente von H
- $H \neq \emptyset \Rightarrow \exists a \in H$ weiters $a \cdot a^{-1} = e \in H$

- $b \in M \Rightarrow eb^{-1} = b^{-1} \in H$, also Inverse existiert in H
- H abgeschlossen unter $\cdot$, denn mit $a, b \in H$ ist $a \cdot b = a \cdot (b^{-1})^{-1} \in H$

□

Bemerkung:

(i) Die Untergruppe $\{e\}$ und G gibt es immer - das sind sogenannte **triviale Untergruppen**.

(ii) $H_1 < G$ und $H_2 < G \Rightarrow H_1 \cap H_2 < G$ (Beweis in UE, gilt auch für beliebig viele Untergruppen).

Satz: Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge.

$$\text{Erz}(M) := \{a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdot \cdots a_n^{\varepsilon_n} | n \in \mathbb{N}, a_i \in M, \varepsilon_i = \pm 1\}$$

(Menge aller endlichen Produkte von Elementen aus M und ihren Inversen) ist eine Untergruppe von G, die sogenannte **von M erzeugte Untergruppe**. $\text{Erz}(\emptyset) := \{e\}$ (bzw. n=0 oben).

Beweis:

Wegen $\{e\} \subseteq$ Erz(M) ist Erz(M)$\neq \emptyset$. Ist $a := a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n}, b := b_1^{\delta_1} \cdot \ldots \cdot b_m^{\delta_m} \in$ Erz(M), dann

$$ab^{-1} = a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \cdot b_m^{-\delta_m} \cdot \ldots \cdot b_1^{-\delta_1} = c_1^{\alpha_1} \cdot \ldots \cdot c_{n+m}^{\alpha_{n+m}}$$

mit $c_i = a_i \quad (1 \leq i \leq n)$, $c_j = b_{n+m+1-j} \quad (n+1 \leq j \leq n+m)$
$\alpha_i = \varepsilon_i, \quad \alpha_j = -\delta_{n+m+1-j}$.
also $a \cdot b^{-1} \in$ Erz(M); Lemma $\Rightarrow$ Erz(M) ist Untergruppe.

□

Bemerkung:

(iii) G abelsch, dann können gleiche Faktoren in Erz(M) immer zusammengeführt werden, z.B. $a \cdot b^{-1} \cdot a \cdot c = a^2 \cdot b^{-1} \cdot c$; somit

$$\text{Erz(M)} = \{a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} | n \in \mathbb{N}, k_i \in \mathbb{Z}\}$$

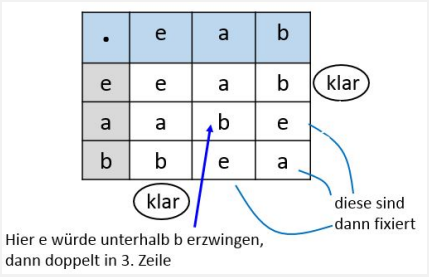
bzw. additiv geschrieben

$$\{k_1 \cdot a_1 + \ldots + k_n \cdot a_n | k_i \in \mathbb{Z}\}$$

(iv) Eine Gruppe G heißt **endlich erzeugt**, falls eine endliche Menge $M \subseteq G$ existiert mit $G = Erz(M)$. Falls $|M| = 1$ gilt heißt G **zyklisch** - dann ist $G = \{a^k | k \in \mathbb{Z}\}$.

Beispiele:

1. $\mathbb{Z} = Erz(\{1\})$, also ist es eine zyklische Gruppe
2. Endliche Gruppen können (im Prinzip) durch Gruppentafeln beschrieben werden: z.B. für 3 Elemente in jeder Zeile und Spalte muss jedes Element einmal vorkommen $\sim$ „algebraisches Sudoku“:



   $a^3 = e$, $G = Erz(a)$

3. V $\mathbb{K}$-Vektorraum

$$GL(V) := \{f : V \to V | \underbrace{\text{f linear und bijektiv}}_{\text{VR-Isomorphismus}}\}$$

   mit Verknüpfung $\circ$ von Abb. Verknüpfung linearer Abbildung ist linear, Assoziativgesetz gilt sowieso für alle Abbildungen bzgl. $\circ$.
   Neutrales Element ist id_V, Inverse einer bijetkiven linearen Abbildung ist linear.
   „**general linear group**“ (daher Gl...general linear)

   - für $V = \mathbb{R}^n$ ist GL(V) beschreibbar als $GL(n, \mathbb{R})$...invertierbare $n \times n$-Matrix über $\mathbb{R}$ mit Matrixmultiplikation. Neutrales Element ist $I_n = \begin{pmatrix} 1 & & \emptyset \\ & \ddots & \\ \emptyset & & 1 \end{pmatrix}$.
     Nichtkommutativ für $n \geq 2$.
   - analog $GL(n, \mathbb{C})$

4. $O(n) := \{A \in GL(n, \mathbb{R}) | A \cdot A^\dagger = I_n\} \underbrace{<}_{\text{Beweis in UE}} GL(n, \mathbb{R})$= **orthogonale Gruppe**
5. $(\mathbb{R}_+, \cdot)$ positive reelle Zahlen mit Multiplikation sind Gruppe
6. $S^1 := \{z \in \mathbb{C} : |z| = 1\}$ ist Untergruppe von $\mathbb{C}^* := \mathbb{C} \backslash \{0\}$ bzgl. Multiplikation

Kapitel 2

Homomorphismen und Normalteiler

2.1 Homomorphismen

(homo-morph kommt aus dem griechishen und bedeutet „gleichgestaltig“).

Definition:
Seien $(G, *)$ und $(G', *')$ Gruppen. $\varphi : G \to G'$ heißt **Homomorphismus**, wenn gilt:

$$\varphi(a * b) = \varphi(a) *' \varphi(b) \quad \forall a, b \in G$$

(„φ respektiert die Gruppenverknüpfungen“).

Ein bijektiver Homomorphismus heißt **Isomorphismus**, dann ist G **isomorph** mit G', wir schreiben $G \cong G'$.
Homomorphismen $G \to G$ werden auch **Endomorphismen** genannt, Isomorphismen $G \to G$ werden auch **Automorphismen** genannt.

Bild von φ...$Im(\varphi) := \varphi(G) \subseteq G'$

Kern von φ...$Ker(\varphi) := \{a \in G | \varphi(a) = e'\}$ (e' = neutrales Element in G').

Eigenschaften:

(a) $\varphi(e) = e'$

(b) $\forall a \in G : \varphi(a)^{-1} = \varphi(a^{-1})$

(c) $H < G \Rightarrow \varphi(H) < G'$

(d) $H' < G' \Rightarrow \underbrace{\varphi^{-1}(H')}_{\substack{\text{Urbildmenge} \\ \{a \in G | \varphi(a) \in H'\}}} < G$

(e) φ injektiv $\Leftrightarrow \mathrm{Ker}(\varphi) = \{e\}$

(f) φ Isomorphismus $\Rightarrow \varphi^{-1} : G' \to G$ Isomorphismus

(g) $\psi : G' \to G''$ weiterer Homomorphismus $\Rightarrow \psi \circ \varphi : G \to G''$ Homomorphismus.

Beweis:

(a) $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \overset{\text{Kürz.}}{\Rightarrow} \varphi(e) = e'$
Wieder Schreibweise vereinfacht zu $\varphi(a) \cdot \varphi(b)$ statt $\varphi(a) *' \varphi(b)$ etc.

(b) $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) \Rightarrow \varphi(a)^{-1} = \varphi(a^{-1})$

(c) $a',\ b' \in \varphi(H) \Rightarrow \exists a, b \in H : a' = \varphi(a), b' = \varphi(b)$
$\Rightarrow a' \cdot (b')^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(\underbrace{ab^{-1}}_{\in H}) \in \varphi(H)$
$[\varphi(e) \in \varphi(H) \Rightarrow \varphi(H) \neq \emptyset]$

(d) $a, b \in \varphi^{-1}(H') \Rightarrow \varphi(a), \varphi(b) \in H'$
$\Rightarrow \varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} \in H' \Rightarrow a \cdot b^{-1} \in \varphi^{-1}(H')$

(e) $\boxed{\Rightarrow:}$ $e \in \mathrm{Ker}(\varphi)$, weil $\varphi(e) = e'$; $\varphi(a) = e' = \varphi(e) \Rightarrow a = e$, weil φ injektiv ist.
$\boxed{\Leftarrow:}$ $a, b \in G$ mit $\varphi(a) = \varphi(b)$
$\Rightarrow \varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e' \Rightarrow ab^{-1} \in \mathrm{Ker}(\varphi) = \{e\} \Rightarrow a = b$; also ist φ injektiv.

(f)
- φ^{-1} Homomorphismus:
  $a', b' \in G' \Rightarrow \exists a, b \in G : a' = \varphi(a),\ b' = \varphi(b)$, daher auch
  $a = \varphi^{-1}(a'),\ b = \varphi^{-1}(b')$; somit

$$\underline{\varphi^{-1}(a'b')} = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b = \underline{\varphi^{-1}(a') \cdot \varphi^{-1}(b')}$$

- φ^{-1} bijektiv weil Inverse einer Abbildung φ.

(g) $a, b \in G$:

$$\underline{(\psi \circ \varphi)(a \cdot b)} = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)) = \underline{(\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)}$$

□

Korollar: $\mathrm{Aut}(G) := \{\varphi : G \to G |\ \varphi \text{ Automorphismus}\}$ ist eine Gruppe bzgl. Verknüpfung von Abbildungen.

Beweis:

- φ, ψ bijektiv $\Rightarrow \varphi \circ \psi$ bijektiv.
- $\varphi, \psi : G \to G$ Homomorphismus $\Rightarrow \psi \circ \varphi$ Homomorphismus [wegen (g)]
  Also: $\psi, \varphi \in \mathrm{Aut}(G) \Rightarrow \psi \circ \varphi \in \mathrm{Aut}(G)$.
- neutrales Element: id_G
- Assozativität von $\circ$ gilt für alle Abbildungen
- Inverses zu φ ist φ^{-1} und $\varphi^{-1} \in \mathrm{Aut}(G)$ [wegen (f)]

□

Beispiele:

1. $m \in \mathbb{N}, m \geq 1, \varphi_m : \mathbb{Z} \to \mathbb{Z}, k \mapsto m \cdot k$ ist ein injektiver Homomorphismus:

$$\varphi_m(k+l) = m \cdot (k+l) = m \cdot k + m \cdot l = \varphi_m(k) + \varphi_m(l)$$
$$\varphi_m(k) = 0 \Leftrightarrow m \cdot k = 0 \Leftrightarrow k = 0, \text{ also } Ker(\varphi_m) = \{0\}$$
$$Im(\varphi_m) = \varphi_m(\mathbb{Z}) = m \cdot \mathbb{Z}$$

2. $\varphi : \mathbb{Z} \to \mathbb{Z}_m, k \mapsto \overline{k} = k + m \cdot \mathbb{Z}$ ist surjektiver Homomorphismus:

$$\varphi(k+l) = \overline{k+l} = \overline{k} + \overline{l} = \varphi(k) + \varphi(l) \text{ also Homomorphismus}$$
$$\overline{l} \in \mathbb{Z}_m, \text{ dann } \varphi(l) = \overline{l}, \text{also surjektiv.}$$

$$Ker(\varphi) : \varphi(m \cdot l) = \overline{ml} = \overline{0}, \varphi(k) = \overline{0} \Rightarrow k \in \mathbb{Z}, \text{ somit } Ker(\varphi) = m\mathbb{Z}$$

3. $\varphi : \mathbb{Z} \to S^1 = \{z \in \mathbb{C} : |z| = 1\}, k \mapsto \zeta_m^k = (e^{\frac{2\pi i}{m}})^k$ ist Homomorphismus:

$$\varphi(k+l) = \zeta_m^{k+l} = \zeta_m^k \cdot \zeta_m^l = \varphi(k) \cdot \varphi(l)$$
$$Im(\varphi) = C_m = \{\zeta_m^k | k \in \mathbb{Z}\} = \text{Gruppe der m-ten Einheitswurzeln.}$$
$$Ker(\varphi) : \varphi(ml) = \zeta_m^{m \cdot l} = e^{\frac{2\pi i m l}{m}} = e^{2\pi i l} = 1$$
$$\varphi(k) = 1 \Rightarrow \zeta_m^k = 1 \Rightarrow e^{\frac{2\pi i k}{m}} = 1 \Rightarrow \frac{k}{m} \in \mathbb{Z} \Rightarrow k \in m \cdot \mathbb{Z} \text{ also } Ker(\varphi) = m \cdot \mathbb{Z}$$

4. $\tilde{\varphi} : \mathbb{Z}_m \to C_m, \overline{k} \mapsto \zeta_m^k$ ist Isomorphismus von $(\mathbb{Z}_m, +)$ mit $(C_m, \cdot)$ (UE)

5. $exp : \mathbb{R} \to \mathbb{R}^* = \mathbb{R}\backslash\{0\}, x \mapsto e^x$ ist injektiver Homomorphismus mit $Im(exp) = \mathbb{R}_+ =]0, \infty[$ (UE)

6. $exp : \mathbb{C} \to \mathbb{C}^*, z \mapsto e^z$ ist surjektiver Homomorphismus.
   $Ker(exp) = \{2\pi in | n \in \mathbb{Z}\}$ (UE)

7. $det : GL(n, \mathbb{R}) \to \mathbb{R}^*, A \mapsto detA$ ist surjektiver Homomorphismus:

   $det(A \cdot B) = det(A) \cdot det(B)$

   $$det \begin{pmatrix} C & 0 & \dots & 0 \\ 0 & 1 & \dots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} = C \text{ also surjektiv}$$

   $Ker(det) = \{A \in GL(n, \mathbb{R}) | det(A) = 1\} =: SL(n, \mathbb{R})$

8. Signum einer Permutation:

   $$sign : S_n \to \{-1, +1\}, \sigma \mapsto sign(\sigma)$$

   ist ein Homomorphismus:

   $$sign(\sigma \circ \gamma) = sign(\sigma) \cdot sign(\gamma)$$
   $$Ker(sign) = \{\sigma \in S_n | sign(\sigma) = +1\} =: A_n = \textbf{alternierende Gruppe}$$

9. G beliebige Gruppe, $a \in G$.
   Konjugation:
   $$\varkappa_a : G \to G, x \mapsto axa^{-1}$$
   ("Sandwich mit a und seinem Inversen")
   ist ein **innerer Automorphismus**:

   $$\underline{\varkappa_a(xy)} = axya^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = \underline{\varkappa_a(x) \cdot \varkappa_a(y)}$$

   $$\text{injektiv: } \varkappa_a(x) = e \Rightarrow axa^{-1} = e \Rightarrow ax = a \Rightarrow x = e$$

   $$\text{surjektiv: } y \in G; x := a^{-1}ya \Rightarrow \varkappa_a(x) = a(a^{-1}ya)a^{-1}) = y$$

   Bemerkung:

   - $\varkappa_a^{-1} = \varkappa_{a^{-1}}$
   - G abelsch $\Rightarrow \varkappa_a(x) = x \quad \forall x \in G$, d.h. $\varkappa_a = id_G$

2.2 Nebenklassen

Sei H eine Untergruppe von G, $a, b \in G$. Idee:

$$a \underset{l}{\sim} b, \text{ wenn } \exists x \in H : b = a \cdot x \Leftrightarrow a^{-1} \cdot b = x \in H$$

Man bezeichnet dies als "$a \underset{l}{\equiv} b \pmod{M}$" bzw. **linkskongruent**.

$\underset{l}{\sim}$ ist eine Äquivalenzrelation:

- $a \underset{l}{\sim} a$ klar [x=e] (Reflexivität)
- $a \underset{l}{\sim} b \Rightarrow b = ax \Rightarrow a = bx^{-1} \Rightarrow b \underset{l}{\sim} a$ (Symmetrie)
- $a \underset{l}{\sim} b, b \underset{l}{\sim} c \Rightarrow b = ax, c = by, \quad x, y \in H \Rightarrow c = a\underbrace{x \cdot y}_{\in H} \Rightarrow a \underset{l}{\sim} c$. (Transitivität)

Äquivalenzklasse von a bzgl. $\underset{l}{\sim}$ ist

$$\{b \in G | \exists x \in H : b = a \cdot x\} =: a \cdot H$$

aH...**linke Nebenklasse** von a bzgl. H
analog $a \underset{r}{\sim} b$, wenn $\exists x \in H : b = x \cdot a \Leftrightarrow b \cdot a^{-1} \in H \Leftrightarrow a \cdot b^{-1} \in H$.
$Ha := \{b \in G | \exists x \in H : b = x \cdot a\}$...**rechte Nebenklasse** von a bzgl. H

Lemma: Folgende Aussagen sind äquivalent:

(i) $aH = bH$

(ii) $b \in aH$

(iii) $a^{-1}b \in H$

ebenso:

(i') $Ha = Hb$

(ii') $b \in Ha$

(iii') $ab^{-1} \in H$

Beweis:
(i)⇒(ii): $b = b \cdot e \in bH = aH$

(ii)⇒(iii): $\exists x \in H : b = a \cdot x \Rightarrow \exists x \in H : a^{-1}b = x \Rightarrow a^{-1}b \in H$

(iii)⇒(i):

- $aH \subseteq bH$:

$$y \in aH \Rightarrow \exists x \in H : y = a \cdot x \Rightarrow y = (b \cdot b^{-1})ax = b(b^{-1}a)x =$$

$$= b \cdot \underbrace{\underbrace{(a^{-1}b)^{-1}}_{\in H} \underbrace{x}_{\in H}}_{\in H} \Rightarrow y \in bH$$

- $bH \subseteq aH$:

$$y \in bH \Rightarrow \exists x \in H : y = bx \Rightarrow y = (a \cdot a^{-1})bx = a \underbrace{(a^{-1}b)}_{\in H} \underbrace{x}_{\in H} \in aH$$

(für Rechtsnebenklassen analog)

□

G kann in entsprechende Äquivalenzklassen zerlegt werden:

$$G/H := \{aH | a \in G\}$$

$$H\backslash G := \{Ha | a \in G\}$$

Es ist $aH = bH$ oder $aH \cap bH = \emptyset$, weil $\underset{l}{\sim}$ eine Äquivalenzrelation ist. $G = \bigcup_{a \in G} aH$

Bemerkung: $\Phi : G/H \to H\backslash G, aH \mapsto Ha^{-1}$ ist bijektiv.

