Einführung in die Algebra

Jun.-Prof. Dr. Caroline Lassueur
TU Kaiserslautern

Kurzskript zur Vorlesung, WS 2016/17

Version: 28. März 2017
(Stand: 30. Sept. 2017)

Vorwort

Dieses Skript basiert auf einer früheren Fassung der Vorlesung von Prof. Dr. G. Malle [Mal12]. Der generelle Schreibstil dieses Skriptes ist bewusst knapp gehalten, da es schon viele Skripte für diese Vorlesung zur Verfügung gestellt werden. Siehe z. B.:

[Gat11] Andreas Gathmann, Einführung in die Algebra, Vorlesungsskript, WS 2010/11, TU Kaiserslautern.

[Mar15] Thomas Markwig, Einführung in die Algebra, Vorlesungsskript, WS 2014/15, TU Kaiserslautern.

[PS10] Gehrard Pfister und Stefan Seidel, Einführung in die Algebra, Vorlesungsskript, WS 2009/10, TU Kaiserslautern.

Für Fernstudierende empfehle ich insbesondere, das Lesen von [Gat11] als Komplement. Weitere Literatur, die für die Vorbereitung dieses Skriptes benutzt wurde, ist die folgende:

[Bos06] Siegfried Bosch, *Algebra*, 6th ed., Springer-Lehrbuch, Springer, Berlin, 2006.

[Bou70] Nicolas Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 1 à 3*, Hermann, Paris, 1970.

[Gec14a] Meinolf Geck, *Algebra: Gruppen, Ringe, Körper*, edition delkhofen, 2014.

[Gec14b] Meinolf Geck, On the characterization of Galois extensions. Amer. Math. Monthly **121** (2014), no. 7, 637–639.

[Lan84] Serge Lang, *Algebra*, second ed., Addison-Wesley Publishing Company (A.B.P.), Reading, MA,1984.

[Mal12] Gunter Malle, Einführung in die Algebra, Vorlesungsskript WS 2011/12, TU Kaiserslautern.

Ich möchte den Leser aufmerksam machen, dass der Teil über Körper und Galoistheorie anders als im [Gat11, Mal12, Mar15, PS10] gelesen wurde. Er folgt [Gec14] und dies ergibt den relativ kurzen Zugang zum Hauptsatz der Galoistheorie, basierend auf [Gec14b], welcher Artikel eine Verkürzung der Charakterisierung der Galois-Erweiterungen präsentiert.

Ich danke G. Malle für die Verfügbarkeit seines Skriptes und Pablo Luka für das Lesen dieser Fassung des Skriptes. Ich danke auch Benjamin Sambale und den Studierenden, die verschiedene Arten von Druckfehler gemeldet haben. Diese wurden mit der Farbe *Cyan* korrigiert. Weitere Kommentare und Korrekturen sind auch herzlich willkommen!

Symbolverzeichnis

Teil I: Gruppen

A_n	alternierende Gruppe vom Grad n
$C_G(x)$	Zentralisator von x in G
D_{2n}	die Diedergruppe der Ordnung $2n$
G'	Kommutatoruntergruppe von G
G_x	Stabilisator von x in G
G/N	Faktorgruppe von G nach N
$\mathrm{GL}_n(K)$	allgemeine lineare Gruppe über K
$H \leq G$, $H < G$	H ist eine Untergruppe von G, bzw. eine echte Untergruppe
$N \trianglelefteq G$, $N \triangleleft G$	N ist ein Normalteiler von G, bzw. ein echter Normalteiler
$N_G(U)$	Normalisator von U in G
$\mathcal{O}_x$	Bahn von x
$\mathrm{PGL}_n(K)$	projektive lineare Gruppe über K
S_n	symmetrische Gruppe vom Grad n
$\mathrm{SL}_n(K)$	spezielle lineare Gruppe über K
$\mathrm{Syl}_p(G)$	Menge der p-Sylow-Untergruppen der Gruppe G
$Z(G)$	Zentrum der Gruppe G
Z_m	zyklische Gruppe der Ordnung m (auch $\mathbb{Z}/m\mathbb{Z}$)
$\lvert G\rvert$	Ordnung der Gruppe G
$\lvert G : H\rvert$	Index von H in G
$[x]$	Konjugiertenklasse von x
$[g, h]$	Kommutator von g und h
$\langle g\rangle$	die von g erzeugte zyklische Gruppe

Teil II: Ringe

$\mathrm{Char}(R)$	Charakteristik des Ringes R
deg	Grad eines Polynoms
$I \trianglelefteq R$, $I \triangleleft R$	I ist ein Ideal von R, bzw. ein echtes Ideal
$K(X)$	Körper der ratiotialen Funktionen in einer Unbestimmten X
$Q(R)$	Quotientenkörper des Ringes R
$R[X]$	Polynomring in einer Unbestimmten X über R
$R^\times$	Einheiten des Ringes R
R/I	Faktorring von R nach I
$\mathbb{Z}[i]$	Ring der ganzen Gaußschen Zahlen
(a)	Hauptideal erzeugt von a
$a \mid b$	a teilt b
$a \simeq b$	a ist assoziiert zu b

Teil III: Körper

$\mathrm{Aut}(K)$	Automorphismengruppe des Körpers K
$\mathrm{Aut}(L/K)$	Automorphismengruppe der Körpererweiterung L/K
$\mathbb{F}_q$	endlicher Körper mit q Elementen
$\mathrm{Gal}(L/K)$	Galoisgruppe der Galois-Eweiterung L/K
K^H	Fixkörper von H
$K[\alpha]$	Bild des Einsetzungshomomorphismus von α
$K(\alpha)$	Körper erzeugt von K und α
L/K	Körpererweiterung
μ_α	Minimalpolynom von α
$[L:K]$	Grad der Körpererweiterung L/K

Generell

$\mathbb{C}$	Körper der komplexen Zahlen
i	$\sqrt{-1}$ in $\mathbb{C}$
Id_M	Identische Abbildung auf der Menge M
ker	Kern
$\mathbb{N}$	die Natürlichen Zahlen ohne 0
$\mathbb{N}_0$	die Natürlichen Zahlen mit 0
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{R}$	Körper der reellen Zahlen
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathbb{Z}_{\geq a}, \mathbb{Z}_{>a}, \mathbb{Z}_{\leq a}, \mathbb{Z}_{<a}$	$\{m \in \mathbb{Z} \mid m \geq a$ (bzw. $m > a, m \leq a, m < a)\}$
$\lvert X \rvert$	Mächtigkeit der Menge X
$\bigcup$	Vereinigung
$\bigsqcup$	disjunkte Vereinigung
$\bigcap$	Schnitt
$\emptyset$	leere Menge

Inhaltsverzeichnis

Vorwort **1**

Symbolverzeichnis **2**

Teil I: Gruppen **6**
1 Der Homomorphiesatz (∗) . . . 6
1.1 Gruppen, Untergruppen und Normalteiler (∗) . . . 6
1.2 Faktorgruppen (∗) . . . 8
2 Operationen von Gruppen auf Mengen . . . 11
2.1 Definitionen und Beispiele . . . 11
2.2 Die Bahnbilanzgleichung . . . 13
2.3 Die Sylowsätze . . . 15
2.4 Einfache und Auflösbare Gruppen . . . 18

Teil II: Ringe **22**
3 Ringe, Ideale und Homomorphismen (∗) . . . 22
3.1 Ringe, Körper, Integritätsbereiche (∗) . . . 22
3.2 Ideale (∗) . . . 24
3.3 Faktorringe und Ringhomomorphismen . . . 25
4 Teilbarkeit und Primzerlegung . . . 29
4.1 ZPE-Ringe . . . 29
4.2 Quotientenkörper . . . 31
4.3 Irreduzibilität in Polynomringen . . . 34

Teil III: Körper **39**
5 Endliche Körpererweiterungen . . . 39
5.1 Körpererweiterungen . . . 39
5.2 Körper-Automorphismen . . . 42
5.3 Stammkörper und Zerfällungskörper . . . 43
5.4 Die endlichen Körper . . . 46
6 Galoistheorie . . . 47
6.1 Galois-Erweiterungen . . . 47

6.2 Der Hauptsatz der Galoistheorie 50
6.3 Der Hauptsatz der Algebra 54
7 Konstruktionsaufgaben aus der Antike 56
7.1 Radikalerweiterungen 56
7.2 Konstruktionen mit Zirkel und Lineal 57
7.3 Unlösbare Konstruktionsaufgaben der Antike 59
8 Auflösbarkeit von Polynomgleichungen 61

TEIL I: GRUPPEN

1 Der Homomorphiesatz (∗)

1.1 Gruppen, Untergruppen und Normalteiler (∗)

In diesem Abschnitt fangen wir mit Erinnerungen von Begriffen und Beispielen aus der Vorlesung Algebraische Strukturen an.

Definition 1.1 (*Gruppe*)

Eine nicht-leere Menge G zusammen mit einer Verknüpfung

$$\begin{array}{rccc} \star\colon & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \star b\,, \end{array}$$

heißt **Gruppe**, falls gelten:

(G1) *Assoziativität*: $(a \star b) \star c = a \star (b \star c) \quad \forall\, a,b,c \in G$.

(G2) *Existenz eines neutralen Elementes*: Es existiert ein $e \in G$ mit $e \star a = a = a \star e \quad \forall\, a \in G$.

(G3) *Existenz inverser Elemente*: Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a \star a' = e = a' \star a$.

Gilt zudem für alle $a, b \in G$: $a \star b = b \star a$ (*Kommutativität*), so heißt G eine **abelsche** oder **kommutative** Gruppe.

Notation: Wir schreiben eine solche Gruppe als $(G, \star)$, oder einfach als G, wenn die betrachte Verknüpfung aus dem Kontext klar ist.
Meistens schreiben wir die Verknüpfung als $a \cdot b$ oder einfach ab. Das neutrale Element wird dann auch mit 1_G (oder einfach 1) bezeichnet, sowie das inverse Element mit a^{-1}. Falls die Gruppe abelsch ist, wird die Verknüpfung auch oft als Addition $a + b$ geschrieben, das neutrale Element mit 0 bezeichnet und das inverse Element mit $-a$.

Definition 1.2 (*Untergruppe*)

Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt eine **Untergruppe** von G (in Zeichen: $U \leq G$), wenn gelten:

$$1_G \in U, \qquad a \cdot b \in U \qquad \text{und} \qquad a^{-1} \in U \qquad \forall\, a, b \in U.$$

Beispiel 1

(a) $(\mathbb{Z},+)$,$(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ sind abelsche Gruppen.

(b) Für $n\in\mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z},+)=:Z_n$ eine abelsche Gruppe, die **zyklische Gruppe der Ordnung** n.

(c) Ein Vektorraum V über einem Körper K ist zunächst eine Gruppe $(V,+)$.

(d) Sei $X\neq\emptyset$ eine Menge und $S_X:=\{\pi: X\longrightarrow X\,|\,\pi \text{ bijektive Abbildung}\}$. Dann ist S_X eine Gruppe mit Hintereinanderausführung $\circ$ von Abbildungen als Verknüpfung. Diese Gruppe heißt die **Symmetrische Gruppe auf** X. (Neutrales Element: id_X, die identische Abbildung. Inverses Element: π^{-1}, die Umkehrabbildung von π.)
Für $X:=\{1,\dots,n\}$, heißt $S_n:=S_{\{1,\dots,n\}}$ die **Symmetrische Gruppe vom Grad** n. Die **alternierende Gruppe** A_n der geraden Permutationen ist eine Untergruppe von S_n.

(e) Sei K ein Körper und $n\geq 1$, dann bildet

$$\mathrm{GL}_n(K)=\{A\in M_n(K)\,|\,\det(A)\neq 0\}$$

die **allgemeine lineare Gruppe** über K. Dann ist

$$\mathrm{SL}_n(K)=\{A\in \mathrm{GL}_n(K)\,|\,\det(A)=1\}$$

eine Untergruppe von $\mathrm{GL}_n(K)$, die **spezielle lineare Gruppe**. (Nicht abelsch im allgemeinen!)

(f) Die Symmetriegruppe des regulären ebenen n-Ecks bildet eine Gruppe, die sogenannte **Diedergruppe der Ordnung** $2n$:

$$D_{2n}=\langle\sigma,\tau\,|\,\sigma^n=\tau^2=1,\tau\sigma\tau=\sigma^{-1}\rangle,$$

wobei σ eine Drehung um $\frac{2\pi}{n}$ ist und τ die Spiegelung an einer Symmetrieachse des n-Ecks ist. (Nicht abelsch im allgemeinen!)

Wir beschreiben jetzt verschiedene wichtige Untergruppen.

Definition 1.3 (*die von einer Teilmenge erzeugte Untergruppe*)

Sei $(G,\cdot)$ eine Gruppe und $M\subseteq G$ eine Teilmenge. Dann heißt

$$\langle M\rangle:=\bigcap_{M\subseteq U\leq G} U$$

die **von** M **erzeugte Untergruppe**.

Anmerkung 1.4 (*Ordnung eines Element*)

Für $M=\{g\}\subseteq G$ gilt $\langle M\rangle=\langle g\rangle=\{g^m\,|\,m\in\mathbb{Z}\}$. Dies ist die **von** g **erzeugte zyklische Untergruppe** von G. Ist $|\langle g\rangle|=n$, also $g^n=1$ und $\langle g\rangle=\{1,g,g^2,\dots,g^{n-1}\}$, so heißt $o(g):=|\langle g\rangle|$ die **Ordnung des Elementes** g.

Definition 1.5 (*Normalteiler, einfache Gruppe*)

(a) Eine Untergruppe $N \leq G$ heißt **Normalteiler** von G (in Zeichen $N \trianglelefteq G$) genau dann, wenn für alle $g \in G$ gilt $gNg^{-1} = N$.

(b) Die Gruppe G heißt **einfache Gruppe** genau dann, wenn $G \neq \{1\}$ ist und $\{1\}, G$ die einzigen Normalteiler von G sind.

Definition 1.6 (*Zentrum, Kommutator, Kommutatoruntergruppe*)

Sei $(G, \cdot)$ eine Gruppe. Dann:

(a) $Z(G) := \{g \in G \mid gh = hg \; \forall h \in G\}$ heißt **Zentrum** von G.

(b) Für $g, h \in G$, heißt $[g, h] := ghg^{-1}h^{-1}$ der **Kommutator** von g und h.

(c) $G' := \langle [g, h] \mid g, h \in G \rangle$ heißt **Kommutatoruntergruppe** von G.

Beispiel 2

(a) $A_n \trianglelefteq S_n$, da

$$\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = 1 \quad \forall\, \sigma \in S_n, \forall\, \tau \in A_n\,.$$

(b) $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$, da

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B) = 1$$

$\forall\, A \in \mathrm{GL}_n(K)$, $\forall\, B \in \mathrm{SL}_n(K)$.

(c) G abelsche Gruppe $\Longrightarrow$ jede Untergruppe $U \leq G$ ist ein Normalteiler, da $gUg^{-1} = gg^{-1}U = 1U = U \; \forall\, g \in G$.
Ferner gelten dann auch $Z(G) = G$ und $G' = \{1_G\}$.

(d) $G = S_n$ $(n \geq 3) \Longrightarrow Z(G) = \{1\}$ und $G' = A_n$.

(e) $G = A_4 \Longrightarrow Z(G) = \{1\}$ und $G' = \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} =: V_4$.

1.2 Faktorgruppen (∗)

Erinnerung: Für eine Gruppe G, $H \leq G$ und $g \in G$ heißt $gH := \{gh \mid h \in H\}$ **Linksnebenklasse** (LNK) von H in G. Die Anzahl der LNK von H in G heißt **Index von H in G** (in Zeichen $|G : H|$).
Falls $N \trianglelefteq G$ ein Normalteiler ist, schreiben wir $G/N := \{gN \mid g \in G\}$ für die Menge der Linksnebenklassen.

Satz 1.7 (*Indexmultiplikationssatz*)

Sei $(G, \cdot)$ eine Gruppe und seien $V \leq U \leq G$ Untergruppen. Dann gilt:

$$|G : V| = |G : U| \cdot |U : V|$$

Beweis: Seien $\{g_i \mid i \in I\}$ ein Vertretersystem der LNK von U in G und $\{h_j \mid j \in J\}$ eines der LNK von V in U. Dann:

$$G = \bigsqcup_{i\in I} g_i U \qquad \text{und} \qquad U = \bigsqcup_{j\in J} h_j V, \qquad \text{also } G = \bigsqcup_{i\in I}\bigsqcup_{j\in J} g_i h_j V$$

Daraus folgt, dass $\{g_i h_j \mid i \in I, j \in J\}$ ein Vertretersystem der LNK von V in G ist. ■

Folgerung 1.8 (*Satz von Lagrange*)

Sei $(G, \cdot)$ eine endliche Gruppe und $U \leq G$ eine Untergruppe. Dann gilt $|G| = |G : U| \cdot |U|$, insbesondere teilt $|U|$ die Gruppenordnung $|G|$.

Beweis: Wähle $V = \{1\}$ im Indexmultiplikationssatz: dies liefert

$$|G : \{1\}| = |G : U| \cdot |U : \{1\}|\,.$$

Aber jede LNK von $\{1\}$ in G, bzw. in U, ist einelementig, so dass $|G : \{1\}| = |G|$ und $|U : \{1\}| = |U|$. Die Aussage folgt. ■

Beispiel 3

Sei G eine Gruppe mit $|G| = p$ eine Primzahl. Sei $U \leq G$ eine Untergruppe. Der Satz von Lagrange liefert $|U| = 1$ oder $|U| = p$, d.h. $U = \{1\}$ oder $U = G$, somit ist G einfach.

Folgerung 1.9 (*Kleiner Fermat der Gruppentheorie*)

Sei G eine endliche Gruppe. Dann gilt $g^{|G|} = 1$ für alle $g \in G$.

Beweis: Siehe AGS. ■

Bemerkung 1.10

Seien G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Dann ist G/N mit der Verknüpfung

$$\begin{array}{rccc} \cdot : & G/N \times G/N & \longrightarrow & G/N \\ & (gN, hN) & \mapsto & gN \cdot hN := ghN\,, \end{array}$$

eine Gruppe mit $|G/N| = |G : N|$. Wir nennen G/N die **Faktorgruppe** von G nach N.

Beweis: Siehe AGS. ■

Beispiel 4

(a) Für $G = S_n$, $N = A_n$ ist $S_n/A_n \cong Z_2 = \mathbb{Z}/2\mathbb{Z}$.

(b) Für $G = \mathrm{GL}_n(K)$ ist $Z(G) = \{a \cdot I_n \mid a \in K^\times\} \trianglelefteq G$ und $G/Z(G) =: \mathrm{PGL}_n(K)$ heißt die **projektive lineare Gruppe**.

Definition 1.11 (*Gruppenhomomorphismus, Kern, Bild*)

Seien $(G, \cdot)$ und $(H, \star)$ Gruppen. Eine Abbildung $\varphi : G \longrightarrow H$ heißt **(Gruppen)-Homomorphismus**, wenn $\varphi(g_1 \cdot g_2) = \varphi(g_1) \star \varphi(g_2)$ für alle $g_1, g_2 \in G$.

· Ein Homomorphismus $\varphi : G \longrightarrow G$ heißt **Endomorphismus**, ein bijektiver Homomorphismus

heißt **Isomorphismus**, ein bijektiver Endomorphismus heißt **Automorphismus**. Die Menge $\mathrm{Aut}(G) := \{\varphi : G \longrightarrow G \mid \varphi \text{ Automorphismus}\}$ heißt **Automorphismengruppe** von G.

- Der **Kern** von φ ist die Untergruppe $\ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\} \leq G$. Das **Bild** von φ ist die Untergruppe $\varphi(G) := \{\varphi(g) \mid g \in G\} \leq H$.

Beispiel 5

(a) $\det : \mathrm{GL}_n(K) \longrightarrow K^\times, A \mapsto \det(A)$ ist ein Homomorphismus mit $\ker(\det) = \mathrm{SL}_n(K)$.

(b) $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}, \sigma \mapsto \mathrm{sgn}(\sigma)$ ist ein Homomorphismus mit $\ker(\mathrm{sgn}) = A_n$. (Der Signum-Homomorphismus)

(c) Sei G eine Gruppe. Für $g \in G$ definiert

$$\begin{array}{rccc} c_g : & G & \longrightarrow & G \\ & x & \mapsto & gxg^{-1} \end{array}$$

einen Automorphismus von G (siehe Blatt 1). Wir nennen $\mathrm{Inn}(G) := \{c_g \mid g \in G\} \subseteq \mathrm{Aut}(G)$ die **Gruppe der inneren Automorphismen** von G.

Bemerkung 1.12

Sei G eine Gruppe. Dann ist $\mathrm{Aut}(G)$ eine Gruppe und $\mathrm{Inn}(G)$ ein Normalteiler von $\mathrm{Aut}(G)$.

Beweis: Übung 4, Blatt 1. ∎

Satz 1.13 (*Homomorphiesatz*)

Sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gibt es einen eindeutigen Homomorphismus $\overline{\varphi} : G/\ker(\varphi) \longrightarrow H$ mit $\varphi = \overline{\varphi} \circ \pi$, wobei $\pi : G \longrightarrow G/\ker(\varphi), g \mapsto g\ker(\varphi)$ der kanonische Homomorphismus ist. Es gelten $\overline{\varphi}(G/\ker(\varphi)) = \varphi(G)$ und $\overline{\varphi}$ is injektiv. Insbesondere

$$G/\ker(\varphi) \cong \varphi(G)\,.$$

Beweis: Siehe AGS. ∎

Satz 1.14 (*2. Isomorphiesatz*)

Sei G eine Gruppe, $N \trianglelefteq G$, $H \leq G$. Dann ist HN eine Untergruppe von G, $H \cap N$ ein Normalteiler von H, und es gilt

$$HN/N \cong H/(H \cap N)\,.$$

Beweis: Siehe AGS. (2016: Übungsblatt 9, SS 2016) ∎

2 Operationen von Gruppen auf Mengen

Ziel: Die Struktur der Gruppen und Mengen, wie z. B. geometrische Objekte, besser verstehen!

Sei stets G eine Gruppe. Wir schreiben von nun an die Multiplikation in G als ab für $a, b \in G$, anstelle von $a \star b$ oder $a \cdot b$.

2.1 Definitionen und Beispiele

Definition 1.15 (*Gruppenoperation*)

Sei X eine nicht-leere Menge. Eine **Gruppenoperation** (oder **Operation**) von G auf X ist eine Abbildung

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & g.x\,, \end{array}$$

mit folgenden Eigenschaften:

(GM1) $1_G.x = x \quad \forall\, x \in X$;

(GM2) $(gh).x = g.(h.x) \quad \forall\, g, h \in G$ und $\forall\, x \in X$.

Wir sagen auch, dass G **auf** X **operiert**, oder dass X eine G**-Menge** ist.

Bemerkung 1.16

Die Gruppenoperationen von G auf X (d.h. die G-Mengen X) entsprechen genau den Gruppen-Homomorphismen $\Sigma : G \longrightarrow S_X$.

Beweis:

'$\Rightarrow$' Sei X eine G-Menge. Definiere dann $\Sigma : G \longrightarrow S_X$, $g \mapsto \Sigma(g) =: \sigma_g$, wobei $\sigma_g : X \longrightarrow X$, $x \mapsto \sigma_g(x) := g.x$. ($\Sigma$ wohldefiniert: Übung.)
Die Abbildung Σ ist ein Homomorphismus, da $\forall\ g, h \in G$ und $\forall\ x \in X$,

$$\Sigma(gh)(x) = \sigma_{gh}(x) = (gh).x \overset{(GM2)}{=} g.(h.x) = \sigma_g(h.x) = \sigma_g(\sigma_h(x)) = \sigma_g \circ \sigma_h(x) = (\Sigma(g) \circ \Sigma(h))(x)$$

so dass $\Sigma(gh) = \Sigma(g) \circ \Sigma(h)$.

'$\Leftarrow$' Ist umgekehrt $\Sigma : G \longrightarrow S_X$ ein Gruppenhomomorphismus, dann ist die Abbildung

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & g.x := \Sigma(g)(x)\,, \end{array}$$

eine Gruppenoperation, denn $\forall\ x \in X$, $\forall\ g, h \in G$,

$$1_G.x = \Sigma(1_G)(x) = \mathrm{Id}_X(x) = x \quad \text{und}$$

$$(gh).x = \Sigma(gh)(x) = \Sigma(g) \circ \Sigma(h)(x) = \Sigma(g)(\Sigma(h)(x)) = g.(h.x)\,,$$

so dass $(GM1)$ und $(GM2)$ gelten. ■

Definition 1.17 (*Bahn, Stabilisator, treue/transitive Operation*)

Sei X eine G-Menge und $x \in X$ fest. Dann ist

(i) $\mathcal{O}_x := \{g.x \mid g \in G\} \subseteq X$ die **Bahn** von x, und

(ii) $G_x := \mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\}$ der **Stabilisator** von x in G.

Die Operation von G auf X ist **transitiv**, falls $X = \mathcal{O}_x$ für ein (also alle) $x \in X$ (d.h. es gibt nur eine Bahn); und die Operation von G auf X ist **treu**, falls $\bigcap_{x \in X} G_x = \{1\}$.

Anmerkung 1.18

Eine G-Menge X ist treu genau dann, wenn die zugehörige Permutationsdarstellung $\Sigma : G \longrightarrow S_X$ injektiv ist.

Bemerkung 1.19

Sei X eine G-Menge und $x \in X$. Dann ist G_x eine Untergruppe von G.

Beweis: (i) $1_G.x \overset{(GM1)}{=} x \Rightarrow 1_G \in G_x$.

(ii) $g, h \in G_x \Rightarrow (gh).x \overset{(GM2)}{=} g.(h.x) = g.x = x$, also $gh \in G_x$.

