# ALGEBRA, WINTERSEMESTER 2014

KARIN BAUR

ZUSAMMENFASSUNG. Algebra, Wintersemester 2014, KFU Graz.
Di 10.15 bis 11.45, Fr 10:15-11:45, jeweils SR 11.32.
Baut z.T. auf die Einführung in die Algebra auf.

## INHALTSVERZEICHNIS

## Vorbemerkung [Vorlesung 1, 3. Oktober 2014]

Zur Algebra gibt es sehr viele Textbücher, einige davon sind auf der Literaturliste von G. Lettl zu finden, [Le]. Als Grundlage für die Vorlesung wurde v.a. das Buch [Hu]verwendet. Die beiden Bücher von Jacobson, [Ja], sowie ein weiteres Buch von Hungerford, *Algebra*, sind ebenfalls Standard und empfehlenswert. Ausserdem gibt es neuere Bücher, wie etwa [JS], die ebenfalls empfehlenswert sind.

Ab Wintersemester 2014 ist die Vorlesung 4stündig. Der Stoffumfang ist dementsprechend vergrössert im Vergleich zur Algebra I vom Wintersemester 2013.

**Inhalt in Stichworten.**

- Gruppentheorie (Struktur endlicher Gruppen, Sylowsätze),
- Integritätsbereiche (eindeutige Faktorisierung in Polynomringen),
- Körpertheorie (normale und separable Körpererweiterungen, Zerfällungskörper),
- Galoistheorie (Fundamentalsatz der Galoistheorie, Auflösbarkeit mittels Radikalen),
- Modultheorie (Grundbegriffe).

# **Teil** 1. Gruppen

## 1. Symmetrische und alternierende Gruppen

1.1. **Vorbemerkungen.** Erinnerung: Permutationen einer Menge $M$ ($|M| = \infty$ erlaubt) sind bijektive Abbildungen $M \to M$. Die Permutationen von $M$ formen eine Gruppe (mit der Verknüpfung von Permutationen), die symmetrische Gruppe. Wird als $\mathrm{Perm}(M)$ geschrieben. Ist $M$ endlich, $|M| = n$, so schreibt man meistens $S_n$ für die Permutationsgruppe von $M$. $S_n$ hat $n!$ Elemente. Ist $\sigma$ ein Element von $S_n$, so schreiben wir $\sigma$ oft als $2 \times n$-Matrix, in der ersten Zeile stehen $1, 2, \ldots, n$, in der zweiten Zeile die $\sigma(i)$. Beispiel $M = \{1, 2, 3\}$, $S_3$ hat 6 Elemente, ein paar davon:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

**Satz 1.1** (Satz von Cayley)**.** *Jede Gruppe $G$ ist isomorph zu einer Untergruppe einer Permutationsgruppe.*

*Beweisstrategie.* Gesucht ist eine Untergruppe von $\mathrm{Perm}(M)$, die isomorph ist zu $G$. Dazu konstruiert man einen injektiven Homomorphismus $f : G \to \mathrm{Perm}(G)$. Dann gilt dann $G \cong \mathrm{im}(f)$.
Die Abbildung $f$ schickt $a \in G$ auf $\varphi_a : G \to G$, wobei $\varphi_a(g) := ag$ die Linksmultiplikation mit $a$ ist (überlegen: das ist bijektiv, i.e. $\varphi_a \in \mathrm{Perm}(G)$). Man muss überprüfen: $f$ ist ein injektiver Gruppenhomomorphismus. □

**Korollar 1.2.** *Jede endliche Gruppe $G$ der Ordnung $n$ ist isomorph zu einer Untergruppe von $S_n$.*

*Beweis.* Es ist $G \cong H$, mit $H \leq \mathrm{Perm}(G)$ nach dem Beweis von Satz 1.1, hier $\mathrm{Perm}(G) = S_n$. □

Daher ist es also wichtig, symmetrische Gruppen zu verstehen, wenn man endliche Gruppen beschreiben will. Unter den Untergruppen von $S_n$, die wir in diesem Kapitel behandeln werden, sind nicht-abelsche einfach Gruppen. Die sind besonders wichtig, sie sind die Grundbausteine für alle endlichen Gruppen.

**Beispiel.** Man schaue die symmetrische Gruppe $S_3$ an und ihre Untergruppen.

1.2. **Klassifikationsproblem für endliche Gruppen.** Gesucht ist eine Liste von Gruppen, so dass jede endliche Gruppe isomorph ist zu genau einer Gruppe von dieser Liste. (Schwieriges Problem).

**Bemerkung.** Teilresultate, bekannt aus der Einführung in die Algebra:

(1) Jede endliche zyklische Gruppe $G$ ist isomorph zu $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ für $n = |G|$.
(2) Strukturssatz für endliche abelsche Gruppen. Sei also $G$ endlich, abelsch, dann gilt $G$ ist direktes Produkt von endlichen zyklischen Gruppen der Ordnungen $d_1, \ldots, d_r$ für ein $r \geq 1$, wobei $d_1 \mid d_2 \mid \cdots \mid d_r$ gilt.

Ausserdem hilft der Satz von Lagrange weiter.

**Beispiele.**
a) Sei $p$ prim. Jede Gruppe der Ordnung $p$ ist isomorph zu $\mathbb{Z}_p$.
b) Ist $|G| = 4$, so gilt $G \cong \mathbb{Z}_4$ oder $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
c) Ist $|G| = 6$, so ist $G \cong \mathbb{Z}_6$ oder $G \cong S_3$.
(Bei b) und c) Satz von Lagrange verwenden).

Mit obigem Beispiel kann man die vollständige Klassifikation aller endlichen Gruppen der Ordnung $< 8$ hinschreiben:

| $\lvert G\rvert$ | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| $G \cong$ | $\mathbb{Z}_2$ | $\mathbb{Z}_3$ | $\mathbb{Z}_4$ oder $\mathbb{Z}_2 \times \mathbb{Z}_2$ | $\mathbb{Z}_5$ | $\mathbb{Z}_6$ oder $S_3$ | $\mathbb{Z}_7$ |

1.3. **Einfache Gruppen.** Spielen Schlüsselrolle bei dem Klassifikationsproblem endlicher Gruppen. Zur Erinnerung: $G$ beliebig, $G$ hat immer zwei normale Untergruppen, $G$ selbst und das Neutralelement $\{e\}$. Wir nennen diese die trivialen normalen Untergruppen. Ist die Untergruppe $H \leq G$ von $G$ normal in $G$, so schreiben wir $H \lhd G$.

**Definition.** Eine Gruppe $G \neq \{e\}$ heisst *einfach*, falls $G$ keine nicht-trivialen normalen Untergruppen hat.

**Beispiel.** $\mathbb{Z}_p$ ist einfach für jedes $p \in \mathbb{P}$: $\mathbb{Z}_p$ ist abelsch, jede Untergruppe $H \leq \mathbb{Z}_p$ ist daher normale Untergruppe. Nach Satz von Lagrange gilt: $|H|$ teilt $|\mathbb{Z}_p|$. Also ist $|H| \in \{1, p\}$ und damit $H = \{0\}$ oder $H = \mathbb{Z}_p$.

**Satz 1.3.** *$G$ ist eine einfache abelsche Gruppe $\iff$ $G \cong \mathbb{Z}_p$ für ein $p \in \mathbb{P}$.*

($\Longleftarrow$ gilt nach obigem Beispiel)

*Beweis.* (noch zu zeigen: $\Longrightarrow$) Sei $G$ einfach, abelsch. Jede U'Gr von $G$ ist normal. Die einzigen U'Gr. von $G$ sind also $\{e\}$ und $G$.
O.E. ist $G$ zyklisch, d.h. von einem Element erzeugt (w¨re $G$ von mehr als einem Element erzeugt, so würde man durch weglassen eines erzeugenden Elementes nicht-triviale Untergruppen finden, diese wären nicht-triviale Normalteiler).
Sei $a \in G$, $a \neq e$, mit $< a >= G$. Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}_m$ für ein $m$. Wäre $G$ unendlich, so wäre dann $G \cong \mathbb{Z}$. $\mathbb{Z}$ hat unendlich viele echte Untergruppen und kann daher nicht einfach sein.
Also ist $G$ endlich, $G$ zyklisch der Ordnung $m$.
Behauptung: $m$ ist prim.
Ann.: $m = t \cdot d$ mit $1 < d < m$. Dann hat $< a^t >$ die Ordnung $d$ und wäre eine Untergruppe von $G$, $\{e\} \neq < a^t > \neq G$, ein Widerspruch.
Also muss $G \cong \mathbb{Z}_p$ sein für ein $p \in \mathbb{P}$. □

Nicht-abelsche einfache Gruppen sind selten: es existieren nur 5 von Ordnung $< 1000$, nur 56 der Ordnung $< 1'000'000$. Alternierende Gruppen sind Beispiele von nicht-abelschen einfachen Gruppen (später mehr dazu).

**Einfache Gruppen als Grundbausteine** [Vorlesung 2, 7. Oktober 2014]

Sei $G$ endlich. $G$ hat also nur endlich viele Normalteiler $\neq G$ (und mindestens einen, $\{e\}$). Wir sehen nun, wie einfache Gruppen in beliebigen endlichen Gruppen als Grundbausteine auftreten. Wir benötigen vorher noch ein Resultat über Restklassen von Gruppen.

**Satz 1.4** (Beweis: [Hu], Kapitel 7)**.** *Sei $N \triangleleft G$, $K \leq G$ mit $N \subseteq K$. Dann gilt:*

(1) *$K/N \leq G/N$ ist Untergruppe*
(2) *$K/N \triangleleft G/N \iff K \triangleleft G$*
(3) *Ist $T \leq G/N$ Untergruppe, so ist $T = H/N$, wobei $H \leq G$ eine Untergruppe ist, die $N$ enthält (d.h. alle UGruppen von $G/N$ sind Restklassengruppen (nach $N$) von UGruppen von $G$).*

Ausserdem werden wir ab und zu folgende direkte Folgerung vom Satz von Lagrange verwenden (Beweis: selber überlegen):

**Lemma 1.5.** *Sei $N \triangleleft G$ eine normale Untergruppe von $G$. Ist $G$ endlich, so ist die Ordnung der Restklassengruppe $G/N$ gleich $|G|/|N|$.*

Sei nun $G$ eine endliche Gruppe.

- Sei $G_1 \triangleleft G$ mit $G_1 \neq G$, mit $|G_1|$ maximal.
  Beh.: $G/G_1$ ist einfach.
  Ann.: $G/G_1$ ist nicht einfach. Dann existiert ein nicht-trivialer Normalteiler

in $G/G_1$, der ist von der Form $M/G_1$ für einen Normalteiler $M \triangleleft G$ (Satz 1.4 (2) und (3)) mit $G_1 \lneq M \lneq G$, also $|M| > |G_1|$, Widerspruch.
Damit ist $G/G_1$ einfach.

- Ist $G_1 \neq \{e\}$: suchen $G_2 \triangleleft G_1$, $G_2 \neq G_1$, mit $|G_2|$ maximal. Analog wie vorher zeigt man $G_1/G_2$ ist einfach.
- Etc. (Ist $G_2 \neq \{e\}$, so finden wir $G_3 \triangleleft G_2$ $G_3 \neq G_2$, $|G_3|$ maximal, mit $G_2/G_3$ einfach.)
- Dieses Verfahren liefert eine Folge

$$G =: G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq \cdots \supsetneqq G_{n-1} \supsetneqq G_n = \{e\}$$

von Gruppen mit $\begin{cases} G_i \triangleleft G_{i-1} & \text{für } i = 1, \ldots, n \\ G_i/G_{i+1} \text{ einfach} & \text{für } i = 0, \ldots, n-1. \end{cases}$
(Im allgemeinen ist $G_i$ nicht Normalteiler in $G$!)

- Man nennt die einfachen Gruppen $G_i/G_{i+1}$ $(i = 0, \ldots, n-1)$ *Kompositionsfaktoren von* $G$.

**Bemerkung.** Man kann zeigen (Satz von Jordan-Hölder), dass die Kompositionsfaktoren von $G$ unabhängig von der Wahl der $G_i$ sind. Die Kompositionsfaktoren sind also vollständig durch die Struktur von $G$ bestimmt.

Die Strategie für das Klassifikationsproblem ist dann:

(i) Bestimmung aller einfachen Gruppen
(ii) Untersuchung, wie die Kompositionsfaktoren einer beliebigen Gruppe die Struktur der Gruppe bestimmen.

Teil (i) wurde 1981 erreicht, vollst. Liste aller einfachen Gruppen. Riesiger Aufwand, viele Gruppentheoretiker weltweit hatten daran gearbeitet. Der Beweis davon braucht ca. 10'000 Seiten.

**Bemerkung.** Die Liste der endlichen einfachen Gruppen ist genau die folgende:

- die zyklischen Gruppen deren Ordnung ein $p \in \mathbb{P}$ ist (das sind alle abelschen endlichen einfachen Gruppen);
- die alternierenden Gruppen[1] $A_n$ für $n > 4$;
- einfache Gruppen vom Lie-Typ (dazu kommen wir in dieser Vorlesung nicht). Das sind 16 unendliche Familien von einfachen Gruppen;
- eine der 26 sporadischen Gruppen (das sind 26 Gruppen, die nicht in die obigen drei Typen gehören - die letzte sporadische Gruppe, die man entdeckt hatte, wird das "Monster" genannt, wegen ihrer Grösse). Die kleinste sporadische Gruppe ist die Mathieu-Gruppe, $M_{11}$, sie hat 7920 Elemente. Die Grössenordnung der Monstergruppe liegt bei $10^{53}$ ([Ar]).

(Die alternierende Gruppe $A_3$ ist auch einfach, sie ist jedoch zyklisch, fällt also in den ersten Typ rein. $A_2$ ist die triviale Gruppe, also nicht einfach. Dass $A_4$ nicht einfach ist, muss man beweisen, siehe Satz 1.12).

[1]Definition weiter unten.

1.4. **Symmetrische Gruppen.** Sei $n \geq 2$, $S_n$ die Permutationsgruppe von $n$ Elementen.

Notationen: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} \in S_6$

$\rightsquigarrow \quad 2 \to 4 \to 6 \to 5 \to 2$, sowie $\overset{3}{\circlearrowleft}$ und $\overset{1}{\circlearrowleft}$ besser kurz: (2465).

- Jedes Elemen wird auf seinen rechten Nachbarn geschickt
- das Element ganz rechts wird auf das erste links geschickt
- Elemente, die nicht auftauchen, bleiben fix

Und formaler

**Definition.** Seien $a_1, \ldots, a_k$, $k \geq 1$ verschiedene Elemente von $\{1, 2, \ldots, n\}$. Dann ist $(a_1 a_2 \cdots a_k)$ die Permutation von $S_n$, die

$$\begin{cases} a_i \text{ auf } a_{i+1} \text{ schickt } (1 \leq i < k) \\ a_k \text{ auf } a_1 \text{ schickt} \\ \text{jedes andere Element von } \{1, 2, \ldots, n\} \text{ fest lässt} \end{cases}$$

$(a_1 a_2 \cdots a_k)$ heisst *Zykel der Länge $k$* oder *$k$-Zykel.*

**Beispiele.** a) In $S_4$ wird $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ durch (143) oder durch (314) oder durch (431) beschrieben.
b) In $S_n$ ist $(k)$ die Identität $(1 \leq k \leq n)$.

**Produkt/Komposition von Zykeln** Am Beispiel $S_4$
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ (Reihenfolge der Verknüpfung: von rechts nach links)

$$(243)(1243) \;=\; ? \;=\; (1423)$$

Elementweise durchführen: die 1 wird zur 2 (4-Zykel), dann zur 4 (im 3-Zykel). Also fängt das Resultat mit $1 \to 4$ an. Die 4 wird zur 3 (im 4-Zykel), dann zur 2 (im 3-Zykel). Also $1 \to 4 \to 2$. Dann die 2: die wird zur 4 (im 4-Zykel), dann zur 3. Zuletzt noch die 3, sie geht auf die 1 (im 4-Zykel), im 3-Zykel bleibt die 1 fest. Also geht die 3 wirklich auf die 1 und wir sind fertig.

**Übung.** Man überprüfe, dass $(243)(1243) \neq (1243)(243)$ ist.

**Definition.** Zwei Zykel heissen *disjunkt*, falls sie keine gemeinsamen Elemente haben.

**Lemma 1.6.** *Sind $\sigma = (a_1 a_2 \cdots a_k)$ und $\tau = (b_1 b_2 \cdots b_r)$ disjunkt, so gilt $\sigma\tau = \tau\sigma$.*

*Beweis.* Übung. □

**Satz 1.7.** *Jede Permutation in $S_n$ ist das Produkt von disjunkten Zykeln.*

*Beweisidee.* Ist $\tau =$id, so stimmt die Aussage.
Rest:

- Sei $a_1 \in \{1, \dots, n\}$ ein Element mit $\tau(a_1) \neq a_1$. Definiere $a_2 := \tau(a_1)$, $a_3 := \tau(a_2)$, etc. Sei $k$ minimal mit $\tau(a_k) \in \{a_1, \dots, a_{k-1}\}$ (so ein $k$ existiert sicher, da $\tau$ eine Bijektion ist).
  Beh.: Es ist $\tau(a_k) = a_1$ (sonst wäre $\tau$ nicht surjektiv). Dann operiert $\tau$ auf der Menge $\{a_1, \dots, a_k\}$ wie der Zykel $(a_1 \cdots a_k)$.
- Ist $k = n$, so sind wir fertig, es ist $\tau = (a_1 \cdots a_k)$.
- Ist $k < n$ und bleiben alle andern Elemente von $\{1, 2, \dots, n\}$ fix, so ist ebenfalls $\tau = (a_1, \cdots, a_k)$.
- Andernfalls sei $b_1 \in \{1, 2, \dots, n\} \setminus \{a_1, \dots, a_k\}$ mit $\tau(b_1) \neq b_1$. Man definiert $b_2 := \tau(b_1)$, $b_3 := \tau(b_2)$, etc.
  Beh.: Kein $\tau(b_i)$ ist Element von $\{a_1, \dots, a_k\}$ (sonst wäre $\tau$ nicht injektiv). Wie oben findet man $r$, so dass $\tau(b_r) = b_1$, $\tau$ operiert auf $\{b_1, \dots, b_r\}$ wie der $r$-Zykel $(b_1 b_2 \cdots b_r)$.
- So geht es weiter mit $c_1 \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k, b_1, \dots, b_r\}$ mit $c_1 \neq \tau(c_1)$ (falls keines existiert, sind wir fertig), etc.
- Dann gilt $\tau = (a_1 \cdots a_k)(b_1 \cdots b_r)(c_1 \cdots c_2) \cdots$ und diese Zykel sind alle disjunkt.

□

**Definition.** Ein 2-Zykel heisst eine *Transposition.*

Beobachtung:
Es ist $(12)(12) = (1) =$id und $(1234) = (14)(13)(12)$ (Achtung: nicht disjunkt)

**Korollar 1.8.** *Jede Permutation von $S_n$ ist ein Produkt von Transpositionen.*

*Beweis.* Nach Satz 1.7 ist jede Permutation ein Produkt von Zykeln. Bleibt zu zeigen: jeder Zykel ist ein Produkt von Transpositionen.

$$\begin{aligned} (a_1 \cdots a_k) &= (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2) \\ \text{oder} &= (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k) \end{aligned}$$

tun es (von re nach li vernküpfen). □

1.5. **Alternierende Gruppen.** Faktorisierungen als 2-Zykel sind nicht eindeutig, siehe obige Beispiele (Beweis von Korollar 1.8). So etwa

$$\begin{aligned} (123) &= (13)(12) \\ &= (13)(23)(12)(13) \\ &= (23)(13)(12)(13)(12)(23) \\ (1235) &= (15)(24)(24)(13)(23)(23)(12) \\ &= (13)(24)(35)(14)(24) \\ &= (15)(13)(12) \end{aligned}$$

((123) mittels 2,4,6 Transpositionen, (1235) mittels 7,5,3 Transpositionen)

**Lemma 1.9.** *Die Identität in $S_n$ kann nicht als Produkt einer ungeraden Anzahl von Transpositionen geschrieben werden.*

*Beweis.* Annahme, $(1) = \tau_k \cdots \tau_1$ mit $\tau_i$ Transpositionen, $k$ ungerade. Sei $c$ eine Zahl aus $\{1, 2, \ldots, n\}$, die in mindestens einem $\tau_i$ vorkommt, also in $\tau_r$ mit $r$ minimal, $\tau_r = (cd)$. Die Strategie ist, zu zeigen, dass man die Permutation so umformen kann, dass $\tau_{r+1}\tau_r = (cd)(cd)$ ist. D.h. wir können $\tau_{r+1}\tau_r$ aus der Permutation streichen.

- $c$ tritt nicht in $\tau_{r-1} \cdots \tau_1$ auf, bleibt also fest unter $\tau_{r-1} \cdots \tau_1$. Wäre $r = k$, so ginge $c$ auf $d$, Widerspruch (denn die Permutation ist die Identität).
- Also ist $r < k$. Wir betrachten $\tau_{r+1}$, es gibt vier mögliche Fälle für $\tau_{r+1}$ (mit $c, d, x, y$ vier **verschiedene** Elemente von $\{1, 2, \ldots, n\}$:

  $$(I): (xy) \quad (II): (xd) \quad (III): (cy) \quad IV: (cd)$$

  Dann sieht $\tau_{r+1}\tau_r$ so aus:

  $$(I): (xy)(cd) \quad (II): (xd)(cd) \quad (III): (cy)(cd) \quad IV: (cd)(cd)$$

- Im Fall (I) gilt: $(xy)(cd) = (cd)(xy)$, da die Transpositionen disjunkt sind. Man ersetzt $\tau_{r+1}\tau_r$ durch $\tau_r\tau_{r+1}$ und hat das erste Auftreten von $c$ eine Transposition nach links geschoben.
- Im Fall (II) gilt $(xd)(cd) = (xc)(xd)$ (selber nachprüfen). Man ersetzt $\tau_{r+1}\tau_r$ durch $(xc)(xd)$ und hat das erste Auftreten von $c$ um eine Transposition nach links geschoben.
- Im Fall (III) gilt $(cy)(cd) = (cd)(dy)$ (selber nachprüfen), analog wie bei (II) schiebt man das erste Auftreten von $c$ um eine Transposition nach links.
- Jedes Auftreten der Fälle (I)-(III) erlaubt also, $c$ um eine Transposition nach links zu schieben. Irgendwann muss der Fall (IV) auftreten (sonst könnte man $c$ bis in $\tau_k$ schieben, was wir ja bereits ausgeschlossen haben).
- Im Fall (IV) ist $(cd)(cd) = (1)$, diese zwei Transpositionen können gelöscht werden, also

  $$(1) = \tau_k \cdots \widehat{\tau_{r+1}}\,\widehat{\tau_r}\,\tau_{r-1} \cdots \tau_1$$

  Das Ganze kann man mit jedem Symbol, das irgendwo auftritt, durchspielen und sukzessive Paare von Transpositionen löschen. Falls $k$ ungerade war, endet das irgendwann in $(1) = (ab)$, Widerspruch.

□

**Satz 1.10.** *Ist $\alpha \in S_n$, so kann $\alpha$ nicht gleichzeitig als Produkt einer geraden und als Produkt einer ungeraden Anzahl von Transpositionen geschreiben werden.*

*Beweis.* Sei $\alpha \in S_n$ mit

$$\alpha = \sigma_1 \cdots \sigma_k = \tau_1 \cdots \tau_r$$

mit $\sigma_i$, $\tau_j$ Transpositionen, $k$ ungerade, $r$ gerade.

$$\begin{aligned}(1) = \alpha\alpha^{-1} &= (\sigma_1 \cdots \sigma_k)(\tau_1 \cdots \tau_r)^{-1} \\ &= \sigma_1 \cdots \sigma_k \tau_r^{-1} \cdots \tau_1^{-1} \\ &= \sigma_1 \cdots \sigma_k \tau_r \cdots \tau_1\end{aligned}$$

mit $k + r$ ungerade. Das ist im Widerspruch zu Lemma 1.9. □

[Vorlesung 3, 14. Oktober 2014]

**Definition.** $\alpha \in S_n$ heisst *gerade*, falls $\alpha$ als Produkt einer geraden Anzahl von Transpositionen geschrieben, *ungerade* im andern Fall.

**Beispiel.** $(1) = (12)(12)$ ist gerade, die Permutation $(134)(25) = (14)(13)(25)$ ist ungerade.

Mit Korollar 1.8 und Satz 1.10 gilt: jede Permutation ist entweder gerade oder ungerade.

(Zur Erinnerung: $n \geq 2$)

**Definition.** Die Menge aller geraden Permutationen von $S_n$ heisst die *alternierende Gruppe vom Grad* $n$, geschrieben $A_n$.

**Satz 1.11.** *Es gilt* $A_n \triangleleft S_n$ *und* $|A_n| = \frac{n!}{2}$, $(S_n : A_n) = 2$.

*Beweis.* Sei $f : S_n \to \mathbb{Z}_2$ definiert durch

$$f(\sigma) \mapsto \begin{cases} 0 & \sigma \text{ gerade} \\ 1 & \sigma \text{ ungerade} \end{cases}$$

$f$ ist wohldefiniert (keine Permutation kann sowohl gerade als auch ungerade sein). Beh.: $f$ ist $\underbrace{\text{surjektiver}}_{\text{ist einfach}}$ $\underbrace{\text{Gruppenhomomorphismus}}_{\text{ist einfach}}$ mit $\underbrace{\text{Kern } A_n.}_{\text{nach Definition}}$ Nun ist der Kern eines surjektiven Gruppenhomomorphismus ein Normalteiler, [EA], also $A_n \triangleleft S_n$. Nach dem Isomorphiesatz gilt dann $S_n/A_n \cong \mathbb{Z}_2$, also

$$2 = |\,\mathbb{Z}_2\,| = |S_n/A_n| \overset{\text{Lemma1.5}}{=} \frac{|S_n|}{|A_n|} = \frac{n!}{|A_n|},$$

also $|A_n| = n!/2$. Und mit dem Satz von Lagrange

$$(S_n : A_n) = \frac{|S_n|}{|A_n|} = \frac{n!}{n!/2} = 2$$

□

**Beispiele.** a) $(1)$, $(123)$, $(132) = (12)(13)$ in $S_3$ sind alle gerade. $A_3$ hat Ordnung $\frac{3!}{2} = 3$, also haben wir $A_3$ gefunden, $A_3 = \{(1), (123), (132)\}$. Zu welcher Gruppe ist $A_3$ isomorph?

b) $|A_4| = \frac{4!}{2} = 12$. Man kann zeigen: $A_4$ hat keine UGruppe der Ordnung 6, die Umkehrung des Satzes von Lagrange gilt also nicht.

**Bemerkung.** Man kann den Index 2 von $A_n$ in $S_n$ auch so illustrieren:
$S_n = A_n \dot\cup A_n(12)$ (Übung).

**Beispiel.** $A_4$ enthält eine normale Untergruppe, die nicht-trivial ist:
$N := \{(1), (12)(34), (13)(24), (14)(23)\} \lhd A_4$.

**Satz 1.12.** *Für $n \neq 2, 4$ ist die Gruppe $A_n$ einfach.*

(Ohne Beweis hier. Wichtiger Bestandteil beim Beweis: man zeigt, dass für $n \geq 3$ die alternierende Gruppen von den 3-Zykeln in $S_n$ erzeugt werden).

**Bemerkung.** Unter den alternierenden Gruppen sind nur $A_2$ und $A_3$ abelsch.

## 2. Sylow-Sätze

Die Hauptwerkzeuge, nicht-abelsche Gruppen zu verstehen, zu klassifizieren: Die Sylowsätze und die Aussage Konjugation $\leftrightsquigarrow$ Isomorphie.

Nicht-abelsche endliche Gruppen sind viel komplizierter als endliche abelsche Gruppen (die wir aus [EA] kennen).

Die Sylow-Sätze sind die ersten Schritte fürs Verstehen von nicht-abelschen endlichen Gruppen. Hier kommen zuerst die Aussagen mit Beispielen und Anwendungen, die Beweise erst nachher. Die Gruppen sind immer multiplikativ geschrieben.

### 2.1. Die Aussagen.

**Bemerkung.** Hauptthema ist der enge Zusammenhang

$$\text{Struktur einer Gruppe} \quad \leftrightsquigarrow \quad \text{arithmetische Eigenschaften von } |G|.$$

Mit dem Satz von Lagrange wissen wir schon: Ist $H \leq G$, so gilt $|H|$ teilt $|G|$. Der folgende Satz liefert eine partielle Umkehrung dazu.

**Satz 2.1** (Erster Sylowsatz)**.** *Sei $G$ endlich. Ist $p$ prim und teilt $p^k$ die Ordnung $|G|$ ($k \geq 0$), so besitzt $G$ eine U-Gruppe der Ordnung $p^k$.*

**Beispiel.** $|S_6| = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$. Der erste Sylowsatz sagt für
$p = 2$: $S_6$ besitzt UGruppen der Ordnung 2, 4, 8 und 16. Das können mehrere sein (es gibt mindestens 60 UGr der Ordnung 4).
$p = 3$: $\exists$ UGr. der Ordnung 3, 9.
$p = 5$: $\exists$ UGr. der Ordnung 5.

Gilt insbesondere $p \mid |G|$ für ein $p \in \mathbb{P}$, so enthält $G$ eine UGr. $K$ der Ordnung $p$ (Satz 2.1). Da $p$ prim ist, ist $K$ zyklisch, $K =< a >$ für ein $a$ ein Element von $G$ der Ordnung $p$, damit hat man folgende Aussage bereits:

**Korollar 2.2** (Satz von Cauchy)**.** *Sei $G$ endlich, $p \mid |G|$ mit $p \in \mathbb{P}$. Dann gilt: $G$ enthält ein Element der Ordnung $p$.*

**Definition.** Sei $G$ endlich, $p \in \mathbb{P}$. Sei $n$ maximal, so dass $p^n$ die Ordnung $|G|$ teilt. Ist $H$ eine UGr. von $G$ der Ordnung $p^n$, so heisst $H$ *$p$-Sylow-Untergruppe*. Solche existieren nach Satz 2.1.

(Ist $G$ eine Gruppe, in der jedes Element Ordnung eine Potenz von $p$ hat, mit $p$ prim, so sagt man, $G$ sei eine $p$-Gruppe).

**Beispiel.** Sei $G = S_4$. Jede UGruppe von $G$ der Ordnung 8 ist eine 2-Sylow-Untergruppe. Jede UGruppe von $G$ der Ordnung 3 ist eine 3-Sylow-Untergruppe. Übung: Suchen Sie Beispiele von $p$-Sylow-Untergruppen für $p = 2, 3$.

**Beispiel.** Sei $p \in \mathbb{P}$ und $G$ eine endliche abelsche Gruppe der Ordnung $p^n m$ mit $p \nmid m$. Dann ist

$$G(p) := \{a \in G \mid a^{p^k} = e \text{ für ein } k \geq 0\}$$

eine $p$-Sylow-Untergruppe von $G$, denn $G(p)$ hat Ordnung $p^n$. (Dass $G(p)$ Ordnung $p^n$ hat, soll man selber überprüfen). Wir werden später sehen: $G(p)$ ist die einzige $p$-Sylow-Untergruppe von $G$. Nach dem Struktursatz über endliche abelsche Gruppen ist $G$ das direkte Produkt all ihrer Sylow-Untergruppen (eine für jede Primzahl, die $|G|$ teilt).

Sei $G$ eine Gruppe, $x \in G$. Die Abbildung $f : G \to G$, $f(a) = x^{-1}ax$, ist ein Isomorphismus ([EA], siehe Definition von Normalteilern). Ist $K$ eine Untergruppe von $G$, so ist $x^{-1}Kx = \{x^{-1}kx \mid k \in K\}$ das Bild von $K$ unter $f$. Das ist eine Untergruppe von $G$, die isomorph ist zu $K$, die Ordnungen von $x^{-1}Kx$ und $K$ sind gleich. Daher gilt:

**Bemerkung.** Ist $K$ eine $p$-Sylow-Untergruppe, so ist $x^{-1}Kx$ ebenfalls eine $p$-Sylow-Untergruppe, für jedes $x \in G$.

Der nächste Satz zeigt, dass wir jede $p$-Sylow-Untergruppe so erhalten:

**Satz 2.3** (Zweiter Sylow-Satz)**.** *Sind $P$ und $K$ zwei $p$-Sylow-Untergruppen von $G$, so existiert ein $x \in G$ mit $P = x^{-1}Kx$.*

**Korollar 2.4.** *Sei $G$ eine endliche Gruppe, $p \in \mathbb{P}$.*

1. *Je zwei $p$-Sylow-Untergruppen von $G$ sind isomorph.*
2. *Eine $p$-Sylow-Untergruppe $K$ von $G$ ist normal in $G$ genau dann, wenn sie die einzige $p$-Sylow-Untergruppe von $G$ ist.*

*Beweis.* Teil 1 folgt sofort aus Satz 2.3 und der obigen Bemerkung.

Teil 2: $\Longleftarrow$ $x^{-1}Kx$ ist eine $p$-Sylow-Untergruppe für jedes $x \in G$. Ist $K$ die einzige $p$-Sylow-Untergruppe von $G$, so gilt also $x^{-1}Kx = K$ für jedes $x \in G$, also $K \lhd G$.

$\Longrightarrow$ Sei umgekehrt $K \triangleleft G$, sei $P$ eine beliebige $p$-Sylow-Untergruppe von $G$. Nach Satz 2.3 existiert $x \in G$ mit $P = x^{-1}Kx$. Da $K$ normal ist, muss jedoch $x^{-1}Kx = K$ sein, also $P = K$. □

Bis jetzt wissen wir, dass $p$-Sylow-Untergruppen existieren und wie sie zusammenhängen. Der nächste Satz zeigt, wieviele $p$-Sylow-Untergruppen eine Gruppe $G$ haben kann.

**Satz 2.5** (Dritter Sylow-Satz)**.** *Die Anzahl der $p$-Sylow-Untergruppen einer endlichen Gruppe $G$ ist ein Teiler von $|G|$ und ist gleich $1 + kp$ für ein $k \geq 0$.*

2.2. **Anwendungen der Sylow-Sätze.** Einfache Gruppen sind ja die Grundbausteine aller Gruppen. Dazu ist es nützlich, zu wissen, ob eine Gruppe Untergruppen einer gegebenen Ordnung hat. Es ist möglich, den dritten Sylow-Satz (Satz 2.5) mit Korollar 2.4. 2) zu verwenden, um die Existenz von echten Normalteilern einer Gruppe $G$ zu zeigen. Insbesondere zeigt man damit, dass dann $G$ nicht einfach ist.

**Beispiel.** Eine Gruppe der Ordnung 63 kann nicht einfach sein. Übung.

**Beispiel.** Behauptung: es gibt keine einfache Gruppe der Ordnung $56 = 2^3 \cdot 7$.

Sei $G$ eine Gruppe der Ordnung 56. Die einzigen Teiler von 56 der Form $1 + 7k$ sind 1 und 8. $G$ hat also entweder eine oder acht 7-Sylow-Untergruppen.
Fall A) Falls es nur eine ist, so ist sie normal (Korollar 2.4) und dann ist $G$ nicht einfach.
Fall B) Hat $G$ acht 7-Sylow-Untergruppen, so hat jede davon sechs Elemente verschieden von $e$. Jedes dieser Elemente muss Ordnung 7 haben (Folge aus dem Satz von Lagrange). Zwei verschiedene Untergruppen von $G$, die beide dieselbe Primzahl als Ordnung haben, haben nur $e$ als gemeinsames Element (Übung). D.h. die acht verschiedenen 7-Sylow-Untergruppen besitzen zusammen $8 \cdot 6 = 48$ Elemente der Ordnung 7 in $G$. Neben $e$ sind noch 7 Elemente übrig. Jede 2-Sylow-Untergruppe von $G$ muss Ordnung 8 haben. Die Elemente einer solchen haben als Ordnung einen Teiler von 8, sind also sicher nicht von Ordnung 7, d.h. sie gehören sicher zur Restmenge der 7 Elemente oder sind gleich $e$. D.h. es kann nur eine 2-Sylow-Untergruppe der Ordnung 8 geben, die ist dann ein Normalteiler (Korollar 2.4) und $G$ ist nicht einfach.

**Korollar 2.6.** *Sei $G$ eine Gruppe der Ordnung $pq$, mit $p$ und $q$ prim, $p > q$. Gilt $q \nmid (p-1)$, so ist $G \cong \mathbb{Z}_{pq}$.*

*Beweis.* Die einzigen Teiler von $|G|$ sind 1, $p$, $q$ und $pq$. Daher hat $G$ entweder eine oder $q$ $p$-Sylow-Untergruppen (Satz 2.5), und weil $q$ nicht als $1 + kp$ geschrieben werden kann mit $k > 0$ (denn $p > q$), muss es eine $p$-Sylow-Untergruppe $H$ von $G$ sein, die Ordnung $p$ hat, sie ist dann auch normal (Korollar 2.4).

Fast analog hat $G$ nur eine $q$-Sylow-Untergruppe $K$ der Ordnung $q$ ($G$ kann nicht $p = 1 + kq$ $p$-Sylow-Untergruppen haben mit $k > 0$, da nach Voraussetzung $q \nmid (p-1)$ gilt). Diese ist auch ein Normalteiler.

Der Durchschnitt $H \cap K$ ist eine Untergruppe von $H$ und von $K$, ihre Ordnung teilt (Satz von Lagrange) also $q$ und $p$, ist also $= 1$, $H \cap K = \{e\}$. Dann ist $G = HK$ (überlegen), also $G \cong H \times K$. Wir wissen auch, dass $H \cong \mathbb{Z}_p$ und $K \cong \mathbb{Z}_q$ sind. Und es gilt, da $\mathrm{ggT}(p, q) = 1$ ist, dass $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ ([EA]). □

2.3. **Die Beweise.** [Vorlesung 4, 17. Oktober 2014]

Zur Erinnerung: Ist $G$ eine Gruppe und $a, b \in G$, so sagen wir, $a$ ist *konjugiert* zu $b$, falls ein $x \in G$ existiert mit $b = x^{-1}ax$. So ist beispielsweise die Transposition $(12)$ konjugiert zu $(13)$ in $S_3$, da gilt

$$(123)^{-1}(12)(123) = (132)(12)(123) = (13).$$

Wir werden folgende Tatsache ausnutzen:

**Lemma 2.7.** *Die Konjugation ist eine Äquivalenzrelation auf $G$.*

(Selber überlegen).

Die Äquivalenzklassen von $G$ unter der Konjugation heissen die *Konjugationsklassen von $G$*. Zwei Konjugationsklassen sind entweder disjunkt oder gleich, $G$ ist die disjunkte Vereinigung seiner verschiedenen Konjugationsklassen.

**Beispiel.** Wir betrachten $G = S_3$. Die Konjugationsklasse von $(12)$ ist gerade $\{(12), (23), (13)\}$. (Man kann nachrechnen, dass für jedes $x \in S_3$ das Element $x^{-1}(12)x$ eines der drei hier ist). Man rechnet nach, dass es drei verschiedene Konjugationsklassen in $S_3$ gibt:

$$\{(1)\} \qquad \{(123), (132)\} \qquad \{(12), (23), (13)\}.$$

Man beachte: die Anzahl der Elemente in einer Konjugationsklasse von $S_3$ teilt die Ordnung von $S_3$.

**Definition.** Sei $G$ eine Gruppe, $a \in G$. Der *Zentralisator von $a$*, geschrieben $Z(a)$, ist die Menge aller Elemente von $G$, die mit $a$ kommutieren:

$$Z(a) := \{g \in G \mid ga = ag\}.$$

Ist beispielsweise $G = S_3$ und $a = (123)$, so ist $Z(a) = \{(1), (123), (132)\}$ und das ist eine Untergruppe von $S_3$. Ist $a$ ein Element der multiplikativen Gruppe $\mathbb{Q}^* = \mathbb{Q} \setminus \{0, \cdot\}$, so ist $Z(a) = \mathbb{Q}^*$.

**Lemma 2.8.** *Ist $G$ eine Gruppe, $a \in G$, so ist $Z(a) \leq G$ eine Untergruppe.*

*Beweis.* (Ist klar! Beweis in Vorlesung weggelassen)
Wegen $ae = ea$ ist sicher $e \in Z(a)$, also ist $Z(a)$ nicht leer. Sind $g, h \in Z(a)$, so gilt

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh),$$

also kommutieren $a$ und $gh$, $Z(a)$ ist abgeschlossen. Zu den Inversen: multiplizieren wir $ga = ag$ von links und von rechts mit $g^{-1}$, so erhalten wir $ag^{-1} = g^{-1}a$, also ist mit $g \in Z(a)$ auch $g^{-1}$ in $Z(a)$, $Z(a)$ ist eine Untergruppe. □

**Satz 2.9.** *Sei $G$ eine endliche Gruppe, $a \in G$. Dann gilt: Die Kardinalität der Konjugationsklasse von $a$ ist gleich dem Index $(G : Z(a))$ vom Zentralisator in $G$, sie teilt also $|G|$.*

*Beweis.* Seien $x, y \in G$. Dann gilt

$$\begin{aligned} x^{-1}ax = y^{-1}ay &\iff a = xy^{-1}ayx^{-1} \\ &\iff a = (yx^{-1})^{-1}a(yx^{-1}) \\ &\iff (yx^{-1})a = a(xy^{-1}) \\ &\iff yx^{-1} \in Z(a) \\ &\iff Z(a)y = Z(a)x \end{aligned}$$

Die Elemente $x$ und $y$ geben also das gleiche Konjugierte von $a$ genau dann, wenn $x$ und $y$ zur gleichen Nebenklasse von $Z(a)$ gehören. Anders gesagt: liegen $x$ und $y$ in verschiedenen Nebenklassen von $Z(a)$, so gilt $x^{-1}ax \neq y^{-1}ay$. $G$ ist die (disjunkte) Vereinigung der verschiedenen Nebenklassen, sagen wir

$$G = Z(a)x_1 \dot\cup Z(a)x_2 \dot\cup \cdots \dot\cup Z(a)x_t$$

für ein $t \geq 1$. Die Konjugierten von $a$ findet man unter den Elementen $z^{-1}az$ $(z \in G)$, also haben wir genau $t$ zu $a$ konjugierte Elemente:

$$x_1^{-1}ax_1, x_2^{-1}ax_2, \ldots, x_t^{-1}ax_t$$

und $t = (G : Z(a))$ ist gerade die Anzahl der Nebenklassen. Dass $t$ die Ordnung $|G|$ von $G$ teilt, folgt mit dem Satz von Lagrange. □

**Klassengleichung** Wir benutzen das obige Resultat, um die sogenannte Klassengleichung von $G$ herzuleiten: Seien $C_1 \cup \cdots \cup C_t$ die verschiedenen Konjugationsklassen einer Gruppe $G$. Da diese paarweise disjunkt sind, ist

$$|G| = |C_1 \cup \cdots \cup C_t| = |C_1| + |C_2| + \cdots + |C_t| \tag{1}$$

Wenn wir nun für jedes $C_i$ ein Element $a_i \in C_i$ wählen, so ist $C_i$ gerade die Menge der zu $a_i$ konjugierten Elemente, mit $|C_i| = (G : Z(a_i))$ nach Satz 2.9. Die Gleichung hier kann man dann wie folgt schreiben:

$$|G| = (G : Z(a_1)) + (G : Z(a_2)) + \cdots + (G : Z(a_t)) \tag{2}$$

und das ist die (zweite Version der) *Klassengleichung von $G$*. Sie wird sehr nützlich sein, wenn wir die Sylow-Sätze beweisen.

**Beispiel.** Im ersten Beispiel von Kapitel 2.3 haben wir die Konjugationsklassen von $S_3$ notiert, sie haben 1, 2 bzw. 3 Elemente. Die Klassengleichung von $S_3$ ist also $6 = 1 + 2 + 3$.

Sind $c$ und $x$ Elemente von $G$, so gilt $cx = xc$ genau dann, wenn $x^{-1}cx = c$ ist. Also ist $c$ im *Zentrum*[2] *von* $G$, $Z(G)$, genau dann, wenn $c$ genau ein zu $c$

[2]Das Zentrum von $G$ sind die Menge aller Elemente $c$ mit $xc = cx$ für jedes $x \in G$.

konjugiertes Element hat, sich selbst nämlich. Also ist das Zentrum von $G$, $Z(G)$ die Vereinigung aller ein-elementigen Konjugationsklassen von $G$. Damit kann man die Klassengleichung nochmals anders aufschreiben:

$$|G| = |Z(G)| + |C_1| + |C_2| + \dots |C_r|, \tag{3}$$

wobei die $C_i$ $(i = 1, \dots, r)$ diejenigen Konjugationsklassen von $G$ sind, die mind. zwei Elemente haben und jedes $|C_i|$ die Ordnung $|G|$ teilt.

Ein weiteres Resultat ist wichtig für den Beweis der Sylow-Sätze (Bemerkung: das Korollar 2.2 ist eine Folge des ersten Sylow-Satzes).

**Lemma 2.10** (Satz von Cauchy für endliche abelsche Gruppen)**.** *Ist $G$ eine endliche abelsche Gruppe und $p$ eine Primzahl, die die Ordnung von $G$ teilt, so enthält $G$ ein Element der Ordnung $p$.*

Dies folgt aus dem Strukturs atz für endliche abelsche Gruppen. Man könnte es auch direkt mit Induktion über die Ordnung von $G$ zeigen.

*Beweis des ersten Sylow-Satz (Satz 2.1).* Der Beweis benutzt Induktion über die Ordnung von $G$. (Und zeigt konkret, wie man eine UGr findet wie in der Aussage von Satz 2.1). Falls $|G| = 1$ ist, so ist $p^0$ die einzige Primpotenz, die $|G|$ teilt, $G$ ist selber eine Untergruppe der Ordnung $p^0$.
Sei also $|G| > 1$ und wir nehmen an, die Aussage gelte für Gruppen der Ordnung $< |G|$. Ist $k = 0$, so ist die Aussage für $G$ klar (wie oben). Wir können also o.E. annehmen, dass $k > 0$ gilt.