! Im Allgemeinen wird G/H nicht durch $(aH) * (bH) := (ab)H$ zur Gruppe!

2.3 Ordnung und Index

Sei G eine Menge:

$$ord(G) := \begin{cases} |G| & \text{falls G endlich} \\ \infty & \text{falls nicht endlich} \end{cases}$$

Wegen Bemerkung in 2.2: G Gruppe, H Untergruppe, $ord(G/H) = ord(H\backslash G)$.

Definition:

Index von H in G ist

$$ind(G : H) := ord(G/H)$$

Satz (von Lagrange): G eine endliche Grupppe,

$$H < G \Rightarrow ord(G) = ord(H) \cdot ind(G : H)$$

Beweis:
Setze $m := ind(G : H), \exists a_1, ..., a_m \in G$ sodass $G = a_1H \cup ... \cup a_mH$ disjunkte Vereinigung ist(Zerlegung in Äquivalenzklassen).
Jedes a_jH enthält genauso viele Elemente wie H, weil $x \mapsto a_jx, H \to a_jH$ bijektiv ist (vgl. Manuskript). Also hat G demnach $m \cdot ord(H)$ viele Elemente.

□

Korollar: Ist $ord(G)$ eine Primzahl, dann hat G nur die trivialen Untergruppen $\{e\}$ und G.

Beweis:
Nach Satz von Lagrange ist $ord(H)$ ein Teiler von $ord(G)$.

□

Ordnung eines Elements $a \in G$ ist definiert als

$$ord(a) := ord(Erz(\{a\}))$$

(Erz....Erzeugnis)
Wegen

$$Erz(\{a\}) = \{a^k | k \in \mathbb{Z}\} \text{ und } a^{k+l} = a^l \cdot a^k$$

gilt

$$ord(a) = min\{k \in \mathbb{N}\backslash\{0\} \ | a^k = e\} \text{ falls } ord(a) < \infty$$

Lemma: $ord(a) < \infty, k \in \mathbb{Z}$

$$a^k = e \Leftrightarrow ord(a) | k$$

Speziell:

$$a^{ord(G)} = e \text{ in endlichen Gruppen}$$

(In UE haben wir es für endliche abelsche Gruppen bewiesen.

Beweis:

$\boxed{\Leftarrow}$: klar

$\boxed{\Rightarrow}$: $\varphi : \mathbb{Z} \to G, l \mapsto a^l$ ist Homomorphismus und $Ker(\varphi) < \mathbb{Z}$ (Ü7) $\Rightarrow \exists m \in \mathbb{Z}$: $Ker(\varphi) = m\mathbb{Z}$. Somit:

$$a^m = \varphi(m) = e,\ a^j = \varphi(j) \neq e \quad (1 \leq j < m)$$

d.h. $m = ord(a)$ und $a^k = e \Rightarrow \varphi(k) = e \Rightarrow k \in Ker(\varphi) = m\mathbb{Z} \Rightarrow m|k$ (also $ord(a)|k$).

□

Bemerkung: Es muss nicht zu jedem Teiler n von ord(G) immer eine Untergruppe H mit $n =$ ord(H) geben.

Beispiele:

1. $G = \mathbb{Z}, H = m\mathbb{Z}$, hier ist ind$(\mathbb{Z} : m\mathbb{Z}) = m$, weil

   $$\mathbb{Z}/m\mathbb{Z} = \{k + m\mathbb{Z} | k \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{m-1}\} = \mathbb{Z}_m$$

   für $m = 6$: ord$(\overline{2}) = 3$, ord $(\overline{3}) = 2$, ord$(\overline{4}) = 3$, ord$(\overline{5}) = 6$

2. $G = GL(n, \mathbb{R}), H := \{A \in GL(n, \mathbb{R}) | \det A > 0\}$
   (H ist Untergruppe, denn $\det A \cdot B^{-1} = \det A \cdot (detB)^{-1} > 0$)

   Sei $C \in GL(n, \mathbb{R})$ beliebig mit $\det C < 0$;

   $$\forall A \in H : \det(A \cdot C) = \underbrace{\det A}_{>0} \cdot \underbrace{\det C}_{<0} < 0$$

   also $H \cdot C \subseteq \{B | \det B < 0\} =: N$;
   ist $B \in N$, dann $A := B \cdot C^{-1} \in H$, weil $\det A = \underbrace{\det B}_{<0} \cdot \underbrace{(\det C)^{-1}}_{<0} > 0$, somit

   $$B = A \cdot C \in H \cdot C, \text{ also } H \cdot C = N$$

   weiters: $C \cdot H = H \cdot C$, weil

   $$X = A \cdot C \text{ mit } A \in H \Leftrightarrow X = C \cdot \underbrace{C^{-1}AC}_{\det>0} = C \cdot A' \text{ mit } A' \in H$$

   Schließlich

   $$G = \underbrace{\{A | \det A > 0\}}_{H} \cup \underbrace{\{B | \det B < 0\}}_{C \cdot H}$$

$$\text{ind}(G:H)=2; \quad ord\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}=\infty, \quad ord\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=2$$

2.4 Normalteiler und Faktorgruppen

Definition:

$H < G$ heißt **Normalteiler**, wir schreiben $H \lhd G$, wenn

$$\forall a \in G : aH = Ha$$

(d.h. die linken und rechten Nebenklassen stimmen überein).

Beispiel:

Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus, $H := Ker(\varphi)$; dann ist H Normalteiler, denn für $x \in H, a \in G$ ist

$$ax = \underbrace{axa^{-1}}_{y}\cdot a \text{ und } \varphi(\underbrace{axa^{-1}}_{y}) = \varphi(a)\underbrace{\varphi(x)}_{e'}\varphi(a^{-1}) = \varphi(a)\cdot\varphi(a)^{-1} = e'$$

Also $y \in Ker(\varphi) = H$ und somit $ax = ya \in Ha$; ebenso $xa = a \cdot a^{-1}xa \in aH$; insgesamt $aH = Ha$.

Varianten der Normalteilerbedingung

Für $H < G$ sind folgende Eigenschaften äquivalent:

(i) $aH = Ha$

(ii) $aHa^{-1} \subseteq H$

(iii) $aHa^{-1} = H \quad \forall a \in G$

Beweis:

(i)⇒ (ii): $x \in aHa^{-1} \Rightarrow \exists y \in H : x = aya^{-1} \Rightarrow xa = ay \in aH = Ha \Rightarrow x \in H$
($xa = za$ mit $z \in H$, daher $x = z \in H$)

(ii)⇒ (iii): nach **(ii)** ist $\varkappa_a(H) \subseteq H \quad \forall a \in G$, also auch $\varkappa_{a^{-1}}(H) \subseteq H$, somit

$$\underline{H = (\varkappa_a \circ \varkappa_{a^{-1}})(H) = \varkappa_a(\varkappa_{a^{-1}}(H)) \subseteq \varkappa_a(H) \subseteq H}$$

also $H = \varkappa_a(H) = aHa^{-1}$.

(iii)⇒ (i): $ah = \underbrace{aHa^{-1}}_{H} \cdot a = Ha$

□

Bemerkung: $\{e\}$ und G sind Normalteiler in G. In abelschen Gruppen ist jede Untergruppe Normalteiler.

Lemma: $\varphi : G \to G'$ ein Gruppenhomomorphismus

(i) $N' \lhd G' \Rightarrow \varphi^{-1}(N') \lhd G$
(Spezialfall: $N' = \{e\}$, dann $\varphi^{-1}(N') = Ker(\varphi)$)

(ii) φ surjektiv und $N \lhd G \Rightarrow \varphi(N) \lhd G'$

Beweis:

(i) $\varphi^{-1}(N') < G$ nach 2.1 (Eigenschaften). Wir zeigen: $a\varphi^{-1}(N')a^{-1} \subseteq \varphi^{-1}(N')$, dann fertig;
Sei $x \in \varphi^{-1}(N')$, d.h. $x' := \varphi(x) \in N'$, dann $\varphi(axa^{-1}) = \varphi(a)x'\varphi(a)^{-1} \in N'$, somit $axa^{-1} \in \varphi^{-1}(N')$.

(ii) Gemäß 2.1 (Eigenschaften) ist $\varphi(N) < G'$;
wir zeigen $a'\varphi(N)a'^{-1} \subseteq \varphi(N)$, dann fertig; $x' \in \varphi(N)$, d.h. $\exists x \in N : x' = \varphi(x)$;
Sei $a' = \varphi(a) \Rightarrow a'x'a'^{-1} = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(\underbrace{axa^{-1}}_{\in N}) \in \varphi(N)$
(Surjektivität von φ!)

□

Satz: G Gruppe und $N \lhd G$, dann definiert $(aN) * (bN) := (ab) \cdot N$ eine Verknüpfung auf G/N, sodass $(G/N, *)$ eine Gruppe ist und die **kanonische surjektive Abbildung** $\rho : G \to G/N, a \mapsto aN (= Na)$ ein Homomorphismus ist.
Das neutrale Element in G/N ist N, das Inverse zu aN ist $a^{-1}N$ und $Ker(\rho) = N$.

$(G/N, *)$ heißt **Faktorgruppe** von G nach N und $*$ ist eine eindeutige Verknüpfung, die ρ zu einem Homomorphismus macht. (Wir schreiben später einfach $(aN)\cdot(bN)$ statt $(aN)*(bN)$).

Beweis:

Wenn ρ ein Homomorphismus sein soll, so muss $(aN)*(bN) = \rho(a)*\rho(b) = \rho(ab) = (ab)N$ gelten, daher $*$ eindeutig.

Wohldefiniertheit von $*$ (also Unabhängigkeit des "Wertes" $(aN)*(bN)$ von den Repräsentanten $a \in aN, b \in bN$):

Seien $a' \in aN$ und $b' \in bN$, d.h. $aN = a'N,\ bN = b'N.\ \forall x \in N\ \exists\ y \in N$ mit $xb' = b'y$, weil $Nb' = b'N$ (Normalteiler!). Setze $x = a^{-1}a' (\in N$, weil $aN = a'N)$, dann folgt

$$\underline{(ab)^{-1}(a'b')} = b^{-1}\overbrace{\underbrace{a^{-1}a'}_{=b'y}b'}^{x} = \underbrace{\underline{b^{-1}b'}}_{\in N}\underline{y \in N}$$

$(b^{-1}b' \in N$, weil $bN = b'N.)$

$\Rightarrow (ab)N = (a'b')N$, somit ist $*$ wohldefiniert. Assoziativität folgt leicht:

$$((aN)*(bN))*(cN) = ((ab)N)*(cN) = ((ab)c)N = (a(bc))N = (aN)*(bc)N = (aN)*((bN)*(cN))$$

$N = eN$ ist neutrales Element:

$$(eN)*(aN) = (ea)N = aN = (ae)N = (aN)*(eN)$$

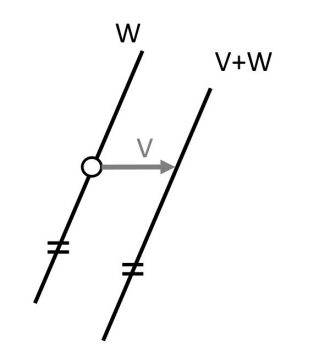
$(aN)^{-1} = a^{-1}N$, denn: $\underline{(a^{-1}N)*(aN)} = (a^{-1}a)N = \underline{N} = (aa^{-1}N) = \underline{(aN)*(a^{-1}N)}$

□

Beispiele:

1. Sei V Vektorraum über $\mathbb{K}$, W ein Teilraum; dann ist W Normalteiler der additiven Gruppe $(V,+)$ und V/W entspricht dem Faktorraum (**Quotientenraum**) mit

$$(V+W)+(V'+W) := (V+V')+W$$



($V+W$ ist ein parallel verschobener Teilraum)

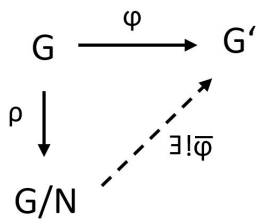
2. $G = \mathbb{Z}, N = m\mathbb{Z} \lhd \mathbb{Z}$ (weil $\mathbb{Z}$ abelsch).

Faktorgruppe ist $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ wie in 2.3, Bsp. 1), $\mathbb{Z}$ ist zyklische Gruppe mit $ord(\mathbb{Z}) = \infty$, $\mathbb{Z}_m$ ist zyklische Gruppe mit $ord(\mathbb{Z}_m) = m$.

3. $G = GL(n, \mathbb{R})$ besitzt z.B. die Normalteiler
   $GL_+(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R}) | det(A) > 0\}$ (vgl. 2.3. Bsp. 2) und
   $SL(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R}) | det(A) = 1\}$ (Details in UE).

2.5 Isomorphiesatz

Satz (Faktorisierungssatz): Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. $N \lhd G$ mit $N \subseteq Ker(\varphi)$ und $\rho : G \to G/N$ die kanonische Surjektion auf die Faktorgruppe. Dann $\exists!$ Gruppenhomomorphismus $\overline{\varphi} : G/N \to G'$, sodass $\varphi = \overline{\varphi} \circ \rho$ gilt, d.h. das Diagramm (vgl. Abb.) ist kommutativ (es kommt also nicht darauf an, in welche Richtung wir den Pfeilen folgen).



Es ist dann weiters $\overline{\varphi}(G/N) = \varphi(G)$ und $Ker(\overline{\varphi}) = Ker(\varphi/N)$

Beweis:
Die Eindeutigkeit von $\overline{\varphi}$ folgt aus der Bedingung $\varphi = \overline{\varphi} \circ \rho$, denn
$\overline{\varphi}(\underbrace{aN}_{\rho(a)}) = (\overline{\varphi} \circ \rho)(a) = \varphi(a)$. Also setzen wir $\overline{\varphi} : G/N \to G'$, $\overline{\varphi}(aN) := \varphi(a)$.

- $\overline{\varphi}$ wohldefiniert:

$$aN = bN \Rightarrow a^{-1}b \in N \overset{N \subseteq Ker(\varphi)}{\Longrightarrow} e' = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \Rightarrow \varphi(a) = \varphi(b)$$

- $\overline{\varphi}$ Homomorphismus:

$$\overline{\varphi}((aN) \cdot (bN)) = \overline{\varphi}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aN) \cdot \overline{\varphi}(bN)$$

- $\varphi = \overline{\varphi} \circ \rho$ laut Konstruktion
- wegen $\overline{\varphi}(aN) = \varphi(a)$ ist $\overline{\varphi}(G/N) = \varphi(G)$.

- $N \lhd G$ und $N \subseteq \ker(\varphi) \Rightarrow N \lhd \ker(\varphi)$
- $\underline{Ker(\overline{\varphi}) \subseteq Ker(\varphi)/N :}$

$$aN \in Ker(\overline{\varphi}) \Rightarrow \varphi(a) = \overline{\varphi}(aN) = e' \Rightarrow a \in Ker(\varphi) \Rightarrow aN \in Ker(\varphi/N)$$

- $\underline{Ker(\overline{\varphi}) \supseteq Ker(\varphi)/N :}$

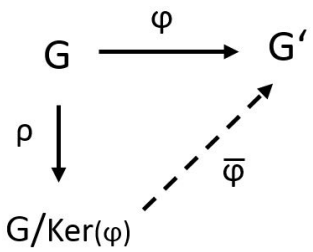
$$aN \in Ker(\varphi/N) \Rightarrow \exists b \in Ker(\varphi) : aN = bN \Rightarrow a^{-1}b \in N \subseteq Ker(\varphi) \Rightarrow$$

$$a^{-1} = a^{-1}bb^{-1} \in Ker(\varphi) \Rightarrow a \in Ker(\varphi) \Rightarrow \overline{\varphi}(aN) = \varphi(a) = e' \Rightarrow aN \in Ker(\overline{\varphi})$$

Somit $Ker(\overline{\varphi}) = Ker(\varphi/N)$.

□

Anwendung auf die Bestimmung von Faktorgruppen (bis auf Isomorphie):
Für $N = Ker(\varphi)$ (ist immer Normalteiler!) ergibt sich:



wobei $\overline{\varphi}$ nun injektiv ist, weil $Ker(\overline{\varphi}) = Ker(\varphi)/Ker(\varphi) = \{N\}$, also ist $\overline{\varphi}$ injektiv als Abbildung $G/Ker(\varphi) \to \varphi(G)$, d.h.

$$\boxed{\varphi(G) \cong G/Ker(\varphi)} \text{ (vermöge } \overline{\varphi})$$

sogenannter **erster Isomorphiesatz**.

($\cong$...“isomorph“)

Bemerkung: Ist φ surjektiv, also $\varphi(G) = G'$, folgt $G' \cong G/Ker(\varphi)$ (vermöge $\overline{\varphi}$).

Beispiel:
$\varphi : \mathbb{Z} \to S^1, k \mapsto \zeta_m^k$ aus 2.1, Bsp. 3);
$\varphi(\mathbb{Z}) = C_m, Ker(\varphi) = m\mathbb{Z}$, somit $\mathbb{Z}_m = \underline{\mathbb{Z}/m\mathbb{Z} \cong C_m} = \varphi(\mathbb{Z})$.

2.6 Klassifikation der zyklischen Gruppe

Erinnere: G heißt **zyklisch**, wenn $\exists a \in G$ mit

$$G = Erz(\{a\}) = \{a^k | k \in \mathbb{Z}\}$$

mit anderen Worten: $\varphi : \mathbb{Z} \to G, k \mapsto a^k$ ist ein surjektiver Gruppenhomomorphismus.

Bemerkung:
(i) Jede zyklische Gruppe ist kommutativ, denn

$$a^k \cdot a^l = a^{k+l} = a^l \cdot a^k$$

(ii) G endliche Gruppe mit $ord(G)$ prim, $a \in G \backslash \{e\} \Rightarrow G$ zyklisch und $G = Erz(\{a\})$

Beweis:
(ii): $p := ord(G), H := Erz(\{a\})$. Wegen $a \neq e$ ist $ord(H) \geq 2$; nach Satz von Lagrange (2.3) gilt auch $ord(H)|p$; somit muss $ord(H) = p$ sein, also $H = G$.