(iii) $g \in G_x \Rightarrow x \overset{(GM1)}{=} 1_G.x = (g^{-1}g).x \overset{(GM2)}{=} g^{-1}.(g.x) = g^{-1}.x$, also $g^{-1} \in G_x$. ■

Hier ist das erste Beispiel von Informationen über Gruppen, die man durch eine Gruppenoperation bekommt:

Satz 1.20 (*Satz von Cayley*)

Jede Gruppe G besitzt eine injektive Permutationsdarstellung. Insbesondere ist G eine endliche Gruppe, dann existiert ein $n \in \mathbb{N}$ mit $G \leq S_n$.

Beweis: Die Verknüpfung $\cdot : G \times G \longrightarrow G, (g, h) \mapsto g \cdot h$ definiert eine Operation von G auf $X = G$ selbst.
Es gilt $G_1 = \{g \in G \mid g \cdot 1 = 1\} = \{1\}$, so dass

$$\bigcap_{x \in X} G_x = G_1 \cap \bigcap_{1 \neq x \in X} G_x = \{1\} \cap \bigcap_{1 \neq x \in X} G_x = \{1\},$$

also ist die Operation treu. Nach Anmerkung 1.18 ist dann die zugehörige Permutationsdarstellung $\Sigma : G \longrightarrow S_G$ injektiv.
Ist nun G eine endliche Gruppe, so ist G isomorph zu $\Sigma(G)$ nach dem Homomorphiesatz. Auf diese Weise sehen wir $G \cong \Sigma(G)$ als eine Untergruppe von S_G. Setze $n := |G|$. ■

Wir wollen nun einige wichtige Beispiele für Operationen kennen lernen.

Beispiel 6

Siehe `Beamer_Woche_2.pdf`.

(a) Operation von G auf $X = G$ selbst durch Linksmultiplikation.

(b) Operation von G auf $X = G$ selbst durch Konjugation.
Für $x \in X = G$:

- heißt der Stabilisator $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} =: C_G(x)$ **Zentralisator** von x in G.
- heißt die Bahn $\mathcal{O}_x = \{gxg^{-1} \mid g \in G\} =: [x]$ **Konjugiertenklasse** von x in G.

(c) Operation von G auf $X = \{LNK \text{ von } U \text{ in } G\}$, wobei $U \leq G$.

(d) Operation von G auf $X = \{U \leq G\}$ durch Konjugation.
Für $U \in X$

- heißt der Stabilisator $G_U = \{g \in G \mid gUg^{-1} = U\} =: N_G(U)$ **Normalisator** von U in G.
(Anmerkung: $U \trianglelefteq G \Leftrightarrow N_G(U) = G$)
- heißt die Bahn $\mathcal{O}_U = \{gUg^{-1} \mid g \in G\} =: [U]$ **Konjugiertenklasse** von U in G.

(e) Operation von $G = \mathbb{Z}/4\mathbb{Z}$ auf dem regulären Oktaeder.

2.2 Die Bahnbilanzgleichung

Satz 1.21 (*Bahnbilanzgleichung*)

Sei X eine G-Menge und $x \in X$ fest. Dann gelten:

(a) Die Abbildung

$$\begin{array}{rccc} \mu_x: & \mathcal{O}_x & \longrightarrow & \{LNK \text{ von } G_x \text{ in } G\} \\ & g.x & \mapsto & gG_x \end{array}$$

ist wohl-definiert und bijektiv.

(b) $|\mathcal{O}_x| = |G : G_x|$.

(c) Je zwei Bahnen sind entweder gleich oder disjunkt. Ist $X/\sim$ ein Vertretersystem der Bahnen von G auf X, so gilt

$$X = \bigsqcup_{x \in X/\sim} \mathcal{O}_x \,.$$

Insbesondere ist

$$|X| = \sum_{x \in X/\sim} |\mathcal{O}_x| = \sum_{x \in X/\sim} |G : G_x| \,.$$

Beweis:

(a) Ist $g.x = h.x$ für $g, h \in G$, so gilt $(g^{-1}h).x = g^{-1}.(h.x) = g^{-1}.(g.x) = 1.x = x$ also $g^{-1}h \in G_x$ und damit $hG_x = gG_x$. Dies zeigt, dass μ_x wohl-definiert ist.
Die Surjektivität von μ_x ist klar nach Definition. Schließlich ist $gG_x = hG_x$, so gilt $g^{-1}h \in G_x$ also $g.x = g.((g^{-1}h).x) = (gg^{-1}h.x) = h.x$; damit ist μ_x auch injektiv.

(b) folgt direkt aus (a), da $|\{LNK \text{ von } G_x \text{ in } G\}| = |G : G_x|$.

(c) Für $x, y \in X$, schreiben wir $x \sim y$, falls es ein $g \in G$ mit $y = g.x$ existiert. Dies definiert eine Relation auf X. Wir zeigen erst, dass $\sim$ eine Äquivalenzrelation ist:

Wegen $1.x = x$, ist $\sim$ reflexiv.
Ist $x \sim y$, also $\exists\ g \in G$ mit $y = g.x$, so gilt $g^{-1}.y = g^{-1}.(g.x) = (g^{-1} \cdot g).x = 1.x = x$, also $y \sim x$; damit ist $\sim$ symmetrisch.
Seien nun $x \sim y$ und $y \sim z$, also $\exists\ g, h \in G$ mit $y = g.x$ und $z = h.y$. Dann ist $z = h.y = h.(g.x) = (hg).x$, also $x \sim z$ und damit ist $\sim$ transitiv.
Es folgt, dass die Bahnen mit den Äquivalenzklassen von $\sim$ übereinstimmen, also je zwei Bahnen entweder gleich oder disjunkt sind. Insbesondere ist

$$X = \bigsqcup_{x \in X/\sim} \mathcal{O}_x$$

und die Gleichung $|X| = \sum_{x \in X/\sim} |\mathcal{O}_x| = \sum_{x \in X/\sim} |G : G_x|$ folgt aus (b). ■

Wir betrachten jetzt wichtige Folgerungen der Bahnbilanzgleichung für das Studium von Gruppen.

Folgerung 1.22

Sei G eine Gruppe. Dann gelten:

(a) $|[g]| = |G : C_G(g)|$ für alle $g \in G$.

(b) $|G| = \sum_{g \in G/\sim} |[g]| = \sum_{g \in G/\sim} |G : C_G(g)|$, wobei g über ein Vertretersystem $G/\sim$ der Bahnen von G unter der Konjugationsoperation läuft.

Beweis: Dies ist Satz 1.21 für die Konjugationsoperation von G auf G. (Siehe Beispiel 6(b).) ■

Definition 1.23 (*p-Gruppe*)

Eine endliche Gruppe G mit $|G| = p^n$ für eine Primzahl p und eine natürliche Zahl $n \in \mathbb{N}_0$ heißt p-**Gruppe**.

Satz 1.24

Seien p eine Primzahl und G eine nicht-triviale p-Gruppe. Dann ist $Z(G) \gneq \{1\}$.

Beweis: Nach Definitionen

$$x \in Z(G) \Leftrightarrow gx = xg\ \forall\ g \in G \Leftrightarrow [x] = \{gxg^{-1} \mid g \in G\} = \{x\} \Leftrightarrow |[x]| = 1\,.$$

Nach Folgerung 1.22(a) ist dann in diesem Fall $|G : C_G(x)| = 1$, also $G = C_G(x)$.
Nach Folgerung 1.22(b) ist

$$|G| = \sum_{x \in G/\sim} |G : C_G(x)| = |Z(G)| + \sum_{\substack{x \in G/\sim \\ x \notin Z(G)}} |G : C_G(x)|\,.$$

Der zweite Summand ist nach dem Satz von Lagrange durch p teilbar, also

$$p \mid |Z(G)| = |G| - \sum_{\substack{x \in G/\sim \\ x \notin Z(G)}} |G : C_G(x)|$$

und damit ist $|Z(G)| \geq p > 1$. Insbesondere ist $Z(G) \gneq \{1\}$. ■

Folgerung 1.25

Seien p eine Primzahl und G eine endliche Gruppe mit $|G| = p^2$. Dann ist G eine abelsche Gruppe.

Beweis: [Aufgabe 5, Blatt 2]. ■

2.3 Die Sylowsätze

In diesem Abschnitt ist G stets eine endliche Gruppe und p eine Primzahl.

Definition 1.26 (*p-Untergruppe, p-Sylow-Untergruppe*)

Sei $|G| = p^a m$ mit $a \geq 0$ und $p \nmid m$.

(i) Eine Untergruppe $U \leq G$ heißt **p-Untergruppe**, wenn $|U| = p^k$ für ein $k \in \mathbb{N}_0$ (also $k \leq a$).

(ii) Eine Untergruppe $P \leq G$ heißt **p-Sylow-Untergruppe**, wenn $|P| = p^a$ gilt. Es sei $\mathrm{Syl}_p(G)$ die Menge aller p-Sylow-Untergruppen von G und $n_p := |\mathrm{Syl}_p(G)|$.

Beispiel 7

Sei $G = A_4$ die alternierende Gruppe vom Grad 4. Dann ist $|G| = 2^2 \cdot 3$. Es gilt

$$P := \{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} = V_4 \in \mathrm{Syl}_2(A_4) \quad \textit{und} \quad Q := \langle (1\,2\,3) \rangle \in \mathrm{Syl}_3(A_4)\,.$$

Denn: P hat Ordnung 4 und Q hat Ordnung 3, also ist Q eine zyklische Gruppe der Ordnung 3.

Anmerkung 1.27

Beachte, dass es **nicht** zu jedem Teiler d von G eine Untergruppe $U \leq G$ mit $|U| = d$ gibt.
Zum Beispiel hat A_4 keine Untergruppe der Ordnung 6. (Wurde in der AGS-Vorlesung gesehen.)

Lemma 1.28

Sei $H \leq G$ eine Untergruppe. Ist $P \in \mathrm{Syl}_p(G)$, so existiert es ein $g \in G$ mit $gPg^{-1} \cap H \in \mathrm{Syl}_p(H)$.
Insbesondere gilt: $\mathrm{Syl}_p(G) \neq \emptyset \Rightarrow \mathrm{Syl}_p(H) \neq \emptyset$.

Beweis: Die Gruppe H operiert auf $X = \{LNK \text{ von } P \text{ in } G\}$ durch Linksmultiplikation wie im Beispiel 6(c):

$$\begin{array}{ccc} H \times X & \longrightarrow & X \\ (h, gP) & \mapsto & h.gP = hgP \end{array}$$

Sei

$$X = \mathcal{O}_1 \sqcup \ldots \sqcup \mathcal{O}_r \qquad (r \in \mathbb{N})$$

die Zerlegung in H-Bahnen gegeben durch Satz 1.21(c) (Bahnbilanzgleichung). Dies ist eine endliche disjunkte Vereinigung, da G und somit auch X endlich ist.

Weil P eine p-Sylow-Untergruppe ist, nach Definition $p \nmid |X| = |G : P|$, also muss es ein $1 \leq i \leq r$ mit $p \nmid |\mathcal{O}_i|$ geben. Sei $g_i \in G$ ein Vertreter der Bahn $\mathcal{O}_i$, d.h. $x_i := g_i P \in \mathcal{O}_i = \mathcal{O}_{x_i}$. Dann ist

$$\begin{aligned} H_{x_i} = \mathrm{Stab}_H(g_i P) &= \{h \in H \mid hg_iP = g_iP\} \\ &= \{h \in H \mid g_i^{-1} h g_i \in P\} \\ &= \{h \in H \mid h \in g_i P g_i^{-1}\} \\ &= g_i P g_i^{-1} \cap H\,. \end{aligned}$$

Nun ist nach der Bahnbilanzgleichung (Satz 1.21(b)) $|H : H_{x_i}| = |O_i|$ und dies ist nicht durch p teilbar, also ist die Untergruppe H_{x_i} eine p-Sylow-Untergruppe von H (da $|g_i P g_i^{-1}| = |P|$). ■

Lemma 1.29 (*Satz von Cauchy*)

Sei p ein Teiler von $|G|$. Dann enthält G ein Element der Ordnung p.

Beweis: Sei $X := \{(g_1, \ldots, g_p) \in G \times \cdots \times G \mid g_1 \cdots g_p = 1_G\}$. Es gilt $|X| = |G|^{p-1}$, da zu vorgegebenen $g_1, \ldots, g_{p-1}$ das letzte Element g_p eindeutig festgelegt ist. Sei $\sigma := (1\ 2\ \ldots\ p) \in S_p$ und setze $S := \langle\sigma\rangle$ die von σ erzeugte zyklische Gruppe. Dann operiert S auf X durch

$$\sigma.(g_1, \ldots, g_p) := (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) = (g_2, \ldots, g_p, g_1)$$

denn

$$g_1 \cdots g_p = 1_G \Rightarrow g_2 \cdots g_p g_1 = g_1^{-1}(g_1 g_2 \cdots g_p) g_1 = g_1^{-1} \cdot 1_G \cdot g_1 = 1_G\,.$$

Betrachte dann die Bahnen von dieser Operation: offensichtlich liegt $(g_1, \ldots, g_p) \in X$ in einer Bahn der Länge 1 genau dann, wenn $g_1 = \ldots = g_p$. Alle anderen Bahnen haben Länge p. Nach Satz 1.21(c), ist $X = X_0 \sqcup X_1$, wobei $X_0 = \{(g_1, \ldots, g_p) \mid g_1 = \ldots = g_p\}$ und X_1 die Vereinigung der Bahnen der Länge p ist. Aber dann $|X_0| = |X| - |X_1| = |G|^{p-1} - |X_1|$, so dass $p \mid |X_0|$, da $p \mid |X_1|$ und $p \mid |G|$. Aber $|X_0| \geq 1$ da $(1_G, \ldots, 1_G) \in X_0 \Rightarrow |X_0| \geq p$, und damit gibt es ein $g \in G \setminus \{1_G\}$ mit $g^p = 1$. ■

Satz 1.30 (*Sylowsätze*)

Sei G eine endliche Gruppe mit $|G| = p^a m$, wobei $a \geq 0$ und $p \nmid m$.

(a) [**1. Sylowsatz**] Es existiert eine Untergruppe $P \leq G$ mit $|P| = p^a$.

(b) [**2. Sylowsatz**] Sind $P, Q \in \mathrm{Syl}_p(G)$, so gibt es ein $g \in G$ mit $Q = gPg^{-1}$.
[In Worten: je zwei p-Sylow-Untergruppen sind in G zueinander konjugiert.]

(c) [**3. Sylowsatz**] Es gelten $n_p(G) \equiv 1 \pmod p$ und $n_p(G) \mid m$.

Beweis:

(a) Induktion nach $|G|$. Klar für $|G| = 1$ und auch für $|G| = p^a \cdot m > 1$ mit $a = 0$: wähle $P = \{1_G\}$. Sei nun $|G| > 1$ und $a \geq 1$. Nach Folgerung 1.22 ist

$$|G| = \sum_{g \in G/\sim} |[g]| = \sum_{g \in G/\sim} |G : C_G(g)|\,,$$

wobei g über ein Vertretersystem $G/\sim$ der Bahnen von G unter der Konjugationsoperation läuft.

1. Fall: $p \nmid |Z(G)| \Rightarrow \exists\, g \in G \setminus Z(G)$ mit $p \nmid |G : C_G(g)|$, also $p^a \,||C_G(g)|$ und $|C_G(g)| < |G|$. Per Induktion existiert eine Untergruppe $P \leq C_G(g)$ mit $|P| = p^a$. Offensichtlich ist $P \leq G$, da $P \leq C_G(g) < G$.

2. Fall: $p \mid |Z(G)| \Rightarrow$ nach dem Satz von Cauchy gibt es ein $g \in Z(G)$ mit $o(g) = p$. Setze $N := \langle g\rangle \cong Z_p$. Wegen $g \in Z(G)$, ist $N \trianglelefteq G$.
(Da $hNh^{-1} = \langle hgh^{-1}\rangle = \langle ghh^{-1}\rangle = \langle g\rangle = N$ für alle $h \in G$.)
Nun ist $|G/N| = |G|/|N| = \frac{1}{p}|G| = p^{a-1} \cdot m < |G| \Rightarrow$ Per Induktion gibt es eine Untergruppe $U \leq G/N$ mit $|U| = p^{a-1}$. Sei $P := \pi^{-1}(U)$ das volle Urbild von P unter dem Restklassenhomomorphismus $\pi : G \longrightarrow G/N$. Dann ist $U \cong P/N$, also

$$|P| = |U| \cdot |N| = p^{a-1} \cdot p = p^a\,.$$

(b) Wähle $H = Q$ in Lemma 1.28. Dies zeigt, dass es ein $g \in G$ mit $gPg^{-1} \cap Q \in \mathrm{Syl}_p(Q)$ gibt. Wegen $Q \in \mathrm{Syl}_p(G)$, ist aber $\mathrm{Syl}_p(Q) = \{Q\}$, also gilt

$$gPg^{-1} \cap Q = Q$$

und damit $Q \subseteq gPg^{-1}$. Wegen $p^a = |Q| = |P| = |gPg^{-1}|$ folgt $Q = gPg^{-1}$.

(c) Für $P \in \mathrm{Syl}_p(G)$ und $g \in G$ ist auch $gPg^{-1} \in \mathrm{Syl}_p(G)$, da $|gPg^{-1}| = |P| = p^a$. Daraus folgt, dass die Gruppe G auf der Menge $X := \mathrm{Syl}_p(G)$ durch Konjugation operiert:

$$\begin{array}{ccc} G \times \mathrm{Syl}_p(G) & \longrightarrow & \mathrm{Syl}_p(G) \\ (g, P) & \mapsto & g.P := gPg^{-1} \end{array}$$

(GM1) und (GM2) gelten offensichtlich, da $1_G.P = 1_G P (1_G)^{-1} = P$ und $\forall\, P \in \mathrm{Syl}_p(G), \forall g, h \in G$:

$$g.(h.P) = g.(hPh^{-1}) = ghPh^{-1}g^{-1} = (gh)P(gh)^{-1} = (gh).P$$

Nach (b) ist diese Operation transitiv, d.h. es gibt genau eine Bahn. Sei $P \in \mathrm{Syl}_p(G)$ fest. Der Stabilisator von P unter dieser Operation ist

$$G_P = \{g \in G \,|\, gPg^{-1} = P\} = N_G(P)\,,$$

also der Normalisator von P in G. Es folgt dann aus der Bahnbilanzgleichung (Satz 1.21(b)), dass

$$n_p = |\mathrm{Syl}_p(G)| = |G : N_G(P)|\,.$$

Wegen $P \leq N_G(P) \leq G$ gilt nach dem Indexmultiplikationssatz, dass

$$|G : N_G(P)| \cdot |N_G(P) : P| = |G : P| = m\,,$$

also $n_p(G) \,|\, m$.
Um $n_p(G) \equiv 1 \pmod p$ zu zeigen, schränken wir die obige Operation auf P ein:

$$\begin{array}{ccc} P \times \mathrm{Syl}_p(G) & \longrightarrow & \mathrm{Syl}_p(G) \\ (g, Q) & \mapsto & g.Q := gQg^{-1} \end{array}$$

Diese Operation wird im Allgemeinen nicht mehr transitiv sein, also betrachten wir die Zerlegung in P-Bahnen:

$$X = \mathrm{Syl}_p(G) = \mathcal{O}_1 \sqcup \ldots \sqcup \mathcal{O}_r \qquad (r \in \mathbb{N})\,,$$

und wir wählen ein Vertretersystem $P_1, \ldots, P_r$ der P-Bahnen mit $P_i \in \mathcal{O}_i \;\forall\; 1 \leq i \leq r$. O.B.d.A. wählen wir $P_1 = P$. Nach der Bahnbilanzgleichung (Satz 1.21(b)) ist $\forall\; 1 \leq i \leq r$

$$|\mathcal{O}_i| = |P : N_P(P_i)| = p^{k_i} \quad \text{für ein } k_i \geq 0\,.$$

Für $i = 1$ ist $gP_1g^{-1} = gPg^{-1} = P$ für alle $g \in P$, also $\mathcal{O}_1 = \{P\}$ und $k_1 = 0$. Sei nun $i \geq 2$. Wir zeigen, dass in diesem Fall $k_i \geq 1$ gilt. Wäre auch $k_i = 0$, d.h. $\mathcal{O}_i = \{P_i\}$, so folgte $gP_ig^{-1} = P_i$ für alle $g \in P$, also nach Definition $P \subseteq N_P(P_i) \subseteq N_G(P_i)$. Damit wären P, P_i in $\mathrm{Syl}_p(N_G(P_i))$ enthalten. Nach (b) gäbe es ein Element $h \in N_G(P_i)$ mit $P = hP_ih^{-1} = P_i$. Widerspruch zu $i \geq 2$. Also ist $k_i \geq 1$ und damit $p \,|\, |\mathcal{O}_i|$ für alle $i \geq 2$. Es folgt dann aus der Bahnbilanzgleichung, dass

$$n_p = |\mathrm{Syl}_p(G)| = |\mathcal{O}_1| + \sum_{i=2}^{r} |\mathcal{O}_i| \equiv 1 + \sum_{i=2}^{r} 0 \pmod p \equiv 1 \pmod p\,.$$

■

Folgerung 1.31

Sei $P \in \mathrm{Syl}_p(G)$. Dann gilt: $P \trianglelefteq G \Leftrightarrow \mathrm{Syl}_p(G) = \{P\}$.

Beweis: Nach Satz 1.30(b) (2. Sylowsatz) sind alle Gruppen in $\mathrm{Syl}_p(G)$ konjugiert zu P. Daraus folgt, dass

$$P \trianglelefteq G \overset{Def.}{\iff} gPg^{-1} = P \;\forall\, g \in G \overset{1.30(b)}{\iff} \mathrm{Syl}_p(G) = \{P\}\,.$$

■

2.4 Einfache und Auflösbare Gruppen

Erinnerung: Die **Kommutatoruntergruppe** einer Gruppe G ist die Untergruppe $G' := \langle [g,h] \,|\, g,h \in G \rangle$. Es gilt: G abelsch $\iff G' = \{1_G\}$.

Bemerkung 1.32

Sei G eine Gruppe.

(a) Ist $\varphi : G \longrightarrow H$ surjektiver Gruppen-Homomorphismus, so gilt $\varphi(G') = H'$.

(b) Es gilt $G' \trianglelefteq G$ und G/G' ist abelsch.

(c) Ist $H \trianglelefteq G$ beliebig mit G/H abelsch, so ist $G' \subseteq H$.

Beweis: (a) Es gilt $\varphi(G') \subseteq H'$, denn für alle $g_1, g_2 \in G$ ist

$$\varphi([g_1,g_2]) = \varphi(g_1 g_2 g_1^{-1} g_2^{-1}) = \varphi(g_1)\varphi(g_2)\varphi(g_1)^{-1}\varphi(g_2)^{-1} = [\varphi(g_1),\varphi(g_2)] \in H' .$$

Es gilt auch $H' \subseteq \varphi(G')$: Sind $h_1, h_2 \in H$, so gibt es $g_1, g_2 \in G$ mit $\varphi(g_i) = h_i$ für $i = 1,2$, da φ surjektiv ist. Dann zeigt die obige Rechnung, dass $[h_1,h_2] = \varphi([g_1,g_2]) \in \varphi(G')$ gilt.

(b) Sei $g \in G$ und $c_g : G \longrightarrow G, x \longrightarrow gxg^{-1}$ der zugehörende innere Automorphismus (siehe 5(c)). Nach (a) ist $gG'g^{-1} = c_g(G') \overset{(a)}{=} G'$ für alle $g \in G$, also ist $G' \trianglelefteq G$.
Betrachte nun den Restklassenhomomorphismus $\pi : G \longrightarrow G/G', g \longrightarrow gG'$ (surjektiv). Nach (a) gilt $(G/G')' = \pi(G') = \{1_{G/G'}\}$, also ist G/G' abelsch.

(c) Sei $\pi_H : G \longrightarrow G/H, g \longrightarrow gH$ der Restklassenhomomorphismus bezüglich H. Mit (a) folgt $\pi_H(G') = (G/H)'$. Aber $(G/H)' = \{1_{G/H}\}$, weil G/H abelsch ist. Also ist $G' \subseteq \ker(\pi_H) = H$. ■

Definition 1.33 (*Auflösbare Gruppe*)

Sei G eine Gruppe.

- Wir setzen $G^{(0)} := G$, $G^{(1)} := G'$, und induktiv $G^{(i)} := (G^{(i-1)})'$ für $i \geq 2$.
- Die Gruppe G heißt **auflösbar**, falls es ein $r \in \mathbb{N}$ mit $G^{(r)} = \{1_G\}$ gibt.
  [Auf Englisch sagt man **soluble** (BE) oder **solvable** (AE).]

Aufgabe 9 (*Aufgabe 9, Blatt 3*)

Sei G eine Gruppe. Dann gelten:

(a) Ist G auflösbar, dann ist jede Untergruppe $H \leq G$ auflösbar.

(b) Ist G auflösbar, dann ist jede Faktorgruppe G/N auflösbar, wobei $N \trianglelefteq G$ ein beliebiger Normalteiler ist.

(c) Sei $N \trianglelefteq G$. Genau dann ist G auflösbar, wenn N und G/N auflösbar sind.
['Sandwich-Prinzip']

Beispiel 8

(a) G abelsch $\Longrightarrow G' = \{1_G\}$, also ist G auflösbar. ($r = 1$ reicht in diesem Fall.)

(b) $|G| = p^n$, d.h. G ist eine endliche p-Gruppe $\Longrightarrow G$ auflösbar.

Beweis: Induktion nach $|G|$.
Ist G abelsch, dann ist G auflösbar nach (a).
Ist G nicht abelsch, dann ist $G \neq Z(G)$. Außerdem ist $Z(G) \neq \{1_G\}$ nach Satz 1.24, da G und somit $Z(G)$ eine p-Gruppe ist. Insgesamt:

$$\{1_G\} \lneq Z(G) \lneq G$$

Wegen $|G/Z(G)| = |G|/|Z(G)| < |G|$ ist $G/Z(G)$ auflösbar nach Induktion. Außerdem ist $Z(G)$ eine abelsche Gruppe, also auflösbar nach (a). Daher ist G auflösbar nach Aufgabe 9(c). ■

Wir untersuchen jetzt hauptsächlich endliche Gruppen und insbesondere den Zusammenhang zwischen einfachen und auflösbaren Gruppen.

