Algebra
Vorlesung im Wintersemester 2015/2016

Prof. Dr. G. Nebe, Lehrstuhl D für Mathematik, RWTH Aachen

Inhaltsverzeichnis

1 Elementare Körpertheorie. 3
1.1 Preludium: Mengenlehre. . . . 3
1.1.1 Grundlegende Axiome der Mengenlehre . . . 3
1.1.2 Das Zorn'sche Lemma und das Auswahlaxiom . . . 4
1.1.3 Beweis des Hauptsatzes. . . . 6
1.2 Primkörper, Körpererweiterungen und Gradsatz . . . 8
1.3 Transzendente Erweiterungen. . . . 11
1.4 Zerfällungskörper. . . . 12
1.5 Der algebraische Abschluss. . . . 14
1.6 Endliche Körper. . . . 16
1.7 Separable Erweiterungen . . . 17
1.8 Normale Erweiterungen . . . 19

2 Intermezzo: Gruppentheorie. 21
2.1 Wiederholung: Normalteiler und Homomorphiesatz. . . . 21
2.2 Der Noethersche Isomorphiesatz und semidirekte Produkte. . . . 23
2.3 Untergruppenverbände. . . . 24
2.4 Kompositionsreihen und der Satz von Jordan-Hölder. . . . 29
2.5 Auflösbare Gruppen. . . . 33
2.6 Der Satz von Schur-Zassenhaus. . . . 36

3 Galoistheorie. 39
3.1 Galoiserweiterungen . . . 39
3.2 Kreisteilungskörper . . . 44
3.3 Norm und Spur . . . 47
3.4 Zyklische Körpererweiterungen. . . . 48
3.5 Auflösbarkeit von Gleichungen . . . 50
3.6 Konstruktionen mit Zirkel und Lineal. . . . 51
3.7 Ganze Zahlen und die Diskriminante . . . 53

4 Ringe und Moduln. 57
4.1 Einfache Moduln und der Satz von Jordan Hölder . . . 57
4.2 Halbeinfache Ringe und Moduln . . . 60
4.3 Noethersche und Artinsche Ringe . . . 62
4.4 Das Jacobson-Radikal eines Rings . . . 64
4.5 Der Satz von Krull-Schmidt . . . 67
4.6 Idempotente . . . 70
4.6.1 Liften von Idempotenten. . . . 72
4.7 Projektive und injektive Moduln . . . 72
4.7.1 Projektive Moduln . . . 72
4.7.2 Injektive Moduln. . . . 74

5 Einfache und halbeinfache Algebren 77
5.1 Einfache Algebren . . . 78
5.1.1 Der Doppelzentralisatorsatz . . . 78
5.1.2 Zentral einfache Algebren. . . . 79
5.1.3 Die Brauergruppe von K . . . 81
5.2 Separable Algebren. . . . 84
5.2.1 Reduzierte Norm und Spur. . . . 84
5.2.2 Assoziative Bilinearformen und das Casimirelement. . . . 85
5.2.3 Ordnungen in separablen Algebren. . . . 86
5.3 Gruppenalgebren. . . . 88
5.3.1 Die Orthogononalitätsrelationen . . . 93
5.3.2 Eine Anwendung: Der $p^a q^b$ Satz von Burnside . . . 94
5.3.3 Die Frobenius Reziprozität . . . 95

Kapitel 1

Elementare Körpertheorie.

1.1 Preludium: Mengenlehre.

Literatur: Halmos, Naive Mengenlehre.

1.1.1 Grundlegende Axiome der Mengenlehre

Elementbeziehung. Ist A eine Menge, so schreiben wir $x \in A$ wenn x ein Element von A ist, ansonsten $x \notin A$.

(Unsere Vorstellung, dass x in A liegt, wenn $x \in A$ gilt, ist nicht Teil der Definition.)

Gleichheit. (Extensionalitätsaxiom) Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.

(Dass dies eine Forderung ist, veranschauliche man sich z.B. indem man alle Menschen betrachtet und $x \in A$ schreibt, wenn x ein Vorfahr von A ist. Sind die beiden Menschen gleich $A = B$, so haben sie dieselben Vorfahren ($x \in A \Leftrightarrow x \in B$), die Umkehrung gilt jedoch z.B. bei Geschwistern i.a. nicht.)

Aussonderungsaxiom. Ist A eine Menge und B eine Bedingung an die Elemente der Menge A, so ist auch $\{x \in A \mid B(x)\}$ eine Menge.

Existenzaxiom. Es gibt eine Menge.

Dann gibt es auch die **leere Menge**, $\emptyset = \{x \in A \mid x \neq x\}$, die kein Element enthält. Sie ist Teilmenge jeder anderen Menge.

Paarbildungsaxiom. Sind A, B Mengen so gibt es eine Menge M mit $A \in M$ und $B \in M$.

Mit Hilfe dieses Axioms haben wir aus der leeren Menge alle natürlichen Zahlen konstruiert. $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$ und im allgemeinen $n + 1 = \{\emptyset, n\}$.

Vereinigungsaxiom. Zu jeder Menge von Mengen $\mathcal{M}$ gibt es eine Menge X, die alle Elemente enthält, die zu mindestens einer Menge von $\mathcal{M}$ gehören.

Daraus kann man die Vereinigungsmenge bilden, als die Menge all der Elemente von X, die in einem $M \in \mathcal{M}$ liegen, indem man das Aussonderungsaxiom anwendet. Zur Bildung des **Durchschnitts** $A \cap B$ (auch für beliebige Mengensysteme) benötigt man kein weiteres Axiom, dies geht mit dem Aussonderungsaxiom alleine, ebenso bei **Komplementen** $A \setminus B = \{x \in A \mid x \notin B\}$.

Potenzmengenaxiom. Zu jeder Menge M existiert eine Menge X, die alle Teilmengen von M als Elemente enthält.

Damit definiert man dann wieder die **Potenzmenge** von M

$$\mathrm{Pot}(M) := \{x \in X \mid x \subseteq M\}.$$

Mit diesen Axiomensystem haben wir in den Grundlagen gearbeitet ohne diese Axiome als solche zu bezeichnen. Sie sind anschaulich. Wir konnten mit ihnen kartesische Produkte, Relationen und Funktionen definieren. Ein weiterer Begriff ist der der **Familie** von Mengen. Ist Λ eine Menge und $f : \Lambda \to \mathcal{X}$ eine Funktion, die jedem $\lambda \in \Lambda$ eine Menge $f(\lambda) = X_\lambda \in \mathcal{X}$ zuordnet, so heißt der Wertebereich von f auch **Familie** von Mengen $(X_\lambda \mid \lambda \in \Lambda)$. Eine ausführlichere Darstellung finden Sie in dem (für Sie jetzt) schön zu lesenden Büchlein, "Naive Mengenlehre".

1.1.2 Das Zorn'sche Lemma und das Auswahlaxiom

Definition 1.1.

- *Ein* **Ordnung** *auf einer Menge M ist eine Relation $\leq$ auf M mit*
  (i) $a \leq a$ für alle $a \in M$. (reflexiv)
  (ii) $a \leq b$ und $b \leq a \Rightarrow a = b$. (antisymmetrisch)
  (iii) $a \leq b$ und $b \leq c \Rightarrow a \leq c$. (transitiv)

- *Eine geordnete Menge $(M, \leq)$ heißt* **vollständig geordnet**, *wenn für alle $a, b \in M$ entweder $a \leq b$ oder $b \leq a$ gilt.*

- *Eine geordnete Menge $(M, \leq)$ heißt* **wohlgeordnet**, *wenn jede nichtleere Teilmenge von M ein kleinstes Element enthält. ($\emptyset \neq N \subset M \Rightarrow \exists\, n \in N$, so dass $n \leq x$ für alle $x \in N$.)*

- *$(M, \leq)$ heißt* **induktiv geordnet**, *wenn jede vollständig geordnete Teilmenge $N \subset M$ eine* **obere Schranke** *in M besitzt, es also $x \in M$ gibt mit $n \leq x$ für alle $n \in N$.*

- *Ein* **maximales Element** *von M ist ein $m \in M$ mit $m \leq x \Rightarrow x = m$ für alle $x \in M$.*

- *Eine Teilmenge S von $(M, \leq)$ heißt* **Segment**, *falls für jedes $m \in M$ gilt: $\exists s \in S$ mit $m \leq s \Rightarrow m \in S$.*

Beispiele.
$(\mathbb{N}, \leq)$ ist vollständig geordnet und wohlgeordnet, jedoch nicht induktiv geordnet.
$(\mathbb{R}_{>0}, \leq)$ ist vollständig geordnet, jedoch nicht wohlgeordnet.
$(0, 1]$ ist vollständig geordnet und induktiv geordnet, jedoch nicht wohlgeordnet.
Sei M eine Menge und $\mathrm{Pot}(M) := \{N \subset M\}$ die Potenzmenge von M. Dann ist $\mathrm{Pot}(M)$ durch die Relation $X \leq Y \Leftrightarrow X \subseteq Y$ eine geordnete Menge. Hat M mehr als ein Element, so ist sie nicht vollständig geordnet.

Bemerkung 1.2. *Sei $(M, \leq)$ eine geordnete Menge.*

- *Ist M wohlgeordnet, so ist sie vollständig geordnet. (Die Menge $\{a, b\} \subset M$ hat ein kleinstes Element.)*

- *Für $x \in M$ ist*
$$M_{<x} := S(M, <, x) := \{m \in M \mid m < x\}$$
ein Segment.

- *Ist M vollständig geordnet und $S \subset M$ ein Segment, so gilt $S \subset M_{<x}$ für jedes $x \in M \backslash S$.*

Hauptsatz 1.3. *Folgende Aussagen sind äquivalent.*

(A) (Auswahlaxiom) Sei $\Lambda \neq \emptyset$ und für jedes $\lambda \in \Lambda$ eine nichtleere Menge X_λ gegeben. Dann ist das kartesische Produkt
$$\prod_{\lambda \in \Lambda} X_\lambda = \{(x_\lambda)_{\lambda \in \Lambda} \mid x_\lambda \in X_\lambda\}$$
nicht leer.
(Man kann also simultan für jedes $\lambda \in \Lambda$ ein $x_\lambda \in X_\lambda$ auswählen.)

(Z) (Lemma von Zorn) Sei $(M, \leq)$ eine nicht leere geordnete Menge. Ist $(M, \leq)$ induktiv geordnet, so besitzt $(M, \leq)$ maximale Elemente.
(Hat also jede Kette in M eine obere Schranke in M, so gibt es ein $x \in M$ mit $m \geq x \Rightarrow m = x$ für jedes $m \in M$.)

(W) (Wohlordnungssatz) Jede Menge M besitzt eine Ordnung, bezüglich der sie wohlgeordnet ist.

(A), (Z), (W) sind also äquivalente Axiome, sie folgen nicht aus den Grundaxiomen der Mengenlehre, man muss eines (und wegen der Äquivalenz somit alle) von ihnen zusätzlich fordern.

Bevor wir zum Beweis kommen wollen wir erstmal exemplarisch zwei wichtige Anwendungen zeigen.

Satz 1.4. *Jeder Vektorraum besitzt eine Basis.*

Beweis. Sei V ein Vektorraum und $\mathcal{B} := \{B \subset V \mid B \text{ linear unabhängig }\}$. Dann ist $\mathcal{B}$ geordnet durch $B_1 \leq B_2 \Leftrightarrow B_1 \subset B_2$. Ist nun $\mathcal{K} \subset \mathcal{B}$ eine Kette, also eine total geordnete Menge, so ist die Vereinigung
$$K := \bigcup_{B \in \mathcal{K}} B$$
eine linear unabhängige Teilmenge von V (beachten Sie, l.u. heißt dass jede endliche Linearkombination der 0 trivial ist) und somit ein Element von $\mathcal{B}$. Nach dem Zorn'schen Lemma hat also $\mathcal{B}$ maximale Elemente, also maximal linear unabhängige Teilmengen $X \subset V$. Jedes solche X ist ein Erzeugendensystem, denn für $v \in V \setminus \langle X \rangle$ ist $X \cup \{v\}$ linear unabhängig. □

Beachten Sie, dass man nicht unbedingt eine Basis von V angeben kann. Ist z.B. $V = K[x]$, so ist $(1, x, x^2, \ldots)$ eine unendliche Basis von V. Jedoch für $V = K[[x]]$, $V = \mathbb{R}^{[0,1]}$ oder $V = \{f : [0,1] \to \mathbb{R} \mid f \text{ stetig }\}$ kann man keine solche Basis angeben, glaubt man an das Auswahlaxiom, was durchaus sinnvoll erscheint, so gibt es aber eine Basis.

Eine weitere Anwendung ist

Satz 1.5. *Sei R ein Ring. Dann liegt jedes echte Ideal von R in einem maximalen Ideal.*

Beachte: Ein Ideal $I \trianglelefteq R$ heißt **maximales Ideal**, wenn $I \neq R$ und $I \subseteq M \trianglelefteq R$ impliziert $M = I$ oder $M = R$. Äquivalent dazu R/I ist ein Körper. Beweis. Sei $I \trianglelefteq R$ ein Ideal. Betrachte die durch Inklusion geordnete Menge $M(I)$ aller Ideale $R \neq J \trianglelefteq R$, die I enhalten. Diese Menge ist wieder induktiv geordnet, denn für jede total geordnete Menge von Idealen ist ihre Vereinigung wieder ein Ideal. (Beweis an Tafel). Nach dem Lemma von Zorn hat $M(I)$ also maximale Elemente. Jedes maximale Element von $M(I)$ ist aber ein maximales Ideal von R, das I enthält. □

1.1.3 Beweis des Hauptsatzes.

Dazu 2 Lemmata.

Lemma 1.6. *Sei $(X_\lambda \mid \lambda \in \Lambda)$ eine Familie von Teilmengen einer Menge M und für jedes $\lambda \in \Lambda$ sei $\leq_\lambda$ eine Wohlordnung auf X_λ so dass für $X_\mu \subseteq X_\lambda$ gilt:*

X_μ ist ein Segment in X_λ und die Ordnung $\leq_\mu$ ist die Einschränkung von $\leq_\lambda$ auf X_μ.

Falls für je zwei $\lambda, \mu \in \Lambda$ stets gilt $X_\mu \subseteq X_\lambda$ oder $X_\lambda \subseteq X_\mu$ so induzieren die Ordnungen $(\leq_\lambda | \ \lambda \in \Lambda)$ eine Wohlordnung auf $X := \cup_{\lambda \in \Lambda} X_\lambda$.

Beweis. Sind $x, y \in X$, so gibt es $\lambda, \mu \in \Lambda$ mit $x \in X_\lambda$, $y \in X_\mu$. Nun gilt entweder $X_\mu \subseteq X_\lambda$ oder $X_\lambda \subseteq X_\mu$ also nehmen wir an, dass $x, y \in X_\mu$. Dann erklärt man $x \leq y$ genau dann wenn $x \leq_\mu y$. Dies definiert eine Ordnung auf X deren Einschränkung auf jedes X_λ gleich $\leq_\lambda$ ist. Dies ist eine Wohlordnung auf X, denn sei $\emptyset \neq A \subseteq X$. Dann gibt es ein $\lambda \in \Lambda$ mit $A \cap X_\lambda \neq \emptyset$. Sei $a \in A \cap X_\lambda$ ein kleinstes Element.
Behauptung. a ist auch ein kleinstes Element von A.
Denn sei $x \in A$. Ist $x \in X_\lambda$ so gilt $a \leq x$ nach Konstruktion. Ansonsten ist $x \in X_\mu$ mit $\mu \neq \lambda$. Da $x \notin X_\lambda$ gilt nicht $X_\mu \subseteq X_\lambda$ und also nach Voraussetzung $X_\lambda \subseteq X_\mu$ und X_λ ein Segment in X_μ. Dann ist aber $a \leq x$ nach Bemerkung 1.2. □

Lemma 1.7. *(Fundamentallemma von Bourbaki) Sei $\emptyset \in \mathcal{T} \subseteq \mathrm{Pot}(M)$ und $p : \mathcal{T} \to M$ eine Abbildung mit $p(T) \notin T$ für alle $T \in \mathcal{T}$. Dann gibt es eine Teilmenge $X \subseteq M$ und eine Wohlordnung $\leq$ auf X, so dass gilt:*
1) Für jedes $x \in X$ ist $X_{<x} \in \mathcal{T}$ und $p(X_{<x}) = x$.
2) $X \notin \mathcal{T}$.

Beweis. Sei $\mathcal{F} = (X_\lambda, \leq_\lambda)$ die Familie aller geordneten Mengen mit

a) $X_\lambda \in \mathcal{T}$

b) $(X_\lambda, \leq_\lambda)$ wohlgeordnet,

c) Für alle $x \in X_\lambda$ liegt $S(X_\lambda, <_\lambda, x) \in \mathcal{T}$ und $p(S(X_\lambda, <_\lambda, x)) = x$.

Dann erfüllt $\mathcal{F}$ die Voraussetzungen von Lemma 1.6:
Denn für $\lambda, \mu \in \Lambda$ sei

$$V := \{x \in X_\lambda \cap X_\mu \mid (S(X_\lambda, <_\lambda, x), \leq_\lambda) = (S(X_\mu, <_\mu, x), \leq_\mu)\}.$$

Dann ist V ein Segment von X_λ und auch von X_μ. (leichte Übung.)
Wir zeigen jetzt, dass $V = X_\lambda$ oder $V = X_\mu$ gilt:
Sonst gäbe es ein kleinste Elemente $x_\lambda \in X_\lambda \setminus V$, $x_\mu \in X_\mu \setminus V$. Dann ist $V = S(X_\mu, <_\mu, x_\mu) = S(X_\lambda, <_\lambda, x_\lambda)$ und wegen c) daher

$$x_\mu = p(V) = x_\lambda \in X_\lambda \cap X_\mu$$

und somit $x_\mu = x_\lambda \in V$ ein Widerspruch.
Setze nun $X := \cup_{X_\lambda \in \mathcal{F}} X_\lambda$ und $\leq_X$ die von $\leq_\lambda$, $\lambda \in \Lambda$ nach Lemma 1.6 induzierte Wohlordnung auf X. Für jedes $x \in X$ gibt es ein $\lambda \in \Lambda$ mit $x \in X_\lambda$ und dann ist

$$S(X, <_X, x) = S(X_\lambda, <_\lambda, x) \in \mathcal{T}$$

und somit $p(S(X, <_X, x)) = x$. Die Menge X erfüllt also den Punkt 1. der Behauptung. Gilt $X \notin \mathcal{T}$, so ist X die gesuchte Menge. Ansonsten ist $X \in \mathcal{T}$ und es gilt $p(X) =: x_0 \notin X$. Betrachte die Menge

$$X_0 := X \cup \{x_0\}, x \leq_0 x_0 \text{ für alle } x \in X \text{ und } \leq_0 = \leq_X \text{ auf } X.$$

Dann ist auch $(X_0, \leq_0)$ eine wohlgeordnete Menge und die Segmente von X_0 sind entweder Segmente von X oder gleich $X = S(X_0, <_0, x_0)$. Damit erfüllt auch X_0 die 1. Bedingung der Behauptung. Weiter gilt $X_0 \notin \mathcal{T}$, denn sonst wäre $(X_0, \leq_0) \in \mathcal{F}$ eines der X_λ eine Teilmenge von X. □

Beweis. (vom Hauptsatz 1.3)
(A) $\Rightarrow$ (Z) Sei $(M, \leq)$ eine geordnete Menge und

$$\mathcal{T} := \{T \subseteq M \mid T \text{ besitzt obere Schranke } t' \in M \setminus T\}.$$

Für $T \in \mathcal{T}$ sei $X_T := \{t' \in M \setminus T \mid t' \text{ ist obere Schranke von } T\}$. Nach dem Auswahlaxiom gibt es eine Abbildung

$$p : \mathcal{T} \to M, p(T) \in X_T \text{ für alle } T \in \mathcal{T}.$$

Dann gibt es aber nach Lemma 1.7 eine Teilmenge $X \subset M$ und eine Wohlordnung $\leq_X$ auf X mit folgenden Eigenschaften:
1) Für jedes $x \in X$ ist $S(X, <_X, x) \in \mathcal{T}$ und $p(S(X, <_X, x)) = x$.
2) $X \notin \mathcal{T}$.
Beachte, dass $\leq_X$ noch nichts mit der Ordnung $\leq$ auf M zu tun hat.
Wir zeigen jetzt, dass $(X, \leq)$ vollständig geordnet ist. Seien dazu $x_1, x_2 \in X$. Da $(X, \leq_X)$ wohlgeordnet ist gelte Œ $x_1 \leq_X x_2$, $x_1 \neq x_2$. Dann gilt aber $x_1 \in S(X, <_X, x_2)$. Wegen $S(X, <_X, x_2) \in \mathcal{T}$ ist $p(S(X, <_X, x_2)) = x_2$. Damit ist also x_2 eine obere Schranke von $S(X, <_X, x_2)$ bezüglich $\leq$. Da aber $x_1 \in S(X, <_X, x_2)$ liegt, folgt $x_1 \leq x_2$.
Nach Voraussetzung (Z), hat $(X, \leq)$ eine obere Schranke x_X. Da $X \notin \mathcal{T}$ hat X keine obere

Schranke in $M \setminus X$, also gilt $x_X \in X$ und x_X ist ein maximales Element von $(M, \leq)$, da jedes $y \in M$ mit $y \geq x_X$ auch eine obere Schranke von X wäre.
(Z) $\Rightarrow$ (W) Sei $M \neq \emptyset$ und betrachte

$$\mathcal{M} := \{(T, \leq_T) \mid T \subseteq M, \leq_T \text{ Wohlordnung auf } T\}.$$

Auf $\mathcal{M}$ definiere die Ordnung

$$(T_1, \leq_1) \leq (T_2, \leq_2) \Leftrightarrow \begin{cases} T_1 \subseteq T_2 & \text{und} \\ \leq_1 = (\leq_2)_{T_1} & \text{und} \\ t_1 \leq_2 t_2 & \text{für alle } t_1 \in T_1, t_2 \in T_2 \setminus T_1. \end{cases}$$

Bezüglich dieser Ordnung ist $\mathcal{M}$ induktiv geordnet. Nach (Z) gibt es ein maximales Element $(X, \leq_X)$ in $\mathcal{M}$. Für dieses maximale Element gilt $X = M$, denn sonst sei $m \in M \setminus X$ und $\leq_0$ die Ordnung auf $X \cup \{m\}$ die die Ordnung $\leq_X$ fortsetzt, so dass $x \leq_0 m$ für alle $x \in X$. Dann ist $(X \cup \{m\}, \leq_0) > (X, \leq_X)$ ein Widerspruch zur Maximalität von $(X, \leq_X)$. Also besitzt M eine Wohlordnung.
(W) $\Rightarrow$ (A) Sei Λ eine Menge und $(X_\lambda \mid \lambda \in \Lambda)$ eine Familie nichtleerer Mengen. Wegen (W) besitzt

$$\bigcup_{\lambda \in \Lambda} X_\lambda$$

eine Wohlordnung $\leq$ und insbesondere hat jede Teilmenge X_λ ein kleinstes Element x_λ bezüglich dieser Ordnung. Damit haben wir eine Auswahlabbildung $X_\lambda \mapsto x_\lambda$. □

1.2 Primkörper, Körpererweiterungen und Gradsatz

Definition 1.8. *Sei K ein kommutativer Ring mit 1. K heißt genau dann* **Körper***, wenn $(K \setminus \{0\}, \cdot)$ eine Gruppe ist.*

Definition 1.9. *Seien K, E Körper.*

(i) Das Paar (E/K) heißt **Körpererweiterung***, falls $K \subseteq E$ und $\cdot_K$, $+_K$ durch Einschränkung von $\cdot_E$, $+_E$ entstehen. K heißt dann* **Teilkörper** *von E, und E* **Erweiterungskörper** *von K.*

(ii) Die Körpererweiterung (E/K) heißt **endlich***, falls $[E : K] := dim_K E < \infty$. $[E : K]$ heißt der* **Grad** *von E über K.*

Beispiel. Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann ist $E := K[x]/(f)$ ein Körper und $K \hookrightarrow E, a \mapsto a\overline{1}$ eine Einbettung bezüglich der wir E als Körpererweiterung von K ansehen. Es ist $[E : K] =$Grad(f).

Satz 1.10. *(Gradsatz) Seien E_1, E_2, E_3 Körper mit $E_1 \subseteq E_2 \subseteq E_3$. Dann gilt: $[E_3 : E_1] = [E_3 : E_2] \cdot [E_2 : E_1]$.*

BEWEIS: Seien $[E_3 : E_2] = n < \infty, [E_2 : E_1] = m < \infty$. Sei weiter $(e_1, \ldots, e_n)$ eine E_2-Basis von E_3 und $(f_1, \ldots, f_m)$ eine E_1-Basis von E_2
Beh.: Dann ist $\mathcal{B} := (e_1 f_1, e_1 f_2, \ldots, e_n f_m)$ eine E_1-Basis von E_2
Bew.:

(i) $\mathcal{B}$ ist Erzeugendensystem: Sei $x \in E_3$. Dann existieren $\alpha_i \in E_2$, so dass $x = \sum_{i=1}^{n} \alpha_i e_i$.

Also existieren $\alpha_{ij} \in E_1$, so dass $\alpha_i = \sum_{j=1}^{m} \alpha_{ij} f_j$. Daraus folgt $x = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} e_i f_j$.

(ii) $\mathcal{B}$ ist linear unabhängig:

$$\text{Sei } \alpha_{ij} \in E_1, \text{ so dass } \sum_{i,j} \alpha_{ij} e_i f_j = 0. \text{ Dann gilt: } \sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha_{ij} f_j) e_i = 0.$$

Da aber nun die e_i über E_2 linear unabhängig sind, muß für alle i gelten:

$$\sum_{j=1}^{m} \alpha_{ij} f_j = 0$$

Da auch die f_j linear unabhängig sind (über E_1), folgt $\alpha_{ij} = 0$ für alle i, j.

Ist nun $[E_3 : E_2]$ oder $[E_2 : E_1]$ unendlich so folgt sofort, daß $[E_3 : E_1] = \infty$. □

BEISPIELE 1.

a) $[K(x) : K] = \infty$

b) $[K(x) : K(x^2)] = 2$

Bemerkung 1.11. *Sei R ein Integritätsbereich. $\psi : \mathbb{Z} \to R$ definiert durch $n \mapsto n \cdot 1$. Dann ist $Bild(\psi) \leq R$ ein Integritätsbereich, also $ker(\psi)$ ein Primideal in $\mathbb{Z}$. Also $ker(\psi) = (0)$ oder $ker(\psi) = (p)$ für eine Primzahl p.*
p heißt die Charakteristik von R, *$p = Char(R)$. Ist ψ injektiv, so setzen wir $Char(R) = 0$.*

Bemerkung: Man sieht auch leicht "zu Fuß", dass $\ker(\psi)$ entweder 0 oder ein Primideal ist. Denn sei ψ nicht injektiv und $n \in \mathbb{N}$ minimal mit $n \cdot 1 = 0$. Ist n keine Primzahl, dann gibt es $n_1, n_2 \in \mathbb{N}_{>1}$ mit $n = n_1 n_2$. Dann ist aber $0 = n \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1)$. Da R nullteilerfrei ist, gilt $(n_1 \cdot 1) = 0$ oder $(n_2 \cdot 1) = 0$, was ein Widerspruch zur Minimalität von n ist.

Satz 1.12. *Sei K ein Körper. Sei*

$$K_0 := \cap\{L \mid L \text{ ist Teilkörper von } K\}$$

der **Primkörper** *von K. Ist $Char(K) = 0$, so ist $K_0 \cong \mathbb{Q}$ isomorph zum Körper der rationalen Zahlen. Ist $Char(K) = p > 0$ eine Primzahl, so ist $K_0 \cong \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

BEWEIS: Klar ist K_0 ein Körper und $1 \in K_0$. Dann ist aber auch $1+1 = 2 \cdot 1$ in K_0 und also mit den Bezeichnungen aus Bemerkung 1.11 $\psi(\mathbb{Z}) \subset K_0$. Ist $Char(K) = p > 0$, so ist $ker(\psi) = (p) \trianglelefteq \mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$ und $\psi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ ein Körper. Also ist $K_0 = \psi(\mathbb{Z})$. Ist $Char(K) = 0$, dann ist ψ injektiv und $\mathbb{Z} \hookrightarrow K_0$. Da K_0 ein Körper ist, hat ψ eine eindeutig bestimmte Fortsetzung $\tilde{\psi} : \mathbb{Q} = Quot(\mathbb{Z}) \hookrightarrow K_0$. Also ist $K_0 = \mathbb{Q}$ in diesem Fall. □

Definition 1.13. *Sei (E/K) eine Körpererweiterung.*

(i) Für beliebige $a_1, \ldots, a_n \in E$ bezeichnet $K(a_1, \ldots, a_n)$ den kleinsten Teilkörper von E, der $K, a_1, \ldots, a_n$ enthält, und $R := K[a_1, \ldots, a_n]$ den kleinsten Teilring von E, der $K, a_1, \ldots, a_n$ enthält,

(ii) (E/K) heißt **einfache** *Körpererweiterung, falls ein $a \in E$* existiert *mit $E = K(a)$.*

Bemerkung:
$K(a_1, \ldots, a_n) = Quot(K[a_1, \ldots, a_n])$.
Insbesondere ist $K(x) = \{\frac{p(x)}{q(x)} \mid p, q \in K[x], q \neq 0\}$ der Körper der rationalen Funktionen.

Bemerkung 1.14. *Sei $E = K(a)$ einfache Körpererweiterung über K. Dann gilt entweder $E = K[a]$ oder $E \cong K(x)$. Im 1.Fall heißt a* **algebraisch** *über K. Im 2.Fall heißt a* **transzendent** *über K.*

BEWEIS: Sei $\varphi : K[x] \to K(a)$ der K-Algebrenhomomorphismus definiert durch $x \mapsto a$. Da $K(a)$ nullteilerfrei ist, ist auch $Bild(\varphi)$ ein Integritätsring. Also ist $\ker(\varphi)$ ein Primideal in dem Hauptidealbereich$K[x]$.

(i). $\ker(\varphi) \neq 0$. Dann ist $\ker(\varphi) = (m(x))$ für ein irreduzibles Polynom $m(x) \in K[x]$. (Es gilt $m(a) = 0$ in E und der normierte Erzeuger $\mu_{a,K}(x)$ von $\ker(\varphi)$ heißt das **Minimalpolynom** von a (über K).) Also ist $\ker(\varphi)$ ein maximales Ideal und daher $Bild(\varphi) = K[a]$ ein Körper, d.h. $K[a] = K(a) = E$.

(ii). $\varphi : K[x] \longrightarrow E$ ist injektiv. Also ist $Bild(\varphi) \cong K[x]$ kein Körper, aber $Bild(\varphi) = K[a]$ und $E = Quot(K[a]) \cong K(x)$.

□

Übung: Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann ist $K[a]$ ein endlich dimensionaler K-Vektorraum und $m_a : K]a] \to K[a], z \mapsto az$ eine K-linerare Abbildung. Es gilt $\mu_{a,K} = \mu_{m_a} = \chi_{m_a}$, d.h. das Minimalpolynom von a über K stimmt mit dem Minimalpolynom dieser linearen Abbildung überein. Es ist $(1, a, \ldots, a^{d-1})$ eine K-Basis von $K[a]$, $d = \text{Grad}(\mu_{a,K})$.

Übung: Sei L/K eine Körpererweiterung. Definieren den **algebraischen Abschluss von K in L**

$$\text{Alg}_L(K) := \{a \in L \mid a \text{ ist algebraisch über } K\}.$$

Zeigen Sie, dass $\text{Alg}_L(K)$ ein Körper ist.

Definition 1.15. (E/K) *heißt* **algebraisch**, *falls a algebraisch über K ist* für alle $a \in E$.

Satz 1.16. *(i) Ist $[E : K] < \infty$ so ist (E/K) algebraisch.*

(ii) Ist $E = K(\alpha_1, \ldots, \alpha_n)$ mit α_i algebraisch, so ist $[E : K] < \infty$.

BEWEIS:

(i) Sei $\alpha \in E$. Dann wird die Folge $(1, \alpha, \alpha^2, \ldots)$ irgendwann linear abhängig über K, d.h. es gibt $n \in \mathbb{N}$, $a_i \in K$ $(1 \leq i \leq n)$ mit $a_n \neq 0$ mit $\sum_{i=0}^{n} a_i \alpha^i = 0$, d.h. α ist algebraisch über K.

(ii) Wegen des Gradsatzes genügt es, die Behauptung für $n = 1$ zu zeigen. Dann ist sie aber klar, da die Potenzen $(1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{n-1})$ (n=Grad des Minimalpolynoms von α_1) eine K-Basis von E bilden.

□

Lemma 1.17. *Algebraisch zu sein ist transitiv, d.h. ist (L/K) algebraisch und (F/L) algebraisch, so ist (F/K) algebraisch.*

BEWEIS: Sei $\alpha \in F$. Zu zeigen: α ist algebraisch über K. Es ist α algebraisch über L, d.h. es gibt $a_0, \ldots, a_{n-1} \in L$ mit $\alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i = 0$. Die Körpererweiterung $(K(a_0, \ldots, a_{n-1})/K)$ ist nach Satz 1.16 endlich. Ebenso ist $(K(a_0, \ldots, a_{n-1}, \alpha)/K(a_0, \ldots, a_{n-1}))$ endlich also nach dem Gradsatz $(K(a_0, \ldots, a_{n-1}, \alpha)/K)$ endlich und damit algebraisch. Insbesondere ist α algebraisch über K. □

1.3 Transzendente Erweiterungen.

Definition 1.18. *Sei L/K eine Körpererweiterung. Eine Teilmenge $\{a_1, \ldots, a_n\} \subseteq L$ heißt* **algebraisch abhängig** *über K, falls ein Polynom $f \in K[X_1, \ldots, X_n]$ existiert mit $f(a_1, \ldots, a_n) = 0$ und ansonsten* **algebraisch unabhängig**. *Eine beliebige Teilmenge $A \subseteq L$ heißt* **algebraisch unabhängig** *über K, falls jede endliche Teilmenge algebraisch unabhängig ist. Eine* **Transzendenzbasis** *B von L über K ist eine algebraisch unabhängige Teilmenge $B \subset L$ so dass $(L/K(B))$ eine algebraische Erweiterung ist. Gibt es eine Transzendenzbasis B mit $L = K(B)$, so heißt L über K* **rein transzendent**.