Die zweite und dritte Version der Klassengleichung liefern kombiniert:

$$|G| = |Z(G)| + (G : Z(a_1)) + \dots + (G : Z(a_r))$$

mit $(G : Z(a_i)) > 1$ für $i = 1, \dots, r$. Ausserdem ist $|Z(G)| \geq 1$ (da $e \in Z(G)$ liegt) und $|Z(a_i)| < |G|$ für jedes $i$ (sonst wäre $(G : Z(a_i)) = 1$).

A) Wir nehmen zuerst an, dass ein $j$ existiert, so dass $p$ *nicht* $(G : Z(a_j))$ teilt. Nach Voraussetzung teilt $p^k$ die Ordnung $|G|$ und es ist $|G| = |Z(a_j)| \cdot (G : Z(a_j))$ (S.v. Lagrange), also muss $p^k$ die Ordnung der UGruppe $Z(a_j)$ teilen (mit $k \geq 1$).

Wegen $|Z(a_j)| < |G|$ können wir die Induktionshypothese für die Gruppe $Z(a_j)$ anwenden: $Z(a_j)$ (und damit $G$!) besitzt also eine Untergruppe der Ordnung $p^k$.

B) Teilt andrerseits $p$ den Index $(G : Z(a_i))$ für jedes $i$, so muss $p$ (da es die Ordnung von $G$ teilt) die Zahl $|G| - (G : Z(a_1)) - \dots - (G : Z(a_r)) = |Z(G)|$ teilen. Da das Zentrum $Z(G)$ abelsch ist, folgt mit Lemma 2.10, dass $Z(G)$ ein Element $c$ der Ordnung $p$ enthält. Sei $N$ die zyklische Gruppe, die von $c$ erzeugt wird. $N$ hat Ordnung $p$ und ist normal in $G$ (Übung). Daher ist die Ordnung $|G|/p$ der Quotientengruppe $G/N$ echt kleiner als $|G|$ und durch $p^{k-1}$ teilbar. Nach Induktionsannahme besitzt $G/N$ also eine Untergruppe $T$ der Ordnung $p^{k-1}$. Und mit Satz 1.4 wissen wir, dass eine UGr $H$ von $G$ existiert mit mit $N \subseteq H$ und

$T = H/N$. Der Satz von Lagrange liefert

$$|H| = |N| \cdot |H/N| = |N| \cdot |T| = pp^{k-1} = p^k.$$

Also hat $G$ im Fall B) auch eine Untergruppe der Ordnung $p^k$. □

Die Beweise der andern beiden Sylow-Sätze benutzen ähnliche Methoden. Hier arbeiten wir jedoch mit konjugierten Untergruppen anstatt mit konjugierten Elementen. Ist $H$ eine Untergruppe von $G$ und $A$ und $B$ zwei beliebige UGr von $G$, so sagt man, $A$ sei *$H$-konjugiert zu $B$*, falls ein $x \in H$ existiert mit

$$B = x^{-1}Ax = \{x^{-1}ax \mid a \in A\}.$$

Falls $H = G$ ist, so sagt man $A$ sei *konjugiert zu $B$*.

**Lemma 2.11.** *Sei $H \leq G$. Dann ist $H$-Konjugiertheit eine Äquivalenzrelation auf der Menge aller Untergruppen von $G$.*

(ebenfalls selber überlegen, analog wie Lemma 2.7).

Sei $A$ eine Untergruppe einer Gruppe $G$. Der *Normalisator von $A$* ist die Menge

$$N(A) := N_G(A) := \{g \in G \mid g^{-1}Ag = A\}.$$

**Satz 2.12.** *Ist $A \leq G$, so ist $N(A) \leq G$ und $A$ ist eine normale Untergruppe von $N(A)$.*

*Beweis.* Es ist $A \subseteq N(A)$ und es gilt $g \in N(A) \iff Ag = gA$
Aus $g \in N(A)$ folgt natürlich $Ag = gA$.
Für die Umkehrung ($Ag = gA \Longrightarrow g \in N(A)$):
a) $Ag = gA \Longrightarrow gAg^{-1} \subseteq A$:
Sei $Ag = gA$. Dann folgt, dass für jedes beliebige $a \in A$ ein $b \in A$ existiert mit $ag = ba$. Daraus folgt, dass für dieses $a$ gilt $gag^{-1} = b \in A$, also gilt sicher $gAg^{-1} \subseteq A$.
b) $gAg^{-1} \subseteq A \Longrightarrow gAg^{-1} = A$:
Für $a \in A$ beliebig ist $a = g(g^{-1}ag)g^{-1} \in gAg^{-1}$, also ist $a \in gAg^{-1}$.

Damit kann man den Beweis von Lemma 2.8 einfach anpassen und zu zeigen, dass $N(A)$ eine Untergruppe von $G$ ist. Dass $A$ normale UGr von $N(A)$ ist folgt aus der Definition von $N(A)$. □

**Satz 2.13.** *Seien $H$ und $A$ zwei Untergruppen der endlichen Gruppe $G$. Die Anzahl der verschiedenen $H$-Konjugierten von $A$ ist gleich $(H : H \cap N(A))$ und teilt damit $|H|$.*

*Beweis.* Analog zum Beweis von Satz 2.9, man muss einfach $G$ durch $H$ ersetzen, $a$ durch $A$ und $Z(a)$ durch $H \cap N(A)$. □

**Lemma 2.14.** *Es sei $Q$ eine $p$-Sylow Untergruppe einer endlichen Gruppe $G$. Ist die Ordnung des Elements $x \in G$ eine Potenz von $p$ und gilt $x^{-1}Qx = Q$, so ist $x \in Q$.*

*Beweis.* Da $Q$ Normalteiler von $N(Q)$ ist (Satz 2.12), ist die Restklassengruppe $N(Q)/Q$ definiert. Nach Voraussetzung liegt $x$ in $N(Q)$. Da die Ordnung $|x|$ von $x$ eine Potenz von $p$ ist, ist die Ordnung der Nebenklasse $Qx$ in $N(Q)/Q$ ebenfalls eine Potenz von $p$.
Sei $T$ die von $Qx$ erzeugte zyklische Untergruppe von $N(Q)/Q$, die Ordnung von $T$ ist dann eine Potenz von $p$. Nach Satz 1.4 ist $T = H/Q$, für eine Untergruppe $H$ von $G$ ist, die $Q$ enthält. Da die Ordnungen der Gruppen $Q$ und $T$ beides Potenzen von $p$ sind und nach dem Satz von Lagrange $|H| = |Q| \cdot |T|$ ist, muss $|H|$ ebenfalls eine Potenz von $p$ sein. Da $Q \subseteq H$ und $|Q|$ die grösste Potenz von $p$ ist, die die Ordnung $|G|$ teilt, muss $Q = H$ sein und $T = H/Q$ die triviale Untergruppe sein. Damit muss der Erzeuger $Qx$ von $T$ die Identitätsnebenklasse $Qe$ sein. Aus der Gleichheit $Qx = Qe$ folgt $x \in Q$. □

[Vorlesung 5, 21. Oktober 2014]

*Beweis des zweiten Sylow-Satzes, Satz 2.3.* *Idee:* Man schaut sich die konjugierten von $K$ (unter Elementen aus $G$) an, sei $S = \{K_1 = K, K_2, \dots, K_t\}$ die Menge der zu $K$ konjugierten UGruppen von $G$. Dann muss man zeigen, dass $P$ eine der $K_j$ ist. Dazu schaut man die $P$-konjugierten von den $K_i$ in $S$ an.
Da $K$ eine $p$-Sylow-Untergruppe von $G$ ist, hat $K$ Ordnung $p^n$, für $|G| = p^n \cdot m$ mit $p \nmid m$. Seien $K = K_1, K_2, \dots, K_t$ die verschiedenen Konjugierten von $K$. Nach Satz 2.13 (mit $H = G$ und $K = A$) ist $t = (G : N(K))$. Dabei kann $p$ kein Teiler von $t$ sein (Denn: es ist $p^n m = |G| = |N(K)| \cdot (G : N(K)) = |N(K)| \cdot t$ und $p^n$ teilt $|N(K)|$, da $K$ eine UGr von $N(K)$ ist). Wir müssen zeigen, dass die $p$-Sylow Untergruppe $P$ (aus dem 2. Sylow-Satz) konjugiert ist zu $K$, d.h. dass $P$ eines der $K_i$ ist. Wir nutzen dazu die Äquivalenzrelation "$P$-Konjugiertheit" auf der Menge $S$ aus.

Jede Konjugierte von $K_i$ ist eines der $K_j$. Also enthält die Äquivalenzklasse von $K_i$ unter $P$-Konjugiertheit nur verschiedene der $K_j$ und keine anderen Untergruppen. Somit ist die Menge $S = \{K_1, K_2, \dots, K_t\}$ aller zu $K$ Konjugierten eine Vereinigung verschiedener Äquivalenzklassen unter $P$-Konjugiertheit. Die Anzahl der UGruppen in jeder diese Äquivalenzklassen ist eine Potenz von $p$, da nach Satz 2.13 die Anzahl der UGruppen, die $P$-konjugiert zu $K_i$ sind, gleich $(P : P \cap N(K_i))$ ist und das ein Teiler von $|P| = p^n$ ist (nach dem S. v. Lagrange). Die Zahl $t$ (der Anzahl UGruppen in der Menge $S$) ist dann Summe von diversen Potenzen von $p$ (jedes davon ist die Anzahl von UGruppen in einer der verschiedenen Äquivalenzklassen deren Vereinigung gleich $S$ ist). Da $p$ die Zahl $t$ nicht teilt, muss wenigstens eine dieser Potenzen von $p$ gleich $p^0 = 1$ sein. Also muss eines der $K_j$ eine Äquivalenklasse für sich selbst sein, d.h. es ist $x^{-1}K_j x = K_j$ für jedes $x \in P$. Lemma 2.14 impliziert (mit $Q = K_i$), dass $x \in K_i$ ist für jedes solche $x$, also $P \subseteq K_j$. Da $P$ und $K_j$ beides $p$-Sylow-Untergruppen sind, müssen sie die gleiche Ordnung haben, d.h. $P = K_j$. □

*Beweis des dritten Sylow-Satzes, Satz 2.5.* Sei $S = \{K_1, \ldots, K_t\}$ die Menge aller $p$-Sylow-Untergruppen von $G$. Nach dem zweiten Sylow-Satz sind die Elemente von $S$ alle ($G$-)Konjugierte von $K_1$. Mit Satz 2.13 ist also $t = (G : N(K_1))$ und wegen dem Satz von Lagrange teilt damit $t$ die Ordnung von $G$.
Sei $P$ eines der $K_i$, wir betrachten die $P$-Konjugiertheit. Die einzige $P$-Konjugierte von $P$ ist $P$ selbst (Abgeschlossenheit). Der Beweis des zweiten Sylow-Satzes zeigt, dass die einzige Äquivalenzklasse (unter $P$-Konjugiertheit), die aus einer einzigen U-Gruppe besteht, die Klasse der Gruppe $P$ selbst ist. Der Beweis zeigt auch, dass $S$ die Vereinigung von verschiedenen Äquivalenzklassen ist und dass die Anzahl der Untergruppen in jeder Klasse eine Potenz der Zahl $p$ ist. Nur eine dieser Klassen enthält $P$, also muss die Anzahl der UGruppen in jeder andern eine positive Potenz von $p$ ist. Daher ist die Anzahl $t$ der $p$-Sylow-Untergruppen gleich 1+ diverse positive Potenzen von $p$, kann also geschrieben werden als $1 + kp$ für ein $k \geq 0$. □

Eine weitere Folgerung der Sylow-Sätze ist z.B., dass für jede Gruppe $G$ der Ordnung 21 gilt, dass $G \cong \mathbb{Z}_{21}$ oder $G$ von zwei Elementen $x, y$ erzeugt wird mit $x^7 = e$, $y^3 = e$ und $yx = x^2y$.

## 3. Struktur endlicher Gruppen

Wir verwenden nun einige Resultate aus dem Kapitel 2, um die Struktur endlicher Gruppen zu bestimmen. Wir können dann insbesondere alle Gruppen bis und mit Ordnung 15 angeben.

**Satz 3.1.** *Ist $G$ eine Gruppe der Ordnung $p^n$, wobei $p$ prim ist und $n \geq 1$, so besteht das Zentrum $Z(G)$ aus mehr als einem Element. Insbesondere gilt $|Z(G)| = p^k$ für ein $1 \leq k \leq n$.*

*Beweis.* Nach dem Satz von Lagrange ist $|Z(G)| = p^k$ (mit $0 \leq k \leq n$). Wir müssen nur noch zeigen, dass $k \geq 1$ ist. Die dritte Form der Klassengleichung, (3), zeigt

$$|Z(G)| = |G| - |C_1| - \cdots - |C_r|$$

wobei für jedes $1 \leq i \leq r$ gilt: $|C_i| \geq 2$ und $|C_i|$ teilt $|G| = p^n$. Die Ordnungen der $C_i$ sind also auch positive Potenzen von $p$. Also ist jedes $|C_i|$ durch $p$ teilbar, $|G|$ ist sowieso durch $p$ teilbar. Damit muss auch $|Z(G)|$ durch $p$ teilbar sein. □

**Korollar 3.2.** *Es gibt keine einfache Gruppe der Ordnung $p^n$ ($p$ prim und $n > 1$).*

*Beweis.* Sei $|G| = p^n$ mit $n > 1$. Das Zentrum $Z(G)$ ist ein Normalteiler von $G$. Ist $Z(G) \neq G$, so ist also $Z(G)$ ein nicht-trivialer Normalteiler in $G$. Ist $Z(G) = G$, so ist $G$ abelsch und kann dann nach Satz 1.3 nicht einfach sein. □

**Korollar 3.3.** *Ist $G$ eine Gruppe der Ordnung $p^2$, $p$ prim, so ist $G$ abelsch. Damit ist $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

*Beweis.* Nach dem Satz von Lagrange und nach Satz 3.1 hat das Zentrum von $G$ Ordnung $p$ oder Ordnung $p^2$. Falls $Z(G)$ Ordnung $p^2$ hat, so ist $G = Z(G)$, also $G$ abelsch. Hat $Z(G)$ Ordnung $p$, dann hat die Restklassengruppe $G/Z(G)$ Ordnung $p^2/p = p$ nach Lemma 1.5. Also ist $G/Z(G)$ eine zyklische Gruppe und daher ist $G$ abelsch (Übungsaufgabe, vermutlich Blatt 5). Der letzte Teil folgt dann mit dem Struktursatz für endliche abelsche Gruppen ([EA]). □

In Korollar 2.6 haben wir gewisse Gruppen der Ordnung $pq$ charakterisiert. Nun können wir analog eine Aussage über Gruppen der Ordnung $p^2q$ beweisen:

**Lemma 3.4.** *Seine $p \neq q$ zwei Primzahlen mit $q \not\equiv 1$ (mod $p$) und $p^2 \not\equiv 1$ (mod $q$). Ist $G$ eine Gruppe der Ordnung $p^2q$, so ist $G$ isomorph zu $\mathbb{Z}_{p^2q}$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$.*

*Beweis.* Nach dem dritten Sylow Satz ist die Anzahl der $p$-Sylow-Untergruppen von $G$ kongruent zu 1 modulo $p$ und teilt $|G|$. Die Teiler von $|G|$ sind 1, $p$, $q$, $p^2$, $pq$, $p^2q$. Also muss die Anzahl der $p$-Sylow-Untergruppen entweder 1 oder $q$ sein. $q$ geht nicht, da nach Voraussetzung $1 \not\equiv q$ ist (mod $p$). Damit gibt es eine einzige $p$-Sylow-UGr von $G$, sagen wir $H$, sie ist nach Korollar 2.4 ein Normalteiler von $G$.

Analog: $G$ hat 1, $p$ oder $p^2$ $q$-Sylow-Untergruppen und weder $p$ noch $p^2$ sind möglich wegen der Voraussetzung $p^2 \not\equiv 1$ (mod $q$). Also gibt es eine einzige $q$-Sylow-Untergruppe $K$ in $G$. Die Ordnung der Untergruppe $H \cap K$ ist ein Teiler von $|H| = p^2$ und von $|K| = q$ (nach dem Satz von Lagrange), also ist $H \cap K =< e >$. Damit ist $HK = G$ (selber überlegen - Stoff aus [EA][3]) und man erhält $G = H \times K \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_q \cong \mathbb{Z}_{p^2q}$ oder $H \times K \cong \mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_q$. □

Mit Lemma 3.4 (mit $p = 3$ und $q = 5$) sieht man, dass jede Gruppe der Ordnung 45 isomorph ist zu $\mathbb{Z}_{45}$ oder zu $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Man kann mit dem Satz alle Gruppen der Ordnung 99, 153, 175, 207, etc. klassifizieren.

**Korollar 3.5.** *Es gibt keine einfach Gruppe der Ordnung $p^2q$ für $p$ und $q$ zwei verschiedene Primzahlen.*

*Beweis.* Sei $G$ eine Gruppe der Ordnung $p^2q$ mit $q \neq p$.
Gilt $p^2 \not\equiv 1$ (mod $q$) oder $q \not\equiv 1$ (mod $p$), so zeigt der Beweis von Lemma 3.4, dass $G$ eine normale Sylow-Untergruppe besitzt und daher nicht einfach ist.
Falls sowohl $p^2 \equiv 1$ (mod $q$) und $q \equiv 1$ (mod $p$) gilt, dann hat man $q \mid (p^2 - 1)$ und $p \mid (q - 1)$, woraus $p \leq q - 1$ folgt, oder, anders gesagt, $q \geq p + 1$. Wegen $p^2 - 1 = (p+1)(p-1)$ muss $q$ die Zahl $p-1$ oder die Zahl $p+1$ teilen. Das erstere geht nicht ($q \geq p + 1$). Aus dem letzteren folgt $q \leq p + 1$, also $q = p + 1$.

Die einzige Möglichkeit ist $p = 2$ und $q = 3$. Dann überprüft man, dass keine Gruppe der Ordnung 12 einfach ist (indem man jeweils zeigt, dass eine normale Sylow-Untergruppe existiert). □

[3]damit das Produkt von zwei UGruppen - hier $HK$ - eine Untergruppe ist, braucht man allgemein, dass eine davon ein Normalteiler ist.

3.1. **Diedergruppen.** Die Diedergruppen spielen eine wichtige Rolle bei der Klassifikation der Gruppen der Ordnung $2p$ ($p$ prim). Die Diedergruppen sind Symmetriegruppen von Polygonen. Genauer gesagt:

**Definition.** Sei $P$ ein regelmässiges Polygon mit $n$ Ecken ($n \geq 3$). Die *Symmetrien von $P$* sind die Bewegungen in der Ebene, die das Polygon auf sich selbst abbilden. Sie bilden unter Verknüpfung von Bewegungen eine Gruppe, die sogenannte *Diedergruppe $D_n$* vom Grad $n$.

(Zur Erinnerung: Bewegungen in der Ebene sind Verknüpfungen von Spiegelungen, also Spiegelungen, Rotationen, Verschiebungen, Gleitspiegelungen). Da das Polygon auf sich selbst abgebildet wird, sind die Symmetrien von $P$ gewisse Spiegelungen oder Rotationen (nur endlich viele Möglichkeiten).

**Lemma 3.6.** *Die Diedergruppe $D_n$ ist eine Gruppe der Ordnung $2n$, die durch zwei Elemente $r$ und $d$ erzeugt wird mit*

$$|r| = n, \quad |d| = 2, \quad \textit{und} \quad dr = r^{-1}d.$$

[Vorlesung 6, 24. Oktober 2014]

*Beweis.* Dass $D_n$ eine Gruppe ist, soll man sich selbst überlegen.

Wir platzieren $P$ so, dass sein Mittelpunkt im Nullpunkt eines Koordinatensystems vom $\mathbb{R}^2$ liegt und nummerieren die Eckpunkte von $P$ im Gegenuhrzeigersinn, dabei nehmen wir an, dass die Ecke 1 auf dem Punkt $(-1, 0)$ liegt (also auf der $x$-Achse). Sei $r$ die Rotation im Gegenuhrzeigersinn um $360°/n$ um das Zentrum von $P$. Also schickt $r$ den Eckpunkt $i$ auf $i+1$. Dass $r$ Ordnung $n$ hat ist klar. Sei $d$ die Spiegelung an der $x$-Achse. Dann hat $d$ Ordnung 2. $d$ ändert die Orientierung des Polygons (also insbesondere die Nummerierung der Eckpunkte).

Unter einer beliebigen Symmetrie von $P$ werden benachbarte Punkte von $P$ auf benachbarte Punkte geschickt. Also wird das Bild von $P$ durch die folgenden zwei Faktoren bestimmt: durch die neue Orientierung von $P$ und durch die neue Position vom Eckpunkt 1. Dann muss aber jede Symmetrie entweder von der Form $r^i$ oder von der Form $r^i d$ sein für ein $0 \leq i < n$. Dabei bewirkt $r^i$ eine Rotation im Gegenuhrzeigersinn um $i(360/n)$ Grad, Eckpunkt 1 geht an die Stelle, wo vorher $i+1$ war. Und $r^i d$ bewirkt eine Spiegelung an der $x$-Achse und eine Rotation im Gegenuhrzeigersinn um $i(360/n)$ Grad. Damit ist

$$D_n = \{e = r^0, r, r^2, \ldots, r^{n-1}, d = r^0 d, rd, r^2 d, \ldots, r^{n-1}d\}.$$

Die $2n$ Elemente sind dabei nach der obigen Diskussion alle verschieden.

Ausserdem sieht man leicht, dass $drd = r^{-1}$ ist: die Ecke 1 wird auf die ursprüngliche Ecke $n$ verschoben und die Ordnung ist die ursprüngliche, also ist $drd$ die Rotation um $360/n$ Grad im Uhrzeigersinn, d.h. gleich $r^{-1} = r^{n-1}$. Das zeigt $dr = r^{-1}d$. □

**Satz 3.7.** *Sei $G$ eine Gruppe der Ordnung $2p$, $p > 2$ eine Primzahl. Dann ist $G$ isomorph zu $\mathbb{Z}_{2p}$ oder zu $D_p$.*

Eine Folge davon ist, dass es genau zwei nicht-isomorphe Gruppen der Ordnung 6 gibt (wie früher behauptet). Ausserdem kriegt man mit dem Satz 3.7 eine vollständige Liste der Gruppen der Ordnung 10, 14, 22, 26, 34, etc.

*Beweis von Satz 3.7.* $G$ enthält ein Element $a$ der Ordnung $p$ und ein Element $b$ der Ordnung 2 (Korollar 2.2), also $a \neq b$ (hier wird $p > 2$ benötigt!). Wegen $b^2 = e$ ist $b^{-1} = b$. Sei $H$ die zyklische Gruppe, die von $a$ erzeugt wird. Da $|G| = 2p$ ist, hat die UGruppe $H$ Index 2 und ist daher ein Normalteiler von $G$ ([EA]). Also ist $bab = bab^{-1} \in H$. Nun ist $H$ zyklisch, also muss $bab = a^t$ sein für ein $t$. Also hat man (mit $b^2 = e$)

$$a^{t^2} = (a^t)^t = (bab)^t = (ba \underbrace{b)(b}_{=bb^{-1}} ab) \cdots (bab) = ba^t b = b(bab)b = a$$

Also muss $t^2 \equiv 1 \pmod p$ sein ([EA]: $a^k = e$ genau dann wenn die Ordnung $p$ von $a$ ein Teiler von $k$ ist). Also teilt $p$ die Zahl $t^2 - 1 = (t-1)(t+1)$, d.h. $p \mid (t-1)$ oder $p \mid (t+1)$, in andern Worten $t \equiv 1 \pmod p$ oder $t \equiv -1 \pmod p$.
A) $t \equiv 1 \pmod p$: Es ist dann $bab = a^t = a$. Das liefert $ba = ab$. Daraus folgt, dass $ab$ Ordnung $2p = |G|$ hat (für $a$ und $b$ relativ prim folgt aus $ab = ba$, dass die Ordnung von $ab$ gerade das Produkt der Ordnung von $a$ und von $b$ ist). $G$ ist damit zyklisch und isomorph zu $\mathbb{Z}_{2p}$.
B) $t \equiv -1 \pmod p$: Dann ist $bab = a^{-1}$.
*Behauptung*: Die Abbildung $f : D_p \to G$, $r^i d^j \mapsto a^i b^j$ ist ein Homomorphismus.
*Beweis*: Man benutzt, dass $bab = a^{-1}$ äquivalent ist zu $ba = a^{-1}b$, damit und mit Lemma 3.6 kann man Produkte in $G$ und in $D_p$ berechnen.
Sei $K =< b >$ die von $b$ erzeugte UGruppe. Wegen $|H| = p$ (und $p$ ungerade) und $|K| = 2$ ist $H \cap K =< e >$ (Satz von Lagrange) und damit gilt $G = HK$. Jedes Element von $G$ kann also geschrieben werden als $a^i b^j$, d.h. $f$ ist surjektiv. Weil $D_p$ und $G$ dieselbe Ordnung haben, ist $f$ injektiv, d.h. ein Isomorphismus. □

3.2. **Mehr zu Gruppen kleiner Ordnung.** (Ordnung 8 und Ordnung 12) Wir setzen die Klassifizierung Gruppen von kleiner Ordnung fort. In Kapitel 1.2 hatten wir die Gruppen bis und mit Ordnung 7 aufgelistet. Wir kennen bereits drei abelsche Gruppen der Ordnung 8, nämlich $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ und $\mathbb{Z}_8$ und eine nicht abelsche ($D_4$). Eine weitere nicht abelsche Gruppe der Ordnung 8 ist die Gruppe $Q$ der Quaternionen, diese ist nicht isomorph zu $D_4$ (siehe Serie 5, Übung 17). Dies sind alle Gruppen der Ordnung 8, wie Lemma 3.8 zeigt.

**Beispiel.** *Die Quaternionengruppe*
Wir betrachten die folgenden vier Matrizen mit Einträgen in $\mathbb{C}$:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Die Menge $Q := \{\mathbf{1}, \mathbf{i}, -\mathbf{1}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ bildet eine Gruppe bildet unter der Matrizenmultiplikation, die Gruppe $Q$ der *Quaternionen.*
(Übung.)

**Lemma 3.8.** *Ist $G$ eine Gruppe der Ordnung 8, dann ist $G$ isomorph zu einer der fünf hier:*

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8, \quad D_4, \quad Q.$$

*Beweis.* Falls $G$ abelsch ist, so ist $G$ eine der ersten drei, nach der Klassifizierung endlicher abelscher Gruppen ([EA]). Sei also $G$ eine nicht abelsche Gruppe der Ordnung 8. Nach dem Satz von Lagrange haben die Elemente $\neq e$ die Ordnung 2, 4 oder 8. $G$ kann jedoch kein Element der Ordnung 8 haben, da es $G$ erzeugen würde, dann wäre $G = \mathbb{Z}_8$ zyklisch und abelsch. Die Elemente $\neq e$ können auch nicht alle Ordnung 2 haben, denn dann wäre $G$ wieder abelsch (man überlegt, dass gilt $|a| = 2 \iff a \neq e$ und $a = a^{-1}$), $G$ muss also ein Element $a$ der Ordnung 4 enthalten.

Sei $b$ ein Element von $G \setminus \{e, a, a^2, a^3\}$. Damit finden wir acht verschiedene Elemente, nämlich

$$e, a, a^2, a^3, b, ab, a^2b, a^3b$$

(sind sind alle verschieden, da $|a| = 4$ ist und da aus $a^i = a^j b$ folgt, dass $b = a^{i-j} \in < a >$, ein Widerspruch zur Wahl von $b$), d.h. $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b, a^4b\}$.

Die Strategie ist nun, die Multiplikationstafel von $G$ zu bestimmen. Dazu leitet man zunächst $ba = a^{-1}b$ her.

Die Untergruppe $H :=< a >$ hat Ordnung 4 und Index 2 in $G$, sie ist also ein Normalteiler. Das Element $bab^{-1}$ hat Ordnung 4 (nachrechnen) und liegt in $H$, da $H$ Normalteiler ist. Also muss $bab^{-1} \in \{a, a^3\}$ sein ($e$ hat Ordnung 1, $a^2$ hat Ordnung 2, fallen somit weg). Falls $bab^{-1} = a$, so folgt $ba = ab$ und $G$ ist abelsch. D.h. wir haben $bab^{-1} = a^3 = a^{-1}$ oder anders gesagt $ba = a^{-1}b$. Damit kriegen wir einen Grossteil der Multiplikationstafel (z.B. ist $(ab)a^2 = a(ba)a = a(a^{-1}b)a = ba = a^{-1}b = a^3b$):

| | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $e$ | $ab$ | $a^2b$ | $a^3b$ | $b$ |
| $a^2$ | $a^2$ | $a^3$ | $e$ | $a$ | $a^2b$ | $a^3b$ | $b$ | $ab$ |
| $a^3$ | $a^3$ | $e$ | $a$ | $a^2$ | $a^3b$ | $b$ | $ab$ | $a^2b$ |
| $b$ | $b$ | $a^3b$ | $a^2b$ | $ab$ | | | | |
| $ab$ | $ab$ | $b$ | $a^3b$ | $a^2b$ | | | | |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $a^3b$ | | | | |
| $a^3b$ | $a^3b$ | $a^2b$ | $ab$ | $b$ | | | | |

Um die Tafel fertig zu stellen, müssen wir noch $b^2$ bestimmen. Wäre $b^2 = a^i b$, so wäre $b \in < a >$, Widerspruch. Also muss $b^2 \in \{e, a, a^2, a^3\}$ sein. Ist $b^2 = a$, so folgt $ab = b^2b = bb^2 = ba$, also ist $G$ abelsch. Man überprüft, dass aus $b^2 = a^3$ auch folgt,

dass $G$ abelsch ist. D.h. $b^2 \in \{e, a^2\}$. Beide Möglichkeiten führen zu verschiedenen Vervollständigungen der Multiplikationstafel. Vergleicht man sie mit den Tafeln für $D_4$ bzw. für $Q$, so sieht man, dass $G \cong D_4$ oder $G \cong Q$ ist. (Zur Diedergruppe: es entspricht $a^i$ der Rotation $r^i$ und $b$ der Spiegelung $d$ an der $x$-Achse, in der Notation vom Beweis von Satz 3.6). □

Nach der Klassifizierung von endlichen abelschen Gruppen gibt es zwei abelsche Gruppen der Ordnung 12, $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$ und $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Wir kennen auch zwei nicht abelsche Gruppen der Ordnung 12: $A_4$ und $D_6$. Es gibt eine dritte nicht abelsche Gruppe der Ordnung 12, die Gruppe $T$, die durch $a$ und $b$ erzeugt wird mit $|a| = 6$, $b^2 = a^3$ und $ba = a^{-1}b$ (und keine zwei von $A_4$, $D_6$ und $T$ sind isomorph):

**Lemma 3.9.** *Ist $G$ eine Gruppe der Ordnung 12, so ist $G$ isomorph zu einer der folgenden 5 Gruppen:*

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \quad \mathbb{Z}_{12}, \quad A_4, \quad D_6, \quad T$$

Hier ohne Beweis, die Argumente sind ähnlich wie beim Beweis von Lemma 3.8.

**Bemerkung.** Hinweis von N. Hammerlindl: Die Multiplikationstafel von $D_6$ erscheint auf der Titelseite von 12 × 12 Schlüsselkonzepte zur Mathematik, siehe etwa
http://www.springer.com/springer+spektrum/mathematik/book/978-3-8274-2297-2

Damit haben wir die vollständige Klassifizierung der Gruppen bis und mit Ordnung 15 zusammen:

| Ordnung | Gruppen |
|---|---|
| 2 | $\mathbb{Z}_2$ |
| 3 | $\mathbb{Z}_3$ |
| 4 | $\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | $\mathbb{Z}_5$ |
| 6 | $\mathbb{Z}_6,\ S_3$ |
| 7 | $\mathbb{Z}_7$ |
| 8 | $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_8, D_4,\ Q$ |
| 9 | $\mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_9$ |
| 10 | $\mathbb{Z}_{10},\ D_5$ |
| 11 | $\mathbb{Z}_{11}$ |
| 12 | $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3,\ \mathbb{Z}_{12}\ , A_4,\ , D_6,\ T$ |
| 13 | $\mathbb{Z}_{13}$ |
| 14 | $\mathbb{Z}_{14},\ D_7$ |
| 15 | $\mathbb{Z}_{15}$ |

Man könnte hier weitermachen bis zu Ordnung 100 oder mehr. Dabei reichen die Strategien, die wir hier verwendet haben, für mehr als die Hälfte der Gruppen. Für einige muss man aber viel zusätzliche Arbeit leisten. So gibt es z.B. 267 Gruppen

der Ordnung 64. Soweit ist keine Formel bekannt, die die Anzahl der verschiedenen Gruppen der Ordnung $n$ angeben kann.

## **Teil** 2. Arithmetik in Integritätsbereichen

Die Ringe $\mathbb{Z}$ der ganzen Zahlen und $k[X]$ der Polynome über einem Körper $k$ haben ähnliche Eigenschaften, so haben wir Divisionsalgorithmen in beiden, grösste gemeinsame Teiler existieren, sowie eindeutige Faktorisierung in Primzahlen/in irreduzible Faktoren. In diesem Kapitel suchen wir nach Bedingungen, unter denen diese Eigenschaften für beliebige Integritätsbereiche gelten. Insbesondere geht es um die eindeutige Faktorisierung.

### 4. Euklidische Bereiche

Kurze Repetition der Begriffe Teilbarkeit, Einheiten, assoziierte Elemente, Primelemente/irreduzible Elemente, in allgemeiner Form für Integritätsbereiche.

**Definition.** Sei $(R, +, \cdot)$ ein kommutativer Ring. Dann heisst $R$ ein Integritätsbereich (*domain* im Englischen), falls die Menge der Nullteiler $\mathrm{NT}(R)$ von $R$ gleich $\{0\}$ ist.

Sei $R$ ein Integritätsbereich (für den Rest vom Kapitel). Seien $a, b \in R$, $a \neq 0$. Dann *teilt* $a$ das Element $b$ ($a$ *ist ein Faktor von* $b$), geschrieben $a \mid b$, falls gilt $b = ac$ für ein $c \in R$. Ein Element $u \in R$ heisst *Einheit*, falls ein $v \in R$ existiert mit $uv = 1_R$. Die Einheiten in $R$ sind also die Faktoren vom Neutralelement $1_R$.

**Beispiel.** Die Einheiten in $\mathbb{Z}$ sind $\pm 1$, die Einheiten in $k[X]$, für einen Körper $k$ sind die konstanten Polynome $\neq 0$.

**Beispiel 4.1.** Die Menge $\mathbb{Z}[\sqrt{2}] = \{r + s\sqrt{2} \mid r, s \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{R}$. Das Element $1 + \sqrt{2}$ ist eine Einheit in $\mathbb{Z}[\sqrt{2}]$, denn

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

**Bemerkung.** Der Ring aus Beispiel 4.1 wird immer wieder auftauchen. Ist $d$ eine Zahl, so ist $\mathbb{Z}[\sqrt{d}] := \{r + s\sqrt{d} \mid r, s \in \mathbb{Z}\}$ ein Integritätsbereich, der in $\mathbb{C}$ enthalten ist. Ist $d \geq 0$, so ist $\mathbb{Z}[\sqrt{d}]$ ein Unterring von $\mathbb{R}$ (wann ist $\mathbb{Z} \subsetneqq \mathbb{Z}[\sqrt{d}]$?) Im Fall $d = -1$ nennt man $\mathbb{Z}[i]$ den *Ring der Gauss'schen Zahlen.*

[Vorlesung 7, 28. Oktober 2014]

**Bemerkung.** Einheiten teilen jedes Element von $R$: Sei $u \in R$ eine Einheit mit Inversem $v \in R$. Ist $b \in R$ beliebig, so gilt

$$u(vb) = (uv)b = 1_R b = b.$$

Ein Element $a \in R$ heisst zu $b \in R$ *assoziiert*, falls $a = bu$ ist für eine Einheit $u \in R$. Es gilt:

- $(i)$ $a$ ist assoziiert zu $b$ genau dann, wenn $b$ assoziiert ist zu $a$.
- $(ii)$ Jedes Element $a \neq 0$ von $R$ ist durch all seine Assoziierten teilbar.

Das sieht man so: Zu $u$ existiert ein Inverses, sei das $v$, $v$ ist auch Einheit. Nun multipliziert man beide Seiten von $a = bu$ mit $v$ und erhält $av = buv = b1_R = b$.

**Beispiele.** In $\mathbb{Z}$ hat jedes $n \neq 0$ genau zwei assoziierte, $n$ und $-n$.
Ist $k$ ein Körper, so sind die zu $f(x) \in k[X]$ assoziierten die Polynome $cf(x)$ mit $c \in k \setminus \{0\}$.
Im Ring $\mathbb{Z}[\sqrt{2}]$ sind die Elemente $\sqrt{2}$ und $2 - \sqrt{2}$ assoziiert:
Es ist $\sqrt{2} = (2 - \sqrt{2})(1 + \sqrt{2})$, wobei $1 + \sqrt{2}$ eine Einheit ist.

**Definition.** Ein Element $p \neq 0$ aus $R$ heisst *irreduzibel*, falls $p$ keine Einheit ist und die einzigen Teiler von $p$ seine Assoziierten und die Einheiten von $R$ sind.

Für Elemente in einem Polynomring $k[x]$ ($k$ ein Körper) ist die Definition von irreduzibel dieselbe wie die von irreduziblen Polynomen.

**Beispiel.** Die irreduziblen Elemente von $\mathbb{Z}$ sind die Primzahlen und ihre negativen. (Die einzigen Teiler von $p$ sind $\pm p$, seine Assoziierten, und $\pm 1$).

Man kann zeigen, dass das Element $1 + i$ ist irreduzibel im Ring $\mathbb{Z}[i]$ (dazu braucht man den Begriff der Norm).

Ein Kriterium für Irreduzibilität ist das folgende (wird manchmal zur Definition von irreduzibel verwendet).

**Satz 4.2.** *Sei $p \in R$, $p \neq 0$ und $p$ keine Einheit. Dann gilt:*

$$p \text{ ist irreduzibel} \iff \text{Aus } p = rs \text{ folgt } r \text{ ist Einheit oder } s \text{ ist Einheit.}$$

*Beweis.* $\Longrightarrow$: Ist $p$ irreduzibel und $p = rs$, so ist $r$ ein Teiler von $p$. Also muss $r$ eine Einheit sein (und dann sind wir fertig) oder zu $p$ assoziiert. Ist $r$ zu $p$ assoziiert, so ist $r = pv$ für eine Einheit $v$, somit $p = rs = pvs$. Wir können $p$ auf beiden Seiten kürzen (kürzen ist in Integritätsbereichen erlaubt) und erhalten $1_R = vs$, $s$ ist also eine Einheit.
$\Longleftarrow$: Sei $p$ ein Element mit der obigen Eigenschaft (aus $p = rs$ folgt, dass $r$ oder $s$ eine Einheit ist). Sei $c$ ein beliebiger Teiler von $p$, $p = cd$. Dann ist entweder $c$ oder $d$ eine Einheit. Falls $d$ die Einheit ist, so ist $p$ zu $c$ assoziiert und die Behauptung folgt mit (ii) von oben (Bemerkung zur Assoziiertheit).
Im andern Fall ist $c$ die Einheit und wir sind fertig. $p$ ist also irreduzibel. □

4.1. **Definition der Euklidischen Bereiche.** Der Divisionsalgorithmus ist essentiell, um die arithmetischen Eigenschaften von $\mathbb{Z}$ und von $k[X]$ zu studieren ($k$ ein Körper). Euklidische Bereiche haben eine ähnliche Eigenschaft. Zur Erinnerung: der Grad eines Polynoms kann als Funktion der Polynome $\neq 0$ von $k[X]$ in die nicht-negativen Zahlen aufgefasst werden. In der folgenden Definition wird die Rolle des Grades von $\delta$ gespielt.

**Definition 4.3.** Ein Integritätsbereich $R$ ist ein *Euklidischer Bereich*, falls eine Funktion $\delta$ von den Elementen von $R \setminus \{0\}$ in die nicht-negativen Zahlen existiert mit den Eigenschaften

(i) Sind $a, b \in R$ verschieden von Null, so ist $\delta(a) \leq \delta(ab)$
(ii) Zu $a, b \in R$ und $b \neq 0_R$ existieren $q, r \in R$ mit $a = bq + r$, wobei entweder $r = 0_R$ ist oder $\delta(r) < \delta(b)$.

**Beispiele.** (1) Ist $k$ ein Körper, so ist $k[x]$ ein Euklidischer Bereich, man wählt für $\delta$ die Gradfunktion. Die Eigenschaft (i) folgt wegen $\delta(f(x)g(x)) = \deg(f(x)g(x)) = \deg f(x) + \deg g(x) \geq \deg f(x) = \delta(f(x))$. Eigenschaft (ii) ist der Divisionsalgorithmus für Polynome.

(2) $\mathbb{Z}$ ist ein Euklidischer Bereich, man wählt als $\delta$ die Betragsfunktion, $\delta(a) = |a|$. Es ist $|ab| = |a| \cdot |b| \geq |a|$, falls $a \neq 0$ ist. Der Divisionsalgorithmus liefert Eigenschaft (ii).

(3) Die Gauss'schen Zahlen $\mathbb{Z}[i] = \{s+ti \mid s,t \in \mathbb{Z}\}$, zusammen mit $\delta(s+ti) := s^2+t^2$ bilden auch einen Euklidischen Bereich.
So ist $s+ti = 0$ genau dann, wenn $s = t = 0$ gilt. Daher ist $\delta(s+ti) \geq 1$ für alle Elemente verschieden von Null.
Man zeigt, dass gilt $\delta(ab) = \delta(a)\delta(b)$.

$$\begin{aligned}
\delta(ab) &= \delta(s+ti)(u+vi) \\
&= \delta(su - tv + i(sv+tu)) \\
&= (su-tv)^2 + (sv+tu)^2 \\
&= s^2u^2 - 2sutv + t^2v^2 + s^2v^2 + 2svtu + t^2u^2 \\
&= s^2(u^2+v^2) + t^2(v^2+u^2) \\
&= (s^2+t^2)(v^2+v^2) \\
&= \delta(a)\delta(b)
\end{aligned}$$

Damit kann man für $b \neq 0$ die Eigenschaft (i) aus Definition 4.3 zeigen:

$$\delta(a) = \delta(a) \cdot 1 \leq \delta(a)\delta(b) = \delta(ab)$$

Für (ii) überlegt man zuerst, dass für $b \neq 0$ $a/b$ eine komplexe Zahl ist, die als $c+di$ geschrieben werden kann mit $c$ und $d$ in $\mathbb{Q}$.

$$\begin{aligned}
\frac{a}{b} &= \frac{s+ti}{u+vi} = \frac{(s+ti)(u-vi)}{u^2+v^2} = \frac{su+tv+(-sv+tu)i}{u^2+v^2} \\
&= \frac{su+tv}{u^2+v^2} + \frac{-sv+tu}{u^2+v^2}i
\end{aligned}$$

Die Zahl $c \in \mathbb{Q}$ liegt zwischen zwei ganzen Zahlen, ebenso $d$. Also existieren Zahlen $m, n \in \mathbb{Z}$ mit $|m-c| \leq \frac{1}{2}$ und $|n-d| \leq \frac{1}{2}$. Wegen $a/b = c+di$ gilt dann

$$\begin{aligned}
a &= b(c+di) = b((c-m+m) + (d-n+n)i) \\
&= b((m+ni) + ((c-m) + (d-n)i)) \\
&= b(m+ni) + b((c-m) + (d-n)i) \\
&= bq + r
\end{aligned}$$

für $q = m+ni \in \mathbb{Z}[i]$ und $r = b((c-m)+(d-n)i)$, wobei $r$ auch in $\mathbb{Z}[i]$ liegt. (Ausführlich, z.B.: Da $r = a - bq$ gilt mit $a, b, q \in \mathbb{Z}[i]$, ist auch

$r \in \mathbb{Z}[i]$.) Die Eigenschaft (ii) aus Definition 4.3 gilt nun wegen

$$\begin{aligned} \delta(r) &= \delta(b)\delta((c-m)+(d-n)i) = \delta(b)((c-m)^2+(d-n)^2) \\ &\leq \delta(b)(\frac{1}{2}^2 + \frac{1}{2}^2) = \frac{1}{2}\delta(b) < \delta(b). \end{aligned}$$

## 5. Hauptidealbereiche, faktorielle Bereiche

Zur Erinnerung: Ein *Hauptidealbereich* ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, d.h. von einem Element erzeugt wird.

**Beispiel 5.1.** Der Polynomring $\mathbb{Z}[x]$ ist kein Hauptidealbereich: Die Menge aller Polynome deren konstante Term gerade ist, bildet ein Ideal $I$ in $\mathbb{Z}[x]$ (überlegen!).
*Behauptung:* $I$ ist kein Hauptideal.
Annahme, $I$ bestehe aus den Vielfachen eines einzigen Polynoms $p(x)$.
Das konstante Polynom 2 liegt in $I$, also muss 2 ein Vielfaches von $p(x)$ sein. Das geht jedoch nur, wenn der Grad von $p(x)$ gleich Null ist, also $p(x) = c$ für ein $c \in \mathbb{Z}$. Da ja $p(x) \in I$ liegt, muss $c = \pm 2$ sein.
Das Element $x \in \mathbb{Z}[x]$ ist auch in $I$ (sein konstanter Term ist 0). D.h. dass $x$ ein Vielfaches von $p(x) = \pm 2$ ist, was nicht möglich ist, denn die Polynome haben alle ganzzahlige Koeffizienten ($\frac{1}{2}$ wäre benötigt). Also kann $I$ nicht aus allen Vielfachen von $p(x)$ bestehen und ist nicht ein Hauptideal.