□

Satz: Sei G zyklische Gruppe mit erzeugendem Element $a \in G$. Dann ist entweder $G \cong \mathbb{Z}$ oder $\exists m \in \mathbb{N}, m \geq 1$, sodass $\psi : \mathbb{Z}_m \to G, \overline{k} \mapsto a^k$ ein Isomorphismus ist, also $G \cong \mathbb{Z}_m$ ist.

Beweis:
Der Homomorphismus $\varphi : \mathbb{Z} \to G, k \mapsto a^k$ ist wegen $G = \{a^k | k \in \mathbb{Z}\}$ jedenfalls surjektiv,

- falls $Ker(\varphi) = \{0\}$, also φ auch injektiv ist, dann gilt $G \cong \mathbb{Z}$ (vermöge φ); hier ist $ord(G) = \infty$.
- falls $\{0\} \subsetneq Ker(\varphi) \subseteq \mathbb{Z}$ gibt es wegen $Ker(\varphi) \lhd \mathbb{Z}$ (wobei $<$ genügt) gemäß UE7 ein $m \in \mathbb{N}, m \geq 1$ mit $Ker(\varphi) = m \cdot \mathbb{Z}$; nach dem Isomorphiesatz 2.5 gilt also $\mathbb{Z}_m = \mathbb{Z}/Ker(\varphi) \cong G$ mittels $\overline{\varphi}(\overline{k}) = \varphi(k) = a^k = \psi(\overline{k})$

□

In diesem Sinne sind $(\mathbb{Z}_m, +)$ bzw. $(\mathbb{Z}, +)$ die "Grundmodelle" für alle zyklischen Gruppen.

Bemerkung: (ohne Beweis)

- Jede Untergruppe einer zyklischen Gruppe ist zyklisch.
- Sei G eine endliche zyklische Gruppe, $m = ord(G)$, dann existiert zu jedem Teiler k von m genau eine Untergruppe $H < G$ mit $ord(H) = k$.

Teil II

Ringe

Kapitel 3

Grundbegriffe und Polynomringe

3.1 Ringe, Nullteiler, Integritätsbereiche

Wir betrachen nun eine Menge R mit zwei inneren Verknüpfungen $+$ und $\cdot$, die durch sogenannte **Distributivgesetze** gekoppelt sind (z.B, $\mathbb{Z}$ mit $+$ und $\cdot$).

Definition:
$(\mathbb{R}, +, \cdot)$ ist ein **Ring**, falls

(R1) $(\mathbb{R}, +)$ eine abelsche Gruppe ist

(R2) $(\mathbb{R}, \cdot)$ eine Halbgruppe ist (also $\cdot$ assoziativ ist)

(R3) die Distributivgesetze gelten:
$\forall a, b, c \in R$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(b + c) \cdot a = b \cdot a + c \cdot a$.

Das neutrale Element 0 bzgl. $+$ heißt **Nullelement** von R. Wegen **(R3)** und "um Klammern zu sparen" soll "Punktrechnung vor Strichrechnung" gelten, wobei der "Punkte" oft auch nicht geschrieben wird.

R heißt **kommutativer Ring**, falls $(R, \cdot)$ kommutativ ist.

Ein Element $1 \in \mathbb{R}$ heißt **Einselelement**, falls $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$. (Beide Gleichungen müssen i.A. verlangt werden.)

Lemma (Mini-Lemma)**:** In einem Ring $(R, +, \cdot)$ gilt:

(i) $0 \cdot a = a \cdot 0 = 0$

(ii) $(-a)b = a(-b) = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) Wenn R ein Einselelement 1 besitzt: $1 = 0 \Leftrightarrow R = \{0\}$...**Nullring**

Beweis in Übung.

Definition:

$a \in R$ heißt rechter bzw. linker **Nullteiler**, wenn $\exists b \in R\backslash\{0\} : b \cdot a = 0$ bzw. $a \cdot b = 0$ gilt. (Somit ist 0 bei uns immer ein Nullteiler, falls $R \neq \{0\}$; es gibt aber auch andere Konventionen, bei denen nur Elemente $\neq 0$ überhaupt als Nullteiler zugelassen werden.)

R heißt **nullteilerfrei**, wenn es keine rechten oder linken Nullteiler außer 0 gibt.

Lemma (Mini-Lemma 2)***:*** Für einen Ring R ist äquivalent:

(i) R ist nullteilerfrei

(ii) auf $R\backslash\{0\}$ ist $\cdot$ eine innere Verknüpfung

(iii) es gelten die Kürzungsregeln - für $x \neq 0$ gilt:
$ax = bx \Rightarrow a = b$ und
$xa = xb \Rightarrow a = b$

Beweis in Übung.

Definition:

Ein Ring R heißt **Integritätsbereich** oder **Integritätsring**, falls gilt:

(a) R hat ein Einselelement $1 \neq 0$

(b) R ist kommutativ

(c) R ist nullteilerfrei

Beispiele:

1. $(\mathbb{Z}, +, \cdot)$ ist Integritätsbereich
2. $\overline{2}$ ist Nullteiler in $\mathbb{Z}_6$, denn $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ und $\overline{2} \neq 0, \overline{3} \neq 0$

3.2 Einheiten, Körper, Unterringe

Definition:

R ein Ring mit $1, a \in R$ heißt **Einheit**, falls $\exists\, \tilde{a} \in R : a \cdot \tilde{a} = \tilde{a} \cdot a = 1$.
(i.A. muss man beide Gleichungen verlangen)

Es ist dann die Menge $R^\times := \{a \in R | a \text{ ist Einheit } \}$ eine Gruppe bzgl. $\cdot$, die sogenannte **Einheitengruppe** von R:

- $a, b \in R^\times \Rightarrow \exists \tilde{a}, \tilde{b} \in R :$
  $\tilde{a}a = a\tilde{a} = 1 = b\tilde{b} = \tilde{b}b \Rightarrow (ab)(\tilde{b}\tilde{a}) = ab\tilde{b}\tilde{a} = a\tilde{a} = 1 \Rightarrow ab \in R^\times$; ähnlich $(\tilde{a}\tilde{b})(ab) = 1$.
- $1 \in R^\times$
- a^{-1} (in $R^\times$) Inverses zu a

□

Beispiel:

$\mathbb{Z}^\times = \{-1, 1\}$
Für $1 \neq 0$ ist also zwingend $R^\times \subseteq R\backslash\{0\}$; falls sogar $R^\times = R\backslash\{0\}$, also jedes Element $a \neq 0$ ein multiplikatives Inverses besitzt, dann sprechen wir von einem **Schiefkörper**, im kommutativen Fall von einem **Körper**: $(K, +, \cdot)$ heißt **Körper**, falls gilt:

(K1) $(K, +)$ ist eine abelsche Gruppe (mit neutralem Element 0)

(K2) $(K\backslash\{0\}, \cdot)$ ist abelsche Gruppe (mit neutralem Element $1[\neq 0]$)

(K3) Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

Definition:

Sei $(R, +, \cdot)$ ein Ring. $S \subseteq R$ heißt **Unterring** von R, falls gilt:

(a) $\forall a, b \in S : a + b \in S$ und $a \cdot b \in S$

(b) S ist mit den von R geerbten Verknüpfungen $+$ und $\cdot$ ein Ring

---

Ist $(K, +, \cdot)$ ein Körper, so heißt $L \subseteq K$ ein **Unterkörper**, wenn L ein Unterring und mit diesen geerbten Verknüpfungen selbst ein Körper ist. Konsequenter Weise heißt K **Oberkörper** von L oder (häufiger) **Körpererweiterung** von L.

Ist $M \subseteq R$, so heißt der kleinste Unterring von R, der M enthält, der von M **erzeugte Unterring** und wird mit $\text{Erz}(M)$ bezeichnet. In „Formeln“ ist $\text{Erz}(M) = \bigcap_{M \subseteq S^*} S$ (S ein

Unterring von R) - ein beliebiger Durchschnit von Untergruppen ergeben wieder einen Unterring.
Ist $S \subseteq R$ ein Unterring und $a \in R$, so schreiben wir $S[a] := Erz(S \cup \{a\})$ (kleinster Unterring, der S und a enthält) und sagen, a werde zu S **adjungiert**.

Bemerkung: $S \subseteq R$ ist Untering $\Leftrightarrow$

(i) $S \neq \emptyset$

(ii) $\forall a, b \in S : a - b \in S$ und $a \cdot b \in S$

(Verwende Untergruppencharakterisierung in Lemma 1.3 für $(S, +)$ und automatische Vererbung von Assoziativgesetz für $\cdot$ und Distributivgesetz von R auf S).

3.3 Ringhomomorphismen

Definition:

Seien $(R, +, \cdot)$ und $(R', +', \cdot')$ Ringe. Eine Abbildung $\varphi : R \to R'$ heißt **Ringhomomorphismus**, falls $\forall a, b \in R$ gilt:

$$\varphi(a + b) = \varphi(a) +' \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$$

Ein bijektiver Homomorphismus heißt **Isomorphismus** bzw. **Automorphismus** für $R' = R$.

Ker $\varphi := \{a \in R | \varphi(a) = 0'\}$ heißt **Kern** von φ
Im $\varphi := \{\varphi(a) | a \in R\} = \varphi(R)$ heißt **Bild** von φ.

Eigenschaften

(a) Ist $\varphi : R \to R'$ ein Ringhomomorphismus $\Rightarrow$ Ker $\varphi \subseteq R$ und Im $\varphi \subseteq R'$ sind jeweils Unteringe

(b) Ist $\psi : R' \to R''$ ein weiterer Ringhomomorphismus $\Rightarrow \psi \circ \varphi : R \to R''$ ist ebenfalls ein Ringhomomorphismus

(c) Ist φ ein Ringisomorphismus $\Rightarrow \varphi^{-1} : R' \to R$ ist ebenfalls ein Ringisomorphismus

(d) φ injektiv $\Leftrightarrow$ Ker $\varphi = \{0\}$

(e) Ist R ein Körper, dann gilt: φ ist injektiv oder $\varphi(a) = 0'$ $\forall a \in R$.

Beweis:
(a) - **(d)** sind leichte Routineüberlegungen
(e): falls $\exists a \in R^\times$ mit $\varphi(a) = 0'$, dann $\varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = 0' \cdot \varphi(a^{-1}) = 0'$, daher weiter $\forall b \in R : \varphi(b) = \varphi(b \cdot 1) = \varphi(b) \cdot \varphi(1) = \varphi(b) \cdot 0' = 0'$

□

3.4 Beispiele

Beispiele:

1. $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$
2. $\mathbb{R}$ ist eine Körpererweiterung von $\mathbb{Q}$
3. $\mathbb{C}$ ist eine Körpererweiterung von $\mathbb{R}$
4. $\mathbb{Z} + i\mathbb{Z} := \{m + n \cdot i | m, n \in \mathbb{Z}\}$ ist Unterring von $\mathbb{C}$
5. $\mathbb{R}^2$ mit $(a, b) + (c, d) := (a + c, b + d)$ und $(a, b) \cdot (c, d) := (ac, bd)$ ist ein Ring mit Nullteilerln, z.B.: $(1, 0) \cdot (0, 1) = (0, 0)$.
6. Sei M eine Menge, dann ist $\mathcal{F}(M, \mathbb{R}) := \{f : M \to \mathbb{R}\}$ ein Ring mit punktweise definierten $(f + g)(x) := f(x) + g(x)$, $(f \cdot g)(x) := f(x) \cdot g(x)$ (geht analog mit beliebigem Ring R statt $\mathbb{R}$).
   Bem.: Für $M = \mathbb{N}$ erhalten wir gerade alle reellen Folgen mit komponentenweiser Addition und Multiplikation (erinnere, dass eine Folge eine Abbildung $a : \mathbb{N} \to \mathbb{R}$ mit vereinbarter Schreibweise $a_n := a(n)$; $(a_n)_{n \in \mathbb{N}}$.
7. $M = [0, 1]$ in 6. und $S := C([0, 1], \mathbb{R}) = \{f : [0, 1] \to \mathbb{R} | f \text{ ist stetig}\}$, dann ist S ein Unterring von $\mathcal{F}([0, 1], \mathbb{R})$.
   (Summe und Differenz stetiger Funktionen sind stetig, ebenso Produkte.)
8. $M(n, \mathbb{R})$ und $M(n, \mathbb{C})$ sind Ringe mit Matrixaddition und -multiplikation. Einselelement ist I_n, $GL(n, \mathbb{R})$ bzw. $GL(n, \mathbb{C})$ sind Einheiten.

3.5 Polynomringe

„Naiv“ bzw. „praktisch“ gesehen ist ein Polynom ein Ausdruck der Art

$$f(x) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$$

mit Koeffizienten a_j, die einer Addition und Multiplikation unterworfen werden können müssen, also Elemente eines Ringes sein sollen, und einer „Unbekannten“ X. Aber was ist

das formal korrekt?

Das X müsste so wie anderer Ringelemente mit den Koeffizienten multipliziert und auch potenziert werden können. Aber festgelegt ist ein Polynom eigentlich durch seine Koeffizienten und mit diesen wird hauptsächlich gerechnet:

$$(a_3X^3+a_2X^2+a_1X+a_0)+(b_1X+b_0)=(a_3+0)X^3+(a_2+0)X^2+(a_1+b_1)X+(a_0+b_0)$$

$$(a_3X^3+...+a_0)\cdot(b_1X+b_0)= \underbrace{(a_3b_1)}_{\text{Indexsumme=4}} X^4+\underbrace{(a_2b_1+a_3b_0)}_{\text{Indexsumme=3}}X^3+...$$

Der Trick fürs Formale ist also, nur die Koeffizienten mit ihren Positionen zu notieren: Man fängt besser links mit „kleinen Potenzen von X“ an:

$$(a_0,a_1,a_2,a_3)+(b_0,b_1,0,0)=(a_0+b_0,...)$$

$$(a_0,a_1,a_2,a_3)\cdot(b_0,b_1,0,0)=(a_0b_0,a_1b_0+a_0b_1,...)$$

Die Koeffizientenfolgen sind endlich, aber beliebig lang, daher können wir sagen es sind Folgen $(a_j)_{j\in\mathbb{N}}$, wobei $a_j=0$ für fast alle j ist.

Definition (Polynomring):
Sei R ein kommutativer Ring mit 1.

$$R[X]:=\{(a_0,a_1,a_2,...)\in \underbrace{R^{\mathbb{N}}}_{\text{Folgen in } R} \mid \underbrace{a_j=0 \text{ für fast alle } j\in\mathbb{N}}_{\text{d.h. nur für endlich viele j ist } a_j\neq 0}\}$$

mit komponentenweiser Addition

$$(a_j)_{j\in\mathbb{N}}+(b_j)_{j\in\mathbb{N}}:=(a_j+b_j)_{j\in\mathbb{N}}$$

und dem sogenannten **Cauchy-Produkt**

$$(a_0,a_1,a_2,...)\cdot(b_0,b_1,b_2,...):=(c_0,c_1,c_2,...)$$

wobei

$$c_k:=\sum_{l=0}^{k}a_l\cdot b_{k-l}=a_0b_k+a_1b_{k-1}+...+a_kb_0$$

(Indexsumme = k)

Das ergibt einen kommutativen Ring mit Einselelement $(1,0,0,0,...)$:

$$(1,0,...)\cdot(a_0,a_1,...)=(c_0,c_1) \text{ mit } c_0=1\cdot a_0, c_1=1\cdot a_1+0\cdot a_0=a_1 \text{ etc.}$$

Wir schreiben wieder 1 statt $(1,0,0,...)$.

Mittels $R \to R[X], a \mapsto (a, 0, ...)$ ist R in $R[X]$ eingebettet, d.h. diese Abbildung ist ein injektiver Rinhomomorphismus, der die Einselelemente auf einander abbildet. Daher fassen wir R gleich als Unterring von $R[X]$ auf. Wir können nun auch $X := (0, 1, 0, ...)$ setzen, dann ist $X^k = (0, ..., 0, \underbrace{1}_{(k+1)\text{te Stelle}}, 0, ...)$ und

$$R[X] \ni (a_0, a_1, a_2, ...) = a_0 \cdot 1 + a_1 X + a_2 X^2 + ... \quad \text{(endliche Summe!)}$$

$\rightsquigarrow$ also „alles in Butter“. [Details dazu in UE].
$(R[X], +, \cdot)$ heißt **Polynomring über** R.

Einsetzen für X geht nun so:
Ist R' ein Ring mit $R' \supseteq R$, $\alpha \in R'$ und $f = a_0 + a_1 X + ... + a_n X^n \in R[X]$, so setzen wir $f(\alpha) := a_0 + a_1\alpha + ... + a_n\alpha^n \in R'$. Durch $f \mapsto f(\alpha)$ erhalten wir eine Abbildung $R[X] \to R'$.

Bemerkung: R' statt R ist praktisch, weil dann z.B. komplexe Zahlen in reelle Polynome eingesetzt werden können. Es ist aber auch $R' = R[X]$ möglich, insbesondere für $\alpha = X$ erhalten wir also id: $R[X] \to R[X]$. (Jetzt ist alles formal sauber auseinander zu halten, aber dennoch eine einfache Notation möglich!)

Polynom versus Polynomfunktion:
Ist $f = a_0 + a_1 X + ... + a_n X^n \in R[X]$, so erhalten wir daraus die zugeordnete **Polynomfunktion** $\overline{f} : R \to R,\ x \mapsto a_0 + a_1 x + ... + a_n x^n$ [hier ist $x \in R$].

Achtung: Polynome sind durch ihre Koeffizienten immer eindeutig bestimmt, für Polynomfunktion gilt das über allgemeine Ringen aber nicht immer!

Beispiel:
$R = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\},\ f = X^2 + X \in \mathbb{Z}_2[X]$, dann ist $\overline{f}(\overline{0}) = \overline{0}$ und $\overline{f}(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{1} + \overline{1} = \overline{2} = \overline{0}$, somit $\overline{f}$ die Nullfunktion, die dem Nullpolynom $(0, 0, ...) = 0 + 0 \cdot X + ...$ entspricht, obwohl $f \neq$ Nullpolynom $[f = (0, 1, 1, 0, ...)]$.