Sei $L = K(x)$ der Körper der rationalen Funktionen. Dann ist $B = \{x\}$ eine Transzendenzbasis und L über K rein transzendent. Jedoch ist auch $B = \{x^3\}$ eine Transzendenzbasis, $[L : K(x^3)] = 3$.

Satz 1.19. *Sei L/K eine Körpererweiterung.*
(a) Jede algebraisch unabhängige Teilmenge von L läßt sich zu einer Transzendenzbasis ergänzen. Transzendenzbasen sind also maximal algebraisch unabhängige Teilmengen. Insbesondere gibt es Transzendenzbasen.
(b) Je zwei Transzendenzbasen haben gleich viel Elemente (oder sind unendlich). Im endlichen Fall heißt diese Anzahl auch der **Transzendenzgrad** *von L über K,* $\mathrm{trdeg}(L, K)$.

Beweis. (a) Sei $A \subseteq L$ eine algebraisch unabhängige Teilmenge und

$$\mathcal{B}(A) := \{A \subseteq U \subset L \mid U \text{ ist algebraisch unabhängig } \}.$$

Dann ist $\mathcal{B}(A)$ durch Inklusion induktiv geordnet und besitzt nach dem Lemma von Zorn ein maximales Element B. Dann ist $L/K(B)$ algebraisch, denn für jedes $a \in L \setminus B$ ist $\{a\} \cup B$ algebraisch abhängig.
(b) Wir zeigen dies für den endlichen Fall. Sei also $B := \{b_1, \ldots, b_n\}$ eine Transzendenzbasis von L über K und sei $\{a_1, \ldots, a_m\} \subset L$ algebraisch unabhängig. Dann ist a_1 über $K(B)$ algebraisch, also gibt es ein Polynom $0 \neq f(t, X_1, \ldots, X_n) \in K[t, X_1, \ldots, X_n]$ mit $f(a_1, b_1, \ldots, b_n) = 0$. Da a_1 transzendent über K ist, kommt eines der X_i ($\mathbb{E}$ X_1) in f vor. Dann ist aber b_1 algebraisch über $K(a_1, b_2, \ldots, b_n)$ also auch L algebraisch über $K(a_1, b_2, \ldots, b_n)$. Die Menge $\{a_1, \ldots, b_n\}$ ist algebraisch unabhängig, da jede algebraische Abhängigkeit dieser Menge auch eine von $\{b_1, \ldots, b_n\}$ liefert, also ist auch $\{a_1, \ldots, b_n\}$ eine Transzendenzbasis von L. □

Folgerung 1.20. *Sei L/K eine Körpererweiterung. Dann gibt es einen Körper E mit L/E algebraisch und E/K rein transzendent.*

Beispiel: Andersherum geht es nicht: Betrachten Sie den Körper $L = \mathbb{C}(X)[Y]/(Y^3 - (X^2 + X))$ und $K = \mathbb{C}$. Dann ist $K = \mathrm{Alg}_L(K)$, da $\mathbb{C}$ algebraisch abgeschlossen ist. L ist algebraisch über $E = \mathbb{C}(X)$, sogar endlich mit $[L : E] = 3$. Jedoch ist L nicht rein transzendent.

Bemerkung 1.21. *Sei $E > L > K$ Körpererweiterungen. Dann gilt* $\mathrm{trdeg}(E, K) = \mathrm{trdeg}(E, L) + \mathrm{trdeg}(L, K)$.

1.4 Zerfällungskörper.

Definition 1.22. *(i) Seien E_1 und E_2 Körper. Ein Ringhomomorphismus $\varphi : E_1 \longrightarrow E_2$ heißt auch* **Körperhomomorphismus**.
Ein Körperisomorphismus $\varphi : E \longrightarrow E$ heißt **Körperautomorphismus**.

(ii) Seien $(E_1/K), (E_2/K)$ Körpererweiterungen. Ein K-Algebrenhomomorphismus $\varphi : E_1 \longrightarrow E_2$ heißt **Körperhomomorphismus über** K.

(iii) $E_1 \overset{\cong}{K} E_2$, falls K-Algebrenisomorphismus zwischen E_1 und E_2 existiert.

(iv) $\mathcal{A}ut(E) := \{\varphi | \varphi : E \longrightarrow E$ *ist Körperautomorphismus*$\}$
$\mathcal{A}ut_K(E) = \mathcal{A}ut(E/K) := \{\varphi | \varphi : E \longrightarrow E$ *ist Körperautomorphismus über* K $\}$

Beachte: Körperhomomorphismen sind immer injektiv. Denn der Kern ist ein Ideal, also $= 0$ oder $= E_1$. Aber 1 wird unter Körperhomomorphismen auf 1 abgebildet, also ist 1 nicht im Kern, also Kern $= 0$.

Bemerkung 1.23. *Sei $\psi : K \to K'$ ein Körperhomomorphismus. Dann gibt es genau einen Ringhomomorphismus $\tilde{\psi} : K[x] \to K'[x]$ der ψ fortsetzt, mit $\tilde{\psi}(x) = x$. Es gilt $\tilde{\psi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \psi(a_i) x^i$.*

Definition 1.24. *Sei K ein Körper und $f(t) \in K[t]$.*

(i) E heißt ein **Wurzelkörper** *von $f(t)$, falls (E/K) eine Körpererweiterung ist und ein $\xi \in E$ existiert mit $f(\xi) = 0$.*

(ii) Der Erweiterungskörper E von K heißt ein **Zerfällungskörper** *von $f(t)$, falls $f(t)$ über E in Linearfaktoren zerfällt und E minimal ist, d.h. $f(t)$ zerfällt nicht in Linearfaktoren in $F[t]$ für $K \subseteq F \subset E$, $F \neq E$.*
(Dann existieren $\xi_i \in E$, so dass $f(t) = \prod(t - \xi_i)$ in $E[t]$.)
Beachte: $f(t)$ hat dann keine weiteren Wurzeln in E.

Satz 1.25. *Sei $f(t) = \sum_{i=0}^{n} a_i t^i \in K[t]$, $a_n \neq 0$ ein Polynom vom Grad $n \geq 1$.*

(i) Ein Wurzelkörper von $f(t)$ existiert .

(ii) Jeder minimale Wurzelkörper L von f ist von der Form $L = K[\alpha]$ mit $f(\alpha) = 0$.

(iii) Sei $f(t)$ irreduzibel in $K[t]$, $\psi : K \to K_1$ ein Körperisomorphismus, und $\tilde{\psi}$ wie in Bemerkung 1.23. Sei $f_1(t) = \sum_{i=0} \psi(a_i) t^i = \tilde{\psi}(f(t)) \in K_1[t]$. Ist $L = K[\alpha]$ ein minimaler Wurzelkörper von f und $L_1 = K_1[\alpha_1]$ ein minmaler Wurzelkörper von f_1, dann definiert $\psi_1 : L \to L_1, \sum_{i=0}^{m} a_i \alpha^i \mapsto \sum_{i=0}^{m} \psi(a_i) \alpha_1^i$ einen Körperisomorphismus (der ψ fortsetzt).

(iv) Insbesondere folgt aus (iii): Ist $f(t)$ irreduzibel in $K[t]$, so sind je zwei minimale Wurzelkörper isomorph über K.

BEWEIS:

(i) Sei $\tilde{E} = K[t]/(f(t))$ "Wurzelring" mit $f(\bar{t}) = 0$ $(\bar{t} = t + (f(t)))$. Jedes maximale Ideal $I \trianglelefteq \tilde{E}$ liefert einen (sogar minimalen) Wurzelkörper $E = \tilde{E}/I$.
Alternativ sei f_1 ein irreduzibler Teiler von f in $K[t]$ und setze $E := K[t]/(f_1)$.

(ii) Ist L ein minimaler Wurzelkörper von f, so enthält L ein α mit $f(\alpha) = 0$. Da $K(\alpha) \leq L$ ein Wurzelteilkörper von L ist, folgt $L = K(\alpha)$. Weiter ist α algebraisch über K, also $L = K[\alpha]$.

(iii) Da $f(t) \in K[t]$ irreduzibel ist, ist auch sein Bild $f_1 = \tilde{\psi}(f) \in K_1[t]$ irreduzibel. Daher ist $L \cong K[t]/(f(t)) \cong K_1[t]/(f_1(t)) \cong L_1$.

□

Beispiel Das irreduzible Polynom $t^4 - 2 \in \mathbb{Q}[x]$ hat $\mathbb{Q}[\sqrt[4]{2}]$ und $\mathbb{Q}[i\sqrt[4]{2}]$ als minimale Wurzelkörper. Der Wurzelkörper ist also nicht physikalisch eindeutig, sondern nur bis auf Isomorphie.

Satz 1.26. *Sei $f(t) \in K[t] \setminus K$.*

(i) Es gibt einen Erweiterungskörper von K, über welchem $f(t)$ in Linearfaktoren zerfällt.

(ii) Je zwei Zerfällungskörper von f sind isomorph über K.

BEWEIS:

(i) folgt aus 1.25 durch Iteration.

(ii) Sei L ein Zerfällungskörper von f über K. Durch Induktion über $m := [L : K]$ zeigen wir: Ist $\psi : K \to K'$ ein Körperisomorphismus und L' ein Zerfällungskörper von $\tilde{\psi}(f) \in K'[t]$ über K', so läßt sich ψ zu einem Körperisomorphismus $\psi' : L \to L'$ fortsetzen.
Ist $m = 1$, dann zerfällt f in $K[t]$ in Linearfaktoren und $L' = K' \cong K = L$.
Sei also $m > 1$ und $g(t) \in K[t]$ ein irreduzibler Faktor von f vom Grad $d > 1$. Sei $g_1 := \tilde{\psi}(g)$. Sei $\alpha \in L$ mit $g(\alpha) = 0$ und $\alpha' \in L'$ mit $g_1(\alpha') = 0$. Dann sind die Teilkörper $L_1 = K[\alpha] \leq L$ und $L_2 = K'[\alpha'] \leq L'$ beides minimale Wurzelkörper von g (bzw. g_1) und nach Satz 1.25 (iii) läßt sich ψ zu einem Isomorphismus $\psi_1 : L_1 \to L_2$ fortsetzen. Weiter ist $[L : L_1] = \dim_{L_1}(L) = \frac{\dim_K(L)}{\dim_K(L_1)} = \frac{\dim_K(L)}{d} < [L : K]$ und L (bzw. L') ist ein Zerfällungskörper von $f(t) \in L_1[t]$ (bzw. $\tilde{\psi}_1(f(t)) \in L_2[t]$). Nach Induktionsvoraussetzung läßt sich ψ_1 zu einem Körperisomorphismus von L nach L' fortsetzen, der dann natürlich auch ψ fortsetzt.

□

1.5 Der algebraische Abschluss.

Bemerkung 1.27. *Sei L/K eine Körpererweiterung. Dann ist*

$$Alg_K(L) := \tilde{K} := \{a \in L \mid a \text{ ist algebraisch über } K\}$$

ein Teilkörper von L. $\tilde{K}$ heißt der **algebraische Abschluss von K in L.** *$\tilde{K}$ ist der größte Teilkörper von L, der algebraisch über K ist.*

Definition 1.28. *Ein Körper K heißt* **algebraisch abgeschlossen**, *falls jedes $f \in K[t]$ eine Nullstelle in K hat.*

Bemerkung 1.29. *Äquivalent sind:*

(i) K is algebraisch abgeschlossen.

(ii) Jedes irreduzible Polynom in $K[t]$ hat Grad 1.

(iii) Ist (L/K) eine algebraische Erweiterung, so gilt $L = K$.

Definition 1.30. *Sei K ein Körper. Ein Erweiterungskörper E von K heißt ein* **algebraischer Abschluss** *von K, falls*

(i) E ist algebraisch abgeschlossen.

(ii) (E/K) ist algebraisch.

Bemerkung 1.31. *Ist L/K eine Köpererweiterung so dass L algebraisch abgeschlossen ist, so ist $Alg_K(L)$ ein algebraischer Abschluss von K. (Beweis als nette Übung.)*

Satz 1.32. *Jeder Körper K hat einen algebraischen Abschluss.*

BEWEIS: Sei $P := \{f \in K[t], \text{ irreduzibel, normiert }\}$ und

$$\mathcal{X} := \{\xi_1^{(f)}, \ldots, \xi_{Grad(f)}^{(f)} \mid f \in P\}$$

Ist $f(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \cdots + (-1)^n a_n \in P$ so setze

$$R_f := \{ \sum_{i_1 < \ldots < i_k} \xi_{i_1}^{(f)} \cdots \xi_{i_k}^{(f)} - a_k \mid k = 1, \ldots, n\}.$$

Nun betrachte das Ideal

$$A := \langle \bigcup_{f \in P} R_f \rangle \trianglelefteq K[\mathcal{X}].$$

Wir zeigen gleich, dass $A \neq K[\mathcal{X}]$ ist. Dann gibt es nach dem Lemma von Zorn ein maximales Ideal M von $K[\mathcal{X}]$ mit $A \subseteq M$. Setze $E := K[\mathcal{X}]/M$. Dann ist E ein Körper der K (identifiziert mit seinem Bild $K \cong K \cdot 1 + M \subset K[\mathcal{X}]/M$) enthält. Jedes Element von E ist algebraisch über K, also ist E eine algebraische Erweiterung von K. Weiter zerfällt jedes (irreduzible normierte) Polynom $f \in K[t] \setminus K$ in Linearfaktoren

$$f = \prod_{i=1}^{n} (t - \overline{\xi}_i) \in E[t].$$

Beh. E ist algebraisch abgeschlossen.
Dazu sei α algebraisch über E. Dann ist auch α algebraisch über K und damit Nullstelle eines Polynoms in $K[t]$. Dieses zerfällt in Linearfaktoren in $E[t]$ und damit ist $\alpha \in E$.
Bleibt zu sehen, dass $A \neq K[\mathcal{X}]$ ist. Ansonsten wäre $1 \in A$ eine endliche Linearkombination $1 = \sum_i a_i x_i$ für geeignete $a_i \in K$ und x_i endliche Produkte von Ausdrücken der Form $\sum_{i_1 < \ldots < i_k} \xi_{i_1}^{(f)} \cdots \xi_{i_k}^{(f)} - a_k$. Spezialisiert man in diesem Ausdruck die $\xi_j^{(f)}$ zu Nullstellen von f, so wird der Ausdruck gleich 0. Da nur endlich viele f, sagen wir $f_1, \ldots, f_k$ vorkommen, kann man diese Nullstellen im Zerfällungskörper L des Produkts $\prod_{i=1}^{k} f_i$ finden. Setzt man diese Nullstellen ein, so werden alle x_i zu Null und somit $1 = \sum_i a_i x_i = 0 \in L$, ein Widerspruch. □

Satz 1.33. *Je zwei algebraische Abschlüsse $\bar{K}$ und $\bar{K}'$ von K sind über K isomorph.*

BEWEIS: Sei $\bar{K}$ ein algebraischer Abschluss von K. Wir zeigen:

Lemma 1.34. *Ist $K \subset L \subset F$ eine algebraische Erweiterung und $\varphi : L \to \bar{K}$ ein Ringhomomorphismus mit $\varphi_{|K} = id$, dann gibt es einen Ringhomomorphismus $\psi : F \to \bar{K}$ mit $\psi_{|L} = \varphi$.*

Daraus ergibt sich der Satz als Spezialfall: $L = K$, $F = \bar{K}'$, $\varphi = id$.
Sei $\mathcal{A} := \{(F', \varphi') \mid F \supseteq F' \supseteq L, \varphi'_{|L} = \varphi\}$. Dann ist $\mathcal{A}$ durch

$$(F_1, \varphi_1) \leq (F_2, \varphi_2) :\Leftrightarrow F_1 \leq F_2, (\varphi_2)_{|F_1} = \varphi_1$$

induktiv geordnet, d.h. jede Kette hat eine obere Schranke:
Sei $\{(F_i, \varphi_i) \mid i \in I\}$ eine vollständig geordnete Teilmenge von $\mathcal{A}$. Dann hat sie die obere Schranke $(\bigcup_{i\in I} F_i, \psi)$ mit $\psi_{|F_i} = \varphi_i$. Mit dem Zorn'schen Lemma existiert ein maximales Element (F', φ') von $\mathcal{A}$. Ist $F' \neq F$, so wähle $\alpha \in F \setminus F'$ und setze φ' auf $F'(\alpha)$ fort: Ist $\mu_\alpha \in F'[t]$ das Minimalpolynom von α über F', so zerfällt μ_α in $\bar{K}[t]$ in Linearfaktoren. Insbesondere gibt es ein $\beta \in \bar{K}$ mit $\mu_\alpha(\beta) = 0$. Setze φ' auf $F'(\alpha)$ fort durch $\varphi'(\alpha) := \beta$. Widerspruch. Also ist $F' = F$. □

1.6 Endliche Körper.

Satz 1.35. *Sei K ein Körper und $U \leq K^*$ endlich. Dann ist U zyklisch, d.h. es gibt ein $z \in K$ mit $U =< z >$.*

Beweis. K^* ist eine abelsche Gruppe, also ist auch U eine endliche abelsche Gruppe. Angenommen U ist nicht zyklisch. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es dann eine Primzahl p und eine Untergruppe $X := C_p \times C_p \cong \langle a, b\rangle \leq U$. Die p^2 Elemente von X erfüllen aber alle $x^p = 1$, sind also Nullstellen des Polynoms $t^p - 1 \in K[t]$. Dieses hat aber (da $K[t]$ faktoriell ist) höchstens p Nullstellen in K, ein Widerspruch. □

Lemma 1.36. *Sie K ein Körper und $f : K \to K$ ein Körperendomorphismus. Dann ist*

$$F := Fix(f) := \{k \in K \mid f(k) = k\}$$

ein Teilkörper von K.

Beweis. Mit $a, b \in F$ liegen auch $a + b$ und $a \cdot b$ in F. Weiter gilt $0, 1 \in F$ und für $0 \neq a \in F$ auch $a^{-1} \in F$. □

Lemma 1.37. *Ist K ein Körper der Charakteristik p, dann ist die Abbildung $\Phi_p : K \to K, a \mapsto a^p$ ein Körperendomorphismus von K, der sogenannte* Frobeniusendomorphismus. *Ist K endlich, so ist Φ_p bijektiv also ein Automorphismus von K, der* **Frobeniusautomorphismus**.

Beweis: Φ_p ist ein Ringhomomorphismus, denn $\Phi_p(ab) = \Phi_p(a)\Phi_p(b)$ und

$$\Phi_p(a + b) = (a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p \text{ für alle } a, b \in K.$$

Der Kern eines Ringhomomorphismus ist ein Ideal, also ist Φ_p injektiv und damit auch surjektiv, wenn K endlich ist. □

Satz 1.38. *Sei K ein endlicher Körper. Dann ist $Char(K) = p$ eine Primzahl und $|K| = p^n$ eine Potenz dieser Primzahl. Umgekehrt gibt es zu jeder Primzahlpotenz p^n genau einen Körper mit p^n Elementen. Dieser wird mit $\mathbb{F}_{p^n}$ bezeichnet.*

Beweis. Der Primkörper von K ist auch endlich und daher $\cong \mathbb{F}_p$ für eine Primzahl p. Also ist K ein endlich dimensionaler $\mathbb{F}_p$-Vektorraum und daher $|K| = p^n$ mit $n = [K : K_0]$.
Sei umgekehrt $n \in \mathbb{N}$ und p eine Primzahl.
Existenz: Sei K der Zerfällungskörper des Polynoms $f(t) = t^{p^n} - t \in \mathbb{F}_p[t]$. Dann gilt $f(t) = \prod_{i=1}^{p^n}(t - a_i) \in K[t]$ mit $Z := \{a_1, \ldots, a_{p^n}\} \subseteq K$. Da $ggT(f, f') = 1$ gilt $|Z| = p^n$, die Nullstellen von f sind also paarweise verschieden. Weiter gilt: $f(1) = f(0) = 0$ und $a \in K$ ist Nullstelle von f genau dann wenn $\Phi_p^n(a) = a$. Da die n-te Potenz des Frobeniusautomorphismus von K wieder ein Automorphismus von K ist, bilden die Nullstellen von f in K also einen Teilring von K, und damit $K = Z$.
Eindeutigkeit. Sei L ein Körper mit p^n Elementen. Dann ist der Primkörper $L_0 = \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Weiter ist $L^* = L \setminus \{0\}$ eine Gruppe mit $p^n - 1$ Elementen, also gilt $a^{p^n-1} = 1$ für alle $0 \neq a \in L$. Also enhält L die p^n verschiedenen Nullstellen von $t^{p^n} - t \in \mathbb{F}_p[t]$ und damit ist L der Zerfällungskörper dieses Polynoms. □

Bemerkung 1.39. *Jeder Erzeuger $a \in \mathbb{F}_{p^n}$ mit $\langle a \rangle = \mathbb{F}_{p^n}^*$ heißt* **Primitivwurzel** *von $\mathbb{F}_{p^n}$.*
Jede Primitivwurzel erzeugt den Körper $\mathbb{F}_{p^n} = \mathbb{F}_p[a]$.
Die Teilkörper von $\mathbb{F}_{p^n}$ sind genau die Körper $\mathbb{F}_{p^d}$ für die Teiler d von n.
Für $d \mid n$ ist

$$\mathbb{F}_{p^d} := \{a \in \mathbb{F}_{p^n} \mid a^{p^d} = a\} = Fix(\Phi_p^d).$$

1.7 Separable Erweiterungen

Definition 1.40. *(i) Ein Polynom $f(t) \in K[t]$ heißt* **separabel**, *falls die Wurzeln von $f(t)$ in einem Zerfällungskörper von f paarweise verschieden sind.*

(ii) Sei (E/K) algebraische Körpererweiterung. $a \in E$ heißt **separabel**, *falls das Minimalpolynom über K von a separabel ist. (E/K) heißt* **separabel**, *falls jedes $a \in E$ separabel ist. (Beachte: Das Minimalpolynom ist irreduzibel über K.)*

(iii) Die Abbildung $': K[t] \longrightarrow K[t]:$ $\begin{array}{ccc} f(t) & \mapsto & f'(t) \\ \| & & \| \\ \sum_{i=0}^{n} a_i t^i & & \sum_{i=1}^{n} i a_i t^{i-1} \end{array}$ *heißt* **Ableitung** *von f.*

Lemma 1.41. *Seien $f, g \in K[x]$ und (E/K) eine Körpererweiterung. Sei weiter $h = ggT(f, g)$ in $K[x]$. Dann gilt: $h = ggT(f, g)$ in $E[x]$.*

Beweis: $*:$ $h = \alpha f + \beta g$ mit geeigneter Wahl von $\alpha, \beta \in K[x]$. Sei nun $s \in E[x]$ mit $s|f$ und $s|g$. Dann folgt mit $*$: $s|h$ (in $E[x]$). Da $h|f$ und $h|g$ in $K[x]$, also auch in $E[x]$ folgt $h = \mathrm{ggT}(f, g)$ in $E[x]$. □

Satz 1.42. *Sei $f \in K[t]$ vom Grad ≥ 1. f ist genau dann inseparabel, wenn $ggT(f, f') \neq 1$ in $K[t]$.*

BEWEIS: Wegen 1.41 sei O.B.d.A. K Zerfällungskörper von f.

"$\Rightarrow$" f ist genau dann inseparabel, wenn ein $a \in K$ existiert mit $(t-a)^2 | f(t)$. Das impliziert $f(t) = (t-a)^2 \cdot g(t)$ mit $g(t) \in K[t]; f' = 2(t-a) \cdot g(t) + (t-a)^2 g'(t) = (t-a)\underbrace{[2g(t) + (t-a)g'(t)]}_{\in K[t]}$. Also $(t-a) | ggT(f, f')$.

"$\Leftarrow$" $(t-a) | ggT(f, f')$ impliziert $f(t) = (t-a)h(t)$ und $f'(t) = h(t) + (t-a)h'(t)$, daraus folgt $(t-a)|h(t)$, also $f(t) = (t-a)^2 \tilde{h}(t)$.

□

BEISPIELE 2.

a) Jedes irreduzible Polynom über $\mathbb{Q}$ ist separabel.

b) $t^p - x \in \mathbb{F}_p(x)[t]$ ist irreduzibel aber inseparabel, denn es gilt: $(t^p - x)' = pt^{p-1} \equiv 0 \pmod{p}$. Dann gilt $ggT(0, t^p - x) = t^p - x$.

Definition 1.43. *K heißt* **perfekt** *(vollkommen), falls jede endliche Erweiterung von K separabel ist. (d.h. jedes irreduzible Polynom in $K[t]$ ist separabel)*

Satz 1.44. *(i) Falls $Char(K) = 0$, so ist K perfekt.*

(ii) Falls $|K| < \infty$, so ist K perfekt.

BEWEIS:

(i) Sei $f(t) \in K[t]$ irreduzibel und $grad(f) \geq 1$. Dann ist $f'(t) \neq 0$ und $grad(f') < grad(f)$. Also gilt $ggT(f, f') = 1$.

(ii) Sei $f \in K[t]$ irreduzibel. Es sind nun 2 Fälle zu unterscheiden :

(i). $f' \neq 0$, dann gilt $ggT(f, f') = 1$ (wie oben).

(ii). $f' = 0$. Sei $f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0$. Dann ist $f'(t) = n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \ldots + a_1 = 0$. $i a_i = 0$ für alle $i = 1 \ldots n$, falls $a_i \neq 0$, dann $p | i$.
Beh.: $f = g^p$ für ein $g \in K[t]$.
Da $a \mapsto a^p$ eine bijektive Abbildung von K ist, gibt es $b_i \in K$ mit $b_i^p = a_i$ $(0 \leq i \leq n)$. Sei $g := \sum_i b_i t^{i/p}$.
Dann gilt $g^p = \sum_i b_i^p t^i = f$.

□

Erinnerung: Eine Körpererweiterung L/K heißt einfach, falls ein $x \in L$ existiert mit $L = K(x)$. In dem Fall nennt man x auch ein **primitives Element** von L/K.

Satz 1.45. *(Satz vom primitiven Element) Sei $L = K(y, z)$ eine endliche Körpererweiterung von K so dass z separabel über K ist. Dann gibt es ein $x \in L$ mit $L = K(x)$. Insbesondere ist jede endliche separable Körpererweiterung einfach.*

Beweis. Für endliche Körper ist dies aus dem Struktursatz ersichtlich. Sei also Œ K unendlich. Seien μ_y und μ_z die Minimalpolynome von y bzw. z über K und E ein Zerfällungskörper von $\mu_y\mu_z$ über L. Dann ist

$$\mu_y = \prod_{i=1}^{n}(t - y_i), \mu_z = \prod_{i=1}^{m}(t - z_i) \in E[t]$$

mit $z_i \neq z_j$ für alle $i \neq j$. Sei Œ $z = z_1, y = y_1$. Da K unendlich ist, gibt es ein $a \in K$ mit

$$y_i + az_j \neq y + az \text{ für alle } 1 \leq i \leq n, 2 \leq j \leq m.$$

Setze $x := y + az$.
Behauptung. $K(x) = L$:
Weil $\mu_y(x - az) = \mu_y(y) = 0$ gilt, ist z Nullstelle von $h := \mu_y(x - at) \in K(x)[t]$. Also ist z auch Nullstelle von $f := \mathrm{ggT}(h, \mu_z)$ in $K(x)[t]$. Ist $j \neq 1$, so gilt $h(z_j) = \mu_y(y + az - az_j) \neq 0$ nach Konstruktion von a. Also ist $(t - z)$ der einzige gemeinsame Teiler von h und μ_z und somit $f = t - z \in K(x)[t]$, woraus sich $z \in K(x)$ ergibt. □

Definition 1.46. *Sei L/K eine algebraische Erweiterung und $\overline{K}$ ein algebraischer Abschluss von K. Dann heißt*

$$[L : K]_s := |\{\varphi : L \to \overline{K} \mid \varphi \text{ ist } K\text{-Algebrenhom. } \}| = |\operatorname{Hom}_K(L, \overline{K})|$$

der **Separabilitätsgrad** *von L über K.*

Bemerkung 1.47. *Ist $L \cong K[t]/(f)$ der Wurzelkörper eines irreduziblen Polynoms, so ist $[L : K]_s = |\{a \in \overline{K} \mid f(a) = 0\}|$. Insbesondere gilt $[L : K]_s \leq [L : K]$ mit Gleichheit genau dann wenn f ein separables Polynom ist.*

Satz 1.48. *Seien $E > L > K$ Körpererweiterungen mit $[E : K]$ endlich. Dann ist*

$$[E : L]_s[L : K]_s = [E : K]_s.$$

Beweis. Als Übung. □

1.8 Normale Erweiterungen

Definition 1.49. *Sei K ein Körper und $\bar{K}$ sein algebraischer Abschluss. Eine algebraische Erweiterung $K \subset E \subset \bar{K}$ heißt* **normal** *über K, falls für jeden K-Algebrenhomomorphismus $\varphi : E \to \bar{K}$ gilt $\varphi(E) = E$.*

Beispiel. $E := \mathbb{Q}[\sqrt[4]{2}]$ ist nicht normal über $\mathbb{Q}$, da z.B. der durch $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ definierte $\mathbb{Q}$-Algebrenhomomorphismus von E in $Alg_{\mathbb{Q}}(\mathbb{C}) \cong \bar{\mathbb{Q}}$ den Körper E nicht in sich selbst abbildet.

Satz 1.50. *Äquivalent sind:*

(i) (E/K) *normal.*

(ii) Jedes irreduzible Polynom in $K[t]$*, das eine Nullstelle in* E *hat, zerfällt in* $E[t]$ *in Linearfaktoren.*

(iii) Das Minimalpolynom jedes Elements von E *über* K *zerfällt in* $E[t]$ *in Linearfaktoren.*

(iv) Das Minimalpolynom jedes Erzeugers von E *über* K *zerfällt in* $E[t]$ *in Linearfaktoren.*

Beweis: (i) $\Rightarrow$ (ii) Sei $f \in K[t]$ irreduzibel, $\alpha \in E$ eine Nullstelle von f. Sei $\beta \in \bar{K}$ eine weitere Nullstelle von f. Zu zeigen: $\beta \in E$. Es gilt $K[\alpha] \cong K[\beta]$. Dieser Isomorphismus läßt sich nach Lemma 1.34 zu einem Körperhomomorphismus $\varphi : E \to \bar{K}$ fortsetzen. Da E normal ist, gilt $\varphi(E) = E$. Also gilt $\beta \in E$.
(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) Klar.
(iv) $\Rightarrow$ (i) Sei $\varphi : E \to \bar{K}$ ein Körperhomomorphismus mit $\varphi_{|K} = id$. Sei α ein Erzeuger von E über K, $\beta = \varphi(\alpha) \in \text{Bild}(\varphi)$ und sei $f(t) \in K[t]$ das Minimalpolynom von β. Dann ist $f(t)$ auch das Minimalpolynom von $\alpha \in E$. Nach Voraussetzung zerfällt f in Linearfaktoren in $E[t]$, d.h. E enthält alle Nullstellen von f in $\bar{K}$ und damit auch β. □

Beispiel Die Eigenschaft, normal zu sein, ist nicht transitiv. Sei $L = \mathbb{Q}[\sqrt{2}]$ und $E = \mathbb{Q}[\sqrt[4]{2}]$. Dann sind $(L/\mathbb{Q})$ und (E/L) normale Erweiterungen, als Erweiterungen vom Grad 2, aber $(E/\mathbb{Q})$ ist nicht normal.

Satz 1.51. *Eine endliche Erweiterung* (E/K) *ist normal, genau dann wenn* E *der Zerfällungskörper eines Polynoms in* $K[t]$ *ist.*

Beweis: $\Rightarrow$: Sei (E/K) normal. Da E endlich ist, gibt es $a_1, \ldots, a_n \in E$ mit $E = K[a_1, \ldots, a_n]$. Ist p_i das Minimalpolynom von a_i über K, so ist E der Zerfällungskörper von $\prod_{i=1}^{n} p_i$.
$\Leftarrow$: Sei E der Zerfällungskörper eines Polynoms p in $K[t]$. Dann ist E von den Nullstellen $a_1, \ldots, a_n$ von p über K erzeugt und das Minimalpolynom jedes dieser a_i über K teilt p und zerfällt daher in $E[t]$ in Linearfaktoren. Also ist E normal über K. □

Satz 1.52. *Sei* E/K *eine algebraische Körpererweiterung. Dann gibt es eine eindeutig bestimmte minimale normale Körpererweiterung* $\tilde{E}/K$*, mit* $E \subseteq \tilde{E}$*.* $\tilde{E}$ *heißt die* **normale Hülle** *von* E *über* K*.*
Ist E/K *endlich, so auch* $\tilde{E}/K$*.*

Beweis: Setze $\tilde{E}$ gleich dem Zerfällungskörper aller Minimalpolynome (über K) von Elementen von E. Dann ist $\tilde{E}/K$ normal und $\tilde{E}$ minimal. Ist $E = K[a_1, \ldots, a_n]$ endlich über K, so ist $\tilde{E}$ der Zerfällungskörper des Produkts der Minimalpolynome der a_i und damit endlich über K. □

Kapitel 2

Intermezzo: Gruppentheorie.