Euklidische Bereiche sind Hauptidealbereiche ([EA]), also sind $\mathbb{Z}$, $k[x]$ und $\mathbb{Z}[i]$ alles Hauptidealbereiche.

Die Umkehrung ist jedoch falsch: ein Hauptidealbereich muss nicht ein Euklidischer Bereich sind. Dazu findet sich ein Gegenbeispiel im Artikel, J.C. Wilson "A Principal Ideal Domain that is not a Euclidean Ring", Mathematics Magazine, 46 (1973), Seiten 34–38. Und (eine vereinfachte Version davon): K.S. Williams, "Note on Non-Euclidean Principal Ideal Domains", Mathematics Magazine 48 (1975), Seiten 176–177.

5.1. **Faktorielle Bereiche.** Das Hauptresultat bei den Euklidischen und bei den Hauptidealbereichen ist, dass sie eindeutige Faktorisierungen besitzen. Umgekehrt kann man fragen, welche Bereiche eine eindeutige Faktorisierung haben und dann überlegen, was für weitere Eigenschaften diese Bereiche haben. Dazu die folgende Definition:

**Definition.** Ein Integritätsbereich $R$ heisst *faktoriell*, falls jedes Element $a \neq 0$ von $R$, das keine Einheit ist ein Produkt von (endlich vielen) irreduziblen Elementen

$$a = p_1 p_2 \cdots p_n, \ n \geq 1$$

ist[4], wobei diese Faktorisierung eindeutig ist bis auf Assoziiertheit. Ist also

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

wobei die $p_i$ und $q_j$ alle irreduzibel sind, so gilt $r = s$ und

$$p_i \text{ ist zu } q_i \text{ assoziiert zu } i = 1, \ldots, r.$$

(falls nötig nummeriert man dazu die $q_i$ zuerst um).

Faktorielle Bereiche heissen auch faktorielle Ringe oder ZPE (Zerlegung in Primelemente ist eindeutig)-Ringe oder Gauss'sche Ringe. Auf Englisch: Unique factorization domain, kurz UFD.

**Beispiel.** Hauptidealbereiche sind faktorielle Bereiche, wie man beweisen kann. Dabei nutzt man aus, dass in Hauptidealbereichen die ansteigende Kettenbedingung für Hauptideale erfüllt ist (jede Inklusionskette von Hauptidealen stabilisiert nach einer endlichen Anzahl von Schritten).

**Beispiele.**
(1) Sei $\mathbb{Q}_{\mathbb{Z}}[x]$ der Ring der Polynome mit rationalen Koeffizienten und ganzzahligen konstanten Summanden. Elemente davon sind z.B. $x$, $\frac{1}{2}x$, 2. Man kann überprüfen, dass $\mathbb{Q}_{\mathbb{Z}}[x]$ ein Integritätsbereich ist und dass das konstante Polynom 2 irreduzibel in diesem Ring ist (Übung) . Man kann $x$ faktorisieren als $2 \cdot (\frac{1}{2}x)$, also ist 2 ein irreduzibler Faktor von $x$. Analog ist 2 ein irreduzibler Faktor von $\frac{1}{2}x$, da $\frac{1}{2}x = 2 \cdot \frac{1}{4}x$ ist. Man erhält $x = 2 \cdot 2 \cdot \frac{1}{4}x$. Dieser Prozess hört nie auf, das Element $x$ ist nicht Produkt von endlich vielen Irreduziblen.
(2) $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist nicht faktoriell: Es ist $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ (und die sind nicht assoziiert).
(3) Der Polynomring $\mathbb{Z}[x]$ ist faktoriell (werden wir in Kapitel 7 sehen). Da $\mathbb{Z}[x]$ kein Hauptidealbereich ist (Beispiel 5.1) gibt es also mehr UFD's als Hauptidealbereiche.

[Vorlesung 8, 30. Oktober 2014 - Selbststudium]

**Bemerkung.** Bei Faktorisierungen von zwei ganzen Zahlen kann man die so schreiben, dass beide Faktorisierungen die selben Primzahlen verwenden. Dazu nehmen wir $-18$ und 40 als Beispiele. So ist etwas $-18 = 2 \cdot 3 \cdot (-3)$ und $40 = 2 \cdot (-2) \cdot (-2) \cdot 5$. Die Primelemente, die in den beiden Faktorisierungen auftauchen sind $\pm 2$, $\pm 3$ und 5, wobei 2 und $-2$ assoziiert, sowie 3 und $-3$. Wir streichen die assoziierten und benutzen die Einheiten $\pm 1$, um die Vorzeichen zu korrigieren.

$$\begin{aligned} -18 &= (-1) \cdot 2 \cdot 3 \cdot 3 = (-1) \cdot 2^1 \cdot 3^2 \cdot 5^0 \\ 40 &= (-1)(-1) \cdot 2 \cdot 2 \cdot 2 \cdot 5 = (1) \cdot 2^3 \cdot 3^0 \cdot 5^1 \end{aligned}$$

Ein analoges Verfahren existiert in jedem faktoriellen Bereich.

[4]Dabei erlauben wir ein Produkt mit genau einem Element, d.h. wir erlauben, dass das Element selbst irreduzibel ist.

**Satz 5.2.** *Sind $c, d$ Elemente von einem faktoriellen Bereich $R \setminus \{0\}$, dann existieren Einheiten $u$, $v$ und irreduzible Elemente $p_1, p_2, \ldots, p_k$ (paarweise nicht assoziiert) mit*

$$c = up_1^{m_1}p_2^{m_2}\cdots p_k^{m_k} \text{ und } d = vp_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$$

*wobei alle $m_i$ und $n_i$ in $\mathbb{Z}_{\geq 0}$ sind. Ausserdem gilt*

$$c \mid d \iff m_i \leq n_i \text{ für jedes } i = 1, \ldots, k$$

(Sind $c$ und $d$ beide Einheiten, so stehen da keine irreduziblen Faktoren!)

*Beweis.* Da $R$ ein UFD ist, können $c$ und $d$ faktorisiert werden, $c = q_1q_2\cdots q_s$ und $d = r_1\cdots r_t$ mit $q_i$ und $r_j$ irreduzibel. Unter den $q_1, \ldots, q_s, r_1, \ldots, r_t$ kann man alle Elemente streichen, zu denen vorher schon ein assoziiertes Element aufgetreten ist. Dann nennt man die übrig gebliebenen $p_1, p_2, \ldots, p_k$ für ein $k$. Diese sind paarweise nicht assoziierte Primelemente. Jedes der $q_j$, $r_l$ ist assoziiert zu einem $p_i$. In der Faktorisierung $c = q_1q_2\cdots q_s$ von $c$ kann man also jedes $q_j$ als $w_ip_i$ schreiben, $w_i$ eine geeignete Einheit. Schreibt man also $c$ um, so kann man $c$ schreiben als

$$\underbrace{(\text{Produkt von Einheiten})}_{\text{Einheit}} \cdot (\text{Produkt von } p_i's).$$

Das Produkt von Einheiten ist wieder eine Einheit, sagen wir $u$. Indem wir, wenn nötig, Faktoren $p_i^0$ einfügen, so können wir $c = up_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ schreiben wie gewünscht ($m_i \geq 0\ \forall i$). Analog geht man bei $d$ vor.

Für die zweite Aussage sei zuerst $c \mid d$. Dann ist $d = cb$ für ein $b \in R$. Da das irreduzible $p_i$ genau $n_i$ mal in der Faktorisierung von $d$ auftritt, muss es auch $n_i$ mal in derjenigen von $cb$ auftauchen. Da $p_i$ bereits $m_i$ mal in der Faktorisierung von $c$ auftaucht und ev. auch in $b$, muss $m_i \leq n_i$ sein für jedes $i$.

Umgekehrt: ist $m_i \leq n_i$ für jedes $i$. Dann gilt $d = ca$ für

$$a = (u^{-1}v)(p_1^{n_1-m_1}p_2^{n_2-m_2}\cdots p_k^{n_k-m_k})$$

(selber überlegen). Also gilt $c \mid d$. □

Eine Eigenschaft irreduzibler Elemente in Euklidischen und Hauptidealbereichen gilt auch bei faktoriellen Bereichen:

**Satz 5.3.** *Sei $p$ ein irreduzibles Element in einem faktoriellen Bereich $R$. Ist $p \mid bc$, so folgt $p \mid b$ oder $p \mid c$*[5].

*Beweis.* Ist $b = 0_R$ oder $c = 0_R$, so sind wir fertig, denn $p \mid 0_R$. Ist $c$ eine Einheit und $p = bc$, so gilt $pt = bc$ für ein $t \in R$ und $ptc^{-1} = b$, also teilt $p$ das Element $b$. Analog teilt $p$ das Element $c$, falls $b$ ein Einheit ist.

[5]Das ist gerade die Definition von einem Primelement in $R$: Ein Primelement in einem kommutativen Ring ist ein Element $c$ in dem Ring, das weder die Null noch eine Einheit ist und für das gilt: teilt $c$ das Produkt $a \cdot b$, so folgt $c \mid a$ oder $c \mid b$. Damit ist also ein irrezubles Element von $R$ auch ein Primelement (und umgekehrt)

Seien also $b$ und $c$ beides nicht Einheiten und beide verschieden von Null. Wir schreiben $b = q_1 \cdots q_k$ und $c = q_{k+1} \cdots q_s$ ($q_i$ irreduzibel, sie sind nicht unbedingt verschieden). Da $p \mid bc$ gilt, ist $pr = bc = q_1 \cdots q_s$ für ein $r \in R$. Wegen der eindeutigen Faktorisierung muss $p$ ein Assoziiertes sein zu einem $q_i$. Also teilt $p$ dieses $q_i$ und damit $b$ oder $c$. □

**Satz 5.4.** *Seien $a_1, \ldots, a_n$ Elemente (nicht alle gleich 0) in einem faktoriellen Bereich $R$. Dann besitzen $a_1, \ldots, a_n$ einen grössten gemeinsamen Teiler in $R$.*

*Beweis.* Der ggT einer Menge von Elementen ist der ggT der Elemente $\neq 0$ in dieser Menge. Wir können daher o.E. annehmen, dass alle $a_i$ verschieden von Null ist. Nach Satz 5.2 existieren irreduzible $p_1, \ldots, p_t$ (darunter sind keine zwei assoziiert), Einheiten $u_1, \ldots, u_n$ und nicht negative Zahlen $m_{ij}$ mit

$$\begin{aligned} a_1 &= u_1 p_1^{m_{11}} p_2^{m_{12}} \cdots p_t^{m_{1t}} \\ a_2 &= u_2 p_1^{m_{21}} p_2^{m_{22}} \cdots p_t^{m_{2t}} \\ &\vdots \\ a_n &= u_n p_1^{m_{n1}} p_2^{m_{n2}} \cdots p_t^{m_{nt}} \end{aligned}$$

Sei $k_1$ das kleinste Element, das unter den Exponenten von $p_1$ auftritt, $k_2 := \min(m_{12}, m_{22}, \ldots, m_{n2})$, etc. Mit Satz 5.2 ist $d := p_1^{k_1} \cdots p_t^{k_t}$ ein ggT von $a_1, \ldots, a_n$. □

[Vorlesung 9, 4. November 2014]

In einem beliebigen faktoriellen Bereich ist es im allgemeinen nicht möglich, einen ggT von zwei Elementen $a$ und $b$ als Linearkombination von $a$ und $b$ zu schreiben (wie es in $\mathbb{Z}$ und $k[x]$ möglich ist). Wir werden im Kapitel 7 sehen, dass im faktoriellen Bereich $\mathbb{Z}[x]$ das Einselement ggT der Polynome $x$ und 2 ist. Die 1 ist jedoch nicht eine Linearkombination von $x$ und 2 in $\mathbb{Z}[x]$ (Übung). In einem Hauptidealbereich kann ein ggT von $a$ und $b$ immer als Linearkombination von $a$ und $b$ geschrieben werden. (Übung, Hinweis: Sei $R$ ein Hauptidealbereich, definiere $I$ als das von $a$ und $b$ erzeugte Ideal. Dann ist $I = (d)$ für ein $d \in R$. Man zeige, dass $d$ ein ggT von $a$ und $b$ ist).

## 6. Der Quotientenkörper eines Integritätsbereichs

Zu jedem Integritätsbereich $R$ konstruieren wir einen Körper $k$, der $R$ enthält und dessen Elemente "Quotienten" von Elemente von $R$ sind. Für $R = \mathbb{Z}$ ist dieser Körper gleich $\mathbb{Q}$. Dies wird hier verallgemeinert. Dieser Körper $k$ (zu $R$) ist dann essentiell bei der Untersuchung von Faktorisierungen in $R[x]$ in Kapitel 7. Dabei hilft die Erfahrung mit rationalen Zahlen, die Beweise sind jedoch unabhängig von der Kenntnis von $\mathbb{Q}$.

Eine rationale Zahl $a/b$ wird durch die Zahlen $a$ und $b$ (mit $b \neq 0$) bestimmt. Unterschiedliche Paare können zur gleichen Zahl führen. Allgemein gilt

$$\frac{a}{b} = \frac{c}{d} \quad \text{genau dann, wenn} \quad ad = bc \quad \text{ist.}$$

Die rationalen Zahlen erhalten wir mit Hilfe einer Äquivalenzrelation auf Paaren von ganzen Zahlen. Analoges tun wir jetzt für $R$.

Sei $R$ ein Integritätsbereich, $S$ die folgende Menge von Paaren

$$S := \{(a, b) \mid a, b \in R,\ b \neq 0_R\}$$

Wir definieren eine Äquivalenzrelation $\sim$ auf $S$ durch

$$(a, b) \sim (c, d) \quad \text{falls} \quad ad = bc \quad \text{gilt in } R.$$

**Lemma 6.1.** *Die Relation $\sim$ ist eine Äquivalenzrelation auf $S$.*

*Beweis.* Reflexivität: Da $R$ kommutativ ist gilt $ab = ba$, also ist $(a, b) \sim (a, b)$ für alle $(a, b) \in S$.
Symmetrie: Ist $(a, b) \sim (c, d)$, so gilt $ad = bc$. Dank der Kommutativität ist $cb = da$, also $(c, d) \sim (a, b)$.
Transitivität: Sind $(a, b) \sim (c, d)$ und $(c, d) \sim (r, s)$, so ist $ad = bc$ und $cs = dr$. Multipliziert man $ad = bc$ mit $s$, so hat man
$ads = (bc)s = b(cs) = bdr$. Da $d \neq 0_R$ ist (Definition von $S$) und $R$ ein Integritätsbereich ist, können wir $d$ aus $ads = bdr$ kürzen, also ist $as = br$ und somit $(a, b) \sim (r, s)$. □

Die Relation $\sim$ unterteilt $S$ in disjunkte Äquivalenklassen. Wir schreiben kurz $[a, b]$ für die Äquivalenzklasse von $(a, b)$. Sei $k$ die Menge aller Äquivalenzklassen unter $\sim$. Dann ist

$$[a, b] = [c, d] \ \in k \Longleftrightarrow (a, b) \sim (c, d) \ \in S$$

Anders gesagt:

$$[a, b] = [c, d] \ \in k \Longleftrightarrow ad = bc \ \in R$$

Wir wollen sehen, dass $k$ ein Körper ist. Addition und Multiplikation von Äquivalenzklassen sind folgendermassen definiert (zur Illustration schaue man sich die Addition und Multiplikation von rationalen Zahlen an).

$$\begin{array}{lrcl} (i) & [a, b] + [c, d] & = & [ad + bc, bd] \\ (ii) & [a, b][c, d] & = & [ac, bd] \end{array}$$

Wir müssen überprüfen, dass diese Operationen wohldefiniert sind.
Die Ausdrücke auf der rechten Seite sind tatsächlich Elemente von $k$: nach Definition von $S$ ist $b \neq 0_R \neq d$ und da $R$ als Integritätsbereich nullteilerfrei ist, ist dann auch $bd \neq 0_R$. Also gehören $(ad+bc, bd)$ und $(ac, bd)$ zu $S$ und die Ausdrücke $[ad + bc, bd]$ und $[ac, bd]$ liegen in $k$.

Wir müssen jedoch auch noch zeigen, dass die Ausdrücke nicht davon abhängen, welche Vertreter wir für $[a, b]$ und $[c, d]$ wählen (im Fall $R = \mathbb{Z}$ wissen wir: $\frac{1}{2} \cdot \frac{3}{5}$ ist $\frac{3}{10}$ und es ist auch $\frac{4}{8} \cdot \frac{3}{5} = \frac{12}{40} = \frac{3}{10}$). Dazu das folgende Lemma.

**Lemma 6.2.** *Addition und Multiplikation in $k$ sind unabhängig von der Wahl der Vertreter der Äquivalenzklassen.*

*Beweis.* Seien $[a, b] = [a', b']$ und $[c, d] = [c', d']$. Es gilt $[ad+bc, bd] = [a'd'+b'c', b'd']$ in $k$ genau dann, wenn $(ad + bc)b'd' = bd(a'd' + b'c')$ gilt in $R$.

Wir zeigen also letzteres. Da $[a, b] = [a', b']$ und $[c, d] = [c', d']$ gilt, wissen wir, dass

$$ab' = ba' \qquad cd' = dc' \qquad (*)$$

gilt. Multipliziert man die erste Gleichung mit $dd'$ und die zweite mit $bb'$ und addiert die beiden, so kriegt man

$$\begin{aligned} ab'dd' + cd'bb' &= ba'dd' + dc'bb' \\ (ad + bc)b'd' &= bd(a'd' + b'c') \end{aligned}$$

und damit ist $[ad + bc, bd] = [a', d' + b'c', b'd']$. Für den zweiten Teil des Beweises multipliziert man die erste Gleichung in (*) mit $cd'$, die zweite mit $ba'$ und erhält

$$ab'cd' = ba'cd' \text{ und } cd'ba' = dc'ba'$$

Wegen der Kommutativität ist die rechte Seite der ersten Gleichung gleich der linken Seite der zweiten Gleichung, also $ab'cd' = dc'ba'$ und damit

$$(ac)(b'd') = ab'cd' = dc'ba' = (bd)(a'c').$$

Womit wir $[ac, bd] = [a'c', b'd']$ haben. □

**Lemma 6.3.** *Ist $R$ ein Integritätsbereich und $k$ wie oben definiert, dann gilt für alle $a, b, c, d, t \in R \setminus \{0\}$:*

(1) $[0_R, b] = [0_R, d]$,
(2) $[a, b] = [ta, tb]$,
(3) $[a, a] = [c, c]$

*Beweis.* Übung □

**Lemma 6.4.** *Definiert man Addition und Multiplikation wie oben, dann ist $k$ ein Körper.*

*Beweis.* Abgeschlossenheit unter Addition und Multiplikation folgt aus Lemma 6.2 und den Bemerkungen davor. Die Addition ist kommutativ in $k$, da Addition und Multiplikation in $R$ kommutativ sind:

$$[a, b] + [c, d] = [ad + bc, bd] = [cb + da, db] = [c, d] + [a, b].$$

Sei $0_k$ die Äquivalenzklasse von $[0_R, d]$ mit $d \in R$, $d \neq 0_R$, beliebig (wegen Lemma 6.3 (1) sind alle $(0_R, d)$ mit $d \neq 0$ in der gleichen Äquivalenzklasse). Ist $[a, b] \in k$, so gilt nach Lemma 6.3 (2) mit $t = b$:

$$[a, b] + 0_k = [a, b] + [0_R, d] = [ad + b0_R, bd] = [ad, bd] = [a, b]$$

Also ist $0_k$ das Nullelement von $k$. Das Negative (additive Inverse) zu $[a, b]$ ist $[-a, b]$:

$$[a, b] + [-a, b] = [ab - ba, bb] = [0_R, bb] = 0_k$$

Man soll selber überprüfen, dass die Addition assoziativ ist und die Multiplikation assoziativ und kommutativ. Ebenso soll man sich überlegen, dass $[1_R, 1_R]$ das multiplikative Neutralelement von $k$ ist. Für multiplikative Inverse: sei $[a, b]$ ein Element mit $a \neq 0_R$. Dann ist $[b, a]$ auch ein Element von $k$ und es gilt (mit Lemma 6.3 (3)):

$$[a, b][b, a] = [ab, ab] = [1_R ab, 1_R ab] = [1_R, 1_R]$$

Damit ist $[b, a]$ das multiplikativ Inverse zu $[a, b]$. Für die Distributivgesetze in $k$ betrachtet man

$$\begin{aligned} [a, b]([c, d] + [r, s]) &= [a, b][cs + dr, ds] \\ &= [a(cs + dr), b(ds)] \\ &= [acs + adr, bds] \end{aligned}$$

und (mit Lemma 6.3(2) mit $t = b$):

$$\begin{aligned} [a, b][c, d] + [a, b][r, s] &= [ac, bd] + [ar, bs] \\ &= [(ac)(bs) + (bd)(ar), (bd)(bs)] \\ &= [(acs + adr)b, (bds)b] \\ &= [acs + adr, bds] \end{aligned}$$

Es ist also $[a, b]([c, d] + [r, s]) = [a, b][c, d] + [a, b][r, s]$. □

**Lemma 6.5.** *Sei $R$ ein Integritätsbereich und $k$ der Körper von Lemma 6.4. Dann ist die Teilmenge $R^* := \{[a, 1_R] \mid a \in R\}$ ein Integritätsbereich, der isomorph ist zu $R$.*

*Beweis.* Schritte:
(a) $R^*$ ist Unterring von $k$, das neutrale Element $[1_R, 1_R]$ von $k$ liegt in $R^*$, $R^*$ ist auch Identitätsbereich (selber überprüfen).
(b) Isomorphie:
Sei $f : R \to R^*$ definiert durch $a \mapsto [a, 1_R]$. Dies ist ein Ringhomomorphismus (klar: $f$ schickt das Einselement $1_R$ auf das Einselement in $R^*$):

$$\begin{aligned} f(a) + f(c) &= [a, 1_R] + [c, 1_R] = [a1_R + 1_R c, 1_R 1_R] = [a + c, 1_R] = f(a + c) \\ f(a)f(c) &= [a, 1_R][c, 1_R] = [ac, 1_R] = f(ac) \end{aligned}$$

Ist $f(a) = f(c)$, so ist $[a, 1_R] = [c, 1_R]$, woraus $a1_R = 1_R c$ folgt, also muss $a = c$ sein, $f$ ist injektiv. Surjektivität ist klar, $f$ ist also ein Isomorphismus. □

Die Notation mit Äquivalenzklassen $[,]$ ist umständlich und illustriert die Idee vom Quotientennehmen nicht richtig. Daher ändern wir die Schreibweise, anstatt $[a, b]$ für die Äquivalenklasse von $(a, b)$ schreiben wir $a/b$ oder $\frac{a}{b}$. Mit dieser Notation können wir die Aussagen der Lemmata 6.4 und 6.5 so zusammenfassen:

**Satz 6.6.** *Sei $R$ ein Integritätsbereich. Dann existiert ein Körper $k$ dessen Elemente von der Form $a/b$ sind mit $a, b \in R$, $b \neq 0_R$ mit der folgenden Bedingung:*

$$\frac{a}{b} = \frac{c}{d} \text{ in } k \iff ad = bc \text{ in } R.$$

*Addition und Multiplikation in $k$ sind folgendermassen gegeben:*

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

*Die Menge der Elemente von $k$ der Gestalt $a/1_R$ ($a \in R$) bilden einen Integritätsbereich, der isomorph ist zu $R$.*

(Wir hätten von Anfang an die Quotientennotation verwenden können, da das jedoch so sehr wie die rationalen Zahlen aussieht, hätte man ev. zu schnell alles geglaubt ohne die Details genau zu überprüfen.)

Nun ist klar, dass für $R = \mathbb{Z}$ der Körper $k$ dann $\mathbb{Q}$ ist, Satz 6.6 liefert also eine formale Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$. Im allgemeinen werden wir, wie bei $\mathbb{Q} \supset \mathbb{Z}$ den Ring $R$ mit seiner isomorphen Kopie in $k$ identifizieren und sagen, dass $R$ die Teilmenge von $k$ ist, die aus den Elementen der Gestalt $a/1_R$ besteht. Der Körper $k$ heisst der *Quotientenkörper von $R$.*

**Beispiel.** Sei $k$ ein Körper. Der Quotientenkörper des Polynomrings $k[x]$ wird als $k(x)$ geschrieben und besteht aus den Ausdrücken $f(x)/g(x)$, wobei $f(x), g(x) \in k[x]$ sind und $g(x) \neq 0_{k[x]}$ ist[6]. Der Körper $k(x)$ heisst der *Körper der rationalen Funktionen über $k$.*

Der Quotientenkörper eines Integritätsbereiches $R$ ist gewissermassen der kleinste Körper, der $R$ enthält:

**Satz 6.7.** *Sei $R$ ein Integritätsbereich und sei $k$ sein Quotientenkörper. Ist $K$ ein Körper mit $K \supseteq R$, so enthält $K$ einen Unterkörper[7] $F$ mit $R \subseteq F \subseteq K$ und $F$ ist isomorph zu $k$.*

*Beweis.* Sei $a/b \in k$. Also sind $a, b \in R$ und $b \neq 0_R$. Da $R \subseteq K$ gilt, existiert ein Inverses $b^{-1}$ zu $b$ in $K$. Wir definieren eine Abbildung $f : k \to K$ durch $f(a/b) := ab^{-1}$.

[6] d.h. $g(x)$ ist nicht das Nullpolynom; $g(x)$ kann Nullstellen haben!

[7] Unterkörper $K$: ist Teilmenge von $K$, die 0 und 1 enthält, sowie mit den auf die Teilmenge eingeschränkten Verknüpfungen selbst ein Körper ist.

(i) Das ist wohldefiniert, d.h. aus $a/b = c/d$ in $k$ folgt $f(a/b) = f(c/d)$ in $K$.
(ii) Ausserdem gilt: $f$ ist ein injektiver Homomorphismus.
Zu (i) und (ii): siehe Übungen, Blatt 6, Aufgabe 4.
Ist $F$ das Bild von $k$ unter $f$, so gilt daher $k \cong F$. Für alle $a \in R$ ist $a = a1_R^{-1} = f(a/1_R) \in F$, also haben wir $R \subseteq F \subseteq K$. □

## 7. Eindeutige Faktorisierung in Polynomringen

[Vorlesung 10, 7. November 2014]

$R$ sei in diesem Kapitel immer ein faktorieller Bereich. Ziel: Ist $R$ ein faktorieller Ring, so ist auch der Polynomring $R[x]$ faktoriell. Die Grundideen für den Beweis sind relativ einfach: Ist $f(x)$ ein Polynom, so faktorisieren wir $f(x)$ so lange bis es ein Produkt von irreduziblen Elementen ist. Um die Eindeutigkeit zu sehen, betrachtet man $f(x)$ als Polynom in $k[x]$, wobei $k$ der Quotientenkörper von $R$ sei. Da $k[x]$ ein UFD ist ([EA]), ist die Faktorisierung in $R[x]$ eindeutig. Es gibt einige Schwierigkeiten auf dem Weg zu diesem Beweis. Zuerst ein Beispiel, das Unterschiede beim Faktorisieren aufzeigt.

**Beispiel.** Das Polynom $3x^2 + 6$ können wir nicht als Produkt zweier Polynome von kleinerem Grad in $\mathbb{Z}[x]$ schreiben. Ausserdem ist es irreduzibel in $\mathbb{Q}[x]$. Das Polynom ist aber reduzierbar in $\mathbb{Z}[x]$: $3x^2 + 6 = 3(x^2 + 2)$, wobei weder 3 noch $x^2 + 2$ Einheiten sind in $\mathbb{Z}[x]$.

Im ersten Schritt analysieren wir die Rolle der konstanten Polynome in $R[x]$.

**Bemerkung.** Sei $R$ ein Integritätsbereich. Dann gilt (überlegen!):
1) $f(x) \in R[x]$ ist Einheit $\iff$ $f(x)$ ist ein konstantes Polynom, das eine Einheit in $R$ ist.
Ein Folge davon ist im Fall, wo $R = k$ ein Körper ist:
$f(x) \in k[x]$ ist Einheit $\iff$ $f(x) \equiv c$ für ein $c \in k \setminus \{0\}$.
2) Mit Teil 1) lässt sich folgendes beweisen:
$p$ ist irreduzibel in $R \iff$ das konstante Polynom $p \in R[x]$ ist irreduzibel in $R[x]$.

Zusammenfassend:
Die Einheiten von $R[x]$ sind gerade die Einheiten in $R$ und die irreduziblen konstanten Polynome in $R[x]$ sind gleich den irreduziblen Elementen in $R$.

So sind etwa die Einheiten in $\mathbb{Z}[x]$ die Elemente $\pm 1$. Das konstante Polynom 3 ist irreduzibel in $\mathbb{Z}[x]$, obwohl es eine Einheit ist in $\mathbb{Q}[x]$.

Die konstanten irreduziblen Faktoren eines Polynoms in $R[x]$ kann man finden, indem man alle Konstanten ausfaktorisiert und als Produkte von irreduziblen Elementen in $R$ schreibt.

**Beispiel.** In $\mathbb{Z}[x]$ haben wir

$$6x^2 + 18x + 12 = 6(x^2 + 3x + 2) = 2 \cdot 3(x^2 + 3x + 2)$$

Dabei ist $x^2 + 3x + 2$ ein Polynom dessen einzige *konstanten* Divisoren (=Teiler) im Ring $\mathbb{Z}[x]$ die Einheiten $\pm 1$ sind. Aus diesem Beispiel leiten wir eine Strategie für den allgemeinen Fall ab.

**Definition.** Sei $R$ ein faktorieller Bereich. Ein Polynom $f(x) \neq 0_{R[x]}$ in $R[x]$ heisst *primitiv*, falls die einzigen Konstanten, die $f(x)$ teilen, die Einheiten in $R$ sind.

So sind $x^2+3x+2$ etwa und $3x^4-5x^3+2x$ primitive Elemente von $\mathbb{Z}[x]$. Primitive Polynome vom Grad 0 sind Einheiten. Jedes primitive Polynom vom Grad 1 muss irreduzibel sein (existiert eine Faktorisierung von $f(x)$ als $g(x) \cdot h(x)$, so addieren sich die Grad von $g(x)$ und von $h(x)$ auf $1 = \deg f(x)$, also muss $g(x)$ oder $h(x)$ konstantes Polynom sein und kann nur eine Einheit sein, da $f(x)$ primitiv ist).

Primitive Polynome von höherem Grad sind nicht notwenig irreduzibel (es ist z.B. $x^2 + 3x + 2 = (x + 1)(x + 2)$ in $\mathbb{Z}[x]$). Jedoch haben irreduzible Polynome von positivem Grad keine konstanten Divisoren ausser den Einheiten (Satz 4.2), also gilt:

**Bemerkung.** Ein irreduzibles Polynom von positivem Grad ist primitiv.

Zudem hat man:

**Bemerkung.** Jedes Polynom $f(x) \in R[x]$, das nicht das Nullpolynom ist faktorisiert als $f(x) = cg(x)$ mit $g(x)$ primitiv ($c \in R$).

Begründung: Nach Satz 5.4 existiert für die Koeffizienten von $f(x)$ (die alle Elemente von $R$ sind) ein ggT, sei das $c$. Also ist $f(x) = cg(x)$ für ein $g(x)$. Behauptung: Dieses $g(x)$ ist primitiv. Falls es nicht primitiv ist, so existiert ein $d \in R$, das das Polynom $g(x)$ teilt, also $g(x) = dh(x)$ und $f(x) = cdh(x)$. Da $cd$ ein konstanter Teiler von $f(g)$ ist, muss er die Koeffizienten von $f(x)$ teilen und damit $c$, ggT der Koeffizienten. Also ist $cdu = c$ für eine Einheit $u \in R$. Da $c \neq 0_R$ ist, erhalten wir $du = 1_R$, $d$ ist eine Einheit. Damit ist $g(x)$ doch primitiv.

Mit Hilfe der diskutierten Eigenschaften von primitiven Polynomen können wir die Argumente zu $\mathbb{Z}[x]$ vom Anfang des Kapitels modifizieren und die ersten zwei Bedingungen beweisen, die $R[x]$ erfüllen muss, um ein UFD zu sein (die Schreibbarkeit als endliches Produkt von irreduziblen Polynomen).

**Satz 7.1.** *Sei $R$ ein faktorieller Bereich. Dann ist jedes Polynom $f(x) \in R[x]$, das weder Null noch eine Einheit ist, ein Produkt von (endlich vielen) irreduziblen Polynomen.*

(es darf natürlich ein Produkt mit nur einem Faktor sein).

*Beweis.* Sei $f(x) = cg(x)$ mit $g(x)$ primitiv. Da $R$ faktoriell ist, ist $c$ entweder eine Einheit oder ein Produkt von irreduziblen Elementen in $R$ (und damit in $R[x]$). Wir müssen also zeigen, dass $g(x)$ entweder eine Einheit ist oder ein Produkt von irreduziblen Elementen in $R[x]$. Ist $g(x)$ eine Einheit oder irreduzibel, so ist nichts zu zeigen. Falls nicht, so gilt nach Satz 4.2 $g(x) = h(x)k(x)$, wobei weder

$h(x)$ noch $k(x)$ Einheiten sind. Da $g(x)$ primitiv ist, sind seine einzigen Teiler vom Grad 0 die Einheiten. D.h. es muss gelten $0 < \deg h(x) < \deg g(x)$ und $0 < \deg k(x) < \deg g(x)$. Ausserdem sind $h(x)$ und $k(x)$ primitiv (jede Konstante, die sie teilt muss auch $g(x)$ teilen, also eine Einheit sein). Sind sie irreduzibel, so sind wir fertig. Falls nicht, so können wir das obige Argument wiederholen und beide als Produkte von primitiven Polynomen von kleinerem Grad schreiben, etc. Dieser Prozess muss nach einer endlichen Zahl von Schritten aufhören, da die Grade der Faktoren in jedem Schritt abnehmen. Also ist $g(x)$ ein Produkt von irreduziblen in $R[x]$. □

Um zu zeigen, dass Faktorisierung in $R[x]$ eindeutig ist (Satz 7.8), benötigen wir mehrere Hilfsschritte, die nun entwickelt werden (Lemma 7.2 bis Korollar 7.7).

**Lemma 7.2.** *Sei $R$ faktoriell und $g(x)$, $h(x) \in R[x]$. Ist $p$ ein irreduzibles Element in $R$, das $g(x)h(x)$ teilt, so gilt $p$ teilt $g(x)$ oder $p$ teilt $h(x)$.*

*Beweis.* Das geht völlig analog wie die entsprechende Aussage für $\mathbb{Z}[x]$, siehe Beispiel 7.3 hier anschliessend. Man ersetzt dabei Primzahl durch irreduzibles Element und benutzt den Satz 5.3. □

**Beispiel 7.3.** Seien $f(x)$, $g(x)$, $h(x)$ in $\mathbb{Z}[x]$ mit $f(x) = g(x)h(x)$. Ist $p$ eine Primzahl, die jeden Koeffizienten von $f(x)$ teilt, so gilt: teilt $p$ jeden Koeffizienten von $g(x)$ oder $p$ teilt jeden Koeffizienten von $h(x)$.

Widerspruchsbeweis: Falls die Aussage nicht stimmt, so gibt es einen Koeffizienten von $g(x)$ und einen Koeffizienten von $h(x)$, die nicht durch $p$ teilbar sind. Sei $f(x) = a_0 + a_1x + \cdots + a_kx^k$, $g(x) = \sum_{i=0}^{m} b_ix^i$, $h(x) = \sum_{i=0}^{n} c_ix^i$. Sei $b_r$ der erste Koeffizient von $g(x)$, der nicht durch $p$ teilbar ist, $c_t$ der erste Koeffizient von $h(x)$, der nicht durch $p$ teilbar ist. Dann gilt $p \mid b_i$ für $i < r$ und $p \mid c_j$ für $j < t$. Wir betrachten den Koeffizienten $a_{r+t}$ von $f(x)$. Da $f(x) = g(x)h(x)$ ist, ist

$$a_{t+r} = b_0c_{r+t} + \cdots + b_{r-1}c_{t+1} + b_rc_t + b_{r+1}c_{t-1} + \cdots + b_{r+t}c_0$$

Also

$$b_rc_t = a_{r+t} - (b_0c_{r+t} + \cdots + b_{r-1}c_{t+1}) - (b_{r+1}c_{t-1} + \cdots + b_{r+t}c_0)$$

Nach Voraussetzung teilt $p$ den Koeffizienten $a_{r+t}$. Ausserdem teilt $p$ jeden Term in der ersten Klammer (da $r$ minimal war mit $p \nmid b_i$) und $p$ teilt jeden Term in der zweiten Klammer ($t$ war minimal mit $p \nmid c_j$). Insgesamt teilt $p$ jeden Term auf der rechten Seite, also auch die linke Seite, $p \mid b_rc_t$. Da $p$ prim ist, folgt daraus, $b \mid b_r$ oder $b \mid c_t$ (Einf Alg). Widerspruch.

**Korollar 7.4** (Lemma von Gauss)**.** *Sei $R$ ein UFD. Dann ist das Produkt von primitiven Polynomen in $R[x]$ wieder primitiv.*

*Beweis.* Sind $g(x)$ und $h(x)$ primitiv und ist $g(x)h(x)$ nicht primitiv, so ist $g(x)h(x)$ teilbar durch ein $c \in R$, das keine Einheit ist. Jeder irreduzible Faktor $p$ von $c$ teilt auch das Produkt $g(x)h(x)$. Nach Lemma 7.2 teilt $p$ dann $g(x)$ oder $h(x)$, ein Widerspruch zur Primitivität der beiden. □

**Satz 7.5.** *Sei $R$ faktoriell und seien $r, s$ Elemente $\neq 0$ von $R$. Sind $f(x)$ und $g(x)$ primitive Polynome von $R[x|$ mit $rf(x) = sg(x)$, so sind $r$ und $s$ in $R$ assoziiert, sowie $f(x)$ und $g(x)$ in $R[x]$ assoziiert.*

*Beweis.* Ist $r$ eine Einheit, so ist $f(x) = r^{-1}sg(x)$. Da $r^{-1}s$ das primitive Polynom $f(x)$ teilt, muss $r^{-1}s$ eine Einheit sein, etwa $(r^{-1}s)u = 1_R$. Damit sind $f(x)$ und $g(x)$ assoziiert in $R[x]$. Ausserdem ist $u$ eine Einheit in $R$ und $su = r$, also sind $r$ und $s$ assoziiert in $R$.

Ist $r$ keine Einheit, so schreiben wir $r = p_1 \cdots p_m$, wobei jedes $p_i$ ein irreduzibles Element von $R$ ist. Es ist dann $p_1 \cdots p_m f(x) = sg(x)$, also teilt $p_1$ das Element $sg(x)$. Nach Lemma 7.2 teilt $p_1$ dann $s$ oder $g(x)$. Da $p_1$ keine Einheit ist und $g(x)$ primitiv ist, muss $p_1$ also $s$ teilten, wir schreiben $s = p_1 t$. Das gibt $p_1 \cdots p_m f(x) = sg(x) = p_1 tg(x)$. Wir kürzen $p_1$ und erhalten $p_2 \cdots p_m f(x) = tg(x)$. Analog gehen wir mit $p_2$ vor und erhalten $p_3 \cdots p_m f(x) = zg(x)$ mit $p_2 z = t$ und $p_1 p_2 z = p_1 t = s$. Nach $m$ solchen Schritten haben wir $f(x) = wg(x)$ mit $s = p_1 \cdots p_m w$ (für ein $w \in R$). Da $w$ das primitive Polynom $f(x)$ teilt, ist $w$ eine Einheit. Also sind $f(x)$ und $g(x)$ assoziiert in $R[x]$. Weil $s = p_1 \cdots p_m w = rw$ gilt, sind $r$ und $s$ assoziiert in $R$. □

**Korollar 7.6.** *Sei $R$ faktoriell und $k$ sein Quotientenkörper. Seien $f(x)$, $g(x)$ zwei primitive Polynome in $R[x]$. Sind $f(x)$ und $g(x)$ assoziiert in $k[x]$, so sind sie assoziiert in $R[x]$.*

*Beweis.* Sind $f(x)$ und $g(x)$ assoziert in $k[x]$, so gilt $g(x) = \frac{r}{s} f(x)$ für ein Element $0 \neq \frac{r}{s}$ von $k$ (die Einheiten in $k[x]$ sind die von Null verschiedenen konstanten Polynome). Also gilt $sg(x) = rf(g)$ in $R[x]$. Mit Satz 7.5 folgt dann die Behauptung. □

[Vorlesung 11, 11. November 2014]

**Korollar 7.7.** *$R$ sei ein UFD und $k$ sein Quotientenkörper. Hat $f(x) \in R[x]$ positiven Grad und ist irreduzibel in $R[x]$, so ist $f(x)$ irreduzibel in $k[x]$.*

*Beweis.* (Widerspruch) Falls $f(x)$ nicht irreduzibel in $k[x|$ ist, können wir $f(x) = g(x)h(x)$ schreiben mit $g(x)$ und $h(x)$ Elemente aus $k[x]$ mit positivem Grad. Sei $b$ ein kgV der Nenner der Koeffizienten von $g(x)$. Dann liegen die Koeffizienten von $bg(x)$ in $R$. Also ist $bg(x) = ag_1(x)$ mit $a \in R$ und $g_1(x)$ primitiv, von positivem Grad, in $R[x]$ und es ist $g(x) = \frac{a}{b} g_1(x)$. Analog findet man $h(x) = \frac{c}{d} h_1(x)$, wobei $c, d \in R$ sind und $h_1(x)$ ein primitives Element von positivem Grad von $R[x]$ ist. Damit ist

$$f(x) = g(x)h(x) = \frac{a}{b} g_1(x) \frac{c}{d} h_1(x) = \frac{ac}{bd} g_1(x)h_1(x),$$

d.h. es ist $bdf(x) = acg_1(x)h_1(x)$ in $R[x]$. Da $f(x)$ irreduzibel ist in $R[x]$, ist es primitiv. Das Produkt $g_1(x)h_1(x)$ ist primitiv nach dem Lemma von Gauss (Korollar 7.4). Damit sind $bd$ und $ac$ assoziiert (Satz 7.5), $bdu = ac$ für eine

Einheit $u \in R$. Das liefert

$$f(x) = \frac{ac}{bd} g_1(x)h_1(x) = ug_1(x)h_1(x).$$

Nun sind $ug_1(x)$ und $h_1(x)$ Polynome in $R[x]$ von positivem Grad, das widerspricht also der Irreduzibilität von $f(x)$ in $R[x]$, $f(x)$ muss also auch in $k[x]$ irreduzibel sein. □

Damit haben wir nun alles zusammen, um den Hauptsatz dieses Kapitels zu beweisen.

**Satz 7.8.** *Ist $R$ ein UFD, so ist auch $R[x]$ ein UFD.*

*Beweis.* Sei $f(x)$ ein Element von $R[x]$, das weder eine Einheit noch das Nullelement ist. Nach Satz 7.1 ist $f(x)$ ein Produkt von Irreduziblen. Hat $f(x)$ Grad 0, dann ist diese Faktorisierung eindeutig (da $R$ faktoriell ist). Also betrachten wir den Fall, wo $f(x)$ positiven Grad hat. Jede Faktorisierung von $f(x)$ besteht aus einem Produkt von irreduziblen Konstanten[8] (irreduziblen Elementen von $R$) mit einem Produkt von irreduziblen Polynomen von positivem Grad. Seien

$$c_1 \cdots c_m p_1(x) \cdots p_r(x) = d_1 \cdots d_n q_1(x) \cdots q_t(x)$$

zwei solche Faktorisierungen, $c_i$ und $d_j$ irreduzible Elemente in $R$ (mit $m, n \geq 0$), jedes $p_i(x)$, $q_j(x)$ ist irreduzibel (und somit primitiv), von positivem Grad (dabei müssen $r$ und $t$ beide $\geq 1$ sein). Wir müssen zeigen, dass die beiden Faktorisierungen gleich sind (bis auf Assoziiertheit). Nach Korollar 7.4 sind die Produkte $p_1(x) \cdots p_r(x)$ und $q_1(x) \cdots q_t(x)$ primitiv. Nach Satz 7.5 ist das Produkt $c_1 \cdots c_m$ zu $d_1 \cdots d_n$ assoziiert in $R$ und $p_1(x) \cdots p_r(x)$ ist assoziiert zu $q_1(x) \cdots q_t(x)$ in $R[x]$. Wir können schreiben $c_1 \cdots c_m = ud_1 \cdots d_n$ für eine Einheit $u \in R$. Assoziierte von irreduziblen Elementen sind auch irreduzibel (selber überlegen), also ist $ud_1$ irreduzibel. Weil $R$ ein UFD ist, gilt $m = n$ und $c_1$ ist assoziiert zu $ud_1$ sowie zu $d_1$, $c_i$ assoziiert zu $d_i$ für $i \geq 2$ (dies alles nach allfälligem Umnummerieren).

Sei $k$ der Quotientenkörper von $R$. Jedes der Polynome $q_i(x)$, $q_j(x)$ ist irreduzibel in $k[x]$ (Korollar 7.7). In $k[x]$ haben wir eindeutige Faktorisierung, denn $k[x]$ ist ein euklidischer Bereich (mit der Gradabbildung $\delta : k[x] \setminus \{0_{k[x]}\} \to \mathbb{Z}_{\geq 0}$) ein analoges Argument wie oben zeigt, dass $r = t$ sein muss und dass (nach allfälligem Umnummerieren) $p_i(x)$ in $k[x]$ assoziiert ist zu $q_i(x)$ für $i = 1, \ldots, r$. Nach Korollar 7.6 sind sie auch in $R[x]$ assoziiert, die Behauptung folgt. □

**Korollar 7.9.** *$\mathbb{Z}[x]$ ist ein UFD, der kein Hauptidealbereich ist.*

Das ist eine direkte Folge der eindeutigen Faktorisierung in $\mathbb{Z}$, des Satzes 7.8 und von Beispiel 5.1.