Bemerkung: Wenn R ein Integritätsbereich mit ∞ vielen Elementen ist, dann ist $f \mapsto \overline{f}$ injektiv, weil es in diesem Fall für $f \neq 0$ nicht ∞ viele Nullstellen geben kann (später).

3.6 Grad eines Polynoms und Division mit Rest

Sei R ein kommutativer Ring mit 1.
Für $f = a_nX^n + ... + a_1X + a_0$ mit $a_n \neq 0$ nennen wir die höchste auftretende Potenz den **Grad** von f, wir schreiben deg $f = n$ und nennen a_n den **Leitkoeffizienten**, a_nX^n den **Leitterm** von f.
Für $f = 0$ (Nullpolynom) setzen wir künstlich deg $0 := -\infty$ (damit es sich gut von allen Polynomen abhebt und so, dass spätere Gradformeln auch in diesem Fall noch sinnvoll lesbar sind.)

Ein konstantes Polynom $f \neq 0$ hat demnach deg $f = 0$, weil $f = a_0$ mit $a_0 \in R\backslash\{0\}$; $\deg(aX + b) = 1$, falls $a \neq 0$ usw.

Gradformel: $\forall f, g \in R[X]$ gilt

$$\deg(f \cdot g) \leq \deg(f) + \deg(g)$$

Gleichheit gilt, falls der Leitkoeffizient von f oder g kein Nullteiler ist.

Bemerkung: deg $(f + g) \leq \max(\deg(f), \deg(g))$ (Leitkoeffizienten könnten einander auslöschen)

Beweis (der Gradformel):
Falls $f = 0$ oder $g = 0$ ist, dann ist $f \cdot g = 0$ und Ungleichung gilt im Sinne $-\infty \leq -\infty$.
Seien also $f \neq 0$ und $g \neq 0$ mit Darstellungen $f = a_mX^m + ... + a_0$, $a_m \neq 0$ und $g = b_nX^n + ... + b_0$, $b_n \neq 0$.
Wir haben also deg $f = m$.; deg $g = n$. In $f \cdot g$ ist der Koeffizient mit dem größtmöglichen Index $c_{m+n} = a_m \cdot b_n$, daher ist $\deg(f \cdot g) \leq m + n$.
Falls a_m oder b_n kein Nullteiler, dann ist sicher $c_{m+n} \neq 0$, also $\deg(f \cdot g) = m + n$.

□

Ein Polynom mit Leitkoeffizienten 1 heißt **normiert**. Ist $f = a_nX^n + ... + a_0$ und $a_n \in R^\times$, also eine Einheit, so können wir $\tilde{f} := a_n^{-1} \cdot f$ bilden und erhalten ein normiertes Polynom.

Sätzchen:

(i) $R[X]$ ist nullteilerfrei $\Leftrightarrow$ R ist nullteilerfrei

(ii) R nullteilerfrei $\Rightarrow (R[X])^\times = R^\times$ (insbesondere alle Einheiten deg$= 0$).

Beweischen:

(i) $\boxed{\Rightarrow}$ Wegen $R \subseteq R[X]$ klar
$\boxed{\Leftarrow}$ es gilt $\deg(f \cdot g) = \deg(f) + \deg(g)$; falls $(f \cdot g) = 0$, muss entweder $\deg(f) = -\infty$ oder $\deg(g) = -\infty$ gelten, also $f = 0$ oder $g = 0$.

(ii) $R^\times \subseteq (R[X])^\times$ klar $(a_0 \in R^\times, f = a_0; g := a_0^{-1} \Rightarrow g \cdot f = 1)$.
Wir zeigen $(R[X])^\times \subseteq R^\times$: $f \in (R[X])^\times \Rightarrow \exists g \in R[X] : f \cdot g = 1$.
Somit $0 \leq \underbrace{\deg(f)}_{\geq 0} + \underbrace{\deg(g)}_{\geq 0} = \deg(f \cdot g) = deg(1) = 0$
(weder $f = 0$ noch $g = 0$ möglich, wenn $f \cdot g = 1$).
$\Rightarrow \deg(f) = 0 = \deg(g)$; daher sind f und g „konstante“ Polynome, also $f = a_0$ mit $a_0 \in R^\times$

□

Satz (über die Division mit Rest): Sei K ein Körper und $f, g \in K[X]$ mit $g \neq 0$. Dann $\exists!\ q \in K[X]$ und $\exists!\ r \in K[X]$, sodass $f = q \cdot g + r$ und $\deg(r) <$deg(g).

Beweis:
Eindeutigkeit: Wenn $qg + r = \tilde{q}g + \tilde{r}$ mit $\deg(r) < \deg(g)$ und $\deg(\tilde{r}) \leq \deg(g)$, dann folgt:

$$r - \tilde{r} = (\tilde{q} - q) \cdot g$$

$\deg(r - \tilde{r}) < \deg(g)$; aus Gradsatz folgt:

$$deg(r - \tilde{r}) = deg(\tilde{q} - q) + deg(g)$$

$\Rightarrow \tilde{q} - q = 0 \Rightarrow \tilde{q} = q$ und $\tilde{r} = r$

Existenz: Sei $f = a_n X^n + ... + a_0$, $g = b_m X^m + ... + b_0$, $n = \deg(f), m = \deg(g) \geq 0$ $[g \neq 0; b_m \neq 0]$.

- falls $n < m$, dann fertig mit $q = 0$ und $r = f$
- falls $n \geq m$, dann konstruieren wir sukzessive $q_1, ..., q_k \in K[X]$ mit $k \leq n - m + 1$ derart, dass $q := q_1 + ... + qk$ mit $r := f - qg$ eine Lösung ergibt.

1. Schritt: Setze $f_0 := f,\ q_1 := \frac{a_n}{b_m} \cdot X^{n-m}$ (In Körperschreibweise $\frac{a_n}{b_m}$ statt $a_n b_m^{-1}$).
$f_1 := f_0 - q_1 g,\ deg(f_1) < deg(f_0) \quad [q_1 \cdot g = a_n X^n + ...]$

- falls $\deg(f_1) < deg(g)$, dann fertig mit $q = q_1, r = f_1$
- falls $\deg(f_1) \geq deg(g)$: mit f_1 wie oben mit f_0 verfahren, also $q_2 := c \cdot X^{deg(f_1)-m}$: $q_2 \cdot g$ gleichen Leitterm wie f_1 hat, $f_2 := f_1 - q_2 g,\ deg(f_2) < deg(f_1)$.
- Verfahren fortsetzen, bis $f_k := f_{k-1} - q_k g$ die Bedingung $deg(f_k) < deg(g)$ erfüllt - das ist spätenstens bei $k = n-m+1$ der Fall, weil $deg(f_k) < deg(f_{k-1}) < ... < deg(f_1) < n$ und $deg(g) = m \leq n$ ist.

Insgesamt $f = q_1 g + f_1 = q_1 g + q_2 g + f_2 = ... = \underbrace{(q_1 + ... + q_k)}_{=:q} g + \underbrace{f_k}_{=:r}$

□

Variante des Divisionssatzes für Integritätsbereich R statt K

Sei R ein Integritätsbereich und $f, g \in R[X]$ mit $g \neq 0$. Ist $b_m \in R$ der Leitkoeffizient von g, dann $\exists\ q, r \in R[X]$ und $k \in \mathbb{N}$, sodass

$$b_m^k \cdot f = q \cdot g + r \text{ und } deg(r) < deg(g)$$

Bem.: q und r sind bis auf eine Potenz von b_m eindeutig.
Begründung für die Gültigkeit der Variante: im obigen Beweis im ersten Schritt mit $b_m f$ und $q_1 \cdot b_m = a_n X^{n-m}$ arbeiten (durch b_m kann im Allgemeinen nichtdividiert werden, aber b_m ist jedenfalls kein Nullteiler).
$f_1 = b_m f_0 - \tilde{q_1} \cdot g$, dann $f_2 = b f_1 - \tilde{q_2} g$ etc., bzw. $bf = f_1 + \tilde{q_1} g,\ b^2 f = f_2 + \tilde{q_2} g$ usw.

Beispiele:

1. $f = X^2 - 1,\ g = 2 \cdot X$ in $\mathbb{Z}[X]$
   $2 \cdot f = 2X^2 - 2 = \underbrace{X}_{q} \cdot \underbrace{2X}_{g} - 2$ und $r = -2$
   $f = q \cdot g + r$ würde $q = \frac{1}{2}x$ erfordern, geht nicht in $\mathbb{Z}[X]$

2. in $\mathbb{R}[X]$: Verfahren eigentlich aus Schule bekannt:
   $f = X^3 - X + 1,\ g = X + 1$

$$\begin{array}{rl} \left(X^3 - X + 1 \right) : \left(X + 1 \right) = X^2 - X + \dfrac{1}{X+1} & \\ \underline{-X^3 - X^2} & \\ -X^2 - X & \\ \underline{X^2 + X} & \end{array}$$

Also $1 = r,\ q = X^2 - X \Rightarrow X^3 - X + 1 = (X^2 - X) \cdot (X + 1) + 1$

3.7 Nullstellen von Polynomen

Satz: Ist R ein Integritätsbereich und $f \in R[X]$ mit $\deg(f) \geq 1$ und $a \in R$ mit $f(a) = 0$, dann

$$\exists!\ q \in R[X] : f = (X - a) \cdot q \text{ und } deg(q) = deg(f) - 1$$

Insbesondere hat ein Polynom vom Grad $n \geq 1$ höchstens n verschiedene **Nullstellen** in R.

Beweis:

Division von f durch $g = X - a$ mit Rest ergibt $f = q \cdot (X - a) + r,\ deg(r) < 1 = deg(g)$.
Wegen $0 = f(a) = r(a)$ folgt $r = 0$, also $f = q \cdot (X - a)$; daher $deg(f) = deg(q \cdot (X - a)) = deg(q) + 1$.
Sind $a_1, ..., a_m \in R$ (paarweise) verschiedene Nullstellen, d.h. $f(a_j) = 0$ $(j = 1, ..., m)$ und $a_i \neq a_j$ $(i \neq j)$, dann ergibt sich durch sukzessive Anwendung das Obige:
$f = (X - a_1)...(X - a_m) \cdot h$ mit
$0 \underset{\uparrow}{\leq} deg(h) = deg(f) - m = n - m \Rightarrow m \leq n$
[$h \neq 0$, sonst $f = 0$.]

□

Korollar: Sind $a_1, ..., a_m \in R$ (paarweise) verschiedene Nullstellen von $f \in R[X], \deg(f) \geq 1$, dann $\exists!\ h \in R[X]$:

$$f(X - a_1)...(X - a_m) \cdot h,\ deg(h) = deg(f) - m \geq 0$$

Beispiel:
$f = (X-1)(X-2)(2X-1) \quad [= 2X^3 - 7X^2 + 7X - 2]$

in $\mathbb{R}[X]$: $\quad f = (X-1)(X-2)(X-\frac{1}{2}) \cdot \boxed{2}$ ↖

minimaler „h-Anteil“

in $\mathbb{Z}[x]$: $\quad f = (X-1)(X-2) \cdot \boxed{(2X - 1)}$ ↙

3.8 Komplexe Einheitswurzeln

$n \in \mathbb{N}, n \geq 1 : \zeta \in \mathbb{C}$ wird eine **n-te Einheitswurzel** genannt, wenn $\zeta^n = 1$ gilt. Äquivalent dazu ist, dass ζ eine Nullstelle des Polynoms $X^n - 1$ ist. Es gibt nach 3.7. höchstens n verschiedene n-te Einheitswurzeln und für $\zeta_n := e^{\frac{2\pi i}{n}}$ ist jede der n Zahlen ζ_n^k $(k = 0, 1, ..., n-1)$ eine solche.
Es ist

$$\zeta_n^{k+l\cdot n} = e^{2\pi ik/n + 2\pi il} = e^{2\pi ik/n} = \zeta_n^k$$

somit ist

$$C_n\{\zeta_n^k | k \in \mathbb{Z}\} = \{1, \zeta_n, ..., \zeta_n^{n-1}\} \subseteq S^1$$

gerade die Menge der n-ten Einheitswurzeln.
Weiters gilt gemäß 3.7:

$$X^n - 1 = (X-1)(X-\zeta_n)...(X-\zeta_n^{n-1})$$

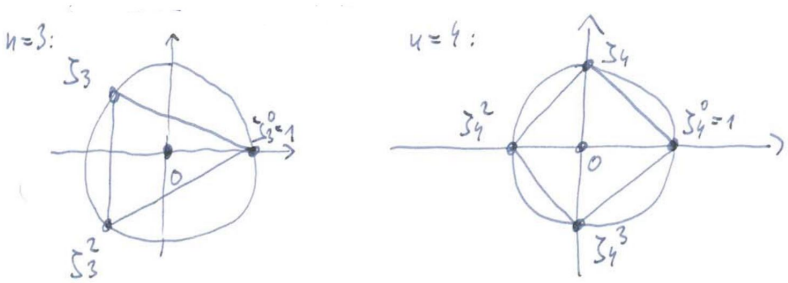
In früheren Beispielen und Übungsaufgaben haben wir gesehen: $\varphi : \mathbb{Z} \to C_n,\ k \mapsto \zeta_n^k$ ist ein Gruppenhomomorphismus und faktorisiert wegen $\ker(\varphi) = n\mathbb{Z}$ zu einem Isomprphismus $\overline{\varphi} : \mathbb{Z}_n \to C_n,\ \overline{k} \mapsto \zeta_n^k$; C_n ist also eine endliche zyklische Gruppe.
Es ist

$$(X^n - 1) = (X-1) \cdot (X^{n-1} + ... + X + 1)$$

$(X-1)$ hat einzige Nullstelle $\zeta_n^0 = 1$ bzw. $\zeta_1 = 1$, daher ist für $n \geq 2$ sicherlich ζ_n eine Nullstelle des zweiten Faktors, also

$$\zeta_n^{n-1} + \zeta_n^{n-2} + ... + \zeta_n + 1 = 0$$

Als Vektorsumme in $\mathbb{R}^2$ interpretiert sagt dies, dass 0 der „Schwerpunkt“ des regelmäßigen n-Ecks C_n ist:



Bemerkung:

$$C_m \cap C_n = C_{ggT(m,n)}$$

(Ohne Beweis, siehe Fischer II, 1.9)

3.9 Vom Integritätsbereich zum Quotientenkörper

Es ist ein häufiges mathematisches Ziel, „unfertige“ Strukturen zu „vervollständigen“ - oft als formale Nachbildung von historisch mühevoll gewachsenen Erweiterngen. z.B. kann die Halbgruppe $(\mathbb{N}, +)$ zur Gruppe $(\mathbb{Z}, +)$ erweitert werden, indem Differenzen wie z.B. $3 - 7$ durch Äquivalenzklassen von Paaren $(3, 7) \sim (4, 8) \sim (5, 9)...$ dargestellt werden. Somit muss nicht gesagt werden, was negative Zahlen sind, und es kann mit diesen (Klassen von) Paaren einfach gerechnet werden: $(k, l) + (r, s) = (k + r, l + s)$. Damit wird $\mathbb{N} \times \mathbb{N}/\sim$ zur Gruppe mit neutralem Element $=$ die Klasse von $(0, 0)$ [$\sim (1, 1)$ etc.] und zur Klasse von (k, l) ist die Klasse von (l, k) invers, weil $(k, l) + (l, k) = (k + l, l + k) \sim (0, 0)$.
(Allgemeiner Hintergrund für diese Konstruktion findet sich in Fischer II, 1.12)

Ähnlich kann ein Integritätsbereich R zu einem Körper $Q(R)$ erweitert werden, indem man die multiplikative Halbgruppe $(R\backslash\{0\}, \cdot)$ auf ähnliche Art um die nötigen „Brüche“ erweitert wird: statt „$\frac{a}{b}$“ führen wir das Paar $(a, b) \in R \times R\backslash\{0\}$ ein und erinnern uns an „$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$“, was wir durch $(a, b) \sim (a', b') \Leftrightarrow a \cdot b' = a' \cdot b'$ in R modellieren.
Multiplikation von „Brüchen“ ist leicht:

$$(a, b) \cdot (c, d) := (ac, bd)$$

Addition von „Brüchen“ erfolgt nach dem Muster

$$\text{“}\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}\text{“} : (a, b) + (c, d) := (ad + bc, bd)$$

$0 \hat{=} (0, 1), 1 \hat{=} (1, 1)$ (bzw. deren Klassen).

Die Menge $Q(R)$ dieser Klasse von „Brüchen“ wird so ein Körper (vgl. Fischer II, 1.13) und das Standardbeispiel ist $Q(\mathbb{Z}) = \mathbb{Q}$, wo dann die Paare $(m, n) \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ als Bruch $\frac{m}{n}$ notiert werden.

Ein weiteres wichtiges Beispiel ist für einen Körper K

$$Q(K[X]) =: K(X) \ldots \textbf{Körper der rationalen Funktionen}$$

also Brüche von Polynomen $\frac{f}{g},\ f \in K[X], g \in K[X], g \neq 0$.

Achtung: $\frac{\overline{f}}{\overline{g}}$ ergibt die zugeordnete rationale Funktion, die in den endlich vielen Nullstellen von $\overline{g}$ nicht definiert ist ($g \neq 0$ heißt ja nur „ungleich dem Nullpolynom“) - hier hat die formale Einführung der Polynome seine Vorteile gegenüber der konkreten Modellierung als Funktion.

Kapitel 4

Ideale und Restklassenringe

4.1 Ideale

Wenn $\varphi : R \to R'$ ein Ringhomomorphismus, dann ist gemäß 3.3 $I := Ker(\varphi)$ ein Unterring. I hat hier aber sogar eine weitere starke Eigenschaft:
Sei $x \in R$ und $a \in I$, dan gilt $\varphi(ax) = \underbrace{\varphi(a)}_{0} \cdot \varphi(x) = 0,\ \varphi(xa) = \varphi(x) \cdot \underbrace{\varphi(a)}_{0} = 0$
also $x \cdot a \in I$ und $a \cdot x \in I$ (für Unterring ist nur $b \cdot a \in I \wedge a \cdot b \in I$ für $b \in I$ nötig). Allgemeiner führen wir nun einen danach modellierten Begriff für Unterringe ein:

Definition:
Ist R ein Ring und $I \subseteq R$, dann heißt I **Ideal**, falls gilt:

(I1) I ist bzgl. $+$ eine Untergruppe von R

(I1) $a \in I, x \in R \Rightarrow x \cdot a \in I \wedge a \cdot x \in I$

Insbesondere ist ein Ideal daher ein Untering.