2.1 Wiederholung: Normalteiler und Homomorphiesatz.

Definition 2.1. *Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt* **Homomorphismus** *(von Gruppen), falls:*

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \text{ für alle } g_1, g_2 \in G$$

φ heißt ein **Isomorphismus**, *falls φ zusätzlich bijektiv ist. Wir schreiben $G \cong H$ (G ist isomorph zu H), falls ein Isomorphismus mbox $\varphi : G \to H$.*
$\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ ist Isomorphismus } \}$ *heißt die* **Automorphismengruppe** *von G.*

Klar: Ist φ Gruppenhomomorphismus, so ist $\varphi(1) = 1$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Beispiel: $\kappa : G \to \mathrm{Aut}(G), g \mapsto \kappa_g$, wobei $\kappa_g(x) := gxg^{-1}$ für alle $x \in G$ ist ein Homomorphismus. Sein Bild heißt auch die Gruppe der **inneren Automorphismen** $\mathrm{Inn}(G)$ von G.

Definition 2.2. *Sei G eine Gruppe.*
(a) Eine Untergruppe $N \leq G$ heißt **Normalteiler** *in G, falls $gNg^{-1} = N$ für alle $g \in G$. In Zeichen $N \trianglelefteq G$.*
(b) Die Untergruppe N heißt **charakteristisch** *in G, falls $\alpha(N) = N$ für alle $\alpha \in \mathrm{Aut}(G)$. In Zeichen N char G.*
(c) Das **Zentrum** *ist $Z(G) := \{g \in G \mid gh = hg \text{ für alle } g \in G\} = \mathrm{Kern}(\kappa)$.*
(d) Die **Kommutatoruntergruppe** *ist*

$$G' := \langle [g,h] = g^{-1}h^{-1}gh \mid g, h \in G \rangle.$$

Bemerkung 2.3. *(a) N char $G \Rightarrow N \trianglelefteq G$, denn für $g \in G$ ist $\kappa_g : x \mapsto gxg^{-1}$ ein Automorphismus von G.*
(b) Das Zentrum und die Kommutatoruntergruppe sind charakteristische Untergruppen von G.
(c) Ist $\varphi : G \to H$ ein Homomorphismus, so ist $\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = 1\} \trianglelefteq G$ und $\mathrm{Bild}(\varphi) \leq H$.
(d) Ist $\mathrm{Syl}_p(G) = \{P\}$ so ist P char G.

Satz 2.4. *Sei G eine Gruppe, $N \trianglelefteq G$ und U char N, dann ist $U \trianglelefteq G$.*

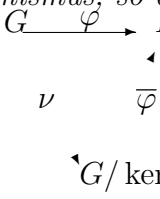
BEWEIS: Sei $g \in G$. Dann ist die Abbildung $\kappa_g : N \to N, n \mapsto gng^{-1}$ ein Automorphismus von N (da $N \trianglelefteq G$). Also ist $\kappa_g(U) = gUg^{-1} = U$ für alle $g \in G$. □

Gegenbeispiel: Achtung: $U \trianglelefteq N \trianglelefteq G$ impliziert nicht unbedingt $U \trianglelefteq G$.
Sei $G = D_8 = \langle (1,2,3,4), (1,4)(2,3) \rangle$, $U = \langle (1,4)(2,3) \rangle \trianglelefteq \langle (1,4)(2,3), (1,3)(2,4) \rangle = N$. Dann ist $N \trianglelefteq G$ und $U \trianglelefteq N$, aber U kein Normalteiler von G.

Hauptsatz 2.5. *(Homomorphiesatz)*

(i) *Sei G eine Gruppe, N ein Normalteiler von G, dann ist G/N eine Gruppe mit $gNhN := ghN$ für alle h, g in G und die Abbildung $\nu : G \to G/N : g \mapsto gN$ ist ein Epimorphismus (G/N heißt die* **Faktorgruppe** *von G nach N und ν der* natürliche Epimorphismus*).*

(ii) *Falls die Abbildung $\varphi : G \to H$ ein Gruppenhomomorphismus ist, dann ist der Kern von φ ein Normalteiler von G, und $\overline{\varphi} : G/\ker\varphi \to H : g \ker\varphi \mapsto \varphi(g)$ ist ein Monomorphismus, so dass*



kommutiert, d.h. $\varphi = \overline{\varphi} \circ \nu$; insbesondere gilt: $\mathrm{Bild}(\varphi) \cong G/\ker(\varphi)$.

Beispiel: $\mathrm{Inn}(G) \cong G/Z(G)$.

Satz 2.6. *Sei G ein p-Gruppe ungleich $\{1\}$, d.h. $|G| = p^\alpha$ mit $\alpha \in \mathbb{Z}_{>0}$ und p eine Primzahl. Dann gilt:*

(i) $Z(G) \neq \{1\}$

(ii) *Ist $N \trianglelefteq G$ und $N \neq \{1\}$, dann ist $N \cap Z(G) \neq \{1\}$.*

(iii) $G' \neq G$

BEWEIS:

(i) folgt aus (ii), falls $N = G$.

(ii) G operiert auf N durch Konjugation. Somit ist $1 < p^\beta = |N| = \sum l_i$ (l_i = Bahnlänge = p^{α_i} mit p^{α_i} teilt $|G|$). Da $1^G = \{1\}$, ist ein $\alpha_{i_0} = 0$, und damit sind noch mehr $p^{\alpha_i} = 1$. Die Vereinigung dieser Bahnen bilden den Schnitt des Zentrums von G mit N.

(iii) Sei G ein Gegenbeispiel kleinster Ordnung. Dann ist $G/Z(G)$ *kein* Gegenbeispiel, da die Ordnung des Zentrums von G größer als 1 ist, also gilt $|G/Z(G)| = 1$ oder $(G/Z(G))' \neq G/Z(G)$. Im ersten Fall ist G abelsch, also $G' = 1$. Dies ist ein Widerspruch dazu, daß G Gegenbeispiel ist. Im zweiten Fall folgt aus $(G/Z(G))' = \langle [aZ(G), bZ(G)] \mid a, b \in G \rangle \neq G/Z(G)$, daß $G'Z(G) \neq G$ und damit insbesondere $G' \neq G$,was ein Widerspruch ist.

□

Bemerkung 2.7. *Sei G eine beliebige Gruppe. Falls $G/Z(G)$ zyklisch ist, ist G abelsch.*

BEWEIS: $G/Z(G) = \langle aZ(G)\rangle$. Sei $g \in G$, dann ist $g = a^i z$ für ein $z \in Z(G)$; $i \in \mathbb{Z}$.

$$\left.\begin{array}{rclcl} a^i z a^j \tilde{z} & = & a^i a^j z\tilde{z} & = & a^{i+j} z\tilde{z} \\ a^j \tilde{z} a^i z & = & a^j a^i \tilde{z} z & = & a^{j+i} z\tilde{z} \end{array}\right\} \text{ Aus der Gleichheit folgt die Behauptung.}$$

□

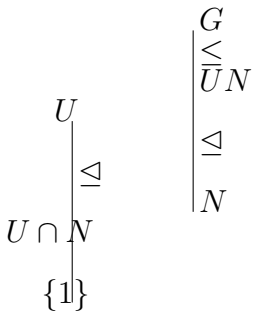
2.2 Der Noethersche Isomorphiesatz und semidirekte Produkte.

Satz 2.8. *(**Noetherscher Isomorphiesatz**) Sei G eine Gruppe, $N \trianglelefteq G$ und $U \leq G$. Dann gilt:*

(i) $N \cdot U = \{nu | n \in N, u \in U\} \leq G$

(ii) $N \trianglelefteq NU$

(iii) $N \cap U \trianglelefteq U$



(iv) $NU/N \cong U/N \cap U$

BEWEIS:

(i) $(NU)(NU)^{-1} = NUUN = NUN = NNU = NU$

(ii) ist trivial.

(iv) $\varphi : U \to G/N : u \mapsto uN$ ist ein Homomorphismus.

$$\left.\begin{array}{l} \text{Bild}(\varphi) = UN/N \\ \ker\varphi = U \cap N \end{array}\right\} \text{ impliziert mit Satz 2.5: } UN/N \cong U/U \cap N$$

(iii) folgt aus $\ker\varphi = U \cap N$.

□

Definition 2.9. *Seien G_1, G_2 Gruppen. Dann wird $G_1 \times G_2$ zu einer Gruppe mit komponentenweiser Multiplikation: $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$ für alle $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$. das äußere* **direkte Produkt** *von G_1 und G_2.*

Satz 2.10. *Seien $N_1, N_2 \trianglelefteq G$ mit $N_1 \cap N_2 = \{1\}$ und $N_1 \cdot N_2 = G$. Dann gilt:*
$G \cong N_1 \times N_2$
Bezeichnung: G heißt dann **inneres direktes Produkt** *von N_1 und N_2.*

BEWEIS: Als Übung. □

Beispiel: Falls G eine Gruppe der Ordnung 35 ist, dann ist G abelsch:
$|Syl_5(G)| \equiv 1 \bmod 5$, $|Syl_5(G)|$ teilt 7, also gilt $|Syl_5(G)| = 1$.
Analog folgt: $|Syl_7(G)| = 1$. Also: die Sylowgruppen sind Normalteiler, deren Schnitt das 1-Element ist, hier insbesondere sind die Sylowgruppen abelsch, da zyklisch. Dann ist G das innere direkte Produkt der beiden zyklischen Sylowuntergruppen und damit auch abelsch.

Satz 2.11. *(i) Sei G eine Gruppe, U eine Untergruppe und N ein Normalteiler von G mit $U \cap N = \{1\}$ und $NU = G$. Dann läßt sich jedes Element g in G eindeutig schreiben als $g = nu$ mit $u \in U$; $n \in N$, und es gilt: $(n_1u_1)(n_2u_2) = (n_1\ {}^{u_1}n_2)(u_1u_2)$.*
Insbesondere ist $\varphi : G \to U : nu \mapsto u$ ein Epimorphismus mit $\ker \varphi = N$; d.h.: G/N ist isomorph zu U. (G heißt (inneres) semidirektes Produkt *von N mit U, in Zeichen $G = N \rtimes U = U \ltimes N$.)*

(ii) Gegeben seien die Gruppen U und N und ein Homomorphismus $\alpha : U \to \mathrm{Aut}(N)$. Schreibweise: ${}^{u}n := \alpha(u)(n)$ $(n \in N, u \in U, \alpha(u) \in \mathrm{Aut}(N))$. Dann gilt:
Auf der Produktmenge $N \times U$ ist ein Produkt definiert durch:
$(n_1, u_1)(n_2, u_2) = (n_1\alpha(u_1)(n_2), u_1u_2)$, so dass eine Gruppe vorliegt.
Bezeichnung: Äußeres semidirektes Produkt *von N mit U vermöge $\alpha : U \quad N$ (ist auch wieder inneres semidirektes Produkt von $\overline{N} := \{1\} \times N$ mit $\overline{U} := U \times \{1\}$).*

BEWEIS: Als Übung. □

Beispiel: Alle Gruppen der Ordnung 20.

2.3 Untergruppenverbände.

Definition 2.12. **(i)** *Sei M eine Menge, $\leq$ eine Relation auf M (also $\leq \subseteq M \times M$). Eine* **partiell geordnete Menge** *ist ein Paar $(M, \leq)$, sodaß gilt:*

- **(a)** *Falls: $a \leq b$ und $b \leq a$, dann folgt $a = b$.*
- **(b)** *Falls: $a \leq b$ und $b \leq c$, dann folgt $a \leq c$.*
- **(c)** *$a \leq a$ für alle $a \in M$.*

(ii) *Sei $(M, \leq)$ eine partiell geordnete Menge, $A \subseteq M$.*
$m \in M$ heißt **kleinste obere Schranke** *von A ("Supremum" von A), falls $a \leq m$ für alle a in A und: aus $a \leq n$ für alle a in A folgt $m \leq n$. (Falls das Supremum existiert, ist es eindeutig bestimmt.)*
Analog: Infimum A

(iii) *Ein* **Verband** *ist eine partiell geordnete Menge $(M, \leq)$, sodaß für je zwei Elemente $m, n \in M$ sowohl* $\sup(\{m, n\})$ *(Bez.: $m \cup n$) als auch* $\inf(\{m, n\})$ *(Bez.: $m \cap n$) existieren.*

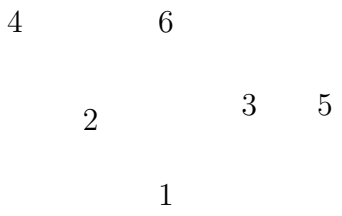
(iv) *Sei $(M, \cap, \cup)$ ein Verband. $N \subseteq M$ heißt ein* **Teilverband***, falls $n_1 \cup n_2 \in N$ und $n_1 \cap n_2 \in N$ für alle $n_1, n_2 \in N$.*
Bem.: *N ist wieder ein Verband.*

(v) *Seien N, M Verbände. $\varphi : M \to N$ heißt* **Verbandshomomorphismus***, falls $\varphi(a \cap b) = \varphi(a) \cap \varphi(b)$ und $\varphi(a \cup b) = \varphi(a) \cup \varphi(b)$ für alle $a, b \in M$.*
φ heißt Verbandsisomorphismus, falls φ ein bijektiver Homomorphismus ist und φ^{-1} auch ein Verbandshomomorphismus ($a \leq b$ genau dann, wenn $\varphi(a) \leq \varphi(b)$).

Beispiele 3.

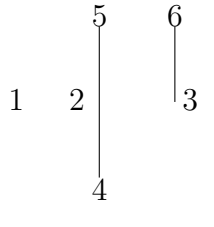
a) Sei $M = \{1, 2, 3, 4, 5, 6\}$ $a \leq b$ heißt z.B. übliches "kleiner gleich". $(M, \leq)$ ist ein Verband.

b) M wie oben; $a \leq b$ genau dann, wenn a teilt b. Diagramm:



In diesem Fall ist $(M, \leq)$ kein Verband, nur eine partielle Ordnung, da $\sup(\{4, 6\})$ nicht existiert.

c) Sei M wieder wie oben:



d.h.:

$\leq$	1	2	3	4	5	6
1	$\vee$				$\vee$	
2		$\vee$			$\vee$	$\vee$
3			$\vee$		$\vee$	$\vee$
4	$\vee$	$\vee$	$\vee$	$\vee$	$\vee$	$\vee$
5					$\vee$	
6						$\vee$

Dies ist kein Verband, da das Supremum von 2 und 3 nicht eindeutig ist.

Satz 2.13. (i) *Sei $(M, \leq)$ ein Verband. Dann gilt:*

(V_1) $a \cup b = b \cup a$ *und* $a \cap b = b \cap a$

(V_2) $(a \cup b) \cup c = a \cup (b \cup c)$ *und* $(a \cap b) \cap c = a \cap (b \cap c)$

(V_3) $a \cup a = a$ *und* $a \cap a = a$

(V_4) $(a \cup b) \cap a = a$ *und* $(a \cap b) \cup a = a$

(ii) *Auf M seien $\cup$ und $\cap$ definiert, so daß (V_1)-(V_4) gelten. Dann ist $(M, \leq)$ ein Verband mit $a \leq b$, genau dann, wenn $a \cap b = a$ (genau dann, wenn $a \cup b = b$).*

BEWEIS:

(i) folgt sofort aus der Definition.

(ii) Zeige: Aus $a \cap b = a$ folgt $a \cup b = b$. Aus $a \cap b = a$ folgt: $a \cup b = (a \cap b) \cup b \overset{(V_4)}{=} b$. Die Umkehrung ist ebenso klar. Zeige also weiter: Aus $a \leq b$ und $b \leq a$ folgt $a = b$. Da $a \leq b$ und $b \leq a$ folgt $a \cap b = a$ bzw. $a \cap b = b$. Zur Transitivität: Sei $a \leq b$ und $b \leq c$. D.h., $a \cap b = a$ und $b \cap c = b$. Daraus folgt: $a \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a$. Also ist $\leq$ transitiv und $(M, \leq)$ damit eine partiell geordnete Menge. Es verbleibt zu zeigen: $a \cap b = \inf(a, b)$ bzw. $a \cup b = \sup(a, b)$. Sei $x \leq a$ und $x \leq b$. Daraus folgt: $x \cap a = x$ und $x \cap b = x$ und somit: $x \cap (a \cap b) = (x \cap a) \cap b = x \cap b = x$. Also gilt: $x \leq a \cap b$. Ebenso folgt die Aussage für das Supremum.

□

BEISPIELE 4.

a) Sei M ein Verband, $a, b \in M$, und es gelte $a \leq b$. $[a, b] = \{x \in M \mid a \leq x \leq b\}$ wird als "Intervall" bezeichnet. Dies ist wieder ein Verband (Teilverband).

b) Sei $\tilde{M}$ eine Menge. $(\mathrm{Pot}(\tilde{M}), \cap, \cup)$ ist ein Verband. ($\cap$ und $\cup$ bedeuten hier die mengentheoretische Vereinigung bzw. den mengentheoretischen Schnitt.)

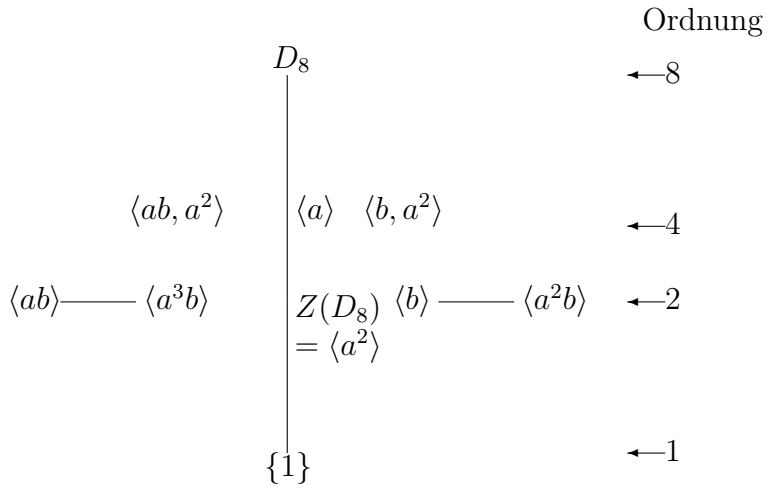
c) Sei G eine Gruppe, $\mathcal{U}(G) = \{U \mid U \leq G\}$. Dann ist $(\mathcal{U}(G), \cap, \langle\ ,\ \rangle)$ ein Verband, wo $U \leq V$ bedeutet U ist Untergruppe von V. Beweis über $\leq$:
Die kleinste Untergruppe, die U_1 und U_2 enthält, ist $\langle U_1, U_2 \rangle$. (! Beachte: $\mathcal{U}(G)$ ist kein Teilverband von $\mathrm{Pot}(G)$, obwohl $\leq$ in beiden Fällen eine Inklusion ist.)

d) Sei G eine Gruppe, $\mathcal{N}(G) = \{N \mid N \trianglelefteq G\}$. $(\mathcal{N}(G), \leq)$ ist ein Teilverband von $(\mathcal{U}(G), \leq)$, denn: Seien $N_1, N_2 \trianglelefteq G$. Dann ist $N_1 \cap N_2 \trianglelefteq G$ und $\langle N_1, N_2 \rangle = N_1 N_2 \trianglelefteq G$.

2.14. Folgerung aus dem Homomorphiesatz: *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann induziert φ einen Verbandsisomorphismus $\hat{\varphi}$ von $[\ker\varphi, G]$ $(\subseteq \mathcal{U}(G))$ auf $\mathcal{U}(\mathrm{Bild}(\varphi))(= [\{1\}, \mathrm{Bild}(\varphi)] \subseteq \mathcal{U}(H)$, welcher zusätzlich folgendes erfüllt: $\hat{\varphi}(U^g) = (\hat{\varphi}(U))^{\varphi(g)}$. $(\hat{\varphi} : U \mapsto \varphi(U) = \{\varphi(u) \mid u \in U\}.)$*

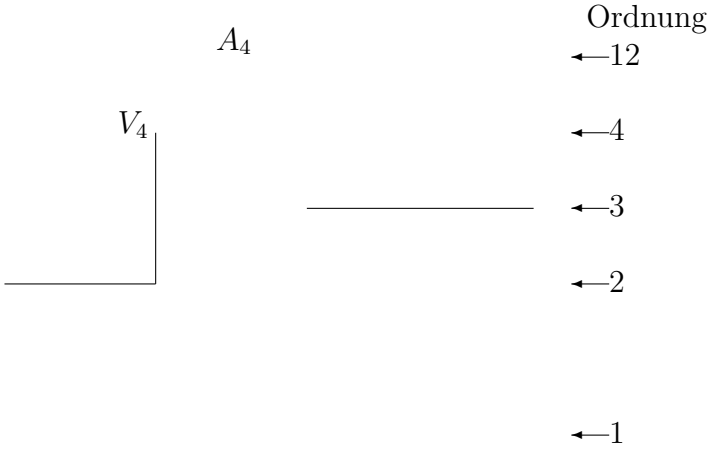
BEISPIELE 5.

a) Der Untergruppenverband der D_8:
$D_8 = \langle a = (1,2,3,4), b = (1,4)(2,3) \rangle$
$D_8 \to D_8/Z(D_8) \cong C_2 \times C_2$



Bedeutung der waagerechten Linien: konjugiert.

b) Der Untergruppenverband der A_4:
$A_4 \trianglerighteq V_4 = \langle (1,2)(3,4), (1,3)(2,4)\rangle \cong C_2 \times C_2$; $\{V_4\} = Syl_2(A_4)$;
$Syl_3(A_4) = \{\langle (1,2,3)\rangle, \langle (1,2,4)\rangle, \langle (1,3,4)\rangle, \langle (2,3,4)\rangle\}$



Es ist dazu zu zeigen: Falls U eine Untergruppe der A_4 ist, dann ist die Ordnung von U ungleich 6. Dazu gibt es z.B. folgende Beweismöglichkeiten:

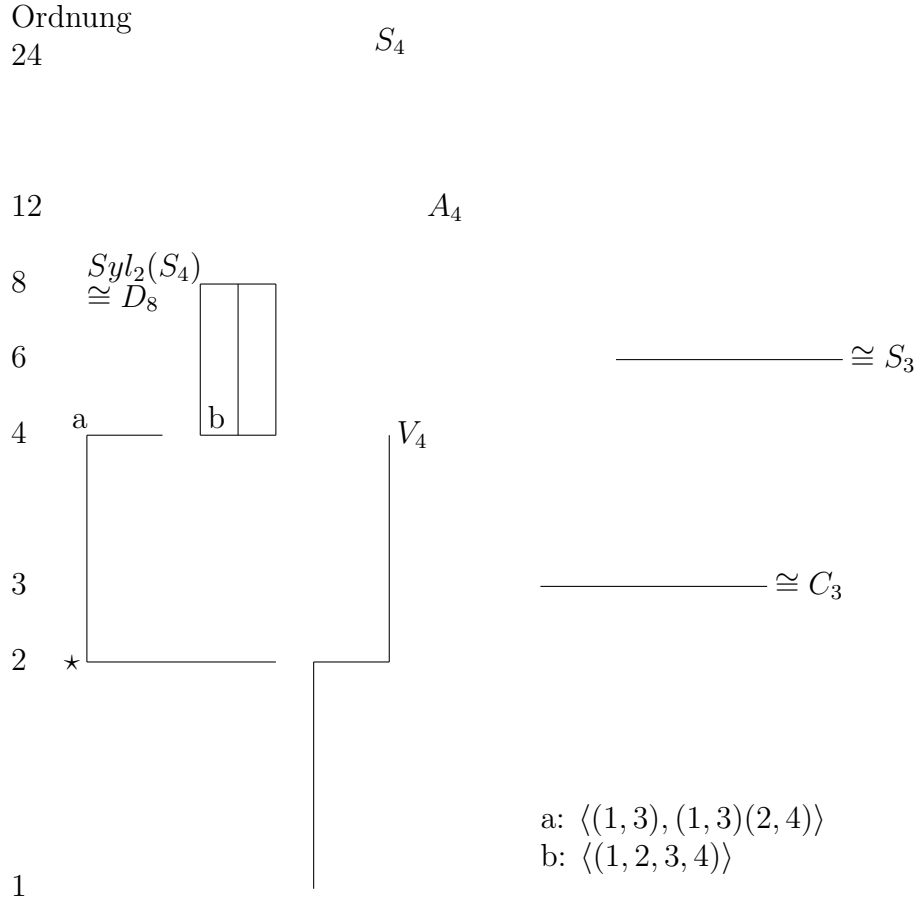
(i) Falls U die Ordnung 6 hat, dann ist U ein Normalteiler der A_4, und damit ist $A_4' = V_4$ Teilmenge von U. Dies ist jedoch eine Widerspruch, da $|V_4| = 4$ nicht die Ordnung von U teilt.

(ii) Sei $|U| = 6$. Wenn X eine 3-Sylowuntergruppe von U ist, dann ist X Normalteiler in U, und X ist eine 3-Sylowuntergruppe der A_4. Damit ist U eine Untergruppe von $N_{A_4}(X)$, aber $N_{A_4}(\langle (1,2,3)\rangle) = \langle (1,2,3)\rangle$, was der Annahme $|U| = 6$ widerspricht.

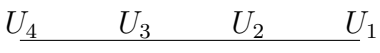
c) Der Untergruppenverband der S_4:
V_4 ist Normalteiler in S_4. S_4/V_4 ist isomorph zu S_3. Sei $U \leq S_4$, $U \not\leq A_4$, $|U| \neq 2^\alpha$, dann ist $U/(U \cap A_4) \cong C_2$. Kandidaten für $U \cap A_4$ sind die 3-Sylowuntergruppen der A_4. U ist in $N_{S_4}(U \cap A_4)$ enthalten, da die A_4 Normalteiler in S_4 ist. $N_{S_4}(\langle (1,2,3)\rangle) = \langle (1,2,3), (1,2)\rangle \cong S_3$

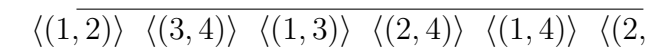
Dies kann man auch anders erkennen:

$$|Syl_3(S_4)| = 4 \text{ genau dann, wenn } \frac{|S_4|}{N_{S_4}(\langle(1,2,3)\rangle)|} = \frac{24}{6} = 4.$$



Die konjugierten Untergruppen $\star$ sind Untergruppen der Untergruppen, die isomorph zur S_3 sind. Der Übersicht halber sind die Verbindungslinien in obigem Schaubild nicht eingezeichnet, sondern in einem eigenen Diagramm aufgeführt (U_i bedeutet die symmetrische Gruppe auf $\{1,2,3,4\}\backslash\{i\}$ für $i = 1,\ldots,4\}$):





2.4 Kompositionsreihen und der Satz von Jordan-Hölder.

Definition 2.15. (i) *Es sei Ω eine Menge. Eine Gruppe G heißt* **Ω-Gruppe** *(Gruppe mit Operatorenbereich Ω, Operatorgruppe), falls eine Abbildung $\Omega \times G \to G,\ (\omega, g) \mapsto \omega(g)$ gegeben ist mit $\omega(gh) = \omega(g)\omega(h)$, für alle $g, h \in G,\ \omega \in \Omega$. Mit anderen Worten: Jedes $\omega \in \Omega$ operiert auf G wie ein Endomorphismus von G.*

(ii) *Sind G, H Ω-Gruppen, so heißt eine Abbildung $\varphi : G \to H$* **Ω-Homomorphismus**, *falls φ ein Gruppenhomomorphismus ist mit $\varphi(\omega(g)) = \omega(\varphi(g))$, für alle $g \in G, \omega \in \Omega$.*

(iii) *Es sei G eine Ω-Gruppe. Eine Untergruppe U von G heißt* **Ω-(zulässige) Untergruppe**, *falls $\omega(u) \in U$, für alle $u \in U, \omega \in \Omega$. (Dann ist U auch eine Ω-Gruppe bezüglich der Restriktion der gegebenen Operation.) Schreibweise: $U \underset{\Omega}{\leq} G$.*

Beispiele 6.

a) Jede Gruppe ist eine $\emptyset$-Gruppe.

b) Es sei K ein Körper und V ein K-Vektorraum. Dann ist V eine K-Gruppe, die linearen Abbildungen sind K-Homomorphismen, und die K-zulässigen Untergruppen sind die Teilräume von V. (Beachte: Nicht jede abelsche K-Gruppe ist auch ein K-Vektorraum.)

c) Es sei G eine Gruppe und $\Omega = G$. Durch die Definition $\omega(g) := \omega g \omega^{-1}$ (Konjugation), für $g \in G, \omega \in \Omega = G$, wird G eine Ω-Gruppe. Die Ω-zulässigen Untergruppen sind die Normalteiler von G.

d) Es sei G eine Gruppe, $\Omega = \mathrm{Aut}(G)$. Dann ist G eine Ω-Gruppe durch Abbildung. Die $\mathrm{Aut}(G)$-zulässigen Untergruppen sind die charakteristische Untergruppen.

e) Es seien V_1,V_2 K-Vektorräume, φ_i sei eine lineare Abbildung von V_i nach V_i für $i = 1, 2$. Ω sei $K \cup \{\star\}$, V_i ist Ω-Gruppe mit $\star(v_i) = \varphi_i(v_i)$ für $v \in V_i$. Die Ω-zulässigen Untergruppen sind die Teilräume U_i von V_i mit $\varphi_i(U_i) \subseteq U_i$. $\psi : V_1 \to V_2$ ist ein Ω-Homomorphismus, genau dann, wenn ψ linear ist und gilt: $\psi \circ \varphi_1 = \varphi_2 \circ \psi$.

2.16. Faktorgruppe und Homomorphiesatz

(i) *Es sei G eine Ω-Gruppe und N ein Ω-zulässiger Normalteiler von G. Dann ist G/N eine Ω-Gruppe mit $\omega(gN) := \omega(g)N$ für alle $g \in G, \omega \in \Omega$, und $\nu : G \to G/N : g \mapsto gN$ ist ein Ω-Epimorphismus.*

(ii) *Es seien G, H Ω-Gruppen und $\varphi : G \to H$ ein Ω-Homomorphismus. Dann ist* $\ker\varphi$ *ein Ω-Normalteiler von G,* Bild φ *ist eine Ω-Untergruppe von H, und $\tilde{\varphi} : G/\ker\varphi \to$* Bild $\varphi,\ g\ker\varphi \mapsto \varphi(g)$ *ist ein Ω-Isomorphismus.*

2.17. Isomorphiesätze

(i) *Es sei U eine Ω-Untergruppe von G und N ein Ω-Normalteiler. Dann ist UN eine Ω-Untergruppe von G, $U \cap N$ ist Ω-Normalteiler von U und es gilt: $UN/N \underset{\Omega}{\cong} U/(U \cap N)$.*

(ii) *Es sei $\varphi : G \to H$ ein surjektiver Ω-Homomorphismus von Ω-Gruppen. Wir bezeichnen mit $[\ker\varphi, G]_\Omega$ diejenigen Ω-Untergruppen von G welche $\ker\varphi$ enthalten, und mit $\mathcal{U}_\Omega(H)$ die Menge der Ω-Untergruppen von H. Dann induziert φ eine Bijektion*

$$[\ker\varphi, G]_\Omega \to \mathcal{U}_\Omega(H),\ U \mapsto \varphi(U),$$

deren Umkehrabbildung gegeben ist durch

$$\mathcal{U}_\Omega(H) \to [\ker\varphi, G]_\Omega,\ V \mapsto \varphi^{-1}(V).$$

Ferner gilt für $N \in [\ker\varphi, G]_\Omega$: $N \underset{\Omega}{\trianglelefteq} G \iff \varphi(N) \underset{\Omega}{\trianglelefteq} H$, und dann induziert φ einen $\Omega-$Isomorphismus $G/N \to H/\varphi(N)$.

(iii) *Es seien N_1, N_2 Ω-Normalteiler von G mit $N_1 \subseteq N_2$. Dann gilt: N_2/N_1 ist Ω-Normalteiler von G/N_1 und $(G/N_1)/(N_2/N_1) \underset{\Omega}{\cong} G/N_2$. (Kürzungssatz)*

Beispiele 7.

a) Es sei N ein Ω-Normalteiler einer Ω-Gruppe G. Dann sind die Ω-Untergruppen von G/N genau die Faktorgruppen U/N, wobei $U \in [N, G]_\Omega$, und die Zuordnung $U \mapsto U/N$ liefert eine Bijektion zwischen $[N, G]_\Omega$ und $\mathcal{U}_\Omega(G/N)$.

b) Es sei $m \in \mathbb{N}$. Dann ist $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, und die Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ sind genau die Faktorgruppen $k\mathbb{Z}/m\mathbb{Z}$, wobei $k \in \mathbb{N}_0$ und $k|m$.

c) Es sei $V_4 := \langle (12)(34), (14)(23)\rangle \leq S_4$. Dann gilt $[V_4, S_4] = \{S_4, M_1, M_2, M_3, A_4, V_4\}$, wobei M_1, M_2, M_3 die 2-Sylow-Untergruppen von S_4 seien. Dann sind die Untergruppen von S_4/V_4 gerade die Faktorgruppen $S_4/V_4, A_4/V_4, M_1/V_4, M_2/V_4, M_2/V_4, M_3/V_4$ und $V_4/V_4 = \{1\}$, und die Normalteiler sind $S_4/V_4, A_4/V_4$ und $\{1\}$.