[8]Es ist möglich, dass eine solche Faktorisierung keine Konstanten enthält, die nicht Einheiten sind.

## **Teil** 3. Körpererweiterungen

Ziel dieses Kapitels ist, die Grundtheorie von Körpern und ihren Erweiterungen bereit zu stellen, die für die Galoistheorie nötig sind. Dabei geht es meist um das Zusammenspiel zwischen einem Körper und seinen verschiedenen Unterkörpern.

Aus der Schule kennt man v.a. die Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, sowie die Vektorräume $\mathbb{R} \times \mathbb{R}$ und $\mathbb{R}^3$. Ein Grossteil der klassischen Mathematik spielt sich in $\mathbb{C}$ und Unterkörpern davon ab. Es gibt jedoch auch andere Körper (z.B. kennen wir aus [EA] die endlichen Körper $\mathbb{Z}_p$, $p$ prim), sie spielen ebenso eine wichtige Rolle in neueren Gebieten der Mathematik (Analysis, Algebraische Geometrie, Zahlentheorie), Anwendungen finden sich z.B. in der Kodierungstheorie, in der algebraischen Kryptographie.

### 8. Wiederholung und Bemerkungen über Körper

Wiederholung: Sei $k$ ein Körper. Ein $k$-Vektorraum (oder ein Vektorraum über $k$) ist eine additive abelsche Gruppe $V$ mit einer Skalarmultiplikation, so dass für alle $a$, $a_1$, $a_2 \in k$ und für alle $v$, $v_1$, $v_2 \in V$ gilt:

$$\begin{array}{lrcl} (i) & a(v_1+v_2) & = & av_1+av_2 \\ (ii) & (a_1+a_2)v & = & a_1v+a_2v \\ (iii) & a_1(a_2v) & = & (a_1a_2)v \\ (iv) & 1_kv & = & v \end{array}$$

Ein paar bekannte Beispiele von Körpern sind hier:

**Beispiele.**

(1) Die Menge $M_2(\mathbb{R})$ der $2 \times 2$-Matrizen mit Einträgen in $\mathbb{R}$, mit Skalarmultiplikation $\lambda A = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$ für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\lambda \in \mathbb{R}$. Die Addition von Matrizen ist kommutativ, wie verlangt. Also ist $M_2(\mathbb{R})$ ein $\mathbb{R}$-Vektorraum. (Was ist das Neutralelement der Addition? Was das Negative einer Matrix?).

(2) Die Menge $\mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q}$ ist eine Gruppe unter der Addition, mit Nullelement $(0,0)$, das Negative zu $(s,t)$ ist $(-s,-t)$. Die Skalarmultiplikation ist $\lambda(s,t) = (\lambda s, \lambda t)$ (für jedes $\lambda \in \mathbb{Q}$). Damit wird $\mathbb{Q}^2$ zum Vektorraum über $\mathbb{Q}$.

(3) Das obige Beispiel funktioniert natürlich für jeden Körper $k$ (anstelle von $\mathbb{Q}$) und für jedes $n \geq 1$: Die Menge $k^n$ ist ein VR über $k$. (Man überlege sich, wie Addition, Skalarmultiplikation aussehen).

(4) Die komplexen Zahlen $\mathbb{C}$ bilden einen $\mathbb{R}$-Vektorraum. Addition von komplexen Zahlen wie üblich, Skalarmultiplikation ist auch die übliche Multiplikation (multipliziert man eine komplexe Zahl mit $\lambda \in \mathbb{R}$, so ist das Resultat wiederum eine komplexe Zahl).

Das letzte Beispiel ist speziell, dort haben wir als Vektorraum einen Körper (nämlich $\mathbb{C}$) über einem Körper (nämlich $\mathbb{R}$). Dazu folgender Begriff:

**Definition.** Sind $k \subseteq F$ zwei Körper, so sagen wir, $F$ sei ein *Erweiterungskörper von* $k$.

**Bemerkung.** Ist $F$ ein Erweiterungskörper von $k$, so ist $F$ ein VR über $k$, wobei die Addition von Vektoren die übliche Addition in $F$ ist und die Skalarmultiplikation die übliche Multiplikation in $F$ ist (dabei wird ein Element von $F$ mit einem Element von $k$ multipliziert, das Ergebnis ist natürlich auch ein Element von $F$).

In diesem Kapitel interessieren wir uns v.a. für VRe, die Erweiterungskörper sind.

Weiter Begriffe aus der linearen Algebra: sind $v_1, \dots, v_n$ Vektoren eines VRs $V$ über $k$ und lässt sich jedes $v \in V$ als Linearkombination der $v_i$ schreiben, so sagen wir, $\{v_1, \dots, v_n\}$ spannt $V$ über $k$ auf. Eine Menge $\{v_1, \dots, v_n\} \subset V$ heisst linear unabhängig (über $k$), falls aus

$$c_1 v_1 + \cdots + c_n v_n = 0$$

(mit $c_i \in k$) immer folgt, dass $c_1 = \cdots = c_n = 0$ ist. Andernfalls heisst die Menge linear abhängig. Spannt eine linear unabhängige Menge $\{v_1, \dots, v_n\}$ den VR $V$ auf, so heisst die Menge eine Basis von $V$. Ist $V$ ein $k$-VR, so besitzt jede Basis von $V$ dieselbe Anzahl Elemente. Hat $V$ eine endliche Basis, so nennt man die Anzahl der Vektoren in einer Basis die Dimension von $V$ (über $k$). Wir schreiben in dem Fall $[V : k]$ für die Dimension von $V$ über $k$. Hat $V$ keine endliche Basis, so heisst $V$ unendlich-dimensional über $k$.

**Beispiele.** A) Die Dimension von $k^n$ über $k$ ist gleich $n$. Als Basis kann man die Menge $\{(1, 0, \dots, 0), (0, 1, 0, \dots), \dots, (0, \dots, 0, 1)\}$ der Einheitsvektoren wählen (die 1 ist das Einselement von $k$).

B) Die Menge $\{1, i\}$ ist eine Basis von $\mathbb{C}$ über $\mathbb{R}$. Die Menge $\{1 + i, 2i\}$ ist auch eine Basis von $\mathbb{C}$ über $\mathbb{R}$. Die komplexen Zahlen bilden also einen 2-dimensionalen VR über den reellen Zahlen.

8.1. **Anwendungen zum Begriff Körpererweiterung.** Für diesen Kapitel sei $K$ ein Erweiterungskörper von $k$. Wir sagen, $K$ sei eine *endlich-dimensionale Erweiterung* von $k$, falls $K$, als $k$-VR aufgefasst, endlich-dimensional ist.

**Bemerkung.** Ist $[K : k] = 1$ und $\{u\}$ eine Basis von $K$, so ist jedes Element von $K$ von der Form $cu$ (mit $c \in k$). Insbesondere ist $1_k = cu$ (für ein $c$) und damit liegt $u = c^{-1}$ in $k$. Also ist $k = K$ (da das Basiselement $u$ in $k$ liegt).

Ist $k = K$, so ist $\{1_k\}$ eine Basis von $K$, also $[K : k] = 1$. Damit gilt

$$[K : k] = 1 \quad \Longleftrightarrow \quad K = k$$

Sind $k, K$ und $L$ Körper mit $k \subseteq K \subseteq L$, so kann man $K$ und $L$ als $k$-VRe auffassen. Man kann $L$ auch als $K$-VR auffassen. Für die entsprechenden Dimensionen gilt dann:

**Satz 8.1.** *Seien $k, K$ und $L$ Körper mit $k \subseteq K \subseteq L$. Sind $[K : k]$ und $[L : K]$ endlich, so ist auch $L$ eine endlich-dimensionale Erweiterung von $k$ und es gilt $[L : k] = [L : K][K : k]$.*

*Beweis.* Sei $m = [K : k]$ und $n = [L : K]$. Dann existieren Basen $\{u_1, \dots, u_m\}$ von $K$ über $k$ und $\{v_1, \dots, v_n\}$ von $L$ über $K$. Keines der $u_i$ und der $v_j$ ist Null (sonst wären die Mengen linear abhängig), also ist auch keines der Produkte $u_i v_j$ gleich Null. Die Menge der Produkte $\{u_i v_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ hat genau $n \cdot m$ Elemente (keine zwei davon können gleich sein, denn aus $u_i v_j = u_k v_t$ würde $u_i v_j - u_k v_t = 0_K$ folgen, mit $u_i$, $u_k \in K$, damit wären die $v_j$ linear abhängig über $K$). Wir müssen nur noch zeigen, dass diese Menge mit $mn$ Elementen eine Basis von $L$ über $k$ bildet, denn dann ist $[L : k] = nm = [L : K][K : k]$. Das machen wir mit einsetzen: Sei $w$ ein beliebiges Element von $L$, $w$ ist also Linearkombination der $v_j$, etwa

$$w = b_1 v_1 + \cdots + b_n v_n \qquad \text{wobei jedes } b_j \text{ in } K \text{ liegt.}$$

Die Elemente $b_j$ selber sind Linearkombinationen der $u_i$, also existieren Elemente $a_{ij} \in k$ mit

$$\begin{aligned} b_1 &= a_{11}u_1 + \cdots + a_{m1}u_m \\ b_2 &= a_{12}u_1 + \cdots + a_{m2}u_m \\ &\vdots \\ b_n &= a_{1n}u_1 + \cdots + a_{m2}u_m \end{aligned}$$

Setzt man die rechten Seiten dieser $n$ Gleichungen in den Ausdruck für $w$ ein, so sieht man, dass $w$ eine Linearkombination der $u_i v_j$ ist, die Menge der Produkte $\{u_i v_j \mid i \leq m, j \leq n\}$ spannt also $L$ über $k$ auf.

Es bleibt nun noch die lineare Unabhängigkeit zu zeigen. Seien $c_{ij} \in k$ und es sei

$$\sum_{ij} c_{ij} u_i v_j = c_{11}u_1v_1 + c_{12}u_1v_2 + \cdots + c_{mn}u_m v_n = 0$$

Ordnet man die rechte Seite nach Summanden mit $v_1$, mit $v_2$, etc., so erhält man

$$\begin{aligned} &(c_{11}u_1 + c_{21}u_2 + \cdots + c_{m1}u_m)v_1 + \\ &\quad (c_{12}u_1 + c_{22}u_2 + \cdots + c_{m2}u_m)v_2 \\ &\qquad + \cdots + (c_{1n}u_1 + c_{2n}u_2 + \cdots + c_{mn}u_m)v_n = 0_k \end{aligned}$$

Die Koeffizienten der $v_i$ sind Elemente von $K$ und die $v_i$ sind linear unabhängig, also muss jeder dieser Koeffizienten gleich Null sein. D.h. für $j = 1, \dots, n$ gilt

$$c_{1j}u_1 + c_{2j}u_2 + \cdots + c_{mj}u_m = 0_k.$$

Da alle $c_{ij}$ in $k$ sind und die $u_i$ linear unabhängig sind, muss also auch gelten $c_{ij} = 0_k$ für jedes $i$, $j$. Damit haben wir die lineare Unabhängigkeit auch gezeigt. □

Der folgende Satz ist nötig für den Satz 11.4 im Kapitel 11.

**Satz 8.2.** *Seien $K$ und $L$ endlich-dimensionale Körpererweiterungen von $k$ und sei $f : K \to L$ ein Isomorphismus mit $f(c) = c$ für jedes $c \in k$. Dann gilt $[K : k] = [L : k]$.*

*Beweis.* Sei $[K : k] = n$ und es sei $\{u_1, \dots, u_n\}$ eine Basis von $K$ über $k$. Wir müssen zeigen, dass $[L : k] = n$ ist. Dazu reicht es, wenn wir zeigen, dass die Menge $\{f(u_1), \dots, f(u_n)\}$ eine Basis von $L$ über $k$ ist.

Sei $v \in L$. Da $f$ ein Isomorphismus ist, gilt $v = f(u)$ für ein $u \in K$. Wir schreiben $u$ mit der Basis von $K$, $u = c_1u_1 + \dots c_nu_n$ mit $c_i \in k$ für jedes $i$. Damit ist $v = f(u) = f(c_1u_1 + \dots c_nu_n) = f(c_1)f(u_1) + \dots f(c_n)f(u_n)$. Da der Isomorphismus jedes Elemenent von $k$ festhält ist $f(c_i) = c_i$ für jedes $i$. D.h. $v = c_1f(u_1) + \dots c_nf(u_n)$. Die Menge $\{f(u_1), \dots, f(u_n)\}$ spannt also $L$ auf. Um die lineare Unabhängigkeit zu sehen, nehmen wir an, dass

$$d_1f(u_1) + \dots + d_nf(u_n) = 0_k$$

gilt, mit $d_i \in k$. Wegen $f(d_i) = d_i$ erhalten wir,

$$\begin{aligned} f(d_1u_1 + \dots + d_nu_n) &= f(d_1)f(u_1) + \dots + f(d_n)f(u_n) \\ &= d_1f(u_1) + \dots + d_nf(u_n) = 0_k \end{aligned}$$

Als Isomorphismus ist $f$ injektiv. Es muss also bereits $d_1u_1 + \dots + d_nu_n = 0_k$ gelten. Die $u_i$ sind linear unabhängig, also sind $d_1 = \dots = d_n = 0_k$. Die Menge $\{f(u_1), \dots, f(u_n)\}$ ist damit eine Basis von $L$. □

[Vorlesung 12, 14. November 2014]

## 9. Erweiterungen, in beide Richtungen

Körpererweiterungen kann man von zwei Standpunkten her untersuchen. Von einem Körper kann man aufwärts seine Körperweiterungen studieren oder abwärts die Körper betrachten, die er enthält. Zuerst mal aufwärts. Nachher dann, in Kapitel 9.2, geht es abwärts, dort diskutieren wir die einfachen Erweiterungen.

### 9.1. Der Körper der Kongruenzklassen zu einem irreduziblen Polynom.

Sei $k$ ein Körper. Ein irreduzibles Polynom $p(x)$ in $k[x]$ hat nicht immer eine Nullstelle (im Englischen: root) in $k$ (ausser, es ist linear). Indem man die Kongruenzklassen modulo $p(x)$ anschaut, erhält man ein Körpererweiterung von $k$ mit der Eigenschaft, dass das Polynom $p(x)$ in diesem grösseren Körper eine Nullstelle enthält.

**Definition.** Sei $k$ ein Körper, seien $f(x)$, $g(x)$ und $p(x)$ Polynome in $k[x]$, $p(x)$ nicht das Nullpolynom. Dann heisst $f(x)$ *kongruent zu* $g(x)$ *modulo* $p(x)$, geschrieben $f(x) \equiv g(x) \pmod{p(x)}$, falls $p(x)$ die Differenz $f(x) - g(x)$ teilt.

**Beispiele.** In $\mathbb{Q}[x]$ sind $x^2 + x + 1$ und $x + 2$ kongruent modulo $x + 1$:

$$(x^2 + x + 1) - (x + 2) = x^2 - 1 = (x + 1)(x - 1).$$

In $\mathbb{R}[x]$ gilt $3x^4 + 4x^2 + 2x + 2 \equiv x^3 + 3x^2 + 3x + 4 \pmod{x^2+1}$, denn es ist

$(3x^4+4x^2+2x+2)-(x^3+3x^2+3x+4) = 3x^4-x^3+x^2-x-2 = (x^2+1)(3x^2-x-2)$.

**Bemerkung 9.1.** Sei $p(x) \in k[x]$ ein Polynom ungleich Null.
1) Kongruenz modulo $p(x)$ ist eine Äquivalenzrelation (man überlege sich, dass sie reflexiv, symmetrisch, transitiv ist).
2) Sind $f(x) \equiv g(x)$ und $h(x) \equiv m(x)$ (beide modulo $p(x)$), so folgt

$$\begin{aligned} f(x) + h(x) &\equiv g(x) + m(x) \pmod{p(x)} \\ f(x)h(x) &\equiv g(x)m(x) \pmod{p(x)} \end{aligned}$$

**Definition.** Sei $k$ ein Körper, $p(x)$ ein Polynom, nicht Null, in $k[x]$. Die *Kongruenzklasse* von $f(x)$ modulo $p(x)$ ist die Menge aller Polynome in $k[x]$, die kongruent zu $f(x)$ sind modulo $p(x)$, d.h.

$$[f(x)] = \{g(x) \mid g(x) \equiv f(x) \pmod{p(x)}\} = \{f(x) + h(x)p(x) \mid h(x) \in k[x]\}.$$

Die *Menge aller Kongruenzklassen modulo* $p(x)$ wird als

$$k[x]/(p(x))$$

geschrieben.
(Analog zur Definition von $\mathbb{Z}_m$, $m > 0$.)

Auf der Menge $k[x]/(p(x))$ definiert man Addition und Multiplikation wie folgt:

$$\begin{aligned} [f(x)] + [g(x)] &= [f(x) + g(x)] \\ [f(x)][g(x)] &= [f(x)g(x)] \end{aligned}$$

Damit hat man

**Satz 9.2.** *Sei $p(x)$ ein nicht konstantes Polynom. Mit Addition und Multiplikation wie oben definiert wird $k[x]/(p(x))$ zu einem kommutativen Ring, der einen Unterring enthält, der isomorph ist zu $k$.*

*Zum Beweis.* Dass $k[x]/(p(x))$ ein kommutativer Ring ist, soll man sich selber überlegen. Der zu $k$ isomorphe Unterring von $k[x]/(p(x))$, den wir zur Abkürzung $k'$ nennen ist, ist die Menge der Kongruenzklassen der konstanten Polynome, $\{[a] \mid a \in k\}$, man kriegt einen Homomorphismus $\varphi : k \to k'$, indem man $a \in k$ auf die Kongruenzklasse $[a]$ von $a$ schickt. Das ist nach Definition surjektiv. Damit $\varphi$ ein Homomorphismus ist, muss man sehen, dass $\varphi(a+b) = \varphi(a) + \varphi(b)$ ist, sowie dass überlegen, dass das $\varphi(ab) = \varphi(a)\varphi(b)$ ist. Zur Injektivität: sei $\varphi(a) = \varphi(b)$. D.h. dass $[a] = [b]$ ist, m.a. W. $a \equiv b \pmod{p(x)}$. Also teilt $p(x)$ die Differenz $a - b$. Das Polynom $p(x)$ hat aber Grad $\geq 1$ und $a - b \in k$ (Grad 0). Das geht nur für $a - b = 0_k$, d.h. für $a = b$. □

Wir werden $k$ jeweils mit der isomorphen Kopie von $k$ in $k[x]/(p(x))$ identifizieren.

**Beispiel 9.3.** Kongruenz mod $x^2+1$ in $\mathbb{R}[x]$.
Die Kongruenzklasse von $2x+1$ etwa ist

$$\{(2x+1)+g(x)(x^2+1) \mid g(x) \in \mathbb{R}[x]\},$$

also die Menge aller Polynome in $\mathbb{R}[x]$, die Rest $2x+1$ haben nach Division durch $x^2+1$.

Für jeden möglichen Rest bei der Division durch $x^2+1$ haben wir eine Kongruenzklasse.

- Die möglichen Reste sind Polynome der Gestalt

  $$rx+s, \quad r,s \in \mathbb{R}, \text{ beide dürfen 0 sein - dann ist der Rest 0}$$

- Es ist $[rx+s]=[cx+d] \iff rx+s=cx+d$ und letzteres gilt genau dann, wenn $r=c$ und $s=d$ gilt.
  (Allgemeiner: ist der Grad von $p(x)$ gleich $n$ und sind $f(x)$, $h(x)$ zwei Polynome vom Grad $<n$, so ist $[f(x)]=[h(x)]$ in $k[x]/(p(x))$ genau dann, wenn $f(x)=h(x)$ gilt.)

Wir haben damit unendlich viele Elemente in $\mathbb{R}/(x^2+1)$, jedes Element kann eindeutig als $rx+s$ geschrieben werden, mit $r,s \in \mathbb{R}$, all diese sind verschieden.

Falls $p(x)$ irreduzibel ist, ist $k[x]/(p(x))$ selber ein Körper, der $k$ enthält, also eine Körpererweiterung von $k$, wie wir nun sehen werden.

**Satz 9.4.** *Sei $k$ ein Körper, $p(x)$ ein irreduzibles Polynom in $k[x]$. Dann ist $k[x]/(p(x))$ eine Körpererweiterung von $k$, die eine Nullstelle von $p(x)$ enthält.*

*Beweis.* Wir wissen bereits, dass $k$ in $k[x]/(p(x))$ enthalten ist.
Behauptung A): $k[x]/(p(x))$ ist ein Körper.
Die Strategie ist ähnlich wie bei dem Beweis, dass für jede Primzahl $m$ der Restklassenring $\mathbb{Z}_m := \mathbb{Z}/(m\mathbb{Z})$ ein Körper ist ([EA]).

Man benutzt folgende Beobachtung: sind $f(x) \in k[x]$, $f(x) \neq 0_{k[x]}$ und $p(x)$ relativ prim, so ist $[f(x)]$ eine Einheit in $k[x]/(p(x))$.

Sei zunächst $a(x) \in k[x]$ nicht Null. Dann existieren für $a(x)$ und $p(x)$ (beide nicht Null) Polynome $u(x)$ und $v(x)$ mit $d(x)=a(x)u(x)+p(x)v(x)$, wobei $d(x)$ ein ggT von $a(x)$ und $p(x)$ sei (hier ohne Beweis).

Ist $a(x)$ relativ prim zu $p(x)$, so ist ohne Einschränkung $d(x)=1_{k[x]}$ und $u(x)$ ist das Inverse zu $a(x)$ in $k[x]/(p(x))$, denn $a(x)u(x)-1_{k[x]}=p(x)v(x)$, d.h. $a(x)u(x)=1$ modulo $p(x)$, und $a(x)$ ist also invertierbar.

Ist $a(x)$ nicht relativ prim zu $p(x)$, so ist $a(x)$ in der Kongruenzklasse von $0_k$, da $a(x)=p(x)v(x)$ gilt für ein $v(x) \in k[x]$.

Behauptung B): $k[x]/(p(x))$ enthält eine Nullstelle von $p(x)$.
Es sei $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0$ mit $a_i \in k \subseteq K := k[x]/(p(x))$. Sei $\alpha=[x]$ die Kongruenzklasse von $x$ in $K$. Wir zeigen, dass $\alpha$ eine Nullstelle von

$p(x)$ ist. Wir rechnen dazu mit den Kongruenzklassen.

$$\begin{aligned} a_n\alpha^n + \cdots + a_1\alpha + a_0 &= a_n[x]^n + \cdots + a_1[x] + a_0 \\ &= [a_n x^n + \cdots a_1 x + a_0] \\ &= [p(x)] = 0_k \quad \text{da } p(x) \equiv 0_k \text{ ist modulo } p(x) \end{aligned}$$

Damit ist $\alpha \in K$ eine Nullstelle von $p(x)$. □

**Beispiel.** Das Polynom $p(x) = x^2 + x + 1$ hat keine Nullstelle in $\mathbb{Z}_2$, es ist also irreduzibel in $\mathbb{Z}_2[x]$. Nach Satz 9.4 ist der Körper $K := \mathbb{Z}_2[x]/(x^2 + x + 1)$ eine Körpererweiterung von $\mathbb{Z}_2$. Das Polynom $x^2+x+1$ hat eine Nullstelle in $K$: Setzen wir $\alpha = [x]$, so rechnet man

$$\alpha^2 + \alpha + 1 = [x]^2 + [x] + 1 = [x^2 + x + 1] = 0_K$$

**Bemerkung.** Satz 9.4 sagt folgendes aus: Ist $f(x)$ ein nicht konstantes Polynom in $k[x]$, so existiert eine Körpererweiterung zu $k$ in der das Polynom $f(x)$ eine Nullstelle hat. Ein Beispiel sind die komplexen Zahlen, die im 17. Jahrhundert eingeführt wurden. Über dem Körper $\mathbb{C}$ hat das Polynom $x^2 + 1$ eine Nullstelle, nämlich $i$.

**Beispiel** (Fortsetzung von Beispiel 9.3)**.** Zur Abkürzung: $K := \mathbb{R}[x]/(x^2 + 1)$. Dann ist $K \supseteq \mathbb{R}$ eine Körpererweiterung nach Satz 9.4. $K$ besitzt eine Nullstelle von $x^2 + 1$, nämlich $\alpha := [x]$. In $K$ ist $\alpha$ ein Element dessen Quadrat $-1$ ist.

Jedes Element in $K$ ist von der Form $[rx + s]$ oder:

$$[rx + s] = [r][x] + [s] = [r]\alpha + [s] = r\alpha + s$$

Addition und Multiplikation in $K$ sind klar, konkret die Multiplikation:
$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd\alpha^2 = ac - bd + (ad + bc)\alpha$.

Schickt man $\alpha$ auf $i$, so erhält man einen Isomorphismus $K \cong \mathbb{C}$, so lässt sich also $\mathbb{C}$ definieren.

Als nächstes geht es nun abwärts, von einem Körper aus betrachtet man Unterkörper.

9.2. **Einfache Erweiterungen.** Sei $K$ ein Körper, $k$ ein Unterkörper von $K$. Ist $u \in K$, welches sind dann die Unterkörper von $K$, die $u$ enthalten? Gibt es einen kleinsten solchen Körper? Falls $u$ die Nullstelle eines irreduziblen Polynoms $p(x) \in k[x]$ ist, wie ist der Zusammenhang zwischen diesem kleinsten Unterkörper und dem Erweiterungskörper $k[x]/(p(x))$, der auch eine Nullstelle von $p(x)$ enthält?

Die ersten beiden dieser Fragen kann man theoretisch schnell beantworten. Sei $K \supseteq k$ ein Erweiterungskörper von $k$, sei $u \in K$. Dann sei $k(u)$ der Durchschnitt aller Unterkörper von $K$, die $k$ und $u$ enthalten. Da mindestens $K$ ein solcher ist, ist die Familie solcher Unterkörper nicht leer. Der Durchschnitt einer beliebigen Familie von Unterkörpern von $K$ ist immer noch ein Körper (überlegen!), also ist $k(u)$ ein Körper. Nach Definition liegt $k(u)$ in jedem Unterkörper von $K$, der $k$ und $u$ enthält, somit ist $k(u)$ der kleinste solche Körper.

**Definition.** Seien $K$, $k$ und $u \in K$ wie oben. Dann heisst der Körper $k(u)$ eine *einfache Erweiterung von* $k$.

Diese Beschreibung ist nicht sehr explizit. Der Körper $k(u)$ hängt u.a. davon ab, ob $u$ Nullstelle eines Polynoms ist oder nicht.

**Definition.** Ein Element $u$ eines Erweiterungskörpers $K$ von $k$ heisst *algebraisch* über $k$, falls $u$ eine Nullstelle eines Polynoms $\neq 0$ aus $k[x]$ ist. Gibt es kein Polynom $\neq 0$ in $k[x]$ für das $u$ Nullstelle ist, so heisst $u$ *transzendent* über $k$.

**Beispiele.** 1) Im Erweiterungskörper $\mathbb{C}$ von $\mathbb{R}$ ist $i$ algebraisch über $\mathbb{R}$, da $i$ Nullstelle von $x^2+1$ in $\mathbb{R}[x]$ ist. Das Element $2+i \in \mathbb{C}$ ist eine Nullstelle von $x^3-x^2-7x+15 \in \mathbb{Q}[x]$, also ist $2+i$ algebraisch über $\mathbb{Q}$ (nachrechnen). Analog findet man: $\sqrt[5]{3}$ ist algebraisch über $\mathbb{Q}$, da es eine Nullstelle von $x^5-3$ ist.

2) Jedes Element $c$ eines Körpers $k$ ist algebraisch über $k$, da $c$ die Nullstelle des Polynoms $x-c$ in $k[x]$ ist.

3) Die reellen Zahlen $\pi$ und $e$ sind transzendent über $\mathbb{Q}$. (Einen Beweis kann man in [Ni] finden).

Wir werden uns hier auf algebraische Elemente konzentrieren.

Ist $u$ ein algebraisches Element eines Erweiterungskörpers $K$ von $k$, dann kann es viele Polynome in $k[x]$ geben, die $u$ als Nullstelle haben. Der nächste Satz zeigt, dass sie alle Vielfache eines einzigen Polynoms sind. Dank diesem Polynom werden wir eine genaue Beschreibung der einfachen Körpererweiterung $k(u)$ erhalten.

[Vorlesung 13, 18. November 2014]

**Satz 9.5.** *Sei $K$ eine Körpererweiterung von $k$, $u \in K$ algebraisch über $k$. Dann existiert ein eindeutig bestimmtes normiertes*[9]*, irreduzibles Polynom $p(x) \in k[x]$, das $u$ als Nullstelle hat. Ausserdem gilt: ist $u$ eine Nullstelle von $g(x) \in k[x]$, so teilt $p(x)$ das Polynom $g(x)$.*

*Beweis.* Sei $S := \{g(x) \in k[x] \mid u \text{ ist Nullstelle von } g(x)\}$. $S$ ist nicht leer, da $u$ algebraisch ist über $k$. Die Grade der Polynome in $S$ bilden eine nicht leere Menge von nicht negativen Zahlen, die enthält ein kleinstes Element (Wohlordnungsaxiom). Sei $p(x)$ ein Polynom kleinsten Grades in $S$. Jedes konstante Vielfache (ungleich 0) von $p(x)$ hat auch diesen kleinsten Grad und $u$ als Nullstelle. Wir suchen uns dann $p(x)$ so aus, dass es normiert ist (falls es nicht normiert ist, so multipliziert man mit dem Inversen des führenden Koeffizienten).

Wäre $p(x)$ nicht irreduzibel in $k[x]$, so würden Polynome $s(x)$ und $t(x)$ existieren mit $p(x) = s(x)t(x)$, $\deg s(x) < \deg p(x)$ und $\deg t(x) < \deg p(x)$. Folglich würde gelten $s(u)t(u) = p(u) = 0_k$ in $K$. Da $K$ ein Körper ist, muss dann $s(u) = 0_k$ oder $t(u) = 0_k$ gelten. D.h. $s(x)$ oder $t(x)$ gehört zu $S$. Das ist unmöglich, da $p(x)$ das Polynom vom kleinsten Grad in $S$ ist. Also ist $p(x)$ irreduzibel.

[9] der führende Koeffizient ist $= 1$.

Als nächstes zeigen wir, dass $p(x)$ jedes Polynom $g(x)$ in $S$ teilt. Sei $g(x) \in S$ beliebig. Nach dem Divisionsalgorithmus ist $g(x) = p(x)q(x) + r(x)$, wobei $r(x) = 0_k$ ist oder $\deg r(x) < \deg p(x)$. Da $u$ eine sowohl Nullstelle von $g(x)$ als auch von $p(x)$ folgt

$$r(u) = g(u) - p(u)q(u) = 0_k - 0_k q(u) = 0_k$$

$u$ ist also auch Nullstelle von $r(x)$. Wäre $r(x)$ nicht Null, so würde $r(x)$ auch zu $S$ gehören, ein Widerspruch dazu, dass der Grad von $p(x)$ minimal ist unter den Elementen von $S$. Somit ist $r(x) = 0_k$ und $g(x) = p(x)q(x)$, $p(x)$ teilt also jedes $g(x)$ in $S$.

Um zu sehen, dass $p(x)$ eindeutig ist, nehmen wir an, $t(x)$ sei ein normiertes irreduzibles Polynom in $S$. Dann gilt $p(x) \mid t(x)$. Da $p(x)$ irreduzibel (und nicht konstant) ist und $t(x)$ irreduzibel ist, folgt $t(x) = cp(x)$ für ein $c \in k$. Da $p(x)$ normiert ist, muss $c = 1_k$ sein, $p(x) = t(x)$ und $p(x)$ ist eindeutig bestimmt. □

Ist $K$ ein Erweiterungskörper von $k$ und $u \in K$ algebraisch über $k$, dann nennt man das normierte, irreduzible Polynom aus Satz 9.5 das *Minimalpolynom* von $u$ über $k$. Die Eindeutigkeitsaussage in Satz 9.5 bedeutet Folgendes: haben wir ein normiertes, irreduzibles Polynom in $k[x]$ gefunden, das $u$ als Nullstelle hat, so muss es gerade das Minimalpolynom von $u$ über $k$ sein.

**Beispiele.** A) $x^2 - 3$ ist ein normiertes, irreduzibles Polynom in $\mathbb{Q}[x]$, das $\sqrt{3} \in \mathbb{R}$ als Nullstelle hat. Also ist $x^2 - 3$ das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$. Bemerkung: $x^2 - 3$ ist natürlich reduzibel über $\mathbb{R}$, es faktorisiert, $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ in $\mathbb{R}[x]$. Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{R}$ ist $x - \sqrt{3}$, dieses Polynom ist normiert und irreduzibel in $\mathbb{R}[x]$.

B) Sei $u = \sqrt{3} + \sqrt{5} \in \mathbb{R}$. Dann ist $u^2 = 8 + 2\sqrt{15}$. Also gilt $u^2 - 8 = 2\sqrt{15}$, das liefert $(u^2 - 8)^2 = 60$ bzw. $(u^2 - 8)^2 - 60 = 0$. Somit ist $u = \sqrt{3} + \sqrt{5}$ Nullstelle des Polynoms $(x^2 - 8)^2 - 60 = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. Man überprüfe, dass dieses Polynom irreduzibel ist in $\mathbb{Q}[x]$, damit ist es das Minimalpolynom von $\sqrt{3} + \sqrt{5}$ über $\mathbb{Q}$.

Das Minimalpolynom von $u$ liefert die Verbindung zwischen aufwärts und abwärts gerichtetem Blickwinkel bei einfachen Körpererweiterungen und gibt uns eine nützliche Beschreibung des Körpers $k(u)$.

Wir benötigen noch die folgende Aussage für das Ziel von diesem Abschnitt (Satz 9.7). Der Beweis davon kann z.B. in [Hu] gefunden werden (Theorem 5.10). Die Beweisstrategie ist ähnlich wie bei der Aussage über $\mathbb{Z}_m$ ($m$ ist prim $\Leftrightarrow$ $\mathbb{Z}_m$ ist Körper $\Leftrightarrow$ $\mathbb{Z}_m$ ist Integritätsbereich). Die Implikation (1) $\Rightarrow$ (2) haben wir in Satz 9.4 gezeigt (Behauptung A)), (2) $\Rightarrow$ (3) ist klar.

**Satz 9.6.** *Sei $k$ ein Körper, $p(x)$ ein Polynom in $k[x]$ vom Grad $\geq 1$. Dann sind die folgenden Aussagen äquivalent:*

(1) *Das Polynom $p(x)$ ist irreduzibel in $k[x]$.*
(2) *$k[x]/(p(x))$ ist ein Körper.*

(3) $k[x]/(p(x))$ *ist ein Integritätsbereich.*

**Satz 9.7.** *Sei $K$ Erweiterungskörper von $k$, $u \in K$ ein algebraisches Element über $k$ mit Minimalpolynom $p(x)$ vom Grad $n$. Dann gilt:*

(1) $k(u) \cong k[x]/(p(x))$.
(2) $\{1_k, u, u^2, \ldots, u^{n-1}\}$ *ist eine Basis des Vektorraums $k(u)$ über $k$.*
(3) $[k(u) : k] = n$.

Satz 9.7 zeigt, dass für ein Element $u$, das algebraisch ist über $k$, der Körper $k(u)$ nicht von $u$ abhängt, sondern bereits vollständig durch $k[x]$ bestimmt ist und das Minimalpolynom $p(x)$. Daher sagt man auch, der Körper $k(u)$ sei der Körper, den man erhält, indem man $u$ *zu* $k$ *adjungiert*.

*Beweis von Satz 9.7.* (1): Da $k(u)$ ein Körper ist, der $u$ enthält, muss auch jede positive Potenz von $u$ in $k(u)$ liegen. Da $k(u)$ auch $k$ selbst enthält, liegt jedes Element der Form

$$b_0 + b_1 u + \cdots + b_t u^t \text{ mit } b_i \in k$$

in $k(u)$, d.h. $k(u)$ enthält das Element $f(u)$ für jedes Polynom $f(x) \in k[x]$.

Behauptung: Die Abbildung $\varphi : k[x] \to k(u)$, $\varphi(f(x)) = f(u)$, ist ein Ringhomomorphismus. (Nachprüfen!). Ein Polynom in $k[x]$ liegt im Kern von $\varphi$ genau dann, wenn $u$ eine Nullstelle von diesem Polynom ist. Nach Satz 9.5 ist der Kern von $\varphi$ das Hauptideal $(p(x))$. Nach dem ersten Isomorphiesatz, [EA], ist daher $k[x]/(p(x))$ isomorph $\operatorname{im}\varphi$, dem Bild von $\varphi$.

Ausserdem gilt wegen der Irreduzibilität von $p(x)$, dass der Ring $k[x]/(p(x))$ ein Körper ist (Satz 9.6), also ist auch das Bild $\operatorname{im}\varphi$ ein Körper. Jedes konstante Polynom wird unter $\varphi$ auf sich selbst abgebildet und $\varphi(x) = u$. Daher ist $\operatorname{im}\varphi$ ein Unterkörper von $k(u)$, der $k$ und $u$ enthält. Da $k(u)$ der kleinste Körper ist, der $k$ und $u$ enthält, folgt $k(u) = \operatorname{im}\varphi \cong k[x]/(p(x))$.

(2) und (3): Wegen $k(u) = \operatorname{im}\varphi$ ist jedes Element $\neq 0$ von $k(u)$ von der Form $f(u)$ für ein $f(x) \in k[x]$. Sei $\deg p(x) = n$. Nach dem Divisionsalgorithmus ist $f(x) = p(x)q(x) + r(x)$, für ein $r(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in k[x]$. Daraus folgt $f(u) = p(u)q(u) + r(u) = 0_k q(u) + r(u) = r(u) = b_0 1_k + b_1 u + \cdots + b_{n-1}u^{n-1}$. Die Menge $\{1_k, u, \ldots, u^{n-1}\}$ spannt also $k(u)$ auf.
Für die lineare Unabhängigkeit nehmen wir an, es gelte

$$c_0 + c_1 u + \cdots + c_{n-1}u^{n-1} = 0_k$$

mit $c_i \in k$. Das Element $u$ ist also eine Nullstelle von $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Dieses Polynom (von Grad $\leq n-1$) wird folglich durch $p(x)$ geteilt (und $p(x)$ hat Grad $n$). Dies ist nur möglich, wenn $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ das Nullpolynom ist, i.e. wenn $c_i = 0_k$ ist für jedes $i$. Damit ist die lineare Unabhängigkeit über $k$ gezeigt und $\{1_k, u, \ldots, u^{n-1}\}$ ist eine Basis von $k(u)$, die Behauptung $[k(u) : k] = n$ folgt dann sofort. □

**Beispiel 9.8.** Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ ist $x^2-3$. Wenden wir Satz 9.7 an mit $n = 2$ so sehen wir, dass $\{1, \sqrt{3}\}$ eine Basis von $\mathbb{Q}(\sqrt{3})$ über $\mathbb{Q}$ ist und somit ist $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Analog sieht man aus dem vorherigen Beispiel (Beispiel B weiter oben), dass das Minimalpolynom von $\sqrt{3} + \sqrt{5}$ über $\mathbb{Q}$ das Polynom $x^4 - 16x^2 + 4$ ist, also gilt $[\mathbb{Q}(\sqrt{3} + \sqrt{5}), \mathbb{Q}] = 4$ und die Menge $\{1, \sqrt{3} + \sqrt{5}, (\sqrt{3} + \sqrt{5})^2, (\sqrt{3} + \sqrt{5})^3\}$ ist eine Basis.

Eine direkte Folge von Satz 9.7 ist:
*haben $u$ und $v$ dasselbe Minimalpolynom $p(x)$ in $k[x]$, so gilt $k(u) \cong k(v)$.*
Dies gilt übrigens auch, wenn $u$ und $v$ nicht im gleichen Erweiterungskörper von $k$ liegen. Im Rest dieses Kapitels werden wir diese Idee verallgemeinern. Am besten betrachte man dazu zuerst Beispiel 9.10, es illustriert das Korollar 9.9. Wir werden die Überlegungen um Korollar 9.9 dann im Kapitel 11 brauchen.

[Vorlesung 14, 21. November 2014]

Seien $F$ und $E$ zwei Körper, sei $\sigma : F \to E$ ein Isomorphismus. Man überzeuge sich davon, dass die Abbildung $F[x] \to E[x]$, die $f(x) = a_0 + a_1x + \cdots + a_nx^n$ auf das Polynom $\sigma f(x) := \sigma(a_0)+\sigma(a_1)x+\ldots\sigma(a_n)x^n$ schickt, ein Ringisomorphismus ist. Unter dieser Abbildung wird jedes konstante Polynom $f(x) = c$ in $F[x]$ auf das Element $\sigma(c) \in E$ geschickt. Man sagt daher, der Isomorphismus $F[x] \to E[x]$ sei eine *Erweiterung* des Isomorphismus $\sigma : F \to E$, wir schreiben auch $\sigma$ für den Isomorphismus von $F[x]$ nach $E[x]$.

**Korollar 9.9.** *Sei $\sigma : F \to E$ ein Körperisomorphismus. Sei $u$ ein algebraisches Element in einem Erweiterungskörper von $F$, mit Minimalpolynom $p(x) \in F[x]$. Sei $v$ ein algebraisches Element in einem Erweiterungskörper von $E$ mit Minimalpolynom $\sigma p(x) \in E[x]$. Dann lässt sich $\sigma$ zu einem Körperisomorphismus $\overline{\sigma} : F(u) \to E(v)$ erweitern mit $\overline{\sigma}(u) = v$ und $\overline{\sigma}(c) = \sigma(c)$ für jedes $c \in F$.*

Im Spezialfall, wo $\sigma$ die Identitätsabbildung $F \to F$ ist, bedeutet dies: Haben $u$ und $v$ dasselbe Minimalpolynom, so gibt es einen Isomorphismus $F(u) \cong F(v)$, der $u$ auf $v$ abbildet und jedes Element von $F$ auf sich selbst.

Das Beispiel 9.10 weiter unten illustriert das Korollar am Fall $F = E$. Der Beweis von Korollar 9.9 ist der Vollständigkeit halber hier, in der Vorlesung wurde er ausgelassen.

*Beweis.* Nach den Bemerkung vor dem Korollar kann der Isomorphismus $\sigma$ zu einem Isomorphismus $F[x] \to E[x]$ erweitert werden, den wir auch mit $\sigma$ bezeichnen. Nach dem Beweis von Satz 9.7 existiert ein Isomorphismus
$\overline{\tau} : E[x]/(\sigma p(x)) \to E(v)$, der durch $\overline{\tau}[g(x)] = g(v)$ definiert ist. Sei $\pi$ der surjektive Homomorphismus

$$E[x] \to E[x]/(\sigma p(x))$$

der $g(x)$ auf $[g(x)]$ abbildet. Wir betrachten die Verknüpfungen

$$\begin{array}{ccccccc} F[x] & \xrightarrow{\sigma} & E[x] & \xrightarrow{\pi} & E[x]/(\sigma p(x)) & \xrightarrow{\overline{\tau}} & E(v) \\ f(x) & \mapsto & \sigma f(x) & \mapsto & [\sigma f(x)] & \mapsto & \sigma f(v) \end{array}$$

Da alle drei Abbildungen surjektiv sind, ist die Verknüpfung auch surjektiv. Der Kern dieser Verknüpfung sind die $h(x) \in F[x]$ mit $\sigma h(v) = 0_E$. Da $\overline{\tau}$ ein Isomorphismus ist, ist $\sigma h(v) = 0_E$ genau dann, wenn $[\sigma h(x)]$ in der Klasse der Null von $E[x]/(\sigma p(x))$ liegt, d.h. genau dann, wenn $\sigma h(x)$ ein Vielfaches ist von $\sigma p(x)$. Aus $\sigma h(x) = k(x) \cdot \sigma p(x)$ folgt jedoch, indem man die Umkehrung des Isomorphismus $\sigma$ anwendet, dass $h(x) = (\sigma^{-1}k(x))p(x)$ ist. Also ist der Kern der Verknüpfung der drei Funktionen das Hauptideal $(p(x))$ in $F[x]$. Nach dem ersten Isomorphiesatz gilt daher $F[x]/(p(x)) \cong E(v)$. Der Isomorphism (nennen wir ihn $\theta$) wird durch $\theta([f(x)]) = \sigma f(v)$ gegeben. Es gilt dabei $\theta([x]) = v$ und $\theta([c]) = \sigma(c)$ für jedes $c \in F$. Wir sind damit in der folgenden Situation (mit dem Isomorphismus $\overline{\varphi}$ aus Satz 9.7):

$$\begin{array}{ccccccc} F[u] & \xleftarrow{\overline{\varphi}} & F[x]/(p(x)) & \xrightarrow{\theta} & E(v) & & \\ f(u) & \leftarrow\!\shortmid & [f(x)] & \mapsto & \sigma f(v) & & \\ c & \leftarrow\!\shortmid & [c] & \mapsto & \sigma c & & c \in F \end{array}$$

Die Verknüpfung $\theta \circ \overline{\varphi}^{-1} : F(u) \to E(v)$ ist ein Isomorphismus, der die Abbildung $\sigma$ erweitert und $u$ auf $v$ schickt. □

**Beispiel 9.10.** Das Polynom $x^3 - 2$ ist irreduzibel in $\mathbb{Q}[x]$ (das folgt direkt mit dem Kriterium von Eisenstein[10]
In $\mathbb{R}$ hat es die Nullstelle $\sqrt[3]{2}$. Man überprüfe, dass für $\omega = \frac{-1+\sqrt{3}i}{2}$ eine dritte Wurzel der Eins das Element $\sqrt[3]{2}\omega \in \mathbb{C}$ auch Nullstelle von $x^2 - 3$ ist.