Lemma 1.34

Sei G eine endliche Gruppe. Genau dann ist G einfach und auflösbar, wenn $|G| = p$ eine Primzahl ist, d.h. wenn G eine zyklische Gruppe der Ordnung p ist.

Beweis: Zunächst ist für eine Primzahl p die Gruppe Z_p abelsch und damit auflösbar nach Beispiel 8(a).
Sei nun G (beliebig) endlich, einfach und auflösbar. Es gelten:

- $G \neq \{1_G\}$, da G einfach ist;
- $G' \neq G$, da G auflösbar ist.

Weil G einfach ist, folgt jetzt, dass $G' = \{1_G\}$ ist, und damit ist G abelsch. Sei $g \in G \setminus \{1_G\}$ und $o(g) =: m > 1$. Sei p eine Primzahl mit $p \mid m$, also $m = p \cdot b$ mit $b \in \mathbb{N}$. Dann ist $o(g^b) = p$, da $g^m = 1_G$ und $g^b \neq 1_G$. (Siehe Aufgabe 2(b).) Also ist $U := \langle g^b \rangle$ eine Untergruppe mit $|U| = p$. Weil G abelsch ist, ist $\{1_G\} \lneq U \trianglelefteq G$. Also folgt $U = G$, da G einfach ist. ■

Satz 1.35 (*Charakterisierung der endlichen auflösbaren Gruppen*)

Sei G eine endliche Gruppe. Dann gilt:

G ist auflösbar $\Longleftrightarrow$ es gibt eine Kette von Untergruppen $\{1_G\} = G_1 \leq G_2 \leq \ldots \leq G_n = G$ mit:
(i) $G_i \trianglelefteq G_{i+1}$ und
(ii) $G_{i+1}/G_i \cong Z_{p_i}$ (zyklisch von Primzahlordnung p_i), für alle $1 \leq i \leq n-1$.

Beweis:

'$\Rightarrow$' Induktion nach $|G|$. Der Fall $|G| = 1$ ist klar und der Fall $|G| = p$ eine Primzahl ist auch klar nach Lemma 1.34. Ist G auflösbar mit $|G| > 1$, so existiert ein $r \in \mathbb{N}$ mit $\{1_G\} = G^{(r)} = (G^{(r-1)})'$ und $G^{(r-1)} \neq \{1_G\}$, und daher ist $G^{(r-1)}$ abelsch. Nun ist $G/G^{(r-1)}$ auflösbar nach Aufgabe 9(b) und

$$|G/G^{(r-1)}| < |G|\,.$$

Es folgt per Induktion, dass $G/G^{(r-1)}$ eine Kette von Untergruppen

$$\{1\} = \overline{G_1} \leq \overline{G_2} \leq \ldots \leq \overline{G_n} = G/G^{(r-1)}$$

besitzt, wobei (i) und (ii) gelten. Aber für alle $1 \leq i \leq n$ ist $\overline{G_i} = G_i/G^{(r-1)}$, wobei $G_i := \pi^{-1}(\overline{G_i})$ das Urbild von $\overline{G_i}$ unter dem Restklassenhomomorphismus ist. Es gilt

$$G^{(r-1)} = G_1 \leq G_2 \leq \ldots \leq G_n = G\,,$$

wobei für alle $1 \leq i \leq n-1$ $G_i \trianglelefteq G_{i+1}$ (da $\overline{G_i} \trianglelefteq \overline{G_{i+1}}$) und

$$G_{i+1}/G_i \cong (G_{i+1}/G^{(r-1)})/(G_i/G^{(r-1)}) = \overline{G_{i+1}}/\overline{G_i} \cong Z_{p_i}\,.$$

Wir konstruieren jetzt eine Kette von Untergruppen mit Bedingungen (i) und (ii) zwischen $\{1_G\}$ und $G^{(r-1)}$. Sei p eine Primzahl mit $p \mid |G^{(r-1)}|$. Nach dem Satz von Cauchy besitzt $G^{(r-1)}$ ein Element g der Ordnung p, also ist $G^{(r-1)} \geq \langle g \rangle =: G_0$ zyklisch der Ordnung p. Aber $G_0 \trianglelefteq G^{(r-1)}$, da $G^{(r-1)}$ abelsch ist, und $|G^{(r-1)}/G_0| = \frac{1}{p}|G^{(r-1)}| < |G|$. Also per Induktion hat $G^{(r-1)}/G_0$ eine Kette von Untergruppen

$$\{1\} = \overline{H_1} \leq \overline{H_2} \leq \ldots \leq \overline{H_m} = G^{(r-1)}/G_0$$

wobei (i) und (ii) gelten für alle $1 \leq i \leq m-1$. Ein ähnliches Argument wie oben liefert eine Kette von Untergruppen

$$G_0 = H_1 \leq H_2 \leq \ldots \leq H_m = G^{(r-1)}\,,$$

wobei (i) und (ii) gelten für alle $1 \leq i \leq m-1$. Also ist insgesamt

$$\{1_G\} \leq G_0 = H_1 \leq H_2 \leq \ldots \leq H_m = G^{(r-1)} = G_1 \leq G_2 \leq \ldots \leq G_n = G$$

eine Kette von Untergruppen wie gesucht.

'$\Leftarrow$' Induktion nach n. Die Untergruppe $G_1 = \{1_G\}$ ist offensichtlich auflösbar. Sei nun $n > 1$. Per Induktion können wir annehmen, dass die Untergruppe G_{n-1} auflösbar ist. Andererseits ist die Faktorgruppe $G/G_{n-1} = G_n/G_{n-1}$ zyklisch von Primzahlordnung p_{n-1} nach Voraussetzung, also auch auflösbar nach Lemma 1.34. Damit ist G auflösbar nach Aufgabe 9(c). ■

Bemerkung 1.36

(a) Die alternierende Gruppe A_5 ist einfach.

(b) Für $n \geq 5$ sind die symmetrische Gruppe S_n und die alternierende Gruppe A_n nicht auflösbar.

Beweis:

(a) Zu zeigen: A_5 hat keine nichttrivialen Normalteiler.
Die Ordnung von A_5 ist $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. Die Elemente von A_5 sind die geraden Permutationen in S_5, also vom Zykeltyp $1^5, 2^2.1, 3.1^2$ und 5. Dies liefert (nachzählen!), dass es in A_5 genau

- 24 Elemente der Ordnung 5 gibt (Zykeltyp 5) $\Longrightarrow n_5 = 6$ (da die 5-Sylow-Untergruppen von A_5 zyklisch der Ordnung 5 sind).
- 20 Elemente der Ordnung 3 gibt (Zykeltyp 3.1^2) $\Longrightarrow n_3 = 10$ (da die 3-Sylow-Untergruppen von A_5 zyklisch der Ordnung 3 sind).
- 15 Elemente der Ordnung 2 gibt (Zykeltyp $2^2.1$) $\Longrightarrow n_2 = 5$.

Sei nun $\{1_G\} \neq N \trianglelefteq A_5$. Ist $|N|$ durch 5 teilbar, dann enthält N eine 5-Sylow-Untergruppen von A_5, also alle sechs 5-Sylow-Untergruppe von A_5, nach dem 2. Sylowsatz. Also ist $|N| \geq 1 + 24$, und daher ist $30 \mid |N|$, da $6 = n_5 \mid \frac{1}{5}|N|$ nach dem 3. Sylowsatz. Also ist $|N| \in \{30, 60\}$. Aber dann enthält N auch alle 3-Sylow-Untergruppen, da jede 3-Sylow-Untergruppe von G auch eine

3-Sylow-Untergruppe von N sein muss. Also ist $|N| > 1 + 24 + 20 = 44$, und damit ist $|N| = 60$. d.h. $N = A_5$.

Ist $|N|$ durch 3 teilbar, so sieht man mit einem ähnlichen Argument, dass $N = A_5$ ist.
Also ist $|N| \in \{2, 4\}$. Falls $|N| = 4$, dann enthält N eine 2-Sylow-Untergruppe, also alle 2-Sylow-Untergruppen da $N \trianglelefteq A_5$. Also ist $|N| \geq 1 + 15$, Widerspruch. Ist schließlich $|N| = 2$, so hat N genau ein Element m der Ordnung $2 \Longrightarrow m \in Z(A_5)$. Aber $Z(A_5) = \{1\}$, Widerspruch.
Damit hat A_5 keine nichttrivialen Normalteiler.

(b) Nach (a) ist A_5 einfach $\overset{\text{Lem. 1.34}}{\Longrightarrow}$ A_5 ist nicht auflösbar, da $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ keine Primzahl ist. Aber $A_5 \leq A_n \leq S_n$ für alle $n \geq 5$. Daher sind A_n und S_n nicht auflösbar nach Aufgabe 9(a). ■

Anmerkung 1.37

Für weitere Resultate über auflösbare und einfache endliche Gruppen:
siehe `Beamer_Woche_4.pdf`.
(Hier nur für das Allgemeinwissen. Diese Resultate können nicht mit dem Material dieser Vorlesung bewiesen werden.)

TEIL II: RINGE

3 Ringe, Ideale und Homomorphismen (∗)

3.1 Ringe, Körper, Integritätsbereiche (∗)

Wir fangen mit Erinnerungen von Begriffen und Beispielen aus der Vorlesung AGS an.

Definition 2.1 (*Ring*)

Eine nicht-leere Menge R zusammen mit zwei Verknüpfungen

$$\begin{array}{rccccccc} +\colon & R\times R & \longrightarrow & R & \qquad \cdot\colon & R\times R & \longrightarrow & R \\ & (a,b) & \mapsto & a+b\,, & & (a,b) & \mapsto & a\cdot b\,, \end{array}$$

heißt **Ring**, falls die folgenden Bedingungen gelten.

(R1) $(R,+)$ ist eine abelsche Gruppe. (Neutrales Element: 0_R. Inverses von $a\in R$: $-a$.)

(R2) $(R,\cdot)$ ist ein **Monoid**, d.h.:
(i) die Multiplikation $\cdot$ ist assoziativ ($(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall\, a,b,c\in R$)
(ii) $\exists 1\in R$ mit $1\cdot a = a\cdot 1 = a$ für alle $a\in R$ (1 ist ein neutrales Element für $\cdot$).

(R3) *Distributivität von $\cdot$ über $+$*: für alle $a,b,c\in G$ gelten

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{und} \quad (a+b)\cdot c = a\cdot c + b\cdot c\,.$$

Gilt zudem für alle $a,b\in G$: $a\cdot b = b\cdot a$ (*Kommutativität von* $\cdot$), so heißt R ein **kommutativer** Ring.

Notation: Wir schreiben einen solchen Ring $(R,+,\cdot)$, oder einfach als R, wenn die betrachteten Verknüpfungen aus dem Kontext klar sind. Wir nennen die Verknüpfung $+$ *Addition* und die Verknüpfung $\cdot$ *Multiplikation*. Meistens schreiben wir die Multiplikation einfach als ab anstelle von $a\cdot b$.

Definition 2.2 (*Einheitengruppe, Schiefkörper, Körper*)

Sei R ein Ring.

(a) Die Menge $R^\times := \{a\in R \mid 1 = a\cdot b = b\cdot a \text{ für ein } b\in R\}$ der invertierbaren Elemente

bildet eine Gruppe bezüglich der Multiplikation (siehe AGS). Diese Gruppe heißt **Einheitengruppe** von R.

(b) Wenn $1 \neq 0$ und $R^\times = R\backslash\{0\}$ gilt, so heißt R **Schiefkörper**. Ein **Körper** ist ein kommutativer Schiefkörper.

Definition 2.3 (*Nullteiler, Integritätsbereich*)

Sei R ein Ring.

(a) Ein Element $a \in R$ heißt **Nullteiler**, wenn es ein $c \in R\backslash\{0\}$ gibt mit $a \cdot c = 0$ oder $c \cdot a = 0$. Der Ring R heißt **nullteilerfrei**, falls es keine Nullteiler außer 0 in R gibt.

(b) Der Ring R heißt **Integritätsbereich**, falls R kommutativ und nullteilerfrei ist.

Beispiel 9

(a) $(\mathbb{Z}, +, \cdot)$ ist ein Ring.
$\mathbb{Z}$ ist kommutativ und Nullteilerfrei $\Longrightarrow \mathbb{Z}$ ist ein Integritätsbereich.
$\mathbb{Z}^\times = \{\pm 1\}$

(b) K Körper $\Longrightarrow K[X] = \{f(X) = \sum_{i=0}^{n} a_i X_i \mid n \in \mathbb{N}_0, a_i \in K\}$ ist ein Ring, bezüglich Polynomaddition und -multiplikation.
$K[X]$ heißt **Polynomring in einer Unbestimmten über** K.
$K[X]$ ist kommutativ und nullteilerfrei $\Longrightarrow K[X]$ ist ein Integritätsbereich.
$K[X]^\times = K^\times = K \setminus \{0\}$

(c) K Körper $\Longrightarrow M_n(K)$ $(n \in \mathbb{N})$ ist ein Ring, bezüglich Matrizenaddition und -multiplikation.
Für ein $n \geq 2$ ist $M_n(K)$ nicht kommutativ.
$(M_n(K))^\times = \mathrm{GL}_n(K)$ (die Gruppe der invertierbaren $n \times n$-Matrizen).
Z.B. für $n = 2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ sind Nullteiler.}$$

$\Longrightarrow M_n(K)$ ist i.A. kein Integritätsbereich.

(d) $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ ist ein kommutativer Ring, bezüglich Restklassenaddition und -multiplikation.
$\mathbb{Z}/m\mathbb{Z}$ ist i.A. kein Integritätsbereich, denn z.B. im Ring $\mathbb{Z}/10\mathbb{Z}$ gilt $\overline{2} \cdot \overline{5} = \overline{0}$.
$(\overline{2}, \overline{5} \in (\mathbb{Z}/10\mathbb{Z})\backslash\{\overline{0}\}$ sind Nullteiler.)

(e) $R = \mathbb{Z}[i] := \{a + b \cdot i \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist ein Ring, der **Ring der ganzen Gaußschen Zahlen**. (Siehe Aufgabe , Blatt 3).

(e) Der triviale Ring $\{0\}$ ist kein Integritätsbereich, da 0 kein Nullteiler in $\{0\}$ ist!

3.2 Ideale (∗)

In diesem Abschnitt ist R stets ein kommutativer Ring.

Definition 2.4 (*Ideal*)

Eine Teilmenge I von R heißt **Ideal** von R (in Zeichen $I \trianglelefteq R$), falls gelten:

(i) $(I, +)$ ist eine Untergruppe von $(R, +)$; und

(ii) $a \cdot c \in I \ \forall\ a \in I, \forall\ c \in R$.

Bemerkung 2.5

(a) Seien $I, J \trianglelefteq R$. Dann sind auch $I \cap J, I + J \trianglelefteq R$.

(b) Seien $a_1, \ldots, a_n \in R$, dann ist

$$I = a_1R + \ldots + a_nR := \{a_1c_1 + \ldots + a_nc_n \mid c_i \in R \ \forall\, 1 \leq i \leq r\} \trianglelefteq R.$$

Beweis: Siehe AGS. ■

Definition 2.6 (*Hauptideal, Hauptidealring*)

(a) In der Situation von Bemerkung 2.5 heißt $\{a_1, \ldots, a_n\}$ ein Erzeugendensystem von I. Wir schreiben dafür $I = (a_1, \ldots, a_n)$. Wenn $n = 1$ ist, heißt

$$I = aR = \{ac \mid c \in R\} = (a)$$

ein **Hauptideal** (**erzeugt von** a).

(b) Ein Integritätsbereich R heißt **Hauptidealring** (HIR), wenn jedes Ideal von R ein Hauptideal ist.

Beispiel 10

(a) $\mathbb{Z}$ ist ein Hauptidealring, denn:

- $\mathbb{Z}$ ist ein Integritätsbereich nach Beispiel 9(a); und
- jedes Ideal von $\mathbb{Z}$ hat die Form $m\mathbb{Z} = (m)$ für ein $m \in \mathbb{Z}$ (siehe AGS).

(b) Jeder euklidische Ring ist ein Hauptidealring (siehe AGS).
Insbesondere: K Körper $\Longrightarrow$ der Polynomring $K[X]$ ist ein HIR, da er ein euklidischer Ring ist (siehe AGS).

[Erinnerung: Nach Definition ist $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ eine *Primzahl* $:\Longleftrightarrow [p \mid ab \Longrightarrow p \mid a$ oder $p \mid b]$.

Definition 2.7 (*Primideal, maximales Ideal*)

Sei $I \triangleleft R$ ein echtes Ideal.

(a) I heißt **Primideal** $:\Longleftrightarrow$ aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

(b) I heißt **maximales Ideal** $:\Longleftrightarrow$ aus $I \subsetneq J \trianglelefteq R$ folgt $J = R$.

Bemerkung 2.8

Sei $R = \mathbb{Z}$.

(a) $\{0\} \neq I \triangleleft \mathbb{Z}$ Primideal $\Longleftrightarrow$ $I = (p)$ für eine Primzahl p.

(b) $\{0\} \neq I \triangleleft \mathbb{Z}$ Primideal $\Longrightarrow$ I maximales Ideal von $\mathbb{Z}$.

Beweis:

(a) '$\Rightarrow$' $I \triangleleft \mathbb{Z} \Longrightarrow \exists\, m \in \mathbb{Z}$ mit $I = (m)$. Behauptung: m ist eine Primzahl.
Aber $m \mid ab$ mit $a, b \in \mathbb{Z} \Longrightarrow ab = mc$ für ein $c \in \mathbb{Z} \Longrightarrow ab \in I \Longrightarrow a \in I$ oder $b \in I$, da I ein Primideal ist. Aber $I = (m)$ liefert $m \mid a$ oder $m \mid b$, also ist m eine Primzahl.
'$\Leftarrow$' Sei umgekehrt $p \in \mathbb{Z}$ eine Primzahl. Seien $a, b \in \mathbb{Z}$ mit $ab \in (p) \Longrightarrow p \mid ab \Longrightarrow p \mid a$ oder $p \mid b \Longrightarrow a \in (p)$ oder $b \in (p) \Longrightarrow (p)$ Primideal.

(b) Nach (a) ist $I = (p)$ für eine Primzahl p. Sei nun $a \in \mathbb{Z} \setminus (p)$. Da $\mathbb{Z}$ ein HIR ist (Beispiel 10(a)), gilt $(p, a) = (d)$ für ein $d \in \mathbb{Z} \Longrightarrow \exists\, b, c \in \mathbb{Z}$ mit $p = db$ und $a = dc$, also $d \mid p$ und $d \mid a \Longrightarrow d \in \{\pm 1\}$ (da $a \in \mathbb{Z} \setminus (p)$ ist) $\Longrightarrow (p, a) = (1) = \mathbb{Z}$, so dass I maximal ist. ∎

3.3 Faktorringe und Ringhomomorphismen

Sei weiterhin R ein kommutativer Ring.

Erinnerung (AGS): Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann definiert $a \equiv b :\Leftrightarrow a - b \in I$ eine Äquivalenzrelation auf R mit folgenden Eigenschaft:

$$a_1 \equiv b_1 \text{ und } a_2 \equiv b_2 \quad \Longleftrightarrow a_1 + a_2 \equiv b_1 + b_2 \text{ und } a_1 \cdot a_2 \equiv b_1 \cdot b_2\,.$$

Bezeichne $\overline{a} := a + I$ die Klasse (oder Restklasse) von $a \in R$. Dann ist die Menge

$$R/I := \{a + I \mid a \in\ R\}$$

der Äquivalenzklassen ein Ring, bezüglich der Verknüpfungen

$$+: \begin{array}{ccc} R \times R & \longrightarrow & R \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b}\,, \end{array} \qquad \cdot: \begin{array}{ccc} R \times R & \longrightarrow & R \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b}\,, \end{array}$$

der **Faktorring von R nach I**.
Ist R kommutativ, so ist natürlich auch R/I kommutativ.
Es gelten: $\overline{0}$ ist das neutrale Element für die Addition in R/I und $\overline{1}$ ist das neutrale Element für die Multiplikation in R/I.
Außerdem ist $a \in R$, dann ist $-\overline{a} = \overline{-a}$, und falls $a \in R^\times$, so ist $\overline{a} \in (R/I)^\times$ und $\overline{a}^{-1} = \overline{a^{-1}}$ gilt.

Satz 2.9

Sei $I \triangleleft R$ ein echtes Ideal. Dann gelten:

(a) I ist ein Primideal $\iff$ R/I ist ein Integritätsbereich.

(b) I ist ein maximales Ideal $\iff$ R/I ist ein Körper.

Beweis:

(a) I ist ein Primideal $\iff \forall\ a, b \in R$ gilt $[ab \in I \implies a \in I$ oder $b \in I]$
$\iff \forall\ \overline{a}, \overline{b} \in R/I$ gilt $[\overline{a}\overline{b} = \overline{0} \implies \overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}]$
$\iff R/I$ ist ein Integritätsbereich.

(b) Es gilt: $I \triangleleft R$ echtes Ideal $\iff R/I \neq \{\overline{0}\}$. Insbesondere ist $\overline{1} \neq \overline{0}$, da $1 \notin I$ ($I \neq R$). Daraus folgt:
I ist ein maximales Ideal $\iff \forall\ a \in R \setminus I$ gilt $(a) + I = R$
$\iff \forall\ a \in R \setminus I, \exists\ c \in R$ mit $1 - ca \in I$
$\iff \forall\ \overline{0} \neq \overline{a} \in R/I, \exists\ \overline{c} \in R/I$ mit $\overline{1} - \overline{ca} = \overline{0}$.
$\iff \forall\ \overline{0} \neq \overline{a} \in R/I, \exists\ \overline{c} \in R/I$ mit $\overline{ca} = \overline{1}$.
$\iff (R/I)^\times = (R/I) \setminus \{\overline{0}\}$
$\iff R/I$ ist ein Körper. ■

Folgerung 2.10

Jedes maximale Ideal von R ist auch ein Primideal von R.

Beweis: Sei $I \triangleleft R$ ein maximales Ideal. Nach Satz 2.9(b) ist R/I ein Körper, also insbesondere ein Integritätsbereich. Nun ist I ein Primideal nach Satz 2.9(a). ■

Achtung: die Umkehrung ist im Allgemeinen falsch!

Beispiel 11

Sei $R = \mathbb{Z}$. Dann hat jedes Ideal $I \neq \{0\}$ von $\mathbb{Z}$ die Form $I = (m) = m\mathbb{Z}$ für ein $m \in \mathbb{N}$. (Siehe AGS.)
Frage: Ist $R/I = \mathbb{Z}/m\mathbb{Z}$ ein Körper?
Antwort: Nach Satz 2.9(b) ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper genau dann, wenn (m) ein maximales Ideal ist, also nach Folgerung 2.10 und Proposition 2.8 genau dann, wenn m eine Primzahl ist, d.h.:

$$\mathbb{Z}/m\mathbb{Z} \text{ Körper} \quad \iff \quad m \text{ Primzahl}$$

Notation: Für p eine Primzahl heißt $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ **Körper mit p Elementen**.

Definition 2.11 (*Homo-, Endo-, Iso-, Automorphismus, Kern, Bild*)

Seien R und S Ringe. Eine Abbildung $\varphi : R \longrightarrow S$ heißt **Ringhomomorphismus** (oder **Homomorphismus**), wenn für alle $a_1, a_2 \in R$ gilt:

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \qquad \varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2) \qquad \text{und} \qquad \varphi(1_R) = 1_S$$

· Ein Homomorphismus $\varphi : R \longrightarrow R$ heißt **Endomorphismus**, ein bijektiver Homomorphismus heißt **Isomorphismus** (in Zeichen: $R \cong S$), ein bijektiver Endomorphismus heißt **Automorphismus**.

· Der **Kern** von φ ist $\ker(\varphi) := \{a \in R \mid \varphi(a) = 0\} \subseteq R$. Das **Bild** von φ ist $\varphi(R) := \{\varphi(a) \mid a \in R\} \subseteq S$.

Beispiel 12

Sei R ein Ring und $I \trianglelefteq R$ ein Ideal von R. Dann ist der **Restklassenhomomorphismus**

$$\begin{array}{rccc} \pi\colon & R & \longrightarrow & R/I \\ & a & \mapsto & \overline{a} = a + I \end{array}$$

ein Ringhomomorphismus. Nach Teil I ist π ein Gruppenhomomorphismus zwischen $(R, +)$ und $(R/I, +)$. Ferner gilt für alle $a_1, a_2 \in R$:

$$\pi(a_1 \cdot a_2) = \overline{a_1 \cdot a_2} = \overline{a_1} \cdot \overline{a_2} = \pi(a_1) \cdot \pi(a_2) \quad \text{und} \quad \pi(1) = \overline{1} = 1_{R/I}$$

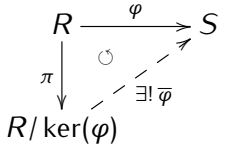
Es gibt natürlich auch Isomorphiesätze für Ringe. (Beweise: siehe AGS.)

Satz 2.12 (*Homomorphiesatz für Ringe (1. Isomorphiesatz)*)

Seien R und S Ringe und $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gelten:

(a) $\ker(\varphi)$ ist ein Ideal von S und $\varphi(R)$ ist ein Teilring von S.

(b) Sei $\pi : R \longrightarrow R/\ker(\varphi)$, $a \mapsto \overline{a}$ der Restklassenhomomorphismus. Es gibt einen eindeutigen Ringhomomorphismus $\overline{\varphi} : R/\ker(\varphi) \longrightarrow S$ mit $\varphi = \overline{\varphi} \circ \pi$. Insbesondere ist das folgende Diagramm kommutativ:



Es gelten $\overline{\varphi}(R/\ker(\varphi)) = \varphi(R)$ und $\overline{\varphi}$ is injektiv. Insbesondere gibt es einen Ringisomorphismus $R/\ker(\varphi) \cong \overline{\varphi}(R)$.