Definition 2.18. (i) *Eine Ω-Gruppe $G \neq \{1\}$ heißt* **Ω-einfach**, *falls gilt: Ist U ein Ω-Normalteiler von G, dann ist $U = \{1\}$ oder $U = G$.*

(ii)

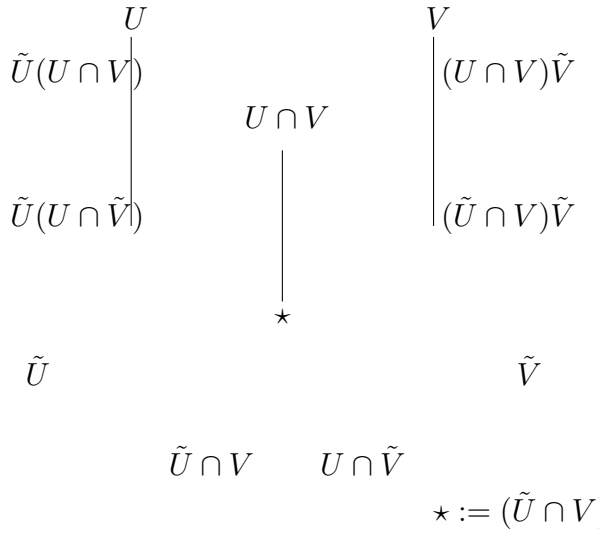
$$G = G_0 \underset{\Omega}{\trianglerighteq} G_1 \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} G_r = \{1\}$$

heißt eine **Ω-Subnormalreihe** *von G. (Beachte: $G_i \underset{\Omega}{\trianglelefteq} G_{i-1}$, aber nicht notwendigerweise gilt $G_i \underset{\Omega}{\trianglelefteq} G$.)*

(iii) *Eine Ω-Subnormalreihe für die gilt, G_{i-1}/G_i ist Ω-einfach, heißt eine* **Ω-Kompositionsreihe**.

2.19. Schmetterlingslemma von H. Zassenhaus: *Sei G eine Ω-Gruppe und $\tilde{U}, U, \tilde{V}, V$ Ω-Untergruppen von G, und es gelte: $\tilde{U} \underset{\Omega}{\trianglelefteq} U$ und $\tilde{V} \underset{\Omega}{\trianglelefteq} V$. Dann folgt:*

$$\tilde{U}(U \cap V)/\tilde{U}(U \cap \tilde{V}) \underset{\Omega}{\cong} (U \cap V)\tilde{V}/(\tilde{U} \cap V)\tilde{V}$$



BEWEIS: Nach dem Isomorphiesatz (i) sind $\tilde{U} \cap V$ und $U \cap \tilde{V}$ jeweils Ω-Normalteiler von $U \cap V$, und es gibt Ω-Isomorphismen:

$$\begin{aligned} \varphi &: {}^{U \cap V}/_{\tilde{U} \cap V} \longrightarrow {}^{\tilde{U}(U \cap V)}/_{\tilde{U}}, \\ \psi &: {}^{U \cap V}/_{U \cap \tilde{V}} \longrightarrow {}^{(U \cap V)\tilde{V}}/_{\tilde{V}}. \end{aligned}$$

Ferner ist auch $\star = (\tilde{U} \cap V)(U \cap \tilde{V})$ ein Ω-Normalteiler von $U \cap V$, und es gilt:

$$\begin{aligned} \varphi\left({}^{\star}/_{\tilde{U} \cap V}\right) &= {}^{\star\tilde{U}}/_{\tilde{U}} = {}^{\tilde{U}(U \cap \tilde{V})}/_{\tilde{U}} \\ \psi\left({}^{\star}/_{U \cap \tilde{V}}\right) &= {}^{\star\tilde{V}}/_{\tilde{V}} = {}^{(\tilde{U} \cap V)\tilde{V}}/_{\tilde{V}} \end{aligned}$$

Also induziert φ einen Ω-Isomorphismus ${}^{\tilde{U}(U \cap V)}/_{\tilde{U}(U \cap \tilde{V})} \overset{\cong}{\underset{\Omega}{}} {}^{U \cap V}/_{\star}$,
und ψ induziert einen Ω-Isomorphismus ${}^{(U \cap V)\tilde{V}}/_{(\tilde{U} \cap V)\tilde{V}} \overset{\cong}{\underset{\Omega}{}} {}^{U \cap V}/_{\star}$. □

Satz 2.20. Verfeinerungssatz von Schreier-Zassenhaus *Es sei G eine Ω-Gruppe.*

$$\begin{aligned} (\star) &: G = G_0 \underset{\Omega}{\trianglerighteq} G_1 \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} G_r = \{1\} \text{ und} \\ (\star\star) &: G = H_0 \underset{\Omega}{\trianglerighteq} H_1 \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} H_s = \{1\} \end{aligned}$$

seien Ω-Subnormalreihen. Dann definieren

$$G_{i,j} = G_i(G_{i-1} \cap H_j) \text{ und } H_{i,j} = H_j(H_{j-1} \cap G_i)$$

Verfeinerungen von $(\star)$ *und* $(\star\star)$*:*

$$\begin{aligned}(\star') \quad &: \quad G = G_{1,0} \underset{\Omega}{\trianglerighteq} G_{1,1} \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} G_{1,s} = G_{2,0} \underset{\Omega}{\trianglerighteq} G_{2,1} \underset{\Omega}{\trianglerighteq} \ldots G_{2,s} = G_{3,0} \underset{\Omega}{\trianglerighteq} \ldots \\ &\quad \underset{\Omega}{\trianglerighteq} G_{r,0} \underset{\Omega}{\trianglerighteq} G_{r,1} \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} G_{r,s} = \{1\} \\ (\star\star') \quad &: \quad G = H_{0,1} \underset{\Omega}{\trianglerighteq} H_{1,1} \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} H_{r,1} = H_{0,2} \underset{\Omega}{\trianglerighteq} H_{1,2} \underset{\Omega}{\trianglerighteq} \ldots H_{r,2} = H_{0,3} \underset{\Omega}{\trianglerighteq} \ldots \\ &\quad \underset{\Omega}{\trianglerighteq} H_{0,s} \underset{\Omega}{\trianglerighteq} H_{1,s} \underset{\Omega}{\trianglerighteq} \ldots \underset{\Omega}{\trianglerighteq} H_{r,s} = \{1\}\end{aligned}$$

mit

$$G_{i,j-1}/G_{i,j} \underset{\Omega}{\cong} H_{i-1,j}/H_{i,j},$$

d.h. die Faktorgruppen von $(\star')$ *und* $(\star\star')$ *sind nach Umnumerierung paarweise isomorph.*

BEWEIS: Aus Satz 2.19 folgt, daß dies Ω-zulässige Untergruppen sind: $H_j \cap G_i \underset{\Omega}{\trianglerighteq} H_{j+1} \cap G_{i-1}$. Daraus folgt: $G_{i,j} = G_i(G_{i-1} \cap H_j) \underset{\Omega}{\trianglerighteq} G_i(G_{i-1} \cap H_{j+1}) = G_{i,j+1}$, d.h.: $G_{i,j-1}/G_{i,j} = G_i(G_{i-1}/H_{j-1})/G_i(G_{i-1} \cap H_j)$. Nach Satz 2.19 ist dies isomorph zu: $H_j(G_{i-1} \cap H_{j-1})/H_j(G_i \cap H_{j-1}) = H_{i-1,j}/H_{i,j}$ □

Satz 2.21. Jordan-Hölder: *Es sei* G *eine* Ω*-Gruppe und* $G = G_0 \underset{\Omega}{\triangleright} G_1 \underset{\Omega}{\triangleright} \ldots \underset{\Omega}{\triangleright} G_r = \{1\}$ *eine* Ω*-Kompositionsreihe (d.h.,* G_i/G_{i+1} *sind einfache* Ω*-Gruppen), und sei* $G = H_0 \underset{\Omega}{\triangleright} H_1 \underset{\Omega}{\triangleright} \ldots \underset{\Omega}{\triangleright} H_s = \{1\}$ *eine weitere* Ω*-Kompositionsreihe. Dann ist* $r = s$*, und es existiert ein* $\pi \in S_r$*, sodaß* G_i/G_{i+1} Ω*-isomorph zu* $H_{\pi(i)}/H_{\pi(i)+1}$ *ist.*

BEWEIS: Wenn man in Satz 2.20 die trivialen Faktoren wegläßt, so erhält man: $r = s$. Die Isomorphie erhält man dadurch, daß keine der beiden Subnormalreihen verfeinert werden kann. □

BEISPIELE 8.

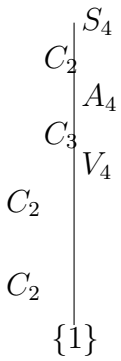
a) Sei $G = C_6$, $\Omega = \emptyset$.

$C_6 = \langle a \rangle$

$\langle a^3 \rangle$ (3 / 2) $\langle a^2 \rangle$ (2 / 3)

$\{1\}$

b) Sei $G = S_4$, $\Omega = \emptyset$



Die Ω-Kompositionsfaktoren sind: C_2, C_3, C_2, C_2.

c) Sei $G = S_4$, $\Omega = S_4$ und Ω operiere durch Konjugation. Dann sind die Ω-Kompositionsfaktoren: C_2, C_3, V_4. (Zu C_3: A_4 operiert trivial, $S_4 - A_4$ invertiert.)

d) Sei V ein K-Vektorraum und φ eine lineare Abbildung von V nach V. Sei $\Omega = K \cup \{\star\}$ $(V\star : V \to \varphi(V))$, und alle Eigenwerte von φ seien in K. Dann erhält man folgende Kompositionsreihe:
$V = V_n \overset{\geq}{K} V_{n-1} \overset{\geq}{K} \ldots$ mit $\varphi(V_i) \subseteq V_i$, und $\dim V_i = i$. Eine zweite Kompositionsreihe liefert dieselben Eigenwerte in anderer Reihenfolge.

Beachte: Kompositionsreihen existieren nicht immer; z.B.: $G = \mathbb{Z}$, $\Omega = \emptyset$. Eine endliche Ω-Gruppe besitzt aber stets eine Ω-Kompositionsreihe.

Definition 2.22. *Ω-Kompositionsreihen heißen:*
Kompositionsreihen, *falls $\Omega = \emptyset$;*
Hauptreihen, *falls $\Omega = G$ (und Ω operiert durch Konjugation.);*
charakteristische Reihen, *falls $\Omega = \mathrm{Aut}(G)$.*

2.5 Auflösbare Gruppen.

Definition 2.23. (i) *Für eine Gruppe G setzt man induktiv*

$$G^{(0)} := G,\ G^{(k)} := (G^{(k-1)})'\ (k \in \mathbb{N}).$$

Man nennt $G^{(k)}$ die k-te Kommutatorgruppe (oder k-te derivierte Gruppe) von G. Die Reihe $G = G^{(0)} \geq G' \geq G^{(2)} \geq G^{(3)} \geq \ldots$ heißt **Kommutatorreihe** *von G.*

(ii) *G heißt* **auflösbar**, *falls $G^{(k)} = \{1\}$ für ein $k \in \mathbb{N}$.*

(iii) *G heißt* **perfekt**, *falls $G' = G$ (d.h. $G^{(k)} = G$ für alle $k \in \mathbb{N}$).*

Bemerkung: Eine abelsche Gruppe ist stets auflösbar (denn die erste Kommutatorgruppe ist trivial.) Eine nicht-abelsche einfache Gruppe ist stets perfekt (denn die Kommutatoruntergruppe ist Normalteiler). Es gibt auch nicht-einfache perfekte Gruppen, z.B. $SL_2(\mathbb{Z}/5\mathbb{Z})$.

Lemma 2.24. *Es sei G eine Gruppe.*

(i) *Für jeden Homomorphismus $\varphi : G \to H$ und $k \in \mathbb{N}$ gilt: $\varphi(G^{(k)}) = (\varphi(G))^{(k)}$.*

(ii) $G^{(k)}$ char G *für alle* $k \in \mathbb{N}_0$.

(iii) *Ist G endlich, so gibt es ein $k \in \mathbb{N}_0$ mit $G^{(k+1)} = G^{(k)}$. Dann ist $G^{(k)}$ perfekt und $G/G^{(k)}$ ist auflösbar.*

BEWEIS:

(i) Zunächst gilt für $a, b \in G$ stets $\varphi([a,b]) = [\varphi(a), \varphi(b)]$. Daraus folgt sofort

$$\varphi(G') = \varphi(\langle\{[a,b] |\ a,b \in G\}\rangle) = \langle\{[\varphi(a),\varphi(b)] |\ a,b \in G\}\rangle = (\varphi(G))'.$$

Der allgemeine Fall folgt dann durch Induktion.

(ii) Sei $\sigma \in \mathrm{Aut}(G)$. Dann ist nach (i) $\sigma(G^{(k)}) = (\sigma(G))^{(k)} = G^{(k)}$. Daher ist $G^{(k)}$ charakteristische Untergruppe von G, also auch Normalteiler von G.

(iii) Da die Kommutatorreihe absteigend ist und G endlich ist, muß es ein solches $k \in \mathbb{N}$ geben. Dann ist $G^{(k)}$ perfekt. Ferner gilt für den kanonischen Epimorphismus $\nu : G \to G/G^{(k)}$ nach Teil (i):

$$(G/G^{(k)})^{(k)} = \nu(G)^{(k)} = \nu(G^{(k)}) = G^{(k)}/G^{(k)} = \{1\}.$$

□

Satz 2.25. *Eine Gruppe G ist auflösbar genau dann, wenn es eine Subnormalreihe*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

von G gibt mit abelschen Faktorgruppen $G_{i-1}/G_i,\ i = 1 \ldots r$.

BEWEIS: Zuerst sei G auflösbar, d.h. $G^{(k)} = \{1\}$ mit minimalem $k \in \mathbb{N}_0$. Dann ist die Kommutatorreihe $G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(k)} = \{1\}$ eine Subnormalreihe von G, und die Faktorgruppen $G^{(i-1)}/G^{(i)}$ sind abelsch. Umgekehrt sei nun eine Subnormalreihe wie oben gegeben von G. Dann ist $G'_{i-1} \subseteq G_i$ für jedes $i \in \{1, \ldots r\}$ und damit induktiv $G^{(i)} \subseteq G_i$. Insbesondere ist dann $G^{(r)} = \{1\}$, d.h. G ist auflösbar. □

Definition 2.26. *Eine endlich erzeugte abelsche Gruppe G heißt* elementar abelsch*, falls es eine Primzahl p gibt mit $x^p = 1$ für alle $x \in G$.*

Bemerkung 2.27. *Die endlichen elementar abelschen Gruppen sind von der Form $(C_p)^n = \underbrace{C_p \times \ldots \times C_p}_{n \text{ mal}}$. Es ist $\mathrm{Aut}(C_p^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$ und C_p^n ist einfach als $\mathrm{Aut}(C_p^n)$-Gruppe.*

Lemma 2.28. *Es sei G eine endliche auflösbare Gruppe, die als $Aut(G)$-Gruppe einfach ist. Dann ist G elementar abelsch.*

BEWEIS: G' ist eine charakteristische Untergruppe von G. Nach Voraussetzung ist $G' = G$ oder $G' = \{1\}$. Da G' auflösbar ist, kann unmöglich $G' = G$ gelten, also ist $G' = \{1\}$, d.h. G ist abelsch. Es sei p ein Primteiler von $|G|$, und S eine p-Sylow-Untergruppe von G. Dann ist $S \trianglelefteq G$ und daher sogar S charakteristisch in G. Nach Voraussetzung folgt $S = G$, d.h. G ist eine $p-$Gruppe. Schließlich ist $G^p := \{g^p |\ g \in G\}$ eine charakteristische Untergruppe von G. Ist $g \in G$ ein Element maximaler Ordnung in G, so kann g nicht in G^p liegen. Daher ist $G^p = \{1\}$, d.h. G ist elementar abelsch (mit Exponent p). □

Satz 2.29. *Endliche p-Gruppen sind auflösbar.*

BEWEIS: Es sei G ein "kleinster Verbrecher", d.h. eine nicht auflösbare p-Gruppe minimaler Ordnung. Nach Satz 4.6 ist $G' \neq G$. Dann ist G' eine p-Gruppe von kleinerer Ordnung als G und folglich auflösbar. Dann ist auch G auflösbar. □

Satz 2.30. *Es sei G eine endliche Gruppe. Dann sind folgende Aussagen äqivalent:*

(i) *G ist auflösbar.*

(ii) *Jeder Kompositionsfaktor von G ist zyklisch von Primzahlordnung.*

(iii) *Jeder Hauptfaktor von G ist elementar abelsch*

BEWEIS: Aus (i) folgt (ii):
Man verfeinere die Kommutatorreihe zu einer Kompositionsreihe. Dann ist jeder Kompositionsfaktor H isomorph zu einer Faktorgruppe einer Untergruppe einer Faktorgruppe der Kommutatorreihe. Also ist H endlich, abelsch und einfach. Es sei p ein Primteiler von $|H|$. Dann gibt es eine Untergruppe U von H der Ordnung p. Da H einfach ist, folgt $H = U$, d.h. $|H| = p$ und H ist zyklisch.
Aus (i) folgt (iii):
Jeder Hauptfaktor H von G ist Faktorgruppe einer Untergruppe von G, also auflösbar nach dem folgenden Lemma. Die charakteristischen Untergruppen von H sind auch G-zulässige Untergruppen von H, also trivial. Daher ist H einfach als $\mathrm{Aut}(H)$-Gruppe. Dann folgt die Behauptung aus dem vorangehenden Lemma.
Aus (ii) oder (iii) folgt (i):
Das folgt sofort aus Satz 2.25 □

Beispiel: Die S_4

S_4
|
$A_4 = S_4'$
|
$V_4 = A_4'$ ← verfeinert zu Kompositionsreihe
|
$\{1\} = V_4$

Die Kommutatorreihe ist Hauptreihe,

Die Kompositionsfaktoren sind C_2, C_3, C_2 und C_2. Die Hauptfaktoren sind C_2, C_3 und $C_2 \times C_2$. S_4 ist auflösbar.

Lemma 2.31. *Es sei G eine Gruppe*

(i) *Ist G auflösbar, so auch jede Untergruppe und Faktorgruppe von G.*

(ii) *Ist $N \trianglelefteq G$, und sind N und G/N auflösbar, so ist auch G auflösbar.*

BEWEIS:

(i) Es gelte $G^{(k)} = \{1\}$. Ist U eine Untergruppe von G, so folgt $U^{(i)} \subseteq G^{(i)}$ für alle $i \in \mathbb{N}$ und damit $U^{(k)} = \{1\}$. Ist N ein Normalteiler von G, so betrachte man den kanonischen Epimorphismus $\nu : G \to G/N$. Dann ist $(G/N)^{(k)} = (\nu(G))^{(k)N/N} = \nu(G^{(k)})N/N = \{1\}$.

(ii) Es gibt $k, n \in \mathbb{N}$ mit $N^{(k)} = \{1\}$ und $(G/N)^{(n)} = \{1\}$. Es sei $\nu : G \to G/N$ der kanonische Epimorphismus. Dann ist $\{1\} = (G/N)^{(n)} = \nu(G^{(n)})$, d.h. $G^{(n)} \subseteq N$. Dann folgt $G^{(n+k)} = (G^{(n)})^{(k)} \subseteq N^{(k)} = \{1\}$, also $G^{(n+k)} = \{1\}$.

□

Beispiel: $D_{2n} = \langle a, \tau \rangle \leq S_n$ mit $a = (1, 2, \ldots, n)$ und $\tau(i) = n + 1 - i,\ i = 1, \ldots n$. Dann ist $D_{2n} = \langle a \rangle \rtimes \langle \tau \rangle$, und $\langle a \rangle$ sowie $D_{2n}/\langle a \rangle \cong \langle \tau \rangle$ sind auflösbar. Nach Lemma 2.31 ist daher auch D_{2n} auflösbar.

2.6 Der Satz von Schur-Zassenhaus.

Satz 2.32. *(Spezialfall von Schur-Zassenhaus) Sei G endlich $N \trianglelefteq G$ abelsch,* $\mathrm{ggT}([G : N], |N|) = 1$. *Dann gibt es eine Untergruppe $U \leq G$ mit $N \cap U = 1$ und $G = NU$. Eine solche Untergruppe heißt auch* **Komplement** *von N in G. Je zwei Komplemente sind in N konjugiert.*

Beweis. Sei $\mathcal{S} := \{R \subset G \mid G = \dot{\cup}_{r \in R} Nr\}$ die Menge aller Transversalen von N in G. Zu zeigen: Es gibt ein $R \in \mathcal{S}$ mit $R \leq G$.
G operiert auf $\mathcal{S}$ durch $(g, R) \mapsto gR = \{gr \mid r \in R\}$.
Für $R, T \in \mathcal{S}$ setze

$$\frac{R}{T} := \prod_{Nr = Nt} rt^{-1} \in N$$

Dann gilt für $g \in G$, $n \in N$

$$\frac{gR}{gT} = g\frac{R}{T}g^{-1} \text{ und } \frac{nR}{T} = n^{[G:N]}\frac{R}{T}.$$

Setze $R \sim T$ genau dann wenn $\frac{R}{T} = 1$. Dann ist $\sim$ eine G-verträgliche Äquivalenzrelation auf $\mathcal{S}$. G operiert also auf den Äquivalenzklassen. Da $\mathrm{ggT}(|N|, [G : N]) = 1$ ist jedes $n \in N$ eine $[G : N]$-te Potenz und es gilt sogar, dass N transitiv auf der Menge der Äquivalenzklassen operiert. Sei $[R]$ eine Äquivalenzklasse und $U = \mathrm{Stab}_G([R])$ der Stabilisator in G von $[R]$. Dann ist $U \leq G$ eine Untergruppe und

$$U \cap N = \{n \in N \mid [nR] = [R]\} = \{h \in N \mid h^{[G:N]} = 1\} = \{1\}.$$

Aus der Transitivität von N auf $\{[T] \mid T \in \mathcal{S}\}$ folgt $G = NU$.
Ist H eine weitere solche Untergruppe. Dann ist $H \in \mathcal{S}$ und $H \leq \mathrm{Stab}_G([H])$ und aus Ordnungsgründen folgt die Gleichheit. Also $H = nUn^{-1}$, wobei $n \in N$ mit $[H] = [nR]$. □

Satz 2.33. *(Schur-Zassenhaus) Sei G endlich $N \trianglelefteq G$, $\mathrm{ggT}([G:N],|N|) = 1$. Dann besitzt N ein Komplement in G.*

Beweis. Sonst sei G ein Gegenbeispiel minimaler Ordnung und $N \trianglelefteq G$ ein Normalteiler mit $\mathrm{ggT}([G:N],|N|) = 1$, so dass N kein Komplement besitzt.
Sei p ein Primteiler von $|N|$ und $P \in \mathrm{Syl}_p(N)$.
1. Schritt. $G = N_G(P)N$ (das ist das übliche Frattini-Argument).
Denn für jedes $g \in G$ ist $gNg^{-1} = N$ und daher $gPg^{-1} \in \mathrm{Syl}_p(N)$. Nach den Sylowsätzen gibt es also ein $n \in N$ mit $gPg^{-1} = nPn^{-1}$ und damit $n^{-1}g \in N_G(P)$.
2. Schritt. $P \trianglelefteq G$:
Denn es ist

$$G/N = N_G(P)N/N \cong N_G(P)/N_G(P) \cap N = G_1/N_1$$

mit $N_1 := N_G(P) \cap N$ und $G_1 := N_G(P)$. Dann ist $\mathrm{ggT}([G_1 : N_1], |N_1|) = 1$. Ist nun $G_1 \neq G$, so besitzt N_1 nach Induktionsvoraussetzung ein Komplement H_1 mit $G_1 = N_1H_1$, $N_1 \cap H_1 = \{1\}$. Es gilt $|H_1| = [G_1 : N_1] = [G : N]$ (s.o) und $N \cap H_1 = N_1 \cap H_1 = \{1\}$. Also ist H_1 auch ein Komplement von N in G, ein Widerspruch. Daher $N_G(P) = G$ und $P \trianglelefteq G$. Insbesondere ist $\mathrm{Syl}_p(N) = \{P\}$.
Zusammenfassung. Wir haben also gezeigt, dass N das direkte Produkt seiner p-Sylowgruppen ist. Die Kommutatoruntergruppe N' von N ist also auch das direkte Produkt der Kommutatoruntergruppen P' aller Sylowgruppen von N, insbesondere $\neq N$.
3. Schritt: Anwendung von Satz 2.32.
Nach der Zusammenfassung ist $N' \neq N$ eine echte Untergruppe von N. Da N' *char* N ist $N' \trianglelefteq G$ und wir gehen über zu

$$G_2 := G/N', N_2 := N/N', G_2/N_2 \cong G/N (\text{Kürzungssatz}).$$

Weiter ist N_2 ein abelscher Normalteiler von G_2, hat also nach Satz 2.32 ein Komplement $H_2 = U/N'$ in G_2 für eine Untergruppe $U \leq G$ mit $N' = U \cap N \leq U$. Dann ist

$$|H_2| = [G_2 : N_2] = [G : N] \text{ teilerfremd zu } |N| \text{ insbesondere also zu } |N'|.$$

Also ist $N' \trianglelefteq U$, $[U : N']$ teilerfremd zu $|N'|$ und $|U| = |H_2||N'| = [G : N]|N'| < |G|$. Nach Induktionsvoraussetzung hat also N' ein Komplement H in $U = HN'$. Dann ist $HN = G$ und $H \cap N = \{1\}$ also H ein Komplement von N in G. □

Satz 2.34. *(Zusatz zu Satz 2.33) Seien G, N wie in Satz 2.33. Ist N oder G/N auflösbar, so sind alle Komplemente von N in G konjugiert.*

Beachte: Der Satz von Feit und Thompson sagt aus, dass alle Gruppen ungerader Ordnung auflösbar sind. Da $|N|$ oder $|G/N|$ ungerade ist, ist diese zusätzliche Voraussetzung an die Auflösbarkeit also überflüssig.
Beweis. Wieder per Induktion nach $|G|$. Seien H und H_1 Komplemente von N in G und $1 \neq M \trianglelefteq N$ ein minimaler Normalteiler von G. Dann sind HM/M und H_1M/M Komplemente von N/M in G/M und nach Induktionsvoraussetzung gibt es also ein $g \in G$ mit $HM = gH_1g^{-1}M$. Dann sind aber H und gH_1g^{-1} Komplemente von M in HM und nach

Induktion in HM konjugiert, falls $M \neq N$.
Wir können also annehmen, dass N selbst ein minimaler Normalteiler von G ist. Ist N auflösbar, so ist N elementar abelsch nach Lemma 2.28 insbesondere also abelsch und die Behauptung folgt aus Satz 2.32.
Ist G/N auflösbar, so hat G einen Normalteiler A mit $N < A < G$ und $|G/A| = p$ Primzahl. Sind H, H_1 Komplemente von N in G, so sind $H \cap A$ und $H_1 \cap A$ Komplemente von N in A. Nach Induktionsvoraussetzung sind $H \cap A$ und $H_1 \cap A$ in A konjugiert, also Œ $H \cap A = K = H_1 \cap A$. Es ist K ein Normalteiler von H und H_1 und $|H/K| = |H_1/K| = p$. Seien P, P_1 p-Sylowgruppen von H bzw. H_1. Dann ist $KP = H$ und $KP_1 = H_1$. Weiter sind P und P_1 sogar p-Sylowgruppen von G, da $[G : H] = [G : H_1] = |N|$ nicht durch p teilbar ist. Also $P, P_1 \in \mathrm{Syl}_p(N_G(K))$ und es gibt ein $g \in N_G(K)$ mit $gP_1g^{-1} = P$. Für dieses g ist dann aber $gH_1g^{-1} = H$. □

Kapitel 3

Galoistheorie.

3.1 Galoiserweiterungen

Wiederholung: Eine algebraische Körpererweiterung E/K heißt **normal**, falls für jeden K-Algebrenhomomorphismus $\varphi : E \to \overline{E} \cong \overline{K}$ in einen algebraischen Abschluss von E gilt, dass $\varphi(E) = E$ ist. Da man K-Automorphismen von E zu K-Automorphismen von $\overline{K}$ fortsetzen kann (Lemma 1.34) liefert also die Einschränkung einen Gruppenepimorphismus

$$\mathrm{Aut}_K(\overline{K}) \to \mathrm{Aut}_K(E), \varphi \mapsto \varphi_{|E}.$$

Der Kern dieses Epimorphismus ist $\mathrm{Aut}_E(\overline{E})$ ein Normalteiler in $\mathrm{Aut}_K(\overline{K})$ und es gilt

$$\mathrm{Aut}_K(E) \cong \mathrm{Aut}_K(\overline{K})/\mathrm{Aut}_E(\overline{K}).$$

Eine Erweiterung E/K ist genau dann normal, wenn jedes Minimalpolynom eines Elements von E in $E[t]$ in Linearfaktoren zerfällt.

Eine algebraische Körpererweiterung E/K heißt **separabel**, falls das Minimalpolynom eines jeden Elements von E in $\overline{K}[t]$ in paarweise verschiedene Linearfaktoren zerfällt. Für jedes $a \in E$ gilt also $\mathrm{ggT}(\mu_a, \mu_a') = 1$.

Eine endliche Erweiterung E/K ist genau dann separabel, wenn

$$[E : K] = [E : K]_s = |\mathrm{Hom}_K(E, \overline{K})|.$$

Folgerung 3.1. *Eine endliche Körpererweiterung E/K ist genau dann normal und separabel wenn $|\mathrm{Aut}_K(E)| = [E : K]$.*

Definition 3.2. *Sei M ein Monoid und K ein Körper. Ein Homomorphismus $\lambda : M \longrightarrow K^*$ heißt* **Charakter** *(von M über K).*

Satz 3.3. (Artin) *Sei M ein Monoid und K ein Körper. Je n verschiedene Charaktere über K sind linear unabhängig (als Elemente von K^M).*

Beweis: Induktion über n: $n = 1$: klar
$n - 1 \to n$: Seien $\sigma_1, \ldots, \sigma_n$ Charaktere. Ann.: $\sigma_1, \ldots, \sigma_n$ sind linear abhängig. Dann existieren $a_i \in K$ mit nicht alle $a_i = 0$, sodaß gilt:

$$* : \ a_1\sigma_1(m) + \ldots + a_n\sigma_n(m) = 0 \text{ für alle } m \in M.$$

Mit der Induktionsannahme folgt $a_i \neq 0$ für alle i . Sei nun $m_0 \in M$. Setzt man nun $m_0 m$ für m in $*$ ein und bildet zum anderen $\sigma_1(m_0)*$, so erhält man nach Bildung der Differenz:

$$-\left\{\begin{array}{l} a_1\sigma_1(m_0)\sigma_1(m)+ \quad \ldots \quad \ldots..\ldots+a_n\sigma_n(m_0)\sigma_n(m)=0 \\ a_1\sigma_1(m_0)\sigma_1(m)+a_2\sigma_1(m_0)\sigma_2(m)) + \ldots+a_n\sigma_1(m_0)\sigma_n(m)=0 \end{array}\right.$$

$$\underbrace{a_1(\sigma_1(m_0)-\sigma_1(m_0))\sigma_1(m)}_{=0}+\ldots\ldots\ldots+\underbrace{a_n(\sigma_n(m_0)-\sigma_1(m_0))}_{\text{neueKoeff.}}\sigma_n(m)=0 \qquad \text{für alle } m \in M$$

Nun sind $\sigma_2, \ldots, \sigma_n$ linear unabhängig (nach Ind.Ann). Damit gilt: $a_i(\sigma_i(m_0) - \sigma_1(m_0)) = 0$ für alle $i = 1, \ldots, n$. Da die a_i alle ungleich 0 sind, folgt $\sigma_i(m_0) = \sigma_1(m_0)$ für alle $i = 1, \ldots, n$. $m_0 \in M$ war beliebig gewählt, also gilt: $\sigma_i = \sigma_1$. Dies ist ein Widerspruch. □

Folgerung 3.4. *Sei L/K eine separable Körpererweiterung vom Grad n und* $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ *Für $(v_1, \ldots, v_n) \in L^n$ gilt:*

$$(v_1, \ldots, v_n) \text{ ist } K\text{-Basis von } L \Leftrightarrow \det((\sigma_i(v_j))_{i,j=1}^n) \neq 0.$$

Beweis. als Übung. □

Hauptsatz 3.5. *Sei E ein Körper und $G \leq \mathrm{Aut}(E)$.*
Sei $K = Fix_G(E) := \{k \in E | gk = k$ für alle $g \in G\}$ der Fixkörper von G.
Dann gilt: $[E : K] = |G|$.

Beweis: Sei $r := [E : K]$ und $n := |G|$.
Sei zunächst $r < \infty$. Dann ist $E = K[a_1, \ldots, a_d]$ für gewisse $a_i \in E$. Jeder K-Automorphismus von E ist durch die Bilder der a_i eindeutig bestimmt. Ist m_i der Grad des Minimalpolynoms von a_i über K, so gibt es höchstens m_i mögliche Bilder von a_i in E. Also gilt $n = |G| \leq |\mathrm{Aut}_K(E)| \leq m_1 \cdot \ldots \cdot m_d < \infty$.
(i) Zeige $r \geq n$.
Annahme: $r < n$. Dann ist $n < \infty$. Nun fasst man $g \in G$ als Charakter auf $g : E^* \longrightarrow E^*,\ x \mapsto gx$. Sei $(a_1, \ldots, a_r)$ eine K-Basis von E. Dann ist

$$\sum_{g \in G} x_g(ga_i) = 0 \text{ für } i = 1, \ldots, r \tag{3.1.1}$$

ein lineares homogenes Gleichungssystem in x_g über E mit r Gleichungen und $n = |G| > r$ Unbekannten. Damit existiert eine nichttriviale Lösung $(x_g)_{g \in G}$. Da alle Elemente in E K-Linearkombinationen der a_i sind und G aus K-linearen Abbildungen besteht, gilt $\sum_{g \in G} x_g g = 0$ (als lineare Abbildung von E nach E). Also ist G linear abhängig, was einen Widerspruch zu Satz 3.3 impliziert.
(ii) Zeige $n \geq r$. Sei nun o.B.d.A. n endlich (d.h., $|G| < \infty$).

$$S : E \longrightarrow K : a \mapsto \sum_{g \in G} ga \text{ ist eine K-lineare Abbildung. Nach 3.3 ist } S \neq 0.$$

Zeige nun: Sind $a_1, \ldots, a_{n+1} \in E$, so sind $(a_1, \ldots, a_{n+1})$ linear abhängig über K.
Bew.:$*$: $\sum_{i=1}^{n+1} x_i(g^{-1}a_i) = 0$ mit $g \in G$ ist ein homogenes lineares Gleichungssystem in x_i

über E mit $|G| = n$ Gleichungen und $n+1$ Unbekannten. Also existiert eine nichtriviale Lösung von $* :(x_1, \ldots, x_{n+1})$. O.B.d.A. sei $S(x_1) \neq 0$ (durch eine Permutation der Indizes wird erreicht, daß $x_1 \neq 0$ und durch Multiplikation mit einem geeigneten Element aus E wird erreicht, daß $S(x_1) \neq 0$) Nun bildet man $g *$und summiert anschließend über alle $g \in G$. Man erhält:

$$\sum_{g\in G}\sum_{i=1}^{n+1} a_i g(x_i) = \sum_{i=1}^{n+1} a_i \underbrace{S(x_i)}_{\in K} = 0 \text{ mit } S(x_1) \neq 0$$

Also sind $(a_1, \ldots, a_{n+1})$ linear abängig über K . □

Folgerung 3.6. *Seien die Voraussetzungen wie bei 3.5 mit $|G| < \infty$. Dann gilt:*
$G = \mathrm{Aut}_K(E)$.