Wendet man Korollar 9.9 auf die Identitätsabbildung $\mathbb{Q} \to \mathbb{Q}$ an, so sieht man, dass der reelle Unterkörper $\mathbb{Q}(\sqrt[3]{2})$ (von $\mathbb{C}$) isomorph ist zum komplexen Unterkörper $\mathbb{Q}(\sqrt[3]{2}\omega)$ unter einer Abbildung, die $\sqrt[3]{2}$ auf $\sqrt[3]{2}\omega$ schickt und jedes Element von $\mathbb{Q}$ auf sich selbst.

## 10. Algebraische Erweiterungen

Im Kapitel 9.2 ging es um einzelne algebraische Elemente. Hier betrachten wir Körpererweiterungen, die ganz aus algebraischen Elementen bestehen:

**Definition.** Eine Körpererweiterung $K$ von $k$ heisst *algebraische Erweiterung* von $k$, falls jedes Element von $K$ algebraisch ist über $k$.

**Beispiel.** Jedes beliebige Element $a + ib \in \mathbb{C}$ ist eine Nullstelle von

$$(x - (a + bi))(x - (a - bi)) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$$

[10]Erkärungen dazu in [Co], Artikel von Gotthold Eisenstein, 1850 im Crelle Journal veröffentlicht, bereits vorher von T. Schönemann im Crelle Journal veröffentlicht, siehe Wikipedia [W2]. Es lohnt sich, den Beweis des Kriteriums anzuschauen (auch dort)

Damit ist jedes beliebige Element $a + ib$ von $\mathbb{C}$ algebraisch über $\mathbb{R}$, daher ist $\mathbb{C}$ eine algebraische Körpererweiterung von $\mathbb{R}$.

Andrerseits sind weder $\mathbb{R}$ noch $\mathbb{C}$ eine algebraische Erweiterung von $\mathbb{Q}$, da es reelle Zahlen gibt, die nicht algebraisch sind über $\mathbb{Q}$ (z.B. $e$, $\pi$). Siehe dazu auch Bemerkung 10.4.

Jedes algebraische Element $u$ über $k$ liegt in einem endlich-dimensionalen Erweiterungskörper von $k$, nämlich in $k(u)$ (Satz 9.7). Beginnen wir andrerseits mit einer endlich-dimensionalen Körpererweiterung von $k$, so haben wir das folgende Resultat:

**Satz 10.1.** *Ist $K$ eine endlich-dimensionale KE*[11] *von $k$, so ist $K$ eine algebraische Erweiterung von $k$.*

*Beweis.* Nach Voraussetzung besitzt $K$ eine endliche Basis über $k$, sagen wir $\{v_1, \dots, v_n\}$. Da diese $n$ Elemente $K$ aufspannen hat jede linear unabhängige Menge in $K$ höchstens $n$ Elemente. Ist $u \in K$ und gilt $u^i = u^j$ für $0 \leq i < j$, so ist $u$ eine Nullstelle von $x^i - x^j \in k[x]$ und damit algebraisch.

Für jedes andere Element $u \in K$ ist die Menge $\{1_k, u, u^2, \dots, u^n\}$ eine Menge mit $n + 1$ Elementen, muss also linear abhängig sein über $k$. Damit existieren $c_i \in k$, nicht alle gleich 0, so dass $c_0 1_k + c_1 u + \cdots + c_n u^n = 0_k$ gilt. Also ist $u$ Nullstelle des Polynoms $c_0 + c_1 x + \cdots + c_n x^n \in k[x]$ (das ungleich ist) und somit algebraisch über $k$. □

**Bemerkung.** Enthält ein Erweiterungskörper $K$ von $k$ ein transzendentes Element $u$, so muss $K$ unendlich-dimensional sein über $k$ (sonst wäre $u$ algebraisch nach Satz 10.1). Die Umkehrung von Satz 10.1 gilt jedoch nicht, es existieren unendlich-dimensionale algebraische Erweiterungen.

Ist $k(u)$ eine einfache Körpererweiterungen, so muss man nur überprüfen, ob $u$ algebraisch ist über $k$, um zu wissen, dass ganz $k(u)$ eine algebraische KE ist, denn $k(u)$ ist nach Satz 9.7 endlich-dimensional und somit nach Satz 10.1 algebraisch.

Diese Eigenschaft suggeriert die folgende Verallgemeinerung des Begriffs "einfache KE": Körper, bei denen es ausreicht, für eine endliche Anzahl ihrer Elemente zu überprüfen, ob sie algebraisch sind.

Sind $u_1, \dots, u_n$ Elemente eines Erweiterungskörper $K$ von $k$. Dann sei

$$k(u_1, \dots, u_n)$$

der Durchschnitt aller Unterkörper von $K$, die $k$ und jedes $u_i$ enthalten. Wie im Fall von einfachen Erweiterungen ist $k(u_1, \dots, u_n)$ der kleinste Unterkörper von $K$, der $k$ und alle $u_i$ enthält. $k(u_1, \dots, u_n)$ heisst *endlich erzeugte Körpererweiterung von $k$*, erzeugt durch $u_1, \dots, u_n$.

[11] Körpererweiterung

**Beispiele.** 1) $\mathbb{Q}(\sqrt{3}, i)$ ist der kleinste Unterkörper von $\mathbb{C}$, der sowohl alle rationalen Zahlen also auch $\sqrt{3}$ und $i$ enthält.

2) Eine endlich erzeugte KE kann eine einfache KE sein: So liegen etwa $i$ und $-i$ in $\mathbb{Q}(i)$, es gilt damit $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$.

3) Jede endlich-dimensionale KE ist endlich erzeugt: Ist $\{u_1, \ldots, u_n\}$ eine Basis von $K$ über $k$, so liegen alle Linearkomb. der $u_i$ (mit Koeff. in $k$) in $k(u_1, \ldots, u_n)$. Also gilt $K = k(u_1, \ldots, u_n)$.

Die wichtigste Beobachtung im Zusammenhang mit endlich erzeugten Erweiterungen ist, dass man sie durch sukzessive einfache Erweiterungen erhalten kann. Sei $K$ eine KE von $k$, seien $u$, $v \in K$. Dann ist $k(u, v)$ ein UKörper von $K$, der $k$ und $u$ enthält, also auch $k(u)$. Wegen $v \in k(u, v)$ enthält also $k(u, v)$ den Körper $k(u)(v)$, den kleinsten UKörper, der $k(u)$ und $v$ enthält.

Andrerseits ist $k(u)(v)$ ein Körper, der $u$ und $v$ enthält, somit auch $k(u, v)$, wir haben damit $k(u)(v) = k(u, v)$, die endlich erzeugte KE $k(u, v)$ erhält man also mittels einer Kette von einfachen Erweiterungen

$$k \subseteq k(u) \subseteq k(u)(v) = k(u, v).$$

**Beispiel.** Wir haben

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})(i) = \mathbb{Q}(\sqrt{3}, i).$$

In Beispiel 9.8 haben wir gesehen, dass $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ ist. Ausserdem ist $i$ eine Nullstelle von $x^2 + 1$, dessen Koeffizienten in $\mathbb{Q}(\sqrt{3})$ sind. Die Zahl $i$ ist also algebraisch über $\mathbb{Q}(\sqrt{3})$. Nach Satz 9.7 ist daher $[\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})]$ endlich. Satz 8.1 liefert dann, dass

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

endlich ist. Die endlich erzeugte Erweiterung $\mathbb{Q}(\sqrt{3}, i)$ ist damit endlich-dimensional und - Satz 10.1 - algebraisch über $\mathbb{Q}$.

Die gleiche Argumentation kann man im allgemeinen Fall verwenden:

**Satz 10.2.** *Ist $K = k(u_1, \ldots, u_n)$ eine endlich erzeugte KE von $k$ und ist jedes $u_i$ algebraisch über $k$, so ist $K$ eine endlich-dimensionale algebraische KE von $k$.*

*Beweis.* Man kann $K$ mit einer Kette von KE erreichen,

$$k \subseteq k(u_1) \subseteq k(u_1, u_2) \subseteq k(u_1, u_2, u_3) \subseteq \cdots \subseteq k(u_1, \ldots, u_n) = K.$$

Dabei gilt $k(u_1, u_2) = k(u_1)(u_2)$, $k(u_1, u_2, u_3) = k(u_1, u_2)(u_3)$, etc., allgemeiner gesagt ist jede KE $k(u_1, \ldots, u_i)$ eine einfache KE $k(u_1, \ldots, u_{i-1})(u_i)$. Jedes $u_i$ ist algebraisch über $k$ und somit auch über $k(u_1, \ldots, u_{i-1})$. Nach Satz 9.7 ist jede einfache Erweiterung mit einem algebraischen Element endlich-dimensional, also ist

$$[k(u_1, \ldots, u_i) : k(u_1, \ldots, u_{i-1})]$$

endlich für $i = 2, \dots, n$. Wiederholtes Anwenden von Satz 8.1 liefert, dass $[K : k]$ gleich dem Produkt

$$[K : k(u_1, \dots, u_{n-1})][k(u_1, \dots, u_{n-1}) : k(u_1, \dots, u_{n-2})] \cdots [k(u_1) : k]$$

ist, also endlich, somit ist $K$ algebraisch über $k$ nach Satz 10.1. □

**Beispiel 10.3.** Die Zahlen $\sqrt{3}$ und $\sqrt{5}$ sind algebraisch über $\mathbb{Q}$, also ist $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ eine endlich-dimensionale KE von $\mathbb{Q}$ nach Satz 10.2. Wir berechnen hier die Dimension der KE $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, wir benutzen dazu die Kette von einfachen KE

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

Wir wissen bereits, dass $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ ist. Um $[\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})]$ zu bestimmen, suchen wir das Minimalpolynom von $\sqrt{5}$ über $\mathbb{Q}(\sqrt{3})$. Das naheliegende ist $x^2 - 5$, irreduzibel in $\mathbb{Q}[x]$. Wir müssen sehen, dass dies auch irreduzibel ist über $\mathbb{Q}(\sqrt{3})$, um schliessen zu können, dass es das Minimalpolynom ist. Falls $\pm\sqrt{5}$ in $\mathbb{Q}(\sqrt{3})$ liegen, dann ist $\pm\sqrt{5} = a + b\sqrt{3}$ für $a, b \in \mathbb{Q}$. Quadriert man auf beiden Seiten, so erhält man $5 = a^2 + 2ab\sqrt{3} + 3b^2$, also $\sqrt{3} = \frac{5-a^2-3b^2}{2ab}$, was der Tatsache, dass $\sqrt{3}$ irrational ist, widerspricht. Also liegen $\pm\sqrt{5}$ nicht in $\mathbb{Q}(\sqrt{3})$ und $x^2 - 5$ ist irreduzibel über $\mathbb{Q}(\sqrt{3})$ (Korollar 4.18). $x^2 - 5$ ist also das Minimalpolynom von $\sqrt{5}$ über $\mathbb{Q}(\sqrt{3})$ und es gilt $[\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$ nach Satz 9.7. Damit hat man (mit Satz 8.1)

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

[Vorlesung 15, 25. November 2014]

**Bemerkung 10.4.** [Transzendente vs algebraische Elemente] Bekannte transzendente Zahlen über $k := \mathbb{Q}$ sind $e$ und $\pi$.
Ein Beweis dafür, dass $e$ transzendent ist, wurde von Ch. Hermite 1873 gefunden (dazu und zum Beweis von Hilbert, siehe wikipedia, Eintrag [W1]). Hilbert hat später einen vereinfachten Beweis gefunden. Die Idee dazu: man nimmt an, dass $e$ algebraisch ist und schreibt

$$c_0 + c_1 e + \cdots + c_n e^n = 0$$

mit ganzzahligen Koeffizienten $c_i$ (eigentlich $c_i \in \mathbb{Q}$, die kann man jedoch mit dem kgV der Nenner aller $c_i$ multiplizieren und erreichen, dass die Koeffizienten in $\mathbb{Z}$ liegen) und mit $c_0 \neq 0 \neq c_n$. Für ein $m > 0$ sei $f_m(x)$ das Polynom

$$f_m(x) := x^m((x-1)\cdots(x-n))^{m+1}$$

Man multipliziert beide Seiten der Gleichung oben mit $\int_0^\infty f_m e^{-x} dx$ und erhält damit

$$c_0(\int_0^\infty f_m e^{-x} dx) + c_1 e(\int_0^\infty f_m e^{-x} dx) + \cdots + c_n e^n(\int_0^\infty f_m e^{-x} dx) = 0$$

Dies teilt man auf als $P+Q=0$ für $P$ und $Q$ wie folgt definiert (die Integrationsgrenzen variieren):

$$\begin{aligned} P &= c_0(\int_0^\infty f_m e^{-x}dx) + c_1 e(\int_1^\infty f_m e^{-x}dx) + \cdots + c_n e^n(\int_n^\infty f_m e^{-x}dx) \\ Q &= c_1 e(\int_0^1 f_m e^{-x}dx) + c_2 e^2(\int_0^2 f_m e^{-x}dx) + \cdots + c_n e^n(\int_0^n f_m e^{-x}dx) \end{aligned}$$

Dann zeigt man zwei Eigenschaften: (1) für ein geeignetes $m$ gilt $\frac{P}{m!}$ ist ganzzahlig und verschieden von Null. (2) für $m$ genügend gross gilt $|\frac{Q}{m!}| < 1$.

Nun kann man $m$ so wählen, dass sowohl (1) als auch (2) gelten und hat dann einen Widerspruch, also muss $e$ transzendent sein.

Es gibt jedoch weit mehr transzendente Zahlen, fast alle komplexen Zahlen sind über $\mathbb{Q}$ transzendent. Und zwar ist die Menge der algebraischen Zahlen über $\mathbb{Q}$ abzählbar unendlich, $\mathbb{R}$ und $\mathbb{C}$ sind jedoch überabzählbar unendlich. Das kann man sich über $\mathbb{Z}$ überlegen:
Warum bilden die algebraischen Zahlen eine abzählbar unendlich Menge? Ganzzahlige Polynome bilden eine abzählbare Menge, jedes solche Polynom hat nur endlich viele Nullstellen und diese Nullstellen sind die algebraischen Elemente über $\mathbb{Z}$.

Transzendente Zahlen (über $k$) in $\mathbb{R}$ sind natürlich irrational. Das gilt auch für transzendente Zahlen über $\mathbb{Z}$, ist nämlich $u \in \mathbb{R}$ rational, so ist $u = \frac{p}{q}$ mit $p$, $q$ ganzzahlig. Dann ist $u$ Nullstelle von $qx - p$, also ist $u$ algebraisch.
Es sind jedoch nicht alle irrationalen Zahlen transzendent (über $k$), so ist etwa $\sqrt{2}$ Nullstelle von $x^2 - 2$.

## 11. Zerfällungskörper

Es sei $k$ ein Körper, $f(x) \in k[x]$ ein Polynom. Wir haben bisher Körpererweiterungen zu $k$ gesucht, in denen eine Nullstelle von $f(x)$ liegt. Nun suchen wir nach KE'en, die alle Nullstellen von $f(x)$ enthalten.

Was genau sind "alle" Nullstellen? Hat $f(x)$ Grad $n$, so wissen wir, dass es in jedem Körper höchstens $n$ Nullstellen hat. Finden wir einen Erweiterungskörper $K$ von $k$, in dem $n$ verschiedene Nullstellen (mit Vielfachheiten gezählt) von $f(x)$ liegen, so können wir sagen, $K$ enthalte alle Nullstellen von $f(x)$. Es kann auch andere Erweiterungskörper von $k$ geben, die ebenso $n$ Nullstellen enthalten. Enthält jedoch $K$ weniger als $n$ Nullstellen von $f(x)$, so kann es sein, dass es eine Erweiterung gibt, die weitere Nullstellen enthält. Falls keine solche Erweiterung existiert, so ist es sinnvoll, zu sagen, $K$ enthalte alle Nullstellen von $f(x)$. Das kann man formal ausdrücken.

Sei $K$ eine KE von $k$ und $f(x)$ ein Polynom von positivem Grad $n$ in $k[x]$. Faktorisiert $f(x)$ folgendermassen in $K[x]$

$$f(x) = c(x-u_1)(x-u_2)\cdots(x-u_n),$$

(also $u_i \in K$ für $i = 1, \ldots, n$) so sagen wir, dass $f(x)$ *über $K$ zerfällt*. In diesem Fall sind die Elemente $u_1, \ldots, u_n \in K$ (die nicht alle verschieden sein müssen) die einzigen Nullstellen von $f(x)$ in $K$ oder in jedem (beliebigen) EK[12] von $K$: Ist nämlich $v$ Element eines beliebigen EKs von $K$ und gilt $f(v) = 0_k$, so ist $c(v-u_1)\cdots(v-u_n) = 0_k$. Da $f(x)$ positiven Grad hat, ist $c \neq 0_k$. Also muss für ein $i$ gelten $v - u_i = 0$, d.h. $v = u_i$.

Zerfällt also ein Polynom $f(x)$ über $K$, so liegen alle Nullstellen von $f(x)$ bereits in $K$. Im nächsten Schritt wird es darum gehen, die kleinste KE zu finden, die alle Nullstellen von $f(x)$ besitzt.

**Definition.** Ist $k$ ein Körper und $f(x)$ ein Polynom in $k[x]$, vom Grad $n > 0$. Dann heisst eine Körpererweiterung $K \supseteq k$ ein *Zerfällungskörper* (ein *Wurzelkörper*) von $f(x)$ über $k$, falls gilt:

$(i)$ $f(x)$ zerfällt über $K$,$f(x) = c(x-u_1)(x-u_2)\cdots(x-u_n)$ mit $u_i \in K$,
$(ii)$ $K = k(u_1, \ldots, u_n)$.

**Beispiel 11.1.** 1) Betrachten wir $x^2+1$ als Polynom in $\mathbb{R}[x]$, so ist $\mathbb{C}$ zu diesem Polynom ein Zerfällungskörper, $x^2+1 = (x-i)(x+i)$. Es ist $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i,-i)$. Analog ist $\mathbb{Q}(\sqrt{2})$ ein Zerfällungskörper von $x^2-2$ in $\mathbb{Q}[x]$, da $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$ ist und $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2},-\sqrt{2})$.

2) $\mathbb{Q}[x] \ni f(x) = x^4 - x^2 - 2 = (x^2-2)(x^2+1)$, die Nullstellen (in $\mathbb{C}$) von $f(x)$ sind $\pm\sqrt{2}$ und $\pm i$. Also ist $\mathbb{Q}(\sqrt{2}, i)$ ein Zerfällungskörper von $f(x)$ über $\mathbb{Q}$.

3) Jedes lineare Polynom $xc + d \in k[x]$ zerfällt über $k$: Es ist $cx + d = c(x - (-c^{-1}d))$ mit $-c^{-1}d \in k$. Der Körper $k$ ist der kleinste Körper, der $k$ und $c^{-1}d$ enthält, also gilt $k = k(c^{-1}d)$, $k$ selbst ist also Zerfällungskörper von $cx+d$ über $k$.

4) Der Zerfällungskörper hängt sowohl vom Polynom als auch vom Körper ab. So ist etwa $\mathbb{C}$ Zerfällungskörper von $x^2+1$ über $\mathbb{R}$, aber nicht über $\mathbb{Q}$, da $\mathbb{C}$ nicht gleich $\mathbb{Q}(i,-i) = \mathbb{Q}(i)$ ist.

Zwei wichtige Fragen über Zerfällungskörper stellen sich hier. Erstens: besitzt jedes Polynom $f(x) \in k[x]$ einen Zerfällungskörper über $k$? Zweitens: Falls es mehr als einen ZK[13] für $f(x)$ über $k$ gibt, was ist der Zusammenhang unter diesen ZK'en?

Die erste Frage kann man kurz so beantworten: Für $f(x) \in k[x]$ kann man eine Erweiterung $k(u)$ finden, die eine Nullstelle $u$ von $f(x)$ besitzt. Dann ist $f(x) = (x-u)g(x)$. Mit $g(x)$ fährt man fort, man findet eine Erweiterung $k(u)(v)$

[12]Erweiterungskörper
[13]Zerfällungskörper

von $k(u)$, die die Nullstelle $v$ von $g(x)$ enthält. So geht es weiter, bis man einen ZK von $f(x)$ gefunden hat. Etwas stärker:

**Satz 11.2.** *Sei $k$ ein Körper, $f(x)$ ein Polynom vom Grad $n \geq 1$ in $k[x]$. Dann existiert ein Zerfällungskörper $K$ von $f(x)$über $k$ mit $[K : k] \leq n!$ .*

*Beweis.* Induktion über den Grad $n$ von $f(x)$. Hat $f(x)$ Grad 1, so ist $k$ selbst der Zerfällungskörper (siehe Beispiel 11.1 (3)), es ist $[k : k] = 1 \leq 1!$ wie behauptet. Sei die Aussage gezeigt für alle Polynome vom Grad $n-1$, $f(x)$ habe Grad $n$. Da $k[x]$ faktoriell ist, hat $f(x)$ einen irreduziblen Faktor in $k[x]$. Multiplizieren wir diesen mit dem Inversen seines führenden Koeffizienten, so haben wir einen normierten irreduziblen Faktor $p(x)$ von $f(x)$. Nach Satz 9.4 existiert ein Erweiterungskörper, der eine Nullstelle $u$ von $p(x)$ (und also von $f(x)$) enthält. Ausserdem ist $p(x)$ das Minimalpolynom von $u$. Nach Satz 9.7 ist $[k(u) : k] = \deg p(x) \leq \deg f(x) = n$. Wir faktorisieren $f(x) = (x-u)g(x)$ mit $g(x) \in k(u)[x]$. Da $g(x)$ Grad $n-1$ hat, existiert ein Zerfällungskörper $K$ von $g(x)$ über $k(u)$ mit $[K : k(u)] \leq (n-1)!$ . In $K[x]$ ist

$$g(x) = c(x-u_1)(x-u_2)\cdots(x-u_{n-1})$$

und somit $f(x) = c(x-u)(x-u_1)\cdots(x-u_{n-1})$. Da

$$K = k(u)(u_1,\ldots,u_{n-1}) = k(u,u_1,\ldots,u_{n-1})$$

gilt, ist $K$ Zerfällungskörper von $f(x)$ über $k$, zudem gilt

$$[K : k] = [K : k(u)] \cdot [k(u) : k] \leq ((n-1)!n) = n!$$

und die Behauptung ist gezeigt. □

Der Zusammenhang zwischen verschiedenen Zerfällungskörpern desselben Polynoms ist einfach zu formulieren:
Je zwei Zerfällungskörper eines Polynoms in $k[x]$ sind isomorph.

Man kann sogar ein stärkeres Resultat zeigen:

**Satz 11.3.** *Sei $\sigma : F \to E$ ein Körperisomorphismus, $f(x)$ ein Polynom vom Grad $n \geq 1$ in $F[x]$, $\sigma f(x)$ das entsprechende Polynom in $E[x]$. Ist $K$ ein ZK von $f(x)$ über $F$ und $L$ ein ZK von $\sigma f(x)$ über $E$, so kann man $\sigma$ zu einem Isomorphismus $K \cong L$ erweitern.*

Im Fall $F = E$, $\sigma$ die Identität $F \to F$ sagt der Satz, dass je zwei Zerfällungskörper von $f(x) \in F[x]$ isomorph sind.

*Der Beweis von Satz 11.3 wurde in der Vorlesung ausgelassen.*

*Beweis.* Man zeigt dies mittels Induktion über den Grad von $f(x)$. Ist $\deg f(x) = 1$, so gilt nach Definition des ZK $f(x) = c(x-u)$ in $K[x]$ und $K = F(u)$. Nun liegt $f(x) = cx - cu$ in $F[x]$, also sind $c$ und $cu$ in $F$, somit auch $u = c^{-1}cu$, es ist $K = F(u) = F$. Dass man $\sigma$ zu einem Isomorphismus $F[x] \cong E[x]$ erweitern kann, haben wir auch schon früher gesehen (Überlegungen vor Korollar 9.9). Das

zeigt, dass $\sigma f(x)$ auch Grad 1 hat. Ein ähnliches Argument liefert dann $E = L$. Hier ist bereits $\sigma$ ein Isomorphismus mit den gewünschten Eigenschaften.

Man nehme nun an, die Aussage des Satzes stimme für Polynome vom (positiven) Grad $\leq n-1$ und dass $f(x)$ Grad $n$ habe. Wie im Beweis von Satz 11.2 hat $f(x)$ einen normierten irreduziblen ($k[x]$ ist faktoriell) Faktor $p(x) \in F[x]$. Wir wissen bereits, dass wir $\sigma$ zu einem Isomorphismus $F[x] \cong E[x]$ erweitern können. Dann ist $\sigma p(x)$ ein normierter irreduzibler Faktor von $\sigma f(x)$ in $E[x]$. Jede Nullstelle von $p(x)$ ist auch Nullstelle von $f(x)$, $K$ enthält alle Nullstellen von $p(x)$ und damit enthält $L$ alle Nullstellen von $\sigma p(x)$. Sei $u \in K$ eine Nullstelle von $p(x)$, $v \in L$ eine Nullstelle von $\sigma p(x)$. Wir können $\sigma$ zu einem Isomorphismus $F(u) \to E(v)$ erweitern, der $u$ auf $v$ abbildet (Korollar 9.9);

$$\begin{array}{ccc} K & & L \\ \cup| & & \cup| \\ F(u) & \xrightarrow{\cong} & E(v) \\ \cup| & & \cup| \\ F & \xrightarrow{\sigma} & E \end{array}$$

Nun ist $u$ eine Nullstelle von $f(x)$ genau dann, wenn $x-u$ ein Faktor von $f(x)$ in $F[x]$ ist. Damit haben wir $f(x) = (x-u)g(x) \in F(u)[x]$, also in $E(v)[x]$

$$\sigma f(x) = \sigma(x-u)\sigma g(x) = (x-\sigma u)\sigma g(x) = (x-v)\sigma g(x)$$

$f(x)$ zerfällt über $K$, etwa $f(x) = c(x-u)(x-u_2)\dots(x-u_n)$. Da $f(x) = (x-u)g(x)$ ist, ist $g(x) = c(x-u_2)\cdots(x-u_n)$. Der kleinste Unterkörper, der alle Nullstellen von $g(x)$ enthält und den Körper $F(u)$ ist $F(u, u_2, \dots, u_n) = K$, der Körper $K$ ist also ein ZK von $g(x)$ über $F(u)$. Analog ist $L$ ein ZK von $\sigma g(x)$ über $E(v)$. Das Polynom $g(x)$ hat Grad $n-1$, die Induktionsannahme sagt, dass der Isomorphismus $F(u) \cong E(v)$ zu einem Isomorphismus $K \cong L$ erweitert werden kann. Dies vervollständigt den Induktionsschritt und den Beweis vom Satz. □

Ein Zerfällungskörper eines Polynoms über $k$ enthält ja alle Nullstellen dieses Polynoms. Er hat jedoch noch weitere Eigenschaften, dazu führen wir den folgenden Begriff ein.

**Definition.** Ein algebraischer EK $K$ von $k$ heisst *normal*, falls gilt: ist $f(x)$ ein beliebiges irreduzibles Polynom in $k[x]$, das eine Nullstelle in $K$ hat, so zerfällt $f(x)$ über $K$[14].

**Satz 11.4.** *Ein Körper $K$ ist ein Zerfällungskörper von einem Polynom $f(x)$ über $k$ genau dann, wenn $K$ eine endlich-dimensionale, normale Erweiterung von $k$ ist.*

[14]Das ist die Bedingung, nämlich, dass *für jedes* irreduzible Polynom $f(x)$, das eine Nullstelle in $K$ besitzt, auch gleich alle Nullstellen in $K$ liegen!

*Beweis.* $\Longrightarrow$: Ist $K$ ein ZK über $k$ des Polynoms $f(x) \in k[x]$, dann ist $K = k(u_1, \ldots, u_n)$, wobei die $u_i$ alle Nullstellen von $f(x)$ sind. Also ist $[K : k]$ endlich (Satz 10.2). Man muss noch zeigen, dass $K$ eine normale Erweiterung von $k$ ist.
Sei $p(x)$ ein irreduzibles Polynom in $k[x]$, *das eine Nullstelle $v$ in $K$ hat.* Als Polynom in $K[x]$ betrachtet, hat $p(x)$ einen ZK $L$ über $K$, $k \subseteq K \subseteq L$. Um zu sehen, dass $p(x)$ schon über $K$ zerfällt, müssen wir zeigen, dass jede Nullstelle in $L$ von $p(x)$ bereits in $K$ liegt.

Sei $w \in L$ eine Nullstelle von $p(x)$, die verschieden ist von $v$. Nach Korollar 9.9 (mit $k = E = F$, $\sigma$ die Identitätsabbildung) existiert ein Isomorphismus $k(v) \cong k(w)$, der $v$ auf $w$ schickt und jedes Element von $k$ auf sich selbst. Wir betrachten den UKörper $K(w)$ von $L$, dabei haben wir folgende Situation:

$$\begin{array}{ccc} K & & K(w) \\ \cup\!| & & \cup\!| \\ k(v) & \xrightarrow{\cong} & k(w) \\ \cup\!| & & \cup\!| \\ k & = & k \end{array}$$

Wegen

$$K(w) = \overbrace{k(u_1, \ldots, u_n)}^{K}(w) = k(u_1, \ldots, u_n, w) = k(w)(u_1, \ldots, u_n)$$

ist $K(w)$ ein ZK von $f(x)$ über $k(w)$. Ausserdem ist $K$ ein ZK von $f(x)$ über $k(v)$, da $v \in K$ liegt und $K$ ein ZK von $f(x)$ über $k$ ist. Nach Satz 11.3 lässt sich dann der Isomorphismus $k(v) \cong k(w)$ zu einem Isomorphismus $K \cong K(w)$ erweitern, der $v$ auf $w$ schickt und jedes Element von $k$ fixiert. Es folgt $[K : k] = [K(w) : k]$ (Satz 8.2). In der Kette

$$k \subseteq K \subseteq K(w)$$

von Erweiterungen ist $[K(w) : K]$ endlich nach Satz 9.7 und $[K : k]$ endlich nach den Bemerkungen im ersten Abschnitt des Beweises. Also liefert Satz 8.1

$$[K : k] = [K(w) : k] = [K(w) : K][K : k]$$

Kürzt man mit $[K : k]$ auf beiden Seiten, so erhält man $1 = [K(w) : K]$, also sind die beiden Körper nicht nur isomorph, es ist wirklich $K = K(w)$, somit ist $w \in K$. Somit liegt jede Nullstelle von $p(x)$ in $L$ bereits in $K$, $p(x)$ zerfällt über $K$, d.h. dass $K$ normal ist über $k$.
$\Longleftarrow$: Sei umgekehrt $K$ eine endlich-dimensionale, normale Erweiterung von $k$ mit Basis $\{u_1, \ldots, u_n\}$. Dann ist $K = k(u_1, \ldots, u_n)$. Wir suchen nun ein Polynom für das $K$ der Zerfällungskörper ist.
Jedes der $u_i$ ist algebraisch über $k$ nach Satz 10.1, mit Minimalpolynom $p_i(x)$. Da

jedes der $p_i(x)$ über $K$ zerfällt (Normalität), zerfällt auch $f(x) = p_1(x)\cdots p_n(x)$ über $K$. Also ist $K$ der ZK von $f(x)$. □

**Beispiel.** Der Körper $\mathbb{Q}(\sqrt[3]{2})$ enthält die reelle Nullstelle $\sqrt[3]{2}$ des irreduziblen Polynoms $x^3-2 \in \mathbb{Q}[x]$, jedoch nicht die komplexe Nullstelle $\sqrt[3]{2}\omega$ (siehe Beispiel 9.10). Damit ist $\mathbb{Q}(\sqrt[3]{2})$ keine normale Erweiterung von $\mathbb{Q}$, es gibt also nach Satz 11.4 kein Polynom in $\mathbb{Q}[x]$, für das $\mathbb{Q}(\sqrt[3]{2})$ der ZK ist.

[Vorlesung 16, 28. November 2014]

Nun stellt sich die Frage, ob ein Körper $k$ einen EK besitzt über dem jedes Polynom in $k[x]$ zerfällt (d.h. einen EK, der alle Nullstellen aller Polynome in $k[x]$ enthält). Die Antwort ist ja, sie führt zum Begriff des *algebraischen Abschlusses*.

**Definition.** Ein Körper, über dem jedes Polynom von positivem Grad zerfällt heisst *algebraisch abgeschlossen*. Ist $K$ eine algebraische Erweiterung von $k$ und $K$ algebraisch abgeschlossen, so heisst $K$ der *algebraische Abschluss von $k$*.

Der folgende Satz liefert die Existenz von algebraischen Abschlüssen (ohne Beweis hier):

**Satz 11.5.** *Jeder Körper besitzt einen algebraischen Abschluss und dieser ist bis auf Isomorphie eindeutig bestimmt.*

Damit macht es Sinn, von "dem" algebraischen Abschluss eines Körpers zu sprechen.

**Bemerkung 11.6.** 1) Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen über $\mathbb{R}$:
Dank dem Fundamentalsatz der Algebra weiss man, dass jedes Polynom $\in \mathbb{R}[x]$ von positiven Grad über $\mathbb{C}$ zerfällt.
Da $\mathbb{C} = \mathbb{R}(i)$ gilt, ist $\mathbb{C}$ algebraisch über $\mathbb{R}$.
2) $\mathbb{C}$ ist aber *nicht* algebraischer Abschluss von $\mathbb{Q}$, weil $\mathbb{C}$ über $\mathbb{Q}$ nicht algebraisch ist.

**Beispiel** (Algebraischer Abschluss von $\mathbb{Q}$)**.** Sei

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\} \subset \mathbb{C}$$

Behauptung: $\overline{\mathbb{Q}}$ ist der algebraische Abschluss von $\mathbb{Q}$.
Beweis: Zu zeigen sind
(i) $\overline{\mathbb{Q}}$ ist ein Körper,
(ii) $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ und $\overline{\mathbb{Q}}$ ist algebraisch über $\mathbb{Q}$,
(iii) $\overline{\mathbb{Q}}$ ist algebraisch abgeschlossen.

ad (i): Es ist klar, dass $\overline{\mathbb{Q}} \neq \emptyset$ ist. Seien $\alpha, \beta \in \overline{\mathbb{Q}}$ mit $\beta \neq 0$. Dann sind $\alpha$ und $\beta$ algebraisch über $\mathbb{Q}$. Nach Satz 10.2 ist dann $\mathbb{Q}(\alpha, \beta)$ eine endl.-dim. (algebraische) KE von $\mathbb{Q}$. Es sind $\alpha \pm \beta$, $\alpha\beta^{-1} \in \mathbb{Q}(\alpha, \beta)$, also sind $\alpha \pm \beta$ und $\alpha\beta^{-1}$ algebraisch über $\mathbb{Q}$ und liegen damit in $\overline{\mathbb{Q}}$.

ad (ii): Es ist klar, dass $\mathbb{Q} \subset \overline{\mathbb{Q}}$ gilt. Und $\overline{\mathbb{Q}}$ ist nach Definition algebraisch über $\mathbb{Q}$.
ad (iii): Es genügt, zu zeigen, dass jedes Polynom $f[x] \in \overline{\mathbb{Q}}[x] \setminus \overline{\mathbb{Q}}$ eine Nullstelle in $\overline{\mathbb{Q}}$ hat.

(Denn dann folgt die Behauptung mit Induktion über den Grad $\deg(f)$: Ist $\deg(f) = 1$, so zerfällt das Polynom.
Ist $\deg(f) = n + 1 > 1$, so existiert $\alpha \in \overline{\mathbb{Q}}$ mit $f(\alpha) = 0$. Mittels Polynomdivision erhält man $f(x) = (x - \alpha)f_0(x)$, wobei $\deg(f_0) < \deg(f)$ gilt.
Nach Induktionsvoraussetzung existieren $c, \alpha_i \in \overline{\mathbb{Q}}$ mit
$f_0(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$. Und damit ist $f = c(x - \alpha)(x - \alpha_1) \cdots (x - \alpha_n)$. )

Sei also $f(x)$ ein nicht-konstantes Polynom in $\overline{\mathbb{Q}}[x]$. Weil $\mathbb{C}$ algebraisch abgeschlossen ist (und da nach Definition $\overline{\mathbb{Q}} \subseteq \mathbb{C}$), existiert $z \in \mathbb{C}$ mit $f(z) = 0$. Wir zeigen: $z \in \overline{\mathbb{Q}}$.
Sei

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \overline{\mathbb{Q}}[x].$$

Nach Satz 10.2 ist $[\mathbb{Q}(a_1, \ldots, a_n) : \mathbb{Q}] < \infty$ (da die $a_i$ alle nach Def. algebraisch sind über $\mathbb{Q}$). Wegen $f(z) = 0$ ist $z$ algebraisch über $\mathbb{Q}(a_1, \ldots, a_n)$, damit folgt $[\mathbb{Q}(a_1, \ldots, a_n)(z) : \mathbb{Q}(a_1, \ldots, a_n)] < \infty$. Mit Satz 8.1 erhält man

$$[\mathbb{Q}(a_1, \ldots, a_n)(z) : \mathbb{Q}] < \infty$$

und das heisst (mit Satz 10.1), dass $z$ algebraisch ist über $\mathbb{Q}$, also $z \in \overline{\mathbb{Q}}$.

## 12. Separabilität

Wir wissen, dass jedes Polynom einen ZK hat, der all seine Nullstellen enthält. Diese können alle verschieden sein oder mehr als einmal auftreten (d.h. ist $f(x) = (x - u_1)(x - u_2) \cdots (x - u_n)$, so kann $u_i = u_j$ vorkommen für $i \neq j$). Bei der Separabilität geht es um den Fall, wo alle Nullstellen verschieden sind, aus dieser Eigenschaft kann man einige nützliche Tatsachen über endlich-dimensionale Erweiterungen folgern.

**Definition.** Sei $k$ ein Körper. Man sagt, dass das Polynom $f(x) \in k[x]$ vom Grad $n$ *separabel* ist, falls es $n$ verschiedene Nullstellen hat in einem Zerfällungskörper (und damit in jedem - sie sind ja alle isomorph).[15]
Ist $K$ ein EK von $k$, so heisst ein Element $u \in K$ *separabel* über $k$, falls $u$ algebraisch ist über $k$ und sein Minimalpolynom $p(x)$ separabel ist.
Der EK $K$ heisst *separable Erweiterung* (oder *separabel über* $k$,), falls jedes Element von $K$ separabel ist über $k$.

[15]D.h. dass $f(x)$ in keinem ZK wiederholte Nullstellen hat.

Eine separable Erweiterung ist notwendig auch algebraisch.

**Beispiel.** Das Polynom $x^2+1$ in $\mathbb{Q}[x]$ ist separabel, da es zwei verschiedene Nullstellen hat in $\mathbb{C}$.
Das Polynom $f(x) = x^4 - x^3 - x + 1 = (x-1)^2(x^2+x+1)$ in $\mathbb{Q}[x]$ ist nicht separabel, $f$ hat eine Nullstelle der Vielfachheit 2 und insgesamt drei verschiedene Nullstellen.

Es gibt verschiedene Möglichkeiten, Separabilität zu überprüfen. Dabei benutzt man die Ableitung eines Polynoms.

**Definition.** Sei $k$ ein Körper. Für $f(x) = \sum_{i=0}^n a_i x^i \in k[x]$ definiert man die formale Ableitung

$$f'(x) := \sum_{i=1}^n i a_i x^{i-1} \in k[x]$$

**Bemerkung.** Die formale Ableitung hat die bekannten Eigenschaften:

- Es gilt für alle $f, g \in k[x]$:
$$\begin{aligned}(f \pm g)'(x) &= f'(x) \pm g'(x)\\ (fg)'(x) &= f'(x)g(x) + f(x)g'(x)\end{aligned}$$
- Sei $K$ ein EK von $k$. $u \in K$ ist mehrfache NSt. von $f(x) \Leftrightarrow f(u) = f'(u) = 0$.
(Beweis: Sei $u \in K$ NSt von $f(x)$. Dann ist $f(x) = (x-u)g(x)$ mit $g(x) \in K[x]$, und somit $f'(x) = g + (x-u)g'(x)$.
$u$ ist mehrfache NSt von $f(x) \iff g(u) = 0$
$\iff f'(u) = g(u) + \underbrace{(u-u)g'(u)}_{=0} = 0$).
- Ist $\mathrm{char}(k) = 0$, so ist $f'(x) \equiv 0 \iff f \in k$.
(Beweis: Sei $f(x) = \sum_{i=0}^n a_i x^i$, also $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$.
Es ist $f'(x) \equiv 0 \iff \forall\, i \in \{1, \dots, n\}$: $ia_i = 0$. Da $k$ hier Charakteristik 0 hat, ist Letzteres gleichbedeutend mit $\forall\, i \in \{1, \dots, n\}$ ist $a_i = 0 \iff f = a_0 \in k$.)

Das folgende Kriterium (Teil (i) in Lemma 12.1) arbeitet in $k[x]$, man muss hier beim Überprüfen auf Separabilität keinerlei Wissen über den ZK haben. (Es gibt weitere Kriterien).

**Lemma 12.1.** *Sei $k$ ein Körper, $f(x) \in k[x]$.*
*(i) $f(x)$ ist separabel $\iff$ $f(x)$ und $f'(x)$ sind teilerfremd in $k[x]$*
*(ii) Ist $f(x)$ irreduzibel, so ist $f(x)$ separabel $\iff$ $f'(x) \neq 0$.*

*Beweis.* (i) $\underline{\Leftarrow}$: durch Widerspruch.
Sei $K$ ein ZK von $f(x)$ und man nehme an, dass $f(x)$ nicht separabel ist. Dann hat $f(x)$ eine Nullstelle $u$ in $K$, die mehrfach ist, i.e. $f(u) = f'(u) = 0$.

Sei $p(x) \in k[x]$ Minimalpolynom von einem solchen $u$. Nach Satz 9.5 gilt $p(x) \mid f(x)$ und $p(x) \mid f'(x)$ und $\deg p(x) > 0$. Dann sind $f(x)$ und $f'(x)$ nicht teilerfremd.

(i) $\underline{\Rightarrow}$: Durch Widerspruch.
Sei $g(x) \in k[x] \setminus k$ ein gemeinsamer Teiler von $f(x)$ und $f'(x)$. Mit $f(x)$ zerfällt auch $g(x)$ über $K$ (ZK von $f(x)$) in Linearfaktoren. Also existiert $u \in K$ mit $g(u) = 0 \Rightarrow f(u) = f'(u) = 0$, $u$ ist daher mehrfache NSt von $f(x)$.

(ii) : Sei $f(x)$ irreduzibel, insbesondere ist $f(x) \in k[x] \setminus k$.
$\underline{\Rightarrow}$: nach (i) sind $f(x)$ und $f'(x)$ teilerfremd, damit muss $f'(x) \neq 0$ sein.

(ii): $\underline{\Leftarrow}$: Wir zeigen: $f(x)$ und $f'(x)$ sind teilerfremd. Dann folgt die Aussage aus Teil (i).
Angenommen, $g(x) \in k[x]$ teilt $f(x)$ und $f'(x)$. Wegen $\deg f(x) > 0$ ist $\deg f'(x) < \deg f(x)$. Dann ist auch $\deg g(x) < \deg f(x)$, also muss $g(x) \in k$ sein (denn $f(x)$ ist irreduzibel). □

**Korollar 12.2.** *Sei $k$ ein Körper der Charakteristik 0. Dann ist jedes irreduzible Polynom in $k[x]$ separabel.*

*Beweis.* Sei $f(x)$ irreduzibel. Dann ist $f(x) \in k[x] \setminus k$, also $f'(x) \neq 0$, die Aussage folgt mit Lemma 12.1(ii) □

Der folgende Satz wird oft der Satz vom primitiven Element genannt, cf. http://de.wikipedia.org/wiki/Satz_vom_primitiven_Element.

**Satz 12.3.** *Sei $K$ eine endlich erzeugte Erweiterung von $k$, $K = k(u_1, \ldots, u_n)$ mit $u_i \in K$, wobei $u_2, \ldots, u_n$ separabel seien über $k$ und $u_1$ algebraisch über $k$. Dann ist $K = k(u)$ für ein $u \in K$.*
*Insbesondere: ist $K$ eine endlich erzeugte separable Erweiterung von $k$, so ist $K = k(u)$ für ein $u \in K$.*

*Beweis.* Wir nehmen zuerst an, dass $|k| = \infty$ ist. Der Beweis für endliche Körper folgt mit Satz 12.4.

Nach Voraussetzung ist $K = k(u_1, \ldots, u_n)$. Wir führen Induktion über $n$ durch. Falls $n = 1$ ist, ist $K = k(u_1)$, es ist nichts zu zeigen.

Sei $n = 2$. Wir zeigen: Ist $K = k(v, w)$ mit $w$ separabel über $k$ und $v$ algebraisch über $k$, so existiert ein $u \in K$ mit $K = k(u)$.