Satz 2.13 (*2. Isomorphiesatz*)

Seien R ein Ring, $S \subseteq R$ ein Teilring von R, und $I \trianglelefteq R$ ein Ideal von R. Dann gelten:

(i) $S + I$ ist ein Teilring von R (ii) $I \trianglelefteq S + I$ (iii) $I \cap S \trianglelefteq S$.

Ferner gibt es einen Ringisomorphismus

$$S/(S \cap I) \cong (S + I)/I.$$

Satz 2.14 (*3. Isomorphiesatz*)

Seien I, J Ideale von R mit $I \subseteq J$. Dann ist $J/I \trianglelefteq R/I$, und es gibt einen Ringisomorphismus

$$(R/I)/(J/I) \cong R/J.$$

Aufgabe 13 (*Two-step quotient; Aufgabe 13, Blatt 4*)

Seien R ein Ring und $I, J \trianglelefteq R$ Ideale von R. Zeigen Sie:

(a) $R/(I+J) \cong (R/I)/((I+J)/I)$;

(b) $(R/J)/((I+J)/J) \cong (R/I)/((I+J)/I)$.

Bemerkung 2.15

Sei R ein Ring. Dann gibt es einen eindeutigen Ringhomomorphismus $\theta_R : \mathbb{Z} \longrightarrow R$. Der Kern von θ_R ist $\ker(\theta_R) = (p)$ für eine eindeutige ganze Zahl $p \in \mathbb{Z}_{\geq 0}$.

Beweis: Für $m \in \mathbb{Z}$ setze

$$\theta_R(m) := \begin{cases} \sum_{i=1}^{m} 1_R = \underbrace{1_R + \ldots + 1_R}_{m\text{-mal}} & \text{falls } m > 0\,, \\ 0 & \text{falls } m = 0\,, \\ -\sum_{i=1}^{-m} 1_R = \underbrace{(-1_R) + \ldots + (-1_R)}_{(-m)\text{-mal}} & \text{falls } m < 0\,. \end{cases}$$

Dann ist $\theta_R : \mathbb{Z} \longrightarrow R$ ein Ringhomomorphismus (siehe Aufgabe 14, Blatt 4).
Nun ist θ_R eindeutig bestimmt nach Konstruktion: wäre $\phi : \mathbb{Z} \longrightarrow R$ ein zweiter Ringhomomorphismus zwischen $\mathbb{Z}$ und R, dann wären $\phi(0_\mathbb{Z}) = 0$ und $\phi(1_\mathbb{Z}) = 1_R$. Damit wären für alle $m > 0$:

$$\phi(m) = \phi(\sum_{i=1}^{m} 1_\mathbb{Z}) = \sum_{i=1}^{m} \phi(1_\mathbb{Z}) = \sum_{i=1}^{m} 1_R = \theta_R(m)$$

und

$$\phi(-m) = \phi((-1_\mathbb{Z})m) = \phi(-1_\mathbb{Z})\phi(m) = -\phi(1_\mathbb{Z})\phi(m) = -1_R\theta_R(m) = -\theta_R(m) = \theta_R(-m)\,.$$

Da $\mathbb{Z}$ ein Hauptidealring ist, gilt also $\ker(\theta_R) = p\mathbb{Z} = (p)$ mit einer eindeutigen ganzen Zahl $p \geq 0$. ■

Definition 2.16 (*Charakteristik eines Ringes*)

Sei R ein Ring. Die eindeutige ganze Zahl $p \in \mathbb{Z}_{\geq 0}$ mit $\ker(\theta_R) = (p)$ heißt **Charakteristik** von R. Wir schreiben $\mathrm{char}(R) := p$.

Beispiel 13

(a) $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\} \Longrightarrow \mathrm{char}(R) = 0$. (Offensichtlich ist $1 + \ldots + 1$ nie 0.)

(b) In $R = \mathbb{Z}/2\mathbb{Z}$ ist $\overline{1} + \overline{1} = \overline{2} = \overline{0} \Longrightarrow \mathrm{char}(R) = 2$.

Bemerkung 2.17

Die Charakteristik eines Integritätsbereichs ist entweder Null oder eine Primzahl.

Beweis: Sei R ein Integritätsbereich. Dann ist $\mathbb{Z}/\ker(\theta_R) \cong \theta_R(\mathbb{Z})$ nach dem Homomorphiesatz.

- Falls $\ker(\theta_R) = (0)$ ist, dann ist $\mathrm{char}(R) = 0$.
- Falls $\ker(\theta_R) \neq 0$, dann ist $\ker(\theta_R) = (p)$ für eine ganze Zahl $p \in \mathbb{Z}_{>0}$. Dann ist $\mathbb{Z}/p\mathbb{Z}$ isomorph zu $\theta_R(\mathbb{Z}) \subseteq R$, also ist $\mathbb{Z}/p\mathbb{Z}$ ein Integritätsbereich, da R ein Integritätsbereich ist. Aber ein endlicher Integritätsbereich ist ein Körper nach [Aufgabe 11, Blatt 3], also ist p eine Primzahl nach Beispiel 11.

■

4 Teilbarkeit und Primzerlegung

In diesem Abschnitt sei R immer ein Integritäsbereich.

4.1 ZPE-Ringe

Definition 2.18 (*teilen, assoziierte Elemente*)

Seien $a, b \in R$ zwei Elemente. Dann:

(a) a **teilt** b (in Zeichen: $a \mid b$), falls ein $c \in R$ mit $a \cdot c = b$ existiert.

(b) a ist **assoziiert** zu b (in Zeichen: $a \simeq b$), falls $a \mid b$ und $b \mid a$.

Beispiel 14

(a) In $R = \mathbb{Z}$ gelten: $2 \mid 8$ und $2 \simeq (-2)$. I.A. $m \simeq (-m)$ für alle $m \in \mathbb{Z}$.

(b) $e \in R^\times \iff e \simeq 1$.

Bemerkung 2.19

Seien $a, b \in R \setminus \{0\}$. Dann gelten:

(a) $a \mid b \implies (b) \subseteq (a)$. ('Teilen für Elemente' = 'enthalten für Ideale')

(b) $a \simeq b \iff (b) = (a) \iff \exists\, e \in R^\times$ mit $a = be$

Beweis: (a) $a \mid b \implies \exists\, c \in R$ mit $ac = b \implies b \in (a) \implies (b) \subseteq (a)$.

(b) Die erste Äquivalenz folgt direkt aus (a), da $a \mid b$ und $b \mid a$, somit bleibt nur die zweite zu beweisen.

'⇒' $a \simeq b \implies a \mid b$ und $b \mid a \implies \exists\, u, v \in R$ mit $au = b$ und $bv = a \implies bvu = au = b \implies b(vu - 1) = 0 \implies$ vu=1, da $b \neq 0$ und R ein Integritätsbereich ist, also sind $u, v \in R^\times$.

'⇐' $a = be$ mit $e \in R^\times \implies b = ae^{-1} \implies a \mid b$ und $b \mid a \implies a \simeq b$ nach Definition. ■

Aus der elementaren Arithmetik ist bekannt, dass sich jedes $n \in \mathbb{N}$ mit $n > 1$ eindeutig schreiben lässt als Produkt $n = p_1 p_2 \cdots p_r$ mit Primzahlen $p_1 \leq p_2 \leq \ldots \leq p_r$. Für allgemeinere Ringe gilt zunächst, dass der gewohnte Begriff 'Primzahl' in zwei Begriffe zerfällt:

Definition 2.20 (*Irreduzible Elemente, Primelemente*)

Sei $0 \neq p \in R \setminus R^\times$ ein Element, das keine Einheit ist.

(a) p heißt **irreduzibel**, wenn gilt: $b \mid p$ (mit $b \in R$) $\Rightarrow b \simeq p$ oder $b \simeq 1$.

(b) p heißt **Primelement** (oder **prim**), wenn gilt: Sind $a, b \in R$ mit $p \mid ab$, so ist $p \mid a$ oder $p \mid b$.

Für $R = \mathbb{Z}$ ist jedes irreduzible Element auch Primelement; hier entsprechen diese beiden Begriffe einfach dem üblichen Begriff 'Primzahl'. Dies gilt allgemeiner für Hauptidealringe, aber nicht i. A. für Integritätsbereiche:

Bemerkung 2.21

Sei $0 \neq p \in R \setminus R^\times$. Dann gelten:

(a) Ist p ein Primelement, so ist p irreduzibel.

(b) p ist ein Primelement $\iff$ (p) ist ein Primideal ($\iff$ $R/(p)$ ist ein Integritätsbereich).

(c) p ist irreduzibel $\iff$ (p) ist maximal unter den Hauptidealen von R.

(d) Ist R ein Hauptidealring, so gilt: p ist ein Primelement $\iff$ p ist irreduzibel.

Beweis:

(a) und (c): AGS.

(b) Genau wie in Bemerkung 2.8 im Fall $R = \mathbb{Z}$.

(d) Noch zu zeigen: p ist irreduzibel $\implies$ p ist ein Primelement.
Aber: p kein Primelement $\overset{(b)}{\implies}$ (p) ist kein Primideal $\overset{Folg.\ 2.10}{\implies}$ (p) ist kein maximales Ideal von R $\implies$ p ist nicht irreduzibel nach (c), da R ein Hauptidealring ist. ∎

Definition 2.22 (*Primzerlegung, ZPE-Ring*)

(a) Sei $a \in R \setminus \{0\}$. Eine Darstellung $a = e \cdot \prod_{i=1}^{r} p_i^{n_i}$ mit $e \in R^\times$ und Primelemente $p_1, \ldots, p_r$ ($r \in \mathbb{N}$) heißt **Primzerlegung** von a.

(b) Der Ring R heißt **ZPE-Ring**, wenn jedes $a \in R \setminus \{0\}$ eine Primzerlegung besitzt.

Bemerkung 2.23

Hat $a \in R \setminus \{0\}$ eine Primzerlegung, so ist diese bis auf Assoziierte und Reihenfolge eindeutig. Insbesondere ist in ZPE-Ringen die Primzerlegung (bis auf Assoziierte und Reihenfolge) eindeutig.

Beweis: Siehe AGS. ∎

Beispiel 15

(a) $R = \mathbb{Z}$. Ist $n \in \mathbb{Z}$, dann hat n eine Primzerlegung der Form $n = (\pm 1)p_1 \cdots p_r$ für positive Primzahlen $p_1, \ldots, p_r$ ($r \in \mathbb{N}$) $\implies$ $\mathbb{Z}$ ist ein ZPE-Ring.

(b) K Körper, $R = K[X]$. Ist $f \in R$, dann hat f eine Darstellung $f = a \cdot \prod_{i=1}^{r} p_i^{n_i}$ mit $a \in R^\times$ und $p_1, \ldots p_r \in K[X]$ Primpolynome mit Leitkoeffizienten 1 $\implies$ $K[X]$ ist ein ZPE-Ring.

Bemerkung 2.24

In einem Hauptidealring wird jede aufsteigende Idealkette stationär.

Beweis: Sei $I_1 \subseteq I_2 \subseteq \dots$ eine aufsteigende Idealkette im R. Setze $I := \bigcup_{i \geq 1} I_i$ (dies ist ein Ideal von R). Da R ein HIR ist, gibt es ein Element $b \in R$ mit $I = (b) \Longrightarrow \exists\, n \in \mathbb{N}$ mit $b \in I_n$. Aber dann gilt

$$I = (b) \subseteq I_n \subseteq I_{n+1} \subseteq \dots \subseteq I\,.$$

Es folgt, dass $I_n = I_{n+1} = \cdots$, also ist die Idealkette stationär. ■

Satz 2.25

Jeder Hauptidealring ist ein ZPE-Ring.

Beweis: Sei $a \in R \setminus \{0\}$. Suche Primzahlzerlegung von a.

- Falls $a \in R^x$ ist, dann a ist schon Primzahlzerlegung von a ✓.
- Falls a ein Primelement ist, dann ist auch a schon eine Primzahlzerlegung von a ✓.
- Sonst ist $a \in R \setminus R^\times$ und $a = a_1 b_1$ mit $a_1, b_1 \in R \setminus R^\times$, da a reduzibel nach Bemerkung 2.21(d) ist. Dann gilt $(a) \subsetneq (a_1)$, denn weil $b_1 \notin R^\times$, ist $a_1 \notin (a)$.
  Falls a_1 nicht prim ist, dann ist $a_1 = a_2 b_2$ mit $a_2, b_2 \in R \setminus R^\times \Longrightarrow (a) \subsetneq (a_1) \subsetneq (a_2)$
  ...
  $a = a_n b_n \cdots b_1$ mit $(a) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n)$.
  Aber dieses Verfahren bricht ab nach Bemerkung 2.24: wir nehmen o.B.d.A. an, dass $a_n := p_1$ ein Primelement ist, d.h. $a = p_1 a'$.
  Falls $a' \in R^\times$ ✓. Sonst selbes Argument für a' liefert $a' = p_2 a''$. Auf diese Weise erhalten wir eine aufsteigende Idealkette $(a) \subsetneq (a') \subsetneq (a'') \subsetneq \cdots$ Bemerkung 2.24 $\Longrightarrow$ auch diese Kette bricht ab, d.h. $\exists\, m \in \mathbb{N}$ mit $e := a^{(m)} \in R^\times$
  $\Longrightarrow a = e p_1 \cdots p_m$ für Primelemente $p_1, \dots, p_m \in R$.

■

4.2 Quotientenkörper

In diesem Abschnitt ist R stets ein Integritätsbereich.

Ziel: Wir möchten den kleinsten Körper finden, in den R eingebettet werden kann.

Definition 2.26 (*Quotientenkörper*)

Ist R Teilring eines Körpers Q und gilt

$$R \subseteq Q = \{ab^{-1} \mid a \in R, b \in R \setminus \{0\}\}\,,$$

so heißt Q ein **Quotientenkörper** von R.
Schreibe $d_{R,Q} : R \longrightarrow Q, a \mapsto a1^{-1}$ für die natürliche Inklusion von R in Q. (Diese ist ein Ringhomomorphismus.)

Warnung: Oben ist $b^{-1} \in K^\times$, d.h.: b ist ein Element von R, das in K invertierbar ist, aber es kann sein, dass b in R nicht invertierbar ist.

Beispiel 16

(a) Z. B. ist $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\} = \{ab^{-1} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$ ein Quotientenkörper von $\mathbb{Z}$.

(b) $\mathbb{Q}$ ist auch Quotientenkörper von $\mathbb{Q}$ selbst.

(c) K Körper $\Longrightarrow$ ein Quotientenkörper des Polynomrings $R = K[X]$ ist der **Körper der rationalen Funktionen** $K(X) = \{\frac{f(X)}{g(X)} \mid f(X), g(X) \in R, g(X) \neq 0\}$.

Satz 2.27

Jeder Integritätsbereich besitzt einen Quotientenkörper.

Beweis: Sei R ein Integritätsbereich. Definiere eine Relation $\sim$ auf $R \times (R \setminus \{0\})$ durch:

$$(a,b) \sim (c,d) \overset{Def.}{\Longleftrightarrow} ad = bc$$

Dies ist eine Äquivalenzrelation:

- **Reflexivität**: R Integritätsbereich $\Longrightarrow$ R kommutativ $\Longrightarrow$ $ab = ba \ \forall\ a,b \in R \Longrightarrow (a,b) \sim (a,b)$ $\forall\ (a,b) \in R \times (R \setminus \{0\})$.
- **Symmetrie**: $(a,b) \sim (c,d) \Longleftrightarrow ad = bc \overset{R \text{ komm.}}{\Longleftrightarrow} cb = da \Longleftrightarrow (c,d) \sim (a,b)$.
- **Transitivität**: $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f) \Longleftrightarrow ad = bc$ und $cf = de$. Also (mit Kommutativität von R) gilt
$$afd = adf = bcf = bde = bed\,.$$
Dies liefert $af = be$, da $d \in R \setminus \{0\}$ und R ein Integritätsbereich ist. Also ist $(a,b) \sim (e,f)$.

Bezeichne mit $\frac{a}{b}$ die Äquivalenzklasse von $(a,b) \in R \times (R \setminus \{0\})$. Definiere dann eine Addition und eine Multiplikation auf der Menge $Q(R) := R \times (R \setminus \{0\})/\sim$ der Äquivalenzklassen durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

für alle $a, c \in R$ und für alle $b, d \in R \setminus \{0\}$.

Die Verknüpfungen $+ : Q(R) \times Q(R) \longrightarrow Q(R)$ und $\cdot : Q(R) \times Q(R) \longrightarrow Q(R)$ sind wohldefiniert: Sind $\frac{a}{b} = \frac{a'}{b'} \in Q(R)$ und $\frac{c}{d} = \frac{c'}{d'} \in Q(R)$, so gilt $ab' = ba'$ und $cd' = dc'$

$$\Longrightarrow (ad + bc)b'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd' + b'c')$$

$$\Longrightarrow \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}, \ \text{d.h.} \ \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$$

Es gilt auch $acb'd' = ab'cd' = ba'dc' = bda'c'$, und damit ist $\frac{ac}{bd} = \frac{a'c'}{b'd'} \Longrightarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$.

Außerdem ist $(Q(R), +, \cdot)$ ist ein Ring: Übung [Aufgabe 15, Blatt 4]

Das Einselement ist $1_{Q(R)} = \frac{1}{1}$, da $\frac{1}{1} \cdot \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b} \cdot \frac{1}{1}$ für alle $\frac{a}{b} \in Q(R)$.

Das Nullelement ist $0_{Q(R)} = \frac{0}{1}$, da $\frac{0}{1} + \frac{a}{b} = \frac{0b + 1a}{1b} = \frac{a}{b}$ und $\frac{a}{b} + \frac{0}{1} = \frac{a1 + b0}{b1} = \frac{a}{b}$ für alle $\frac{a}{b} \in Q(R)$.

Sei nun $\frac{a}{b} \in Q(R) \setminus \{\frac{0}{1}\}$. Dann ist $a \neq 0$, und damit ist $\frac{b}{a} \in Q(R)$. Es gilt: $\frac{a}{b} \cdot \frac{b}{a} := \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1} = 1_{Q(R)}$, da $(ab, ab) \sim (1,1) \Longrightarrow Q(R)$ ist ein Körper.

Nun, für $a, b \in R$, ist $\frac{a}{1} = \frac{b}{1} \Leftrightarrow (a,1) \sim (b,1) \Leftrightarrow a \cdot 1 = 1 \cdot b \Leftrightarrow a = b$. Daraus folgt, dass die Abbildung

$$\begin{array}{rccc} \delta_R : & R & \longrightarrow & Q(R) \\ & a & \mapsto & \frac{a}{1} \end{array}$$

injektiv ist. Außerdem gilt für alle $a, b \in R$:

- $\delta_R(a + b) = \frac{a+b}{1} = \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a}{1} + \frac{b}{1} = \delta_R(a) + \delta_R(b)$;
- $\delta_R(a \cdot b) = \frac{a \cdot b}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = \delta_R(a) \cdot \delta_R(b)$; und

· $\delta_R(1) = \frac{1}{1} = 1_{Q(R)}$.

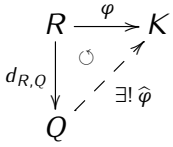
Also ist δ_R ein injektiver Ringhomomorphismus, und damit ist R ein Teilring von $Q(R)$. Dann ist $Q(R)$ ein Quotientenkörper von $\delta_R(R) \cong R$ (Homomorphiesatz!) , da

$$Q(R) = \{\frac{a}{b} \mid a \in R, b \in R \setminus \{0\}\} = \{\delta_R(a)\delta_R(b)^{-1} \mid a \in R, b \in R \setminus \{0\}\}\,.$$

(Insbesondere $d_{R,Q(R)} = \delta_R$.) ■

Bemerkung 2.28 (*Universelle Eigenschaft des Quotientenkörpers*)

Seien R ein Integritätsbereich und Q ein Quotientenkörper von R.
Sei K ein Körper und $\varphi : R \longrightarrow K$ ein injektiver Ringhomomorphismus. Dann gibt es einen eindeutigen injektiven Ringhomomorphismus $\widehat{\varphi} : Q \longrightarrow K$ mit $\widehat{\varphi} \circ d_{R,Q} = \varphi$. Insbesondere ist das folgende Diagramm kommutativ:



Beweis: [Aufgabe 15, Blatt 4] ■

Folgerung 2.29 (*Eindeutigkeit des Quotientenkörpers*)

Ein Quotientenkörper von R ist bis auf Isomorphie eindeutig bestimmt.

Beweis: Seien $Q(R) = R \times (R \setminus \{0\})/\sim$ und $\delta_R : R \longrightarrow Q(R)$ wie im Beweis vom Satz 2.27. Sei Q ein zweiter Quotientenkörper von R. Schreibe $d_{R,Q} : R \longrightarrow Q$ für die inklusion von R in Q. Nach Bemerkung 2.28 gibt es einen eindeutigen injektiven Ringhomomorphismus $\widehat{d_{R,Q}} : Q(R) \longrightarrow Q$ mit $\widehat{d_{R,Q}} \circ \delta_R = d_{R,Q}$. Nach Bemerkung 2.28 gibt es auch einen eindeutigen injektiven Ringhomomorphismus $\widehat{\delta_R} : Q \longrightarrow Q(R)$ mit $\widehat{\delta_R} \circ d_{R,Q} = \delta_R$. Aber dann gelten:

$$d_{R,Q} = \widehat{d_{R,Q}} \circ \delta_R = \widehat{d_{R,Q}} \circ \widehat{\delta_R} \circ d_{R,Q} \quad \text{und} \quad \delta_R = \widehat{\delta_R} \circ d_{R,Q} = \widehat{\delta_R} \circ \widehat{d_{R,Q}} \circ \delta_R$$

und auch

$$d_{R,Q} = \mathrm{Id}_Q \circ d_{R,Q} \quad \text{und} \quad \delta_R = \mathrm{Id}_{Q(R)} \circ \delta_R\,.$$

Die Eindeutigkeit liefert $\mathrm{Id}_Q = \widehat{d_{R,Q}} \circ \widehat{\delta_R}$ und $\mathrm{Id}_{Q(R)} = \widehat{\delta_R} \circ \widehat{d_{R,Q}}$, also $Q \cong Q(R)$. ■

Es ist jetzt gerechtfertigt, von **dem** Quotientenkörper von R zu sprechen. Wir schreiben dafür $Q(R)$.

Anmerkung 2.30

Der Quotientenkörper von R ist der kleinste Körper, der R enthält.
[Dies folgt z.B. aus Bemerkung 2.28.]

Folgerung 2.31

(a) Jeder Körper K der Charakteristik Null besitzt einen zu $\mathbb{Q}$ isomorphen Unterkörper (und muss insbesondere unendlich viele Elemente besitzen).

(b) Jeder Körper K der Charakteristik $p > 0$ besitzt einen zu $\mathbb{F}_p$ isomorphen Unterkörper.

Beweis: (a) Nach Bemerkung 2.15 gibt es einen eindeutigen Ringhomomorphismus $\theta_K : \mathbb{Z} \longrightarrow K$. Nun ist $\ker(\theta_K) = (0)$, da $\mathrm{char}(K) = 0$ ist, also ist θ_K injektiv. Nach Bemerkung 2.28 gibt es einen eindeutigen injektiven Ringhomomorphismus $\widehat{\theta_K} : \mathbb{Q} = Q(\mathbb{Z}) \longrightarrow K$ mit $\widehat{\theta_K} \circ \delta_R = \theta_K$. Damit ist $\mathbb{Q} \cong \widehat{\theta_K}(\mathbb{Q}) \subseteq K$ einen Unterkörper.

(b) Nach Bemerkung 2.15 gibt es einen eindeutigen Ringhomomorphismus $\theta_K : \mathbb{Z} \longrightarrow K$. Da $\mathrm{char}(K) = p$, ist $\ker(\theta_K) = (p) = p\mathbb{Z}$, also ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \theta_K(\mathbb{Z}) \subseteq K$ nach dem Homomorphiesatz. ■

4.3 Irreduzibilität in Polynomringen

Wie zeigen wir, ob ein Polynom $f(X) \in \mathbb{Q}[X]$ irreduzibel ist, zum Beispiel

$$f = X^3 - 5X + 3 \quad X^{25} + 6X^{16} + 15X^6 + 3\,, \text{ oder } X^{100} + X^{56} - 24?$$

Wir stellen hier einige grundlegende Verfahren vor, um diese Frage zu entscheiden.

Wiederholung aus der AGS über Polynomringe:
Sei R ein **Integritätsbereich**. Dann:

- Sei $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ ein Polynom mit Leitkoeffizient $a_n \in R \setminus \{0\}$. Der **Grad** $\deg(f)$ von $f \neq 0$ definiert man als $\deg(f) := n$, und wir setzen $\deg(0) := -\infty$.
  Ist $a_n = 1$, so heißt f **normiert**.
- $f, g \in R[X]$ Polynome $\Longrightarrow \deg(f \cdot g) = \deg(f) + \deg(g)$
- Der Polynomring $R[X]$ ist ein Integritätsbereich $\Longrightarrow R[X_1, \ldots, X_n]$ ist auch ein Integritätsbereich für alle $n \in \mathbb{N}$.
- $R[X]^\times = R^\times$ (konstante Polynome)
- $R = K$ Körper $\Longrightarrow K[X]$ ist ein euklidischer Ring (mit Grundfunktion deg).
- $R = K$ Körper $\Longrightarrow$ für jedes $f \in K[X]$ mit $\deg(f) = n \geq 0$ gilt:
  (i) Ist $a \in K$ eine Nullstelle von f, so gilt $(X - a) \mid f$; und
  (ii) f hat höchstens n Nullstellen.