Beweis: Falls $G < \mathrm{Aut}_K(E)$, so wendet man 3.5 auf $\tilde{G} = \mathrm{Aut}_K(E)$ an. Sei nun $\tilde{K}$ der $\tilde{G}$-Fixkörper: $|G| = [E : K] \overset{K\subseteq\tilde{K}}{\geq} [E : \tilde{K}] \overset{3.5}{=} |\tilde{G}| > |G|$. Dies ist ein Widerspruch, also gilt: $\tilde{G} = G$. □

Folgerung 3.7. *Sei E/K eine endliche Körpererweiterung und $G = \mathrm{Aut}_K(E)$, so gilt:*

(i) $|G| \leq [E : K]$

(ii) $|G| = [E : K]$ *genau dann, wenn* $K = Fix_G(E)$.

Beweis: $\tilde{K} := Fix_G(E) \supseteq K$, also gilt $[E : K] \geq [E : \tilde{K}] \overset{3.5}{=} |G|$. □

Definition 3.8. *Eine endliche Körpererweiterung (E/K) heißt* **galoissch**, *falls* $|\mathrm{Aut}_K(E)| = [E : K]$. *Dann heißt $G = Gal(E/K) := \mathrm{Aut}_K(E)$ die* **Galoisgruppe** *von E über K.*

Satz 3.9. *Für eine endliche Körpererweiterung E/K sind äquivalent:*

(1) E/K ist Galoiserweiterung.

(2) E/K ist normal und separabel, also Zerfällungskörper eines separablen Polynoms.

(3) $K = \mathrm{Fix}_G(E)$ für eine endliche Untergruppe G von $\mathrm{Aut}(E)$.

Beweis: (1) ⇔ (2) ist Folgerung 3.1.
(3) ⇒ (2): Sei $a \in E$. Betrachte die Bahn von a unter G.

$$Ga = \{a = a_1, \ldots, a_n\}.$$

Das Polynom $p_a(x) := \prod_{i=1}^{n}(x - a_i) \in E[x]$ ist invariant unter der Operation von G auf $E[x]$ vermöge $g(\sum b_i x^i) := \sum g(b_i)x^i$ liegt also im Fixring $K[x]$ (da $\mathrm{Fix}_G(E) = K$). Insbesondere zerfällt das Minimalpolynom von a über K (welches ja p_a teilt) in paarweise verschiedene Linearfaktoren in $E[x]$. Damit ist E normal und separabel.
(1) ⇒ (3): Folgt aus Folgerung 3.7 □

Folgerung 3.10. *Sei E/K galoissch mit Galoisgruppe G. Ist $a \in E$, so operiert G transitiv auf den Nullstellen des Minimalpolynoms von a über K. Der Stabilisator ist die Galoisgruppe von E über $K[a]$,*

$$\mathrm{Stab}_G(a) = Gal(E/K[a])$$

.

Hauptsatz 3.11. Fundamentalsatz der Galois-Theorie: *Sei (E/K) Galoiserweiterung und $G = \mathrm{Aut}_K(E)$. Dann gilt:*

(i) $|G| = [E : K]$

(ii) $\begin{array}{rcl} \Phi : \mathcal{U}(G) = \{U | U \leq G\} & \longrightarrow & \mathcal{Z}(K,E) = \{F | F \text{ ist ein Körper und } K \leq F \leq E\} \\ U & \mapsto & Fix_U(E) \end{array}$

ist eine inklusionsumkehrende Ähnlichkeit, wobei G auf $\mathcal{U}$ durch Konjugation und auf $\mathcal{Z}(K,E)$ durch Anwenden operiert.

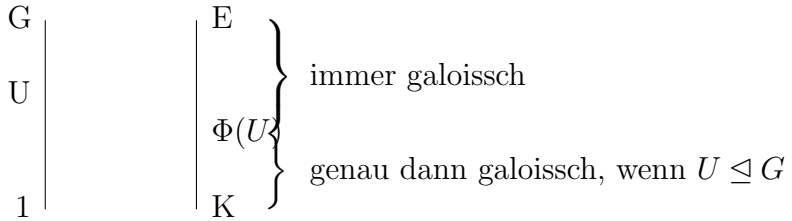
BEWEIS:

(i) Dies ist sofort klar.

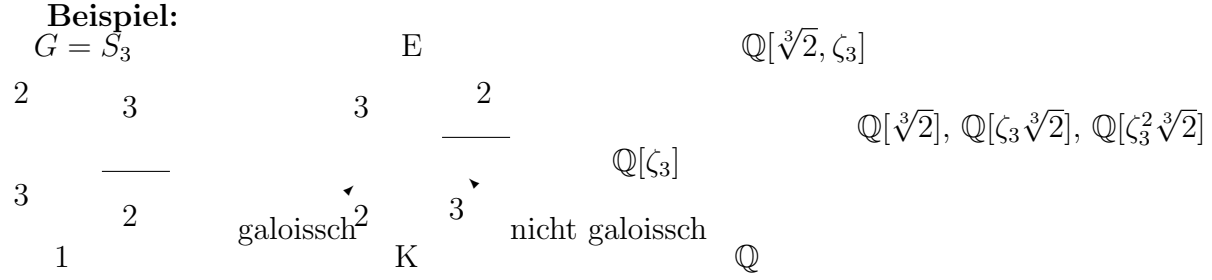
(ii) Zeige: Φ ist injektiv.
Sei $U_i \leq G$ mit $\Phi(U_1) = \Phi(U_2)$. Ersetzt man U_2 durch $\langle U_1, U_2 \rangle$ (beachte $\Phi(\langle U_1, U_2 \rangle) = \Phi(U_2)$), so kann man o.B.d.A. annehmen, dass $U_1 \leq U_2$. Außerdem gilt: $|U_1| = [E : \Phi(U_1)] = [E : \Phi(U_2)] = |U_2|$. Also gilt: $U_1 = U_2$.
Zeige: Φ ist surjektiv.
Ist $F \in \mathcal{Z}$, so ist E/F galoissch, denn E ist Zerfällungskörper eines separablen Polynoms $f(t) \in K[t] \subset F[t]$. Setze $U := \mathrm{Aut}_F(E) \leq \mathrm{Aut}_K(E)$. Dann ist $F = \Phi(U)$.
Dass Φ G-verträglich ist, folgt wegen $\mathrm{Fix}_{gUg^{-1}}(E) = g(\mathrm{Fix}_U(E))$.
Die inklusionsionsumkehrende Eigenschaft folgt sofort.

□

Folgerung 3.12. *Mit den Bezeichnungen aus 3.11 gilt:*
$U \leq G$ genau dann ein Normalteiler von G, wenn $(\Phi(U)/K)$ galoissch ist. Dann ist $Gal_K(\Phi(U)) \cong G/U$ vermöge Einschränken.
(E/F) ist galoissch für alle $F \in \mathcal{Z}(K,E)$.



Beispiel:



Folgerung 3.13. *(Satz vom primitiven Element) Sei (E/K) endlich und separabel. Dann existiert ein $a \in E$ mit $E = K[a]$. (a heißt ein* **primitives Element***.)*

BEWEIS: Ist $|K| < \infty$, so folgt dies aus dem Struktursatz für endliche Körper (jeder Erzeuger von K^* ist ein solches primitives Element). Sei also $|K| = \infty$. Zwischen E und K liegen nur endlich viele Zwischenkörper, also wird die Behauptung für jedes $a \in E \backslash \{$endlich viele Zwischenkörper$\}$ erfüllt. □

Satz 3.14. *Sei E/K eine Körpererweiterung und L, M Zwischenkörper von E/K. Das* **Kompositum** *von L und M ist der kleinste Teilkörper LM von E, der L und M enthält.*
Sei jetzt L/K galoissch.

(a) LM/M und $L/M \cap L$ sind galoissch.

(b) Die Einschränkungsabbildung $\rho : \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K), g \mapsto g_{|L}$ ist injektiv mit Bild $\rho(\mathrm{Gal}(LM/M)) = \mathrm{Gal}(L/M \cap L)$.

(c) $[LM : M]$ teilt $[L : K]$.

Beweis. (a) Da L/K endlich und separabel ist, sind auch $L/M \cap L$ und LM/M endlich und separabel. Für $L/M \cap L$ ist dies klar, für LM/M benutzt man, dass jede K-Basis $(b_1, \ldots, b_n)$ von L auch ein M-Erzeugendensystem von LM ist. Weiter sind die Minimalpolynome aller b_i über K separabel, also auch die der b_i über M, somit LM/M endlich und separabel.
Zur Normalität: Da L normal ist über K ist es auch normal über jedem Zwischenkörper von L/K, also auch über $L \cap M$. Der Erweiterungskörper LM von M wird über M von endlich vielen Elementen $a_1, \ldots, a_n \in L$ erzeugt. Dann enthält L also auch alle Nullstellen von $\mu_{a_i,K}$ und somit auch alle Nullstellen von $\mu_{a_i,M}$. D.h. LM/M ist normal. Aus endlich, normal und separabel folgt somit galoissch.
(b) Sei also L/K galoissch. Dann ist die Einschränkungsabbildung ρ wohldefiniert, da für jedes $g \in \mathrm{Gal}(LM/M)$ gilt, dass $g(L) = L$ ist (da L/K normal ist). Weiter ist $\mathrm{Kern}(\rho) = \{g \in \mathrm{Gal}(LM/M) \mid g_{|L} = id\}$. Da immer $g_{|M} = id$ für $g \in \mathrm{Gal}(LM/M)$ gilt, folgt somit $g = id$ auf LM. Also ist ρ injektiv. Klar ist $\rho(\mathrm{Gal}(LM/M)) \subset \mathrm{Gal}(L/M \cap L)$, denn jedes $g \in \mathrm{Gal}(LM/M)$ lässt $M \cap L$ punktweise fest. Da M der Fixkörper von $\mathrm{Gal}(LM/M)$ ist, ist $M \cap L$ der Fixkörper der Einschränkung $\rho(\mathrm{Gal}(LM/M))$. Also folgt die Gleichheit.
(c) Nach (b) ist $[LM : M] = |\mathrm{Gal}(LM/M)| = |\mathrm{Gal}(L/M \cap L)|$ ein Teiler von $|\mathrm{Gal}(L/K)| = [L : K]$. □

Beispiel: Die Voraussetzung, dass L/K galoissch ist, ist hier wesentlich: Sei $L = \mathbb{Q}[\sqrt[3]{2}]$ und $M := \mathbb{Q}[\zeta_3\sqrt[3]{2}]$. Dann ist $LM = Zerf_{\mathbb{Q}}(x^3 - 2)$, $[LM : M] = [LM : L] = 2$, $[L \cap M] = \mathbb{Q}$ und $[L : \mathbb{Q}] = [M : \mathbb{Q}] = 3$. Folglich teilt $2 = [LM : M]$ nicht $[L : \mathbb{Q}]$.

Satz 3.15. *Sei E/K eine Körpererweiterung und L, M Zwischenkörper, so dass L/K und M/K galoissch sind. Dann gilt*

(a) LM/K ist galoissch.

(b) $\rho : Gal(LM/K) \to Gal(L/K) \times Gal(M/K), g \mapsto (g_{|L}, g_{|M})$ ist injektiv.

(c) Ist $L \cap M = K$, so ist ρ ein Isomorphismus.

Beweis. (a) Da L/K und M/K endlich, normal und separabel sind, hat auch das Kompositum LM/K diese Eigenschaften.
(b) Da L/K und M/K normal sind, gilt $g(L) = L$ und $g(M) = M$ für alle $g \in \mathrm{Gal}(LM/K)$. Somit ist ρ wohldefiniert. Weiter ist jedes $g \in Ker(\rho)$ die Identität auf L und M also auch auf dem Kompositum LM, also ist ρ injektiv.
(c) Sei nun $L \cap M = K$. Seien $g_L \in \mathrm{Gal}(L/K)$ und $g_M \in \mathrm{Gal}(M/K)$. Dann gibt es nach der vorherigen Satz Abbildungen $g_1 \in \mathrm{Gal}(LM/M)$ und $g_2 \in \mathrm{Gal}(LM/L)$ mit $(g_1)_{|L} = g_L$ und $(g_2)_{|M} = g_M$. Also gilt $\rho(g_1 g_2) = (g_L, g_M)$. □

Ab Hier weitermachen

Definition 3.16. *Eine Galoiserweiterung E/K heißt* **zyklisch** *(bzw.* **abelsch***, bzw.* **auflösbar***) wenn die Galoisgruppe zyklisch (bzw. abelsch, bzw. auflösbar) ist.*

Bemerkung 3.17. *Sei $E > L > K$ ein Körperturm mit E/K galoisch.*

(a) Ist E/K zyklisch oder abelsch, so haben auch die Körpererweiterungen E/L und L/K diese Eigenschaft.

(b) Ist E/K auflösbar, so auch E/L.

(c) Ist L/K ebenfalls galoissch, so ist E/K genau dann auflösbar, wenn E/L und L/K auflösbar sind.

Folgerung 3.18. *Seien $K \subset L, M \subset E$ Körper.*
(a) Ist L/K zyklisch (bzw. abelsch bzw. auflösbar) so auch LM/M.
(b) Sind L/K und M/K abelsch bzw. auflösbar, so auch das Kompositum LM/K.

3.2 Kreisteilungskörper

Bemerkung 3.19. *Die Eulersche φ-Funktion ist definiert durch $\varphi(n) := |\mathbb{Z}/n\mathbb{Z}^*|$, die Anzahl der zu n teilerfremden Zahlen in $\{1, \ldots, n\}$.*

(a) $\varphi(p^r) = p^{r-1}(p-1)$ für Primzahlpotenzen.

(b) $\varphi(nm) = \varphi(n)\varphi(m)$, falls $\mathrm{ggT}(n, m) = 1$.

(c) Für $n \in \mathbb{N}$ ist $n = \sum_{d|n} \varphi(d)$.

Beweis. (a) Abzählen. (b) Chinesischer Restsatz. (c) Aus Definition: Es ist

$$n = |\underline{n}| = \sum_{d|n} |\{i \in \underline{n} \mid \mathrm{ggT}(i, n) = d\}| = \sum_{d|n} |\{\frac{i}{d} \mid i/d \in \underline{n/d}, \mathrm{ggT}(i/d, n/d) = 1\}| = \sum_{d|n} \varphi(\frac{n}{d}).$$

□

Definition 3.20. *Sei K ein Körper und $n \in \mathbb{N}$. Ein Element $\zeta \in K$ heißt n-te Einheitswurzel, falls $\zeta^n = 1$. ζ heißt* **primitive n-te Einheitswurzel***, falls $|\langle\zeta\rangle| = n$ ist. $\mu_n(K) \leq K^*$ sei die Gruppe aller n-ten Einheitswurzeln in K.*

Bemerkung 3.21. *(a) Gilt $char(K) = p > 0$, so hat K^* genau eine p^r-te Einheitswurzel für jedes $r \geq 0$.*

(b) Gilt $char(K) \nmid n$, so ist das Polynom $X^n - 1 \in K[X]$ separabel und sein Zerfällungskörper enthält genau n verschiedene n-te Einheitswurzeln.

(c) Gilt $char(K) \nmid n$, so ist $\mu_n(\overline{K})$ zyklisch der Ordnung n.

(d) Gilt $char(K) \nmid n$, so enthält der Zerfällungskörper von $X^n - 1$ genau $\varphi(n)$ primitive n-te Einheitswurzeln.

(e) $\mathbb{F}_q^* = \mu_{q-1}(\mathbb{F}_q)$.

Beweis. (a) $(X^{p^r} - 1) = (X - 1)^{p^r} \in K[X]$ hat also genau eine Nullstelle, nämlich 1.
(b) Klar. (c) folgt aus (b).
(d) Ist ζ eine primitive n-te Einheitswurzel, so ist $\langle \zeta \rangle = \mu_n(K)$. Weiter ist ζ^a primitiv genau dann wenn $\mathrm{ggT}(n, a) = 1$ also für genau $\varphi(n)$ Werte von a. □

Definition 3.22. *Sei K ein Körper mit $char(K) \nmid n$. Sei E ein Zerfällungskörper von $X^n - 1$ über K und $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in E. Dann heißt*

$$\prod_{i=1}^{\varphi(n)} (X - \zeta_i) =: \Phi_n(X)$$

das n-te **Kreisteilungspolynom**.

Beispiel: $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1 = \frac{X^p - 1}{X - 1}$ für Primzahlen p.

Satz 3.23. *Sei K ein Körper mit $char(K) \nmid n$. $X^n - 1 = \prod_{d|n} \Phi_d$ und $\Phi_n \in R[X]$ mit* $R = \mathbb{Z}1_K = \begin{cases} \mathbb{Z} & char(K) = 0 \\ \mathbb{F}_p & char(K) = p > 0 \end{cases}$.

Beweis. Jede Nullstelle von $X^n - 1$ ist eine primitive d-te Einheitswurzel für ein $d \mid n$. Also teilt $X^n - 1$ die rechte Seite. Diese hat aber wegen $n = \sum_{d|n} \varphi(d)$ genau Grad n, also sind die beiden Polynome gleich.
$\Phi_n \in R[X]$ durch Induktion über n. Für $n = 1$ ist dies klar. Für $n > 1$ ergibt sich dies aus der Formel

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d}.$$

Es ist nämlich $f := \prod_{d|n, d<n} \Phi_d$ nach Induktionsvoraussetzung ein normiertes ganzzahliges Polynom, welches $X^n - 1 \in R[X]$ teilt. □

Satz 3.24. *Sei K ein Körper mit $char(K) \nmid n$. Sei $\zeta_n \in \overline{K}$ eine primitive n-te Einheitswurzel. Dann ist $K[\zeta_n]/K$ galoissch und es gibt einen Monomorphismus*

$$m : \mathrm{Gal}(K[\zeta_n]/K) \to (\mathbb{Z}/n\mathbb{Z})^*, g \mapsto m(g) \text{ wobei } g(\zeta_n) = \zeta_n^{m(g)}$$

Insbesondere ist $K[\zeta_n]/K$ abelsch.

Beweis. Da ζ_n die Gruppe aller n-ten Einheitswurzeln erzeugt, zerfällt $\mu_K(\zeta_n)$ als Teiler von X^n-1 über $K[\zeta_n]$ in paarweise verschiedene Linearfaktoren, die Erweiterung $K[\zeta_n]/K$ ist also endlich, normal und separabel, und somit galoissch. Für $g \in \mathrm{Gal}(K[\zeta_n]/K)$ ist $g(\zeta_n)$ auch eine primitive n-te Einheitswurzel also von der Form $g(\zeta_n) = \zeta_n^{m(g)}$ für ein $m(g) \in \mathbb{Z}/n\mathbb{Z}^*$. Der Automorphismus g ist durch $g(\zeta_n)$ eindeutig bestimmt, also ist m eine injektive Abbildung. Es ist

$$h(g(\zeta_n)) = h(\zeta_n^{m(g)}) = h(\zeta_n)^{m(g)} = \zeta_n^{m(g)m(h)}$$

also ist m ein Gruppenhomomorphismus. □

Beisp.: $n = 7$, $K = \mathbb{F}_2$.

Satz 3.25. *Für $K = \mathbb{Q}$ ergibt sich speziell:*

(a) $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$.

(b) $\Phi_n \in \mathbb{Q}[X]$ *irreduzibel.*

(c) $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.

Beweis. Es genügt zu zeigen, dass $\Phi_n \in \mathbb{Z}[X]$ irreduzibel ist. Sei dazu $g \in \mathbb{Z}[X]$ ein normierter irreduzibler Teiler von Φ_n mit $g(\zeta_n) = 0$.
Behauptung: Ist p eine Primzahl, die n nicht teilt, so ist auch $X - \zeta_n^p$ ein Teiler von g. (Daraus ergibt sich dann $g = \Phi_n$.)
Schreibe dazu $\Phi_n = gh$ mit $h \in \mathbb{Z}[X]$ normiert. Ist ζ_n^p keine Nullstelle von g, so ist $h(\zeta_n^p) = 0$, also ζ_n eine Nullstelle von $h(X^p)$. Also gilt $h(X^p) = gf$ für ein $f \in \mathbb{Z}[X]$.
Modulo p gilt aber $h(X)^p \equiv_p h(X^p) = gf$. Somit sind $\overline{h}$ und $\overline{g} \in \mathbb{F}_p[X]$ nicht teilerfremd, also $X^n - 1 \in \mathbb{F}_p[X]$ nicht separabel, ein Widerspruch, da $p \not| n$. □

Zyklotomische Polynome:

2 $x + 1$

3 $x^2 + x + 1$

4 $x^2 + 1$

5 $x^4 + x^3 + x^2 + x + 1$

6 $x^2 - x + 1$

7 $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

8 $x^4 + 1$

9 $x^6 + x^3 + 1$

10 $x^4 - x^3 + x^2 - x + 1$

$n = 105$ ist das erste n, für welches Φ_n einen Koeffizienten von Betrag ≥ 2 hat.

Der Satz von Kronecker Weber sagt aus, dass jede abelsche Erweiterung von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten ist.

3.3 Norm und Spur

Definition 3.26. *Für $a \in E$ sei $\ell_a : E \to E,\ b \mapsto ab$ die K-lineare Abbildung "Multiplikation mit a". Dann definiere die* **Norm** *von a als $N_{E/K}(a) := N(a) := \det(\ell_a)$ und die* **Spur** *von a als $S_{E/K}(a) := S(a) := \mathrm{Spur}(\ell_a)$.*

Bemerkung 3.27. *(a) Das Minimalpolynom von ℓ_a ist gleich dem Minimalpolynom von a über K, insbesondere irreduzibel in $K[X]$.*

(b) Das charakteristische Polynom von ℓ_a ist eine Potenz des Minimalpolynoms: $\chi_a = \mu_a^{[E:K[a]]}$.

(c) Für $a, b \in E$ ist $\ell_{ab} = \ell_a \circ \ell_b$ und daher $N(ab) = N(a)N(b)$. Insbesondere ist die Norm ein Gruppenhomomorphismus $N : E^* \to K^*$.

(d) Die Spur ist eine K-lineare Abbildung von E nach K.

Satz 3.28. *Sei E/K eine endliche separable Körpererweiterung vom Grad n und $\sigma_1, \ldots, \sigma_n : E \to \overline{K}$ die verschiedenen Einbettungen von E in den algebraischen Abschluß von K. Für $a \in E$ ist $N_{E/K}(a) = \prod_{i=1}^n \sigma_i(a)$ und $S_{E/K}(a) = \sum_{i=1}^n \sigma_i(a)$.*

Beweis. Sei zunächst $E = K[a]$ (also $\sigma_1(a), \ldots, \sigma_n(a)$ paarweise verschieden). Das Minimalpolynom von a ist dann $\mu_a = \prod_{i=1}^n (X - \sigma_i(a))$ also ergeben sich Spur und Norm von a als Spur und Determinante von ℓ_a wie behauptet.
Jetzt sei $F := K[a] \leq E$ ein Teilkörper von E und $\tau_1, \ldots, \tau_j$ alle K-linearen Einbettungen von F nach $\overline{K}$, $j = [K[a] : K]$, $n = j[E : K[a]]$. Mit E/K sind auch $K[a]/K$ und $E/K[a]$ separabel. Bezeichnet $\mathrm{Hom}_{K[a]}(E, \overline{K}) = \{\varphi_1, \ldots, \varphi_m\}$, und ist $\tilde{\tau}_i : \overline{K} \to \overline{K}$ eine Fortsetzung von τ_i, so sind die Fortsetzungen von τ_i auf E gegeben durch $\{\tilde{\tau}_i \circ \varphi_1, \ldots, \tilde{\tau}_i \circ \varphi_m\}$ Insbesondere ist

$$\prod_{i=1}^n \sigma_i(a) = (\prod_{i=1}^j \tau_i(a))^m = N_{K[a]/K}(a)^m = N_{E/K}(a) \text{ und}$$
$$\sum_{i=1}^n \sigma_i(a) = m(\sum_{i=1}^j \tau_i(a)) = mS_{K[a]/K}(a) = S_{E/K}(a).$$

□

Satz 3.29. *(Transitivität von Norm und Spur) Sei $K < F < E$ ein Körperturm so dass E/K separabel ist, dann ist für $a \in E$*

$$N_{E/K}(a) = N_{F/K}(N_{E/F}(a)) \text{ und } S_{E/K}(a) = S_{F/K}(S_{E/F}(a)).$$

Beweis. Wie im letzten Beweis seien $\mathrm{Hom}_K(E, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$, $\mathrm{Hom}_F(E, \overline{K}) = \{\varphi_1, \ldots, \varphi_m\}$, $\mathrm{Hom}_K(F, \overline{K}) = \{\tau_1, \ldots, \tau_j\}$ und die $\tilde{\tau}_i$ Fortsetzungen von τ_i auf $\overline{K}$. Dann ist

$$\{\sigma_1, \ldots, \sigma_n\} = \{\tilde{\tau}_k \circ \varphi_i \mid 1 \leq i \leq m, 1 \leq k \leq j\}$$

und

$$N_{E/K}(a) = \prod_{i=1}^n \sigma_i(a) = \prod_{k=1}^j \prod_{i=1}^m \tilde{\tau}_k(\varphi_i(a)) = \prod_{k=1}^j \tilde{\tau}_k N_{E/F}(a) = N_{F/K}(N_{E/F}(a))$$

ebenso für die Spur. □

Bemerkung 3.30. *Sei $\mathbb{F} = \mathbb{F}_{p^n}$ ein endlicher Körper und $\alpha \in \mathbb{F}^*$ eine Primitivwurzel. Sei m ein Teiler von n und $\mathbb{F}_{p^m} \cong K \leq \mathbb{F}$. Dann ist $\langle N_{\mathbb{F}/K}(\alpha)\rangle = K^*$.*

BEWEIS: Sei $n = md$. $Gal(\mathbb{F}/K)$ wird erzeugt von F^m. Also ist

$$\alpha N_{\mathbb{F}/K} = \alpha^{p^m+p^{2m}+\ldots+p^{dm}}\alpha^{1+p^m+p^{2m}+\ldots+p^{(d-1)m}} = \alpha^{\frac{p^n-1}{p^m-1}}.$$

Da α ein Element der Ordnung p^n-1 ist, ist $\alpha N_{\mathbb{F}/K} \in K^*$ ein Element der Ordnung p^m-1, also eine Primitivwurzel. □

Definition 3.31. *(Spurbilinearform) Sei (E/K) eine endliche Körpererweiterung. Definieren $T : E \times E \to K$ durch*

$$T(a,b) := S(ab).$$

Dann ist T eine symmetrische K-Bilinearform auf E und heißt die **Spurbilinearform**.

Satz 3.32. *Sei E/K eine separable endliche Körpererweiterung. Dann ist die Spurbilinearform nicht ausgeartet, d.h. die Abbildung $T : E \to Hom_K(E,K)$ definiert durch $a \mapsto T_a$, wo $bT_a := Spur(ab)$ für alle $b \in E$ ist ein Isomorphismus.*

BEWEIS: Zu zeigen ist, daß für alle $a \in E$. $a \neq 0$ es ein $b \in E$ gibt, so daß $S(ab) \neq 0$ ist. Denn dann ist der Kern von T gleich 0, also T injektiv und aus Dimensionsgründen folgt T surjektiv. Da $aE = E$ für $a \neq 0$ genügt es ein $x \in E$ zu finden mit $S(x) \neq 0$. Sind aber $\sigma_1, \ldots, \sigma_n$ die $n = [E : K]$ verschiedenen K-Algebrenhomomorphismen von E in den algebraischen Abschluss $\overline{K}$, so gilt $S(x) = \sum_{i=1}^n \sigma_i(x)$. Nach dem Satz von Artin ist $\sum_{i=1}^n \sigma_i$ nicht die Nullabbildung. □

3.4 Zyklische Körpererweiterungen.

In diesem kurzen Abschnitt sei E/K eine Galoiserweiterung mit zyklischer Galoisgruppe $G = \langle g\rangle$ der Ordnung n.

Satz 3.33. *(Satz 90 bei Hilbert)*
Sei E/K eine Galoiserweiterung mit zyklischer Galoisgruppe $G = \langle g\rangle$ der Ordnung n. Dann existiert für jedes $a \in E$ mit $N_{E/K}(a) = 1$ ein $b \in E$ mit $a = \frac{b}{gb}$.

BEWEIS: ($N_{E/K}(\frac{b}{gb}) = \frac{N_{E/K}(b)}{N_{E/K}(gb)} = 1$) Nach Satz 3.3 von Artin sind $id, g, g^2, \ldots, g^{n-1}$ linear unabhängig über E. Also ist

$$\tau := id + ag + a\cdot g(a)g^2 + \ldots + ag(a)\ldots g^{n-2}(a)g^{n-1}$$

nicht die Nullabbildung, d.h. es gibt ein $c \in E$ mit $\tau(c) \neq 0$. Setze $b := \tau(c)$. Dann ist

$$a\cdot g(b) = ag(c) + ag(a)g^2(c) + a\cdot g(a)\cdot g^2(a)g^3(c) + \ldots + \underbrace{ag(a)g^2(a)\ldots g^{n-1}(a)}_{N(a)}g^n(c) = b$$

also $a = \frac{b}{g(b)}$. □

Satz 3.34. *Sei $char(K) \nmid n$ und K enthalte primitive n-te Einheitswurzeln.*

(a) Ist E/K zyklisch vom Grad n, so gibt es ein $\alpha \in E$ mit $\alpha^n \in K$ und $E = K[\alpha]$.

(b) Ist $c \in K$ und $\alpha \in \overline{K}$ eine Nullstelle von $X^n - c \in K[X]$, so ist $K[\alpha]/K$ eine zyklische Erweiterung vom Grad d ein Teiler von n und es gilt $\alpha^d \in K$.

BEWEIS: (a) Sei $\mathrm{Aut}_K(E) =: G = \langle g \rangle$, und sei ξ eine primitive n-te Einheitswurzel in K. Sei $N = N_{E/K}$. Dann ist $N(\xi^{-1}) = 1$. Mit Satz 3.33 folgt: Es existiert ein $\alpha \in E$ mit $\xi^{-1} = \frac{\alpha}{g(\alpha)}$, also $g(\alpha) = \alpha\xi$ (Produkt in E). Daraus folgt: $g^i(\alpha) = \alpha\xi^i$. Folglich sind die n Konjugierten unter G paarweise verschieden (d.h. Bahnlänge =n). Also gilt: $[K[\alpha] : K] \geq n = |G|$.
$g(\alpha^n) = g(\alpha)^n = (\alpha\xi)^n = \alpha^n\xi^n = \alpha^n 1 = \alpha^n$, somit ist $\alpha^n \in K$. Definiere $c = \alpha^n$, dann ist $\alpha^n - c = 0$.
(b) Die Wurzeln von $x^n - c$ sind gegeben durch $\alpha, \alpha\xi, \alpha\xi^2, \ldots, \alpha\xi^{n-1}$ (ξ ist n-te primitive Einheitswurzel.). Da ξ ein Element des Körpers K ist, ist $K[\alpha]$ Zerfällungskörper von $x^n - c$. Also ist $[K[\alpha] : K]$ galoissch. Sei $g \in \mathrm{Aut}(K[\alpha]) =: G$; dann ist $g(\alpha) = \xi_g\alpha$ für ein $\xi_g \in \langle\xi\rangle \cong C_n$. Die Abbildung $G \longrightarrow \langle\xi\rangle : g \mapsto \xi_g$ ist ein Monomorphismus, dessen Bild die Ordnung d habe (D.h., $d|n$). Damit ist G zyklisch von der Ordnung d. Sei $g \in G$: $g(\alpha^d) = g(\alpha)^d = (\alpha\xi_g)^d = \alpha^d(\xi_g)^d = \alpha^d 1 = \alpha^d$. Also ist $\alpha^d \in K = Fix_G(K[\alpha])$. □

Satz 3.35. *(Additive Form von Hilbert 90) Sei E/K zyklisch, $\mathrm{Gal}(E/K) = \langle\sigma\rangle$. Für $\alpha \in E$ ist $S_{E/K}(\alpha) = 0$ genau dann wenn es ein $\beta \in E$ gibt mit $\alpha = \beta - \sigma(\beta)$.*

Beweis. Es ist $S(\beta - \sigma(\beta)) = 0$, also $\Leftarrow$ ist klar.
$\Rightarrow$: Sei $\xi \in E$ mit $S_{E/K}(\xi) \neq 0$. Setze

$$\beta := S_{E/K}(\xi)^{-1}(\alpha\sigma(\xi) + (\alpha + \sigma(\alpha))\sigma^2(\xi) + \ldots + (\alpha + \sigma(\alpha) + \ldots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\xi).$$

Dann gilt $\beta - \sigma(\beta) = \alpha$. (Nachrechnen, unter Benutzung von $S_{E/K}(\alpha) = 0$.) □

Satz 3.36. *(Artin-Schreier) Sei $char(K) = p > 0$.*
(a) Ist E/K zyklisch vom Grad p, so gibt es $\alpha \in E$ mit $E = K[\alpha]$ so dass α eine Nullstelle von $X^p - X - a$ ist für ein $a \in K$.
(b) Für $a \in K$ sei $f(X) := X^p - X - a \in K[X]$. Dann zerfällt f in ein Produkt von Linearfaktoren in $K[X]$ oder f ist irreduzibel und $K[\alpha]/K$ ist zyklische Galoiserweiterung von Grad p für jede Nullstelle α von f.