Sei $p(x) \in k[x]$ das Minimalpolynom von $v$, $q(x) \in k[x]$ das Minimalpolynom von $w$. Sei $L$ ein ZK von $p(x)q(x)$ über $K = k(v, w)$. Seien $w = w_1, w_2, \ldots, w_n \in L$ mit $q(x) = \prod_{j=1}^{n}(x - w_j)$. Weil $q(x)$ separabel ist ($w$ ist separabel), sind die $w_j$ paarweise verschieden.
Insbesondere gilt $w - w_j \neq 0$ für $j = 2, \ldots, n$.
Seien $v = v_1, v_2, \ldots, v_m \in L$ mit $p(x) = \prod_{i=1}^{m}(x - v_i)$. Weil $|k| = \infty$ ist, gibt es ein Element $c \in k$ mit

$$c \neq \frac{v_i - v}{w - w_j} \text{ für alle } 1 \leq i \leq m,\ 2 \leq j \leq n$$

Sei $u = v + cw$.
Beh.: $K = k(u)$.
$\supseteq$: Es ist $u = v + cw$ mit $v, w \in K$ und $c \in k$, also $u \in K$ und damit $k(u) \subseteq K = k(v, w)$.
$\subseteq$: Wir zeigen: $w \in k(u)$.
(dann ist auch $v = u - cw \in k(u)$ und damit $K = k(v, w) \subseteq k(u)$)
Wir definieren $h(x) := p(u - cx) \in k(u)[x]$.
• $w$ ist Nullstelle von $h(x)$: $h(w) = p(u - cw) = p(v) = 0$.
• für alle $2 \leq j \leq n$ ist $h(w_j) \neq 0$: Angenommen, $h(w_j) = 0$ für ein $j$. Dann wäre $0 = p(u - cw_j)$, also $u - cw_j = v_i$ für ein $1 \leq i \leq m$. $\stackrel{e=v+cw}{\Longrightarrow} v + cw = v_i + cw_j$ und damit $c = \frac{v_i - v}{w - w_j}$, ein Widerspruch zur Wahl von $c$.
Also ist $w$ die einzige gemeinsame Nullstelle von $q(x)$ und $h(x)$.

Sei $r(x)$ das Minimalpolynom von $w$ über $k(u)$. Nach Satz 9.5 teilt $r(x)$ das Polynom $q(x) \in k[x] \subseteq k(u)[x]$ und $r(x) \mid h(x)$.
Dann ist aber jede Nullstelle von $r(x)$ auch Nullstelle von $q(x)$ und von $h(x)$.

Daraus folgt, dass $r(x)$ nur eine Nullstelle in $L$ hat (nämlich $w$). Ausserdem ist $q(x)$ separabel und zerfällt über $L$ in Linearfaktoren. Daher ist $r(x)$ separabel und zerfällt über $L$ in Linearfaktoren. D.h. $r(x) = x - w \in k(u)[x]$, m.a.W. $w \in k(u)$.

Die Aussage sei bewiesen für $n - 1$, wir betrachten $n \geq 3$. Nach IV existiert $t \in K$ mit $k(u_1, \ldots, u_{n-1}) = k(t)$. Nach den Überlegungen im Fall $n = 2$ existiert $u \in K$ mit $k(t, u_n) = k(u)$ (denn $t$ ist algebraisch und $u_n$ separabel).

Also hat man $k(u_1, \ldots, u_n) = k(u_1, \ldots, u_{n-1})(u_n) = k(t)(u_n) = k(t, u_n) = k(u)$. □

**Bemerkung.** Die Umkehrung von Satz 12.3 gilt im Allgemeinen nicht, es gibt Beispiele von einfachen Erweiterungen $K = k(u)$, $u$ algebraisch über $k$, die nicht separabel sind.
So etwa für $k := \mathbb{Z}_2(t)$ der Quotientenkörper vom Ring $\mathbb{Z}_2[t]$ der Polynome in $t$ mit Koeffizienten in $\mathbb{Z}_2$. Das Polynom $x^2 - t \in k[x]$ ist irreduzibel (ist z.z.,Hinweis: hat $x^2 - t$ eine Nullstelle in $k$, so existieren Polynome $g(t)$, $h(t)$ in $\mathbb{Z}_2[t]$ mit $(g(t)/h(t))^2 = t$, das führt zu einem Widerspruch).

Ausserdem ist $x^2 - t \in k[x]$ nicht separabel (seine Ableitung ist $0_k$, man verwendet Lemma 12.1(ii)).

Analog mit $k := \mathbb{Z}_p(t)$, $p$ prim, und dem Polynom $x^p - t$ in $k[x]$.

**Satz 12.4.** *Sei $K$ ein endlicher Körper, $k \subseteq K$ ein Unterkörper. Dann ist $K$ eine einfache KE von $k$.*

*Beweis.* Die multiplikative Gruppe der Elemente $\neq 0$ von $K$ ist zyklisch. Ist $u$ ein Erzeugender dieser Gruppe, so enthält $k(u)$ das Element $0_k$ und alle Potenzen von $u$, also jedes Element von $K$. Damit ist $K = k(u)$. □

# Teil 4. Galoistheorie

[Vorlesung 17, 2. Dezember 2014]

In der klassischen Algebra ist eine der wichtigsten Frage diejenige, ob es Formeln für die Lösungen von polynomialen Gleichung von höherem Grad gibt, analog zur Lösungsformel für quadratische Gleichungen. Im 16. Jh. hat man Formeln für die Grade 3 und 4 gefunden, danach gab es fast 300 Jahre lang keinen Fortschritt. Ruffini und Abel haben schliesslich gezeigt[16], dass es keine allgemeine Lösungsformel für alle polynomialen Gleichungen vom Grad $n$ geben kann, falls $n \geq 5$ ist. Das sagt noch nichts über Spezialfälle aus, gewisse Typen von Gleichungen können Lösungen haben. Es sagt auch nichts drüber aus, wie diese Lösungen bei Spezialfällen aussehen könnten.

Erst Évariste Galois[17] hat dies dann vollständig geklärt. Dazu gehört ein Kriterium, das bestimmt, wann eine polynomiale Gleichung durch eine Formel gelöst werden kann. Die Ideen von Galois haben grundlegende Einflüsse in der Mathematik gehabt, weit über die anfängliche Fragestellungen, die die Motivation dazu gewesen waren.

Die Lösungen der Gleichung $f(x) = 0$ liegen in einer Erweiterung des Koeffizientenkörpers von $f(x)$. Die Entdeckung von Galois beinhaltete den engen Zusammenhang zwischen solchen Körpererweiterungen und Gruppen (Kapitel 13). Die genaue Beschreibung des Zusammenhangs liefert der Fundamentalsatz der Galoistheorie (Kapitel 14). Mit diesem Satz kann man das Kriterium von Galois über die Auflösbarkeit von Gleichungen zeigen (Kapitel 15).

## 13. Die Galois-Gruppe

Bei der Untersuchung von KE ist die sogenannte Galoisgruppe der KE sehr wichtig.

**Definition.** Sei $K$ eine KE eines Körpers $F$. Ein *$F$-Automorphismus von $K$* ist ein Isomorphismus $\sigma : K \to K$, der den Körper $F$ elementweise festhält[18]. Die Menge aller $F$-Automorphismen bezeichnet man mit $\mathrm{Gal}_F K$, sie heisst die *Galoisgruppe von $K$ über $F$*.

$\mathrm{Gal}_F K$ ist wirklich eine Gruppe:

**Satz 13.1.** *Ist $K \supseteq F$ eine KE, so ist $Gal_F K$ eine Gruppe unter der Verknüpfung von Funktionen.*

[16]Satz von Abel-Ruffini, Paolo Ruffini hat 1799 einen unvollständigen Beweis dazu gegeben, Niels Henrik Abel hat es dann 1823 bewiesen. Évariste Galois hat das Resultat auch bewiesen, sein Beweis wurde 1846 posthum veröffentlicht.

[17]1811-1832

[18]Zur Erinnerung: Ein Automorphismus von $K$ ist ein Körperisomorphismus $K \to K$

*Beweis.* Die Identitätsabbildung $\iota : K \to K$ liegt in $\mathrm{Gal}_F K$, also ist $\mathrm{Gal}_F K$ nicht leer[19]. Die Abbildung $\iota$ liefert auch gleich das neutrale Element.
Sind $\sigma$ und $\tau$ in $\mathrm{Gal}_F K$, so auch deren Verknüpfung $\tau \circ \sigma$. Damit ist $\mathrm{Gal}_F K$ abgeschlossen.
Die Verknüpfung von Funktionen ist assoziativ.
Jede bijektive Funktion hat ein Inverses. Ist also $\sigma : K \to K$ in $\mathrm{Gal}_F K$, so ist auch $\sigma^{-1}$ ein Isomorphismus von $K$ nach $K$. Man muss sich noch überlegen, dass $\sigma^{-1}(c) = c$ ist für jedes $c \in F$, also $\sigma^{-1} \in \mathrm{Gal}_F K$ (Übung).
Dann ist die Behauptung gezeigt. □

Dazu ein erstes Beispiel.

**Beispiel 13.2.** Die komplexe Konjugation $\sigma : \mathbb{C} \to \mathbb{C}$, $a + ib \mapsto a - ib$ ($a$, $b$ in $\mathbb{R}$) ist ein Automorphismus von $\mathbb{C}$. Und natürlich werden dabei die Elemente von $\mathbb{R}$ fest gelassen. Also ist $\sigma \in \mathrm{Gal}_{\mathbb{R}} \mathbb{C}$.
Die Nullstellen $i$ und $-i$ von $x^2 + 1 \in \mathbb{R}[x]$ werden unter $\sigma$ aufeinander abgebildet. Das ist ein Beispiel des folgenden Resultats.

**Satz 13.3.** *Es sei $K \supseteq F$ eine KE und $f(x) \in F[x]$, $u \in K$ eine Nullstelle von $f(x)$. Ist $\sigma \in Gal_F K$, so ist auch $\sigma(u)$ eine Nullstelle von $f(x)$.*

*Beweis.* Ist $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, so ist

$$c_0 + c_1 u + c_2 u^2 + \cdots + c_n u^n = 0_F$$

Da $\sigma$ insbesondere ein Homomorphimus ist und da $\sigma(c_i) = c_i$ ist für jedes $i$ (die $c_i$ liegen ja in $F$) ist

$$\begin{aligned} 0_F = \sigma(0_F) &= \sigma(c_0 + c_1 u + c_2 u^2 + \cdots + c_n u^n) \\ &= \sigma(c_0) + \sigma(c_1)\sigma(u) + \sigma(c_2)\sigma(u)^2 + \cdots + \sigma(c_n)\sigma(u)^n \\ &= c_0 + c_1\sigma(u) + c_2\sigma(u)^2 + \cdots + c_n\sigma(u)^n = f(\sigma(u)). \end{aligned}$$

Damit ist auch $\sigma(u)$ Nullstelle von $f(x)$. □

Sei $u \in K$ algebraisch über $F$, mit Minimalpolynom $p(x) \in F[x]$. Satz 13.3 sagt, dass jedes Bild von $u$ unter einem Element der Galoisgruppe auch Nullstelle von $p(x)$ sein muss.

Ist umgekehrt *jede* Nullstelle von $p(x)$ in $K$ ebenfalls das Bild von $u$ unter einem Element der Galoisgruppe? Das folgende Resultat zeigt einen Fall, wo es stimmt.

**Satz 13.4.** *Sei $K$ Zerfällungskörper eines Polynoms über $F$, seien $u$ und $v \in K$. Dann existiert ein $\sigma \in Gal_F K$ mit $\sigma(u) = v$ genau dann, wenn $u$ und $v$ das gleiche Minimalpolynom haben in $F[x]$.*

*Beweis.* $\Longleftarrow$: Haben $u$ und $v$ das gleiche Minimalpolynom, so existiert nach Korollar 9.9 ein Isomorphismus $\sigma : F(u) \cong F(v)$ mit $\sigma(u) = v$, der ausserdem jedes Element von $F$ auf sich selber schickt.

[19] In diesem Kapitel wird $\iota$ immer für die Identitätsabbildung eines Körpers verwendet

Da $K$ ZK ist eines Polynoms über $F$ ist, ist $K$ auch ZK des gleichen Polynoms über $F(u)$ und über $F(v)$. Also kann man $\sigma$ zu einem $F$-Automorphismus von $K$ erweitern (den wir auch $\sigma$ nennen), nach Satz 11.3. Anders gesagt: $\sigma \in \mathrm{Gal}_F K$ und $\sigma(u) = v$.

Die Richtung $\Longrightarrow$ ist eine direkte Folge von Satz 13.3 (und der Eigenschaften des Minimalpolynoms). □

**Beispiel 13.5.** Nach Beispiel 13.2 wissen wir, dass $\mathrm{Gal}_{\mathbb{R}} \mathbb{C}$ mind. zwei Elemente hat: die Identität und die komplexe Konjugation $\sigma$. Wir zeigen hier, dass die Gruppe $\mathrm{Gal}_{\mathbb{R}} \mathbb{C}$ keine weiteren Elemente besitzt. Sei $\tau$ ein beliebiger Automorphismus in $\mathrm{Gal}_{\mathbb{R}} \mathbb{C}$. Da $i$ eine Nullstelle von $x^2 + 1$ ist, ist auch $\tau(i)$ eine Nullstelle davon (Satz 13.3), es muss daher $\tau(i) = \pm i$ sein. Falls $\tau(i) = i$ ist, ist $\tau = \iota$ die Identität ($\tau$ fixiert ja nach Voraussetzung $\mathbb{R}$ und fixiert auch $i$).

Ist $\tau(i) = -i$, so ist $\tau$ die komplexe Konjugation:

$$\tau(a + ib) = \tau(a) + \tau(i)\tau(b) = a + (-i)b = a - ib$$

Damit ist $\mathrm{Gal}_{\mathbb{R}} \mathbb{C} = \{\iota, \sigma\}$ eine Gruppe der Ordnung 2, also isomorph zu $\mathbb{Z}_2$.

Die $\mathbb{R}$-Automorphismen von $\mathbb{C}$ sind nach Beispiel 13.5 vollständig durch ihre Wirkung auf $i$ bestimmt. Analog hat man:

**Satz 13.6.** *Sei $K = F(u_1, \ldots, u_n)$ eine algebraische Erweiterung von $F$. Sind $\sigma$, $\tau$ in $Gal_F K$ und gilt $\sigma(u_i) = \tau(u_i)$ für $i = 1, \ldots, n$, so ist $\sigma = \tau$.*

*Beweis.* Das ist Theorem 11.4 in [Hu]. Die Strategie ist, dass man zeigt, dass $\beta := \tau^{-1} \circ \sigma$ die Identitätsabbildung $\iota$ ist. Natürlich ist es die Identität auf $F$. Dann überlegt man, dass es die Identität in $F(u_1)$ ist, dann in $F(u_1)(u_2) = F(u_1, u_2)$, etc., bis man zu $K = F(u_1, \ldots, u_n)$ gelangt. Und damit erhält man $\tau = \tau \circ \iota = \underbrace{\tau \circ \tau^{-1}}_{\iota} \circ \sigma = \sigma$. □

**Beispiel 13.7.** Wir betrachten $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \supseteq \mathbb{Q}$. Nach Satz 13.3 schickt jedes Element der Galois-Gruppe $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5}))$ das Element $\sqrt{3}$ entweder auf $\sqrt{3}$ oder auf $-\sqrt{3}$, die beiden Nullstellen von $x^2 - 3$. Analog muss $\sqrt{5}$ auf $\pm\sqrt{5}$ geschickt werden. Nach Satz 13.6 ist ein Automorphismus aus $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ vollständig bestimmt durch seine Wirkung auf $\sqrt{3}$ und auf $\sqrt{5}$. Damit kann es höchstens vier Elemente in $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ geben, entsprechend den möglichen Wirkungen auf $\sqrt{3}$ und auf $\sqrt{5}$:

$$\iota : \left\{ \begin{array}{l} \sqrt{3} \to \sqrt{3} \\ \sqrt{5} \to \sqrt{5} \end{array} \right\} \quad \tau : \left\{ \begin{array}{l} \sqrt{3} \to -\sqrt{3} \\ \sqrt{5} \to \sqrt{5} \end{array} \right\} \quad \alpha : \left\{ \begin{array}{l} \sqrt{3} \to \sqrt{3} \\ \sqrt{5} \to -\sqrt{5} \end{array} \right\} \quad \beta : \left\{ \begin{array}{l} \sqrt{3} \to -\sqrt{3} \\ \sqrt{5} \to -\sqrt{5} \end{array} \right\}$$

Wir zeigen nun, dass $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ tatsächlich 4 Elemente hat, indem wir drei Automorphismen $\tau$, $\alpha$, $\beta$, alle verschieden von der Identität, konstruieren, die die obigen Wirkungen haben.

Da $x^2 - 3$ das Minimalpolynom von $\sqrt{3}$ und von $-\sqrt{3}$ über $\mathbb{Q}$ ist, existiert (Korollar

9.9) ein Isomorphismus $\sigma : \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(-\sqrt{3})$, der $\sqrt{3}$ auf $-\sqrt{3}$ schickt und jedes Element von $\mathbb{Q}$ festhält. Beispiel 10.3 zeigt, dass $x^2 - 5$ das Minimalpolynom von $\sqrt{5}$ über $\mathbb{Q}(\sqrt{3})$ ist. Wiederum nach Korollar 9.9 können wir daher $\sigma$ zu einem $\mathbb{Q}$-Automorphismus $\tau$ von $\mathbb{Q}(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ erweitern, der $\sqrt{5}$ auf $\sqrt{5}$ schickt. Damit ist $\tau$ ein Element von $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ und es schickt $\sqrt{3}$ auf $\tau(\sqrt{3}) = \sigma(\sqrt{3}) = -\sqrt{3}$ und $\sqrt{5}$ auf sich selbst.
Ähnliche 2-Schritt Argumente liefern $\alpha$ und $\beta$ wie oben beschrieben. Jedes dieser drei Elemente von $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ hat Ordnung 2: es ist etwa

$$(\tau \circ \tau)(\sqrt{3}) = \tau(-\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3} = \iota(\sqrt{3})$$

und $\tau \circ \tau(\sqrt{5}) = \sqrt{5} = \iota(\sqrt{5})$. Mit Satz 13.6 gilt also $\tau \circ \tau = \iota$. Analog findet man auch die verschiedenen Verknüpfungen der vier Elemente, es ist z.B. $\tau \circ \alpha = \beta$. Man kann die Multiplikationstafel selbst bestimmen, es ergibt sich $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

In Beispiel 13.7 ist $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ der Zerfällungskörper von $f(x) = (x^2-3)(x^2-5)$ und jeder Automorphismus der entsprechenden Galoisgruppe permutiert die vier Nullstellen $\pm\sqrt{3}$, $\pm\sqrt{5}$ von $f(x)$. Das ist ein Beispiel des folgenden Korollars.

**Korollar 13.8.** *Ist $K$ der Zerfällungskörper eines separablen Polynoms $f(x)$ vom Grad $n$ in $F[x]$, so ist $Gal_F K$ isomorph zu einer Untergruppe von $S_n$.*

($S_n$ ist die symmetrische Gruppe auf $n$ Elementen, siehe Kapitel 1.1).

*Beweis.* Da $f(x)$ separabel ist, hat es $n$ verschiedene Nullstellen $u_1, \ldots, u_n$. Man bildet die symmetrische Gruppe $S_n$ auf der Menge dieser $n$ Nullstellen. Für Elemente $\sigma \in \mathrm{Gal}_F K$ sind die $\sigma(u_i)$ ebenfalls Nullstellen von $f(x)$ (Satz 13.3). Da $\sigma$ injektiv ist, sind die Bilder $\sigma(u_i)$ alle verschieden, d.h. sie sind die $u_i$ (in irgendeiner Reihenfolge), $\sigma$ permutiert die Nullstellen. Damit definiert man eine Abbildung $\theta : \mathrm{Gal}_F K \to S_n$, $\sigma \mapsto \sigma\,|_{\{u_1,\ldots,u_n\}}$. Dieses $\theta$ ist ein Gruppenhomomorphismus (auf beiden Seiten haben wir Verknüpfungen von Funktionen). (Als Zerfällungskörper ist $K = F(u_1, \ldots, u_n)$.)
$\theta$ ist injektiv, denn falls $\sigma\,|_{\{u_1,\ldots,u_n\}} = \tau\,|_{\{u_1,\ldots,u_n\}}$ ist, so ist $\sigma(u_i) = \tau(u_i)$ für jedes $i$, also $\sigma = \tau$ nach Satz 13.6. Damit ist $\mathrm{Gal}_F K$ isomorph zum Bild $\operatorname{im}\theta$, also zu einer Untergruppe von $S_n$ ([EA]). □

Ist $K$ der Zerfällungskörper von $f(x)$, so identifizieren wir $\mathrm{Gal}_F K$ mit der Untergruppe von $S_n$ zu der sie isomorph ist, indem wir jeden Automorphismus mit der Permutation der Nullstellen identifizieren, die er induziert.

[Vorlesung 18, 5. Dezember 2014]

**Beispiel 13.9.** Sei $K$ der Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$. Die Nullstellen von $x^3 - 2$ sind $\sqrt[3]{2}$, $\sqrt[3]{2}w$ und $\sqrt[3]{2}w^2$ mit $w := \frac{-1+\sqrt{3}i}{2}$. $\mathrm{Gal}_{\mathbb{Q}} K$ ist eine Untergruppe von $S_3$ (Korollar 13.8). Nach Satz 13.4 existiert mindestens ein Automorphismus $\sigma$, der

die erste Nullstelle auf die zweite schickt, er muss dann die dritte Nullstelle auf sich selbst oder auf die erste schicken (Satz 13.3). Also ist $\sigma$ entweder die Permutation (12) oder die Permutation (123). Wieviele Elemente hat also $\mathrm{Gal}_{\mathbb{Q}}K$?

**Bemerkung.** Ist $K$ der Zerfällungskörper eines Polynoms $f(x) \in F[x]$, so liefert nach Korollar 13.8 jedes Element von $\mathrm{Gal}_F K$ eine Permutation der Nullstellen von $f(x)$. Es ist aber nicht so, dass jede Permutation der Nullstellen von einem $F$-Automorphismus von $K$ kommt. So ist etwa $\mathbb{Q}(\sqrt{3},\sqrt{5})$ der Zerfällungskörper von $f(x) = (x^2-3)(x^2-5)$, wir wissen aber aus Beispiel 13.7, dass es keinen $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\sqrt{3},\sqrt{5})$ gibt, der die Permutation

$$\begin{array}{cccc} \sqrt{3} & -\sqrt{3} & \sqrt{5} & -\sqrt{5} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \sqrt{5} & -\sqrt{5} & \sqrt{3} & -\sqrt{3} \end{array}$$

der Nullstellen induziert.

**Bemerkung.** Sei $F \subseteq K$ eine KE. Ist $F \subseteq E \subseteq K$, so nennt man $E$ einen Zwischenkörper der Erweiterung. $K$ ist dann auch KE von $E$. Da $\mathrm{Gal}_E K$ die Automorphismen von $K$ sind, die $E$ elementweise festhalten, halten sie automatisch auch alle Elemente von $F \subseteq E$ fest. Daher gilt:

**Ist $E$ ein Zwischenkörper, so ist $\mathrm{Gal}_E K$ eine Untergruppe von $\mathrm{Gal}_F K$.**

**Beispiel 13.10.** $\mathbb{Q}(\sqrt{3})$ ist ein Zwischenkörper der KE $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$. Wir wissen (Beispiel 13.7), dass $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{\iota,\tau,\alpha,\beta\}$ ist. Die Automorphismen, die alle Elemente von $\mathbb{Q}(\sqrt{3})$ festhalten, sind gerade diejenigen, die $\sqrt{3}$ auf sich selbst schicken (Satz 13.4). Also ist

$$\mathrm{Gal}_{\mathbb{Q}(\sqrt{3})}\,\mathbb{Q}(\sqrt{3},\sqrt{5})$$

die Untergruppe $\{\iota,\alpha\}$ von $\{\iota,\tau,\alpha,\beta\}$

Wir können also jedem Zwischenkörper einer Erweiterung eine Untergruppe der Galoisgruppe zuordnen. Umgekehrt: ist $H$ eine Untergruppe der Galoisgruppe, so können wir zu $H$ einen Zwischenkörper zuordnen, dank:

**Satz 13.11.** *Sei $K$ ein EK von $F$. Ist $H$ eine Untergruppe von $Gal_F K$, so sei*

$$E_H := \{t \in K \mid \sigma(t) = t \text{ für jedes } \sigma \in H\}.$$

*Dann ist $E_H$ ein Zwischenkörper der Erweiterung.*

*Beweis.* Das ist Theorem 11.6 in [Hu], man zeigt (1), dass $E_H$ ein Körper ist und (2), dass $F \subseteq E_H$ gilt. □

**Definition.** Der Zwischenkörper $E_H$ aus Satz 13.11 wird *Fixkörper* der Untergruppe $H$ von $\mathrm{Gal}_F K$ genannt.

Es gilt immer $E_{\{\iota\}} = K$.

**Beispiel 13.12.** Wir betrachten die Untergruppe $H = \{\iota, \alpha\}$ der Galoisgruppe $\{\iota, \tau, \alpha, \beta\}$ von $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ über $\mathbb{Q}$ (Beispiel 13.7). Da $\alpha(\sqrt{3}) = \sqrt{3}$ ist, ist der Unterkörper $\mathbb{Q}(\sqrt{3})$ im Fixkörper $E_H$ von $H$ enthalten. Um zu sehen, dass $E_H = \mathbb{Q}(\sqrt{3})$ gilt, muss man zeigen, dass die Elemente von $\mathbb{Q}(\sqrt{3})$ die *einzigen* sind, die unter $\iota$ und $\alpha$ festgehalten werden.

**Beispiel 13.13.** Wir wissen, dass $\mathrm{Gal}_{\mathbb{R}} \mathbb{C} = \{\iota, \sigma\}$ ist ($\sigma$ die komplexe Konjugation), siehe Beispiel 13.2. Der Fixkörper von $\{\iota\}$ ist $\mathbb{C}$. Die komplexe Konjugation $\sigma$ hält jede reelle Zahl fest und verändert jede nicht reelle Zahl. Also ist der Fixkörper von $H = \mathrm{Gal}_{\mathbb{R}} \mathbb{C}$ gerade $\mathbb{R}$.

Im allgemeinen muss jedoch der Fixkörper der ganzen Gruppe $\mathrm{Gal}_F K$ nicht gleich $F$ sein, dazu ein weiteres Beispiel:

**Beispiel 13.14.** Jeder Automorphismus aus der Galoisgruppe von $\mathbb{Q}(\sqrt[3]{2})$ über $\mathbb{Q}$ muss $\sqrt[3]{2}$ auf eine Nullstelle von $x^3 - 2$ abbilden (Satz 13.3). Nun ist $\sqrt[3]{2}$ die einzige reelle Nullstelle von $x^3 - 2$. Die andern beiden sind $\sqrt[3]{2}w$ und $\sqrt[3]{2}w^2$, für $w = \frac{-1+\sqrt{3}i}{2}$ (dritte Wurzel der Eins). Nach Satz 9.7 enthält $\mathbb{Q}(\sqrt[3]{2})$ nur reelle Zahlen, also muss $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$ das Element $\sqrt[3]{2}$ auf sich selbst abbilden. Daraus folgt $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \{\iota\}$ (Satz 13.6). Also ist der Fixkörper von $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$ der ganze Körper $\mathbb{Q}(\sqrt[3]{2})$.

## 14. Fundamentalsatz der Galoistheorie

In diesem Kapitel ist $K$ immer ein endlich-dimensionaler EK von $F$. Die Hauptidee der Galoistheorie ist es, Eigenschaften der Erweiterung mit Eigenschaften der Galoisgruppe $\mathrm{Gal}_F K$ in Verbindung zu setzen. Dazu ist der Fundamentalsatz Hauptspieler. Er sagt unter anderem, dass (unter gewissen Bedingungen) eine *Bijektion zwischen der Menge der Zwischenkörper der Erweiterung und den Untergruppen der Galoisgruppe existiert.*

Zuerst führen wir den Begriff der Galois-Korrespondenz ein. Ist $E$ ein Zwischenkörper, so assoziiert man zu $E$ die Untergruppe $\mathrm{Gal}_E K$ von $\mathrm{Gal}_F K$. Damit kann man eine Funktion von der Menge aller Zwischenkörper $S$ in die Menge aller Untergruppen von $\mathrm{Gal}_F K$ definieren:

$$\begin{array}{rl} E & \longmapsto \mathrm{Gal}_E K \\ \text{wobei } F \subseteq E \subseteq K & \text{dabei ist } \mathrm{Gal}_F K \geq \mathrm{Gal}_E K \geq \mathrm{Gal}_K K = \{\iota\} \end{array}$$

Diese Zuordnung heisst die **Galois-Korrespondenz**.

Unter der Galois-Korrespondenz gehören die trivialen Zwischenkörper, also $F$ und $K$ zu den trivialen Untergruppen: $K$ entspricht der Identitätsuntergruppe $\mathrm{Gal}_K K = \{\iota\}$ und $F$ der ganzen Gruppe $\mathrm{Gal}_F K$.

**Beispiel 14.1.** Am Beispiel $F = \mathbb{Q}$ und $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ können wir das anschauen. Wir betrachten die drei Zwischenkörper $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Wir verwenden die Notation aus Beispiel 13.7

$$\begin{aligned} \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) &\longrightarrow \mathrm{Gal}_{\mathbb{Q}(\sqrt{3},\sqrt{5})} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{\iota\} \\ \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) &\longrightarrow \mathrm{Gal}_{\mathbb{Q}(\sqrt{3})} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{\iota, \alpha\} \\ \mathbb{Q} \subseteq \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) &\longrightarrow \mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{\iota, \tau, \alpha, \beta\} \end{aligned}$$

Aus Beispiel refQ-3-fix wissen wir, dass $\mathbb{Q}(\sqrt{3})$ der Fixkörper der UGruppe $\{\iota, \alpha\}$ $=\mathrm{Gal}_{\mathbb{Q}(\sqrt{3})} \mathbb{Q}(\sqrt{3}, \sqrt{5})$ ist. Der Körper $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$ ist eine normale, separable Erweiterung von $\mathbb{Q}(\sqrt{3})$, da er der ZK von $x^2 - 5$ ist und Charakteristik 0 hat (man benutzt hier Korollar 12.2).

**Lemma 14.2.** *Sei $K$ eine endlich-dimensionale KE von $F$. Ist $H$ eine Untergruppe der Galoisgruppe $Gal_F K$ und $E$ der Fixkörper von $H$, dann ist $K$ eine einfache, normale, separable Erweiterung von $E$.*

*Beweis.* Lemma 11.7 in [Hu]. Die Beweisideen hier:

- Sei $u \in K$. $u$ ist algebraisch über $F$, damit auch algebraisch über $E$. Sei $p(x) \in E[x]$ das Minimalpolynom von $u$. Für jedes $\sigma \in H$ ist dann nach Satz 13.3 das Bild $\sigma(u)$ auch Nullstelle von $p(x)$.
- Die Menge der Bilder $\{\sigma(u) \mid \sigma \in H\}$ von $u$ unter $H$ ist endlich (da $p(x)$ endliche Grad hat). Wir schreiben sie als $\{u_1 = u, \ldots, u_t\}$, $u_i \in K$.
- Jedes Element $\sigma \in H$ permutiert die $u_i$: ist $\sigma \in H$ und $u_i = \tau(u)$ (mit $\tau \in H$), so gilt $\sigma(u_i) = \sigma(\tau(u))$. Da $\sigma \circ \tau$ auch in $H$ liegt, liegt also $\sigma(u_i)$ ebenfalls in der Menge $\{u_1, \ldots, u_t\}$ und da $\sigma$ injektiv ist, sind die $\sigma(u_1), \ldots, \sigma(u_t)$ alle verschiedne Bilder von $u$, also bilden sie grad die Menge $\{u_1, \ldots, u_t\}$.
- Das Polynom $f(x) := (x - u_1) \cdots (x - u_t)$ ist separabel (die $u_i$ sind verschieden).
- Es gilt: $f(x) \in E[x]$: Sei $\sigma \in H$ beliebig. Nun induziert $\sigma$ einen Isomorphismus $K[x] \cong K[x]$ (Diskussion vor Korollar 9.9) und

  $$\sigma f(x) = (x - \sigma(u_1)) \cdots (x - \sigma(u_t))$$

  Das ist gleich $f(x)$, da ja $\sigma$ nur die $u_i$ permutiert. Also schickt jedes $\sigma$ die Koeffizienten des separablen Polynoms $f(x)$ auf sich selbst, und sie liegen daher in $E$ (dem Fixkörper von $H$). Als Nullstelle von $f(x) \in E[x]$ ist $u = u_1$ separabel über $E$.
- Damit ist (weil $u \in K$ beliebig war) ganz $K$ separabel über $E$.
- $K$ ist endlich erzeugt über $F$, also auch über $E$. Damit ist $K = E(u)$ für ein $u \in K$ (Satz 12.3 vom primitiven Element). Das Polynom $f(x)$ (von oben) zerfällt, damit erhält man die Normalität von $K$ (Satz 11.4).

□

**Satz 14.3.** *Sei $K$ eine endlich-dimensionale KE von $F$. Ist $H$ eine Untergruppe von $Gal_F K$ und $E$ der Fixkörper von $H$, dann ist $H = Gal_E K$ und $|H| = [K : E]$. D.h. die Galois-Korrespondenz ist surjektiv.*

*Beweis.* (Theorem 11.8 in [Hu])

- Nach Lemma 14.2 ist $K = E(u)$ für ein $u$ in $K$. Sei $p(x)$ das Minimalpolynom von $u$ über $E$, sei $\deg p(x) = n$, also $[K : E] = n$.
- Es gibt maximal $n$ verschiedene Elemente in $\mathrm{Gal}_E K$, denn verschiedene Elemente von $\mathrm{Gal}_E K$ bilden $u$ auf verschiedene Nullstellen von $p(x)$ ab, also
$$|\mathrm{Gal}_E K| \leq n$$
- Es ist $H \subseteq \mathrm{Gal}_E K$ (nach Definition vom Fixkörper $E = E_H$), also
$$|H| \leq |\mathrm{Gal}_E K| \leq n = [K : E]$$
- Sei $f(x) = (x - u_1) \cdots (x - u_t)$ wie im Beweis von Lemma 14.2 (die $u_i$ sind die verschiedenen Bilder von $u$ unter den Elementen von $H$). Dann hat $H$ mindestens $t$ Elemente. Und es gilt $p(x) \mid f(x)$ (da $f(x)$ die Nullstelle $u$ hat muss es vom Minimalpolynom von $u$ geteilt werden). Somit hat man
$$|H| \geq t = \deg f(x) \geq \deg g(x) = n = [K : E]$$
- Alles zusammen gibt das
$$|H| = |\mathrm{Gal}_E K| = [K : E] \text{ und damit } H = \mathrm{Gal}_E K.$$

□

**Beispiel 14.4.** Nach Beispiel 13.14 ist $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \{\iota\}$, also sind die Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}$ von $\mathbb{Q}(\sqrt[3]{2})$ beide assoziiert mit der Gruppe $\{\iota\}$ unter der Galois-Korrespondenz.
Bemerkung: $\mathbb{Q}(\sqrt[3]{2})$ ist *keine* normale KE von $\mathbb{Q}$ (sie enthält die komplexen Nullstellen von $x^3 - 2$ nicht, das Polynom hat also eine Nullstelle in der Erweiterung, zerfällt aber dort nicht).

[Vorlesung 19, 9. Dezember 2014]

14.1. **Galoiserweiterungen.** Die Galois-Korrespondenz ist surjektiv (Satz 14.3), ist aber i.A. nicht injektiv (Beispiel 14.4).

**Definition.** Ist $K$ eine endlich-dimensionale, normale, separable KE des Körpers $F$, so sagt man, $K$ sei eine *Galoiserweiterung* von $F$ oder dass $K$ *galois'sch* ist über $F$.

**Satz 14.5.** *Sei $K$ eine Galoiserweiterung von $F$ und $E$ ein Zwischenkörper. Dann ist $E$ der Fixkörper der Untergruppe $Gal_E K$.*

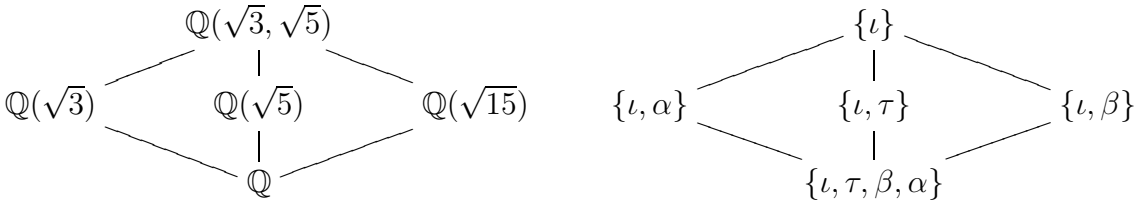
*Beweis.* Das ist Theorem 11.9 in [Hu]. Hier ganz kurz (nicht in der Vorlesung): Der Fixkörper $E_H$ von $H :=\mathrm{Gal}_E K$ enthält $E$ nach Definition. Wir müssen zeigen, dass $E_H \subseteq E$ gilt.

Das kann mit Kontraposition gezeigt werden. Ist $u \notin E$, dann wird $u$ durch einen Automorphismus $\sigma \in \mathrm{Gal}_E K$ bewegt. Da $K$ eine Galoiserweiterung von $E$ ist (und $E$ ist normal, dazu benutzt man Satz 11.4, sowie die Überlegung, dass wenn $K$ ein Zerfällungskörper von einem Polynom $f(x)$ über $F$ ist, $K$ auch ZK von $f(x)$ über $E$ ist. Ausserdem: Die Separabilität von $K$ über $F$ liefert auch die Separabilität von $K$ über $E$), ist $K$ eine algebraische Erweiterung von $E$. Damit ist $u$ algebraisch über $E$ mit Minimalpolynom $p(x) \in E[x]$ vom Grad $\geq 2$ (wäre der Grad 1, so wäre $u \in E$. Die Nullstellen von $p(x)$ sind alle verschieden (Separabilität), alle liegen in $K$ (Normalität). Sei $v$ eine Nullstelle von $p(x)$, $v \neq u$. Dann existiert $\sigma \in \mathrm{Gal}_E K$ mit $\sigma(u) = v$. Also ist $u \notin E_H$ und wir sind fertig. □

Sind $E$ und $L$ zwei Zwischenkörper mit $\mathrm{Gal}_E K = \mathrm{Gal}_L K$, so sind nach Satz 14.5 $E$ und $L$ beide Zwischenkörper der gleichen Gruppe, also $E = L$. Also zeigt Satz 14.5: **bei Galoiserweiterungen ist die Galois-Korrespondenz injektiv** .

**Beispiel 14.6.** Der Körper $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ ist eine Galoiserweiterung von $\mathbb{Q}$, denn er ist der Zerfällungskörper von $f(x) = (x^2 - 3)(x^2 - 5)$. Dann ist die Galois-Korrespondenz bijektiv (Satz 14.3, und Bemerkung nach Satz 14.5). Wir kennen die Galoisgruppe davon, es ist $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{\iota, \tau, \alpha, \beta\}$ (Beispiel 13.7). Man erhält die folgenden Grafiken (selber durchdenken):

**Zw-Körper** **Untergruppen**




Hier sind *alle* Zwischenkörper auch Galoiserweiterungen von $\mathbb{Q}$ (z.B. ist $\mathbb{Q}(\sqrt{5})$ der ZK von $x^2 - 5$). Ausserdem sind die enstprechenden Untergruppen der Galoisgruppe alle Normalteiler.

Etwas ähnliches gilt im allgemeinen Fall, wie das nächste Resultat sagt:

**Satz 14.7** (Fundamentalsatz der Galoistheorie)**.** *Ist $K$ eine Galoiserweiterung von $F$, so gilt*

(1) *Es existiert eine Bijektion zwischen der Menge $S$ aller Zwischenkörper der Erweiterung und der Menge $T$ aller Untergruppen der Galoisgruppe $Gal_F K$, gegeben durch die Zuordnung $E \longmapsto Gal_E K$. Ausserdem gilt*

$$[K : E] = |Gal_E K| \quad \textit{und} \quad [E : F] = [Gal_F K : Gal_E K]$$

(2) *Ein Zwischenkörper $E$ ist eine normale Erweiterung von $F$ genau dann, wenn gilt $Gal_E K \triangleleft Gal_F K$. In diesem Fall ist $Gal_F E \cong Gal_F K / Gal_E K$.*

*Beweis.* Teil (1):
Satz 14.3 und die Bemerkung nach Satz 14.5 zeigen die erste Aussage von Teil 1. Jeder Zwischenkörper $E$ ist der Fixkörper von $\mathrm{Gal}_E K$ (Satz 14.5), also gilt $[K : E] = |\mathrm{Gal}_E K|$ (Satz 14.3). Insbesondere ist $[K : F] = |\mathrm{Gal}_F K|$ falls $F = E$ ist. Der Satz von Lagrange und Satz 8.1 liefern

$$[K : E][E : F] = [K : F] = |\mathrm{Gal}_F K| = |\mathrm{Gal}_E K|[\mathrm{Gal}_F K : \mathrm{Gal}_E K]$$

Daraus folgt (mit kürzen mit $[K : E] = |\mathrm{Gal}_E K|$):

$$[E : F] = [\mathrm{Gal}_F K : \mathrm{Gal}_E K].$$

Teil (2):
$\Longleftarrow$: Sei $\mathrm{Gal}_E K \triangleleft \mathrm{Gal}_F K$. Sei $p(x)$ ein irreduzibles Polynom in $F[x]$ mit Nullstelle $u$ in $E$, wir müssen folgendes zeigen: $p(x)$ zerfällt in $E$. Da $K$ normal ist über $F$ (Definition Galoiserweiterung) wissen wir, dass $p(x)$ in $K[x]$ zerfällt. Also reicht es, zu zeigen, dass jede beliebige Nullstelle $v$ von $p(x)$ bereits in $E$ liegt. Nach Satz 13.4 existiert ein $\sigma \in \mathrm{Gal}_F K$ mit $\sigma(u) = v$. Ist $\tau$ ein beliebiges Element von $\mathrm{Gal}_E K$, so existiert (da die Untergruppe $\mathrm{Gal}_E K$ ein Normalteiler von $\mathrm{Gal}_F K$ ist) ein $\tau_1$ in $\mathrm{Gal}_E K$ mit $\tau \circ \sigma = \sigma \circ \tau_1$. Es gilt dann $\tau(v) = \tau(\sigma(u)) = \sigma(\tau_1(u)) \overset{u \in E}{=} \sigma(u) = v$, $v$ wird also von jedem Element von $\mathrm{Gal}_E K$ fixiert, liegt damit im Fixkörper von $\mathrm{Gal}_E K$ und der ist gleich $E$ (Satz 14.5).
$\Longrightarrow$ Es sei $E$ eine normale Erweiterung von $F$. $E$ ist endlich-dimensional über $F$ nach Teil (1). Nach Lemma 14.9 unten existiert ein surjektiver Gruppenhomomorphismus $\theta : \mathrm{Gal}_F K \longrightarrow \mathrm{Gal}_F E$. Dessen Kern ist $\mathrm{Gal}_E K$. Als Kern eines Gruppenhomomorphismus ist somit $\mathrm{Gal}_E K$ ein Normalteiler von $\mathrm{Gal}_F K$, [EA]. Der erste Isomorphiesatz, [EA], liefert $\mathrm{Gal}_F K / \mathrm{Gal}_E K \cong \mathrm{Gal}_F E$. □

**Beispiel 14.8.** Der Zerfällungskörper $K$ von $x^3 - 2$ ist eine Galoiserweiterung von $\mathbb{Q}$, ihre Galoisgruppe ist eine Untergruppe von $S_3$ nach Beispiel 13.9. Wir haben die Kette $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq K$. Da $x^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ ist, ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. (Satz 9.7). Die zwei Nullstellen $\sqrt[3]{2}w$ und $\sqrt[3]{2}w^2$ sind nicht reell, sie liegen daher nicht in $\mathbb{Q}(\sqrt[3]{2})$, damit ist $[K : \mathbb{Q}] > 3$. Ausserdem ist $[K : \mathbb{Q}] \leq 6$ (Sätze 11.2 und 11.3) und $[K : \mathbb{Q}]$ ist durch 3 teilbar (Satz 8.1), also ist $[K : \mathbb{Q}] = 6$. Damit hat $\mathrm{Gal}_{\mathbb{Q}} K$ Ordnung 6 und ist gleich $S_3$.
Die einzigen echten Untergruppen von $S_3$ sind die zyklische Gruppe der Ordnung 3, die von (123) erzeugt wird und die drei zyklischen Gruppen der Ordnung 2, die von (12), (23) bzw. von (13) erzeugt werden. Die Galois-Korrespondenz ist im Diagramm (Abbildung 1) illustriert (nachprüfen). Zwischenkörper und Untergruppen, die in der gleichen Position liegen, entsprechen dabei einander.
Der Körper $\mathbb{Q}(w)$ ist ein Zwischenkörper, da $w = (1/2)(\sqrt[3]{2})^2)(\sqrt[3]{2}w) \in K$. $\mathbb{Q}(w)$

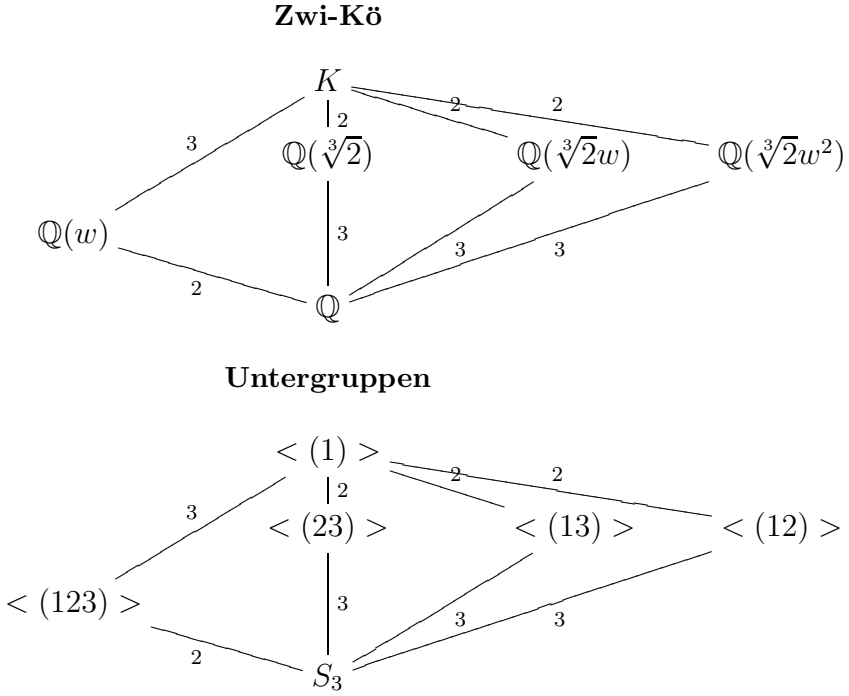



ABBILDUNG 1. Zu Beispiel 14.8

ist der Zerfällungskörper von $x^2+x+1$ (Übung), also galois'sch über $\mathbb{Q}$. Die entsprechende Untergruppe ist der Normalteiler $< (123) >$. Wir wissen (Beispiel 14.4), dass $\mathbb{Q}(\sqrt[3]{2})$ *nicht* galois'sch ist über $\mathbb{Q}$. Damit ist die entsprechende UGruppe $< (23) >$ kein Normalteiler von $S_3$.