Falls R kommutativ mit 1, ist (I1+I2) äquivalent mit

(I) $0 \in I$ und $\forall n \in \mathbb{N}\ \forall a_1, ..., a_n \in I\ \forall x_1, ..., x_n \in R$:

$$x_1 a_1 + ... + x_n a_n \in I$$

(Beweis in UE)

Weiters defiieren wir im kommutativen Fall für $a \in R$ das **von a erzeugte Hauptideal** durch

$$(a) := R \cdot a := \{x \cdot a | x \in R\}$$

(dies ist ein Ideal, denn für $x, y \in \mathbb{R}, \tilde{x}, \tilde{y} \in (a)$ mit $\tilde{x} = xa, \tilde{y} = ya$ ist $\tilde{x} - \tilde{y} = xa - ya = (x - y)a \in (a)$ und für $z \in R$ ist $z \cdot \tilde{x} = z \cdot (x \cdot a) = (z \cdot x) \cdot a \in R$).

Beispiele:

1. oben gesehen: Kern eines Ringhomomorphismus ist immer ein Ideal
2. die **trivialen Ideale** $\{0\}$ und R gibt es immer
3. $m\mathbb{Z}$ ist Ideal in $\mathbb{Z}$

Bemerkung: Sei $\varphi : R \to R'$ ein Ringhomomorphismus, dann gilt:

(i) $I' \subseteq R'$ ein Ideal $\Rightarrow \varphi^{-1}(I') \subseteq R$ ein Ideal

(ii) $I \subseteq R$ ein Ideal und φ surjektiv $\Rightarrow \varphi(I) \subseteq R'$ ein Ideal

(Beweis in UE)

Satz: **(i)** R ein Ring mit 1, $I \subseteq R$ ein Ideal mit $I \cap R^\times \neq \emptyset \Rightarrow I = R$

(ii) Ein Körper K besitzt nur die trivialen Ideale

(iii) R ein kommutativer Ring mit $1 \neq 0$ und besitzt nur die trivialen Ideale $\{0\}$ und R, dann ist R ein Körper.

Beweis: (i) $a \in I \cap R^\times \Rightarrow \exists b \in R^\times : \underbrace{ab}_{\in I} = ba = 1 \Rightarrow 1 \in I \Rightarrow$
$\Rightarrow \forall x \in R : \underbrace{x \cdot 1}_{x} \in I \Rightarrow I = R$

(ii) Es ist $K^\times = K\backslash\{0\}$. Ist I ein Ideal in K und $I \neq \{0\}$, so muss $I \cap K^\times \neq \emptyset$ sein, also $I = K$ nach **(i)**.

(iii) Wir müssen $R^\times = R\backslash\{0\}$ zeigen, dann fertig:
$c \in R\backslash\{0\} \Rightarrow \{0\} \neq (c) = Rc$ und $Rc = R$, weil keine nichttrivialen Ideale in R existieren. Daher $\exists b \in R : bc = 1$ (weil $1 \in R = Rc$), somit $c \in R^\times$, also $R^\times = R\backslash\{0\}$ gezeigt, weil $R^\times \subseteq R\backslash\{0\}$ immer gilt.

□

4.2 Restklassenringe

Nun Verallgemeinerung der Konstruktion $\mathbb{Z}\backslash m\mathbb{Z}$ bzgl. Ringstruktur ($m\mathbb{Z}$ ist Ideal in $\mathbb{Z}$): Sei I ein Ideal in R, dann ist es als Untergruppe der abelschen Gruppe $(R,+)$ stets Normalteiler, also lässt sich Faktorguppe

$$R/I = \{x + I | x \in R\}$$

mit Addition $(x + I) + (y + I) := (x + y) + I$ bilden, die wieder eine abelsche Gruppe ist. Sei $\rho : R \to R/I,\ x \mapsto x + I$ der kanonisches surjektive Gruppenhomomorphismus. Wir wollen nun R/I durch die Multiplikation

$$(x + I) \cdot (y + I) := (x \cdot y) + I$$

zu einem Ring machen - dies ist die einzige Multiplikation auf R/I, die ρ zu einem Ringhomomorphismus machen kann kann:

- Multiplikation ist wohldefiniert:
  $x + I = x' + I, y + I = y' + I \Rightarrow x - x' \in I \wedge y - y' \in I \Rightarrow xy - x'y' =$
  $= \underbrace{(x - x')}_{\in I} y' + x \underbrace{(y - y')}_{\in I)} \in I \Rightarrow (xy) + I = (x'y') + I$
- Assoziativgesetz und Distributivgesetz vererben sich von R auf R/I, weil sie für die Repräsentanten $x, y, ...$ der Klassen gelten.
- $Ker(\varphi) = I$ nach Konstruktion von ρ
- wenn R kommutativ ist, dann auch R/I
- wenn R Einselelement 1 besitzt, dann ist $1 + I$ Einselelement in R/I

Bemerkung: Somit kann jedes Ideal als Kern eines Ringhomomorphismus aufgefasst werden, weil immer $I = Ker(\rho)$ für $\rho : R \to R/I$ kanonische Surjektion.

Wir nennen R/I den **Restklassenring** von R modulo I und schreiben **Kongruenzen modulo** I in R auch so:

$$x \equiv x' \pmod{I} :\Leftrightarrow x + I = x' + I \Leftrightarrow x - x' \in I$$

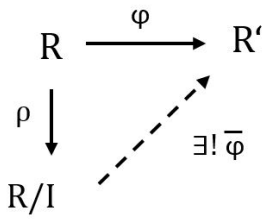
(vgl. $x \equiv x' \pmod{m} \Leftrightarrow x - x' \in m\mathbb{Z}$).

Rechenregeln:

$$x \equiv x' (\text{mod } I),\ y \equiv y' (\text{mod } I) \Rightarrow x \cdot y \equiv x' \cdot y' (\text{mod } I),\ x + y \equiv x' + y' (\text{mod } I)$$

Eigenschaften: analog zu Gruppen gelten (ohne Beweis):

(i) Faktorisierungssatz: Sei $\varphi : R \to R'$ ein Ringhomomorphismus, $I \subseteq R$ ein Ideal mit $I \subseteq Ker(\varphi)$ und $\rho : R \to R/I$ die kanonische Surjektion. Dann $\exists!$ Ringhomomorphismus $\overline{\varphi} : R/I \to R'$, sodass $\boxed{\varphi = \overline{\varphi} \circ \rho}$ gilt, d.h. die folgende Abbildung ist ein kommutatives Diagramm:



Weiters gilt $\overline{\varphi}(R/I) = \varphi(R),\ Ker(\overline{\varphi}) = Ker(\varphi)/I$.

(ii) erster Isomorphiesatz: $\varphi : R \to R'$ ein Ringhomomorphismus $\Rightarrow \overline{\varphi}$ bijektiv als Abbildung $R/Ker(\varphi) \to \varphi(R),\ x+Ker(\varphi) \mapsto \varphi(x)$ ergibt Isomorphismus $\boxed{\varphi(R) \cong R/Ker(\varphi)}$. Ist zudem φ surjektiv, dann ist $R' \cong R/Ker(\varphi)$.

4.3 Beispiele

Beispiele:

1. Jedes Ideal in $\mathbb{Z}$ ist auch additive Untergruppe, also von der Form $m\mathbb{Z}$ (frühere UE-Aufgabe) und jedes $m\mathbb{Z}$ ($m \in \mathbb{N}$) ist auch Hauptideal in $\mathbb{Z}$. Die zugehörigen Restklassenringe $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ sind die „Prototypen“ für 4.2 gewesen.
   $\mathbb{Z}$ ist nullteilerfrei und (für $m \geq 2$) $\mathbb{Z}_m$ ist genau dann nullteilerfrei, wenn m eine Primzahl ist (ebenfalls UE bzw. VO Zahlentheorie).
   Für die Einheiten in $\mathbb{Z}_m$ gilt

$$Z_m^\times = \{\overline{k} | ggT(k,m) = 1\}$$

   ($\exists\ l \in \mathbb{Z},\ x \in \mathbb{Z}, ggT(k,m) = 1 = kl + mx$, d.h. $\overline{k} \cdot \overline{l} = \overline{1}$.)

2. Betrachte $\varphi : \mathbb{R}[X] \to \mathbb{C},\ f \mapsto f(i)$, ein surjektiver Ringhomomorphismus (UE).
   Behauptung: $Ker(\varphi) = \underbrace{(X^2+1)}_{\text{Hauptidealklammern}} = \mathbb{R}[X] \cdot (X^2+1)$ ist Hauptideal.

   $\boxed{\supseteq}$ ist klar, weil $i^2 + 1 = 0$, d.h. $\varphi(X^2+1) = 0$ und somit

$$\varphi(f \cdot (X^2+1)) = \varphi(f) \cdot \underbrace{\varphi(X^2+1)}_{0} = 0$$

$\boxed{\subseteq}$ wird in UE besprochen.

□

Isomorphiesatz: $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$, $\overline{\varphi} : f + (X^2+1) \mapsto f(i)$

- für $a \in \mathbb{R}$ ist $\overline{\varphi}(a + (X^2+1)) = a \in \mathbb{R} \quad [f = a]$
- für $X \in \mathbb{R}[X]$ erhalten wir $\overline{\varphi}(X + (X^2+1)) = i \quad [f = x]$,
  d.h. $\overline{\varphi}(\underbrace{a + bX}_{f} + (X^2+1)) = a + bi$

Also ist Rechnen in komplexen Zahlen wie Rechnen in $\mathbb{R}[X]$ modulo (X^2+1).

4.4 Hauptidealringe und euklidische Ringe

Definition:

Sei R ein Integritätsbereich.

(i) R heißt **Hauptidealring**, wenn jedes ideal I in R ein Hauptideal ist, also $I = (a) = Ra$ für ein $a \in R$.

(ii) R heißt **euklidischer Ring**, wenn es eine Abbildung $\delta : R/\{0\} \to \mathbb{N}$ gibt mit folgender Eigenschaft:

$$\forall a, b \in R\backslash\{0\}\ \exists\ q, r \in R :\ a = q \cdot b + r \text{ und } \delta(r) < \delta(b),\ \text{falls } r \neq 0$$

(Division mit Rest)

Beispiele:

1. $\mathbb{Z}$ ist Hauptidealring, denn wie in 4.3 bemerkt ist jedes Ideal in $\mathbb{Z}$ von der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}$, $m\mathbb{Z} = (m)$.
   In $\mathbb{Z}$ kann $\delta(k) = |k|$ verwendet werden und Division mit Rest gilt, also ist $\mathbb{Z}$ auch ein euklidischer Ring.

2. K ein Körper, dann ist (nach 3.6) $K[X]$ ein euklidischer Ring mit $\delta(f) = \deg(f)$ für $f \neq 0$

3. $\mathbb{Z}[X]$ ist kein Hauptidealring (und gemäß nächstem Satz auch kein euklidischer Ring):
   $I := \{2 \cdot f_1 + X \cdot f_2 | f_1, f_2 \in \mathbb{Z}[X]\}$ ist ein Ideal in $\mathbb{Z}[X]$ und $I \neq \{0\}$. Es ist $1 \neq I$, somit auch $I \neq \mathbb{Z}[X]$.
   Wäre $\mathbb{Z}[X]$ ein Hauptidealring, so müsste es ein $f \in \mathbb{Z}[X]$ mit $I = (f) = \mathbb{Z}[X] \cdot f$ geben: Wegen $2, X \in I$ gibt es $g, h \in \mathbb{Z}[X]$, sodass

$\underbrace{2 = g \cdot f}_{\Rightarrow \deg(g)=0=\deg(f)}$, $\underbrace{X = h \cdot f}_{(*)}$, also $f = a_0$, $g = b_0$ mit $a_0, b_0 \in \mathbb{Z}$ und $a_0 b_0 = 2$, in

$(*): \; X = h \cdot a_0 \Rightarrow h = a_1 \cdot X$ und $a_0 a_1 = 1 \Rightarrow a_0 = \pm 1$, d.h. $f = \pm 1 \Rightarrow \underbrace{(f)}_{=I} = \mathbb{Z}[X]$

↯!

Satz: Ein euklidischer Ring ist ein Hauptidealring.

Beweis:

Sei R ein euklidischer Ring und $I \subseteq R$ ein Ideal.
Im Fall $I = \{0\} = (0)$ fertig, also wird nun $I \neq \{0\}$ angenommen:

$$\text{setze } M := \{n \in \mathbb{N} | \; \exists a \in I \backslash \{0\} : n = \delta(a)\}$$

$I \neq \{0\} \Rightarrow M \neq \emptyset$; sei $k = \min M$ und $a \in I \backslash \{0\}$ mit $k = \delta(a)$

Behauptung: $I = (a)$
$I \supseteq (a)$ ist klar, bleibt z.z. $I \subseteq (a)$
wäre $b \in I \backslash (a)$, dann Division mit Rest:

$$b = qa + r \text{ mit } \delta(r) < \delta(a) = k \text{ falls } r \neq 0$$

- für $r = 0$ wäre $b = qa \in (a)$ ↯
- für $r \neq 0$ ist $\delta(r) < k$ und $r = \underbrace{b}_{\in I} - \underbrace{qa}_{\in I} \in I \Rightarrow \delta(r) \in M$ ↯zur Minimalität von k

□

Korollar: K ein Körper $\Rightarrow K[X]$ ist ein Hauptidealring.

Bemerkung: Für einen Integritätsbereich R ist äquivalent:

(i) R ist ein Körper

(ii) $R[X]$ ist euklidisch

(iii) $R[X]$ ist ein Hauptidealring

4.5 Primideale und maximale Ideale

Problem: Nullteiler in Restklassenring können entstehen, wenn $\underbrace{(X+I)(Y+I)}_{XY+I} = I$, d.h. $XY \in I$ ohne, dass $X \in I$ oder $Y \in I$ gilt.

Definition (1):
Ein Ideal $P \subseteq R$ heißt **Primideal**, wenn

(a) $P \neq R$

(b) $a, b \in R$ und $a \cdot b \in P \Rightarrow a \in P$ oder $b \in P$

Bemerkung: $\{0\}$ ist Primideal $\Leftrightarrow R$ ist nullteilerfrei

---

Satz (1): R ein kommutative Ring mit $1 \neq 0, P \subseteq R$ Ideal:

$$P \text{ Primideal} \Leftrightarrow R/P \text{ Integritätsbereich}$$

Beweis:

$\boxed{\Rightarrow}$

$a + P$ ist Nullteiler in $R/P \Rightarrow \exists b \in R \backslash P$:

$$\underbrace{(a+P)\cdot(b+P)}_{ab+P} = P \Rightarrow ab \in P \overset{b \notin P}{\Rightarrow} a \in P \Rightarrow a + P = P \quad \text{[Nullklasse]}$$

$\boxed{\Leftarrow}$

$a \cdot b \in P \Rightarrow (a+P)(b+P) = ab+P = 0+P \Rightarrow a+P = P$ oder $b+P = P \Rightarrow a \in P$ oder $b \in P$

□

Definition (2):
Ein Ideal $M \subseteq R$ heißt **maximales Ieal**, wenn

(a) $M \neq R$

(b) $\nexists$ Ideal $I \subseteq R$ mit $M \subsetneq I \subsetneq R$

[(b) $\Leftrightarrow \forall$ Ideale $I \subseteq R$ mit $I \supseteq M \Rightarrow I = R$ oder $I = M$]

(Es kann verschiedene maximale Ideale geben.)

Satz (2): R ein kommutativer Ring mit $1 \neq 0$, $M \subseteq R$ ein Ideal:

$$M \text{ maximales Ideal } \Leftrightarrow R/M \text{ Körper}$$

Beweisskizze:

- falls $1 \in M$, dann $M = R$ und $R/M = \{0+M\}$ kein Körper und M nicht maximales Ideal
- $1 \notin M \Rightarrow R/M$ Ring mit $1+M \neq 0+M$. Nach Satz (ii) und (iii) in 4.1 (bzw. UE) ist R/M ein Körper $\Leftrightarrow R/M$ besitzt keine nichttrivialen Ideale $\Leftrightarrow \nexists I \subseteq R$ Ideal mit $M \subsetneq I \subsetneq R$.

□

Korollar: R ein kommutativer Ring mit $1 \neq 0$, dann ist jedes maximale Ideal auch ein Primideal.

Beispiele:

1. In $\mathbb{Z}$ ist jedes Ideal von der Form $m\mathbb{Z}$; $0 \cdot \mathbb{Z} = \{0\}$ und $1 \cdot \mathbb{Z} = \mathbb{Z}$ keine maximalen Ideale; also $m \geq 2$:

   $$\underset{(\Leftrightarrow m\mathbb{Z} \text{ Primideal})}{\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \text{ Integritätsbereich}} \overset{\mathbb{Z}_m \text{endl.}}{\Leftrightarrow} \underset{(\Leftrightarrow m\mathbb{Z} \text{ maximales Ideal})}{\mathbb{Z}_m \text{ Körper}} \Leftrightarrow m \text{ Primzahl}$$

   also: $\underline{m\mathbb{Z} \text{ Primzahl} \Leftrightarrow m\mathbb{Z} \text{ maximales Ideal} \Leftrightarrow m \text{ Primzahl}}$

   Weiters: $m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow m = nk$ mit $k \in \mathbb{Z} \Leftrightarrow n|m$

   Somit: $m\mathbb{Z}$ ist im maximalen Ideal $p\mathbb{Z}$ enthalten, wenn p Primteiler von m ist.