Beweis. (a) Wegen $[E : K] = p$ ist $S_{E/K}(-1) = p(-1) = 0$. Sei nun $\langle\sigma\rangle := \mathrm{Gal}(E/K)$. Dann gibt es nach Satz 3.35 ein $\alpha \in E$ mit $1 = \sigma(\alpha) - \alpha$. Also gilt $\sigma(\alpha) = \alpha + 1$ und somit $\sigma^i(\alpha) = \alpha + i$ für alle $i \in \{0, \ldots, p-1\}$. Folglich hat α genau p konjugierte, also $E = K[\alpha]$. Weiter ist

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$$

ist $a := \alpha^p - \alpha \in K$.
(b) Ist $\alpha \in \overline{K}$ eine Nullstelle von f, so sind die Nullstellen von f genau $\{\alpha + i \mid 0 \leq i \leq p-1\}$. Somit zerfällt f vollständig über $K[\alpha]$ und jeder minimale Wurzelkörper von f ist ein Zerfällungskörper, also f irreduzibel oder Produkt von Linearfaktoren. Im Fall f irreduzibel ist $K[\alpha]/K$ normal und separabel, also galoissch vom Grad p. □

3.5 Auflösbarkeit von Gleichungen

Definition 3.37. *Sei K ein Körper mit $Char(K) = 0$.*

(i) *(F/K) heißt* **auflösbar durch Radikale**, *falls ein Erweiterungskörper E von F existiert derart, dass $K \subset E_1 \subset E_2 \subset \ldots \subset E_n = E$, so dass E_i aus E_{i-1} durch Adjunktion von $a \in E_i$ mit $a^{n_i} \in E_{i-1}$ (n_i-te Wurzel) entsteht.*

(ii) *(E/K) heißt* **auflösbar** *genau dann, wenn eine Galoiserweiterung $(\tilde{E}/K)$ existiert mit $E \subseteq \tilde{E}$, sodass $(\tilde{E}/K)$ galoissch ist mit auflösbarer Galoisgruppe.*

Satz 3.38. *Sei K ein Körper mit $Char(K) = 0$ und (E/K) eine endliche Erweiterung. Es gilt:*
(E/K) ist genau dann auflösbar durch Radikale (Körpertheorie), wenn (E/K) auflösbar ist (Gruppentheorie).

Beweis:

"$\Rightarrow$" Durch Induktion über n:
Für $n = 1$: Die Behauptung ist trivial, falls $a^m = 1$, da dann $K[a]$ ein Kreisteilungskörper ist. Sei also $a^m \neq 1$ und $a^m \in K$. Die Behauptung ist ebenfalls klar, falls K eine m-te primitive Einheitswurzel enthält nach Satz 3.34. Enthält K keine primitive m-te Einheitswurzel, so adjungiere eine primitive m-te Einheitswurzel ξ_m. Dann sind $K[a][\xi_m]/K$ und $K[\xi_m]/K$ galoissch.
($K[a]/K$ ist nicht unbedingt galoissch; z.B. $a = \sqrt[3]{2}$: $x^3 - 2$ hat zwei komplexe Wurzeln.)
Da die Galoisgruppe von $K[a][\xi_m]/K[\xi_m]$ zyklisch ist und die von $K[\xi_m]/K$ abelsch, folgt die Auflösbarkeit.
Annahme: Die Behauptung gilt für $n-1$: Adjungiere eine primitive k-te Einheitswurzel ξ_k für ein geeignetes k (z.B. $k = [E : K]$). Dann ist $E[\xi_k]/K$ galoissch und die Schritte von K nach $E[\xi_k]$ sind alle zyklisch, also ist (E/K) auflösbar (= multizyklisch).

"$\Leftarrow$" Ist (E/K) auflösbar, dann existiert eine galoissche Körpererweiterung $(\tilde{E}/K)$ mit auflösbarer Galoisgruppe G und $\tilde{E} \supset E$. O.B.d.A. habe $\tilde{E}$ genügend Einheitswurzeln. Dann folgt die Behauptung aus Satz 3.34 zusammen mit der Charakterisierung endlicher auflösbarer Gruppen als "multizyklische" Gruppen (alle Kompositionsfaktoren zyklisch). (Eine zyklische Erweiterung ist das Adjungieren einer n-ten Wurzel, falls genügend Einheitswurzeln existieren.)

□

Folgerung 3.39. *Polynomgleichungen 3. und 4. Grades kann man durch Wurzelziehen unter Verwendung von Einheitswurzeln lösen.*

Beweis: Die Galoisgruppen G sind Untergruppen der S_4 bzw. der S_3, welche auflösbar sind, also ist G auflösbar. □

3.6 Konstruktionen mit Zirkel und Lineal.

Definition 3.40. *Sei* $\{0,1\} \subseteq M \subseteq \mathbb{C}$.

(a) *Für* $a \neq b \in M$ *sei* $G(a,b)$ *die* **Gerade** *durch* a *und* b.

(b) *Für* $p, a, b \in M$ *sei* $K(p, |a-b|)$ *der* **Kreis** *um* p *mit Radius* $|a-b|$.

(c) *Ein Punkt* $a \in \mathbb{C}$ *heißt* **elementar aus** M **konstruierbar**, *falls er entweder Schnittpunkt von zwei Geraden durch Punkte aus* M *oder als Schnittpunkt von Gerade und Kreis, oder von 2 Kreisen* $K(p_i, |a_i - b_i|)$ *für Elemente* $p_i, a_i, b_i \in M$ *ensteht.*

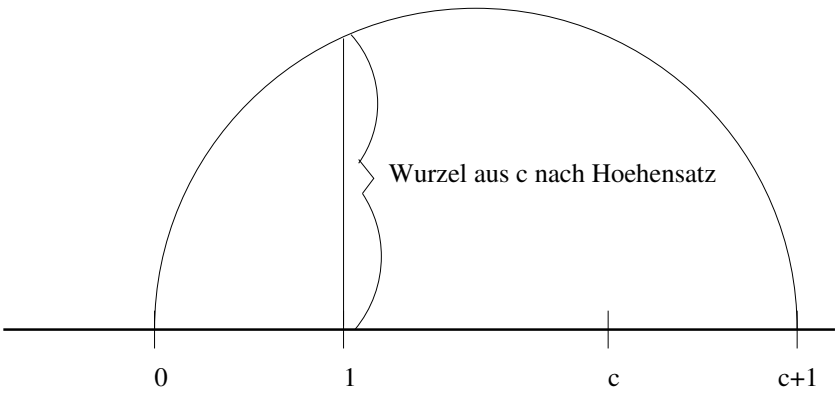
(d) *Ein Punkt* $a \in \mathbb{C}$ *heißt aus* M *mit* **Zirkel und Lineal konstruierbar**, *falls es eine Folge*

$$M = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n \subseteq \mathbb{C}$$

gibt, so dass alle Punkte von M_i *elementar aus* M_{i-1} *konstruierbar sind und* $a \in M_n$ *liegt. Bezeichne* $Kon(M)$ *die Menge, der aus* M *konstruierbaren Punkte von* $\mathbb{C}$.

Lemma 3.41. *Sei* $\{0,1\} \subset M \subset \mathbb{C}$ *und* $\overline{M} := \{\overline{z} \mid z \in M\}$.
(a) $Kon(M) \subset \mathbb{C}$ *ist ein Teilkörper von* $\mathbb{C}$ *mit* $\mathbb{Q}(M \cup \overline{M}) \subset Kon(M)$.
(b) Ist $b \in \mathbb{C}$ *mit* $b^2 \in Kon(M)$ *so ist* $b \in Kon(M)$.

Beweis. Wir zeigen $Kon(M)$ abgeschlossen unter Subtraktion und Division: $\overline{a0} \cap K(0, |a-0|) = \{a, -a\}$, also ist $-a$ konstruierbar aus a und 0. $a+b$ ergibt sich als 4. Ecke des Parallelogramms $(0, a, b, a+b)$, also als $K(b, |a-0|) \cap K(a, |b-0|)$.
Multiplikation von 2 komplexen Zahlen durch Addition der Winkel und Multiplikation der Beträge, ebenso wie Inversion auch konstruierbar (Übung).
Komplexe Konjugation: $\{a, \overline{a}\} = K(0, |a-0|) \cap K(1, |a-1|)$.
Zum Wurzelziehen: Konstruiere $b \in \mathbb{C}$ mit $b^2 = c$ durch Winkelhalbierende und Konstruktion von $\sqrt{|c|}$ mittels des Höhensatzes. □



Lemma 3.42. *Sei* $L \leq \mathbb{C}$ *ein Teilkörper mit* $L = \overline{L}$ *und* $i \in L$. *Ist* $z \in \mathbb{C}$ *in einem elementaren Schritt aus* L *konstruierbar, so gibt es* $w \in \mathbb{C}$ *mit* $w^2 \in L$ *so dass* $z \in L[w]$.

Beweis. Wegen $i \in L = \overline{L}$ liegen für jedes $p \in L$ auch sein Realteil und Imaginärteil in L und damit $|p|^2$ in L. Sei nun $z \in \mathbb{C}$ in einem Schritt aus L konstruierbar. Dann ist entweder

(a) z Schnitt von 2 Geraden über L und somit Lösung eines inhomogenen GLS über L also $z \in L$.

(b) Schnittpunkt einer Gerade und eines Kreises: $z \in \overline{ab} \cap K(p, |c-d|)$.
Sei $r := |c-d|^2$. Dann ist $r \in L$ und $z \in \overline{ab}$ hat eine Darstellung der Form $z = a+t(b-a)$ für ein $t \in \mathbb{R}$. Weiter ist $|z-p|^2 = r$, also

$$r = (t\Re(b-a) + \Re(a-p))^2 + (t\Im(b-a) + \Im(a-p))^2.$$

Die reelle Zahl t genügt also einer quadratischen Gleichung $t^2+\alpha t+\beta = 0$ mit $\alpha, \beta \in L$, also $[L(z) : L] \leq 2$.

(c) Schnitt von 2 Kreisen. $z \in K_1 \cap K_2$ mit $K_j := K(a_j + ib_j, r_j)$ für $j = 1, 2$, wobei $a_j, b_j, r_j^2 \in L$. Dann erfüllt $z = x + iy$ die Gleichungen $(x-a_j)^2 + (y-b_j)^2 = r_j^2$. Bildet man die Differenz, so fallen die quadratischen Terme weg und wir finden die Geradengleichung $(a_1 - a_2)x + (b_1 - b_2)y = c$ für ein $c \in L$. Also ist z wieder im Schnitt von Gerade und Kreis und wir sind im Fall (b).

□

Satz 3.43. *Sei $\{0, 1\} \subset M \subset \mathbb{C}$. Für $z \in \mathbb{C}$ sind äquivalent*

(a) $z \in Kon(M)$

(b) Es gibt einen Körperturm

$$\mathbb{Q}(M \cup \overline{M}) =: L_0 \subset L_1 \subset \ldots \subset L_k \subset \mathbb{C}$$

mit $z \in L_k$, so dass $[L_i : L_{i-1}] = 2$.

Beweis. Klar aus dem Lemma. □

Bemerkung 3.44. *Sei p eine ungerade Primzahl der Form $p = 2^m + 1$. Dann ist $m = 2^k$ für ein k und p eine* **Fermatsche Primzahl**.

Beweis. Ist $m = \ell q$ mit q ungerade, so ist

$$p = 2^{\ell q} + 1 = (2^\ell + 1)(2^{\ell(q-1)} - \ldots - 2^\ell + 1) = (2^\ell + 1) \sum_{i=0}^{q-1} (-2^\ell)^i.$$

□

Satz 3.45. *(Gauß) Sei $n \geq 3$. Dann sind äquivalent.*
(a) Das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar.
(b) $\varphi(n)$ ist eine Potenz von 2.
(c) $n = 2^m p_1 \ldots p_r$ für $m \in \mathbb{N}_0$ und paarweise verschiedenen Fermat-Primzahlen $p_1, \ldots, p_r$.

Beweis. Das regelmäßige n-Eck ist konstruierbar, genau dann wenn eine primitive n-te Einheitswurzel konstruierbar ist, genau dann wenn $\varphi(n) = [\mathbb{Q}[\zeta_n] : \mathbb{Q}]$ eine Potenz von 2 ist. □

3.7 Ganze Zahlen und die Diskriminante

Definition 3.46. *Sei R ein Ring (mit Eins). $a \in R$ heißt* **ganz über** $\mathbb{Z}$*, falls a Nullstelle eines ganzzahligen normierten Polynoms ist, d.h. es gibt $n \in \mathbb{N}$, $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ mit $a^n + a_{n-1}a^{n-1} + \ldots + a_1 a + a_0 = 0$.*

Beispiel: (Primitive) n-te Einheitswurzeln sind ganz, da sie Nullstellen von $x^n - 1$ sind.
$\sqrt{2}$ ist ganz, da $\sqrt{2}^2 - 2 = 0$.
$\frac{1}{\sqrt{2}}$ ist nicht ganz. (s.u.)

Satz 3.47. *Sei R ein Ring. $a \in R$ ist ganz, genau dann wenn a in einem Teilring von R liegt, der endlich erzeugt als $\mathbb{Z}$-Modul ist.*

Beweis: $\Rightarrow$: Sei $a \in R$ ganz. Dann gibt es $n \in \mathbb{N}$, $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ mit $a^n + a_{n-1}a^{n-1} + \ldots + a_1 a + a_0 = 0$. Also ist der von $1, a, \ldots, a^{n-1}$ erzeugte $\mathbb{Z}$-Teilmodul von $(R, +)$ ein Teilring von R.
$\Leftarrow$. Sei $a \in \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n =: M$ und M ein Teilring von R. O.b.d.A. enthalte M die Eins von R. Dann gilt $aM \subset M$, d.h. es gibt $A_{ij} \in \mathbb{Z}$ (nicht notwendig eindeutig) mit

$$ab_i = \sum_{j=1}^{n} A_{ij} b_j.$$

Das charakteristische Polynom von $A := (A_{ij})$ ist ein normiertes Polynom f mit ganzzahligen Koeffizienten, für das $f(A) = 0$ gilt. Also ist $f(a)M = 0$ und daher auch $f(a)1 = 0$ also $f(a) = 0$. □

Satz 3.48. *Sei R ein Ring und $a, b \in R$ ganz. Gilt $ab = ba$, so sind auch ab und $a + b$ ganz. Insbesondere bilden die ganzen Zahlen in einem kommutativen Ring R einen Teilring, den* **ganzen Abschluß von** $\mathbb{Z}$ **in** *R, $Int_{\mathbb{Z}}(R)$.*

Beweis: $\mathbb{Z}[a] = \sum_{i=0}^{n} \mathbb{Z}a^i$, $\mathbb{Z}[b] = \sum_{i=0}^{m} \mathbb{Z}b^i \Rightarrow \mathbb{Z}[a, b] = \sum_{i=0}^{n}\sum_{j=0}^{m} \mathbb{Z}a^i b^j$, da $ab = ba$. Also liegen $a + b$ und ab in einem endlich erzeugten $\mathbb{Z}$-Modul, der Teilring von R ist. □

Definition 3.49. *Ein* **algebraischer Zahlkörper** *K ist ein endlicher Erweiterungskörper K von $\mathbb{Q}$.*

Satz 3.50. *Sei K ein algebraischer Zahlkörper. Dann bilden die ganzen Zahlen in K einen Ring $Int_{\mathbb{Z}}(K) =: \mathbb{Z}_K$ der* **Ring der ganzen Zahlen in** *K.*
(1) Für alle $a \in K$ existiert ein $h \in \mathbb{N}$ so dass $ha \in \mathbb{Z}_K$. Also enthält $\mathbb{Z}_K$ eine $\mathbb{Q}$-Basis von K.
(2) $a \in K$ ist genau dann ganz, wenn sein Minimalpolynom $\mu(a, \mathbb{Q})$ in $\mathbb{Z}[X]$ liegt.

Beweis: Sei $a \in K$. Dann gibt es ein normiertes $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ mit $p(a) = 0$. Sei h der Hauptnenner der Koeffizienten a_i von $p(x)$. Dann gilt

$$(ha)^n + ha_{n-1}(ha)^{n-1} + \ldots + h^{n-1}a_1(ha) + h^n a_0 = 0$$

d.h. ha ist Nullstelle eines normierten ganzzahligen Polynoms. Also folgt (1).
Sei nun $a \in \mathbb{Z}_K$ und $p \in \mathbb{Z}[X]$ normiert mit $p(a) = 0$. Dann ist $\mu(a, \mathbb{Q})$ ein irreduzibler Teiler von p in $\mathbb{Q}[X]$. Sei L ein Zerfällungskörper von $\mu(a, \mathbb{Q})$, also $\mu(a, \mathbb{Q}) = \prod_{i=1}^{n}(X - \alpha_i) \in L[X]$. Dann sind alle α_i Nullstellen von p also ganz über $\mathbb{Z}$, somit auch die Koeffizienten von $\mu(a, \mathbb{Q})$. Diese sind also rationale Zahlen, die ganz über $\mathbb{Z}$ sind, liegen also in $\mathbb{Z}$. □

Satz 3.51. *Sei $K/\mathbb{Q}$ endlich und $R \subseteq \mathbb{Z}_K$ ein Ring ganzer Zahlen. Sei*

$$R^{\#} := \{a \in K \mid S_{K/\mathbb{Q}}(ar) \in \mathbb{Z} \text{ für alle } r \in R\}$$

die **inverse Differente** *von R.*
(a) Dann ist $R^{\#}$ ein R-Ideal in K, d.h. es gilt $R^{\#}R \subset R^{\#}$.
(b) Weiter gilt

$$R \subseteq \mathbb{Z}_K \subseteq \mathbb{Z}_K^{\#} \subseteq R^{\#}.$$

Beweis. (a) Sei $a \in R^{\#}$ und $s \in R$. Dann ist as wieder in $R^{\#}$.
(b) Klar ist für jede ganze Zahl $t \in \mathbb{Z}_K$ die Spur $S(t)$ wieder ganz, also $\mathbb{Z}_K \subseteq \mathbb{Z}_K^{\#}$.
□

Beispiel. $\mathbb{Z}[\sqrt{d}]^{\#} = (\frac{1}{2\sqrt{d}})\mathbb{Z}[\sqrt{d}]$ und $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^{\#} = (\frac{1}{\sqrt{d}})\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ falls $d \equiv_4 1$.

Satz 3.52. *Sei K ein algebraischer Zahlkörper $[K : \mathbb{Q}] = n$. Dann gibt es eine $\mathbb{Q}$-Basis $(b_1, \ldots, b_n)$ von K, mit $\mathbb{Z}_K = \langle b_1, \ldots, b_n\rangle_{\mathbb{Z}}$.*

Beweis. Sei $K = \mathbb{Q}[\alpha]$ mit α ganz. Setze $R := \mathbb{Z}[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_{\mathbb{Z}}$. Dann ist R ein Ring ganzer Zahlen in K. Für $r \in R$ und $a \in \mathbb{Z}_K$ gilt $ar \in \mathbb{Z}_K$ und insbesondere $S_{K/\mathbb{Q}}(ar) \in \mathbb{Z}$, also

$$\mathbb{Z}_K \subseteq \{a \in K \mid S_{K/\mathbb{Q}}(ar) \in \mathbb{Z} \text{ für alle } r \in R\} =: R^{\#}$$

Ist $B := (b_1^*, \ldots, b_n^*)$ die Dualbasis von $A := (1, \alpha, \ldots, \alpha^{n-1})$ bezüglich der Spurbilinearform T, also $S_{K/\mathbb{Q}}(b_i^*\alpha^{j-1}) = \delta_{ij}$, so ist $R^{\#} = \langle b_1^*, \ldots, b_n^*\rangle$. Die Basiswechselmatrix von B zu A ist genau die Grammatrix $Gram(A) := (T(\alpha^{i-1}\alpha^{j-1})_{i,j}) \in \mathbb{Z}^{n\times n}$ und die Ordnung der endlichen abelschen Gruppe $R^{\#}/R$ die Determinante $\det(Gram(A))$. Insbesondere gilt also

$$\mathbb{Z}^n \cong R^{\#} \supseteq \mathbb{Z}_K^{\#} \supseteq \mathbb{Z}_K \supseteq R \cong \mathbb{Z}^n$$

also $\mathbb{Z}_K$ ebenfalls endlich erzeugter $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$. □

Definition 3.53. *Sei K ein algebraischer Zahlkörper. Eine $\mathbb{Z}$-Basis $B = (b_1, \ldots, b_n)$ von $\mathbb{Z}_K$ heißt* **Ganzheitsbasis** *von K. Die Determinante der* **Grammatrix**

$$Gram(B) := (T(b_i, b_j))_{i,j=1}^n$$

heißt die **Diskriminante** *d_K von K.*

Bemerkung 3.54. *$Gram(B) \in \mathbb{Z}^{n\times n}$.*
Jede andere Ganzheitsbasis von K ist von der Form $B' = AB$ für ein $A \in GL_n(\mathbb{Z})$. Es gilt $Gram(B') = AGram(B)A^{tr}$. Insbesondere ist die Diskriminante von K unabhängig von der Wahl der Ganzheitsbasis.
Die Diskriminante von K erfüllt $|d_K| = |\mathbb{Z}_K^{\#}/\mathbb{Z}_K|$. Denn ist $B := (b_1, \ldots, b_n)$ eine Ganzheitsbasis von K und $B^* = (b_1^*, \ldots, b_n^*)$ die bezüglich T duale Basis, so ist $\mathbb{Z}_K^{\#} = \langle b_1^*, \ldots, b_n^*\rangle_{\mathbb{Z}}$. Die Grammatrix von B ist aber genau die Basiswechselmatrix von B^* nach B, also die Ordnung der endlichen abelschen Gruppe $\mathbb{Z}_K^{\#}/\mathbb{Z}_K$.

Beispiel: Sei $K := \mathbb{Q}[\sqrt{5}]$. Für $a := x + y\sqrt{5}$ (mit $x, y \in \mathbb{Q}$) gilt

$$a^2 = (x + y\sqrt{5})^2 = x^2 + 5y^2 + 2\sqrt{5}xy = 2xa - (x^2 - 5y^2) = S_{K/\mathbb{Q}}(a)a - N_{K/\mathbb{Q}}(a).$$

Also ist a ganz $\Leftrightarrow x, y \in \frac{1}{2}\mathbb{Z}, x \equiv y \pmod{\mathbb{Z}}$. Eine Ganzheitsbasis von K ist $(1, \frac{1+\sqrt{5}}{2})$ mit Grammatrix $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ und Diskriminante 5.

Satz 3.55. *Sei $d \in \mathbb{Z}$ quadratfrei und $K := \mathbb{Q}[\sqrt{d}]$. Dann ist*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv_4 1 \\ \mathbb{Z}[\sqrt{d}] & d \equiv_4 2, 3. \end{cases}$$

Die Diskriminante von K ist d falls $d \equiv_4 1$ und $4d$ sonst.

Beweis. Das Minimalpolynom von $a + b\sqrt{d} \in K \setminus \mathbb{Q}$ ist $X^2 - 2aX + (a^2 - db^2)$. Dieses liegt in $\mathbb{Z}[X]$ genau dann wenn $a \in \frac{1}{2}\mathbb{Z}$ und $a^2 - db^2 \in \mathbb{Z}$. Ist $a \in \mathbb{Z}$ so auch $b \in \mathbb{Z}$, da d quadratfrei ist. Ist $a = \frac{a'}{2}$ mit ungeradem a', so muss auch $b = \frac{b'}{2}$ und $(a')^2 - d(b')^2 \in 4\mathbb{Z}$ gelten. Da Quadrate ungerader Zahlen aber kongruent 1 modulo 4 sind, ist dies äquivalent zu $d \equiv_4 1$. Eine Ganzheitsbasis im Fall $d \equiv_4 2, 3$ ist $(1, \sqrt{d})$ mit Grammatrix $\mathrm{diag}(2, 2d)$ und Diskriminante $4d$. Ist $d \equiv_4 1$, so ist $(1, \frac{1}{2}(1 + \sqrt{d}))$ eine Ganzheitsbasis mit Grammatrix $\begin{pmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{pmatrix}$ und Diskriminante d. □

Übungsaufgabe: Sei $0 \neq a \in \mathbb{Z}_K$. Dann ist das Hauptideal $(a) = a\mathbb{Z}_K$ von endlichem Index in $\mathbb{Z}_K$ und $|\mathbb{Z}_K/(a)| = |N_{K/\mathbb{Q}}(a)|$.
Hinweis: (a) ist das Bild der Abbildung $\ell_a : \mathbb{Z}_K \to a\mathbb{Z}_K$. Die Spalten der Matrix von ℓ_a bzgl einer Ganzheitsbasis von K bilden also eine $\mathbb{Z}$-Basis des Teilmoduls $a\mathbb{Z}_K$ von $\mathbb{Z}_K$.

Satz 3.56. *Sei p eine Primzahl und ζ_p eine primitive p-te Einheitswurzel in $\mathbb{C}$. Sei $K := \mathbb{Q}[\zeta_p]$ der p-te Kreisteilungskörper. Dann gilt*

(a) $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$,

(b) $(1, \zeta_p, \ldots, \zeta_p^{p-2})$ *ein Ganzheitsbasis von K.*

(c) $\mathbb{Z}_K^{\#} = (1 - \zeta_p)^{2-p}\mathbb{Z}[\zeta_p] = p^{-1}(1 - \zeta_p)\mathbb{Z}[\zeta_p]$.

(d) $|d_K| = p^{p-2}$.

(e) Für $r, s \in \mathbb{Z}$ mit $p \not| rs$ ist $(1 - \zeta_p^r)/(1 - \zeta_p^s) = 1 + \zeta_p^s + \ldots + \zeta_p^{s(t-1)} \in \mathbb{Z}_K^*$ wobei $st \equiv_p r$.

Beweis. Setze $R := \mathbb{Z}[\zeta_p]$. Dann ist R ein Teilring von K, der aus ganzen Zahlen besteht, also $R \subseteq \mathbb{Z}_K$. (e) folgt durch Nachrechnen.
Aus der Übung wissen wir, dass $N(1 - \zeta_p) = p$. Weiter ist $(1 - \zeta_p)^{p-1} \in pR$ und aus Indexgründen daher $(1 - \zeta_p)^{p-1}R = pR$.
Wir wollen jetzt zeigen, dass $R^{\#} = (1 - \zeta_p)^{2-p}R = \frac{1}{p}(1 - \zeta_p)R$ gilt.
Dann ergibt sich alles andere, denn es ist $R \subseteq \mathbb{Z}_K \subseteq R^{\#}$, und $\mathbb{Z}_K$ ist ein R-Teilmodul. $R^{\#}/R$

ist aber ein einreihiger R-Modul, der einzige minimale Teilmodul ist $(1-\zeta_p)^{-1}R/R$. Da aber $N(1-\zeta_p)^{-1} = p^{-1}$ nicht ganz ist, gilt dann also $\mathbb{Z}_K = R$.
Es ist $S_{K/\mathbb{Q}}(1) = (p-1)$, $S_{K/\mathbb{Q}}(\zeta_p) = -1$, ebenso $S_{K/\mathbb{Q}}(\zeta_p^n) = -1$ für $n = 1, \ldots, p-1$. Also ist

$$S_{K/\mathbb{Q}}((1-\zeta_p)\zeta_p^i) = \begin{cases} 0 & 1 \leq i \leq p-2 \\ p & i = 0 \\ -p & i = p-1 \end{cases}$$

und somit $\frac{1}{p}(1-\zeta_p) \in R^{\#}$.
Sei umgekehrt $\alpha := \sum_{i=0}^{p-2} b_i \zeta_p^i \in R^{\#}$. Dann ist

$$S_{E/\mathbb{Q}}(\alpha\zeta_p^i) = (p-1)b_i - \sum_{j \neq i} b_j \in \mathbb{Z}$$

also (Anwenden für $i = 0$ und $i = i$) $p(b_0 - b_i) \in \mathbb{Z}$ für alle i, α ist also eine $\mathbb{Z}$-Linearkombination von 1 und $\frac{1}{p}(1-\zeta_p^i)$ (mit $i = 1, \ldots, p-1$). Da aber $(1-\zeta_p^i)R = (1-\zeta_p)R$ für diese i gilt, folgt $\alpha \in \frac{1}{p}(1-\zeta_p)R$ und somit ist dies die inverse Differente von R. □

Kapitel 4

Ringe und Moduln.

4.1 Einfache Moduln und der Satz von Jordan Hölder

Definition 4.1. • *Eine Menge* $(A, +, \cdot)$ *heißt* **Ring**, *falls*
$(A, +)$ *abelsche Gruppe mit neutralem Element* 0,
$(A, \cdot)$ *Monoid mit neutralem Element* 1,
$\cdot : A \times A \to A$ *eine* $\mathbb{Z}$*-Bilinearform ist.*

- *Ein Ring* A *heißt*
  kommutativ, *falls* $(A, \cdot)$ *kommutativ ist.*
  Schiefkörper, *falls* $(A \setminus \{0\}, \cdot)$ *eine Gruppe ist.*
  Ein kommutativer Schiefkörper heißt **Körper**.

- *Das* **Zentrum** *von* A *ist*

$$Z(A) := \{z \in A \mid az = za \text{ für alle } a \in A\}.$$

  Das Zentrum eines Ringes ist ein Teilring.

- *Ist* R *ein kommutativer Ring, so heißt* A *eine* R*-Algebra, falls ein Ringhomomorphismus* $R \to Z(A)$ *existiert.*

- *Ein* A**-Modul** *(genauer ein* A*-Linksmodul)* M *ist eine abelsche Gruppe mit einer äußeren Struktur* $A \times M \to M$ *mit Assoziativ und Distributivgesetz, so dass* $1m = m$ *für alle* $m \in M$.

- *Ringhomomorphismus.*

- *Modulhomomorphismus, Teilmodul und Faktormodul.*

- *Ein* A*-Modul* M *heißt* **einfach**, *falls* $M \neq \{0\}$ *und* M *keine* A*-Teilmoduln außer* M *und* $\{0\}$ *besitzt.*

Beispiele: Sei A ein Ring. Dann ist ${}_AA$ ein A-Modul, der **reguläre** A**-Modul**.
Seine Teilmoduln sind die **Linksideale** von A.
Für jeden A-Modul M und jedes $x \in M$ ist

$$f_x : {}_AA \to M, a \mapsto ax$$

ein A-Modulhomomorphismus. Das Bild von f_x ist der von x erzeugte A-Teilmodul von M (ein **zyklischer Modul**). Der Kern von f_x ist der **Annihilator** von x,

$$ann_A(x) := \{a \in A \mid ax = 0\} \text{ ein Linksideal von } A.$$

Der Faktormodul ${}_AA/ann_A(x) \cong Ax$ ist also nach dem Homomorphiesatz isomorph zum Bild.

Bemerkung 4.2. *Sei M ein einfacher A-Modul. Dann ist für jedes $0 \neq x \in M$ der Annihilator $ann_A(x)$ ein maximales Linksideal in A. Es ist $M = Ax \cong A/ann_A(x)$. Umgekehrt ist I ein maximales Linksideal in A, so ist ${}_AA/I$ ein einfacher A-Modul.*

Bemerkung 4.3. *Jeder A-Modul M ist eine abelsche Ω-Gruppe mit $A = \Omega$. Teilmoduln sind Ω-Normalteiler. M ist also einfach als A-Modul, genau dann wenn er einfach als A-Gruppe ist. Insbesondere gelten alle Sätze, die wir für Ω-Gruppen gezeigt haben entsprechend auch für A-Moduln.*

Folgerung 4.4. *(Isomorphiesätze) Sei M ein A-Modul und N_1, N_2, N_3 Teilmoduln von M mit $N_3 \leq N_1$. Dann sind*

$$\alpha : N_1/(N_1 \cap N_2) \to (N_1 + N_2)/N_2, n_1 \mapsto n_1 + N_2$$

$$\beta : (M/N_3)/(N_1/N_3) \to M/N_1, (m + N_3) + (N_1/N_3) \mapsto m + N_1$$

A-Modulisomorphismen

Folgerung 4.5. *(Jordan-Hölder) Sei M ein A-Modul. Hat M eine A-Kompositionsreihe*

$$M = M_0 > M_1 > \ldots > M_n = \{0\}$$

mit M_{i-1}/M_i einfach, so gilt für jede andere A-Kompositionsreihe $M = N_0 > N_1 \ldots > N_m = \{0\}$ dass $n = m$ gilt und es eine Permutation $\pi \in S_n$ gibt mit $N_{\pi(i)-1}/N_{\pi(i)} \cong M_{i-1}/M_i$ für alle i.

Bemerkung 4.6. *Sei $0 \neq \varphi : M \to M'$ ein A-Modulhomomorphismus. Dann sind $Kern(\varphi)$ und $Bild(\varphi)$ Teilmoduln von M bzw. M', die beide nicht trivial sind. Also gilt:*
Ist M einfach, so ist $Kern(\varphi) = 0$ also φ injektiv.
Ist M' einfach, so ist $Bild(\varphi) = M'$ also φ surjektiv.
Sind M und M' einfach, so ist φ ein Isomorphismus.