Bemerkung 2.32 (*Universelle Eigenschaft von Polynomringen*)

Für jeden Ringhomomorphismus $\varphi : T \longrightarrow S$ zwischen zwei kommutativen Ringen T und S und jedes $a \in S$ existiert ein eindeutiger Ringhomomorphismus (genannt **Einsetzungshomomorphismus**) $\varphi_a : T[X] \longrightarrow S$ mit $\varphi_a|_T = \varphi$ und $\varphi_a(X) = a$.

Beweis: Wenn es φ_a mit obigen Eigenschaften gibt, so ist klar, dass φ_a eindeutig bestimmt ist. (Weil jedes Element von $T[X]$ durch Summen und Produkte von X und Elementen aus R gebildet ist.)
Sei nun $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ ein beliebiges Element von $T[X]$. Definiere

$$\varphi_a(f) := \varphi(a_n)a^n + \varphi(a_{n-1})a^{n-1} + \ldots + \varphi(a_1)a + \varphi(a_0)$$

und rechne sofort nach, dass φ_a ein Ringhomomorphismus ist. ■

Anmerkung 2.33

1. Konkret für $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in T[X]$ ist

$$\varphi_a(f) = \varphi(a_n)a^n + \varphi(a_{n-1})a^{n-1} + \ldots + \varphi(a_1)a + \varphi(a_0)\,.$$

   An dieser Formel sieht man, dass $\varphi_a(f)$ durch "Einsetzen" von a für die Unbestimmte X entsteht. Falls falls $\varphi = \mathrm{Id}_T$, schreiben wir dann auch $f(a)$ anstelle von $\varphi_a(f)$, für alle $f \in T[X]$.

2. Falls $T = S$ (oder $T \subseteq S$) und $\varphi = \mathrm{Id}_T$, dann gilt: $f \in \ker(\varphi_a) \iff f(a) = 0$, also genau dann, wenn a eine **Nullstelle** von f ist.

3. Sei R ein Integritätsbereich. Sei $p \in R$ ein beliebiges Element. Dann setzt den Restklassenhomomorphismus $\varphi : R \longrightarrow R/(p), r \mapsto \overline{r} = r + (p)$ zu den Ringhomomorphismus

$$\begin{array}{rccc} \varphi_X : & R[X] & \longrightarrow & (R/(p))[X] \\ & \sum_{i=0}^n a_i X^i & \mapsto & \sum_{i=0}^n \overline{a_i} X^i \end{array}$$

   fort (wende Bemerkung 2.32 mit $T = R$, $S = R/(p)[X]$ und $a = X$ an).
   Offensichtlich ist φ_X surjektiv, $\ker(\varphi_X) = (p) = pR[X] \subseteq R[X]$, und nach dem Homomorphiesatz ist

$$R[X]/(p) \cong (R/(p))[X]\,.$$

Weiterhin nehmen wir an, dass R ein **ZPE-Ring** ist.

Wir wollen jetzt die Eigenschaften des Polynomrings $R[X]$ untersuchen.

Aufgabe: In einem ZPE-Ring haben je n Elemente $\alpha_1, \ldots, \alpha_n$ einen größten gemeinsamen Teiler.

Definition 2.34 (*Inhalt, primitives Polynom*)

Sei $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in R[X] \setminus \{0\}$.

(a) Der **Inhalt** von f ist $c(f) := ggT(a_0, \ldots, a_n)$ (eindeutig bis auf Multiplikation mit Einheiten).

(b) Das Polynom f heißt **primitiv**, falls $c(f) \in R^\times$.

Ist z.B. irgendein Koeffizient von $f \in R[X] \setminus \{0\}$ gleich ± 1, so ist f primitiv.

Bemerkung 2.35 (*Gaußsches Lemma*)

Ist R ein ZPE-Ring, so gilt für $f, g \in R[X]$: f und g primitiv $\Longrightarrow fg$ ist primitiv.

Beweis: Sei φ_X wie in Anmerkung 2.33. Angenommen fg ist nicht primitiv, dann ist $c(fg) \notin R^\times$, also gibt es einen Primelement $p \in R$ mit $p \mid c(fg)$ (da R ZPE-Ring). Nach Bemerkung 2.21(b) ist $R/(p)$ ein Integritätsbereich. Insbesondere sind $\varphi_X(f), \varphi_X(g) \neq 0$, da $c(f), c(g) \in R^\times$, also ist auch $\varphi_X(f)\varphi_X(g) \neq 0$,

da $R/(p)[X]$ auch ein Integritätsbereich ist.
Aber die Polynome f, g sind primitiv, also ungleich $0 \implies fg \neq 0$ (da $R[X]$ Integritätsbereich) $\implies$ $c(fg) \neq 0$. Also gilt:

$$0 \neq \varphi_X(f)\varphi_X(g) = \varphi_X(fg) = \varphi_X(c(fg)\frac{fg}{c(fg)}) = \underbrace{\varphi_X(c(fg))}_{=0_{R/(p)}}\varphi_X(\frac{fg}{c(fg)}) = 0\,. \quad \text{Widerspruch!}$$

■

Lemma 2.36

Sei R ein ZPE-Ring mit Quotientenkörper $Q(R)$. Seien $f \in Q(R)[X] \setminus \{0\}$ und $g \in R[X] \setminus \{0\}$ primitiv mit $fg \in R[X]$. Dann ist $f \in R[X]$.

Beweis: Seien $r, s \in R \setminus \{0\}$ teilerfremd mit $\tilde{f} := \frac{r}{s}f \in R[X]$ primitiv. Dann $s\tilde{f}g = rfg \in rR[X]$, wobei $\tilde{f}g$ primitiv nach dem Gaußschen Lemma. Also ist $r \in R^\times$, da r, s tellerfremd sind. Damit gilt:

$$f = \frac{s}{r}\tilde{f} = \frac{sr^{-1}}{rr^{-1}}\tilde{f} = sr^{-1}\tilde{f} \in R[X]\,.$$

■

Satz 2.37 (*Satz von Gauß*)

Sei R ein ZPE-Ring mit Quotientenkörper $Q(R)$.

(a) Sei $f \in R[X] \setminus \{0\}$ primitiv. Dann gilt:

$$f \text{ irreduzibel in } R[X] \quad \iff \quad f \text{ irreduzibel in } Q(R)[X]$$

(b) Der Polynomring $R[X]$ ist ebenfalls ein ZPE-Ring.

Beweis:

(a) '$\Rightarrow$' Wir nehmen an, dass f irreduzibel in $R[X]$ ist. Sei $f = gh$ mit $g, h \in Q(R)[X] \implies \exists b_1, b_2 \in R$ mit $f_1 := b_1 g$, $f_2 = b_2 h \in R[X]$, und oBdA diese sind primitiv. Dann:

$$b_1 b_2 f = b_1 g b_2 h = f_1 f_2 \in R[X]$$

Da f_1, f_2 primitiv sind, ist auch $b_1 b_2 f$ primitiv nach Bemerkung 2.35, also $b_1 b_2 \in R^\times \implies f \simeq f_1 f_2$ in $R[X] \implies f_1$ oder f_2 konstant in $R[X] \implies g$ oder h konstant in $Q(R)[X] \implies$ irreduzibel in $Q(R)[X]$.

'$\Leftarrow$' f reduzibel in $R[X] \implies f$ reduzibel in $Q(R)[X]$, da $R[X]$ ein Teilring von $Q(R)[X]$ ist.

(b) Wir wissen schon, dass $R[X]$ ein Integritätsbereich ist, da R ein Integritätsbereich ist. Also ist noch zu zeigen, dass jedes $f \in R[X] \setminus \{0\}$ eine Primzerlegung besitzt. Falls $f \in R[X]^\times$ ist, so ist f schon eine Primzerlegung von f selbst $\implies$ wir nehmen an, dass f keine Einheit ist.

Es gilt $f = c(f)g$ mit $g \in R[X]$ primitiv. Weil R ein ZPE-Ring ist, hat $c(f)$ eine Primzerlegung $c(f) = ep_1 \cdots p_r$, wobei $e \in R^\times$ und $p_1, \ldots, p_r \in R$ Primelemente sind, also auch Primelemente von $R[X]$.
(p prim in $R \implies R/(p)$ Integritätsbereich $\implies R/(p)[X]$ Integritätsbereich $\implies R[X]/(p) \cong R/(p)[X]$ Integritätsbereich $\implies p$ prim in $R[X]$.)
Also reicht es noch eine Primzerlegung für g in $R[X]$ zu finden.

Wir sehen jetzt g als Element von $Q(R)[X]$, wobei $Q(R)[X]$ ein Hauptidealring ist, da $Q(R)$ ein Körper ist, also ist $Q(R)[X]$ ein ZPE-Ring nach Satz 2.25. Dann hat g eine Primzerlegung in $Q(R)[X]$, d.h.

$$g = g_1 \cdots g_n$$

mit $g_1, \dots, g_n$ Primelemente in $Q(R)[X]$. Aber für alle $1 \leq i \leq n$ ist

$$g_i = d_i \tilde{g}_i$$

für ein $d_i \in Q(R)^\times$ und $\tilde{g}_i \in R[X]$ primitiv. Dann ist

$$f = c(f)g = ep_1 \cdots p_r d_1 \cdots d_n \tilde{g}_1 \cdots \tilde{g}_n \in R[X]\,.$$

Nun ist $\tilde{g}_1 \cdots \tilde{g}_n \in R[X]$ primitiv nach dem Gaußchen Lemma, und f ist auch primitiv, also folgt daraus, dass $ep_1 \cdots p_r d_1 \cdots d_n$ der Inhalt von f ist (d.h. bis auf Einheit). Insbesondere ist $d_1 \cdots d_n \in R$. Sei also $e' q_1 \cdots q_s$ eine Primzerlegung von $d_1 \cdots d_n$ in R. Damit erhalten wir eine Primzerlegung von f in $R[X]$. ■

Folgerung 2.38

Ist R ein ZPE-Ring, so ist auch $R[X_1, \dots, X_n]$ ein ZPE-Ring.

Beweis: Nach dem Satz von Gauß ist $R[X_1]$ ein ZPE-Ring $\implies$ eine Induktion nach n liefert, dass der Ring $R[X_1, \dots, X_n]$ auch ein ZPE-Ring ist. ■

Anmerkung 2.39

In manche Bücher wird ein ZPE-Ring auch definiert, als ein Integritätsbereich, in dem jedes irreduzibles Element ein Primelement ist. Der Beweis des Satzes von Gauß zeigt warum.

Satz 2.40 (*Irreduzibilitätskriterium von Eisenstein*)

Sei R ein ZPE-Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ mit $n \geq 1$ und $a_n = 1$. Existiert ein Primelement $p \in R$ mit $p \mid a_i$ für alle $0 \leq i \leq n-1$ und $p^2 \nmid a_0$, so ist f irreduzibel in $R[X]$.

Beweis: Annahme, wir hätten $f = gh$ mit $g = \sum_{i=0}^{r} b_i X^i$, $h = \sum_{i=0}^{s} c_i X^i \in R[X]$, $r, s \geq 1$, also $n = r + s$. Da $p \mid a_0 = b_0 c_0$ gilt oBdA $p \mid b_0$ und $p \nmid c_0$.
Behauptung: $p \mid b_i$ für alle $0 \leq i \leq r$. Induktion nach i: $i = 0$ ✓ und sei die Behauptung schon gezeigt für $i-1$, also $p \mid b_k$ für alle $0 \leq k \leq i-1$. Dann:

$$0 \equiv a_i = \sum_{k=0}^{i} b_k c_{i-k} \equiv b_i c_0 \pmod{p}\,,$$

also ist b_i durch p teilbar.
Insbesondere $p \mid b_r \Rightarrow p \mid b_r c_s = a_n = 1$. Widerspruch. ■

Satz 2.41 (*Reduktions-Kriterium*)

Sei R ein ZPE-Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus \{0\}$ primitiv mit $\deg(f) \geq 1$ und Leitkoeffizient a_n. Sei $p \in R$ ein Primelement mit $p \nmid a_n$. Ist $\varphi_X(f)$ irreduzibel in $R/(p)[X]$, so ist auch f irreduzibel in $R[X]$.

Beweis: Wegen $p \nmid a_n$ ist $\varphi_X(f) \neq 0$ in $R/(p)[X]$ und $\deg \varphi_X(f) = n$. Annahme, wir hätten $f = gh$ mit $g, h \in R[X]$. Da R ein ZPE-Ring ist, gilt $n = \deg(g) + \deg(h)$. Weil a_n gleich dem Produkt der Leitkoeffizienten von g und h ist, sind diese auch nicht durch p teilbar, also sind $\varphi_X(g), \varphi_X(h) \neq 0$ und $\deg(g) = \deg(\varphi_X(g))$, $\deg(h) = \deg(\varphi_X(h))$. Nun ist $\varphi_X(f) = \varphi_X(gh) = \varphi_X(g)\varphi_X(h)$. Da $\varphi_X(f)$ nach Vorraussetzung irreduzibel ist, folgt $\deg(\varphi_X(g)) = 0$ oder $\deg(\varphi_X(h)) = 0$, also $\deg(g) = 0$ oder $\deg(h) = 0$. Da f primitiv, muss also $g \in R^\times$ oder $h \in R^\times$ sein. Also ist f irreduzibel. ■

Aufgabe 16 (*Kriterium der ganzen Nullstellen; Aufgabe 16 auf Blatt 4 mit $s = 1$*)

Sei R ein ZPE-Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus \{0\}$ mit Leitkoeffizient $a_n = 1$. Falls $b \in Q(R)$ eine Nullstelle von f ist, dann $b \in R$ und $b \mid a_0$.

Beispiel 17

(a) $f = X^3 - 5X + 3 \in \mathbb{Z}[X]$ ist irreduzibel nach dem Reduktions-Kriterium mit $p = 2$, da $X^3 + X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$ irreduzibel ist, weil es in $\mathbb{Z}/2\mathbb{Z}$ einfach nachzurechnen ist, dass $\overline{0}^3 + \overline{0} + \overline{1} = \overline{1} \neq \overline{0}$ und $\overline{1}^3 + \overline{1} + \overline{1} = \overline{1} \neq \overline{0}$, und der Grad von $\varphi_X(f)$ ist 3.

(b) Das Polynom $X^{25} + 6X^{16} + 15X^6 + 3$ ist irreduzibel nach Eisensteins Irreduzibilitätskriterium mit $p = 3$.

(c) Sei $f = X^{100} + X^{56} - 24 \in \mathbb{Q}[X]$. Die möglichen Nullstellen von f sind ± 1, ± 2, ± 3, ± 4, ± 6, ± 8, ± 12, ± 24 nach dem Kriterium der ganzen Nullstellen.

TEIL III: KÖRPER

5 Endliche Körpererweiterungen

5.1 Körpererweiterungen

Definition 3.1 (*Teilkörper, Körpererweiterung*)

Sei $(L, +, \cdot)$ ein Körper. Dann

(a) heißt $K \subseteq L$ **Teilkörper von** L, falls $(K, +|_K, \cdot|_K)$ ein Körper ist; und

(b) in diesem Fall nennen wir L **Erweiterungskörper von** K, und $L \supseteq K$ eine **Körpererweiterung** und schreiben dafür auch L/K.

Anmerkung 3.2

Ist L/K eine Körpererweiterung, dann ist L ein K-Vektorraum bezüglich der Addition und der Multiplikation in L, da die Vektorraumaxiome direkt aus den Körperaxiomen von L folgen.

Definition 3.3 (*Körpergrad*)

Sei L/K eine Körpererweiterung. Dann heißt $[L : K] := \dim_K(L)$ der **Körpergrad**, oder einfach der **Grad**, von L über K. Ist $[L : K] < \infty$, dann heißt L/K eine **endliche** Körpererweiterung.

Beispiel 18

(a) $\mathbb{C} \supseteq \mathbb{R}$ ist eine Körpererweiterung mit $[\mathbb{C} : \mathbb{R}] = 2$; eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist gegeben durch $\{1, i\}$.

(b) $\mathbb{R} \supseteq \mathbb{Q}$ ist eine Körpererweiterung. [Aufgabe 20, Blatt 5]: $[\mathbb{R} : \mathbb{Q}] = \infty$.

(c) Sei K ein beliebiger Körper. Nach Folgerung 2.31 ist:

- K ein Erweiterungskörper von $\mathbb{Q}$, falls $\mathrm{char}(K) = 0$ ist;
- K ein Erweiterungskörper von $\mathbb{F}_p$, falls $\mathrm{char}(K) = p$ eine Primzahl ist.

Wir nennen $\mathbb{Q}$ bzw. $\mathbb{F}_p$ **Primkörper** von K.

Definition 3.4 (*transzendentes/algebraisches Element, algebraische Erweiterung*)

Sei $L \supseteq K$ eine Körpererweiterung und $\alpha \in L$. Betrachte den Einsetzungshomomorphismus $\varphi_\alpha : K[X] \longrightarrow L, f \mapsto f(\alpha)$. Sei $K[\alpha] := \{f(\alpha) \mid f \in K[X]\}$ das Bild von φ_α; dies ist also ein Teilring von L. Da $K[X]$ ein HIR ist, gibt es zwei Fälle für den Kern von φ_α:

(1) Ist $\ker(\varphi_\alpha) = \{0\}$, so heißt α **transzendent** über K. (In diesem Fall ist $\varphi_\alpha : K[X] \longrightarrow K[\alpha]$, $f \mapsto f(\alpha)$ ein Ringisomorphismus)

(2) Ist $\ker(\varphi_\alpha) \neq \{0\}$, so heißt α **algebraisch** über K. In diesem Fall gibt es ein Polynom $0 \neq \mu_\alpha \in K[X]$ mit $\ker(\varphi_\alpha) = (\mu_\alpha)$. OBdA können wir außerdem verlangen, dass μ_α normiert ist, so dass μ_α eindeutig bestimmt ist, und μ_α heißt das **Minimalpolynom** von α.

Sind alle Elemente $\alpha \in L$ algebraisch über K, so heißt $L \supseteq K$ eine **algebraische Erweiterung**.

Anmerkung 3.5

Im Fall (2) der Definition gelten:

(a) α ist algebraisch $\iff \exists\, g \in K[X] \setminus \{0\}$ mit $g(\alpha) = 0$.

(b) $g \in K[X] \setminus \{0\}$ mit $g(\alpha) = 0 \implies \mu_\alpha \mid g$, da $g \in \ker(\varphi_\alpha) = (\mu_\alpha)$.

(c) $K[X]/(\mu_\alpha) \cong K[\alpha] \subseteq L$ nach dem Homomorphiesatz (für Ringe), also ist $K[X]/(\mu_\alpha)$ ein Integritätsbereich. Nach Satz 2.9(a) ist μ_α prim und nach Bemerkung 2.21(a) ist μ_α irreduzibel. Also ist (μ_α) ein maximales Ideal von $K[X]$ nach Bemerkung 2.21(c), und damit ist $K[X]/(\mu_\alpha) \cong K[\alpha]$ ein Körper nach Satz 2.9(b).

(d) $\deg \mu_\alpha = [K[\alpha] : K] =: n$, und $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ ist eine K-Basis von $K[\alpha]$. Siehe [Aufgabe 18, Blatt 4]. (Hinweis: Zeigen Sie, dass $\{\overline{1}, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1}\}$ eine K-Basis von $K[X]/(\mu_\alpha)$ ist.)

Beispiel 19

(a) Sei L/K eine Körpererweiterung, und $\alpha \in K$. Dann ist α algebraisch über K da α eine Nullstelle von $X - \alpha \in K[X]$.

(b) In $\mathbb{C} \supseteq \mathbb{R}$ sei $\alpha := i = \sqrt{-1} \in \mathbb{C}$. Dann ist $f = X^2 + 1$ irreduzibel in $\mathbb{R}[X]$ und $f(i) = 0$, also ist i algebraisch über $\mathbb{R}$ und $\mu_i = f$.

Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch: Im Allgemeinen ist jedes Element $z = a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$ algebraisch über $\mathbb{R}$, da z eine Nullstelle von $f = (X - a)^2 + b^2 \in \mathbb{R}[X]$ ist.

(c) In $\mathbb{R} \supseteq \mathbb{Q}$ sei $\alpha = \sqrt{2} \in \mathbb{R}$. Dann ist α eine Nullstelle von $f = X^2 - 2 \in \mathbb{Q}[X]$ irreduzibel, also ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$ und $\mu_\alpha = f$.

Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch: $\mathbb{R}$ enthält transzendente Elemente über $\mathbb{Q}$. (Beispiele (ohne Beweis): π, e, $\sqrt{2}^\pi$, ...).

Bemerkung 3.6

Jede endliche Körpererweiterung ist algebraisch.

Beweis: Seien L/K eine endliche Körpererweiterung von Grad $n \in \mathbb{N}$, und $\alpha \in L$. Dann sind $1, \alpha, \ldots, \alpha^n$

linear abhängig über K, also gibt es $a_0, a_1, \ldots, a_n \in K$ (die nicht alle gleich Null sind) mit

$$a_0 + a_1\alpha_1 + \ldots + a_n\alpha^n = 0\,.$$

Damit ist $0 \neq f := a_0 \cdot 1 + a_1 X + \ldots + a_n X^n \in K[X]$ mit $f(\alpha) = 0$, also ist $\ker(\varphi_\alpha) \neq \{0\}$. ■

Satz 3.7 (*Gradmultiplikationssatz*)

Seien L/M und M/K Körpererweiterungen. Dann gilt

$$[L : K] = [L : M] \cdot [M : K]\,.$$

Beweis: · Falls $[L : M] = \infty$ oder $[M : K] = \infty$ ist, so ist $[L : K] = \infty = [L : M] \cdot [M : K]$.

· Seien nun $[M : K] =: n \in \mathbb{N}$, $[L : M] =: m \in \mathbb{N}$, $\{x_1, \ldots, x_n\}$ eine K-Basis von M und $\{y_1, \ldots, y_m\}$ eine M-Basis von L.

Behauptung: $\mathcal{B} := \{x_i y_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ ist eine K-Basis von L.

Beweis: Sei $z \in L$ beliebig. Dann ist $z = \sum_{j=1}^{m} \mu_j y_j$ mit $\{\mu_j \mid 1 \leq j \leq m\} \subset M$. Außerdem $\forall\ 1 \leq j \leq m$ ist $\mu_j = \sum_{i=1}^{n} \lambda_{ij} x_i$ mit $\{\lambda_{ij} \mid 1 \leq i \leq n\} \subset K$. Also erhalten wir eine Summe

$$z = \sum_{j=1}^{m} \sum_{i=1}^{n} \lambda_{ij} x_i y_j\,,$$

so dass die Menge $\mathcal{B}$ ein Erzeugendensystem von L über K ist. Seien nun $\alpha_{ij} \in K$ ($1 \leq i \leq n$, $1 \leq j \leq m$) mit $0 = \sum_{i,j} \alpha_{ij} x_i y_j$. Dann ist

$$0 = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} x_i \right) y_j = \sum_{j=1}^{m} c_j y_j\,, \quad \text{wobei } c_j := \sum_{i=1}^{n} \alpha_{ij} x_i \in M\,.$$

Da $\{y_j \mid 1 \leq j \leq m\}$ linear unabhängig über M ist, folgt also $c_j = 0$ für alle $1 \leq j \leq m$. Weil $\{x_i \mid 1 \leq i \leq n\}$ linear unabhängig über K ist, folgt dann auch $\alpha_{ij} = 0$ für alle $1 \leq i \leq n$, $1 \leq j \leq m$. Also ist $\mathcal{B}$ linear unabhängig über K, und damit eine K-Basis von L. #

Es folgt jetzt, dass $[L : K] = \dim_K(L) = m \cdot n = \dim_M(L) \cdot \dim_K(M) = [L : M] \cdot [M : K]$. ■

Definition 3.8 (*erzeugte Teilkörper*)

Sei L/K eine Körpererweiterung. Für eine Teilmenge $S \subseteq L$ bezeichnen wir mit $K(S)$ **den von K und S erzeugten Teilkörper von L**, d.h. der kleinste Teilkörper von L, der K und S enthält. Ist $S = \{\alpha_1, \cdots, \alpha_r\}$, so schreiben wir $K(\alpha_1, \ldots, \alpha_r)$ anstelle von $K(S)$.
(Für $S = \{\alpha\}$ vergleiche mit Aufgabe 18(ii).)

Anmerkung 3.9

Sei L/K eine Körpererweiterung.

(a) $\alpha \in L$ ist algebraisch über $K \iff K(\alpha) = K[\alpha]$. Siehe Aufgabe 19.

(b) Falls $\alpha_1, \ldots, \alpha_r \in L$ algebraisch über K sind, dann erhalten wir sukzessive:

$$K(\alpha_1) = K[\alpha_1], \quad K(\alpha_1, \alpha_2) = (K(\alpha_1))[\alpha_2], \quad \ldots \quad , K(\alpha_1, \ldots, \alpha_r) = (K(\alpha_1, \ldots, \alpha_{r-1}))[\alpha_r]$$

Wir nennen dies die **Adjunktion** der Elemente $\alpha_1, \ldots, \alpha_r$ an K.

Mit dem Gradmultiplikationssatz folgt:

$$[K(\alpha_1, \ldots, \alpha_r) : K] < \infty,$$

damit ist $K(\alpha_1, \ldots, \alpha_r) \supseteq K$ algebraisch (siehe Bemerkung 3.6).

Folgerung 3.10

Seien L/M und M/K jeweils algebraische Körpererweiterungen. Dann ist auch L/K algebraisch.