2. $K[X]$ mit Körper K (Hauptidealring). Sei $a \in K$ und $\varphi : K[X] \to K$, $f \mapsto f(a)$...Auswertng bei a
   - φ Ringhomomorphismus
   - $f \in Ker(\varphi) \Leftrightarrow f(a) = 0 \Rightarrow f = (X-a)q$, $q \in K[X] \Rightarrow Ker(\varphi) \subseteq (X-a) \cdot K[X]$; da $Ker(\varphi)$ Ideal und $K[X]$ Hauptidealring, muss $Ker(\varphi) = (X-a) \cdot K[X] = (X-a)$ gelten.
   - φ surjektiv, weil $\forall b \in K : \varphi(b) = b$

Isomorphiesatz $\Rightarrow K[X]/(X-a) \cong K$...Körper $\Rightarrow (X-a) = Ker(\varphi)$ ist maximales Ideal in $K[X]$

3. Betrachte nun $\varphi : \mathbb{R}[X] \to \mathbb{C},\ f \mapsto f(i)$ [Variable von 2., $i \notin \mathbb{R}$]
   - φ Ringhomomorphismus (vgl. UE)
   - $Ker(\varphi) = (X^2+1)$ (vgl. UE)
   - φ surjektiv, weil $\varphi(a) = a\ \forall a \in \mathbb{R}$ und $\varphi(X) = i$, also $\varphi(a+bX) = a+ib$ Isomorphiesatz $\Rightarrow \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$... Körper $\Rightarrow (X^2+1)$ maximales Ideal in $\mathbb{R}[X]$

Bemerkung:

(i) In $\mathbb{C}[X]$ sind maximale Ideale von der Form $(X-\lambda),\ \lambda \in \mathbb{C}$

(ii) Jedes Ideal in einem kommutativen Ring mit $1 \neq 0$ ist in einem maximalen Ideal enthalten (Auswahlaxiom).

Kapitel 5

Teilbarkeit und Irreduzibilität in Integritätsbereichen

(R ist nun immer ein Integritätsbereich, also kommutativ mit 1 und nullteilerfrei, $1 \neq 0$.)

5.1 Irreduzible Elemente

Definition:
$q \in R$ heißt **irreduzibel**, wenn:

(a) $q \neq 0$ und $q \notin R^\times$

(b) falls $q = a \cdot b$ mit $a, b \in R$, dann $a \in R^\times$ oder $b \in R^\times$

andernfalls nennen wir q **reduzibel**.
Also sind 0, Einheiten und Produkte von Nichteinheiten reduzibel.

Beispiel:
$\mathbb{Z}^\times = \{-1, +1\}$ und die irreduziblen Elemente in $\mathbb{Z}$ sind genau die Primzahlen und ihre negativ gespiegelten Zahlen.

Satz: R Hauptidealring und $a \in R$ irreduzibel $\Rightarrow R/(a)$ ist ein Körper.
(Verallgemeinerung von p Primzahl $\Rightarrow \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ Körper)

Beweis:
$R/(a)$ ist kommutativer Ring mit Einselelement $[\neq (a)]$.
noch z.z.: Jedes $b + (a) \neq 0 + (a)$ ist invertierbar:
$b + (a) \neq (a) \Rightarrow b \notin (a) \Rightarrow I := \{xa + yb | x, y \in R\} \supsetneq (a)$ (wir schreiben $I = (a, b)$).
I ist (das von a und b erzeugte) Ideal:

- $I \neq \emptyset$; $(x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)a + (y_1 - y_2)b \ \in I$

- $z \in R,\ xa + yb \in I \Rightarrow z \cdot (xa + yb) = (zx)a + (zy)b\ \in I$

R Hauptideal $\Rightarrow \exists c \in R : I = (c)$; $[(c) \supsetneq (a)]$. Wegen $a \in I\ \exists d \in R : a = d \cdot c$. Wäre $d \in R^\times$, dann $c = d^{-1}a \in (a)$, also $(c) \subseteq (a)$↯
Somit $d \notin R^\times$; a irreduzibel$\Rightarrow c \in R^\times$; daher $R = (c) = I \Rightarrow 1 \in I$
$\Rightarrow \exists x, y \in R : 1 = xa + yb$, d.h. $yb - 1 \in (a)$; also $(y + (a)) \cdot (b + (a)) = yb + (a) = 1 + (a)$, d.h. $b + (a)$ ist invertierbar.

□

Bemerkung: $p \neq 0, p \notin R^\times$, dann gilt:

$$p \text{ irreduzibel} \Leftrightarrow (p) \text{ maximal als Hauptideal}$$

[d.h. $\nexists a \in R : (p) \subsetneq (a) \subsetneq R$; Beweis als UE]

5.2 Teiler und Primelemente

$a \in R$ heißt **Teiler** von $b \in R$, wir schreiben $a|b$, wenn gilt:

$$\exists c \in R \text{ mit } b = c \cdot a$$

Einfache Eigenschaften:

(i) $a|b \Leftrightarrow (b) \subseteq (a)$

(ii) $a|0,\ 1|a,\ a|a\ ;\quad 0|a \Leftrightarrow a = 0$

(iii) $a|b$ und $b|c \Rightarrow a|c\ ;\quad a|b$ und $c|d \Rightarrow ac|bd$

(iv) $a|b_1$ und $a|b_2 \Rightarrow a|(x_1b_1 + x_2b_2) \quad \forall x_1, x_2 \in R$

(v) $a|1 \Leftrightarrow a \in R^\times$

(vi) $a|b \Rightarrow (ax)|b \quad \forall x \in R^\times$
($\Leftarrow$ folgt aus $x = 1$)

(Alle Beweise unmittelbar klar; (vi): $b = ca \Rightarrow b = c(x^{-1}x)a = (cx^{-1})(xa)$.)

Bemerkung: Diese Eigenschaften sind allesamt bekannt aus der Zahlentehorie für $R = \mathbb{Z}$, mit der Spezialsituation, dass $\mathbb{Z}^\times = \{-1, +1\}$ besonders einfach ist, sodass in $\mathbb{Z}$: $a|b \Leftrightarrow a|(-b)$. Allgemeiner: $a \sim b :\Leftrightarrow a|b$ und $b|a$, a und b heißen dann **assoziert**.

$$a \sim b \Leftrightarrow \exists x \in R^\times : b = x \cdot a \Leftrightarrow (a) = (b)$$

(Beweis als UE)

Definition:
$p \in R$ heißt **Primelement** oder **prim**, wenn:

(a) $p \neq 0$ und $p \notin R^\times$

(b) falls $p|(ab)$ mit $a, b \in R$, dann $p|a$ oder $p|b$.

Lemma: Jedes Primelement ist irreduzibel.

Beweis:
Sei $p = a \cdot b$, dann muss also $p|a$ oder $p|b$ gelten. O.B.d.A. $p|a$, somit:

$$\exists c \in R : a = cp \Rightarrow \underline{p} = ab = (cp)b = \underline{(cb)p} \overset{\text{KZR}}{\Rightarrow} cb = 1 \Rightarrow b \in R^\times$$

(Verwenden, dass $p = 1(ab),\ p$ prim)

□

Beispiel:
In $\mathbb{Z}$ sind genau die Primzahlen und deren Negative die Primelemente. Wir werden gleich sehen, dass die Begriffe irreduzibel und prim in Hauptdiagonalringen immer zusammentreffen.

Bemerkung: $p \neq 0,\ p \notin R^\times$, dann gilt:

$$p \text{ prim } \Leftrightarrow (p) \text{ Primideal}$$

(Beweis als UE)

Satz: In einem Hauptidealring stimmen die Begriffe Primelement und irreduzibles Element überein. Weiters ist ein Ideal ein Primideal genau dann, wenn es ein maximales Ideal ist.

Beweis:
Wir wissen bereits, dass „prim ⇒ irreduzibel“ (obiges Lemma) und „maximales Ideal ⇒ Primideal“ (Korollar in 4.5) gilt.

- ist p irreduziel im Hauptidealring $R \overset{5.1\ Satz}{\Rightarrow} R/(p)$ Körper $\overset{4.5\ Satz\ 2}{\Rightarrow} (p)$ maximales Ideal $\Rightarrow (p)$ Primideal $\overset{\text{obige Bem}}{\Rightarrow} p$ prim.
- ist I Primideal im Hauptidealring $R \Rightarrow \exists p \in R : I = (p) \overset{\text{obige Bem.}}{\Rightarrow} p$ prim $\Rightarrow p$ irreduzibel $\overset{5.1\ Satz}{\Rightarrow} R/(p)$ Körper $\overset{4.5,\ Satz\ 2}{\Rightarrow} (p)$ maximales Ideal $\overset{(p)=I}{\Rightarrow} I$ maximales Ideal

□

Beispiel:
$\mathbb{Z}[X]$ kein Hauptidealring (4.4, Bsp. 3). $X \in \mathbb{Z}[X]$ Primelement: $X|(f \cdot g) \Rightarrow X|f$ oder $X|g$, daher (X) Primideal, aber nicht maximal: $(X) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$ (siehe 4.4, Bsp. 3)

5.3 Eindeutige Primfaktorenzerlegung

Ohne Beweise soll an dieser Stelle erwähnt werden, dass jeder Hauptidealring - also spzeilell $\mathbb{Z}$ und $K[X]$ für einen Körper K - sowie auch $\mathbb{Z}[X]$ (kein Hauptidealring) die folgende Eigenschaft besitzen:
Für jedes $a \in R,\ a \neq 0$ und $a \notin R^\times$ gibt es irreduzible (oder gleichwertig prime) Elemente $q_1, ..., q_r \in R$ mit $a = q_1 \cdot ... \cdot q_r$ und diese Darstellung ist eindeutig bis auf die Reihenfolge und Einheiten als Faktoren.

Solche Integritätsbereiche heißen **faktorielle Ringe** (oder auch **Gauß'sche Ringe** oder **ZPE-Ringe**).
Es kann dann eine Teilmenge $P \subseteq R$ von Primelementen (bzw. irreduziblen Elementen) ausgewählt werden (je ein Vertreter für alle assoziierten Elemente), sodass wir schreiben können (mit „endlichem“ Produkt):

$$a = \varepsilon(a) \cdot \prod_{p \in P} p^{\nu_p(a)}$$

mit $\varepsilon(a) \in R^\times,\ \nu_p(a) \in \mathbb{N}$, nur endlich viele $\neq 0$.

5.4 Irreduzibilität von Polynomen

Erinnere: $R[X]^\times = R^\times$ für Integritätsbereich R (Sätzchen in 3.6). Also:

$$f \in R[X]^\times \Leftrightarrow f = a_0 \text{ mit } a_0 \in R^\times$$

Beispiele (für die Änderung der Irreduzibilätit beim Übergang zu anderem Grundring):

1. $f = 2X$ irreduzibel in $\mathbb{Q}[X]$, reduzibel in $\mathbb{Z}[X]$:
   - in $\mathbb{Z}[X]$: $f = 2 \cdot X$ und weder 2 noch X sind Einheit
   - in $\mathbb{Q}[X]$: $2X = g \cdot h \Rightarrow \deg(g) + \deg(h) = 1$. O.B.d.A $\deg(g) = 0,\ \deg(h) = 1$, d.h. $g = a_0,\ h = b_0 + b_1 X$. Somit

     $$2X = a_0 \cdot (b_0 + b_1 X) = a_0 b_0 + a_0 b_1 X \Rightarrow a_0 b_0 = 0, a_0 b_1 = 2 \Rightarrow \underbrace{a_0 \neq 0}_{\Rightarrow g \text{ Einheit}}, b_0 = 0$$

2. $f = 2$ ist reduzibel in $\mathbb{Q}[X]$, irreduzibel in $Z[X]$:
   - In $\mathbb{Q}[X]$: 2 ist invertierbar, also eine Einheit
   - in $\mathbb{Z}[X]$: $2 = g \cdot h \Rightarrow \deg(g) = \deg(h) = 0$. $2 = a_0 b_0 \Rightarrow (a_0 = 2 \wedge \underbrace{b_0 = 1}_{\text{Einheit}})$ oder $(\underbrace{a_0 = 1}_{\text{Einheit}} \wedge b_0 = 2) \Rightarrow g$ oder h ist eine Einheit.
3. $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$, reduzibel in $\mathbb{C}[X]$
   - in $\mathbb{C}[X]$: $X^2 + 1 = (X - i)(X + i)$ - beide Terme sind keine Einheiten, weil $\deg > 0$.
   - In $\mathbb{R}[X]$: wissen aus 4.5, Bsp. 3, dass $(X^2 + 1)$ maximales Ideal ist, weil $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ Körper, somit $X^2 + 1$ irreduzibel nach 5.1.

     Kann aber auch direkt bewiesen werden, z.B. so:
     $X^2 + 1 = g \cdot h \Rightarrow \deg(g) + \deg(h) = 2$. $\deg(g) = 0$ oder $\deg(h) = 0$ ergibt, dass g oder h Einheit ist, weil $\mathbb{R}$ ein Körper ist.
     Bleibt $\deg(g) = \deg(h) = 1$ zu betrachten, d.h.

     $$g = a_0 + a_1 X,\ h = b_0 + b_1 X \overset{a_1, b_1 \neq 0}{\Rightarrow} X^2 + 1 = a_1 b_1 (X + \frac{a_0}{a_1})(X + \frac{b_0}{b_1}) \Rightarrow X^2 + 1$$

     hat reelle Nullstellen $-\frac{a_0}{a_1}, -\frac{b_0}{b_1}$, aber $X^2 + 1 \geq 1$ hat keine reellen Nullstellen ↯
4. $a \in R \Rightarrow X - a$ irreduzibel in $R'[X]$ für jeden Oberring R' von R (mit demselben Einselelement):

   $X - a = f \cdot g \Rightarrow f = a_0,\ g = b_0 + b_1 X \Rightarrow a_0 \cdot b_1 = 1 \Rightarrow a_0 \in R^\times \subseteq (R')^\times \Rightarrow f$ ist Einheit

Also: In $K[X]$, K Körper:

- $aX + b$ teilt $f \Leftrightarrow f$ hat Nullstelle $-\frac{b}{a}$
- $f \in K[X]$, $\deg(f) = 2 : f$ irreduzibel $\Leftrightarrow f$ hat keine Nullstelle in K

Bemerkung: Beispiel 2.) (2 reduzibel in $\mathbb{Q}[X]$ und irreduzibel in $\mathbb{Z}[X]$) ist ein Ausnahmefall (man könnte auch „Unfall“ dazu sagen), denn für $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ gilt der **Irreduzibilitätssatz**:

$$f \text{ irreduzibel in } \mathbb{Z}[X] \Rightarrow f \text{ irreduzibel in } \mathbb{Q}[X]$$

Irreduzibilität in $K[X]$ für K Körper:

Wegen $K^\times = K\backslash\{0\}$ sind alle Polynome vom Grad 0 Einheiten in $K[X]$, und dies sind alle Einheiten, also

$$K[X]^\times = \{f = a_0 | a_0 \in K\backslash\{0\}\} = \{f | \deg(f) = 0\}$$

Ist $f = g \cdot h$ und g oder h eine Einheit in $K[X]$, dann folgt also $f = a_0 \cdot q$ mit $a_0 \in K\backslash\{0\}$, $q \in K[X]$, d.h. irreduzible Polynome $f \in K[X]$ erfüllen $\deg(f) \geq 1$ (sonst $f = 0$ oder $\underbrace{f = a_0 \text{ mit } a_0 \neq 0}_{f \text{ Einheit}}$) und lassen sich nur durch Herausheben eines konstanten Faktors $\neq 0$ als Produkt von Polynomen aus $K[X]$ zerlegen.

Insbesondere haben irreduzible Polynome vom Grad ≥ 2 keine Nullstellen in K. (Umkehrung gilt nicht: $(X^2 + 1)(X^2 + 1)$ ist irreduzibel und hat keine Nullstelle in $\mathbb{R}$).

Bemerkung: In $K[X]$, $a, b \in K$:

- $aX + b$ teilt $f \Leftrightarrow f$ hat Nullstelle $-\frac{b}{a}$ $(\in K)$
- Für $\deg(f) = 2$ gilt: f irreduzibel $\Leftrightarrow g$ hat keine Nullstellen in K

Teil III

Körper(Erweiterungen)

Kapitel 6

Grundlegende Begriffe

6.1 Charakteristik

R ein Ring mit 1, $n \in \mathbb{N}$, $a \in R$, dann setze $n \cdot a := \underbrace{a + ... + a}_{n-\text{mal}}$ (bzw. $0 \cdot a = 0$), $(-n) \cdot a := n \cdot (-a)$.
$\varphi : \mathbb{Z} \to R,\ n \mapsto n \cdot 1$ ist Ringhomomorphismus $\Rightarrow \ker(\varphi)$ ist Unterring ($\Rightarrow$ Untergruppe) $\Rightarrow \exists m \in \mathbb{N} : \ker(\varphi) = m\mathbb{Z}$

Wir nennen $\text{char}(R) := m$ die **Charakteristik** von R.

- $\text{char}(R) = 0$ heißt, dass φ injektiv $\mathbb{Z} \to R$ ist
- falls $\text{char}(R) > 0$, dann gilt

$$\text{char}(R) = \min\{k \in \mathbb{N} | k > 0,\ k \cdot 1 = 0\}$$

Satz: K Körper $\Rightarrow \text{char}(K) = 0$ oder $\text{char}(K)$ ist Primzahl.

Beweis:
Sei $m = \text{char}(K)$ und $m > 1$ [$\text{char}(K)$ würde $1 = 0$ implizieren, was für einen Körper unmöglich ist.] Wäre m nicht prim, dann $\exists k, l \in \mathbb{N} :\ m = k \cdot l,\ 1 < k, l < m \Rightarrow 0 = m \cdot 1 = (kl) \cdot 1 = (k \cdot 1) \cdot (l \cdot 1)$....$K$ Körper! $\Rightarrow k \cdot 1 = 0$ oder $l \cdot 1 = 0 \Rightarrow \text{char}(K) < m$ ↯

□

6.2 Grad einer Körpererweiterung

Sei $F \subseteq K$ eine Körpererweiterung (F Unterkörper von K), wenn L weiterer Unterkörper von K mit $F \subseteq L$, dann nenen wir $F \subseteq L \subseteq K$ einen **Zwischenkörper**.

Beispiel:
$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

! Idee: K kann als Vektorraum über F angesehen werden: Vektoraddition in K, skalare Multiplikation $F \times K \to K$, $(x, y) \mapsto x \cdot y$ mittels Einschränkung der üblichen Multiplikation in K.