Daraus erhalten wir sofort das folgende

Lemma 4.7. *(Lemma von Schur)*
(a) Sind M und M' nichtisomorphe einfache A-Moduln, so ist $\mathrm{Hom}_A(M, M') = \{0\}$.
(b) Ist M ein einfacher A-Modul, so ist $\mathrm{End}_A(M)$ *ein Schiefkörper.*

Satz 4.8. $\mathrm{End}_A({}_AA) \cong A^{op}$. *Hierbei ist A^{op} der* **opposite Ring**, *also $A^{op} = (A, +, \star)$ mit $a \star b := ba$ für alle $a, b \in A$.*

Beweis. Sei $\varphi \in \mathrm{End}_A({}_AA)$. Da ${}_AA = A1$ ein zyklischer A-Modul ist, ist φ eindeutig bestimmt durch $\varphi(1) =: a \in A$. Denn dann ist

$$\varphi(b) = \varphi(b \cdot 1) = b\varphi(1) = ba.$$

Also haben wir gesehen, dass $\psi : A \to \mathrm{End}_A({}_AA) : \ a \mapsto (m \mapsto ma)$ und $\phi : \mathrm{End}_A({}_AA) \to A : \ \varphi \mapsto \varphi(1)$ (φ = Rechtsmultiplikation mit $\varphi(1)$) zueinander inverse Homomorphismen sind.

Beispiel

$$A = K^{n\times n},\ {}_AA = \bigoplus^{n} K^{n\times 1},\ Hom_A(K^{n\times 1}, K^{n\times 1}) \cong K$$

Dann gilt

$$End_A(\bigoplus^{n} K^{n\times 1}) = K^{n\times n}$$

Definition 4.9. *Sei I eine Indexmenge und für jedes $i \in I$ sei M_i ein A-Modul. Das* **direkte Produkt** $\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}$ *der M_i wird wieder zu einem A-Modul, durch werteweise Verknüpfung. Die* **direkte Summe**

$$\bigoplus_{i\in I} M_i := \{(x_i) \in \prod_{i\in I} M_i \mid x_i \neq 0 \text{ nur für endlich viele } i\}$$

ist ein Teilmodul von $\prod_{i\in I} M_i$.
Der freie A-Modul auf I ist $\bigoplus_{i\in I}\ {}_AA$.
Allgemeiner nennen wir einen A-Modul M **frei** *auf $(m_i)_{i\in I}$, falls die Abbildung*

$$\bigoplus_{i\in I}\ {}_AA \to M, (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i$$

bijektiv ist.

Beispiel. Sei K ein Körper und $A := \mathrm{End}_K(K[X])$. Dann ist $1_A = id$ eine A-Basis von ${}_AA$. Definiert man die K-Endomorphismen f_1, f_2 durch

$$f_1(X^i) := \begin{cases} X^{i/2} & i \text{ gerade} \\ 0 & i \text{ ungerade} \end{cases} \quad \text{und } f_2(X^i) := \begin{cases} 0 & i \text{ gerade} \\ X^{(i-1)/2} & i \text{ ungerade} \end{cases}$$

so ist für alle $g_1, g_2 \in A$

$$(g_1f_1 + g_2f_2)(X^i) = \begin{cases} g_1(X^{i/2}) & i \text{ gerade} \\ g_2(X^{(i-1)/2}) & i \text{ ungerade} \end{cases}$$

also f_1, f_2 linear unabhängig über A und ${}_AA \cong Af_1 \oplus Af_2$.

Satz 4.10. *Sei R ein kommutativer Ring und F ein R-Modul. Ist F frei auf $\{x_1, \ldots, x_n\}$ und $\{y_1, \ldots, y_m\}$, so gilt $m = n$. Man nennt n auch den* **Rang** *des freien R-Moduls F.*

Beweis. Sei I ein maximales Ideal von R. Dann ist $K := R/I$ ein Körper und sowohl $\{x_1 + IF, \ldots, x_n + IF\}$ als auch $\{y_1 + IF, \ldots, y_m + IF\}$ sind K-Basen des K-Vektorraums F/IF. □

Satz 4.11. *Sei*

$$M = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{k_i} M_i$$

mit M_i paarweise nicht isomorphe einfache Moduln. Sei $D_i := \mathrm{End}_A(M_i)$. Dann ist D_i ein Schiefkörper und

$$\mathrm{End}_A(M) \cong \bigoplus_{i=1}^{n} D_i^{k_i \times k_i}$$

Beweis. Folgt direkt aus Schur's Lemma. Sei $M = \bigoplus N_i$. Dann ist

$$End_A(M) = \begin{pmatrix} Hom_A(N_1, N_1) & \cdots \\ \vdots & \end{pmatrix} = \left(\begin{array}{c|ccc} D_1^{k_1 \times k_1} & 0 & \cdots & 0 \\ \hline 0 & D_2^{k_2 \times k_2} & & \\ \vdots & & \ddots & \\ 0 & & & \end{array}\right)$$

mit den D_i und 0 aus dem Lemma von Schur. Die N_i müssen nur noch nach Isomorphieklassen geordnet werden.

4.2 Halbeinfache Ringe und Moduln

Definition 4.12. *Ein A-Modul heißt* **halbeinfach**, *wenn er direkte Summe von einfachen Teilmoduln ist.*

Lemma 4.13. *Sei M ein A-Modul, $N \leq M$ und $(M_i)_{i \in I}$ eine Familie einfacher A-Teilmoduln von M. Gilt $M = N + \sum_{i \in I} M_i$, so gibt es eine Teilmenge $J \subset I$ mit $M = N \oplus \bigoplus_{i \in J} M_i$.*

Beweis. Sei

$$X := \{J \subset I \mid N + \sum_{i \in J} M_i = N \oplus \bigoplus_{i \in J} M_i\}$$

Dann ist $\emptyset \in X \neq \emptyset$. Weiter ist X durch Inklusion induktiv geordnet hat also nach dem Lemma von Zorn maximale Elemente. Sei J ein solches maximales Element und $M' := N \oplus \bigoplus_{i \in J} M_i$. Dann gilt für alle $i \in I$ dass $M' \cap M_i = M_i$ ist. Denn das ist sicherlich richtig für $i \in J$. Auf jeden Fall ist $M' \cap M_i$ ein Teilmodul des einfachen Moduls M_i also gleich M_i (wie behauptet) oder gleich $\{0\}$. Im letzten Fall wäre aber auch die Summe $M' \oplus M_i$ direkt, ein Widerspruch zur Maximalität von J. □

Satz 4.14. *Sei M ein A-Modul. Äquivalent sind:*

(a) M ist halbeinfach.

(b) M ist Summe von einfachen Teilmoduln.

(c) Für jeden Teilmodul $N \leq M$ gibt es einen Teilmodul $U \leq M$ mit $M = N \oplus U$.

Beweis. (a) $\Rightarrow$ (b) ist klar. (b) $\Rightarrow$ (a) folgt aus Lemma 4.13.
(a) $\Rightarrow$ (c) folgt ebenso aus Lemma 4.13, da nach (a)

$$M = \bigoplus_{i\in I} M_i = N + \sum_{i\in I} M_i = N \oplus \bigoplus_{i\in J} M_i$$

und $U := \bigoplus_{i\in J} M_i$ das Gewünschte leistet.
(c) $\Rightarrow$ (b): Gilt die Bedingung (c) für M, so auch für jeden seiner Teilmoduln $T \leq M$. Denn ist $N \leq T$ ein Teilmodul von T, so hat N ein Komplement $U \leq M$ mit $M = U \oplus N$. Dann ist $T = T \cap U \oplus N$.
Sei nun $N := \sum\{M' \mid M' \leq M, \text{ einfach }\}$ die Summe aller einfachen Teilmoduln von M. Um (b) einzusehen müssen wir zeigen, dass $N = M$ ist. Ist $M \neq N$, so hat N nach (c) ein Komplement $U \neq 0$. Wir wollen einen einfachen Teilmodul von U konstruieren. Dazu sei $0 \neq x \in U$ und betrachte den zyklischen Teilmodul $Ax \cong {}_AA/ann_A(x)$. Das Linksideal $ann_A(x) \neq A$ liegt in einem maximalen Linksideal B von A. Dann ist $Ax = Bx \oplus /C$ mit $C \cong A/B$ einfach. Also hat U einen einfachen Teilmodul C, der somit auch Teilmodul von N ist, ein Widerspruch. □

Folgerung 4.15. *Ist M ein halbeinfacher A-Modul, so sind alle seine Teilmoduln und Faktormoduln halbeinfach.*

Bemerkung 4.16. *Jeder endlich erzeugte halbeinfache A-Modul ist endliche direkte Summe einfacher A-Moduln.*

Definition 4.17. *Ein Ring A heißt* **halbeinfach**, *wenn ${}_AA$ halbeinfach ist.*

Beispiele. Ist A ein Körper oder Schiefkörper, so hat A keine Linksideale außer $\{0\}$ und A, also ist ${}_AA$ ein einfacher A-Modul und daher ist A halbeinfach.
Sind A_1 und A_2 halbeinfach, so auch die ringdirekte Summe $A_1 \oplus A_2$.
$\mathbb{Z}$ ist nicht halbeinfach.
Ist D ein Schiefkörper, so ist der Matrixring $D^{n\times n}$ halbeinfach, da

$$D^{n\times n} = \bigoplus_{i=1}^{n} D^{n\times 1}$$

und $D^{n\times 1}$ ein einfacher $D^{n\times n}$-Modul ist.

Satz 4.18. *Sei A ein halbeinfacher Ring. Dann gilt:*
(a) Jeder A-Modul ist halbeinfach.
(b) Es gibt nur endlich viele Isomorphieklassen einfacher A-Moduln.

Beweis. (a) Da ${}_AA$ halbeinfach ist ist auch jeder freie A-Modul halbeinfach. Jeder A-Modul ist Faktormodul eines freien Moduls also auch halbeinfach nach Folgerung 4.15.
(b) Sei ${}_AA = \bigoplus_{i\in I} N_i$ mit einfachen Teilmoduln N_i. Dann ist $1 \in {}_AA$ eine **endliche** Linearkombination von Elementen $a_i \in N_i$, also gibt es eine endliche Teilmenge $J \subset I$ mit $1 = \sum_{j\in J} a_j$ wobei $a_j \in N_j$ für alle j. Dann ist aber ${}_AA = A1 \subset \bigoplus_{j\in J} N_j$. also A endliche Summe einfacher A-Moduln, ${}_AA = N_1 \oplus \ldots \oplus N_n$. Ist nun M ein einfacher A-Modul, so ist für jedes $x \in M$ der A-Modulhomomorphismus $\varphi_x :_A A \to M, a \mapsto ax$ surjektiv. Insbesondere gibt es ein N_i mit $\varphi_x(N_i) \neq \{0\}$, also $N_i \cong M$. □

Satz 4.19. *(Wedderburn) Sei A ein halbeinfacher Ring, $M_1, \ldots, M_n$ ein Vertretersystem der Isomorphieklassen einfacher A-Moduln, $D_i^{op} = \mathrm{End}_A(M_i)$ und ${}_AA \cong \bigoplus_{i=1}^n \oplus^{k_i} M_i$ wie in Satz 4.11. Dann ist $A \cong \bigoplus_{i=1}^n D_i^{k_i \times k_i}$.*

Beweis. Lemma von Schur und Satz 4.11 liefern die Gestalt von $\mathrm{End}_A({}_AA) \cong A^{op}$. Daraus ergibt sich die Behauptung, unter Beachtung dass $(D^{n\times n})^{op} \cong (D^{op})^{n\times n}$ z.B. vermöge des Isomorphismus $A \mapsto A^{tr}$. □

4.3 Noethersche und Artinsche Ringe

Definition 4.20. *Ein A-Modul M heißt* **Noethersch**, *wenn jeder Untermodul von M endlich erzeugt ist.*

Beispiel: Endlich erzeugte Moduln über Hauptidealbereichen sind Noethersch.

Satz 4.21. *Sei M ein A-Modul. Äquivalent sind:*

(a) M ist Noethersch.

(b) Jede aufsteigende Kette $M_0 \leq M_1 \leq \ldots$ von Teilmoduln von M wird stationär, d.h. es gibt ein $n \in \mathbb{N}$ mit $M_n = M_k$ für alle $k \geq n$.

(c) Jede nichtleere Menge von Teilmoduln von M enthält ein maximales Element.

Beweis. (c) $\Rightarrow$ (b): Wende (c) auf die Menge $\{M_i \mid i \in \mathbb{N}_0\}$ an.
(b) $\Rightarrow$ (a): Sei $U \leq M$ ein Teilmodul. Wähle $0 \neq x_1 \in U$ und setze $T_1 := Ax_1$. Wähle $x_2 \in U \setminus T_1$ und setze $T_2 := Ax_1 + Ax_2$, ... für $x_{i+1} \in U \setminus T_i$ setze $T_{i+1} = T_i + Ax_{i+1}$. Nach (b) bricht dieser Prozess nach endlich vielen Schritten ab, d.h. $U = T_n = \langle x_1, \ldots, x_n \rangle_A$ endlich erzeugt.
(a) $\Rightarrow$ (c): Sei X eine nichtleere Menge von Teilmoduln von M. Wir benutzen das Lemma von Zorn und zeigen nur, dass jede Kette $K = \{X_1 < X_2 < \ldots\}$ von Elementen von X eine obere Schranke in X besitzt. Dazu setze $U := \sum X_i$. Dann ist U wegen (a) endlich erzeugt, d.h. es gibt $x_1, \ldots, x_n \in U$ mit $U = \langle x_1, \ldots, x_n \rangle_A$. Dann gibt es aber ein X_k, das alle x_i enthält, also $X_i < X_k$ für alle i und somit X_k eine obere Schranke von K. □

Bemerkung 4.22. *Sei $N \leq M$ zwei A-Moduln. M Noethersch $\Leftrightarrow$ N und M/N Noethersch.*

Beweis. $\Rightarrow$ klar.
$\Leftarrow$ Ist $M_1 \leq M_2 \leq \ldots \leq M_n \leq \ldots$ eine unendlich aufsteigende Folge von Teilmoduln von M, so sind

$$M_1 \cap N \leq M_2 \cap N \leq \ldots \leq M_n \cap N \leq \ldots$$
$$(M_1 + N)/N \leq (M_2 + N)/N \leq \ldots \leq (M_n + N)/N \leq \ldots$$

ebenso unendlich aufsteigende Ketten von Teilmoduln. Da N und M/N Noethersch sind gibt es ein n mit $M_n \cap N = M_k \cap N$ und $(M_n + N)/N = (M_k + N)/N$ für alle $k \geq n$. Dann ist aber $M_n = M_k$. □

Bemerkung 4.23. *Ist $M = \bigoplus_{i=1}^{n} M_i$ eine endliche direkte von Moduln, so ist M genau dann Noethersch, wenn alle M_i Noethersch sind.*

Definition 4.24. *Ein Ring A heißt* **Noethersch** *(genauer* **Linksnoethersch***, wenn ${}_AA$ Noetherscher A-Modul ist.*

Satz 4.25. *Jeder endlich erzeugte Modul über einem Noetherschen Ring ist Noethersch.*

Beweis. Ist M endlich erzeugter A-Modul, so ist M epimorphes Bild eines endlich erzeugten freien A-Moduls, also Faktormodul eines Noetherschen Moduls und somit Noethersch. □

Definition 4.26. *Ein A-Modul M heißt* **Artinsch***, falls jeder Faktormodul von M endlich koerzeugbar ist, d.h. ist $\{X_j \mid j \in J\}$ eine Familie von Teilmoduln von M so gibt es eine endliche Teilmenge $J_0 \subseteq J$ mit*

$$\bigcap_{j \in J} X_j = \bigcap_{j \in J_0} X_j.$$

Ein Ring A heißt **Artinsch***, falls ${}_AA$ Artinsch ist.*

Beispiel:

(1) $\mathbb{Z}$ ist Noethersch aber nicht Artinsch.

(2) $\mathbb{Q}_p/\mathbb{Z}_p$ ist ein Artinscher $\mathbb{Z}_p$-Modul, der nicht Noethersch ist.

(3) Einfache Moduln sind Artinsch und Noethersch.

(4) Halbeinfache Ringe sind Artinsch und Noethersch.

Satz 4.27. *Äquivalent sind für einen A-Modul M.*

(a) M ist Artinsch.

(b) Jede nichtleere Menge von A-Teilmoduln von M enthält ein minimales Element (bzgl. $\subseteq$).

(c) Jede absteigende Kette $M_1 \supseteq M_2 \supseteq \ldots$ von Teilmoduln von M stationär wird, d.h. es gibt ein $m \in \mathbb{N}$, sodaß $M_m = M_{m+1} = \ldots$.

Beweis. Übung. □

Bemerkung 4.28. *Ist $N \leq M$ so gilt M Artinsch $\Leftrightarrow$ N und M/N Artinsch.*

Bemerkung 4.29. *Ein A-Modul M hat genau dann eine Kompositionsreihe, wenn M Artinsch und Noethersch ist.*

Bemerkung 4.30. *Ist K ein Körper und A eine endlich dimensionale K-Algebra, so ist A Artinsch und Noethersch.*

Lemma 4.31. *(Fitting) Sei M ein A-Modul, $\varphi \in \mathrm{End}_A(M)$.*

(a) *Ist M Artinsch, so gibt es ein $n \in \mathbb{N}$ mit $M = Bild\varphi^m + Kern\varphi^m$ für alle $m \geq n$. φ ist genau dann bijektiv, wenn φ injektiv ist.*

(b) *Ist M Noethersch, so gibt es ein $n \in \mathbb{N}$ mit $0 = Bild\varphi^m \cap Kern\varphi^m$ für alle $m \geq n$. φ ist genau dann bijektiv, wenn φ surjektiv ist.*

(c) *Ist M Artinsch und Noethersch, so gibt es ein $n \in \mathbb{N}$ mit $M = Bild\varphi^m \oplus Kern\varphi^m$ für alle $m \geq n$.*

Beweis. (a) Die absteigende Kette $M > Bild(\varphi) > Bild(\varphi^2) > \ldots$ wird konstant, es gibt also ein $n \in \mathbb{N}$ mit $Bild(\varphi^n) = Bild(\varphi^m)$ für alle $m \geq n$. Für alle $m \geq n$ und $x \in M$ gilt dann $\varphi^m(x) \in Bild(\varphi^m) = Bild(\varphi^{2m})$, also gibt es ein $y \in M$ mit $\varphi^m(x) = \varphi^{2m}(y)$, also $x - \varphi^m(y) \in Kern(\varphi^m)$ und somit $x \in Bild\varphi^m + Kern\varphi^m$. Ist φ injektiv, so ist $Kern(\varphi^m) = 0$ für alle $m \in \mathbb{N}$ und also $M = Bild(\varphi^m)$ für große m und somit auch für alle m und somit φ surjektiv.
(b) als Übung und (c) folgt direkt aus (a) und (b) □

4.4 Das Jacobson-Radikal eines Rings

Definition 4.32. *Sei A ein Ring und M ein endlich erzeugter A-Modul.*
$J(A) := \bigcap\{I \mid I$ ist maximales Linksideal von $A\}$ heißt das **Jacobsonradikal** *von A.*
$J(M) := \bigcap\{N \mid N$ ist maximale Teilmodul von $M\}$ heißt das **Jacobsonradikal** *von M.*

Beispiel: $J(\mathbb{Z}) = \{0\}$.

Lemma 4.33. *Sei $M \neq \{0\}$ ein endlich erzeugter A-Modul. Dann existieren maximale A-Teilmoduln in M.*

Beweis. Falls M Noethersch ist, ist die Behauptung klar, sonst benutzen wir das Lemma von Zorn: Sei $M = \langle m_1, \ldots, m_n \rangle_A$ und $\mathcal{T}$ die Menge aller echten A-Teilmoduln von M. $\mathcal{T}$ ist durch Inklusion partiell geordnet. Jede total geordnete Teilmenge von $\mathcal{T}$ hat eine obere Schranke in $\mathcal{T}$. Sei $K := \{M_j \mid j \in J\}$ total geordnet, dann ist $U := \bigcup_{j \in J} M_j$ eine obere Schranke von K in $\mathcal{T}$. Falls $U = M$, so gibt es für $i = 1, \ldots, n$ ein $j_i \in J$ mit $v_i \in M_{j_i}$. Sei $M' \in K$ das größte dieser M_{j_i}. Dann ist $M = M'$, was im Widerspruch zu der Definition von K steht. Mit dem Lemma von Zorn folgt die Behauptung.

Bemerkung 4.34. *Ist $N < M$ ein echter Teilmodul eines endlich erzeugten A-Moduls M, so zeigt man durch Übergang zu M/N, dass ein maximaler Teilmodul $X < M$ existiert, mit $N \leq X$.*
Ebenso zeigt man: Ist I ein Linksideal von A, dann existiert ein maximales Linksideal M von A mit $I \subseteq M$. (Beachte: $A/I = \langle 1 + I \rangle_A$ ist endlich erzeugt.)

Satz 4.35. *A sei ein Ring (mit 1).*

(i) *$J(A) = \bigcap\{Ann(M) \mid M$ ist einfacher Linksmodul von $A\}$ insbesondere ist $J(A) \trianglelefteq A$.*

(ii) $a \in J(A) \Leftrightarrow 1 - xa$ *hat Linksinverses* für alle $x \in A$.

(iii) $J(A)$ *ist das größte Ideal* I *mit*

$$* \; a \in I \Rightarrow 1 - a \in A^\star.$$

(iv) $J(A) := \bigcap\{I \mid I \text{ ist maximales Rechtsideal von } A\}$

Beweis. Es ist $Ann(M) := \{x \in A \mid xM = 0\} \trianglelefteq A$.

(i) M einfach $\Leftrightarrow M \cong A/I$ für ein maximales Linksideal I. Klar: $Ann(M) \subseteq I$. Also ist $J(A) \supseteq \bigcap\{Ann(M) \mid M \text{ ist einfacher Linksmodul von } A\}$.

Ist M ein einfacher A-Modul, so ist $M = Am$ für jedes $m \in M \setminus \{0\}$. $M = Am \cong A/Ann_A(m)$, wo $Ann_A(m) := \{x \in A \mid xm = 0\}$. $Ann_A(m)$ ist ein maximales Linksideal von A, folglich ist $Ann_A(m) \supseteq J(A)$. Also $J(A)m = 0 \Rightarrow J(A) \subseteq Ann(M)$.

(ii) "$\Rightarrow$" Sei $a \in J(A)$. Angenommen $1 - xa$ hat kein Linksinverses in A für ein $x \in A$. Dann also $A(1 - xa) \neq A$ und es gibt ein maximales Linksideal M von A mit $1 - xa \in A(1 - xa) \subseteq M$. Folglich $1 = (1 - xa) + xa \in M$, Widerspruch!

"$\Leftarrow$" Sei $a \notin J(A)$. Dann ist $a \notin M$ für ein maximales Linksideal M von A. Also ist $A = M + Aa$ und es gibt $x \in A.b \in M$ mit $1 = b + xa$. Dann hat aber $1 - xa = b \in M$ kein Linksinverses in A.

(iii) Sei $a \in J(A)$. Dann gibt es $b \in A$ mit $b(1-a) = 1$. $b = 1+ba$ hat mit (ii) Linksinverses $c \in A$. Folglich ist $c = cb(1 - a) = 1 - a$ und $(1 - a)b = 1$. Also erfüllt $J(A)$ $*$. Sei nun $I \trianglelefteq A$ mit $*$. Falls $I \not\subseteq J(A)$, so gibt es ein maximales Ideal M von A mit $I \not\subseteq M$. $I + M = A \Rightarrow$ es gibt $a \in I, b \in M$ mit $a + b = 1$. Dann ist $1 - a = b \notin A^\star$.

(iv) Definieren $J_{rechts}(A)$ analog. Dann sind (i)-(iii) erfüllt. Die Charakterisierung von $J(A)$ in (iii) ist aber unabhängig von links und rechts.

Bemerkung 4.36. *Sei* M *ein endlich erzeugter* A*-Modul. Dann ist* $J(A)M \subseteq J(M)$. *Ist* A *Artinsch, so gilt sogar* $J(A)M = J(M)$.

Beweis. Übung. □

Aus dem Homomorphiesatz folgt, dass für $I \trianglelefteq A$ die maximalen Linksideale von A/I genau die maximalen Linksideale von A sind, die I enthalten. Insbesondere ergibt sich

Bemerkung 4.37. $I \trianglelefteq A$ *mit* $I \subseteq J(A) \Rightarrow J(A/I) = J(A)/I$.

Satz 4.38. *Ist* A *halbeinfach, so ist* $J(A) = \{0\}$. *Umgekehrt gilt für einen Artinschen Ring* A, *dass* $A/J(A)$ *halbeinfach ist.* $J(A)$ *ist also das kleinste zweiseitige Ideal mit halbeinfachem Faktorring.*

Beweis. Ist A halbeinfach, so ist ${}_AA$ direkte Summe einfacher A-Moduln. Für $a \in J(A)$ gilt $aM = \{0\}$ für jeden einfachen A-Modul, also auch $aA = 0$ und somit $a = a1 = 0$.
Sei jetzt umgekehrt A Artinsch und $\overline{A} := A/J(A)$. Sei $\mathcal{X} := \{X \mid X \text{ ist maximales Linksideal}$

von $A\}$. Da A Artinsch ist, gibt es endlich viele $X_i \in \mathcal{X}$ $(i = 1, \ldots, n)$ mit $J(A) = \bigcap_{i=1}^n X_i$. Dann ist

$$\iota : A/J(A) \to \bigoplus_{i=1}^n A/X_i, a + J(A) \mapsto (a + X_i)_{i=1}^n$$

ein injektiver A-Modulhomomorphismus in den halbeinfachen A-Modul $\bigoplus_{i=1}^n A/X_i$. Also ist $A/J(A)$ als Teilmodul eines halbeinfachen A-Moduls wieder halbeinfach. □

Folgerung 4.39. *Sei A Artinsch. Dann gilt für einen A-Modul M:*
M ist halbeinfach $\Leftrightarrow J(A)M = \{0\}$.

Beweis. Ist M halbeinfach, dann ist M ein $A/J(A)$-Modul, also $J(A)M = \{0\}$. Umgekehrt, ist $J(A)M = 0$, so ist M ein $A/J(A)$-Modul, also halbeinfach. □

Satz 4.40. *(i) $I \trianglelefteq A$ mit jedem $x \in I$ nilpotent $\Rightarrow I \subseteq J(A)$.*

(ii) Ist A Artinsch, so folgt: $J(A)$ ist nilpotent, d. h. es gibt $n \in \mathbb{N}$ mit $J(A)^n = \{0\}$.

Beweis.

(i) $a \in I,\ x \in A \Rightarrow ax$ nilpotent $\Rightarrow 1 - ax \in A^\star$.

(ii) Da A Artinsch ist, wird $J(A) \geq J(A)^2 \geq \ldots$ stationär. Es gibt also $N := J(A)^n = J(A)^{n+1}$. Angenommen $N \neq 0$. Sei $\mathcal{I} := \{I \mid I \text{ Linksideal von } A, NI \neq 0\}$. Dann $N \in \mathcal{I}$. Wähle ein minimales Element $I_0 \in \mathcal{I}$. Dann gibt es $a \in I_0$ so, daß $Na \neq 0$. $Na \subseteq I_0 \Rightarrow Na = I_0$. Also existiert ein $b \in N$ so, daß $ba = a \Rightarrow (1 - b)a = 0 \Rightarrow a = 0$, da $1 - b \in A^\star$. Dies liefert einen Widerspruch zu $Na \neq 0$.

Beispiel: $J(\Delta_n(K))$ (obere Dreiecksmatrizen).

Satz 4.41. *(Asumaya/Nakayama)*

(i) V sei ein A-Modul, W ein A-Teilmodul von V, so dass V/W ein endlich erzeugter A-Modul ist. Gilt $V = W + J(A)V$ so gilt schon $V = W$.

(ii) Ist V ein endlich erzeugter A-Modul mit $J(A)V = V$ so ist $V = \{0\}$.

Beweis.

(i) Falls $W \neq V$ ist, so existiert ein maximaler A-Teilmodul M von V mit $W \subseteq M$. V/M ist ein einfacher A-Modul, also $J(A)V \subseteq M \Rightarrow V = W + J(A)V \subseteq M$.

(ii) Setze $W = 0$ in (i).

Definition 4.42. *Ein Element $e \in A$ heißt* **Idempotent**, *falls $e^2 = e$ und $e \neq 0$ gilt.*

Satz 4.43. *Sei $e \in A$ ein Idempotent Dann ist eAe ein Ring mit Einselement e. $J(eAe) = eJ(A)e = eAe \cap J(A)$.*

Beweis. Klar ist $eAe \cap J(A) = eJ(A)e$.

Zeigen: $eJ(A)e \subseteq J(eAe)$

Sei $a \in J(A)$. Dann ist $eae \in J(A)$,also gibt es $b \in A$ mit $(1-eae)b = 1$ und $b(1-eae) = 1$. Multiplikation von beiden Seiten mit e liefert: $(e - eae)ebe = e$ und $ebe(e - eae) = e$, also $eJ(A)e \subseteq J(eAe)$.

Zeigen: $eJ(A)e \supseteq J(eAe)$

Dazu genügt es zu zeigen, daß $J(eAe)V = 0$ für alle einfachen A-Moduln V ist. Dies ist klar, falls $eV = 0$. Sonst sei $0 \neq W$ ein eAe-Teilmodul von V. Dann ist $AW = V$ und $eV = eAW = eAeW = W$. Also ist eV ein einfacher eAe-Modul. $0 = J(eAe)eV = J(eAe)V$.

Satz 4.44. *Sei A eine endlich dimensionale K-Algebra, K ein Körper.*
Dann ist $J(Z(A)) = J(A) \cap Z(A)$.

Beweis.

'$\supseteq$' Folgt aus Satz 4.40.

'$\subseteq$' $J(Z(A))A$ ist ein nilpotentes Ideal von A, also ist $J(Z(A))A \subseteq J(A)$. Folglich $J(Z(A)) \subseteq J(A) \cap Z(A)$.

Übung: $J(A^{n\times n}) = J(A)^{n\times n}$.

4.5 Der Satz von Krull-Schmidt

Definition 4.45. *Ein A-Modul M heißt* **unzerlegbar**, *falls für jedes Paar von Teilmoduln $S, T \leq M$ mit $S \cap T = \{0\}$ und $S + T = M$ (kurz $M = S \oplus T$) gilt dass $S = \{0\}$ oder $T = \{0\}$.*

Bemerkung 4.46. *Sei M ein A-Modul und $e \in \mathrm{End}_A(M)$ ein Idempotent.*
Dann sind $eM = Bild(e)$ und $(1 - e)M = Kern(e)$ Teilmoduln.
Die Einschränkung von e auf $Bild(e)$ ist die Identität und auf $Kern(e)$ die Nullabbildung.
Insbesondere gilt $M = eM \oplus (1 - e)M$.
Ist umgekehrt $M = S \oplus T$ mit A-Teilmoduln S, T so definiert $e : M \to M, e(s + t) := s$ für alle $s \in S, t \in T$ einen A-Modul-Endomorphismus von M mit $eM = S$, $(1 - e)M = T$.

Folgerung 4.47. *Ein A-Modul M ist unzerlegbar, genau dann wenn 1 das einzige Idempotent in $\mathrm{End}_A(M)$ ist.*

Definition 4.48. *Ein Ring heißt* **lokal**, *wenn die Nichteinheiten ein zweiseitiges Ideal bilden.*

Satz 4.49. *Äquivalent sind für einen Ring A:*

(a) A ist lokal.

(b) $J(A) = A \setminus A^*$ ist ein maximales Ideal in A.

(c) $A/J(A)$ ist ein Schiefkörper.

Beweis. (a) $\Rightarrow$ (b): Ist jedes maximale Ideal von A liegt in $A \setminus A^*$. Bilden die Nichteinheiten also ein Ideal, so ist dies das einzige maximale Ideal von A, also gleich $J(A)$.
(b) $\Rightarrow$ (c): Sei $a \in A \setminus J(A) = A^*$. Dann ist $a \in A$ invertierbar, also auch in $A/J(A)$. In dem Restklassenring ist also jedes Element ungleich 0 invertierbar, also ist dies ein Schiefkörper.
(c) $\Rightarrow$ (a): Wir zeigen $A^* = A \setminus J(A)$. Sei dazu $a \in A \setminus J(A)$. Dann gibt es nach Voraussetzung $c \in A, b \in J(A)$ mit $ac = 1 - b$. Nach Satz 4.35 hat aber dann $(1 - b) \in A^*$ ein Inverses und somit hat a ein Rechtsinverses. Analog hat a ein Linksinverses. Somit ist $a \in A^*$. □

Lemma 4.50. *Sei A ein lokaler Ring und $1 = \sum_{i=1}^{n} a_i$ mit $a_i \in A$. Dann gibt es ein i so dass $a_i \in A^*$.*

Beweis. Ansonsten sind alle a_i Nichteinheiten, liegen also in $J(A)$ und damit auch die Summe, $1 \in J(A)$ ein Widerspruch. □

Satz 4.51. *Ein lokaler Ring hat nur 1 als Idempotent.*
Ist insbesondere M ein A-Modul mit $\mathrm{End}_A(M)$ lokal, so ist M unzerlegbar.