Beweis: Sei $\alpha \in L$ und $\mu_\alpha = \beta_m X^m + \ldots + \beta_1 X + \beta_0 \in M[X]$ das Minimalpolynom von α über M. Jedes β_i $(1 \leq i \leq m)$ ist algebraisch über K. Nach Anmerkung 3.9(b) ist $K_0 := K(\beta_0, \ldots, \beta_m)$ ein Teilkörper von L mit $[K_0 : K] < \infty$. Außerdem ist α algebraisch über K_0 nach Definition von K_0, also $[K_0(\alpha) : K_0] < \infty$. Mit dem Gradmultiplikationssatz folgt $[K_0(\alpha) : K] = [K_0(\alpha) : K_0] \cdot [K_0 : K] < \infty$, also ist α algebraisch über K nach Bemerkung 3.6. Dies gilt für jedes $\alpha \in L$, also ist L/K algebraisch. ■

Folgerung 3.11

Sei L/K eine Körpererweiterung und M die Menge aller $\alpha \in L$, die über K algebraisch sind. Dann ist M ein Teilkörper von L.

Beweis: Seien $0 \neq \alpha, \beta \in M$. Sei $\gamma \in \{\alpha \pm \beta, \alpha \cdot \beta^{\pm 1}\}$. Dann gilt $\gamma \in K(\alpha, \beta)$. Nach Anmerkung 3.9(b) ist damit γ algebraisch über K. ■

5.2 Körper-Automorphismen

Bemerkung 3.12

(a) Ein Ring-Homomorphismus $\sigma : K_1 \longrightarrow K_2$ zwischen zwei Körpern K_1, K_2 ist automatisch injektiv.

(b) Falls L/K eine Körpererweiterung ist, dann ist jeder (Ring-)Automorphismus $\sigma \in \mathrm{Aut}(L)$ mit $\sigma|_K = \mathrm{Id}_K$ eine K-lineare Abbildung.

Beweis: (a) Der Kern von σ ist ein Ideal von K_1. Aber die einzigen Ideale von K_1 sind $\{0\}$ und K_1, weil K_1 ein Körper ist. Da $\sigma(1_{K_1}) = 1_{K_2} \neq 0_{K_2}$ ist $\ker(\sigma) = K_1$ unmöglich und muss $\ker(\sigma) = \{0\}$ sein, also ist σ injektiv.

(b) Für alle $x_1, x_2 \in K$, $y_1, y_2 \in L$ und $\sigma \in \mathrm{Aut}(L)$ gilt

$$\sigma(x_1 y_1 + x_2 y_2) = \sigma(x_1)\sigma(y_1) + \sigma(x_2)\sigma(y_2) = x_1 \sigma(y_1) + x_2 \sigma(y_2)\,.$$

■

Anmerkung 3.13

Seien K_1, K_2 Körper und $\sigma : K_1 \longrightarrow K_2$ ein Isomorphismus (d.h. ein Ring-Isomorphismus). Dann setzt σ zu dem Ringhomomorphismus (eigentlich Ringisomorphismus)

$$\begin{array}{rccc} \widetilde{\sigma}: & K_1[X] & \longrightarrow & K_2[X] \\ & \sum_{i=0}^n a_i X^i & \mapsto & \sum_{i=0}^n \sigma(a_i) X^i \end{array}$$

fort (wende Bemerkung 2.32 mit $T = K_1$, $S = K_2[X]$ und $a = X$ an, so dass $\widetilde{\sigma} = \sigma_X$).

Es gilt also insbesondere:

(a) $f = \prod_{i=1}^{n}(X - \alpha_i)$ mit $\alpha_i \in K_1 \quad \Longrightarrow \quad \widetilde{\sigma}(f) = \prod_{i=1}^{n}(X - \sigma(\alpha_i))$,

(b) $\sigma(f(\alpha)) = \widetilde{\sigma}(f)(\sigma(\alpha))$ für alle $f \in K_1[X]$ und alle $\alpha \in K_1$, und

(c) $f \in K_1[X]$ ist irreduzibel $\quad \Longleftrightarrow \quad \widetilde{\sigma}(f) \in K_2[X]$ ist irreduzibel.

Definition 3.14 (*Automorphismengruppe einer Körpererweiterung*)

Sei L/K eine Körpererweiterung. Dann heißt

$$\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{Id}_K\}$$

zusammen mit der Hintereinanderauführung als Verknüpfung die **Automorphismengruppe** von L/K.

Klar: die Automorphismengruppe $G := \mathrm{Aut}(L/K)$ einer Körpererweiterung L/K ist tatsächlich eine Gruppe. Außerdem operiert diese Gruppe auf L durch

$$\begin{array}{rccc} \cdot : & G \times L & \longrightarrow & L \\ & (\sigma, y) & \mapsto & \sigma \cdot y := \sigma(y)\,. \end{array}$$

(Überprüfen Sie diese zwei Aussagen!)
Wir können also von Stabilisatoren, Bahnen, etc. sprechen.

Lemma 3.15

Ist $[L : K] < \infty$, so ist auch $|\mathrm{Aut}(L/K)| < \infty$.

Beweis: Sei $N := [L : K]$ und $\{y_1, \ldots, y_n\}$ eine K-Basis von L. Nun ist jedes $\sigma \in \mathrm{Aut}(L/K)$ K-linear nach Bemerkung 3.12(b), also eindeutig bestimmt durch die Werte $\sigma(y_1), \ldots, \sigma(y_n)$. Für alle $1 \leq i \leq n$ sei $f_i \in K[X]$ das Minimalpolynom von y_i. Setze $f := f_1 \cdot \cdots \cdot f_n \in K[X] \subseteq L[X]$. Insbesondere ist $f(y_i) = 0$ für alle $1 \leq i \leq n$. Dann für alle $\sigma \in \mathrm{Aut}(L/K)$ und für alle $1 \leq i \leq n$ gilt

$$f(\sigma(y_i)) = \widetilde{\sigma}(f)(\sigma(y_i)) = \sigma(f(y_i)) = 0$$

nach Anmerkung 3.13. Also gibt es für jedes $\sigma(y_i)$ höchstens $d := \deg(f)$ Möglichkeiten, insgesamt ist damit $|\mathrm{Aut}(L/K)| \leq d^n < \infty$. ∎

Definition 3.16

Zwei Körpererweiterungen L_1/K und L_2/K heißen K-isomorph, falls es einen (Ring-)Isomorphismus $\sigma : L_1 \longrightarrow L_2$ mit $\sigma|_K = \mathrm{Id}_K$ gibt.

5.3 Stammkörper und Zerfällungskörper

Wir suchen jetzt nach Körpern, die die Nullstellen eines gegebenen Polynoms enthalten.

Definition 3.17 (*Zerfällungskörper*)

Sei K ein Körper und $f \in K[X] \setminus \{0\}$ mit $\deg(f) \geq 1$. Ein Körper $L \supseteq K$ heißt **Zerfällungskörper** von f falls

(i) $\exists\ \alpha_1, \ldots, \alpha_n \in L$ mit $f = c \cdot \prod_{i=1}^{n}(X - \alpha_i)$ für ein $c \in K$, und

(ii) $L = K(\alpha_1, \ldots, \alpha_n)$ ist.

Beachte, dass jedes α_i $(1 \leq i \leq n)$ algebraisch über K ist. Außerdem ist nach Anmerkung 3.9 $L = K(\alpha_1, \ldots, \alpha_n) \supseteq K$ eine algebraische Erweiterung. Außerdem ist Bedigung (i) äquivalent zu sagen, dass f **in Linearfaktoren** über L **zerfällt**.

Beispiel 20

$L = \mathbb{Q}(\sqrt{2})$ ist ein Zerfällungskörper von $f := X^2 - 2 \in \mathbb{Q}[X]$, denn

$$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}) \in L[X].$$

Hingegen ist $\mathbb{C}$ kein Zerfällungskörper von f, da $\mathbb{C}$ die Minimalitätsbedingung (ii) in obiger Definition nicht erfüllt.

Wir möchten zeigen, dass ein Zerfällungskörper immer existiert. Zunächst suchen wir nach einem Körper, in dem ein vorgegebenes Polynom eine Nullstelle besitzt.

Definition 3.18 (*Stammkörper*)

Sei $f \in K[X]$ ein irreduzibles Polynom über einem Körper K. Ein Erweiterungskörper L von K heißt **Stammkörper** von f über K, wenn es ein Element $\alpha \in L$ gibt mit $f(\alpha) = 0$ und $L = K(\alpha)$.

Satz 3.19 (*Existenz von Stammkörpern*)

Seien K ein Körper und $f \in K[X]$ ein irreduzibles Polynom mit $\deg(f) \geq 1$. Dann ist $K_f := K[X]/(f)$ ein Stammkörper von f über K, wobei $\alpha := \overline{X}$ ein Element mit $f(\alpha) = 0$ und $K_f = K(\alpha)$.

Beweis: Weil $K[X]$ ein HIR ist, ist (f) ein maximales Ideal von $K[X]$ nach Bemerkung 2.21(c), da f irreduzibel ist. Also ist $K_f := K[X]/(f)$ ein Körper nach Satz 2.9(b).
Sei nun $\alpha := \overline{X} = X + (f) \in K_f$, so dass $f(\alpha) = f(\overline{X}) = \overline{f(X)} = \overline{f} = 0$ in K_f. Damit ist $f = \mu_\alpha$ bis auf skalare Vielfachen. Also ist α algebraisch über K und $K_f = K[X]/(\mu_\alpha) = K[\alpha] = K(\alpha)$. ■

Lemma 3.20

Seien K_1, K_2 zwei Körper und $\sigma : K_1 \longrightarrow K_2$ ein Isomorphismus. Ferner seien $f_1 \in K_1[X]$ irreduzibel, $L_1 := K_1(\alpha_1)$ ein Stammkörper von f_1 und $L_2 := K_2(\alpha_2)$ ein Stammkörper von $f_2 = \widetilde{\sigma}(f_1) \in K_2[X]$. Dann gibt es genau einen Isomorphismus $\hat{\sigma} : K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$ mit $\hat{\sigma}|_{K_1} = \sigma$ und $\hat{\sigma}(\alpha_1) = \alpha_2$.

Beweis: Betrachte den Isomorphismus $\widetilde{\sigma} : K_1[X] \longrightarrow K_2[X]$.
(Erinerung: Nach Anmerkung 3.13 ist $f_2 = \widetilde{\sigma}(f_1)$ irreduzibel in $K_2[X]$.)
Für $1 \leq i \leq 2$ schreibe $\pi_i : K_i[X] \longrightarrow K_{f_i} = K_i[X]/(f_i) = K(\alpha_1)$ (siehe Satz 3.19.) für den Restklassen-Homomorphismus.
Klar: nach Konstruktion ist $\ker(\pi_2 \circ \widetilde{\sigma}) = \widetilde{\sigma}^{-1}(\ker(\pi_2)) = \widetilde{\sigma}^{-1}((f_2)) = (\widetilde{\sigma}^{-1}(f_2)) = (f_1)$. Also gibt es nach dem Homomorphiesatz einen eindeutigen Isomorphismus $\hat{\sigma} : K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$, so dass das folgende

Diagramm

$$\begin{array}{ccc} K_1[X] & \xrightarrow{\widetilde{\sigma}} & K_2[X] \\ {\scriptstyle \pi_1}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_2} \\ K(\alpha_1) & \underset{\exists!\,\hat{\sigma}}{\dashrightarrow} & K(\alpha_2) \end{array}$$

kommutativ ist, d.h. $\hat{\sigma} \circ \pi_1 = \pi_2 \circ \widetilde{\sigma}$. Konkret für $g(\alpha_1) = \sum_{i=0}^{n-1} a_i \alpha_1^i \in K(\alpha_1)$ (wobei $n = \deg(f_1)$ and $\{a_i\}_{i=0}^{n-1} \subseteq K_1$) ist

$$\begin{aligned} \hat{\sigma}(g(\alpha_1)) &= \widetilde{\sigma}(g)(\alpha_2) \\ &= \sum_{i=0}^{n-1} \sigma(a_i)\alpha_2^i \ . \end{aligned}$$

Insbesondere ist $\hat{\sigma}(\alpha_1) = \alpha_2$ und $\hat{\sigma}|_{K_1} = \sigma$. ■

Folgerung 3.21 (*Eindeutigkeit von Stammkörpern*)

Seien K ein Körper und $f \in [X]$ ein nicht-konstantes irreduzibles Polynom. Dann ist ein Stammkörper von f über K eindeutig bestimmt bis auf K-Isomorphie.

Beweis: Seien $L_1 := K(\alpha_1)$ ein Stammkörper von $f_1 := f$ über K mit $f(\alpha_1) = 0$ und $L_2 := K(\alpha_2)$ ein Stammkörper von $f_2 := f$ über K mit $f(\alpha_2) = 0$. Wende Lemma 3.20 an mit $\sigma = \mathrm{Id}_K : K \longrightarrow K$. Dies liefert: es gibt genau einen Isomorphismus $\hat{\sigma} : L_1 \longrightarrow L_2$ mit $\hat{\sigma}|_K = \mathrm{Id}_K$ und $\hat{\sigma}(\alpha_1) = \alpha_2$. Also ist σ_1 ein K-Isomorphismus. ■

Nun können wir die Existenz und Eindeutigkeit von Zerfällungskörpern beweisen:

Satz 3.22 (*Existenz von Zerfällungskörpern*)

Seien K ein Körper und $0 \neq f \in K[X]$ ein nicht-konstantes Polynom. Dann existiert ein Zerfällungskörper L von f und es gilt $[L : K] \leq n!$, wobei $n := \deg(f)$ ist.

Beweis: Induktion nach n. Falls $n = 1$ setzen wir einfach $L := K$.
Sei nun $n \geq 2$ und $f_1 \in K[X]$ irreduzibel mit $f_1 \mid f$. Nach Satz 3.19 ist der Stammkörper $K_1 := K_{f_1}$ von f_1 ein Erweiterungskörper von K mit $[K_1 : K] = \deg(f_1) \leq n$, so dass f_1 (und damit auch f) zumindest eine Nullstelle $\alpha_1 \in K_1$ besitzt; und es gilt $K_1 = K(\alpha_1)$.
Schreibe jetzt $f = (X - \alpha_1)g$ mit $g \in K_1[X]$, also ist $\deg(g) = n - 1 \geq 1$. Nach Induktion existiert ein Zerfällungskörper $L \supset K_1$ von g mit $[L : K_1] \leq (n-1)!$; sei also $L = K_1(\alpha_2, \cdots, \alpha_n)$, wobei $g = c \cdot \prod_{i=2}^{n}(X - \alpha_i)$ für ein $c \in K$. Dann ist

$$L = K(\alpha_1, \cdots, \alpha_n)$$

ein Zerfällungskörper von f. Mit dem Gradmultiplikationssatz folgt:

$$[L : K] = [L : K_1] \cdot [K_1 : K] \leq (n-1)! \cdot n = n!$$

■

Satz 3.23 (*Fortsetzungssatz für Körper-Isomorphismen*)

Seien K_1, K_2 zwei Körper und $\sigma : K_1 \longrightarrow K_2$ ein Isomorphismus. Sei $f_1 \in K_1[X]$ nicht-konstant und $f_2 := \widetilde{\sigma}(f_1) \in K_2[X]$. Sei $L_1 \supseteq K_1$ ein Zerfällungskörper von f_1 und $L_2 \supseteq K_2$ ein Zerfällungskörper von f_2. Dann existiert ein Isomorphismus $\Sigma : L_1 \longrightarrow L_2$ mit $\Sigma|_{K_1} = \sigma$. Außerdem bildet jeder solche Isomorphismus die Nullstellen von f_1 auf die Nullstellen von f_2 ab.

Beweis: Induktion nach $n := [L_1 : K_1]$. Ist $n = 1$, so ist $L_1 = K_1$. Setze $\Sigma = \sigma$. ✓
Sei nun $n \geq 2$, $g_1 \in K_1[X]$ irreduzibel mit $g_1 \mid f_1$ und $\alpha_1 \in L_1$ eine Nullstelle von g_1. Also ist $g_2 := \widetilde{\sigma}(g_1) \in K_2[X]$ ein irreduzibler Faktor von $f_2 = \widetilde{\sigma}(f_1)$ in $K_2[X]$, so dass es $\alpha_2 \in L_2$ gibt mit $g_2(\alpha_2) = 0$.
Nach Lemma 3.20 gibt es einen eindeutigen Isomorphismus $\hat{\sigma} := K(\alpha_1) \longrightarrow K(\alpha_2)$ mit $\hat{\sigma}(\alpha_1) = \alpha_2$ und $\hat{\sigma}|_{K_1} = \sigma$. Es gilt $f_1 = (X - \alpha_1)h_1$ für ein $h_1 \in K_1(\alpha_1)[X]$ mit $\deg(h_1) = n - 1 < n$ und $f_2 = (X - \alpha_2)\widetilde{\hat{\sigma}}(h_1)$.
Nach Induktion gibt es einen Isomorphismus $\Sigma : L_1 \longrightarrow L_2$ mit $\Sigma|_{K_1(\alpha_1)} = \hat{\sigma}$, also $\Sigma|_{K_1} = \hat{\sigma}|_{K_1} = \sigma$.
Außerdem bildet Σ die Nullstellen von h_1 auf die Nullstellen von $\widetilde{\hat{\sigma}}(h_1)$ ab, also bildet Σ die Nullstellen von f_1 auf auf die Nullstellen von f_2 ab. ■

Folgerung 3.24 (*Eindeutigkeit von Zerfällungskörpern*)

Sei K ein Körper. Je zwei Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[X]$ sind K-isomorph.

Beweis: Seien $L_1 \supseteq K$ und $L_2 \supseteq K$ zwei Zerfällungskörper von f. Wende einfach Satz 3.23 an mit $\sigma = \mathrm{Id}_K$. ■

Aufgabe 21 (*Aufgabe 21, Blatt 6*)

Seien L/K eine Körpererweiterung und $f \in K[X]$ mit $\deg(f) \geq 1$. Betrachte die gewöhnliche Ableitung $D : K[X] \longrightarrow K[X], f \mapsto D(f) = f'$ (auch **Derivation** gennant). Dann gelten:

(i) Haben f und $D(f)$ keinen gemeinsamen nicht-konstanten Teiler in $K[X]$, so hat f keine mehrfachen Nullstellen in L.

(ii) Ist f irreduzibel und $D(f) \neq 0$, so hat f keine mehrfachen Nullstellen in L.

Aufgabe 29 (*Aufgabe 29*)

Mit der Notation von Satz 3.23: Hat f_1 in L_1 keine mehrfachen Nullstellen, so gibt es mindestens $[L : K]$ Isomorphismen $\Sigma : L_1 \longrightarrow L_2$ mit $\Sigma|_{K_1} = \sigma$.

Lösungsvorschlag: Mit dem Gradmultiplikationssatz sieht man, dass es mindestens $[L : K]$ Möglichkeiten für die Konstruktion von Σ im Beweis von Satz 3.23 gibt.

5.4 Die endlichen Körper

Bemerkung 3.25

Ist K ein endlicher Körper, so gibt es eine Primzahl $p \in \mathbb{P}$ und ein $n \in \mathbb{N}$ mit $|K| = p^n$.

Beweis: $|K| < \infty \Longrightarrow$ Primkörper von K ist $\mathbb{F}_p$ für eine Primzahl $p \in \mathbb{P}$ nach Beispiel 18(c) (da $|\mathbb{Q}| = \infty$).
Also ist K ein $\mathbb{F}_p$-Vektorraum endlicher Dimension, etwa $n \in \mathbb{N} \Longrightarrow |K| = |\mathbb{F}_p|^n = p^n$. ■

Anmerkung 3.26 (*Frobenius-Homomorphismus*)

Für ein Körper K der Charakteristik $p > 0$ ist $F : K \longrightarrow K, x \mapsto x^p$ ein Endomorphismus von K. Dieser heißt **Frobenius-Homomorphismus**.
F ist tatsächlich ein Ring-Homomorphismus, denn $\forall\, x, y \in K$:
· $F(1_K) = 1_K$ ✓
· $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ ✓
· $F(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + 0 + \ldots + 0 + y^p$, da $p \mid \binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i}$

$\forall\ 0 \leq i < p$. ✓

Satz 3.27

Seien p eine Primzahl und $n \in \mathbb{N}$ eine natürliche Zahl. Dann existiert bis auf Isomorphie genau ein endlicher Körper $\mathbb{F}_q$ mit $q = p^n$ Elementen, nämlich der Zerfällungskörper des Polynoms $X^q - X \in \mathbb{F}_p[X]$.

Beweis:

· **Existenz:** Sei L ein Zerfällungskörper von $f := X^q - X \in \mathbb{F}_p[X]$. Dann ist $f = \prod_{i=1}^{q}(X - \alpha_i) \in L[X]$, also $\alpha_i^q = \alpha_i$ $(1 \leq i \leq q)$.
Setze $K := \{\alpha_i \mid 1 \leq i \leq q\} \subset L$.
Behauptung 1: K ist ein Körper.
Ist $\alpha_j \neq 0$, so ist für alle $1 \leq i \leq q$ $(\alpha_i \cdot \alpha_j^{\pm 1})^q = \alpha_i^q \cdot \alpha_j^{\pm q} = \alpha_i \cdot \alpha_j^{\pm 1} \implies \alpha_i \cdot \alpha_j^{\pm 1} \in K$, und
$(\alpha_i \pm \alpha_j)^q = (F(\alpha_i \pm \alpha_j))^{p^{n-1}} = (F(\alpha_i) \pm F(\alpha_j))^{p^{n-1}} = (\alpha_i^p \pm \alpha_j^p)^{p^{n-1}} = \cdots = \alpha_i^q \pm \alpha_j^q = \alpha_i \pm \alpha_j \implies$
$\alpha_i \pm \alpha_j \in K$.
$\implies K$ ist ein Teilkörper von L, also insbesondere ein Körper. #
Aber $L = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q) \subseteq K$, da $\mathbb{F}_p \subseteq K$ und $\alpha_1, \ldots, \alpha_q \in K$, also ist $K = L$.
Behauptung 2: Die Elemente $\alpha_1, \ldots, \alpha_q$ sind alle verschieden.
Wegen $D(f) = -1 \neq 0$ hat f keine mehrfachen Nullstellen. (Siehe Aufgabe 21, Blatt 6). Also enthält K genau p^n Elemente. #

· **Eindeutigkeit:** Sei M ein weiterer Körper mit $|M| = q$. Dann ist $\mathbb{F}_p$ der Primkörper von M. Nun ist $|M^\times| = q-1$, also gilt nach dem Satz von Lagrange $y^{q-1} = 1$, und damit $y^q = y$, für alle $y \in M^\times$. Also ist jedes $y \in M$ eine Nullstelle von $f = X^q - X \in \mathbb{F}_p[X]$. Da f höchstens q Nullstellen hat, ist M ein Zerfällungskörper von $f \implies M \cong L$ nach Folgerung 3.24.

Setze also $\mathbb{F}_q := L$. ■

Aufgabe 23 (*Aufgabe 23, Blatt 6*)

Mit der Notation von Satz 3.27 ist $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) = \langle F \rangle$ zyklisch der Ordnung n.

6 Galoistheorie

In diesem Abschnitt ist L/K stets eine Körpererweiterung und $G := \mathrm{Aut}(L/K)$.

Wir setzen von nun an stets $[L : K] < \infty$.

Also ist L/K algebraisch nach Bemerkung 3.6 und es gilt auch $|G| < \infty$ nach Lemma 3.15.

6.1 Galois-Erweiterungen

Definition 3.28 (*Galois-Erweiterung, Galoisgruppe*)

Ist $|G| = [L : K]$, so heißt L/K eine **Galois-Erweiterung**.
In diesem Fall heißt $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ die **Galoisgruppe** von L/K.

Beispiel 21

(a) $\mathbb{C}/\mathbb{R}$ ist eine Galois-Erweiterung vom Grad 2, da $\mathbb{C} = \mathbb{R}[i]$ und $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$, wobei $\sigma : \mathbb{C} \longrightarrow \mathbb{C}, i \mapsto -i$.

(b) Sei $K = \mathbb{Q}$ und $L := \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Dann ist L/K keine Galois-Erweiterung, da $\mathrm{Aut}(L/K) = \{\mathrm{Id}_L\}$.
Denn: $\sqrt[3]{2}$ ist eine Nullstelle von $f = X^3 - 2$ und jedes $\sigma \in \mathrm{Aut}(L/K)$ bildet $\sqrt[3]{2}$ auf eine weitere Nullstelle von f in L ab. Aber f hat noch 2 weitere konjugiert-komplexe Nullstellen (d.h. in einem Zerfällungskörper), die nicht in L liegen. Also muss $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ sein und damit ist $\sigma = \mathrm{Id}_L$ für alle $\sigma \in \mathrm{Aut}(L/K)$.

(c) Sei $L = \mathbb{F}_q$ ein endlicher Körper mit $q = p^n$ Elementen. Dann ist $L/\mathbb{F}_p$ eine Galois-Erweiterung, da $[L : \mathbb{F}_p] = n$ nach Satz 3.27 und $|\mathrm{Aut}(L/K)| = n$ nach Aufgabe 23, Blatt 6.

Wir möchten jetzt äquivalente Charakterisierungen der Galois-Erweiterungen finden.
Dafür untersuchen wir erst die Operation von G auf L durch $\sigma.y = \sigma(y)$ für alle $\sigma \in G$ und für alle $y \in L$. (Siehe §5.2.) Schreibe $\mathcal{O}_y$ für die Bahn von $y \in L$ unter dieser Operation.

Lemma 3.29

Sei $y \in L$ und $\mu_y \in K[X]$ das Minimalpolynom von y über K. Dann ist $|\mathcal{O}_y| < \infty$ und $\mu_y(x) = 0$ für alle $x \in \mathcal{O}_y$. Insbesondere gilt $[L : K] \geq [K(y) : K] = \deg(\mu_y) \geq |\mathcal{O}_y|$.