Definition:
Der Körpergrad von $F \subseteq K$ ist

$$[F : K] := \dim_F(K) \text{...Vektorraumdimension von } K \text{ als } F\text{-Vektorraum}$$

Beispiele:

1. $[\mathbb{C} : \mathbb{R}] = 2$... $\dim_{\mathbb{R}}(\mathbb{C})$ (klar)
2. $[\mathbb{R} : \mathbb{Q}] = \infty$, denn wäre $\mathbb{R}$ als $\mathbb{Q}-$Vektorraum endlichdimensional mit Basis $x_1, ..., x_n \in \mathbb{R}$
$$\Rightarrow \mathbb{R} = \{\lambda_1 x_1 + ... + \lambda_n x_n | \lambda_1 ... \lambda_n \in \mathbb{Q}\}$$
$\mathbb{R}$ ist überabzählbar, diese Menge ↑ ist abzählbar, da sie gleichmächtig mit $\mathbb{Q}^n$ ist $\Rightarrow$ Widerspruch ↯

Satz (Gradformel): $F \subseteq L \subseteq K$ Zwischenkörper $\Rightarrow [K : F] = [K : L] \cdot [L : F]$

Beweis:
Falls $\dim_L(K) = \infty$ oder $\dim_F(L) = \infty$, dann auch $\dim_F(K) = \infty$, denn eine L-linear unabhängige Menge in K ist sicher auch F-linear unabhängig bzw. eine F-linear unabhängige Menge in L ist auch F-linear unabhängig in $K \supseteq L$.
Bleibt also der Fall $[L : F] = m < \infty$ und $[K : L] = n < \infty$ zu betrachten:
Sei $x_1, ..., x_m$ Basis in F-Vektorraum L und $y_1, .., y_n$ Basis im L-Vektorraum K. Wir zeigen: $\{x_i \cdot y_j | i = 1, ..., m \text{ und } j = 1, ..., n\}$ ist Basis im F-Vektorraum K (das ergibt $m \cdot n$ Basiselemente, also fertig).

- $y \in K$ beliebig hat eindeutige Darstellung $y = b_1 y_1 + ... + b_n y_n$ mit $b_1, ..., b_n \in L$.

$\forall j$: es gibt eindeutige Darstellung $b_j = a_{1j} \cdot x_1 + ... + a_{mj} \cdot x_m$ mit $a_{ij} \in F$, daher $y = \sum_{i,j} a_{ij} x_i y_j$, also $\text{span}\{x_i \cdot y_j\} = K$

- $\{x_i y_j | i = 1, ..., m,\ j = 1, ..., n\}$ ist linear unabhängig über F:

$$\sum_{i,j} \underbrace{a_{ij}}_{\in F} x_i y_j = 0 \Rightarrow \sum_j \underbrace{\left(\sum_i a_{ij} x_i \right)}_{\in L} y_j = 0$$

(y_j linear unabhängig über L)

$$\Rightarrow \forall_j : \sum_i a_{ij} x_i = 0$$

(x_i linear unabhängig über F)

$$\Rightarrow a_{ij} = 0 \ \forall i \forall j$$

□

Korollar: $F \subseteq L \subseteq K$ Zwischenkörper und $[K : F] < \infty$, dann gilt:

(a) $[K : L] = [K : F] \Rightarrow F = L$

(b) $[K : F]$ Primzahl $\Rightarrow F = L$ oder $L = K$

Beweis: (a) $\underbrace{[K : F] = [K : L]}_{\neq \infty} \cdot [L : F] \Rightarrow [L : F] = 1$, also wegen $L \supseteq F$ als Vektorraum $L = F$

(b) $\underbrace{[K : F]}_{\text{prim}} = [K : L] \cdot [L : F] \Rightarrow [K : L] = 1$ oder $[L : F] = 1 \Rightarrow K = L$ oder $L = F$

□

Beispiel:
$[\mathbb{C} : \mathbb{R}] = 2$ prim $\Rightarrow$ es gibt keine echten Zwischenkörper $\mathbb{R} \subsetneq L \subsetneq \mathbb{C}$!

6.3 Adjunktion von Elementen

Sei $F \subseteq K$ eine Körpererweiterung und $A \subseteq K$
$F(A)$...kleinster Zwischenkörper $F \subseteq F(A) \subseteq K$ mit $A \subseteq F(A)$
$F[A]$...kleinster Unterring von K mit $F \cup A \subseteq F(A)$

Beispiele:

1. $F = \mathbb{R},\ K = \mathbb{C},\ A = \{i\} : \{a + bi | a, b \in \mathbb{R}\} = \mathbb{R}(i) = \mathbb{C}$, weil $\mathbb{R}(i) \neq \mathbb{R}$ und $\nexists$ echter Zwischenkörper $\mathbb{R} \subsetneq L \subsetneq C$

2. Im Falle $A = \{a\}$ schreiben wir $F[A] = F[a],\ (F(A) = F(a))$, es gilt

$$F[a] = \{f(a) | f \in F[X]\}$$

   denn $\sigma_a : f \mapsto f(a)$ ist Homomorphismus $F[X] \to K$, daher $S := \sigma_a(F[X]) = \{f(a) \in K | f \in F[X]\}$ ein Unterring von K mit $a \in S$, weil $\sigma_a(X) = a$; somit $F[a] \subseteq S$; ist R ein Unterring von K mit $a \in R$ und $F \subseteq R \Rightarrow f(a) \in R\ \forall f \in F[X]$, weil $f = b_0 + ... + b_n X^n$ ergibt $f(a) = b_0 + ... + b_n a^n \in R$, also $S \subseteq R$; somit S minimal, d.h. $F[a] = S$.

   □

3. Ohne Beweis: $\{a \cdot b^{-1} | a, b \in F[A], b \neq 0\} = F(A) = Q(F[A])$...Quotientenkörper

4. (Bsp-Fortsetzung:) $\mathbb{R}[i] = \{f(i) \in \mathbb{C} | f \in \mathbb{R}[X]\}$ mit $f(X) = a + bX\ (a, b \in \mathbb{R})$ ergibt sich $f(i) = a + bi$, also $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$.

Bemerkung: $F(A_1 \cup A_2) = ((F(A_1))(A_2)$, speziell $F(\{a_1, a_2\}) = (F(a_1))(a_2)$

6.4 Algebraische und transzendente Elemente

Definition:
Sei $K \supseteq F$ eine Körpererweiterung.
$a \in K$ heißt **algebraisch** über F, falls $\exists$ Polynom $f \in F[X], f \neq 0$ mit $f(a) = 0$.
Andernfalls heißt a **transzendent** über F

Bemerkung: (i) $\forall a \in K : a$ algebraisch über K, denn $f = X - a \in K[X]$ hat eine Nullstelle in a.

(ii) $K = F(X) \supseteq F$, ($F(X)$ eine rationale Funktion): hier ist X transzendent über F, denn $\forall f \in F[X]$ mit $f \neq 0$ ist $f(X) = f \neq 0$ [vgl. Ü-Aufgabe 34(b)].

(iii) (Ohne Beweise:) e und π in $\mathbb{R}$ sind transzendent über $\mathbb{Q}$.

Betrachte den **Einsetzungshomomorphismus**

$$\sigma_a : F[X] \to K,\ f \mapsto f(a)$$

Es gilt (klarer Weise):

- a transzendent über $F \Leftrightarrow \ker(\sigma_a) = \{0\} \Leftrightarrow \sigma_a$ ist injektiv
- a algebraisch über $F \Leftrightarrow \ker(\sigma_a) \neq \{0\}$

Satz: Ist $a \in K \supseteq F$ transzendent über F, dann gilt:

(a) σ_a ergibt Isomorphismen $F[X] \to F[a]$ und $F(X) \to F(a)$

(b) $[F(a) : F] = \infty$

Beweis:

(a) Haben in 6.3 gesehen: $F[a] = \sigma_a(F[X])$ und σ_a ist injektiv, daher $F[a] \cong F[X]$, somit auch $F(a) = Q(F[a]) \cong Q(F[X]) = F(X)$.

(b) $\{1, X, X^2, X^3, ...\}$ ist eine unendliche linear unabhängige Menge im F-Vektorraum $F[X] \cong F[a]$, daher auch im F-Vektorraum $F(x) \cong F(a) \Rightarrow \dim_F(F(a)) = \infty$

□

Insbesondere folgt aus (b):

$$(*)[F(a) : F] < \infty \Rightarrow a \text{ algebraisch}$$

was wir aber noch einmal direkt durchspielen können:
Sei $dim_F(F(a)) = n$, dann sind die $n+1$ Vektoren $1, a, a^2, ..., a^n$ sicher linear abhängig, d.h. $\exists \lambda_0, ..., \lambda_n \in F$ (nicht alle 0): $\lambda_0 \cdot 1 + \lambda_1 \cdot a + ... + \lambda_n a^n = 0$, d.h. $f(a) = 0$ für $f = \lambda_0 + \lambda_1 X + ... + \lambda_n X^n \in F[X], f \neq 0$.

Lemma: Sei $a \in K$ algebraisch über F, dann gibt es ein eindeutiges nomiertes Polynom $f_a \in F[X]$ mit $\deg(f_a) \geq 1$, sodass $\ker(\sigma_a) = (f_a)$ gilt. f_a heißt **Minimalpolynom von a über F**.

Beweis:
Wir wissen, dass $\ker(\sigma_a) \neq \{0\}$ gilt. Laut Korallar in 4.4 ist $F[X]$ ein Hauptidealring, daher $\exists g \in F[X] : \ker(\sigma_a) = (g)$. Laut Beweis von Satz in 4.4 haben wir

$$\deg(g) = \min\{deg(f) | f \in \ker(\sigma_a), f \neq 0\}$$

Wir können g normieren (d.h. Leitkoeffizient gleich 1 erreichen), indem wir geeignet multiplizieren:

$$\exists c \in F : \ f_a := c \cdot g \in (g) = \ker(\sigma_a) \text{ normiert}$$

Somit gilt $(f_a) = \ker(\sigma_a)$, f_a normiert und von minimalem Grad.
Ist $h_a \in F[X]$ ebenfalls normiert mit $h_a \in \ker(\sigma_a)$ und $\deg(h_a) = \deg(f_a)$, dann folgt $h_a = r \cdot f_a$ mit $f \in F[X]$, $\deg(r) = 0$, also $r \in F$. Da h_a und f_a normiert, folgt $r = 1$.

□

6.5 Eigenschaften des Minimalpolynoms

Sei $F \subseteq K$ eine Körpererweiterung.

Lemma: Für $a \in K$ und $f \in \ker(\sigma_a)$ normiert sind äquivalent:

(i) f ist das Minimalpolynom von a

(ii) $\forall g \in \ker(\sigma_a), g \neq 0 : \deg(g) \geq \deg(f)$

(iii) f ist irreduzibel in $F[X]$

Beweis:
(i)⇒(ii): $f = f_a$ und $g \in \ker(\sigma_a) = (f_a) \Rightarrow \exists h \in F[X], \ h \neq 0 : g = h \cdot f_a$,
$\deg(h \cdot f_a) = \deg(h) + \deg(f_a) \geq \deg(f_a)$

(ii)⇒(iii): Sei $f = g \cdot h$ mit $g, h \in F[X] \Rightarrow 0 = f(a) = g(a) \cdot h(a) \Rightarrow g \in \ker(\sigma_a)$ oder $h \in \ker(\sigma_a)$, wegen $\deg(f) \leq \deg(g)$ oder $\deg(f) \leq \deg(h)$ muss g oder h den Grad 0 haben, d.h. $g \in F^\times$ oder $h \in F^\times$

(iii)⇒(i): Wegen $f \in \ker(\sigma_a) = (f_a)$ $\exists h \in F[X], \ h \neq 0 : f = h \cdot f_a$. Wegen $f_a \notin F^\times$ (Grad ≥ 1!) muss nach (iii) $h \in F^\times$ gelten. f und f_a normiert $\Rightarrow h = 1$, also $f = f_a$

□

Satz: a algebraisch über F, $f_a \in F[X]$ das Minimalpolynom, dann gilt:

(a) $F[a] = F(a) \cong F[X]/(f_a)$

(b) $[F(a) : F] = \deg(f_a)$

(c) $n = \deg(f_a) \Rightarrow 1, a, a^2, ..., a^{n-1}$ ist Basis des F-Vektorraumes $F(a)$.

(Erinnere: $\sigma_a : F[X] \to K, f \mapsto f(a)$.)

Beweis:

(a) $(f_a) = \ker(\sigma_a)$, $Im(\sigma_a) \overset{6.3}{=} F[a]$. Isomorphiesatz $\Rightarrow F[a] \cong F[X]/(f_a)$, f_a ist nach Lemma irreduzibel, daher ist $F[X]/(f_a)$ und somit $F[a]$ ein Körper (Satz 5.1), also $F(a) = F[a]$

(b),(c) Zunächst Behauptung

$$(*) \quad F[a] = \{h(a) \in K | h \in F[X],\ \deg(h) < \deg(fa)\}$$

denn: $b \in F[a] \Rightarrow \exists g \in F[X] : b = g(a)$. Division mit Rest: $g = q \cdot f_a + h$ mit $\deg(h) < \deg(fa)$. Es ist insbesondere $g(a) = q(a) \cdot \underbrace{f_a(a)}_{0} + h(a) \Rightarrow g(a) = h(a)$, d.h. $b \in$ rechter Seite in $(*)$. $F[a] \supseteq$ rechter Seite in $(*)$ ist klar. Sei also $n = \deg(f_a)$ - nach $(*)$ gilt

$$F[a] = \{\lambda_0 + \lambda_1 a + ... + \lambda_{n-1} a^{n-1} | \lambda_0, ..., \lambda_{n-1} \in F\} =$$

$$= \text{span}\{1, a, a^2, ..., a^{n-1}\} \text{ im F-Vektorraum } F[a] = F(a)$$

noch zu zeigen: $1, a, ..., a^{n-1}$ sind linear unabhängig.
Angenommen $\exists \lambda_0, ..., \lambda_{n-1} \in F$ mit $(\lambda_0, ..., \lambda_{n-1}) \neq 0$ in F^n, sodass $\lambda_0 + \lambda_1 a + ... + \lambda_{n-1} a^{n-1} = 0$, dann wäre $f := \lambda_0 + \lambda_1 X + ... + \lambda_{n-1} X^{n-1} \in F[X]$, $f \neq 0$ mit $f(a) = 0$ und $\deg(f) < \deg(f_a)$ ↯
Somit ist $1, a, ..., a^{n-1}$ Basis von $F(a)$ (also gilt (c)) und $[F(a) : F] = n = \deg(f_a)$ (also gilt (b)).

□

Beispiel:
$F = \mathbb{Q}$, $a \in \mathbb{C}$ mit $b := a^2 \in \mathbb{Q}$, aber $a \notin Q$ (z.B. $a = i$ oder $a = \sqrt{(2)}$,...), dann ist $X^2 - b \in \mathbb{Q}[X]$ irreduzibel [sonst $X^2 - b = (X - b_1)(X - b_2)$ und $b_1, b_2 \in \mathbb{Q}$ Nullstellen von $X^2 - b \Rightarrow \{b_1, b_2\} = \{a, -a\} \not\subseteq \mathbb{Q}$].

Da $X^2 - b$ auch normiert ist, ist $f_a = X^2 - b$ das Minimalpolynom von a über $\mathbb{Q}$.
$[\mathbb{Q}(a) : \mathbb{Q}] = \deg(f_a) = 2$ und $\mathbb{Q}(a) = \mathbb{Q}[a] = \{\alpha + \beta a | \alpha, \beta \in \mathbb{Q}\}$

$$\frac{1}{\alpha + \beta a} = \frac{\alpha - \beta a}{(\alpha + \beta a)(\alpha - 1a)} = \frac{\alpha - \beta a}{\alpha^2 - \beta^2 a^2} = \frac{\alpha}{\alpha^2 - \beta^2 b} + \frac{-\beta}{\alpha^2 - \beta^2 b} \cdot a \in \mathbb{Q}(a)$$

6.6 Kurzer Ausblick

(A) Körpererweiterung $K \supseteq F$ heißt **algebraisch**, falls jedes $a \in K$ algebraisch über F ist.

Im Falle $[K : F] = n < \infty$ („**endliche Körpererweiterung**“) ist $K \supseteq F$ algebraisch, denn für $a \in K$ muss $1, a, ..., a^n$ linear abhängig sein, d.h. $\exists \lambda_0, ..., \lambda_n \in F$ (nicht alle 0): $\lambda_0 + \lambda_1 a + ... + \lambda_n a^n = 0$, d.h. $f := \lambda_0 + \lambda_1 X + ... + \lambda_n X^n \in F[X]$, $f \neq 0$ und $f(a) = 0$.
Insbesondere ist $\mathbb{C} \supseteq \mathbb{R}$ algebraisch. (Konkret tritt $w = a + bi$ als Nullstelle von $(X - (a + bi)) \cdot (X - (a - bi)) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$ auf.)

(B) Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes Polynom $f \in K[X]$ mit $\deg(f) \geq 1$ mindestens eine Nullstelle in K hat.
Durch sukzessive Anwendung von 3.7 (Nullstellen $\rightsquigarrow$ Linearfaktoren) können wir also $f \in K[X]$ mit $n = \deg(f) \geq 1$ in diesem Fall immer in der Form $f = a \cdot (X - x_1) \cdot ... \cdot (X - x_n)$ schreiben mit $a \in K^\times$. $x_1, ..., x_n \in K$ (die Nullstellen). Also:

K algebraisch abgeschlosse n$\Leftrightarrow$ jedes irreduzible Polynom in $K[X]$ hat Grad 1

Fundamentalsatz der Algebra:

$\mathbb{C}$ ist algebraisch abgeschlossen. (Ohne Beweis).
„Ironie dabei“: Es gibt keinen rein algebraischen Beweis davon (Topologie oder komplexe Analysis oder Analysis...)

Reelle Fassung: $f \in \mathbb{R}[X]$ mit $n := \deg(f) \geq 1$ hat Darstellung
$f = (X - x_1) \cdot ... \cdot (X - x_m) \cdot g_1 \cdot ... \cdot g_r$, wobei $m + 2r = n$, $x_1, ..., x_m$ die reellen Nullstellen und $g_1, ..., g_r$ irreduzible quadratische Polynome in $\mathbb{R}[X]$ sind.