[Vorlesung 20, 12. Dezember 2014]

Am obigen Beispiel sehen wir:
**die Galois-Korrespondenz ist inklusionsumkehrend**.

**Lemma 14.9.** *Sei $K$ ein endlich-dimensionale normale Erweiterung von $F$ und $E$ ein Zwischenkörper, der normal ist über $F$. Dann existiert ein surjektiver Gruppenhomomorphismus $\theta : Gal_F K \to Gal_F E$ dessen Kern gleich $Gal_E K$ ist.*

*Beweis.* Sei $\sigma \in \mathrm{Gal}_F K$ und $u \in E$. $u$ ist algebraisch über $F$, sei $p(x)$ sein Minimalpolynom. Da $E$ eine normale Erweiterung von $F$ ist, zerfällt $p(x)$ in $E[x]$, alle Nullstellen von $p(x)$ liegen also in $E$.
Nach Satz 13.3 ist $\sigma(u)$ eine Nullstelle von $p(x)$, also ist $\sigma(u) \in E$. Damit gilt $\sigma(E) \subseteq E$ für jedes $\sigma \in \mathrm{Gal}_F K$. Es folgt, dass die Einschränkung $\sigma \mid_E$ von $\sigma$ auf $E$ ein $F$-Isomorphismus ist $E \cong \sigma(E)$. Nach Satz 8.2 gilt dann $[E : F] = [\sigma(E) : F]$. Mit $F \subseteq \sigma(E) \subseteq E$ erhält man $[E : F] = [E : \sigma(E)] \cdot [\sigma(E) : F]$, also muss $[E : \sigma(E)] = 1$ sein (Satz 8.1). Es ist daher $E = \sigma(E)$ und $\sigma \mid_E$ ein Element von $\mathrm{Gal}_F E$.

Man definiert nun $\theta$ :$\mathrm{Gal}_F K \to \mathrm{Gal}_F E$ durch $\theta(\sigma) := \sigma\mid_E$. Das ist ein Gruppenhomomorphismus, sein Kern besteht aus den Automorphismen von $K$, deren Einschränkung auf $E$ die Identität ist, also aus der Gruppe $\mathrm{Gal}_E K$.

Es bleibt, zu zeigen, dass $\theta$ surjektiv ist: Da $K$ ein ZK über $F$ ist (nach Satz 11.4), ist $K$ ein ZK des gleichen Polynoms über $E$. Daher kann jedes $\tau \in \mathrm{Gal}_F E$ zu einem $F$-Automorphismus $\sigma \in \mathrm{Gal}_F K$ erweitert werden (Satz 11.3). Und für $\sigma$ gilt $\sigma\mid_E = \theta(\sigma) = \tau$, d.h. $\theta$ ist surjektiv. □

Im Beweis von Lemma 14.9 wurde die Normalität erst gegen Ende benutzt. Der erste Teil des Beweises zeigt auch die folgende Aussage:

**Korollar 14.10.** *Sei $K$ ein Erweiterungskörper von $F$ und $E$ ein Zwischenkörper, der nicht normal ist über $F$. Ist $\sigma \in Gal_F K$, so gilt*

$$\sigma\mid_E \in Gal_F E.$$

## 15. Auflösbarkeit mittels Radikalen

Wie bereits erwähnt, haben Ruffini und Abel gezeigt, dass es keine Lösungsformel für *alle* Polynome vom Grad $n \geq 5$ geben kann. Galois hat dann ein Kriterium geliefert, das erlaubt, zu bestimmen, welche polynomialen Gleichungen lösbar sind. Mit Hilfe dieses Kriterium können wir ein Polynom vom Grad 5 angeben, dessen Nullstellen nicht mittels einer Formel gefunden werden können (Beispiel 15.4 weiter unten).

Der Einfachheit halber setzen wir in diesem Kapitel Charakteristik 0 voraus, das wird im Kriterium benötigt.

Eine Lösungsformel für eine polynomiale Gleichung ist ein Rezept, das aus den Koeffizienten eines Polynoms $f(x) \in F[x]$ Nullstellen von $f(x) = 0_F$ liefert, indem nur Körperoperationen (Addition, Subtraktion, Multiplikation und Division) sowie Wurzelziehen erlaubt (Quadratwurzeln, dritte Wurzeln, vierte Wurzeln, etc.). Dabei verstehen wir unter der $n$-ten Wurzel eines Elements $c \in F$ eine Nullstelle des Polynoms $x^n - c$ in einem Erweiterungskörper von $F$.

Führt man Körperoperationen an den Koeffizienten von $f(x) \in F[x]$ durch, so bleibt man im Körper $F$ (Abgeschlossenheit!). Wenn man eine $n$-te Wurzel nimmt, so ist es jedoch möglich, dass man in einem EK von $F$ landet. Zieht man danach nochmals eine Wurzel, sagen wir, eine $m$-te, so landet man ev. in einem noch grösseren EK. Die Existenz einer Formel für $f(x) = 0_F$ impliziert also, dass diese Lösungen in einem speziellen EK von $F$ liegen.

Wir werden dies weiter unten an einer Gleichunge vom dritten Grad illustrieren, siehe Beispiel 15.2, dort konstruieren wir eine Kette von vier Erweiterungen, $F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4$ zu den Nullstellen von $x^3 + 3x + 2 = 0$. (Falls man mehr dazu lesen möchte: Das Material ist nur ein Teil von Kapitel 11 in [Hu]).

**Definition.** Sei $f(x) \in F[x]$. Die *Galoisgruppe von* $f(x)$ ist $\mathrm{Gal}_F K$, wobei $K$ ein Zerfällungskörper von $f(x)$ über $F$ ist[20]

**Satz 15.1** (Kriterium von Galois)**.** *Sei $F$ ein Körper der Charakteristik 0, sei $f(x) \in F[x]$. Das Kriterium von Galois besagt folgendes:*

$$\left.\begin{array}{l} f(x) = 0_F \ \textit{ist} \\ \textit{auflösbar durch Radikale} \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{l} \textit{die Galoisgruppe von } f(x) \textit{ ist} \\ \textit{eine auflösbare Gruppe.} \end{array}\right.$$

*Beweis.* Ein vollständiger Beweis davon ist in [JS, Kapitel VI.5]. Theorem 11.19 in [Hu] beweist die Hälfte. □

Um dies zu verstehen, brauchen wir drei Definitionen.

**Definitionen.** 1) Ein Körper $K$ heisst eine *radikale Erweiterung* (Radikalerweiterung)[21] des Körpers $F$, falls eine Kette

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_t = K$$

von Körpern existiert, so dass für jedes $i = 1, \ldots, t$ gilt:

$$F_i = F_{i-1}(u_i) \text{ und eine Potenz von } u_i \text{ liegt in } F_{i-1}.$$

2) Sei $f(x) \in F[x]$. Die Gleichung $f(x) = 0_F$ heisst *auflösbar durch Radikale*, falls eine radikale Erweiterung von $F$ existiert, die einen Zerfällungskörper von $f(x)$ enthält[22].
3)Eine Gruppe $G$ heisst *auflösbar*, falls sie eine Kette

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \{e\}$$

von Untergruppen besitzt mit den Eigenschaften
(i) $G_i \triangleleft G_{i-1}$ (für $0 < i \leq n$), (ii) $G_{i-1}/G_i$ ist abelsch (für $0 < i \leq n$).

- Jede abelsche Gruppe $G$ ist auflösbar, da jede Quotientengruppe von $G$ auch abelsch ist, insbesondere erfüllt die Kette $G \supseteq \{e\}$ die Bedingungen der Definition.
- $S_3$ ist auflösbar, die Kette $S_3 \supseteq < (123) > \supseteq < (1) >$ hat die Eigenschaften (i) und (ii) der Definition. Aber i.A. gilt das für symmetrische Gruppen nicht, siehe Satz 15.3

Das folgende Beispiel (Beispiel 15.2) zeigt eine radikale Erweiterung von $\mathbb{Q}$, sowie eine Gleichung, die auflösbar ist durch Radikale.

[20]je zwei Zerfällungskörper von $f(x)$ über $F$ sind isomorph (Satz 11.3),also sind die entsprechenden Galoisgruppen isomorph, d.h. die Galoisgruppe von $f(x)$ ist unabhängig von der Wahl des Zerfällungskörpers $K$.

[21]Radikale sind Wurzelausdrücke, Wurzel=Nullstelle.

[22]Damit zerfällt $f(x)$ im grössten Körper der radikalen Erweiterung sicher in Linearfaktoren

**Beispiel 15.2.** Für kubische Gleichungen der Form $x^3 + bx + c = 0$ hat man die folgende Lösungsformel:

$$\begin{aligned} x_1 &= \sqrt[3]{(-c/2) + \sqrt{d}} + \sqrt[3]{(-c/2) - \sqrt{d}} \\ x_2 &= w\sqrt[3]{(-c/2) + \sqrt{d}} + w^2\sqrt[3]{(-c/2) - \sqrt{d}} \\ x_3 &= w^2\sqrt[3]{(-c/2) + \sqrt{d}} + w\sqrt[3]{(-c/2) - \sqrt{d}} \end{aligned}$$

für $d := (b^3/27) + (c^2/4)$, $w = (-1 + \sqrt{3}i)/2$.
Die Lösungsformel mit $b = 3$, $c = 2$ liefert

$$\begin{aligned} x_1 &= \sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}} \\ x_2 &= w\sqrt[3]{-1 + \sqrt{2}} + w^2\sqrt[3]{-1 - \sqrt{2}} \\ x_3 &= w^2\sqrt[3]{-1 + \sqrt{2}} + w\sqrt[3]{-1 - \sqrt{2}} \end{aligned}$$

Alle diese Lösungen liegen in der Kette

$$\begin{array}{ccccccc} \mathbb{Q} & \subseteq & \mathbb{Q}(w) & \subseteq & \mathbb{Q}(w, \sqrt{2}) & \subseteq & \mathbb{Q}(w, \sqrt{2}, \sqrt[3]{-1 + \sqrt{2}}) \\ \| & & \| & & \| & & \| \\ F_0 & \subseteq & F_1 & \subseteq & F_2 & \subseteq & F_3 \end{array}$$

(hier fortgesetzt):

$$\begin{array}{ccc} \mathbb{Q}(w, \sqrt{2}, \sqrt[3]{-1 + \sqrt{2}}) & \subseteq & \mathbb{Q}(w, \sqrt{2}, \sqrt[3]{-1 + \sqrt{2}}, \sqrt[3]{-1 - \sqrt{2}}) \\ \| & & \| \\ F_3 & \subseteq & F_4 \end{array}$$

Jeder Körper in dieser Kette ist eine einfache Erweiterung des Vorherigen, und zwar von der Form $F_j(u)$ für ein $u$ mit $u^n \in F_j$ (für ein $n$), d.h. $u$ ist die $n$-te Wurzel eines Elements von $F_j$:

$$\begin{array}{ll} F_1 = F_0(w) & \text{mit } w^3 = 1 \in F_0 \\ F_2 = F_1(\sqrt{2}) & \text{mit } (\sqrt{2})^2 = 2 \in F_0 \subseteq F_1 \\ F_3 = F_2(\sqrt[3]{-1 + \sqrt{2}}) & \text{mit } (\sqrt[3]{-1 + \sqrt{2}})^3 = -1 + \sqrt{2} \in F_2 \\ F_4 = F_3(\sqrt[3]{-1 - \sqrt{2}}) & \text{mit } (\sqrt[3]{-1 - \sqrt{2}})^3 = -1 - \sqrt{2} \in F_2 \subseteq F_3 \end{array}$$

Da $F_4$ alle Lösungen von $x^3 + 3x + 2 = 0$ enthält, ist $F_4$ eine radikale Erweiterung von $F_0$, die einen Zerfällungskörper (gerade $F_4$ selbst) von $x^3 + 3x + 2$ enthält.
Damit haben wir eine radikale Erweiterung von $\mathbb{Q}$ gefunden und gezeigt, dass $f(x)$ auflösbar ist durch Radikale.

**Satz 15.3.** *Ist $n \geq 5$, so ist $S_n$ nicht auflösbar.*

*Beweis.* Wir nehmen an, $S_n$ sei auflösbar, d.h., es gäbe eine Kette

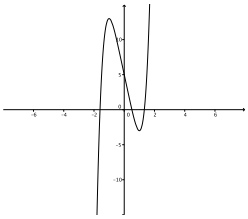
$$S_n = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n =< (1) >$$

wie verlangt (Definition von Auflösbarkeit). Sei $(rst)$ ein 3-Zykel in $S_n$ und $u$, $v$ zwei Elemente von $\{1, 2, \ldots, n\}$, die verschieden von $r$, $s$, $t$ sind (das geht wegen $n \geq 5$). Da $S_n/G_1$ abelsch ist, muss $G_1$ das Element

$$(tus)(srv)(tus)^{-1}(srv)^{-1} = (tus)(srv)(tsu)(svr) = (rst)$$

enthalten[23]. Damit enthält $G_1$ alle 3-Zykeln (denn $(rst)$ war beliebig).
$G_1/G_2$ ist auch abelsch, wir wiederholen das Argument mit $G_1$ anstatt $S_n$ und $G_2$ anstelle von $G_1$. Daraus können wir schliessen, dass $G_2$ alle 3-Zykeln enthält. Nun ist jeder Quotient $G_i/G_{i+1}$ abelsch, wiederholtes Anwenden des gleichen Arguments führt zum Schluss, dass die triviale Untergruppe $G_t =< (1) >$ alle 3-Zykeln enthalten muss, ein Widerspruch. □

**Beispiel 15.4.** Die Galoisgruppe des Polynoms $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ ist $S_5$, diese Gruppe ist nicht auflösbar (Satz 15.3) Damit ist die Gleichung $2x^5 - 10x + 5 = 0$ nicht durch Radikale lösbar (Satz 15.1).
Wir müssen zeigen, dass die Galoisgruppe von $f(x)$ gerade $S_5$ ist. Dazu schauen wir zuerst das Verhalten der Nullstellen des Polynoms an. Man betrachtet $f'(x) = 10x^4 - 10$. Dessen Nullstellen sind $\pm 1$ und $\pm i$. Die zweite Ableitung $f''(x) = 40x^3$, d.h. $f$ hat ein relatives Maximum in $x = -1$, ein relatives Minimum in $x = 1$ und einen Wendepunkt in $x = 0$. Damit hat $f(x)$ drei reelle Nullstellen.



Der (reelle) Graph sieht etwa so aus (mit Geogebra gezeichnet).
Mit dem Kriterium von Eisenstein (mit $p = 5$) ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$. Ist $K$ ein Zerfällungskörper von $f(x)$ in $\mathbb{C}$, so ist die Ordnung von $\mathrm{Gal}_{\mathbb{Q}}K$ gleich $[K : \mathbb{Q}]$ (Fundamentalsatz, Satz 14.7). Ist $r$ irgendeine Nullstelle von $f(x)$, so haben wir $[K : \mathbb{Q}] = [K : \mathbb{Q}(r)][\mathbb{Q}(r) : \mathbb{Q}]$ (Satz 8.1). Wir wissen, dass $[\mathbb{Q}(r) : \mathbb{Q}] = 5$ ist (Satz 9.7). Die Ordnung der Galoisgruppe $\mathrm{Gal}_{\mathbb{Q}}K$ ist daher durch 5 teilbar und enthält dann ein Element der Ordnung 5, 2.2.
Nach Korollar 13.8 gilt $\mathrm{Gal}_{\mathbb{Q}}K \leq S_5$. Die einzigen Elemente der Ordnung 5 in $S_5$ sind die 5-Zykeln. Damit muss $\mathrm{Gal}_{\mathbb{Q}}K$ einen 5-Zykel enthalten. Komplexe Konjugation liefert einen Automorphismus von $K$ (Korollar 14.10). Dieser Automorphismus vertauscht die beiden nicht reellen Nullstellen von $f(x)$ und hält die drei reellen Nullstellen fest. D.h. die komplexe Konjugation ist (als Permutation gesehen) eine Transposition; $\mathrm{Gal}_{\mathbb{Q}}K$ enthält damit eine Transposition. Man muss dann zeigen

[23]Sei $N \triangleleft G$. Dann ist $G/N$ abelsch $\Leftrightarrow$ für alle $a, b \in G$ ist $aba^{-1}b^{-1} \in N$. Hier: $a = tus$, $b = srv$.

(Übung)[24], dass die einzige Unterguppe von $S_5$, die sowohl eine Transposition als auch einen 5-Zykel enthält, die ganze $S_5$ ist. Also ist $\mathrm{Gal}_{\mathbb{Q}}K = S_5$.

## Ergänzung: Geometrische Konstruktionen (Zirkel und Lineal)

Hier eine sehr kurze Übersicht von Wikipedia, [W3]. Mehr kann man z.B. in [Hu, Kapitel 15] lesen.

Die klassischen Probleme der antiken Mathematik, bei denen es um die Konstruierbarkeit einer bestimmten Zahl (als Streckenlänge) allein mit Zirkel und Lineal aus rationalen Zahlen geht, konnten mit der Galoistheorie in gruppentheoretische Fragen umformuliert werden.

Es sei eine Einheitslänge 1 gegeben.

**Definition** ([St])**.** Eine Zahl $\alpha$ heisst *konstruierbar*, wenn, ausgehend von der Einheitslänge mit Zirkel und Lineal eine Strecke der Länge $\alpha$ konstruiert werden kann.

Mit dem Grundgedanken von René Descartes, dass die Punkte auf Geraden (Lineal) und Kreisen (Zirkel) durch analytische Gleichungen darstellbar sind, lässt sich zeigen, dass die konstruierbaren Zahlen genau die folgenden sind:

- Die rationalen Zahlen,
- die Quadratwurzeln aus konstruierbaren Zahlen,
- Summe, Differenz und Produkt von zwei konstruierbaren Zahlen,
- der Kehrwert jeder von 0 verschiedenen konstruierbaren Zahl.

Damit kann man zeigen, dass jede konstruierbare reelle Zahl

- algebraisch und
- vom Grad einer Zweierpotenz $2^n$ über dem Körper $\mathbb{Q}$ der rationalen Zahlen ist.

Dies bedeutet, dass für eine konstruierbare Zahl $c$ die Körpererweiterung $\mathbb{Q}(c) \supseteq \mathbb{Q}$ eine endliche, algebraische Erweiterung vom Grad $2^n$ ($n \in \mathbb{N}$) sein muss. Dies ist noch keine hinreichende Bedingung, genügt aber in den klassischen Fragen für einen Unmöglichkeitsbeweis.

(1) Quadratur des Kreises: Unmöglich, da die Kreiszahl $\pi$ nicht algebraisch ist.
(2) Verdoppelung des Würfels: Unmöglich: Im Verhältnis zum konstruierten Ausgangswürfel (etwa ein Würfel mit der Kantenlänge 1) hätte der neue Würfel die Kantenlänge $\alpha = \sqrt[3]{2}$. Die Körpererweiterung $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$ hat den Grad 3 - keine Zweierpotenz.

[24]Sei $G \leq S_5$, $G$ enthalte eine Transposition $\sigma = (rs)$ und einen 5-Zykel $\alpha$. Dann zeigt man
(a) Es existiert ein $k$, so dass gilt $\alpha^k = (rsxyz)$. Sei $\tau = \alpha^k \in G$. Bis auf Umnummerierung können wir annehmen, dass gilt: $\sigma = (12)$ und $\tau = (12345)$.
(b) Man zeigt, dass (12), (23), (34) und (45) alle in $G$ sind (man betrachte $\tau^k\sigma\tau^{-k}$ für $k \geq 1$)
(c) Man zeigt, dass (13), (14) und (15) in $G$ liegen (was ist (12)(23)(12)?)
(d) Man zeigt, dass jede Transposition in $G$ liegt. Also ist $G = S_5$ (Korollar 1.8)

(3) Dreiteilung des Winkels: Ein Winkel mit dem Gradmass $60°$ kann mit Zirkel und Lineal nicht in drei gleiche Teile geteilt werden. Wäre dieser Winkel - also $20°$ - konstruierbar, dann könnte man auch die reelle Zahl $\xi = \cos 20°$ konstruieren. Für jeden Winkel $\alpha$ gilt das Additionstheorem $\cos(3\alpha) = 4(\cos(\alpha))^3 - 3\cos(\alpha)$. Also löst unsere Zahl $\xi$ die Gleichung $\frac{1}{2} = 4x^3 - 3x$ und ist daher eine Nullstelle von $8x^3 - 6x - 1$. Da dieses Polynom über $\mathbb{Q}$ irreduzibel ist, hat $\xi$ über $\mathbb{Q}$ den Grad 3.

# **Teil** 5. Modultheorie

[Vorlesung 21, 16. Dezember 2014]

Dieses Kapitel gibt eine kurze Einführung in die Modultheorie. Die Hauptquelle ist das Buch [St] von U. Stammbach. Ein Modul ("der Modul"!) über einem Ring ist einerseits eine Verallgemeinerung des Begriffs des Vektorraums über einem Körper, andrerseits ist ein Modul eine abelsche Gruppe. Moduln treten in vielen mathematischen Gebieten auf, insbesondere in der Darstellungstheorie, der Zahlentheorie, in der kommutativen Algebra, der homologischen Algebra und in der algebraischen Topologie.

## 16. Definitionen

Sei $R$ ein Ring (mit Eins), nicht notwendig kommutativ.

**Definition.** Ein *Linksmodul über* $R$ (ein $R$*-Linksmodul*) ist eine abelsche Gruppe $A$ zusammen mit einer Operation $(\lambda, a) \mapsto \lambda a$, $\lambda \in R$, $a \in A$, welche den Axiomen

$$\begin{aligned} \lambda(a+b) &= \lambda a + \lambda b, \\ (\lambda+\mu)a &= \lambda a + \mu a, \\ (\lambda\mu)a &= \lambda(\mu a) \\ 1_R a &= a \end{aligned}$$

genügt, $\forall \lambda, \mu \in R$, $a, b \in A$.

Nach diesen Axiomen ist für festes $\lambda \in R$ die Zuordnung $a \mapsto \lambda a$ ein Homomorphismus $T_\lambda : A \to A$ von abelschen Gruppen.

Analog kann man auch eine "Rechts"-Operation betrachten, das liefert die Definition eines *Rechtsmoduls* über $R$ (eines $R$*-Rechtsmoduls*). Ist $R$ kommutativ, so sind die beiden Begriffe äquivalent, i.A. ist das aber nicht der Fall. Wenn nicht explizit anders erwähnt, werden wir immer Linksmoduln betrachten.

**Definition.** 1) Sei $A$ ein Linksmodul über $R$. Ein *Untermodul* $B$ von $A$ ist eine Untergruppe der abelschen Gruppe $A$ mit $\lambda b \in B$ für alle $\lambda \in R$ und für alle $b \in B$. Unter der induzierten Operation ist $B$ ein Linksmodul über $R$.

2) Es seien $A$ und $A'$ zwei $R$-Linksmoduln. Ein $R$*-Modulhomomorphismus* $f : A \to A'$ ist ein Homomorphismus von abelschen Gruppen mit

$$f(\lambda a) = \lambda(f(a))$$

für alle $\lambda \in R$ und alle $a \in A$.

**Beispiele.** (1) Sei $R = k$ ein Körper. Ein $R$-Modul ist nichts anderes als ein $k$-VR, ein $R$-Untermodul ist ein $k$-Unterraum und ein $R$-Modulhomomorphismus ist eine $k$-lineare Abbildung.

(2) Sei $R = \mathbb{Z}$. Jede abelsche Gruppe $A$ kann als $\mathbb{Z}$-Modul aufgefasst werden. Dabei definiert man für $a \in A$, $n \in \mathbb{Z}$ die Operation von $\mathbb{Z}$ auf $A$ wie folgt:

$$na = \begin{cases} a + a + \cdots + a & n\text{-fach} & n \geq 1 \\ 0 & & n = 0 \\ -(a + a + \cdots + a) & -n\text{-fach} & n < 0 \end{cases}$$

Man soll sich davon überzeugen, dass die Axiome erfüllt sind.
Damit sind die Begriffe "$\mathbb{Z}$-Modul" und "abelsche Gruppe" gleichbedeutend. Homomorphismen von $\mathbb{Z}$-Moduln sind Homomorphismen von abelschen Gruppen.

(3) Der Ring $R$ besteht aus einem Tripel $(R, +, \cdot)$, wobei $(R, +)$ eine abelsche Gruppe ist. Diese ist ein Linksmodul (ein Rechtsmodul) über $R$ unter der Operation, die durch die $R$-Multiplikation von links (von rechts) induziert wird. Dass die Axiome eines Moduls erfüllt sind, ist eine direkte Folgerung der Ringaxiome. Man sagt, $R$ sei ein *Linksmodul über sich selbst* (*ein Rechtsmodul über sich selbst*). Die $R$-Untermoduln des $R$-Linksmoduls $R$ sind die *Links*ideale im Ring $R$, die Untermoduln des $R$-Rechtsmoduls $R$ sind die *Rechts*ideale.

(4) Sei $R$ ein Ring und eine indizierte Menge $S := \{s_i \mid i \in I\}$ sei gegeben. Dann ist der *freie $R$-(Links-)Modul* $F(S)$ auf der Menge $S$ wie folgt definiert:

| | |
|---|---|
| Elemente: | formale Summen $\sum_{i\in I} \lambda_i s_i$, wobei nur endlich viele der $\lambda_i$ verschieden von Null sind |
| Addition: | $\sum_{i\in I} \lambda_i s_i + \sum_{i\in I} \mu_i s_i = \sum_{i\in I} (\lambda_i + \mu_i) s_i$ für $\lambda_i, \mu_i \in R$ |
| $R$-Operation: | $\lambda(\sum_{i\in I} \lambda_i s_i) = \sum_{i\in I} (\lambda\lambda_i) s_i$ für $\lambda, \lambda_i \in R$. |

Die Axiome sind erfüllt, $F(S)$ ist ein $R$-Modul. Unter den Elementen von $F(S)$ sind speziell

$$s_j = \sum_{i\in I} \lambda_i s_i, \quad \text{mit} \quad \lambda_i = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$$

Die Menge dieser Elemente kann mit $S$ identifiziert werden, also kann man $S$ als Teilmenge von $F(S)$ auffassen. Man nennt dies eine *Basis von* $F(S)$:

- $S$ "erzeugt" $F(S)$: jedes Element von $F(S)$ lässt sich als (endliche) Linearkombination von Elementen in $S$ mit Koeffizienten in $R$ schreiben,
- $S$ ist "linear unabhängig": aus $\sum_{i\in I} \lambda_i s_i = 0$ folgt $\lambda_i = 0$ für alle $i \in I$.

**Satz 16.1** (Universelle Eigenschaft des freien Moduls)**.** *Zu jedem $R$-Modul $A$ und zu jeder Funktion $f : S \to A$ ($S$ eine Menge) existiert ein eindeutig bestimmter $R$-Modulhomomorphismus $\psi : F(S) \to A$ mit $\psi\,|_S = f$.*

*Beweis.* Es sei $\varphi : F(S) \to A$ ein beliebiger $R$-Modulhomomorphismus, es ist dann:

$$\varphi(\sum_{i\in I} \lambda_i s_i) = \sum_{i\in I} \lambda_i \varphi(s_i)$$

Der Homomorphismus $\varphi$ ist somit bestimmt, wenn seine Werte auf der Basis $S$ gegeben sind. Daraus folgt, dass der gesuchte Homomorphismus $\psi$ eindeutig bestimmt ist, falls er existiert. Man setzt

$$\psi(\sum_{i\in I} \lambda_i s_i) = \sum_{i\in I} \lambda_i f(s_i)$$

damit ist $\psi : F(S) \to A$ ein $R$-Modulhomomorphismus, der eingeschränkt auf $S$ gerade $f$ ist. □

**Bemerkung.** Ist $R = k$ ein Körper, so ist jeder $R$-Modul $A$ frei, denn jeder $R$-Modul ist ein $k$-VR und besitzt damit eine Basis, d.h. es existiert eine Menge $S$ mit $F(S) = A$

**Definition.** Ein Vektorraum $B$ über einem Körper $k$ mit einer Verknüpfung $B \times B \to B$, $(x, y) \mapsto xy$, heisst *$k$-Algebra* oder *Algebra über $k$* falls für alle $a, b, c \in B$ und für alle $\lambda \in k$ gilt:

| | | | |
|---|---|---|---|
| $(a+b)c$ | $=$ | $ac + bc$ | Rechts-Distributivität |
| $a(b+c)$ | $=$ | $ab + ac$ | Links-Distributivität |
| $\lambda(ab)$ | $=$ | $(\lambda a)b = a(\lambda b)$ | Kompatibilität mit Skalaren |

(d.h. das Produkt ist bilinear bzgl. $k$).

**Bemerkung.** 1) Man kann Algebren auch über kommutativen Ringen definieren, d.h. man ersetzt "ein Vektorraum $B$ über einem Körper" mit "ein $R$-Modul $B$, wobei $R$ ein kommutativer Ring ist".

2) Wir werden im Folgenden nur Algebren betrachten, die selber Ringe mit 1 sind bzgl. der gegebenen Addition und der Algebrenmultiplikation. D.h. dass die Multiplikation assoziativ ist und dass die Algebra ein Neutralelement der Multiplikation besitzt.

Man nennt die Algebren dann auch *unitale assoziative Algebren* wegen der Existenz der 1 und wegen der Assoziativität - es gibt auch nicht-assoziative Algebren.

Beispiele von Algebren sind Polynomringe in mehreren Variablen über einem Körper oder Matrizenringe $M_n(k)$ über einem Körper.

**Beispiel 16.2** (Gruppenalgebren)**.** Sei $G$ eine multiplikativ geschriebene Gruppe, sei $k$ ein Körper. Die Gruppenalgebra $R = kG$ ist wie folgt definiert:
Als $k$-Vektorraum besitzt $kG$ die Basis $\{x \mid x \in G\}$. Die Elemente von $kG$ sind also die Linearkombinationen $\sum_{x\in G} a_x x$, $a_x \in k$.
Die Addition: $\sum_{x\in G} a_x x + \sum_{x\in G} b_x x = \sum_{x\in G}(a_x + b_x)x$, $a_x, b_x \in k$.

Das Produkt zweier Elemente:

$$(\sum_{x\in G} a_x x)\cdot(\sum_{y\in G} b_y y) = \sum_{xy\in G} a_x b_y xy$$

Ist $G$ endlich, $G = \{e = x_1, \dots, x_n\}$, so kann man das Gruppenelement $x_i \in G$ mit dem Ringelement

$$0x_1 + 0x_2 + \cdots + 0x_{i-1} + 1x_i + 0x_{i+1} + \cdots + 0x_n \in kG$$

identifizieren. Unter dieser Identifikation wird das Neutralelement $e = x_1$ der Gruppe $G$ zum Einselement $1_R$ des Rings $R = kG$.

**Beispiele** (Fortsetzung). (5) **Moduln via Ringhomomorphismen**:

Ist $\varphi : R' \to R$ ein Ringhomomorphismus und $A$ ein $R$-Modul, so ist $A$ auch ein $R'$-Modul: Die Operation von $R'$ in $A$ ist definiert durch

$$\lambda' a := (\varphi(\lambda'))a \text{ für alle } a \in A,\ \lambda' \in R'$$

Die Axiome sind erfüllt. Man sagt, dass die Operation von $R$ mittels $\varphi$ auf $R'$ *zurückgezogen wird.*

Ist insbesondere $R \neq \{0\}$ eine Algebra über einem Körper $k$, so hat man einen injektiven Ringhomomorphismus

$$\varphi : k \to R,\ a \mapsto a1_R,\ a \in k$$

Wenn nun $A$ ein $R$-Modul ist, so kann man die Operation von $R$ auf $k$ zurückziehen und erhält damit eine $k$-Vektorraumstruktur auf $A$.

## 17. Quotientenmodul, direkte Summe

Es sei $A$ ein $R$-Modul und $B$ ein Untermodul. $B$ ist insbesondere eine Untergruppe von $A$ (und ein Normalteiler, da es sich ja um abelsche Gruppen handelt). In der Restklassengruppe $A/B$ kann eine Modulstruktur definiert werden:

$$\lambda(a + B) := \lambda a + B,\ \forall\ \lambda \in R, a \in A$$

Damit dies Sinn macht, muss man zeigen, dass diese Definition nicht von der Wahl der Repräsentanten abhängt. Es sei also $a' = a + b$ mit $b \in B$. Dann hat man

$$\lambda(a' + B) = \lambda a' + B = \lambda(a + b) + B = \lambda a + \lambda b + B = \lambda a + B = \lambda(a + B).$$

Man überprüft, dass diese Operation von $R$ auf $A/B$ die Modulaxiome erfüllt. Die kanonische Projektion (Restklassenhomomorphismus) $\pi : A \to A/B$, die ein Homomorphismus von abelschen Gruppen ist, ist wegen

$$\pi(\lambda a) = (\lambda a) + B = \lambda(a + B) = \lambda(\pi(a))$$

ein $R$-Modulhomomorphismus.

Man nennt den $R$-Modul $A/B$ den *Quotienten- oder Faktormodul* der $R$-Moduln $B \subseteq A$.

[Vorlesung 22, 9. Januar 2015]

**Satz 17.1.** *Sei $\varphi : A \to A'$ ein R-Modulhomomorphismus. Dann ist*

$$\ker \varphi = \{a \in A \mid \varphi(a) = 0\}$$

*ein R-Untermodul von A und*

$$\varphi(A) = \operatorname{im} \varphi = \{\varphi(a) \mid a \in A\}$$

*ein R-Untermodul von $A'$*

*Beweis.* Für $a \in \ker \varphi$ gilt

$$\varphi(\lambda a) = \lambda(\varphi(a)) = \lambda \cdot 0 = 0$$

Damit ist $\ker \varphi$ ein Untermodul von $A$.

Sei $a' = \varphi(a)$ mit $a \in A$. Dann folgt $\lambda a' = \lambda(\varphi(a)) = \varphi(\lambda a)$, d.h. $\lambda a' \in \operatorname{im} \varphi$. Damit ist $\operatorname{im} \varphi$ ein Untermodul von $A'$. □

**Satz 17.2** (Isomorphiesatz für Moduln)**.** *Es sei $\varphi : A \to A'$ ein R-Modulhomomorphismus. Dann faktorisiert $\varphi$ über $\pi : A \to A/\ker \varphi$ und die induzierte Abbildung $\psi : A/\ker \varphi \to \varphi(A)$, $\psi(a + \ker \varphi) := \varphi(a)$ ist ein Isomorphismus von R-Moduln.*

*Beweis.* Eine Folge aus dem Homomorphiesatz (Korollar 2.17 in [EA]) Man muss nachprüfen, dass $\psi$ ein Homomorphismus von $R$-Moduln ist:

$$\psi(\underbrace{\lambda(a + \ker \varphi)}_{=\lambda a + \lambda \ker \varphi}) \overset{\ker \varphi \text{UModul}}{=} \psi(\lambda a + \ker \varphi) \overset{\text{Def } \psi}{=} \varphi(\lambda a) = \lambda(\varphi(a)) \overset{\text{Def } \psi}{=} \lambda(\psi(a + \ker \varphi))$$

(beim ersten Gleichheitszeichen links: es ist $\lambda \ker \varphi \subseteq \ker \varphi$) □

Aus diesem Isomorphiesatz ergibt sich analog wie im Fall von Gruppen ([EA]) der folgende Satz:

**Satz 17.3.** *Seien $B$ und $C$ Untermoduln des $R$-Moduls $A$. Es sei $\pi|_C : C \to A/B$ die Einschränkung der kanonischen Projektion $\pi : A \to A/B$. Dann induziert $\pi|_C$ einen Isomorphismus von R-Moduln*

$$C/B \cap C = C/\ker \pi|_C \xrightarrow{\sim} \operatorname{im} \pi|_C = (C + B)/B$$

*Beweis.* Mit dem 1. Isomorphiesatz für Gruppen ([EA], Satz 2.18 ii)), der folgendes sagt:
Sei $G$ eine Gruppe, $N \triangleleft G$ ein Normalteiler und $U \leq G$ eine Untergruppe. Dann ist $UN \leq G$ und $U \cap N \triangleleft U$ und man hat einen Isomorphismus $U/(U \cap N) \to (UN)/N$, $a \cdot (U \cap N) \mapsto aN$.
Hier sind alle Gruppen abelsch (als Moduln), daher alle UGruppen Normalteiler. □

Nun kommen wir zur direkten Summe von zwei oder beliebig vielen $R$-Moduln.

**Definition.** Seien $A$ und $B$ zwei $R$-Moduln. Die (externe) *direkte Summe* $A \oplus B$ der $R$-Moduln $A$ und $B$ ist wie folgt definiert: seien $a,\ a' \in A,\ b, b' \in B,\ \lambda \in R$ beliebig.

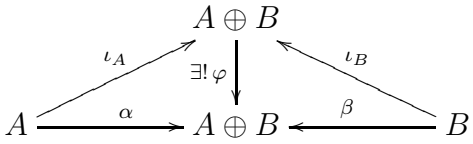
| | |
|---|---|
| Elemente von $A \oplus B$ | die Paare $(a, b)$, $a \in A$, $b \in B$ |
| Addition | $(a, b) + (a', b') := (a + a', b + b')$ |
| $R$-Operation | $\lambda(a, b) := (\lambda a, \lambda b)$ |

Die direkte Summe $A \oplus B$ enthält insbesondere die Untermoduln $A' := \{(a, 0) \mid a \in A\}$ und $B' := \{(0, b) \mid b \in B\}$.

Die kanonische Einbettung $\iota_A : A \hookrightarrow A \oplus B$, die durch $\iota_A(a) = (a, 0)$ definiert ist, induziert einen Isomorphismus $A \cong A'$. Ebenso induziert die Einbettung $\iota_B : B \hookrightarrow A \oplus B$, $\iota_B(b) = (0, b)$ einen Isomorphismus $B \cong B'$.

Zur direkten Summe gehören auch die Projektionen $\pi_A : A \oplus B \to A$ und $\pi_B : A \oplus B \to B$, definiert durch $\pi_A(a, b) = a$, $\pi_B(a, b) = b$. Es ist $\ker \pi_B = A'$, $\ker \pi_A = B'$, man hat also $(A \oplus B)/A' \cong B$ und $(A \oplus B)/B' \cong A$ (cf. Satz 17.2).

**Satz 17.4** (Universelle Eigenschaft[25] der direkten Summe (zwei Summanden))**.** *Zu jedem $R$-Modul $M$ und jedem Paar von $R$-Modulhomomorphismen $\alpha : A \to M$, $\beta : B \to M$ existiert genau ein $R$-Modulhomomorphismus $\varphi : A \oplus B \to M$ mit $\varphi \circ \iota_A = \alpha$ und $\varphi \circ \iota_B = \beta$.*




*Beweis.* Man definiert $\varphi(a, b) := \alpha(a) + \beta(b)$, das ist ein $R$-Modulhomomorphismus, damit hat man die Behauptung. □

**Bemerkung.** Eine direkte Summe kann man sich wie folgt als Diagramm vorstellen:

$$A \underset{\iota_A}{\overset{\pi_A}{\rightleftarrows}} A \oplus B \underset{\iota_B}{\overset{\pi_B}{\rightleftarrows}} B$$

mit $\pi_A \circ \iota_A = 1_A$, $\pi_B \circ \iota_B = 1_B$ und $\iota_A \circ \pi_A + \iota_B \circ \pi_B = 1_{A \oplus B}$.

**Definition.** Der $R$-Modul $C$ heisst (interne) *direkte Summe* der beiden Untermoduln $A$ und $B$, wenn es einen Isomorphismus $\varphi : A \oplus B \to C$ von $R$-Moduln gibt, so dass $\varphi$ den Untermodul $A'$ von $A \oplus B$ isomorph auf den Untermodul $A$ von $C$ abbildet und den UModul $B'$ von $A \oplus B$ isomorph auf den UModul $B$ von $C$.

[25]Zum Begriff "universelle Eigenschaft": die universelle Eigenschaft gibt die Existenz eines "kleinsten" Objektes in der jeweiligen Situation an. Dazu gibt es einige Erläuterungen auf Wikipedia, [W4].

**Satz 17.5.** *Der $R$-Modul $C$ ist interne direkte Summe der beiden UModuln $A$ und $B \iff$ es gelten (i) $C = A + B$ und (ii) $A \cap B = \{0\}$.*

*Beweis.* Ist $C$ die interne direkte Summe der beiden Untermoduln $A$ und $B$, so sind (i) und (ii) offensichtlich erfüllt.

Es seien umgekehrt zwei Untermoduln $A$ und $B$ von $C$ gegeben, die (i) und (ii) erfüllen. Die Einbettungen $\alpha : A \to C$ und $\beta : B \to C$ ergeben mit der universellen Eigenschaft der direkten Summe einen $R$-Modulhomomorphismus $\varphi : A \oplus B \to C$, der durch $\varphi(a, b) = a + b$ definiert ist. Seine Einschränkungen auf $A'$ bzw. auf $B'$ induzieren Isomorphismen auf $A$ bzw. auf $B$. Es bleibt daher zu zeigen, dass $\varphi$ ein Isomorphismus ist.
Wegen (i) ist $\varphi$ surjektiv.
Zur Injektivität betrachten wir $\ker\varphi$: Sei $\varphi(a, b) = a + b = 0$ mit $a \in A$ und $b \in B$. Also ist $b = -a \in A$. Nach (ii) impliziert dies $b = 0$ und folglich $a = 0$. Der Homomorphismus $\varphi$ ist also auch injektiv. □

Man sagt, $C$ sei *die Summe* $A + B$ von $A$ und $B$, wenn (i) in Satz 17.5 erfüllt ist, aber (ii) nicht unbedingt. Ist die Summe direkt, so schreiben wir $A \oplus B$, wie im Fall der externen direkten Summe.

**Definition.** Seien $A, B, C$ drei $R$-Moduln, $\alpha : A \to B$ und $\beta : B \to C$ zwei $R$-Modulhomomorphismen. Die Folge

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

heisst *exakt in* $B$, falls $\operatorname{im}\alpha = \ker\beta$ gilt.

**Beispiele.** Die Folge $0 \to A \xrightarrow{\alpha} B$ ist exakt (an der Stelle $A$) $\iff \alpha$ ist injektiv.
Die Folge $B \xrightarrow{\beta} C \longrightarrow 0$ ist exakt (in $C$) $\iff \beta$ ist surjektiv.

**Definition.** Seien $A, B, C$ drei $R$-Moduln, $\alpha : A \to B$ und $\beta : B \to C$ zwei $R$-Modulhomomorphismen. Die Folge

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

heisst *kurz exakt*, wenn sie in $A$, $B$ und in $C$ exakt ist. In diesem Fall ist $\alpha$ injektiv und $\beta$ surjektiv und es gilt $C \cong B/\operatorname{im}\alpha$.

[Vorlesung 23, 13. Januar 2015]

**Satz 17.6.** *Es sei $0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$ eine kurze exakte Folge von $R$-Moduln. Es existiere ein $R$-Modulhomomorphismus $\sigma : C \to B$ mit $\pi\sigma = \mathrm{id}_C$. Dann ist $B$ die direkte Summe von $\ker\pi$ und $\operatorname{im}\sigma$, d.h. $B \cong A \oplus C$.*

Der Homomorphismus $\sigma$ mit $\pi\sigma = \mathrm{id}_C$ wird auch *Rechtsinverses* von $\pi$ genannt. Falls in einer kurzen exakten Folge $0 \to A \to B \xrightarrow{\pi} C \longrightarrow 0$ der $R$-Modulhomomorphismus $\pi$ ein Rechtsinverses besitzt, so ist $B$ von der Form $A \oplus A'$. Man sagt, $A$ *besitze in* $B$ *ein Komplement* (nämlich $A'$) und es ist $A' \cong C$. Oft wird $\iota$ als Einbettung betrachtet, d.h. $A$ wird mit seinem Bild unter $\iota$ identifiziert.

*Beweis von Satz 17.6.* Vorbemerkung: $\sigma$ ist injektiv. Denn wären $c \neq c'$ mit $\sigma(c) = \sigma(c')$, so würde wegen $\pi\sigma = \mathrm{id}_C$ folgen: $c = \pi\sigma(c) = \pi\sigma(c') = c'$.

Es sei $b \in \ker\pi \cap \mathrm{im}\,\sigma$. Wir zeigen, dass dann $b = 0$ gilt. Wegen $b \in \mathrm{im}\,\sigma$ existiert $c \in C$ mit $b = \sigma(c)$. Da $b \in \ker\pi$ ist $0 = \pi(b) = \pi(\sigma(c)) = c$. Also $c = 0$, und da $\sigma$ injektiv ist, ist $b = \sigma(c) = \sigma(0) = 0$.