Beweis: Wegen $|G| < \infty$ ist auch $|\mathcal{O}_y| = |G : G_y| < \infty$ (Bahnbilanzgleichung!). Nach Anmerkung 3.13 gilt $\mu_y(\sigma(y)) = \sigma(\mu_y(y)) = \sigma(0) = 0$ für alle $\sigma \in G$, also ist $\mu_y(x) = 0$ für alle $x \in \mathcal{O}_y$ (da $x = \sigma(y)$ für ein $\sigma \in G$). Damit ist $[K(y) : K] = \deg(\mu_y) \geq |\mathcal{O}_y|$. ■

Aufgabe 22 (*Aufgabe 22, Blatt 6*)

Seien $M_1, \ldots, M_n$ ($n \in \mathbb{N}$) Zwischenkörper einer Erweiterung L/K (also $L \supseteq M_i \supseteq K \; \forall\, 1 \leq i \leq n$). Gilt $L = \bigcup_{i=1}^{n} M_i$, so existiert ein i mit $L = M_i$.

Bemerkung 3.30

Es gilt $|G| \leq [L : K]$ und es gibt ein Element $\alpha_0 \in L$ mit $G_{\alpha_0} = \{\mathrm{Id}_L\}$. Ist außerdem $|G| = [L : K]$, so ist $L = K(\alpha_0)$.

Beweis: Ist $G = \{\mathrm{Id}_L\}$, so sind die Aussagen klar. Also nehmen wir an, dass $G \neq \{\mathrm{Id}_L\}$ ist. Für $\sigma \in G$ setzen wir $M_\sigma := \{y \in L \mid \sigma(y) = y\}$. Offensichtlich ist M_σ ein Teilkörper von L, der K enthält. Ferner ist $\sigma \neq \mathrm{Id}_L$, so ist $M_\sigma \subsetneq L$. Da $G \neq \{\mathrm{Id}_L\}$ ist, so ist $K \subsetneq L$. Es folgt:

$$L \neq \bigcup_{\sigma \in G \setminus \{\mathrm{Id}_L\}} M_\sigma \qquad \text{(siehe Aufgabe 24)}$$

Es gibt also ein $\alpha_0 \in L$ mit $\sigma(\alpha_0) \neq \alpha_0$ für alle $\sigma \in G \setminus \{\mathrm{Id}_L\}$, d.h. $G_{\alpha_0} = \{\mathrm{Id}_L\}$ und damit hat die Bahn $\mathcal{O}_{\alpha_0}$ von α_0 nach der Bahnbilanzgleichung genau $|G|$ Elemente. Nach Lemma 3.29 ist also

$$[L : K] \geq [K(\alpha_0) : K] = \deg(\mu_{\alpha_0}) \geq |\mathcal{O}_{\alpha_0}| = |G| \,.$$

Ist schließlich $|G| = [L : K]$, so muss $[L : K] = [K(\alpha_0) : K]$ sein und damit ist $L = K(\alpha_0)$. ■

Satz 3.31 (*Charakterisierung der Galois-Erweiterungen*)

Sei L/K eine Körpererweiterung mit $[L:K] < \infty$ und $G := \mathrm{Aut}(L/K)$. Dann sind äquivalent:

(a) L/K ist eine Galois-Erweiterung.

(b) Es gibt ein $\alpha_0 \in L$ mit $L = K(\alpha_0)$ und so, dass das Minimalpolynom $\mu_{\alpha_0} \in K[X]$ über L in Linearfaktoren zerfällt und keine mehrfachen Nullstellen in L hat.

(c) L ist der Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[X]$, welches keine mehrfachen Nullstellen in L hat.

(d) Es gilt $K = \{y \in L \mid \sigma(y) = y \ \forall\, \sigma \in G\}$.

Beweis:

(b) ⇒ (c): Setze einfach $f := \mu_{\alpha_0}$. ✓

(a) ⇒ (b): Sei α_0 wie in Bemerkung 3.30, also ist insbesondere $G_{\alpha_0} = \{\mathrm{Id}_L\}$, so dass

$$|\mathcal{O}_{\alpha_0}| = |G|/|G_{\alpha_0}| = |G|/1 = |G|$$

nach der Bahnbilanzgleichung gilt. Wegen $L = K(\alpha_0)$ ist $\deg \mu_{\alpha_0} = [L:K]$. Aber $[L:K] = |G|$, da L/K eine Galois-Erweiterung ist. Also gilt $\deg \mu_{\alpha_0} = |\mathcal{O}_{\alpha_0}|$. Nun sind nach Lemma 3.29 die Elemente von $\mathcal{O}_{\alpha_0}$ Nullstellen von μ_{α_0}. Daraus folgt:

$$\mu_{\alpha_0} = \prod_{y \in \mathcal{O}_{\alpha_0}} (X - y)$$

(c) ⇒ (a): Sei L wie in (c). Dann gibt es mindestens $[L:K]$ Isomorphismen $\Sigma : L \longrightarrow L$ mit $\Sigma|_K = \mathrm{Id}_K$ nach Konstruktion von Σ in Satz 3.23. (Siehe auch Aufgabe 29 .) Alle diese Σ sind Elemente von G, so dass $|G| \geq |L:K|$ ist. Nach Bemerkung 3.30 ist auch $|G| \leq |L:K|$, also ist $|G| = |L:K|$.

(a) ⇒ (d): Sei $M := \{y \in L \mid \sigma(y) = y\, \forall\, \sigma \in G\}$. Dann ist $M \subseteq L$ ein Teilkörper und nach Definition von G ist $K \subseteq M$; außerdem ist offensichtlich $G = \mathrm{Aut}(L/M)$. Mit Bemerkung 3.30 erhalten wir:

$$|G| = |\mathrm{Aut}(L/M)| \leq [L:M] \leq [L:K]$$

Aber $|G| = [L:K]$ nach Voraussetzung, also muss überall Gleichheit gelten, also ist $[L:M] = [L:K]$ und damit muss $M = K$ sein.

(d) ⇒ (c): Schreibe $L = K(\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i \in L$ für alle $1 \leq i \leq r$ ($r \in \mathbb{N}$). (Möglich da L/K algebraisch ist!) Setze

$$\mathcal{O} := \bigcup_{i=1}^{r} \mathcal{O}_{\alpha_i} = \{\sigma(\alpha_i) \mid 1 \leq i \leq r, \sigma \in G\}\,,$$

$|\mathcal{O}| =: m$ und $\mathcal{O} =: \{y_1, \ldots, y_m\}$. Also gilt für alle $\sigma \in G$:

$$\{\sigma(y_1), \ldots, \sigma(y_m)\} = \{y_1, \ldots, y_m\}$$

Nun sei $f := \prod_{i=1}^{m}(X - y_i) \in L[X]$. Für $\sigma \in G$ ist dann

$$\widetilde{\sigma}(f) = \prod_{i=1}^{m}(X - \sigma(y_i)) = \prod_{i=1}^{m}(X - y_i) = f\,.$$

Mit Voraussetzung (d) folgt also $f \in K[X]$, und L ist ein Zerfällungskörper von f. Außerdem hat f keine mehrfachen Nullstellen nach Konstruktion. ■

Anmerkung 3.32 (*primitives Element*)

Falls $L = K(\alpha)$ gilt, so heißt das Element $\alpha \in L$ **primitives Element** der Erweiterung L/K.

Satz 3.31 zeigt, dass ein primitives Element in einer Galois-Erweiterung stets existiert, nämlich das Element α_0 in Teil (b).

Folgerung 3.33 (*Aufgabe 26, Blatt 7*)

Sei K ein Körper mit $\mathrm{Char}(K) = 0$. Dann gilt:

(a) Ist $f \in K[X]$ nicht-konstant und $L \supseteq K$ ein Zerfällungskörper von f, so ist L/K eine Galois-Erweiterung.

(b) Sei M/K eine endliche Körpererweiterung. Dann gibt es einen Körper L mit $L \supseteq M$, so dass L/K eine Galois-Erweiterung ist.

Beweis: (**Lösungsvorschlag.**)

(a) Weil $K[X]$ als euklidischer Ring ein ZPE-Ring ist, gibt es nicht-konstante paarweise teilerfremde irreduzible Polynome $f_1, \ldots, f_r \in K[X]$ und Vielfachheiten $n_1, \ldots, n_r \geq 1$ mit $f = f_1^{n_1} \cdots f_r^{n_r}$.
Nach Aufgabe 21(b) haben alle f_i nur einfache Nullstellen in L, denn wegen $\mathrm{char}(K) = 0$ verschwinden die formalen Ableitungen nicht-konstanter Polynome nicht.
Weil die f_i paarweise teilerfremd sind, hat also auch das Polynom $\tilde{f} := f_1 \cdots f_r \in K[X]$ nur einfache Nullstellen in L, denn für eine gemeinsame Nullstelle $a \in L$ von f_i und f_j für $i \neq j$ wäre sonst $(X - a)$ ein gemeinsamer Teiler von f_i und f_j von positivem Grad.
Weil die Nullstellen von f in L genau die Nullstellen von $\tilde{f}$ in L sind, ist L auch ein Zerfällungskörper des nicht-konstanten Polynoms $\tilde{f} \in K[X]$, das in L keine mehrfachen Nullstellen hat. Damit folgt die Behauptung aus Satz 3.31.

(b) Sei $\{b_1, \ldots, b_n\}$ eine K-Basis von M und sei L der Zerfällungskörper des Polynoms

$$\prod_{i=1}^{n} \mu_{b_i} \in K[X],$$

wobei μ_{b_i} das Minimalpolynom von b_i über K ist. Dann ist L/K nach Teil (a) eine Galois-Erweiterung. ∎

6.2 Der Hauptsatz der Galoistheorie

(Erinnerung: in diesem Abschnitt ist L/K stets eine endliche Körpererweiterung.)

Definition 3.34 (*Fixkörper*)

Sei $H \subseteq \mathrm{Aut}(K)$. Dann heißt $K^H := \{\alpha \in K \mid \sigma(\alpha) = \alpha \; \forall \, \sigma \in H\}$ **Fixkörper** von H. (Dies ist offensichtlich ein Teilkörper von K.)

Anmerkung 3.35

Für eine Galois-Erweiterung L/K mit Galoisgruppe $\mathrm{Gal}(L/K)$ gilt

$$K = L^{\mathrm{Gal}(L/K)}$$

nach Satz 3.31(d).

Wir nehmen nun an, dass L/K eine Galois-Erweiterung ist. Sei

$$\mathcal{M}(L/K) := \{\text{Zwischenkörper } M \mid L \supseteq M \supseteq K\}$$

und

$$\mathcal{H}(L/K) := \{H \leq \mathrm{Gal}(L/K)\}\,.$$

Hiermit können wir ein Hauptresultat dieser Vorlesung beweisen:

Satz 3.36 (*Hauptsatz der Galoistheorie*)

Sei L/K eine Galois-Erweiterung und $G := \mathrm{Gal}(L/K)$.

(a) Für $M \in \mathcal{M}(L/K)$ ist die Erweiterung L/M ebenfalls eine Galois-Erweiterung.

(b) Sei $M \in \mathcal{M}(L/K)$. Genau dann ist M/K eine Galois-Erweiterung, wenn $\sigma(M) \subseteq M$ für alle $\sigma \in G$ gilt. In diesem Fall ist $\mathrm{Gal}(L/M) \trianglelefteq G$ und $\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$.

(c) Die Abbildung

$$\begin{array}{rccc} \Psi: & \mathcal{M}(L/K) & \longrightarrow & \mathcal{H}(L/K) \\ & M & \mapsto & \mathrm{Gal}(L/M) \end{array}$$

ist eine Bijektion mit Umkehrabbildung

$$\begin{array}{rccc} \Phi: & \mathcal{H}(L/K) & \longrightarrow & \mathcal{M}(L/K) \\ & H & \mapsto & L^H\,. \end{array}$$

Diese Bijektion heißt **Galoiskorrespondenz**.

(d) (i) Für $M \in \mathcal{M}(L/K)$ gelten: $[L : M] = |\mathrm{Gal}(L/M)|$ und $[M : K] = |G : \mathrm{Gal}(L/M)|$.
(ii) Für $H \in \mathcal{H}(L, K)$ gelten: $[L : L^H] = |H|$ und $[L^H : K] = |G : H|$.

(e) Die Galoiskorrespondenz kehrt die Inklusionsordnung um:

$$H_1 \leq H_2 \text{ Elemente von } \mathcal{H}(L/K) \quad \Longrightarrow \quad L^{H_1} \supseteq L^{H_2}$$

$$M_1 \subseteq M_2 \text{ Elemente von } \mathcal{M}(L/K) \quad \Longrightarrow \quad \mathrm{Gal}(L/M_1) \geq \mathrm{Gal}(L/M_2)$$

Beweis: (a) Nach Satz 3.31(c) ist L der Zerfällungskörper eines nicht-konstanten Polynoms $f \in K[X]$, das keine mehrfachen Nullstellen in L hat. Dann ist L auch der Zerfällungskörper von $f \in M[X]$. Jetzt folgt aus Satz 3.31(c), dass L/M eine Galois-Erweiterung ist.

(b) '$\Rightarrow$': M/K Galois-Erweiterung $\Longrightarrow$ nach Satz 3.31(b) $\exists \alpha_0 \in M$ mit $M = K(\alpha_0)$ und so, dass M der Zerfällungskörper von $\mu_{\alpha_0} \in K[X]$ ist. Nun muss $\sigma(M) \subseteq M$ für alle $\sigma \in G$ sein, da $\sigma|_K = \mathrm{Id}_K$ und $\sigma(\alpha_0)$ ist wieder eine Nullstelle von μ_{α_0}, also ist $\sigma(\alpha_0) \in M$.

'$\Leftarrow$': $\sigma(M) \subseteq M\ \forall\ \sigma \in G \Longrightarrow \sigma|_M$ ist ein Automorphismus von M und $(\sigma|_M)|_K = \sigma|_K = \mathrm{Id}_K$. Damit ist

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathrm{Aut}(M/K) \\ & \sigma & \mapsto & \sigma|_M \end{array}$$

ein Gruppenhomomorphismus, da $\varphi(\sigma \circ \tau) = (\sigma \circ \tau)|_M = \sigma|_M \circ \tau|_M = \varphi(\sigma) \circ \varphi(\tau)\ \forall\ \sigma, \tau \in G$. Es gilt

$$\ker(\varphi) = \{\sigma \in G \mid \sigma|_M = \mathrm{Id}_M\} = \mathrm{Gal}(L/M)\,. \qquad (*)$$

Mit dem Homomorphiesatz (für Gruppen) folgt

$$G/\mathrm{Gal}(L/M) \cong \varphi(G) \leq \mathrm{Aut}(M/K)\,. \qquad (**)$$

Aber L/K und L/M sind Galois-Erweiterungen (siehe (a)), also sind $[L:K] = |G|$ und $[L:M] = |\mathrm{Gal}(L/M)|$. Aus dem Gradmultiplikationssatz folgt:

$$[M:K] = \frac{[L:K]}{[L:M]} = \frac{|G|}{|\mathrm{Gal}(L/M)|} = |\varphi(G)| \leq |\mathrm{Aut}(M/K)|$$

Aber mit Bemerkung 3.30 gilt auch $|\mathrm{Aut}(M/K)| \leq [M:K]$. Damit ist $|\mathrm{Aut}(M/K)| = [M:K]$, so dass M/K eine Galois-Erweiterung ist.

Insbesondere: $(*) \Longrightarrow \mathrm{Gal}(L/M) \trianglelefteq G$ (da ein Kern), und
$(**) \Longrightarrow \mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$, da die Gleichheit $\varphi(G) = \mathrm{Aut}(M/K)$ jetzt gilt.

(c) Es folgt aus (a), dass die Abbildung Ψ wohl-definiert ist, da L/M tatsächlich eine Galois-Erweiterung ist, und somit ist $\mathrm{Gal}(L/M) = \mathrm{Aut}(L/M)$ eine Untergruppe von $\mathrm{Gal}(L/K)$ ist.

Behauptung 1: ψ ist injektiv.

Beweis: Seien $M, M' \in \mathcal{M}(L/K)$ mit $\Psi(M) = \Psi(M')$, d.h. $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/M')$. Damit folgt aus Anmerkung 3.35 (zweimal angewendet), dass

$$M = L^{\mathrm{Gal}(L/M)} = L^{\mathrm{Gal}(L/M')} = M'$$

#

Behauptung 2: ψ ist surjektiv.

Beweis: Sei $H \leq G$. Dann ist $L^H \in \mathcal{M}(L/K)$ nach Definition.

Zu zeigen: $H = \Psi(L^H) = \mathrm{Gal}(L/L^H)$.

Die Inklusion $H \subseteq \mathrm{Gal}(L/L^H)$ ist klar nach Definition von L^H. Für die andere Inklusion: nach (a) gilt $[L:L^H] = |\mathrm{Gal}(L/L^H)| \geq |H|$ (dank der 1. Inklusion).
Es genügt also zu zeigen, dass $[L:L^H] \leq |H|$ gilt. Dazu sei $\alpha_0 \in L$ wie in Bemerkung 3.30, d.h. $\mathrm{Gal}(L/K)_{\alpha_0} = \{\mathrm{Id}_L\}$ und $L = K(\alpha_0)$. Dann gelten auch $H_{\alpha_0} = \{\mathrm{Id}_L\}$ und $L = L^H(\alpha_0)$.
Also hat die Bahn $\mathcal{O}_{\alpha_0} = \{\sigma(\alpha_0) \mid \sigma \in H\}$ genau $|H|$ Elemente nach der Bahnbilanzgleichung. Sei

$$g := \prod_{y \in \mathcal{O}_{\alpha_0}} (X - y) \in L[X]\,.$$

Weil $\sigma(\mathcal{O}_{\alpha_0}) = \mathcal{O}_{\alpha_0}$ für alle $\sigma \in H$ ist, gilt $\widetilde{\sigma}(g) = g$ für alle $\sigma \in H$, also ist $g \in L^H[X]$. Aber jetzt muss das Minimalpolynom von α_0 ein Teiler von g sein, also gilt

$$[L:L^H] = [L^H(\alpha_0):L^H] \leq \deg(g) = |\mathcal{O}_{\alpha_0}| = |H|\,,$$

wie verlangt. #
Schließlich ist Φ die Umkehrabbildung von Ψ nach obiger Konstruktion.

(d) In Behauptung 2 wurde gezeigt: für $H \leq \mathrm{Gal}(L/K)$ ist $[L:L^H] = |H|$. Aus dem Gradmultiplikationssatz folgt:

$$[L^H:K] = \frac{[L:K]}{[L:L^H]} = \frac{|G|}{|H|} = |G:H|\,.$$

$\Longrightarrow$ Aussage (ii) gilt.
Aussage (i) folgt jetzt direkt aus der Galoiskorrespondenz: Für $M \in \mathcal{M}(L/K)$ existiert $H \leq G$ mit $M = \Phi(H) = L^H$ und $H = \Psi(M) = \mathrm{Gal}(L/M)$. Also ist $[L:M] = [L:L^H] = |H| = |\mathrm{Gal}(L/M)|$ und $[M:K] = [L^H:K] = |G:H| = |G:\mathrm{Gal}(L/M)|$ nach dem 1. Teil.

(e) Erst $H_1 \leq H_2 \Longrightarrow L^{H_2} = \{\alpha \in L \mid \sigma(\alpha) = \alpha\ \forall\, \sigma \in H_2\} \subseteq \{\alpha \in L \mid \sigma(\alpha) = \alpha\ \forall\, \sigma \in H_1\} = L^{H_1}$.
Nun $M_1 \subseteq M_2 \Longrightarrow \forall\ \sigma \in \mathrm{Gal}(L/M_2)$ gilt $\sigma|_{M_1} = (\sigma|_{M_2})|_{M_1} = \mathrm{Id}_{M_2}|_{M_1} = \mathrm{Id}_{M_1}$, also $\sigma \in \mathrm{Gal}(L/M_1)$, und damit ist $\mathrm{Gal}(L/M_2) \leq \mathrm{Gal}(L/M_1)$. ■

Beispiel 22

Siehe BeamerWoche13.pdf .

Lösungsvorschlag für Aufgabe 27, Blatt 7:
Voraussetzung: $\omega := \exp(\frac{2\pi i}{3})$, $L := \mathbb{Q}(\sqrt[3]{2}, \omega)$, $\sigma, \tau \in \mathrm{Aut}(L/\mathbb{Q})$ mit

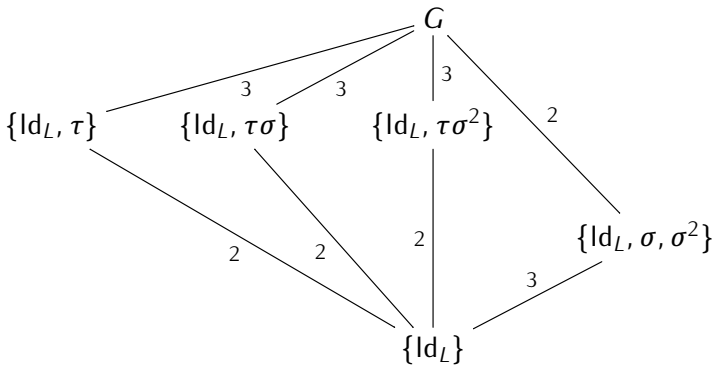
$$\sigma : \ \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \ \ \omega \mapsto \omega$$

und

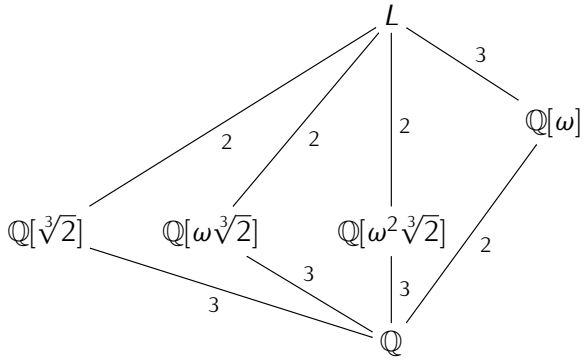
$$\tau : \ \sqrt[3]{2} \mapsto \sqrt[3]{2}, \ \ \omega \mapsto \omega^2.$$

Behauptung: $L/\mathbb{Q}$ ist Galois-Erweiterung, $G := \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$ und die Untergruppen von G und die Zwischenkörper von $L/\mathbb{Q}$ entsprechen sich wie folgt:

Untergruppen:



Zwischenkörper:



Beweis: Das Polynom $X^3 - 2 \in \mathbb{Q}[X]$ ist nach dem Eisensteinkriterium irreduzibel und somit das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Wegen $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R} \not\ni \omega$ und $\omega^2 + \omega + 1 = \frac{\omega^3 - 1}{\omega - 1} = 0$ ist $X^2 + X + 1$ das Minimalpolynom von ω über $\mathbb{Q}[\sqrt[3]{2}]$.
Also ist

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt[3]{2}]] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Weil $X^3 - 2$ über L, aber nicht $\mathbb{Q}[\sqrt[3]{2}]$ in Linearfaktoren zerfällt, muss L der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ sein. Also ist $L/\mathbb{Q}$ eine Galois-Erweiterung und somit $|G| = [L : \mathbb{Q}] = 6$.

Nach Aufgabe 24 erhält man von der Operation von G auf den drei Nullstellen $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ und $\omega^2\sqrt[3]{2}$ einen injektiven Gruppenhomomorphismus $G \to S_3$. Aus Ordnungsgründen ist dieser auch surjektiv und damit $G \cong S_3$.

Wegen $o(\sigma) = 3$ und $o(\tau) = 2$ gilt außerdem $G = \langle \sigma, \tau \rangle$.

Offensichtlich ist $L^{\langle \tau \rangle} = \mathbb{Q}[\sqrt[3]{2}]$. Durch direktes Nachrechnen sieht man, dass $\sigma\tau\sigma^{-1} = \tau\sigma$ und $\sigma^2\tau\sigma^{-2} = \tau\sigma^2$ gilt. Mit Aufgabe 25(a) folgt also

$$L^{\langle \tau\sigma \rangle} = L^{\sigma\langle \tau \rangle\sigma^{-1}} = \sigma(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}[\omega\sqrt[3]{2}]$$

und

$$L^{\langle \tau\sigma^2 \rangle} = L^{\sigma^2\langle \tau \rangle\sigma^{-2}} = \sigma^2(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}[\omega^2\sqrt[3]{2}].$$

Weil $L^G = \mathbb{Q}$ und $L^{\{\mathrm{Id}_L\}} = L$ klar sind, bleibt nur noch $L^{\langle \sigma \rangle} = \mathbb{Q}[\omega]$.

Aufgabe 25 (*Aufgabe 25, Blatt 7*)

Sei L/K eine endliche Galois-Erweiterung mit Galoisgruppe $G := \mathrm{Gal}(L/K)$. Sei $H \leq G$.

(a) Für alle $\sigma \in G$ ist $\sigma(L^H) = L^{\sigma H\sigma^{-1}}$.

(b) $H \trianglelefteq G \iff L^H/K$ ist eine Galois-Erweiterung.

Lösungsvorschlag:

(a) Für $a \in L$ ist

$$\begin{aligned} & a \in L^{\sigma H\sigma^{-1}} \\ \iff \quad & (\sigma h\sigma^{-1})(a) = a \ \forall\ h \in H \\ \iff \quad & (h\sigma^{-1})(a) = \sigma^{-1}(a) \ \forall\ h \in H \\ \iff \quad & a \in \sigma(L^H). \end{aligned}$$

(b) Wir schreiben $M := L^H$. Nach Satz 3.36(c) ist dann $H = \mathrm{Gal}(L/M)$. Ist M/K eine Galois-Erweiterung, dann folgt die Behauptung sofort aus Satz 3.36(b). Sei nun umgekehrt $H \trianglelefteq G$ und sei $\sigma \in G$ beliebig. Dann ist $\sigma^{-1}H\sigma \subseteq H$, also $L^H \subseteq L^{\sigma^{-1}H\sigma}$. Nach Teil (a) ist dies gleichbedeutend mit $M \subseteq \sigma^{-1}(M)$, was äquivalent zu $\sigma(M) \subseteq M$ ist. Weil σ beliebig war, folgt die Behauptung aus Satz 3.36(b).