Bemerkung: Ein algebraisch abgeschlossener Körper muss unendlich viele Elemente besitzen.
(Denn andernfalls $K = \{a_0, a_1, ..., a_n\}$ hätte Polynom $f := (X - a_0) \cdot (X - a_1) \cdot ... \cdot (X - a_n) + 1$ in $K[X]$ ohne Nullstelle, weil $f(a_j) = 1$ $(j = 1, ..., n)$.

(C) Für $f := a_nX^n + ... + a_rX^r + ... + a_1X + a_0 \in F[X]$ ist **formale Ableitung** definiert durch

$$f' = n \cdot a_nX^{n-1} + ... + r \cdot a_rX^{r-1} + ... + a_1 \in F[X]$$

Rechenregeln für $F[X] \to F[X],\ f \mapsto f'$:

- $\forall a, b \in F,\ \forall f, g \in F[X] : (af + bg)' = af' + bg'$ (F-Linearität)
- $(f \cdot g)' = f' \cdot g + f \cdot g'$ (Produktregel)

Satz: $f \in F[X]$, $\deg(f) \geq 1$, dann ist äquivalent:

(i) $\exists$ Erweiterungskörper $K \supseteq F$, in dem f mindestens eine mehrfache Nullstelle hat

(ii) f und f' haben in $F[X]$ einen gemeinsamen Teiler $g \in F[X]$ mit $\deg(g) \geq 1$

Bemerkung:
(i) Ist x Nullstelle von $f \in F[X]$, dann gilt Vielfachheit von

$$x := \max\{r \in \mathbb{N} | (X - x)^r \text{ teilt } f\}$$

(ii) $\text{char}(K) = 0 \Rightarrow$ Vielfachheit der Nullstelle $x = \max\{r \in \mathbb{N} | f(x) = ... = f^{(r-1)}(x) = 0\}$

(D) Wenn $f = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in K[X]$ vollständig in Linearfaktoren zerfällt, d.h. $f = (X - x_1) \cdot ... \cdot (X - x_n)$ mit $x_1, ..., x_n \in K$, dann ergibt sich leicht für die Koeffizienten als Funktion der Nullstellen

$a_0 = (-1)^n \cdot x_1 \cdot x_2 \cdot ... \cdot x_n$
$a_1 = (-1)^{n-1} \cdot (x_2 \cdot x_3 \cdot ... \cdot x_n + x_1x_3 \cdot ... \cdot x_n + ... + x_1 \cdot ... \cdot x_{n-1})$
$\vdots \quad \vdots \quad \vdots$
$a_{n-1} = -(x_1 + x_2 + ... + x_n)$

- sogenannter Wurzelsatz von Vieta. Rechts stehen symmetrische Funktionen, d.h. Permutation der $x_1, ..., x_n$ ändert nichts!

Frage nach Auflösung obiger Formeln nach $x_1, ..., x_n$ als Funktion der Koeffizienten $a_0, ..., a_{n-1}$ entspricht also der Suche nach Lösungsformeln für Nullstellen allgemeiner Polynome, möglichst nur durch Summen und Wurzeln in eventuellen Erweiterungskörpern („Auflösung durch Radikale“), einem sogenannten **Zerfällungskörper** K für $f \in F[X]$, also $K \supseteq F$ so, „dass f in K in Linearfaktoren zerfällt und K möglichst klein gewählt werden kann“. Klärung der Frage gelingt auf Umweg über die Gruppentheorie: Sei $K \supseteq F$ Körpererweiterung, $\text{Aut}(K; f) := \{\varphi \in \text{Aut}(K) | \varphi/_F = id_F\}$ Gruppe der Körperautomorphismen

$\varphi : K \to K$, die F fix lassen.
Wenn $K \supseteq F$ Zerfällungskörper von $f \in F[X]$ ist, so heißt

$$\mathrm{Gal}(f; F) := \mathrm{Aut}(K; F)$$

die **Galoisgruppe** von f über F.

Galoistheorie liefert Korrespondenz:

$$\text{Zwischenkörper von } K \supseteq F \leftrightarrow \text{Untergruppe von } \mathrm{Aut}(K; F)$$

Wenn $\mathrm{char}(F) = 0$, dann gilt für $f \in F[X]$:

$$f \text{ ist durch Radikale auflösbar} \Leftrightarrow \mathrm{Gal}(f; F) \text{ ist eine } \textbf{auflösbare Gruppe}$$

d.h. $\exists$ Untergruppen $N_0, N_1, ..., N_k$ von $\mathrm{Gal}(f; F)$, sodass $G = N_0 \rhd N_1 \rhd ... \rhd N_k = \{e\}$ und N_j/N_{j+1} ist abelsch $(j = 0, ..., k-1)$.

Für allgemeines Polynom n-ten Grades (d.h. mit Koeffizienten als symmetrische Funktion von n Variablen) lässt sich die Galoisgruppe mit der Permutationsgruppe S_n identifizieren (als isomorphes Bild).
Weil man zeigen kann, dass S_n für $n \geq 5$ keine auflösbare Gruppe ist, folgt, dass es keine allgemeine Lösungsformeln durch Radikale für Polynomgleichungen vom Grad ≥ 5 geben kann!
Für Grade $2, 3, 4$ sind Formeln bekannt. Für spezielle Typen/Klassen von Polynomen höheren Grades können Auflösungen durch Radikale gelingen, z.B. Kreisteilungspolynome.

Kapitel 7

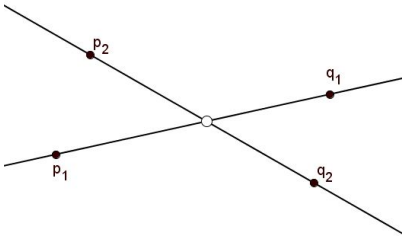
Anwendung auf Konstruktion mit Zirkel und Lineal

Zeichenebene $\mathbb{R}^2$, vorgegebene Teilmenge $M \subseteq \mathbb{R}^2$. Wir werden die Menge, der aus M mit Zirkel und Lineal (ohne Maßeinheiten darauf) exakt konstruierbaren Punkte im $\mathbb{R}^2$ mit Hilfe algebraischer Begriffe und Methoden beschreiben.

7.1 Die geometrischen Konstruktionsregeln

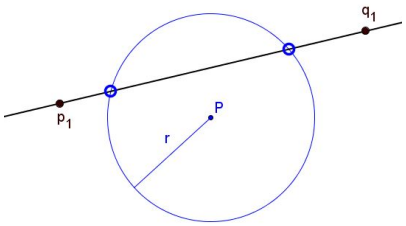
Typ I: Schnittpunkte nicht paralleler Geraden.

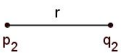
gegeben: •
konstruiert: ∘



Typ II: Schnitt Gerade mit Kreis

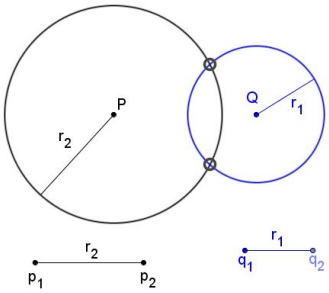
gegeben: •
konstruiert: ∘





Typ III: Schnitt zweier Kreise

gegeben: •
konstruiert: ∘



Definition:
$M \subseteq \mathbb{R}^2$, dann besteht die Menge $\underline{\text{Kon}(M) \subseteq \mathbb{R}^2}$ aus jenen Punkten $p \in \mathbb{R}^2$, für die es ein $n \in \mathbb{N}$ und eine Kette von Teilmengen $M = M_0 \subseteq M_1 \subseteq ... \subseteq M_n$ von $\mathbb{R}^2$ gibt, sodass jedes M_j aus M_{j-1} durch eine Konstruktionsregel I,II oder III entsteht und $p \in M_n$ gilt. Kon(M) heißt die Menge der aus M mit Zirkel und Lineal **konstruierbaren Punkte**. In jedem Schritt kommen 0, 1 oder 2 Punkte hinzu!

7.2 "Algebraisierung" von Kon(M)

Wir identifizieren $\mathbb{R}^2$ mit $\mathbb{C}$, damit wir die Körperstruktur von C verwenden können.

Satz: Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und setze

$$\overline{M} := \{\overline{z} | z \in M\}$$

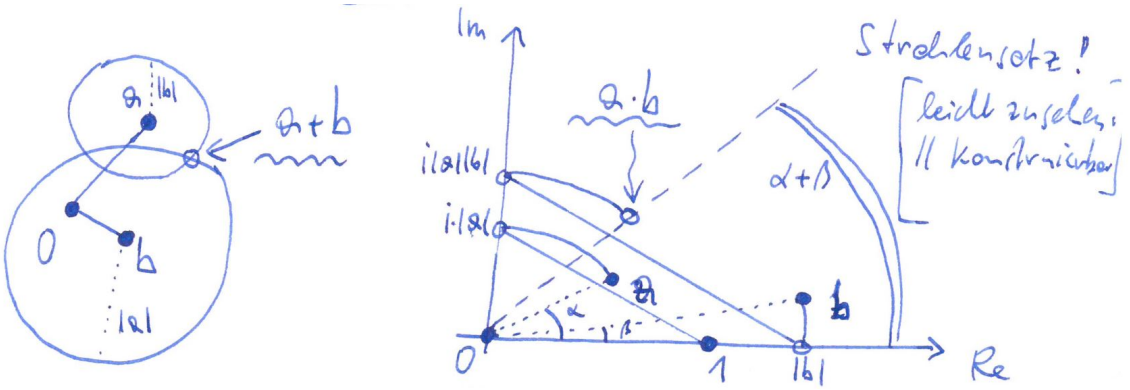
Dann gilt:

(i) Kon(M) ist Unterkörper von $\mathbb{C}$

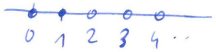
(ii) $\mathbb{Q}(M \cup \overline{M})$ ist Unterkörper von Kon(M) und $\overline{\text{Kon}(M)}$=Kon(M)

(iii) $b \in \mathbb{C}$ und $b^2 \in \text{Kon}(M) \Rightarrow b \in \text{Kon}(M)$
(in Kon(M) können also Quadratwurzeln konstruiert werden).

Beweisskizze:
$\underline{\text{ad (i)}}$: $a, b \in \text{Kon}(M)$

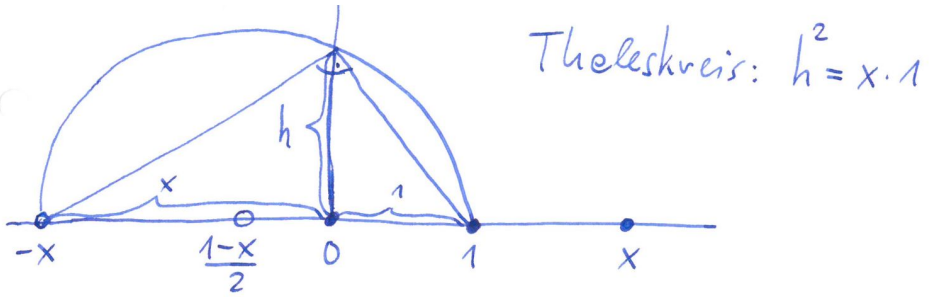


ad (ii): $0, 1 \in M \Rightarrow \mathbb{Z} \subseteq$ Kon(M) weil Kon(M) Körper muss $\mathbb{Q} = Q(\mathbb{Z}) \subseteq$ Kon(M); wegen $\overline{M} \subseteq$ Kon$(M) = \overline{\text{Kon}(M)}$ (leicht zu sehen) auch $Q(M \cup \overline{M}) \subseteq$ Kon(M).



ad (iii):

- für $x \in \mathbb{R},\ x > 0$ konstruiere $\sqrt{x}$ wie folgt:



- für $z \in \mathbb{C}$ mit $|z| = 1$ einfach Winkelhalbierung für Wurzel.

- zusammen: $b^2 \in$ Kon$(M) \Rightarrow b \in$ Kon(M)

□

7.3 Eigenschaften des Körpers Kon(M)

Für $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ haben wir Zwischenkörper $\mathbb{Q} \subseteq$ Kon$(\{0, 1\}) \subseteq$ Kon$(M) \subseteq \mathbb{C}$; es gilt

(1) Die Körpererweiterung Kon$(M) \supseteq \mathbb{Q}(\overline{M} \cup M)$ ist algebraisch (folgt aus Eigenschaft (3) unten)

(2) $[\ \mathrm{Kon}(\{0,1\}) : \mathbb{Q}] = \infty$

Beweis: Sukzessives Wurzelziehen $-1, i, e^{i\pi/4}, ..., e^{i\pi/2^4}, ...$
Minimalpolynom von $w_n := e^{i\pi/2^n}$ über $\mathbb{Q}$ ist (w_n ist eine 2^{n+1}-te Einheitswurzel) $X^{2^n} + 1$, also Index $\geq 2^n\ \forall n \in \mathbb{N}$.

(3) Für $z \in \mathbb{C}$ gilt: $z \in \mathrm{Kon}(M) \Leftrightarrow \exists$ Kette von Zwischenkörpern

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq ... \subseteq L_r \subseteq \mathbb{C}$$

mit $z \in L_r$ und $[L_j : L_{j-1}] \leq 2 \quad (j = 1, ..., r)$.

Beweisidee: Jeder Konstruktionsschritt ergibt höchstens 2 neue Punkte, die nicht im bisherigen Teilkörper liegen, aber durch eine Wurzel erfassbar sind...

Korollar: $M \subseteq \mathbb{C}$ mit $0, 1 \in M,\ L := \mathbb{Q}(M \cup \overline{M}),\ z \in \mathrm{Kon}(M) \Rightarrow [L(z) : L] = 2^m$ für ein $m \in \mathbb{N}$. Insbesondere ist z algebraisch über L.

Dieses Korollar ist entscheidend für Unlösbarkeit einiger klassischer Konstruktionsprobleme!

7.4 Das Delische Problem der Würfelverdoppelung ist unlösbar

? Kantenlänge l eines Würfels mit doppeltem Volumen des Einheitswürfels (also Kantenlänge 1) konstruierbar? Wir müssten $l = 2^{\frac{1}{3}}$ aus $M = \{0, 1\}$ konstruieren.

Behauptung: $2^{\frac{1}{3}} \notin \mathrm{Kon}(\{0,1\})$

Denn: Minimalpolynom von $2^{\frac{1}{3}}$ über $\mathbb{Q} = \mathbb{Q}(\{0,1\})$ ist $X^3 - 2$; daher $\left[\mathbb{Q}\left(2^{\frac{1}{3}}\right) : \mathbb{Q}\right] = 3$, was keine 2er-Potenz ist!

7.5 Winkeldreiteilung ist im Allgemeinen nicht exakt mit Zirkel und Lineal möglich

Natürlich können gewisse Winkel, wie etwa $270° \mathrel{\hat{=}} \frac{3\pi}{2}$ gedrittelt werden, d.h. es kann $e^{\pi i/2}$ aus $\{0, 1, e^{3\pi i/2}\}$ konstruiert werden.
Die Frage ist aber, ob für jeden gegebenen Winkel $\alpha \in [0, 2\pi]$ der Punkt $z := e^{i\alpha/3}$ aus der Menge $M := \{0, 1, \zeta\}$ mit $\zeta := e^{i\alpha}$ konstruierbar ist.

Behauptung: $\underbrace{e^{2\pi i/9}}_{z} \notin \mathrm{Kon}(\{0,1,\underbrace{e^{2\pi i/3}}_{\zeta}\})$ für $\alpha \mathrel{\hat{=}} 120° \mathrel{\hat{=}} \frac{2\pi}{3}$.

Beweis: $\overline{\zeta} = \frac{1}{3} \Rightarrow \mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}(\zeta) =: L$
Wir werden $[L(z) : L]$ aus der Gradformel bestimmen

$$(*) \quad [L(z) : \mathbb{Q}] = [L(z) : L] \cdot [L : \mathbb{Q}]$$

- $\cos\frac{2\pi}{3} = -\frac{1}{2}$, $\sin\frac{2\pi}{3} = \frac{\sqrt{3}}{2}$, also $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\zeta^2 = \frac{1}{4} - 2\cdot\frac{1}{2}i\frac{\sqrt{3}}{2} + i^2\frac{3}{4} = \frac{1}{4} - \frac{3}{4} - i\frac{\sqrt{3}}{2} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ also $\zeta^2 + \zeta = -1$, d.h. $\zeta^2 + \zeta + 1 = 0$. ζ ist Nullstelle von $X^2 + X + 1$; zweite Nullstelle ist $\overline{\zeta} \notin \mathbb{Q}$; somit ist $X^2 + X + 1$ das Minimalpolynom von ζ in $\mathbb{Q}[X]$

  $$\Rightarrow [L : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$$

- $z^6 + z^3 + 1 = e^{4\pi i/3} + e^{2\pi i/3} + 1 = \zeta^2 + \zeta + 1 = 0$, d.h. z ist Nullstelle von $X^6 + X^3 + 1 \in \mathbb{Q}[X]$ und $X^6 + X^3 + 1$ ist irreduzibel (ohne Beweis, siehe Fischer, III, §5.6) $\Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 6$. Wegen $z^3 = \zeta$ gilt $L(z) = \mathbb{Q}(\zeta)(z) = \mathbb{Q}(\{\zeta, z\}) = \mathbb{Q}(z)$ also $[L(z) : \mathbb{Q}] = 6$

- somit ergibt $(*)$: $6 = [L(z) : L] \cdot 2 \Rightarrow [L(z) : L] = 3$ keine Zweierpotenz!

□

7.6 Die Quadratur des Kreises ist unmöglich

? Kann die Seitenlänge l eines Quadrats konstruiert werden, das flächengleich mit dem Kreis vom Radius 1 ist?

Wir müssten $l = \sqrt{\pi}$ aus $M = \{0,1\}$ konstruieren. Mit $\sqrt{\pi}$ wäre aber auch π aus $\mathrm{Kon}(\{0,1\}]$; insbesondere wäre dann π algebraisch über $L = \mathbb{Q}(\{0,1\}) = \mathbb{Q}$ - Widerspruch ↯ zur Transzendenz von π. s

Index