Es sei nun $b \in B$ beliebig. Wir setzen $a := b - \sigma\pi(b)$. Dann gilt $\pi(a) = \pi(b) - \pi\sigma\pi(b) = \pi(b) - \pi(b) = 0$. Damit ist $a \in \ker\pi$. Wegen $b = (b - \sigma\pi(b)) + \sigma\pi(b) = a + \sigma\pi(b)$ ist $B = \ker\pi + \mathrm{im}\,\sigma$.
Damit ist $B$ tatsächlich direkte Summe der Untermoduln $\ker\pi$ und $\mathrm{im}\,\sigma$. Schliesslich gilt wegen der Exaktheit $\ker\pi = \mathrm{im}\,\iota \cong A$ und wegen $\sigma\pi = \mathrm{id}_C$ ist der Homomorphismus $\sigma$ injektiv, also $\mathrm{im}\,\sigma \cong C$. □

**Satz 17.7.** *Es sei* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} F \longrightarrow 0$ *eine kurze exakte Folge von $R$-Moduln, wobei $F = F(S)$ frei sei. Dann existiert ein $R$-Modulhomomorphismus $\sigma : F \to B$ mit $\beta\sigma = \mathrm{id}_F$. Insbesondere besitzt* $\ker\beta$ *in $B$ ein Komplement, das zu $F$ isomorph ist.*

*Beweis.* Zu $s \in S$ wähle man $b_s \in B$ mit $\pi(b_s) = s$ (das geht, da $\beta$ surjektiv ist). Die Funktion $f : S \to B$, die definiert ist durch $f(s) = b_s$ definiert wegen der universellen Eigenschaft des freien Moduls $F = F(S)$ (Satz 16.1) einen $R$-Modulhomomorphismus $\sigma : F \to B$ mit $\sigma(s) = b_s$. Es bleibt zu zeigen, dass $\pi\sigma = \mathrm{id}_F$ ist. Wegen der Wahl von $b_s$ folgt für $s \in S$: $\pi\sigma(s) = \pi(b_s) = s$. Da die Zusammensetzung $\pi\sigma$ und die Identität auf $F$ auf den Elementen von $S$ übereinstimmen, folgt $\pi\sigma = \mathrm{id}_F$.
Der zweite Teil der Behauptung folgt dann sofort aus Satz 17.6. □

- Im Beweis von Satz 17.7 hängt $\sigma$ von der Wahl der Elemente $b_s$, $s \in S$, ab. Deshalb ist das Komplement von $\ker\pi$ in $B$ nicht eindeutig bestimmt.
- Für $R = \mathbb{Z}$ besitzt nicht jede Projektion ein Rechtsinverses. Zum Beispiel besitzt die kanonische Projektion $\mathbb{Z} \to \mathbb{Z}/n\,\mathbb{Z}$ kein Rechtsinverses.

  $$0 \to n\,\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/n\,\mathbb{Z}$$

  mit $\alpha(m) = m$ und $\beta(m) = m + n\,\mathbb{Z}$. Dann hat $\beta$ kein Rechtsinverses.
- Für $R = k$ ein Körper ist jeder $R$-Modul frei. Zu einer surjektiven linearen Abbildung von VRen gibt es deshalb immer ein Rechtsinverses. Daraus folgt dann, dass jeder Unterraum $U$ eines Vektorraums $V$ ein Komplement $W$ besitzt. Auch in diesem Spezialfall ist das Komplement $W$ nicht eindeutig bestimmt. (Man kann zur Illustration $V = \mathbb{R}^2$ nehmen, die euklidische Ebene. Darin kann man die $x$-Achse als $U$ nehmen. Was sind dann Möglichkeiten für $W$?)

Die Definition der direkten Summe lässt sich auf eine beliebige Familie von $R$-Moduln ausdehnen.

**Definition.** Sei $\{B_i\}_{i\in I}$ eine Familie von $R$-Moduln. Die *direkte Summe* $\oplus_{i\in I}B_i$ ist wie folgt definiert (mit $b_i, b_i' \in B_i$, $\lambda \in R$).

| | |
|---|---|
| Elemente | Familien $(b_i)_{i\in I}$ mit $b_i \in B_i$, nur endlich viele der $b_i$ nicht Null |
| Addition | $(b_i)_i + (b_i')_i := (b_i + b_i')_i$ |
| $R$-Operation | $\lambda(b_i)_i := (\lambda b_i)_i$ |

Für jedes $j \in J$ existiert ein kanonischer injektiver $R$-Modulhomomorphismus $\iota_j : B_j \to \oplus_{i\in I}B_i$, definiert durch

$$\iota_j(b_j) = (b_i)_{i\in I}, \quad \text{wobei } b_i = \begin{cases} b_j & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$$

**Satz 17.8** (Universelle Eigenschaft der direkten Summe (bel. viele Summanden))**.** *Zu jedem $R$-Modul $M$ und jeder Familie $\{\varphi_i\}$ von $R$-Modulhomomorphismen $\varphi_i : B_i \to M$ existiert genau ein $R$-Modulhomomorphismus $\varphi : \oplus_{i\in I}B_i \to M$ mit $\varphi \circ \iota_i = \varphi_i$ für alle $i \in I$.*

*Beweis.* Man definiert

$$\varphi(b_i)_{i\in I} := \sum_{i\in I} \varphi_i(b_i)$$

Und damit hat man die Behauptung.
Diese Formel macht nur Sinn wegen der Endlichkeitsvoraussetzung für die Elemente der direkten Summe. □

**Satz 17.9.** *Es sei $S$ die Familie $\{s_i \mid i \in I\}$. Dann ist der freie $R$-Modul $F(S)$ isomorph zur direkten Summe $\oplus_{i\in I}R_i$ mit $R_i \cong R$ für alle $i \in I$.*

*Beweis.* Man definiert einen $R$-Modulhomomorphismus $\chi : F(S) \to \oplus_{i\in I}R_i$ durch

$$\chi(\sum_{i\in I} \lambda_i s_i) = (\lambda_i)_{i\in I}$$

Offensichtlich ist $\chi$ sowohl injektiv wie auch surjektiv. □

Es sei $\Phi = \{a_i \in A \mid i \in I\}$ eine Familie von Elementen des $R$-Moduls $A$ (dabei ist $I = \emptyset$ erlaubt). Dann bezeichnet man mit $\langle\Phi\rangle$ die Menge der Elemente in $A$, die sich als (endliche) Linearkombination der Familie $\Phi$ mit Koeffizienten in $R$ darstellen lassen:

$$\langle\Phi\rangle := \{\sum_{i\in I} \lambda_i a_i \mid \lambda_i \in R\} \subseteq A$$

Die Menge $\langle\Phi\rangle$ ist ein Untermodul von $A$, der kleinste Untermodul von $A$, der die Familie $\Phi$ enthält. $\langle\Phi\rangle$ heisst der *durch $\Phi$ erzeugte Untermodul von $A$*.

[Vorlesung 24, 16. Januar 2015]

**Definition.** Die Familie $\Phi = \{a_i \in A \mid i \in I\}$ heisst *linear unabhängig*, wenn aus $\sum_{i\in I} \lambda_i a_i = 0$ stets folgt $\lambda_i = 0$ für alle $i \in I$. Sie heisst *maximal linear unabhängig*, wenn für jedes $b \in R$ die Familie $\{b\} \cup \Phi$ linear abhängig ist.

**Satz 17.10** (Satz 3.1 in [St])**.** *In jedem $R$-Modul gibt es mindestens eine maximale linear unabhängige Familie $\Phi_m$.*

Dieser Satz ist analog zum Satz, dass jeder Vektorraum eine Basis besitzt. Der Beweis benutzt das Lemma von Zorn über die Existenz von maximalen Mengen. M.a.W. braucht man das Auswahlaxiom. Da es später nochmals benötigt wird, erscheint das Lemma von Zorn hier.

Zuerst zur Terminologie: Es sei $E$ eine Menge, und $\mathcal{M}$ eine Menge von Teilmengen von $E$. Eine *Kette $\mathcal{K}$ von Mengen in $\mathcal{M}$* ist eine Teilmenge von $\mathcal{M}$ mit der Eigenschaft, dass für je zwei Elemente $\Phi$, $\Phi'$ von $\mathcal{K}$ gilt: $\Phi \subseteq \Phi'$ oder $\Phi' \subseteq \Phi$. Eine Menge $\Phi_m \in \mathcal{M}$ heisst *maximal*, wenn aus $\Phi_m \subseteq \Psi \subseteq E$ mit $\Psi \in \mathcal{M}$ immer folgt, dass $\Psi = \Phi_m$ gilt.

**Lemma 17.11.** *Es sei $\mathcal{M}$ eine nicht leere Menge von Teilmengen der Menge $E$. Es gelte, dass mit jeder nicht leeren Kette $\mathcal{K}$ von Mengen in $\mathcal{M}$ die Vereinigung $\bigcup_{\Phi\in\mathcal{K}} \Phi$ in $\mathcal{M}$ ist. Dann existiert in $\mathcal{M}$ eine maximale Menge $\Phi_m$.*

(Hier ohne Beweis).

Nun einige Eigenschaften von linear unabhängigen Familien und Moduln, die sie erzeugen:

**Bemerkung 17.12.**

(1) Ist $A$ ein $R$-Modul, für den jede maximale Familie $\Phi_m$ leer ist. Dann gibt es zu jedem $a \in A$ ein $\lambda \in R \setminus \{0\}$ mit $\lambda a = 0$. Man nennt einen solchen Modul $A$ einen *Torsionsmodul*. Beispiele?

(2) Ist $A = F(S)$ ein freier $R$-Modul, so ist $S$ eine maximale linear unabhängige Menge in $A$.

(3) Es sei $A$ ein $R$-Modul, der durch die (maximale) Familie $\Phi_m = \{a_i \in A\}$ erzeugt wird, $A = \langle \Phi_m \rangle$. Dann lässt sich jedes $a \in A$ *eindeutig* als $\sum \lambda_i a_i$ darstellen (Eindeutigkeit wegen der linearen Unabhängigkeit).

(4) Ist $A = \langle \Phi_m \rangle$, so gilt $A \cong F(\Phi_m)$. (Das ist Satz 3.2 in [St]:
Man bettet $\Phi_m = \{a_i \mid i \in I\}$ in $A$ ein, $f : \Phi_m \to A$, $F(\Phi_m) \ni a_i \mapsto a_i \in A$. Die universelle Eigenschaft des freien Moduls $F(\Phi_m)$ liefert dann einen $R$-Modulhomomorphismus $\psi : F(\Phi_m) \to A$, der durch $\varphi(\sum_{i\in I} \lambda_i a_i) = \sum_{i\in I} \lambda_i f(a_i) = \sum_{i\in I} \lambda_i a_i$. Die Summe links ist die formale Summe im freien Modul $F(\Phi_m)$, in der Mitte und rechts wird die Summe in $A$ gebildet. $\psi$ ist surjektiv, da $\Phi_m$ den Modul $A$ erzeugt, $\psi$ ist injektiv, da $\Phi_m$ linear unabhängig ist.

(5) Ist $\Phi_m$ maximale linear unabhängige Familie in $A$, so ist der Untermodul $\langle \Phi_m \rangle$ von $A$ isomorph zum freien Modul $F(\Phi_m)$.
Ein Beispiel dazu: $R = \mathbb{Z}$, $A = (\mathbb{Q}, +)$, die additive Gruppe der rationalen Zahlen. Ist $\frac{r}{s} \in \mathbb{Q} \setminus \{0\}$, so ist die Familie $\{\frac{r}{s}\}$ eine maximale linear unabhängige Familie in $A$. Für jedes $\Phi_m$ ist damit $B = \langle \Phi_m \rangle \cong \mathbb{Z}$.

(6) Behauptung: Jeder Modul über einem Schiefkörper ist frei.
Sei $R = D$ ein Schiefkörper, $A$ ein $R$-Modul und $\Phi_m$ eine maximale linear

unabhängige Familie in $A$. Dann ist $\langle \Phi_m \rangle = A$.
Beweis: Es ist für jedes $b \in A$ die Familie $\{b\} \cup \Phi_m$ linear abhängig. Es gibt also eine nichttriviale Darstellung $\lambda b + \sum_{i\in I} \lambda_i a_i = 0$ der Null. Hier ist $\lambda \neq 0$ wegen der linearen Unabhängigkeit von $\Phi_m$ (sonst hätte man eine nichttriviale Darstellung der Null mittels $\Phi_m$). Da $R$ ein Schiefkörper ist, existiert $\lambda^{-1}$ in $R$ und daher hat man:

$$b = \lambda^{-1}\lambda b = -\sum_{i\in I} \lambda^{-1}\lambda_i a_i,$$

d.h. $b \in \langle \Phi_m \rangle$. Also ist $A = \langle \Phi_m \rangle$.

[Vorlesung 25, 20. Januar 2015]

**Definition.** Es sei $\Phi$ eine beliebige Familie von Elementen des $R$-Moduls $A$. Gilt $A = \langle \Phi \rangle$, so heisst $\Phi$ ein *Erzeugendensystem von* $A$. Der Modul $A$ heisst *endlich erzeugbar*, falls $A$ ein endliches Erzeugendensystem besitzt.

**Satz 17.13.** *Jeder $R$-Modul $A$ lässt sich als Quotient eines freien $R$-Moduls $F$ darstellen. Ist $A$ endlich erzeugt, so kann $F$ endlich erzeugt gewählt werden.*

*Beweis.* Sei $\Phi = \{a_i\}_{i\in I}$ ein Erzeugendensystem von $A$. Es sei $F$ der freie $R$-Modul auf der Menge $\Phi$. Die Einbettung $f$ von $\Phi$ in $A$ liefert (wegen der universellen Eigenschaft des freien Moduls $F$) einen $R$-Modulhomomorphismus $\psi : F \to A$ mit

$$\psi(\sum_{i\in I} \lambda_i a_i) = \sum_{i\in I} \lambda_i f(a_i) = \sum_{i\in I} \lambda_i a_i$$

Dabei ist die Summe links die formale Summe in $F$, die Summenbildung in der Mitte und rechts findet in $A$ statt. $\psi$ ist surjektiv, da $\Phi$ den Modul $A$ erzeugt. Damit ist $A$ als Quotient $F/\ker\psi$ darstellbar. Der zweite Teil ist klar. (Satz 17.2 $\square$

## 18. Moduln über Hauptidealbereichen

In diesem Abschnitt werden $R$-Moduln im Fall, dass $R$ ein Hauptidealbereich (oder ein Integritätsbereich) ist. Insbesondere umfasst das den Hauptidealbereich $\mathbb{Z}$.

**Satz 18.1.** *Sei $R$ ein Integritätsbereich, seien $S$ und $T$ endliche Mengen. Die freien $R$-Moduln $F(S)$ und $F(T)$ sind isomorph genau dann, wenn $|S| = |T|$ gilt.*

Eine Folgerung des Satzes 18.1 ist, dass die Zahl $|S|$ durch $F(S)$ eindeutig bestimmt ist. Sie heisst der *Rang vom Modul* $F(S)$.

*Beweis.* Es sei $S = \{s_1, \ldots, s_n\}$ und $T = \{t_1, \ldots, t_m\}$. Ein $R$-Modulhomomorphismus $\varphi : F(S) \to F(T)$ wird eindeutig beschrieben durch Elemente $(a_{jk})_{1\leq j\leq m, 1\leq k\leq n}$ von $R$ mit

$$\varphi(s_k) = \sum_{j=1}^{m} a_{jk} t_j, \;\; k = 1, \ldots, n,$$

Ist $\varphi$ ein Isomorphismus, so existiert eine Abbildung $\psi : F(T) \to F(S)$ mit $\varphi \circ \psi = 1$ und $\psi \circ \varphi = 1$. Dabei wird $\psi$ analog beschrieben durch $(b_{il})_{1 \le i \le n, 1 \le l \le m}$ in $R$ und

$$\psi(t_l) = \sum_{i=1}^{n} b_{il} s_i, \ l = 1, \ldots, m$$

Für die Matrizen $A = (a_{jk})$ und $B = (b_{il})$ heisst das, dass $AB = I_m$ und $BA = I_n$ ist (die Einheitsmatrizen vom Rang $m$ bzw. $n$). Betrachtet man $A$ und $B$ als Matrizen über dem Quotientenkörper $Q(R)$ von $R$, so definieren sie Isomorphismen zwischen zwei Vektorräumen über $Q(R)$ der Dimension $m$ bzw. $n$. Damit muss $m = n$ gelten. □

**Definition.** Es sei $R$ ein Integritätsbereich und $A$ ein $R$-Modul. Der *Torsionsuntermodul* $T(A)$ von $A$ ist definiert durch

$$T(A) = \{a \in A \mid \text{es existiert } 0 \neq \lambda \in R \text{ mit } \lambda a = 0\}$$

Ein Modul $A$ mit $T(A) = 0$ heisst *torsionsfrei*.

(Man überlege sich, dass $T(A)$ tatsächlich ein Untermodul von $A$ ist).

**Beispiele.**
(1) Der Modul $A/T(A)$ ist torsionsfrei: Es sei $\lambda(a + T(A)) = T(A)$ (das Nullelement im Quotientenmodul $A/T(A)$). Dann muss $\lambda a \in T(A)$ sein. Also existiert $0 \neq \mu \in R$ mit $\mu\lambda a = 0$. Da $R$ ein Integritätsbereich ist, ist $\mu\lambda \neq 0$, d.h. $a \in T(A)$.
(2) Ist $F$ ein freier $R$-Modul, so ist $R$ torsionsfrei.

**Satz 18.2.** *Sei $R$ ein Hauptidealbereich, $A$ ein freier $R$-Modul vom Rang $n$ und $B$ ein Untermodul von $A$. Dann ist $B$ ein freier $R$-Modul, und für den Rang $m$ von $B$ gilt $m \le n$.*

*Beweis.* Induktion über $n$. Es sei $n = 1$. Dann ist o.E. $A = R$ und $B$ ist ein Linksideal von $R$. Also existiert ein $\mu \in R$ mit $B = (\mu)$ ($R$ ist H.I.B.). Ist $\mu = 0$, so ist $B = 0$ und $B$ ist frei vom Rang 0. Ist $\mu \neq 0$, so definiert $\lambda \mapsto \lambda\mu$ einen $R$-Modulhomomorphismus $R \to B$. Da $R$ nullteilerfrei ist, ist dies ein Isomorphismus. Damit ist $B$ frei vom Rang 1. In beiden Fällen gilt Rang $B \le$ Rang $A = 1$.

Sei $n \ge 2$ und $\{a_1, \ldots, a_n\}$ sei ein linear unabhängiges Erzeugendensystem von $A$. Jedes Element $a$ von $A$ lässt sich eindeutig schreiben als $\sum \lambda_i a_i$. Wir definieren einen $R$-Modulhomomorphismus $\varphi : A \to R$ durch

$$\varphi(a) = \varphi(\sum \lambda_i a_i) = \lambda_n$$

Durch Einschränkung von $\varphi$ auf $B$ erhalten wir einen $R$-Modulhomomorphismus $\psi = \varphi \mid_B : B \to R$. Das Bild $\operatorname{im} \psi$ ist ein Linksideal von $R$. Also existiert ($R$ ist H.I.B.) ein $\mu \in R$ mit $\operatorname{im} \psi = (\mu)$. Es gibt zwei Fälle:
Ist $\mu = 0$, so ist $B \subseteq \langle a_1, \ldots, a_{n-1} \rangle$ (und letzteres ist ein freier Modul vom Rang $< n$), nach Induktion ist $B$ frei mit Rang $B \le n - 1 <$ Rang $A = n$.
Für $\mu \neq 0$ ist, wie oben, $\operatorname{im} \psi = (\mu) \cong R$. Nach dem Isomorphiesatz ist somit

$B/\ker\psi \cong R$. Da der Quotient frei ist, hat nach Satz 17.7 $\ker\psi$ ein Komplement in $B$ und es gilt $B \cong \ker\psi \oplus R$. Nun ist $\ker\psi \subseteq \langle a_1, \dots, a_{n-1}\rangle$, nach Induktion ist also $\ker\psi$ frei vom Rang $\leq n-1$. Damit ist $B$ frei. Und es ist Rang $B$ = Rang $\ker\psi + 1 \leq (n-1)+1 = n$ =Rang $A$. □

(Im Beweis von Satz 18.2 wäre die Fallunterscheidung nicht nötig. Man bemerkt: $B/\ker\psi$ ist frei vom Rang $\leq 1$ und $\ker\psi \subseteq \langle a_1, \dots, a_{n-1}\rangle$.)

**Bemerkung.** Die Aussage von Satz 18.2 kann auch für nicht endlich erzeugbare Moduln über einem Hauptidealbereich bewiesen werden.

**Satz 18.3.** *Es sei $R$ ein Hauptidealbereich und $A$ ein endlich erzeugter torsionsfreier $R$-Modul. Dann ist $A$ frei von endlichem Rang.*

*Beweis.* Es sei $\{a_1, \dots, a_n\}$ ein Erzeugendensystem von $A$. Es sei, nach eventueller Umnumerierung, $\{a_1, \dots, a_m\}$ eine maximale linear unabhängige Teilmenge. Der Untermodul $B := \langle a_1, \dots, a_m\rangle$ ist dann frei. Wir zeigen, dass $A \cong B$ ist.
Für jedes $m < i \leq n$ ist die Menge $\{a_1, \dots, a_m, a_i\}$ linear abhängig. D.h. man findet $\lambda_1, \dots, \lambda_m, \lambda_i \in R$, so dass

$$\lambda_i a_i + \sum_{j=1}^{m} \lambda_j a_j = 0$$

eine nichttriviale Darstellung der Null ist. Da nach Voraussetzung $\{a_1, \dots, a_m\}$ linear unabhängig ist, ist $\lambda_i \neq 0$. Wir definieren $\lambda := \lambda_{m+1} \cdots \lambda_n$. Da $R$ keine Nullteiler hat, ist $\lambda \neq 0$. Mit diesem Element von $R$ definieren wir einen $R$-Modulhomomorphismus $\varphi : A \to B$. Für $a = \sum_{k=1}^{n} \mu_k a_k$ ist

$$\lambda a = \sum_{j=1}^{m} \lambda\mu_j a_j + \lambda\mu_{m+1}a_{m+1} + \lambda\mu_{m+2}a_{m+2} + \cdots + \lambda\mu_n a_n.$$

Das Element $\lambda$ ist ein Vielfaches von $\lambda_i$ für $i = m+1, \dots, n$. Wegen der Wahl der $\lambda_i$ folgt $\lambda\mu_i a_i \in B$ für $i = m+1, \dots, n$. Damit ist $\lambda a \in B$. Und somit erhält man durch $a \mapsto \varphi(a) := \lambda a$ einen $R$-Modulhomomorphismus $\varphi : A \to B$.

Dieser ist injektiv, denn $\ker\varphi = \{a \in A \mid \lambda a = 0\} \subseteq T(A) = 0$ ($A$ ist torsionsfrei). $A$ ist daher isomorph zu einem Untermodul des freien Moduls $B$, nach Satz 18.2 ist also Rang $A \leq$ Rang $B$. □

**Bemerkung.** Satz 18.3 gilt nicht, wenn $A$ nicht endlich erzeugbar ist, so ist z.B. der $\mathbb{Z}$-Modul $(\mathbb{Q}, +)$ torsionsfrei aber nicht frei.

**Satz 18.4.** *Es sei $R$ ein Hauptidealbereich und $A$ ein endlich erzeugbarer $R$-Modul. Dann ist $A/T(A)$ isomorph zu einem freien Modul $F$ und es gilt $A \cong T(A) \oplus F$.*

*Beweis.* Der Quotient $A/T(A)$ ist torsionsfrei und endlich erzeugbar, also ist $A/T(A)$ nach Satz 18.3 isomorph zu einem freien Modul. Die Projektion $A \to A/T(A)$ besitzt daher ein Rechtsinverses und daraus ergibt sich $A \cong T(A) \oplus F$ (Sätze 17.6 und 17.7). □

## 19. Endl. erzeugbare Torsionsmoduln über HIB

Diese Kapitel fällt aus Zeitmangel weg

Es sei $R$ ein Hauptidealbereich. Im letzten Kapitel wurde gezeigt, dass die Struktur von endlich erzeugbaren $R$-Moduln auf die Struktur von endlich erzeugbaren Torsionsmoduln zurückgeführt werden kann (Sätze 18.3 und 18.4). In diesem Kapitel werden wir nun die letzteren untersuchen.

**Definition.** Es sei $A$ ein $R$-Modul. Jedes Element $a \in A$ liefert einen $R$-Modulhomomorphismus $\varphi : R \to A$ durch die Zuordnung $\lambda \mapsto \varphi(\lambda) = \lambda a$. Der *Annihilator von $a$* ist definiert als die Menge

$$\operatorname{Ann}(a) = \ker \varphi = \{\lambda \in R \mid \lambda a = 0\}.$$

Es gilt $R/\operatorname{Ann}(a) \cong \langle a \rangle$. Da $R$ ein H.I.B. ist, existiert ein bis auf Einheiten eindeutig bestimmtes Element $\mu_a \in R$ mit $\operatorname{Ann}(a) = (\mu_a)$. Man nennt $\mu_a$ minimales Annihilatorelement oder kürzer *Exponent von $a$*.
Es sei nun $T$ ein Torsionsmodul. Wir definieren

$$\operatorname{Ann}(T) := \bigcap_{a \in T} \operatorname{Ann}(a) = \{\lambda \in R \mid \lambda a = 0 \ \forall \ a \in T\}.$$

$\operatorname{Ann}(T)$ ist ein Linksideal von $R$, es existiert also $\varepsilon \in R$ mit $\operatorname{Ann}(T) = (\varepsilon)$. $\varepsilon$ wird minimales Annihilatorelement oder *Exponent von $T$* genannt.

**Lemma 19.1.** *Es sei $T$ ein endlich erzeugbarer Torsionsmodul über dem H.I.B. $R$. Dann ist der Exponent $\varepsilon$ von $T$ nicht Null.*

*Beweis.* Es sei $T = \langle a_1, \ldots, a_n \rangle$. Ist $\mu_{a_i}$ der Exponent von $a_i$, so ist das Produkt $\mu_{a_1} \cdots \mu_{a_n}$ verschieden von Null und ein Element von $\operatorname{Ann}(T) = (\varepsilon)$. Also ist $\varepsilon \neq 0$. □

**Definition.** $T$ sei ein endlich erzeugbarer Torsionsmodul über $R$. Für $\pi \in R$ bezeichnen wir mit $T(\pi)$ den Untermodul von $T$, der aus allen Elementen besteht, die einen Exponenten der Form $\pi^r$, $r \geq 1$, besitzen. Es sei $T_\pi := \ker(\pi : T \to T)$.

Wir nutzen nun aus, dass es im H.I.B. $R$ eindeutige Faktorzerlegungen gibt (H.I.B. sind faktoriell, siehe Abschnitt 5.1). Sei $\varepsilon = \pi_1^{r_1} \pi_2^{r_2} \cdots \pi_l^{r_l}$ die Zerlegung von $\varepsilon$, wobei die $\pi_i$ paarweise nicht assoziierte irreduzible Elemente sind. Dann hat man:

**Satz 19.2.** *Es sei $\varepsilon = \pi_1^{r_1} \cdots \pi_l^{r_l}$ die Faktorzerlegung des Exponenten $\varepsilon$ von $T$. Dann gilt*

$$T \cong T(\pi_1) \oplus T(\pi_2) \oplus \cdots \oplus T(\pi_l).$$

*Beweis.* Für jedes $\pi_i$ gilt $T(\pi_i) = T_{\pi_i^{r_i}}$.
Ist $\varepsilon = \alpha\beta$ mit $\mathrm{ggT}(\alpha, \beta) = 1$, dann existieren $\mu, \nu \in R$ mit $1 = \mu\alpha + \nu\beta$. Für $a \in T$ folgt $a = 1 \cdot a = (\mu\alpha + \nu\beta)a = \mu\alpha a + \nu\beta a$, also $\mu\alpha a \in T_\beta$ und $\nu\beta a \in T_\alpha$. Ausserdem ist $T_\alpha \cap T_\beta = 0$. Damit hat man die Zerlegung von $T$ in eine direkte Summe $T_\alpha \oplus T_\beta$.
Induktion über die Anzahl $l$ der verschiedenen Faktoren in der Zerlegung von $\varepsilon$ liefert schliesslich

$$T \cong T(\pi_1) \oplus T(\pi_2) \oplus \cdots \oplus T(\pi_l).$$

wie gewünscht. □

**Satz 19.3.** *Es sei $\pi \in R$ irreduzibel und $\pi^r$ der Exponent von $T(\pi)$. Dann gilt*

$$T(\pi) \cong R/(\pi^{s_1}) \oplus R/(\pi^{s_2}) \oplus \cdots \oplus R/(\pi^{s_m})$$

*mit $r = s_1 \geq s_2 \geq \ldots \geq s_m \geq 1$.*

*Beweis.* Wir geben hier eine Übersicht über den Beweis (siehe Satz 5.3 in [St]).

- Aus $T$ endlich erzeugt folgt, dass $T(\pi)$ endlich erzeugt ist.
- $T_\pi$ ist ein Modul über $T/(\pi)$.
- $T/(\pi)$ ist ein Körper ($\pi$ ist ja irreduzibel, erzeugt ein maximales Ideal).
- $T_\pi$ ist also ein Vektorraum über $T/(\pi)$ und hat damit eine VR-Dimension.

Der Beweis läuft dann mit Induktion über die Dimension von $T_\pi$ als $T/(\pi)$-VR.

- Sei $x \in T$ ein Element mit Exponent $\pi^r$. Sei $\overline{T} = T/\langle x \rangle$.
- $\overline{T}_\pi$ hat kleiner Dimension als $T_\pi$.
- Man zeigt, dass man eine Basis von $\overline{T}_\pi$ zu einer linear unabhängigen Menge von Elementen aus $T_\pi$ hochheben kann (das ist Lemma 5.4 in [St]).
- Mit dem Lemma 5.4 von [St] findet man die gewünschte Zerlegung.

□

**Satz 19.4.** *Es sei $T$ ein endlich erzeugbarer Torsionsmodul über dem H.I.B. $R$. Dann ist $T$ eine direkte Summe $T \cong A_1 \oplus A_2 \oplus \cdots \oplus A_m$ mit $A_i \cong R/(\mu_i)$ für $i = 1, \ldots, m$, wobei $\mu_{i+1}$ ein Teiler von $\mu_i$ ist für $i = 1, \ldots, m-1$.*

*Beweis.* Es sei $\mu = \pi_1^{r_1}\pi_2^{r_2}\cdots\pi_m^{r_m}$ die Faktorzerlegung des Exponenten $\mu$ von $T$. Nach Satz 19.2 lässt sich $T$ in die direkte Summe der $T(\pi_j)$, $j = 1, \ldots, m$ zerlegen, wobei jedes $T(\pi_j)$ nach Satz 19.3 eine direkte Summe $A_1^j \oplus \cdots A_{m_j}^j$ ist, und die $A_k^j$ von der Gestalt $R/(\pi_j^s)$ sind.
Die Aussage des Satzes ergibt sich dann mit der Beobachtung, dass für $\alpha, \beta \in R$ mit $\mathrm{ggT}(\alpha, \beta) = 1$ der Isomorphismus $R/(\alpha) \oplus R/(\beta) \cong R/(\alpha \cdot \beta)$ gilt. □

**Korollar 19.5.** *Es sei $A$ ein endlich erzeugbarer Modul über dem H.I.B. $R$. Dann ist $A$ isomorph zu einer endlichen direkten Summe von Moduln der Form $R/(\mu)$. Die direkte Summe der $R/(\mu)$ mit $\mu = 0$ ist isomorph zu $A/T(A)$, die direkte Summe der $R/(\mu)$ mit $\mu \neq 0$ ist isomorph zu $T(A)$.*

**Korollar 19.6** (Hauptsatz für endlich erzeugte abelsche Gruppen)**.** *Sei $A$ eine endlich erzeugbare abelsche Gruppe. Dann ist $A$ isomorph zu einer endlichen direkten Summe von zyklischen Gruppen*

$$A \cong (\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}) \oplus (\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \oplus \cdots \oplus \mathbb{Z}/n_m)$$

*Dabei ist $n_{i+1}$ ein Teiler von $n_i$ für $i = 1, \ldots, m-1$.*

## 20. Einfache Moduln

[Vorlesung 27, 23. Januar 2015]

**Definition.** Ein $R$-Modul $A$, $A \neq 0$, heisst *einfach*, wenn $A$ ausser 0 und $A$ keine weiteren Untermoduln besitzt.

**Beispiele.**
(1) Es sei $R = k$ ein Körper. Der (bis auf Isomorphie) einzige einfache $k$-Modul ist $k$ selbst.
(2) Es sei $R = \mathbb{Z}$. Die einfachen $\mathbb{Z}$-Moduln sind die abelschen Gruppen von Primzahlordnung, d.h. die Gruppen $\mathbb{Z}/p\mathbb{Z}$, $p$ prim (bis auf Isomorphie).
(3) Sei $A$ ein einfacher $R$-Modul. Zu $0 \neq a \in A$ definieren wir $\varphi : R \to A$ durch $\varphi(\lambda) = \lambda a$, $\lambda \in R$. Es ist $\operatorname{im}\varphi \neq 0$, da $\varphi(1) = a$ ist. Also ist $\operatorname{im}\varphi = \langle a \rangle = A$. Nach dem Isomorphiesatz ist also $A \cong R/\ker\varphi$, wobei $\ker\varphi = \{\lambda \in R \mid \lambda a = 0\} = \mathrm{Ann}(a)$ der sogenannte *Annihilator von $a$* ist.

Das dritte Beispiel beweist den folgenden Satz.

**Satz 20.1.** *Es sei $A$ einfach, $a \in A$, $a \neq 0$. Dann ist $A = \langle a \rangle$.*
*Ist $\varphi : R \to A$ durch $\varphi(\lambda) = \lambda a$ definiert, so hat man $A \cong R/\ker\varphi$.*

**Satz 20.2.** *Es sei $K$ ein Linksideal von $R$. Der Quotient $R/K$ ist ein einfacher Modul genau dann, wenn $K$ ein maximales Linksideal ist.*

*Beweis.* Es sei $I$ ein Linksideal mit $K \subseteq I \subseteq R$. Dann hat man $0 = K/K \subseteq I/K \subseteq R/K$. Ist $R/K$ einfach, so folgt $I/K = 0$ oder $I/K = R/K$, d.h. $I = K$ oder $I = R$, $K$ ist also maximal.
Ist umgekehrt $K$ maximal, so folgt $I = K$ oder $I = R$ und der Modul $R/K$ besitzt keine nichttrivialen Untermoduln. □

Analog beweist man den folgenden Satz:

**Satz 20.3.** *Es sei $C$ ein $R$-Modul und $B$ ein echter Untermodul.*
*$C/B$ ist einfach $\iff$ zwischen $B$ und $C$ gibt es keine weitern Untermoduln.*

**Beispiele.**
(1) Es sei $R = \mathbb{Z}$. Eine abelsche Gruppe $A$ ist genau dann einfach, wenn $A$ von der Form $\mathbb{Z}/K$ ist, wobei $K$ ein maximales Ideal ist. Die maximalen Ideale in $\mathbb{Z}$ sind die Ideale, die von einer Primzahl erzeugt werden. D.h. die einfachen $\mathbb{Z}$-Moduln sind die abelschen Gruppen $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$, $p$ prim.
(2) $R$ ist selbst ein $R$-Modul. $R$ ist nach Satz 20.2 genau dann einfach, wenn es in $R$ keine echten Linksideale gibt. (Hier als Anmerkung: ein Ring wird einfach genannt, wenn er keine nichttrivialen zweiseitigen Ideale hat).

**Definition.** Der $R$-Modul $A$ heisst *halbeinfach*, wenn $A$ direkte Summe von einfachen Moduln ist,

$$A = \oplus_{i \in I} B_i, \text{ mit } B_i \text{ einfach für alle } i \in I.$$

**Beispiele.**
(1) Es sei $R$ ein Schiefkörper. Dann ist jeder $R$-Modul halbeinfach. ev: (cf. Bem 17.12 (6))
(2) Es sei $R = \mathbb{Z}$. Es gibt abelsche Gruppen, die nicht halbeinfach sind, etwa $\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}$, etc.

Man sagt, der Untermodul $B$ von $A$ *besitze ein Komplement (in $A$)*, wenn ein Untermodul $C$ in $A$ existiert mit $A \cong B \oplus C$ (siehe Kommentar nach Satz 17.6).

**Satz 20.4.** *Sei $A$ ein $R$-Modul.*
*$A$ ist halbeinfach $\iff$ jeder Untermodul von $A$ besitzt ein Komplement.*

Für den Beweis benötigen wir zwei Lemmata.

**Lemma 20.5.** *Es sei $N$ ein echtes Linksideal von $R$. Dann existiert ein maximales Linksideal $M$ von $R$ mit $N \subseteq M \subset R$.*

*Beweis.* Wir betrachten die Menge $\mathcal{M}$ der Linksideale $N'$ von $R$ mit $N \subseteq N' \subset R$. Da $N \in \mathcal{M}$ ist, ist diese Menge nicht leer. Ausserdem enthält sie mit jeder Kette $\mathcal{K}$ von Idealen auch die Vereinigung $\bigcup_{K \in \mathcal{K}}$: dazu muss man zeigen, dass diese Vereinigung nicht ganz $R$ sein kann.
Wäre $\bigcup_{K \in \mathcal{K}} = R$, so hätte man $1_R \in \bigcup_{K \in \mathcal{K}} K$, es würde ein $K \in \mathcal{K}$ existieren mit $1_R \in K$. Dann wäre $K = R$, im Widerspruch zur Definition von $\mathcal{K}$. Nach dem Lemma von Zorn (Lemma 17.11) existiert in $\mathcal{M}$ ein maximales Element $M$ und dies ist das gesuchte maximale Linksideal. □

**Lemma 20.6.** *Es sei $A$ ein $R$-Modul, in dem jeder Untermodul ein Komplement besitzt. Dann gilt:*
*(i) Es seien $B$, $D$ Untermoduln mit $B \subseteq D$. Dann besitzt $B$ in $D$ ein Komplement.*
*(ii) Jeder Untermodul $D$, $D \neq 0$, enthält einen einfachen Untermodul $E$.*

*Beweis.* (i) Es sei $C$ ein Komplement von $B$ in $A$. Dann ist $C \cap D$ ein Untermodul von $D$, der das gesuchte Komplement liefert.
(ii) Es sei $0 \neq d \in D$. Die Abbildung $\varphi : R \to D$, $\lambda \mapsto \varphi(\lambda) = \lambda d$ liefert einen Isomorphismus $R/N \cong \langle d \rangle \subseteq D$ für $N = \ker \varphi$. Es sei $M$ ein maximales Ideal von $R$ mit $N \subseteq M$. Dann ist $M/N$ ein Untermodul von $R/N$. Nach (i) hat $M/N$ in $R/N$ ein Komplement $E$, also $R/N = M/N \oplus E$. Da $E \cong R/M$ ist mit $M$ maximal ist $E$ einfach. Damit ist ein einfacher Untermodul $E$ von $D$ gefunden. □

*Beweis von Satz 20.4.* Es sei zuerst $A$ halbeinfach, $A = \oplus_{i \in I} B_i$ mit $B_i$ einfach. Es sei $B$ ein Untermodul von $A$. Wir betrachten die Teilmengen $I'$ der Indexmenge $I$ mit

$$B \cap \sum_{i \in I'} B_i = 0$$

Beh.: die Menge $\mathcal{M}$ der Mengen $I'$ erfüllt die Voraussetzungen des Lemmas 17.11 von Zorn.
$\mathcal{M}$ ist nicht leer, denn die leere Teilmenge von $I$ liegt drin. Es sei $\mathcal{K}$ eine beliebige Kette in $\mathcal{M}$. Wir müssen zeigen, dass $\bigcup_{K \in \mathcal{K}} K$ eine Menge in $\mathcal{M}$ ist. Dazu betrachten wir

$$a \in B \cap \sum_{i \in \cup_{K \in \mathcal{K}} K} B_i.$$

Damit lässt sich $a$ als *endliche!* Summe $b_{i_1} + b_{i_2} + \cdots + b_{i_l}$ mit $b_{i_k} \in B_{i_k}$ schreiben. Da $\mathcal{K}$ eine Kette ist, existiert ein $K \in \mathcal{K}$ mit $i_1, \ldots, i_l \in K$. Damit folgt aber $a = 0$. Nach dem Lemma von Zorn existiert also in $\mathcal{M}$ eine maximale Menge $J$ mit

$$B \cap \sum_{i \in J} B_i = 0$$

Es sei $C := \sum_{j \in J} B_j$. Dies ist ein Komplement von $B$ in $A$: Nach Konstruktion ist $C \cap B = 0$. Wir müssen noch zeigen, dass $A = B + C$ gilt. Dazu genügt es, zu zeigen, dass für jedes beliebige $j \in J$ gilt: $B_j \subseteq B + C$. Für $j \in J$ ist dies klar (Definition von $C$). Es sei also $j \notin J$. Dann ist wegen der Maximalität von $J$

$$B \cap (C + B_j) \neq 0$$

Es existiert also $0 \neq b = c + b_j$ mit $b \in B$, $c \in C$, $b_j \in B_j$. Wäre $b_j = 0$, so wäre $c \neq 0$ und $c \in B \cap C$, d.h. $B \cap C \neq 0$. Daher ist $0 \neq b_j = b - c$, also $0 \neq b_j \in B + C$. Da $B_j$ einfach ist, folgt $B_j \subseteq B + C$ wie gewünscht.
Es gilt also $A = B \oplus C$.

[Vorlesung 28, 27. Januar 2015]

Es besitze nun umgekehrt jeder Untermodul von $A$ ein Komplement. Wir betrachten die Menge aller einfachen Untermodul $B_i$, $i \in I$ von $A$. Es sei $\mathcal{M}$ die Menge der Teilmengen $I'$ von $I$, so dass die Summe $\sum_{i\in I'} B_i$ direkt ist.
Beh.: $\mathcal{M}$ erfüllt die Voraussetzungen des Lemmas von Zorn.
$\mathcal{M}$ ist nicht leer, denn die leere Teilmenge von $I$ liegt in $\mathcal{M}$.
Es sei $\mathcal{K}$ eine Kette in $\mathcal{M}$. Dann ist auch $\bigcup_{K\in\mathcal{K}} K$ in $\mathcal{M}$. (Hier ohne Beweis).
Nach dem Lemma von Zorn existiert also eine maximale Menge $J \in \mathcal{M}$. Behauptung:

$$A = \oplus_{i\in J} B_i$$

Die Summe ist laut Konstruktion direkt. Es ist also $A = \sum_{i\in J} B_i$ zu zeigen. Wäre $\sum_{j\in J} B_j$ ein echter Untermodul von $A$, so hätte er nach Voraussetzung ein Komplement $C$ in $A$. Es sei nun $\widetilde{B}$ ein einfacher Untermodul von $C$ ($\widetilde{B}$ existiert nach Lemma 20.6). Da $C$ ein Komplement zu $\sum_{i\in J} B_i$ ist, ist jedoch die Summe $\widetilde{B} + \sum_{i\in J} B_i$ direkt, ein Widerspruch zur Maximalität von $J$. □

Der letzte Satz in diesem Abschnitt (hier ohne Beweis) sagt, dass die (einfachen) Summanden eines halbeinfachen Moduls bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind. Für endliche Indexmengen folgt der Beweis aus dem Satz von Jordan-Hölder über Kompositionsfaktoren (cf. Korollare 7.3 und 7.4 in [St] oder Theorem 4.12 in [Ba]).

**Satz 20.7** (Satz von Krull-(Remak-)Schmidt)**.** *Es sei $M$ halbeinfach und es seien $M = \oplus_{i\in I} M_i = \oplus_{j\in J} N_j$ zwei Darstellungen von $M$ als direkte Summe von einfachen Moduln. Dann sind die Zerlegungen äquivalent (d.h. es gibt eine Bijektion $f : I \to J$ mit $M_i \cong N_{f(i)}$).*

## Literatur

[Ar] Michael Artin, *Algebra*, Birkhäuser, 1993
[Ba] Michael Barot, *Introduction to the representation theory of algebras*, erhältlich unter http://www.uni-graz.at/∼baurk/lehre/Vorlesung-ws11.html
[Co] David A. Cox, *Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First*, The American Mathematical Monthly, January 2011, http://www.maa.org/pubs/monthly_jan11_toc.html
siehe auch http://www.cs.amherst.edu/∼dac/normat.pdf
[Hu] Thomas Hungerford, *Abstract Algebra. An introduction*, 1997
[Ja] N. Jacobson, *Basic Algebra I*, 2nd edition, and *Basic Algebra II*, 2nd edition. San Francisco: Freeman, 1985 and 1989.
[JS] J.C. Jantzen, J. Schwermer, *Algebra*, Springer, 2005.
[Ni] I. Niven, *Irrational Numbers*, Carus Monograph 11, 1956
[Le] G. Lettl, *Literaturliste zur Algebra 1*,
http://www.uni-graz.at/∼lettl/lehre/algebra1lit-s11.html
[St] Urs Stammbach, *Algebra*, ETH, 2009
[W1] http://en.wikipedia.org/wiki/Transcendental_number# Sketch_of_a_proof_that_e_is_transcendental, aufgerufen im Juni 2013
[W2] http://de.wikipedia.org/wiki/Eisensteinkriterium, aufgerufen im Mai 2013
[W3] http://de.wikipedia.org/wiki/Körpererweiterung, aufgerufen im Juni 2013
[W4] http://de.wikipedia.org/wiki/UniverselleEigenschaft, aufgerufen im Januar 2015

[EA] Stoff der Vorlesung Einführung in die Algebra.