6.3 Der Hauptsatz der Algebra

Wir können jetzt ein zweites Hauptresultat dieser Vorlesung beweisen: nämlich der Hauptsatz der Algebra. Es gibt für diesen Satz mehrere bekannte Beweise, die verschiedene Bereiche der Mathematik nutzen, sowie z.B. komplexe Analysis. Der Beweis, der hier präsentiert wird, nutzt den Hauptsatz der Galoistheorie und den Existenzsatz von Sylowuntergruppen.
Ab jetzt bedeutet ein Querstrich komplexe Konjugation.

Anmerkung 3.37

Wir werden die zwei folgenden wohl-bekannten Tatsachen nutzen:

(i) Jedes nicht-konstantes Polynom $f \in \mathbb{R}[X] \setminus \{0\}$ von ungeradem Grad hat eine Nullstelle in $\mathbb{R}$.
[Denn: O.B.d.A. ist f normiert, also da $\deg(f)$ ungerade ist, ist $\lim_{x\to+\infty} f(x) = +\infty$, $\lim_{x\to-\infty} f(x) = -\infty$. Nach dem Zwischenwertsatz der Analysis muss es also ein $x_0 \in \mathbb{R}$ geben mit $f(x_0) = 0$.]

(ii) Jedes $z = a + bi \in \mathbb{C}$ hat eine Quadratwurzel: nämlich

$$z = \left(\sqrt{\frac{1}{2}(\sqrt{a^2+b^2}+a)} \pm i\sqrt{\frac{1}{2}(\sqrt{a^2+b^2}-a)} \right)^2 ,$$

wobei das $\pm$ Vorzeichen so gewählt wird, dass $\pm b \geq 0$ gilt. (Einfach nachrechnen.)

Satz 3.38 (*Hauptsatz der Algebra*)

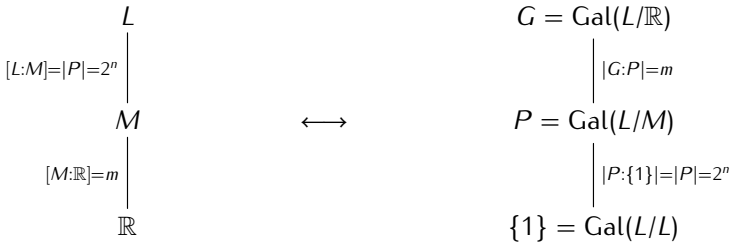
Jedes nicht-konstante Polynom $f \in \mathbb{C}[X] \setminus \{0\}$ zerfällt in Linearfaktoren über $\mathbb{C}$.

[Man sagt dafür auch, dass $\mathbb{C}$ **algebraisch abgeschlossen** ist.]

Beweis: Sei $f \in \mathbb{C}[X]$ ein Polynom mit $\deg(f) \geq 1$. Sei also $L \supseteq \mathbb{C}$ der Zerfällungskörper von $\overline{f}f \in \mathbb{R}[X]$.

Zu zeigen: $L = \mathbb{C}$.

(Denn: damit zerfällt $\overline{f}f$ in Linearfaktoren über $\mathbb{C}$ nach Definition 3.17(i), also zerfällt f auch in Linearfaktoren über $\mathbb{C}$, da $f \mid \overline{f}f$.) Dafür sei $g := (X^2+1)\overline{f}f \in \mathbb{R}[X]$. Klar: L ist auch der Zerfällungskörper von g. Nach Folgerung 3.33 ist $L/\mathbb{R}$ eine Galois-Erweiterung. Sei also $G := \mathrm{Gal}(L/\mathbb{R})$ und schreibe $|G| := 2^n \cdot m$ mit $n \geq 0$ und $m \in \mathbb{N}$ ungerade.
Nach Konstruktion ist $n \geq 1$, denn $(X^2+1) | g$ und es gibt einen Automorphismus $\sigma : L \longrightarrow L$ mit $\sigma(i) = -i$ und σ ist die Identität auf den anderen Nullstellen von g, also hat $\sigma \in \mathrm{Gal}(L/\mathbb{R})$ Ordnung 2. (Siehe Satz 3.23.)
Sei also $P \in \mathrm{Syl}_2(G)$. Nach dem Hauptsatz der Galoistheorie existiert ein Zwischenkörper $\mathbb{R} \subseteq M \subseteq L$ mit $P = \mathrm{Gal}(L/M)$, $[L : M] = |P|$ und $[M : \mathbb{R}] = |G : P| = m$.



Behauptung 1: $M = \mathbb{R}$.
Beweis: Sei $\alpha \in M$ beliebig und $\mu_\alpha \in \mathbb{R}[X]$ das Minimalpolynom von α über $\mathbb{R}$. Mit dem Gradmultiplikationssatz folgt

$$\deg \mu_\alpha = [\mathbb{R}(\alpha) : \mathbb{R}] \mid [M : \mathbb{R}] = m ,$$

also ist $\deg \mu_\alpha$ ungerade. Wegen Anmerkung 3.37(i) muss μ_α eine Nullstelle in $\mathbb{R}$ haben. Aber μ_α ist irreduzibel nach Definition, also folgt daraus, dass $\deg \mu_\alpha = 1$ ist, also ist $[\mathbb{R}(\alpha) : \mathbb{R}] = 1$ und damit ist $\mathbb{R}(\alpha) = \mathbb{R}$, also $\alpha \in \mathbb{R}$. Aber dies gilt für alle $\alpha \in \mathbb{R}$, also muss $M = \mathbb{R}$ sein. #

Aus Behauptung 1 folgt $1 = [M : \mathbb{R}] = m = |G : P|$, also ist $|G| = 2^n$.

Jetzt folgt auch aus dem Hauptsatz der Galoistehorie, Teil (a), dass $L/\mathbb{C}$ auch eine Galois-Erweiterung ist, so dass $[L : \mathbb{C}] = |H|$ ist, wobei $H := \mathrm{Gal}(L/\mathbb{C})$ ist. Nun ist $\mathbb{C} = \mathbb{R}(i)$, wobei $[\mathbb{R}(i) : \mathbb{R}] = 2$ ist, da $i \in \mathbb{C} \setminus \mathbb{R}$ eine Nullstelle von $X^2 + 1$ ist, also gilt

$$2^n = |G| = [L : \mathbb{R}] = [L : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = [L : \mathbb{C}] \cdot [\mathbb{R}(i) : \mathbb{R}] = |H| \cdot 2$$

$\Longrightarrow |H| = 2^{n-1}$.

Behauptung 2: $n = 1$.

Beweis: Wir nehmen an, dass $n > 1$ wäre $\Longrightarrow |H| = 2^{n-1} \geq 2 \Longrightarrow$ es gibt eine Untergruppe $U \leq H$ mit Index 2 [diese Aussage folgt aus Satz 1.35 da H eine 2-Gruppe ist und somit auflösbar nach Beispiel 8(b)]. Nach dem Hauptsatz der Galoistheorie korrespondiert zu U ein Zwischenkörper $M' \in \mathcal{M}(L/\mathbb{C})$ mit $U = \mathrm{Gal}(L/M')$, $[L : M'] = |U|$ und $[M' : \mathbb{C}] = |H : U| = 2$.

$$\begin{array}{ccc} L & & H = \mathrm{Gal}(L/\mathbb{C}) \\ \Big| {\scriptstyle [L:M']=|U|=2^{n-2}} & & \Big| {\scriptstyle |H:U|=2} \\ M' & \longleftrightarrow & U = \mathrm{Gal}(L/M') \\ \Big| {\scriptstyle [M':\mathbb{C}]=2} & & \Big| {\scriptstyle |U:\{1\}|=|U|=2^{n-2}} \\ \mathbb{C} & & \{1\} = \mathrm{Gal}(L/L) \end{array}$$

Nach Aufgabe 20, Blatt 5 gibt es nun ein Element $\alpha \in M' \setminus \mathbb{C}$ mit $z := \alpha^2 \in \mathbb{C}$ und $M' = \mathbb{C}[\alpha]$. Anders gesagt: α ist eine Quadratwurzel von $z \in \mathbb{C}$, also folgt mit Anmerkung 3.37(ii) $\alpha \in \mathbb{C}$, so dass $M' = \mathbb{C}$ und $[M' : \mathbb{C}] = 1$. Widerspruch! #

Aus Behauptung 2 folgt $[L : \mathbb{R}] = |G| = 2^n = 2^1 = 2$. Dann ist

$$2 = [L : \mathbb{R}] = [L : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = [L : \mathbb{C}] \cdot 2$$

und damit ist $[L : \mathbb{C}] = 1$, also ist $L = \mathbb{C}$, wie behauptet.

■

7 Konstruktionsaufgaben aus der Antike

In diesem Abschnitt nehmen wir an, dass jeder betrachtete Körper ein Körper der Charakteristik 0 ist.

7.1 Radikalerweiterungen

Definition 3.39

Sei L/K eine Körpererweiterung. Dann heißt L/K

(a) **einfache Radikalerweiterung**, wenn es ein $\alpha \in L$ und ein $n \in \mathbb{N}$ gibt, so dass $L = K(\alpha)$ und α eine Nullstelle von $X^n - c \in K[X]$ ist. Wenn n minimal mit dieser Eigenschaft ist, heißt L/K auch **einfache n-Radikalerweiterung**.

(b) **Radikalerweiterung**, wenn es eine Kette von Zwischenkörpern

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = L$$

gibt, so dass K_i/K_{i-1} für $1 \leq i \leq s$ einfache Radikalerweiterungen sind. Ist jede diese Erweiterungen eine einfache n-Radikalerweiterungen, so heißt L/K eine **n-Radikalerweiterung**.

Beispiel 23

(a) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine einfache 2-Radikalerweiterung.

(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})/\mathbb{Q}$ ist eine Radikalerweiterung, da

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})$$

ist, wobei $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ eine einfache 2-Radikalerweiterung ist, und $\mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ eine einfache 3-Radikalerweiterung ist.

(c) Dagegen ist $\mathbb{Q}(\sqrt{2}, \sqrt{1+\sqrt{2}})/\mathbb{Q}$ eine 2-Radikalerweiterung.

Lemma 3.40

Sei L/K eine 2-Radikalerweiterung und $\alpha \in L$, dann existieren $m, \ell \in \mathbb{N}$ mit

$$[L : K] = 2^m \text{ und } [K(\alpha) : K] = 2^\ell .$$

Beweis: Weil L/K eine 2-Radikalerweiterung ist, gibt es eine Kette von Zwischenkörpern

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = L ,$$

wobei $[K_i : K_{i-1}] = 2 \; \forall \; 1 \leq i \leq s$ ist. Mit dem Gradmultiplikationssatz folgt $[L : K] = 2^m$ für ein $m \in \mathbb{N}$ und daraus $2^m = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = 2^{m-\ell} \cdot 2^\ell$ für ein $\ell \in \mathbb{N}$. ■

7.2 Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt stellen wir uns eine komplexe Zahl $z = x + yi \in \mathbb{C}$ als Punkt $(x, y) \in \mathbb{R}^2$ vor. Sei $\mathcal{M} \subseteq \mathbb{C}$ eine Teilmenge mit mindestens zwei Elementen; oBdA nehmen wir an, dass $0, 1 \in M$ gilt. Dann sei:

$\mathrm{Ge}(\mathcal{M})$	:=	Menge der Geraden, die durch 2 verschiedene Punkte von $\mathcal{M}$ gehen.
$\mathrm{Kr}(\mathcal{M})$	:=	Menge der Kreise, deren Mittelpunkt in $\mathcal{M}$ liegt und deren Radius gleich dem Abstand zweier Punkte $\mathcal{M}$ ist.

Definition 3.41

Ein Element $z \in \mathbb{C}$ ist **aus $\mathcal{M}$ konstruierbar mit Zirkel und Lineal** (oder einfach **konstruierbar**), wenn z sich durch endlich viele (wiederholte) Anwendungen von den folgenden **Elementaroperationen** ausgehend von Punkten in $\mathcal{M}$ kontuieren lässt:

(1) Schnittpunkt zweier verschiedener Geraden aus $\mathrm{Ge}(\mathcal{M})$;

(2) Schnittpunkt einer Geraden aus $\mathrm{Ge}(\mathcal{M})$ mit einem Kreis aus $\mathrm{Kr}(\mathcal{M})$;

(3) Schnittpunkt zweier verschiedener Kreise aus $\mathrm{Kr}(\mathcal{M})$.

Sei $\mathcal{K}(\mathcal{M}) := \{z \in \mathbb{C} \mid z \text{ ist aus } \mathcal{M} \text{ konstruierbar mit Zirkel und Lineal}\}$

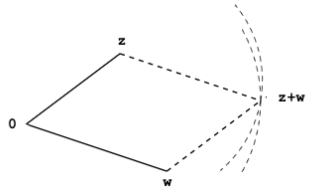
Bemerkung 3.42

Die Menge $\mathcal{K}(\mathcal{M})$ ist ein Teilkörper von $\mathbb{C}$ mit $\overline{\mathcal{K}(\mathcal{M})} = \mathcal{K}(\mathcal{M})$, und für $z \in \mathcal{K}(\mathcal{M})$ ist auch $\sqrt{z} \in \mathcal{M}$.

Beweis: Seien $z, w \in \mathcal{K}(\mathcal{M})$ mit $z \neq 0$. Zu zeigen ist:

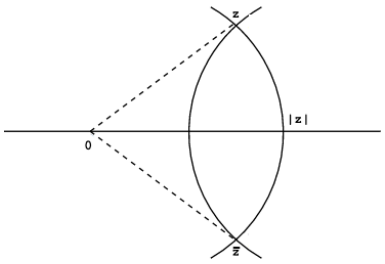
$$z + w, -z, z^{-1} \cdot w, \overline{z}, \sqrt{z} \in \mathcal{K}(\mathcal{M})$$

Dies zeigt man einfach durch geometrische Konstruktion unter Verwendung von einfachen geometrischen Sätzen.
· **Addition:** Liegen z und w auf derselben Geraden durch 0, so ist $z + w$ einer der Schnittpunkte des Kreises um z mit Radius $|w - 0|$ mit der Geraden durch 0 und z. Sind die beiden hingegen $\mathbb{R}$-linear unabhängig, so ist $z + w$ einer der Schnittpunkte der Kreise um z mit Radius $|w - 0|$ und um w mit Radius $|z - 0|$:

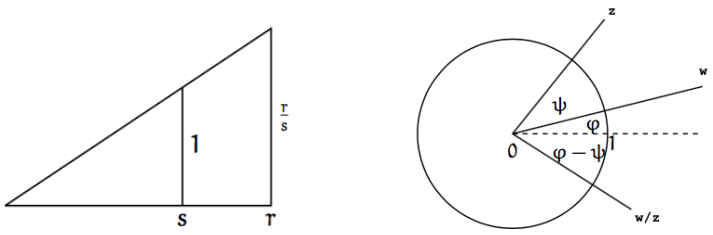


In jedem der Fälle ist $z + w \in \mathcal{K}(\mathcal{M})$.

· Nun ist $-z$ Schnittpunkt der Geraden durch 0 und z mit dem Kreis um 0 und mit Radius $|z - 0|$, also ist $-z \in \mathcal{K}(\mathcal{M})$.
· **Betrag und komplexe Konjugation**: Mit Zirkel und Lineal können wir den Betrag $|z|$ und das komplex Konjugierte von z konstruieren und erhalten so $|z|, \overline{z} \in \mathcal{K}(\mathcal{M})$. Dazu spiegeln wir z an der Geraden durch 0 und 1 und erhalten $\overline{z}$ als das Spiegelbild und $|z|$ als den Schnittpunkt des Kreises um 0 mit Radius $|z - 0|$.



· **Multiplikation**: Wir stellen beide Zahlen in Polarkoordinaten $z = se^{i\psi}$ und $w = re^{i\varphi}$ dar. Um nun das Produkt $z^{-1}w = \frac{r}{s}e^{i}(\varphi - \psi)$ zu konstruieren, müssen wir also die Beträge der beiden Zahlen $-z$ und w multiplizieren und die Winkel addieren. Dazu nutzen wir den Strahlensatz und erhalten:



· **Quadratwurzel**: Übung: Verwende den Höhensatz. ■

Satz 3.43

Sei $\{0, 1\} \subset \mathcal{M} \subset \mathbb{C}$ gegeben. Ein Punkt $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal aus Punkten von M konstruierbar, wenn z in einer 2-Radikalerweiterung von $\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}})$ liegt.

Beweis:

'$\Leftarrow$' Sei $z \in \mathbb{C}$ in einer 2-Radikalerweiterung K_s von $\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}})$ enthalten. Dann gibt es eine Kette

$$\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}}) = K_0 \subset K_1 \subset \cdots \subset K_s\,,$$

wobei K_i/K_{i-1} einfache 2-Radikalerweiterungen sind, d.h. für alle $1 \leq i \leq s$

$$K_i = K_{i-1}(\alpha_i) \quad \text{mit } \alpha_i^2 \in K_{i-1}\,.$$

Also gibt es für $1 \leq i \leq s$ ein $\beta_i \in K_{i-1}$ mit $\alpha_i = \sqrt{\beta_i}$. Folglich entsteht $z \in K_s$ durch sukzessive Anwendung der vier Grundrechenarten und Wurzelziehen und ist deshalb nach Bemerkung 3.42 mit Zirkel und Lineal konstruierbar.

'$\Rightarrow$' Sei umgekehrt $z \in \mathcal{K}(\mathcal{M})$. Alle Punkte, die man durch Konstruktion mit Zirkel und Lineal aus $\mathcal{M}$ erhält, sind Lösungen von linearen oder quadratischen Gleichungen, und diese liegen nach Induktion in 2-Radikalerweiterungen von $\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}})$.

■

7.3 Unlösbare Konstruktionsaufgaben der Antike

Wir betrachten nun die verschiedenen klassischen Probleme aus der Antike, die in der 1. Vorlesung eingeführt wurden.

Beispiel 24 (*Quadratur des Kreises*)

Problem: Ist die Konstruktion eines Quadrates mit dem Flächeninhalt (also π) eines gegebenen Kreises mit Radius 1 mit Zirkel und Lineal (aus $\{0,1\}$) möglich?

Behauptung: Die Quadratur des Kreises ist unmöglich.

Die Seitenlänge eines solchen Quadrates wäre $\sqrt{\pi}$; dann müsste also $\sqrt{\pi}$ konstruierbar, also auch π konstruierbar sein. Insbesondere wäre π nach Satz 3.43 in einer 2-Radikalerweiterung enthalten, und damit wäre $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^\ell$ für ein $\ell \in \mathbb{N}$ nach Lemma 3.40. Dies ist ein Widerspruch zum:

Satz von Lindemann (1882): π ist transzendent. (Ohne Beweis. Zu aufwändig für diese Vorlesung.)

Also ist die Quadratur des Kreises unmöglich.

Beispiel 25 (*Verdopplung des Würfels*)

Problem: Ist die Konstruktion eines Würfels mit doppeltem Volumen eines gegebenen Würfels mit Zirkel und Lineal möglich?

Behauptung: Die Verdopplung des Würfels ist unmöglich.

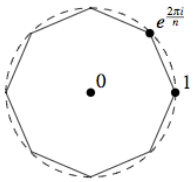
Wäre die Verdopplung des Würfels möglich, dann wäre in diesem Fall $\sqrt[3]{2}$ konstruierbar, also nach Satz 3.43 in einer 2-Radikalerweiterung enthalten, d.h. es muss $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2^\ell$ für ein $\ell \in \mathbb{N}$ nach Lemma 3.40 gelten. Aber $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$; Widerspruch. Also ist die Verdopplung des Würfels unmöglich.

Beispiel 26 (*Konstruktion eines regelmäßigen n-Ecks*)

Problem: Für welche Zahl $n \in \mathbb{N}$ ist ein regelmäßiges n-Eck mit Zirkel und Lineal konstruierbar?

Klar: Ein regelmäßiges n-Eck ist konstruierbar $\iff$ die **primitive n-te Einheitswurzel** $\zeta_n := e^{\frac{2\pi i}{n}}$

ist konstruierbar.



D.h. wir betrachten oBdA, dass der Mittelpunkt unseres n-Eck 0 ist, und einer der Eckpunkte des n-Ecks 1 ist. Offensichtlich genügt es dann, den ersten weiteren Eckpunkt $e^{\frac{2\pi i}{n}}$ zu konstruieren.

Satz 3.44

Sei $n > 2$. Ein regelmäßiges n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^k \cdot p_1 \cdots p_r$ ist, mit $k \geq 0$ und paarweise verschiedenen Fermat-Primzahlen $p_i = 2^{2^{c_i}} + 1$.

Beweis (Sketch): Sei $\mathcal{M} := \{0, 1\}$. Nach Satz 3.43 ist ζ_n konstruierbar genau dann wenn $\mathbb{Q}(\zeta_n)$ eine 2-Radikalerweiterung von $\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}}) = \mathbb{Q}$. Es nun gilt:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

und falls $n = \prod_{j=1}^{r} p_j^{m_j}$ eine Primfaktorzerlegung von n ist, dann erhalten wir

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \prod_{j=1}^{r} p_j^{m_j - 1}(p_j - 1)\,.$$

(Resultat aus der Vorlesung Elementare Zahlentheorie.) Außerdem muss dies eine 2-Potenz nach obigem Argument sein. Also: $p_j = 2 \Rightarrow m_j$ kann beliebig sein; $p_j \neq 2 \Rightarrow 0 \leq m_j \leq 1$, und $p_j - 1 = 2^{a_j}$ falls $m_j = 1$, d.h. alle $p_j \neq 2$ müssen die Form $p_j = 2^{a_j} + 1$ haben. Nun: ist $a_j = u_j \cdot v_j$, mit u_j ungerade, dann ist

$$2^{a_j} + 1 = 2^{u_j \cdot v_j} + 1 = (2^{v_j} + 1)(2^{v_j(u_j - 1)} - 2^{v_j(u_j - 2)} + \ldots + 1)$$

keine Primzahl. Also: $2^{a_j} + 1$ Primzahl $\Longrightarrow a_j = 2^{c_j}$ für ein $c_j \in \mathbb{N}$. ■

Anmerkung: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sind die einzigen bekannten Fermatprimzahlen.

Folgerung 3.45

Ein regelmäßiges 7-Eck ist nicht mit Zirkel und Lineal konstruierbar.

Beweis: Klar: 7 erfüllt nicht die Bedingung von Satz 3.44, also ist ζ_7 nicht konstruierbar. ■

Beispiel 27 (*Dreiteilung des Winkels*)

Problem: Gegeben sei ein Winkel α, also $(\sin(\alpha), \cos(\alpha)) \in \mathbb{R}^2$. Ist $\frac{\alpha}{3}$ konstruierbar?

Behauptung: Eine Winkeldreiteilung ist i.A. unmöglich.

Betrachte z.B. $\alpha = \pi/3$. Es gilt: $\frac{\alpha}{3}$ ist konstruierbar $\Longleftrightarrow$ ζ_{18} ist konstruierbar. Aber dies ist unmöglich nach Satz 3.44, da $18 = 2 \cdot 3^2$.

Übung: Dagegen ist die Dreiteilung von π möglich, da ζ_6 konstruierbar ist.

8 Auflösbarkeit von Polynomgleichungen

Definition 3.46

Sei $K \subset \mathbb{C}$ ein Körper. Ein nicht-konstantes Polynom $f \in K[X]$ heißt **durch Radikale auflösbar**, wenn ein Zerfällungskörper L von f in einer Radikalerweiterung von K liegt.

Damit erhalten wir das folgende Auflösbarkeitskriterium fur Polynome:

Satz 3.47 (*Galois*)

Sei $K \subseteq \mathbb{C}$ ein Körper. Sei $f \in K[X]$ ein nicht-konstantes Polynom und sei L ein Zerfällungskörper von f. Dann gilt:

$$f \text{ ist durch Radikale auflösbar} \iff \mathrm{Gal}(L/K) \text{ ist auflösbar.}$$

Folgerung 3.48

Über einem Körper $K \subseteq \mathbb{C}$ ist jedes nicht-konstantes Polynom vom Grad höchstens 4 durch Radikale auflösbar.

Beweis: Sei L ein Zerfällungskörper von f. Dann operiert $G := \mathrm{Gal}(L/K)$ als Permutationsgruppe auf der Menge der Nullstellen von f, so dass $G \leq S_n$ ist, wobei $n := \deg(f)$ (siehe Aufgabe 24, Blatt 6). Nach Voraussetzung ist $2 \leq n \leq 4 \Rightarrow G \leq S_4$. Nun ist S_4 eine auflösbare Gruppe, da

$$\{\mathrm{Id}\} \leq \{\mathrm{Id}, (1\ 2)\} \leq \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq A_4 \leq S_4$$

eine Kette von Untergruppen wie im Satz 1.35 ist. Aus Satz 3.47 folgt, dass f durch Radikale auflösbar ist. ■

Aber es gibt Polynome vom Grad ≥ 5, die nicht durch Radikale auflösbar sind.

Bemerkung 3.49 (*Abel-Ruffini*)

Das Polynom $f := X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist nicht durch Radikale auflösbar.

Beweis: Nach dem Eisensteinskriterium (mit $p = 2$) ist f irreduzibel über $\mathbb{Z}$, also auch irreduzibel über $\mathbb{Q}$ nach dem Satz von Gauß (Teil (a)). Sei L ein Zerfällungskörper von f, und sei $G := \mathrm{Gal}(L/\mathbb{Q})$. Da $\deg(f) = 5$ ist, teilt 5 die Ordnung von G, also auch $[L : \mathbb{Q}]$.
Nun: man findet, dass f genau 3 reelle Nullstellen hat (verwende z.B. Sturmsche Ketten), also operiert die komplexe Konjugation ($\in \mathrm{Gal}(L/\mathbb{Q})$) als Transposition auf den 2 anderen Nullstellen von f. Daraus folgt, dass G Transpositionen enthält. Aber S_5 hat keine echte Untergruppe mit durch 5 teilbarer Ordnung, die Transpositionen enthält, also muss $G = S_5$ sein. Aber S_5 ist nicht auflösbar (siehe Bemerkung 1.36), und damit ist f nicht durch Radikale auflösbar. ■