Beweis. Sei A ein lokaler Ring und $1 \neq e = e^2 \neq 0 \in A$ ein Idempotent Dann sind sowohl e als auch $1 - e$ keine Einheiten in A, liegen also in $J(A)$. Dann aber auch $1 \in J(A)$ ein Widerspruch. □

Satz 4.52. *Ist M ein unzerlegbarer A-Modul mit endlicher Kompositionsreihe (also Artinsch und Noethersch), so ist $\mathrm{End}_A(M)$ ein lokaler Ring. Alle $\varphi \in \mathrm{End}_A(M) \setminus \mathrm{End}_A(M)^*$ sind nilpotent (erfüllen also $\varphi^m = 0$ für ein $m \in \mathbb{N}$).*

Beweis. Wir benutzen das Lemma von Fitting. Sei $\varphi \in \mathrm{End}_A(M)$ nicht bijektiv. Dann ist nach dem Lemma von Fitting φ weder injektiv noch surjektiv. Weiter gibt es ein $n \in \mathbb{N}$ mit $M = Bild(\varphi^m) \oplus Kern(\varphi^m)$ für alle $m \geq n$. Da M unzerlegbar ist, gilt entweder $Kern(\varphi^m) = 0$ (ein Widerspruch dazu, dass φ nicht injektiv ist) oder $Bild(\varphi^m) = 0$. Dann ist also $\varphi^m = 0$ für ein m und φ ist nilpotent.
Wir zeigen jetzt dass die Nichteinheiten in $\mathrm{End}_A(M)$ ein zweiseitiges Ideal bilden. Dazu sei $\varphi, \psi \in \mathrm{End}_A(M)$ nicht bijektiv und $\alpha \in \mathrm{End}_A(M)$ beliebig. Dann ist $\alpha \circ \varphi$ nicht injektiv (also eine Nichteinheit) und ebenso $\varphi \circ \alpha$ nicht surjektiv, (also auch eine Nichteinheit).
Angenommen $\varphi + \psi$ ist eine Einheit in $\mathrm{End}_A(M)$. Dann gibt es also $\beta \in \mathrm{End}_A(M)$ mit

$$\beta \circ (\varphi + \psi) = (\varphi + \psi) \circ \beta = id$$

Insbesondere vertauschen $\beta\psi = id - \beta\varphi$ und $\beta\varphi$. Weiter gibt es $m \in \mathbb{N}$ mit $(\beta\varphi)^m = (\beta\psi)^m = 0$. Dann ist $(\beta\varphi + \beta\psi)^{2m} = 0$ (ausmultiplizieren, jeder Summand $(\beta\psi)^k(\beta\varphi)^\ell$ enthält einen Faktor 0, da $k + \ell = 2m$ also $\max(k, \ell) \geq m$.) Ein Widerspruch zu $\beta\varphi + \beta\psi = id$ □

Satz 4.53. *Sei M Noethersch oder Artinsch. Dann lässt sich M schreiben als endliche direkte Summe unzerlegbarer A-Moduln, $M = M_1 \oplus \ldots \oplus M_r$.*

Beweis. Ist M unzerlegbar, dann ist die Behauptung klar. Sonst gibt es $S \neq 0 \neq T \leq M$ mit $M = S \oplus T$. Mache weiter so mit S und T anstelle von M. Da M die aufsteigende oder absteigende Kettenbedingung erfüllt terminiert dieser Prozess nach endlich vielen Schritten. □

Beispiel Im allgemeinen ist eine Zerlegung in unzerlegbare Moduln nicht eindeutig. Sei z.B. $R = \mathbb{Z}[\sqrt{-5}]$, $I_1 := (3, 1+2\sqrt{-5})$ $I_2 := (3, 1-2\sqrt{-5})$. Dann ist $I_1 + I_2 = R, I_1 \cap I_2 = 3R$ und

$$R \oplus 3R \cong I_1 \oplus I_2$$

jedoch sind weder I_1 noch I_2 isomorph zu R, da beides keine Hauptideale sind.

Satz 4.54. *(Krull-Schmidt) Seien $M_1, \ldots, M_s, N_1, \ldots N_t$ unzerlegbare A-Moduln mit $\mathrm{End}_A(M_i)$ lokal. Gilt $M := M_1 \oplus \ldots \oplus M_s = N_1 \oplus \ldots \oplus N_t$, so ist $s = t$ und es gibt ein $p \in S_s$ mit $M_{p(i)} \cong N_i$.*

Beweis. Seien $\pi_i : M \to M_i$ die Projektionen bezüglich der Zerlegung.
1. Behauptung. Ist $\sigma \in \mathrm{End}_A(M)$ so dass $\pi_1 \circ \sigma : M_1 \to M_1$ ein Isomorphismus ist, so ist $M = \sigma(M_1) \oplus M_2 \oplus \ldots \oplus M_s$.
Denn sowohl $\sigma_{|M_1} : M_1 \to \sigma(M_1)$ also auch $(\pi_1)_{\sigma(M_1)} : \sigma(M_1) \to M_1$ sind Isomorphismen also ist $\sigma(M_1) \cap ker(\pi_1) = \{0\}$. (Beachte: $ker(\pi_1) = M_2 \oplus \ldots \oplus M_s$ also ist die Summe direkt.) Weiter gibt es für jede $x \in M$ ein $x_1 \in M_1$ so dass $\pi_1(x) = \pi_1(\sigma(x_1))$, also $x - \sigma(x_1) \in ker(\pi_1)$ und daher erzeugen $\sigma(M_1) \oplus M_2 \oplus \ldots \oplus M_s$ ganz M.
2. Schritt. Sei $\sigma_j \in \mathrm{End}_A(M)$ die Projektionen auf N_j bzgl. der Zerlegung $M = N_1 \oplus \ldots \oplus N_t$. Dann ist $\sum_{j=1}^{t} \sigma_j = \mathrm{id}_M$ und daher

$$\mathrm{id}_{M_1} = \sum_{j=1}^{t} \pi_1 \circ (\sigma_j)_{|M_1}.$$

Da $\mathrm{End}_A(M_1)$ lokal ist, gibt es ein j mit $\pi_1 \circ \sigma_j : M_1 \to M_1$ ein Isomorphismus. Also ist nach der ersten Behauptung

$$M = \sigma_j(M_1) \oplus M_2 \oplus \ldots \oplus M_s \text{ und } \sigma_j(M_1) \cong M_1.$$

Dies liefert auch eine Zerlegung von

$$N_j = N_j \cap \sigma_j(M_1) \oplus M_2 \cap N_j \oplus \ldots \oplus M_s \cap N_j.$$

Da $N_j \cap \sigma_j(M_1) \cong M_1 \neq \{0\}$ ist und N_j unzerlegbar gilt $N_j = \sigma_j(M_1)$. Setze also $p(1) := j$.
3. Schritt Fahre fort mit M_2 anstelle von M_1 und finde so $p(2) \neq p(1)$ mit

$$M = N_{p(1)} \oplus N_{p(2)} \oplus M_3 \oplus \ldots \oplus M_s.$$

Man erhält so schließlich $s \leq t$ und

$$M = N_{p(1)} \oplus N_{p(2)} \oplus N_{p(3)} \oplus \ldots \oplus N_{p(s)}.$$

Daraus folgt aber auch $s = t$, da $M = N_1 \oplus \ldots \oplus N_t$. □

Folgerung 4.55. *Sei M ein Modul mit Kompositionsreihe (also M Noethersch und Artinsch). Dann hat M eine Zerlegung $M = M_1 \oplus \ldots \oplus M_t$ mit unzerlegbaren Teilmoduln M_i und für jede weitere solche Zerlegung $M = N_1 \oplus \ldots \oplus N_s$ ist $s = t$ und es gibt ein $\pi \in S_s$ mit $M_i \cong N_{\pi(i)}$.*

4.6 Idempotente

Definition 4.56. *(a) Ein Element $e \in A$ heißt* **Idempotent**, *falls $e^2 = e$ und $e \neq 0$ gilt.*

(b) Zwei Idempotente e und f heißen **orthogonal**, *falls $ef = fe = 0$ gilt. Dann ist $e + f$ ebenfalls ein Idempotent.*

(c) Ein Idempotent $e \in A$ heißt **primitives Idempotent**, *falls e nicht Summe zweier orthogonaler Idempotente ist und* **zentral primitiv**, *falls $e \in Z(A)$ ein primitives Idempotent in $Z(A)$ ist.*

(d) Eine Zerlegung $1 = e_1 + \ldots + e_n$ mit $e_i e_j = \delta_{ij} e_i$, heißt Zerlegung der 1 in orthogonale Idempotente.

Satz 4.57. *Sei R ein kommutativer Ring. Falls $1 = e_1 + \ldots + e_n$ eine Zerlegung der Eins in orthogonale primitive Idempotente ist, so ist $\{e_1, \ldots, e_n\} = \{e^2 = e \in R \mid e \text{ primitiv}\}$ und jedes Idempotent in R ist eine Summe der e_i. Insbesondere bilden die zentral primitiven Idempotente eines Rings A ein System orthogonaler Idempotente.*

Beweis. Sei $e^2 = e \in R$. Dann ist

$$e = e1 = ee_1 + \ldots + ee_n \text{ und } (ee_i)(ee_j) = \delta_{ij} ee_i$$

Weiter ist $e_i = ee_i + (1-e)e_i$ eine Summe orthogonaler Idempotente. Da e_i primitv war folgt $ee_i = 0$ oder $ee_i = e_i$. Also ist $e = \sum_{ee_i \neq 0} e_i$. □

Satz 4.58. *Seien $e, f \in A$ Idempotente und M ein A-Modul. Dann gilt*

(a) $Hom_A(Ae, M) \cong eM$ als abelsche Gruppen vermöge $\epsilon : \varphi \mapsto \varphi(e)$.

(b) $End_A(Ae) \cong eA^{op}e$ als Ring.

Beweis. (a) Sei $\varphi \in Hom_A(Ae, M)$. Dann ist φ eindeutig bestimmt durch das Bild $\varphi(e)$ des Erzeugers. Es gilt $e\varphi(e) = \varphi(e^2) = \varphi(e)$, also liegt $\epsilon(\varphi)$ in eM. Umgekehrt definiert für $m \in M$ die Abbildung $ae \mapsto aem$ einen A-Modulhomomorphismus, d.h. $\epsilon^{-1}(em) = (ae \mapsto aem)$.
(b) Der Isomorphismus als abelsche Gruppen ergibt sich aus (a), indem wir $\varphi \in End_A(Ae)$ abbilden auf $\varphi(e)$. Die Eins des Rings $eA^{op}e$ ist $e = id(e)$. Weiter ist für $\varphi, \psi \in End_A(Ae)$

$$\psi(\varphi(e)) \overset{\varphi(e) \in Ae}{=} \psi(\varphi(e)e) \overset{A-Modulhom}{=} \varphi(e)\psi(e).$$

□

Bemerkung 4.59. *(Idempotente und Projektionen) Ist $e = \sum_{i=1}^n e_i$ eine Summe orthogonaler Idempotente, so ist $Ae = \oplus_{i=1}^n Ae_i$ eine direkte Summe von A-Moduln. Ist umgekehrt $Ae = I_1 \oplus \ldots \oplus I_k$ eine direkte Summe von Linksmoduln so sind die Projektionen $\pi_1, \ldots, \pi_k \in \mathrm{End}_A(Ae) = eA^{op}e \subset A^{op}$ orthogonale Idempotente mit $e = \pi_1 + \ldots + \pi_k$. Da A und A^{op} als Mengen gleich sind und die gleichen orthogonalen Idempotente haben, erhält man eine Zerlegung von e in orthogonale Idempotente in A.*
Analoges gilt für zentrale Idempotente und 2-seitige Ideale.

Folgerung 4.60. *Sei $e \in A$ ein Idempotent. Äquivalent sind:*

(a) e ist primitiv.

(b) Ae ist unzerlegbarer A-Linksmodul.

(b') eA ist unzerlegbarer A-Rechtsmodul.

(c) e ist das einzige Idempotent in eAe.

Satz 4.61. *Seien $e, f \in A$ Idempotente. Äquivalent sind:*

(a) $Ae \cong Af$.

(b) $eA \cong fA$ als A-Rechtsmoduln.

(c) Es gibt $a \in eAf$, $b \in fAe$ mit $ab = e$ und $ba = f$.

In dem Fall heißen die Idempotente e und f **äquivalent**.

Beweis. Wir zeigen nur (a) $\Leftrightarrow$ (c). Die Äquivalenz von (b) und (c) ergibt sich genauso.
Sei $\varphi : Ae \to Af$ ein A-Modulisomorphismus und setze $a := \varphi(e)$, $b := \varphi^{-1}(f)$. Dann ist $a \in eAf$ und $b \in fAe$ und

$$f = \varphi(\varphi^{-1}(f)) = \varphi(b) = \varphi(be) = b\varphi(e) = ba$$

und ebenso $e = ab$.
Sind $a \in eAf$, $b \in fAe$ mit $ab = e$ und $ba = f$ gegeben, so definiere $\varphi : Ae \to Af$ durch $\varphi(e) := a$. Dies definiert einen A-Modulhomomorphismus mit Umkehrhom. def. durch $\psi(f) := b$. Dann ist

$$\varphi(\psi(f)) = \varphi(b) = \varphi(be) = b\varphi(e) = ba = f$$

und ebenso $\psi(\varphi(e)) = e$, also $\psi = \varphi^{-1}$. □

Satz 4.62. *Sei $\overline{A} := A/J(A)$, $e, f \in A$ Idempotente. Dann gilt*

$$Ae \cong Af \Leftrightarrow \overline{A}\overline{e} \cong \overline{Af}.$$

Beweis. $\Rightarrow$ ist klar, zeigen nur $\Leftarrow$: Es gibt nach dem letzten Satz also $a, b \in A$ mit

$$\overline{f}\overline{ae} = \overline{a}, \overline{e}\overline{bf} = \overline{b}, \overline{a}\overline{b} = \overline{f}, \overline{b}\overline{a} = \overline{e}.$$

Indem wir a durch fae und b durch ebf ersetzen können wir annehmen dass $a = fae$ und $b = ebf$ gelten.Es ist $ab = f - c$ für ein $c \in J(A)$. Da $ab \in fAf$ gilt $c \in J(fAf)$, also ist ab eine Einheit in fAf. Also ist Rechtsmultiplikation mit ab ein Automorphismus von fAf. Ebenso ergibt sich, dass ba Einheit in eAe. Also hat die Rechtsmultiplikation mit $a \in fAe$:

$$\varphi_a : Af \to Ae, x \mapsto xa$$

sowohl Rechts- als auch Linksinverses, ist also ein Isomorphismus. □

4.6.1 Liften von Idempotenten.

Sei A ein Artinscher Ring, also insbesondere $J(A)$ ein nilpotentes Ideal. Setze $\overline{A} := A/J(A)$.

Satz 4.63. *Sei $c \in \overline{A}$ ein Idempotent. Dann gibt es ein Idempotent $e \in A$ mit $\overline{e} = c$.*

Beweis. Sei $a \in A$ mit $\overline{a} = c$. Dann ist $a^2 - a \in J(A)$ und daher nilpotent, d.h. es gibt ein minimales $n \in \mathbb{N}$ mit $(a^2 - a)^n = 0$. Setze

$$b := 3a^2 - 2a^3.$$

Dann ist $\overline{b} = \overline{a}$ und $b^2 - b = (a^2 - a)^2(4a^2 - 4a - 3)$, insbesondere $(b^2 - b)^m = 0$ mit $m = \lceil \frac{n}{2} \rceil < n$ falls $n > 1$. Nach endlich vielen Wiederholungen konstruieren wir also ein $e \in A$ mit $\overline{e} = c$ und $e^2 = e$. □

Satz 4.64. *Sei $1 = c_1 + \ldots + c_k$ eine Zerlegung der Eins in orthogonale Idempotent von $\overline{A}$. Dann gibt es orthogonale Idempotente $e_1, \ldots, e_k \in A$ mit $\overline{e}_i = c_i$ für alle i und $1 = e_1 + \ldots + e_k$.*

Beweis. Induktion über k. Für $k = 1$ war dies der letzte Satz. Sei also $k > 1$. Nach Satz 4.63 kann man c_1 zu einem Idempotent $e_1 \in A$ liften. Setze $B := (1 - e_1)A(1 - e_1)$. Dann ist B ein Ring mit Einselement $(1 - e_1)$ und $\overline{1 - e_1} = c_2 + \ldots + c_k \in \overline{B} = B/J(B)$. Nach Induktionsvoraussetzung kann man diese orthogonale Zerlegung zu einer orthogonalen Zerlegung $1 - e_1 = e_2 + \ldots + e_k$ in B liften. Es ist $e_1 e_j = e_1(1 - e_1)e_j(1 - e_1) = 0$ für $j = 2, \ldots, k$ und ebenso $e_j e_1 = 0$, also haben wir orthogonale Idempotente in A mit $1 = e_1 + \ldots + e_k$. □

Folgerung 4.65. *Ein Idempotent $e \in A$ ist primitiv, genau dann wenn $\overline{e} \in A/J(A)$ primitiv ist.*

Bemerkung 4.66. *Jeder einfache A-Modul ist ein (einfacher) $A/J(A)$-Modul. Ist also A Artinsch, so sind die einfachen A-Moduln genau die direkten Summanden von $A/J(A)$. Ist $1 = c_1 + \ldots + c_k$ eine Zerlegung der Eins in primitive orthogonale Idempotente von $A/J(A)$ so ist*

$$\overline{A} = A/J(A) = \bigoplus_{i=1}^{k} \overline{A}c_i \text{ wobei } \overline{A}c_i \text{ einfach .}$$

Durchläuft also c ein Vertretersystem der Äquivalenzklassen primitiver Idempotente in $\overline{A}$, so durchäuft $\overline{A}c$ ein Vertretersystem der einfachen A-Moduln.

Beispiel: $\Delta_n(K)$.

4.7 Projektive und injektive Moduln

4.7.1 Projektive Moduln

Definition 4.67. *Seien $f_i : M_{i-1} \to M_i$ mit $a \leq i \leq b$ (wobei $a = -\infty, b = \infty$ zugelassen sind) A-Modulhomomorphismen. Die Folge*

$$\ldots \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$$

heißt **exakt** *(eine* **exakte Folge von** A**-Moduln***), falls für alle* $a < i \leq b$ *gilt*

$$Kern(f_i) = Bild(f_{i-1}).$$

Eine **kurze exakte Folge** *ist eine exakte Folge*

$$(\star) \quad 0 \to U \xrightarrow{g} M \xrightarrow{f} F \to 0$$

wobei die erste und letze Abbildung die Nullabbildung ist. Also ist g *injektiv,* f *ist surjektiv und* $Bild(g) = Kern(f)$*. Fasst man* $Bild(g) \cong U$ *als Teilmodul von* M *auf, so ist* F *vermöge* f *isomorph zum Faktormodul* M/U*.*
Die k.e.F. $(\star)$ **spaltet***, falls es einen (injektiven)* A*-Modulhomomorphismus* $h : F \to M$ *gibt mit* $f \circ h = \mathrm{id}_F$*. Dann ist* $M = Bild(g) \oplus Bild(h) \cong U \oplus F$*.*

Satz 4.68. *Sei* P *ein* A*-Modul. Dann sind äquivalent*

(a) Jede kurze exakte Folge $0 \to L \to M \to P \to 0$ *von* A*-Moduln spaltet.*

(b) Für jeden surjektiven A*-Modulhomomorphismus* $\pi : M \to N$ *und jeden* A*-Modulhomomorphismus* $\varphi : P \to N$ *gibt es einen* A*-Modulhomomorphismus* $\psi : P \to M$ *mit* $\varphi = \pi \circ \psi$*.*

Erfüllt P *eine der beiden Bedingungen, so heißt* P *ein* **projektiver** A*-Modul.*

Beweis. Angenommen P erfüllt (b). Sei $0 \to L \to M \xrightarrow{\pi} P \to 0$ eine k.e.F. Wenden (b) mit $N = P$, $\varphi = \mathrm{id}_P$ und die surjektive Abbildung $\pi : M \to N$ an. Dann gibt es also eine Abbildung $\psi : P \to M$ mit $\mathrm{id}_P = \pi \circ \psi$. Die Abbildung ψ liefert eine Spaltung der k.e.F.
Nun erfülle P die Bedingung (a). Sei $\pi : M \to N$ surjektiv und $\varphi : P \to N$ gegeben. Dann konstruiere den A-Modul

$$M' := \{(x, y) \in M \oplus P \mid \pi(x) = \varphi(y)\} \leq M \oplus P.$$

Wir erhalten die k.e.F.

$$0 \to \ker(\pi) \xrightarrow{f} M' \xrightarrow{g} P \to 0$$

wobei $f(x) = (x, 0)$ und $g(x, y) = y$. Diese k.e.F. spaltet nach Voraussetzung, es gibt also $h : P \to M'$ mit $g \circ h = \mathrm{id}_P$, also eine Abbildung $\psi : P \to N$ mit $h(y) = (\psi(y), y) \in M'$. Für diese Abbildung ψ ist $\pi \circ \psi = \varphi$. □

Bemerkung. Die Bedingung (b) kann man auch so ausdrücken: Ist $g : M \to N$ ein Epimorphismus, so ist die induzierte Abbildung

$$g_* : Hom_A(P, M) \to Hom_A(P, N), f \mapsto g \circ f$$

ebenfalls surjektiv.

Bemerkung 4.69. *Ist* L *ein freier* A*-Modul, so ist* L *projektiv.*

Beweis. Ist L frei auf X und $M \xrightarrow{\pi} L$ surjektiv. Für jedes $x \in X$ wähle ein $m_x \in M$ mit $\pi(m_x) = x$. Dann existiert genau ein A-Modulhomomorphismus $\psi : L \to M$ mit $\psi(m_x) = x$. Es gilt dann $\psi \circ \pi = \mathrm{id}_P$. □

Satz 4.70. *Ein A-Modul P ist genau dann projektiv, wenn es einen weiteren A-Modul P' gibt, so dass $P \oplus P'$ ein freier A-Modul ist.*
Ist P endlich erzeugt, so gibt es ein P' und ein $n \in \mathbb{N}$ mit $P \oplus P' \cong {}_AA^n$.

Beweis. Jeder A-Modul ist epimorphes Bild eines freien A-Moduls. Also gibt es einen freien A-Modul L und einen Epimorphismus $\pi : L \to P$. Wir erhalten also die k.e.F.

$$0 \to \ker(\pi) \to L \xrightarrow{\pi} P \to 0$$

Ist P projektiv, so spaltet diese Folge, d.h. es gibt einen A-Modul P' mit $L \cong P \oplus P'$.
Sei umgekehrt P ein direkter Summand eines freien A-Moduls $L = P \oplus P'$. Sei $\pi : M \to N$ und $\varphi : P \to N$ wie in Satz 4.68 (b). Wir können φ zu Abbildung $\varphi' : L \to N$ fortsetzen durch $\varphi'(p + p') := \varphi(p)$. Da L frei und somit projektiv ist, gibt es eine Abbildung $\psi : L \to M$ mit $\pi \circ \psi = \varphi'$. Die Einschränkung von ψ auf P ist eine gewünschte Abbildung. □

Folgerung 4.71. *Direkte Summanden von projektiven Moduln sind wieder projektiv.*

Beispiel: $(3, 1 + 2\sqrt{-5}) \trianglelefteq \mathbb{Z}[\sqrt{-5}] =: A$ ist ein projektiver A-Modul, der nicht frei ist, es ist $(3, 1 + 2\sqrt{-5}) \oplus (3, 1 - 2\sqrt{-5}) \cong A \oplus A$ frei.

Bemerkung 4.72. *Ist A ein Hauptidealbereich, so ist jeder endlich erzeugte projektive A-Modul frei.*

Bemerkung 4.73. *Ein* **PIM** *(projective indecompoable module) ist ein projektiver A-Modul, der unzerlegbar ist. Ist A ein Artinscher Ring und durchläuft e ein Vertretersystem der Äquivalenzklassen primitiver Idempotente von A, so durchäuft Ae genau die Menge aller Isomorphieklassen von PIMs (und $\overline{A}\overline{e}$ die Menge der einfachen A-Moduln). Für jeden PIM P gilt $P/J(P)$ einfach. Zwei PIMs P, Q sind genau dann isomorph, wenn $P/J(P) \cong Q/J(Q)$.*

4.7.2 Injektive Moduln.

Satz 4.74. *Sei Q ein A-Modul. Dann sind äquivalent*

(a) Jede kurze exakte Folge $0 \to Q \to M \to N \to 0$ von A-Moduln spaltet.

(b) Für jeden injektiven A-Modulhomomorphismus $\iota : L \to M$ und jeden A-Modulhomomorphismus $\varphi : L \to Q$ gibt es einen A-Modulhomomorphismus $\psi : M \to Q$ mit $\varphi = \psi \circ \iota$.

Erfüllt Q eine der beiden Bedingungen, so heißt Q ein **injektiver** *A-Modul.*

Beweis. (b) ⇒ (a) als Übung.
Umgekehrt erfülle Q die Bedingung (a) und seien $\iota : L \to M$, $\varphi : L \to Q$ wie in (b). Betrachte

$$M' := (Q \oplus M)/\{(\varphi(x), -\iota(x)) \mid x \in L\}$$

Die Klasse eines Elements $(y, z) \in Q \oplus M$ in M' bezeichnen wir mit $[y, z] \in M'$. Setze $N := M/\iota(L)$ und sei $\pi : M \to N$ der kanonische Epimorphismus. Definiere $f : Q \to M'$

durch $f(y) := [y, 0]$ und $g : M' \to N$ durch $g([y, z]) := \pi(z)$. Dann ist g wohldefiniert und wir erhalten die k.e.F.

$$0 \to Q \xrightarrow{f} M' \xrightarrow{g} N \to 0$$

die nach Voraussetzung spaltet. Es gibt also einen A-Modulhomomorphismus $h : M' \to Q$ mit $h \circ f = \mathrm{id}_Q$. Definiere $\psi : M \to Q$ durch $\psi(z) := h([0, z])$. Für alle $x \in L$ gilt dann

$$\psi \circ \iota(x) = h([0, \iota(x)] = h([\varphi(x), 0]) = h \circ f \circ \varphi(x) = \varphi(x).$$

□

Bemerkung: Die Bedingung 4.74 (b) bedeutet, dass für jeden Teilmodul $L \leq M$ jeder A-Modulhomomorphismus $\varphi : L \to Q$ zu einem Homomorphismus $\tilde{\varphi} : M \to Q$ fortgesetzt werden kann.

Beispiel: $\mathbb{Z}$ ist kein injektiver $\mathbb{Z}$-Modul. Denn der Homomorphismus $2\mathbb{Z} \to \mathbb{Z}$ definiert durch $2a \mapsto a$ läßt sich nicht zu einem Homomorphismus $\mathbb{Z} \to \mathbb{Z}$ fortsetzen, dieser müßte 1 auf ein Element x in $\mathbb{Z}$ abbilden mit $2x = 1$.

Satz 4.75. *Ein A-Modul Q ist genau dann injektiv, wenn es zu jedem Linksideal I von A und jedem A-Modulhomomorphismus $\varphi : I \to Q$ einen A-Modulhomomorphismus $\psi : A \to Q$ gibt mit $\psi_{|I} = \varphi$.*

Beweis. Dies ist offensichtlich eine Abschwächung der Bedingung 4.74 (b). Wir müssen also nur zeigen, dass unter der Bedingung des Satzes, der A-Modul Q injektiv ist.
Erfülle Q die Bedingung von Satz 4.75 und seien $\iota : L \to M$, $\varphi : L \to Q$ wie in Satz 4.74 (b). Œ sei $L = \iota(L) \leq M$. Sei

$$X := \{(L', \varphi') \mid L \subset L' \leq M, \varphi' : L' \to Q, \varphi'_{|L} = \varphi\}.$$

Dann ist X durch $(L_1, \varphi_1) \leq (L_2, \varphi_2) \Leftrightarrow L_1 \leq L_2$ und $(\varphi_2)_{|L_1} = \varphi_1$ induktiv geordnet (Vereinigung als obere Schranke einer Kette). Also enthält X ein maximales Element (M', ψ). Wir wollen zeigen, dass $M' = M$ gilt. Sei dazu $x \in M$ beliebig. Dann ist $I := \{a \in A \mid ax \in M'\}$ ein Linksideal von A. Die Abbildung

$$f : I \to Q, f(a) := \psi(ax)$$

lässt sich nach Voraussetzung zu $g : A \to Q$ fortsetzen. Betrachten nun

$$\psi' : M' \oplus A \to Q, \psi'(y, a) := \psi(y) + g(a), \text{ und } \pi : M' \oplus A \to M, \pi(y, a) = y + ax.$$

Für $(y, a) \in \ker(\pi)$ gilt $y = -ax \in M'$, also $a \in I$ und $g(a) = f(a) = \psi(ax) = -\psi(y)$, also $\psi'(y, a) = 0$ Daher definiert ψ' einen Homomorphismus

$$\psi' : (M' \oplus A)/ker(\pi) \cong Bild(\pi) = M' + Ax \to Q$$

der ψ fortsetzt. Da M' maximal ist, folgt $x \in M'$. □

Bemerkung 4.76. *Eine abelsche Gruppe $(G,+)$ heißt* **divisibel**, *falls es für jedes $a \in G$ und $n \in \mathbb{N}_{>0}$ ein $b \in G$ gibt, mit $a = nb$.*
Eine abelsche Gruppe ist genau dann divisibel, wenn sie als $\mathbb{Z}$-Modul injektiv ist.

Beispiel: $\mathbb{Q}$ ist ein injektiver $\mathbb{Z}$-Modul ebenso wie $\mathbb{Q}/\mathbb{Z}$.
Beweis. Wir wenden Satz 4.75 an. Sei $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$ Œ $n \neq 0$, und $\varphi : n\mathbb{Z} \to G$ ein Gruppenhomomorphismus, $g := \varphi(n) \in G$. Da G divisibel ist, gibt es ein $h \in G$ mit $nh = g$. Definiere $\psi : \mathbb{Z} \to G$ durch $\psi(1) := h$. □

Kapitel 5

Einfache und halbeinfache Algebren

Im folgenden sei K immer ein Körper und A eine endlich dimensionale K-Algebra, d.h.

(i). A ist Ring mit 1.

(ii). A ist ein endlich dimensionaler K-Vektorraum. und

(iii). $K \cdot 1 \subseteq Z(A)$ (=Zentrum von $A = \{x \in A \mid xa = ax \forall a \in A\}$)

Eine K-Algebra, die ein Schiefkörper ist, nennt man auch **K-Divisionsalgebra**. Ein **Algebrenhomomorphismus** ist ein linearer Ringhomomorphismus, der 1 auf 1 abbildet.

Beispiel

(i). $A = K^{n \times n}$

(ii). Jeder endliche Erweiterungskörper von K ist eine K-Divisionsalgebra.

(iii). A_1, A_2 K-Algebren $\Rightarrow A_1 \oplus A_2$ ($+, \cdot$ komponentenweise) ist wieder K-Algebra.

(iv). A sei K-Algebra. Dann ist $A^{n \times n}$ wieder eine K-Algebra.

Jeder Modul V einer K-Algebra A ist insbesondere ein K-Vektorraum. Ist $B = (B_1, \ldots, B_n)$ eine K-Basis von V, so operiert A als K-Endomorphismen auf V und wir erhalten eine **Darstellung** $\Delta_B : A \to K^{n \times n}$, also einen K-Algebrenhomomorphismus in eine Matrixalgebra. Mithilfe von Matrizen lässt sich vieles ganz explizit berechnen, z.B. ist $\mathrm{End}_A(V) = \{x \in \mathrm{End}_K(V) \cong K^{n \times n} \mid ax = xa \text{ für alle } a \in A\}$ zu berechnen als

$$C_{K^{n \times n}}(\Delta_B(A)) = \{X \in K^{n \times n} \mid \Delta_B(a)X = X\Delta_B(a) \text{ für alle } a \in A\}$$

wobei es genügt, a durch ein K-Algebrenerzeugendensystem von A laufen zu lassen. Der sogenannte **Zentralisator** $C_{K^{n \times n}}(\Delta_B(A))$ ist also die Lösungsmenge eines homogenen linearen Gleichungssystems.

5.1 Einfache Algebren

5.1.1 Der Doppelzentralisatorsatz

Definition 5.1. *Eine K-Algebra A heißt* **einfach**, *falls sie keine 2-seitigen nicht trivialen Ideale hat.*

Bemerkung:

1) D K-Divisionsalgebra $\Rightarrow$ D einfach.

2) D K-Divisionsalgebra, $n \in \mathbb{N} \Rightarrow D^{n\times n}$ einfach.

Beweis. $A = D^{n\times n}$ hat bis auf Isomorphie nur einen einfachen Modul: $V = D^{n\times 1}$, V ist treu. Sei nun $I \neq A$, dann hat A/I wieder einen einfachen Modul W. Als A-Modul bleibt W einfach, also $W \cong V$ und $I = 0$

Satz 5.2. *Eine einfache K-Algebra A ist halbeinfach, sogar $A \cong D^{n\times n}$ für eine K-Divisionsalgebra D, $n \in \mathbb{N}$.*

Beweis. Sei $M \leq_A A$ einfacher Teilmodul des regulären Moduls. Dann ist $Ma = 0$ oder einfach. Weiter ist $\sum_{a\in A} Ma \trianglelefteq A$ ein zweiseitiges Ideal. Da A einfach ist, ist $\sum_{a\in A} Ma = A$, d.h. ${}_AA$ ist vollständig zerlegbar.

Satz 5.3. *B sei halbeinfache Teilalgebra von $K^{n\times n}$. Definiere*

$$C = C_{K^{n\times n}}(B) := \{x \in K^{n\times n} | xb = bx \text{ für alle } b \in B\}$$

Dann gilt:

(i) C ist eine halbeinfache Teilalgebra von $K^{n\times n}$.

(ii) $B \cap C = Z(B)$, das Zentrum von B.

(iii) $C_{K^{n\times n}}(C) = B$ (Doppelzentralisatorsatz)

(iv) B einfach $\Leftrightarrow$ C einfach.

Beweis.

(i) Beachten Sie: C ist isomorph zu dem Endomorphismenring $\mathrm{End}_B(K^{n\times 1})$, da $K^{n\times n} = \mathrm{End}_K(K^{n\times 1})$ ist.
$K^{n\times 1}$ ist ein B-Modul. Nun ist B halbeinfach, also

$$B \cong \bigoplus_{i=1}^{r} D_i^{n_i\times n_i}$$

Zu jedem $D_i^{n_i\times n_i}$ gehört ein V_i, so dass

$$K^{n\times 1} \cong_B \bigoplus_{i=1}^{r} V_i^{\alpha_i}$$

mit $\alpha_i \geq 1$, da $K^{n\times 1}$ treuer B-Modul ist. Damit gilt

$$End_B(K^{n\times 1}) \cong \bigoplus_{i=1}^{r} (D_i^{op})^{\alpha_i \times \alpha_i} \cong C$$

also C halbeinfach, d.h.(i).

(ii) ist klar.

(iii) Zu den $D_i^{\alpha_i\times\alpha_i}$ gehören irreduzible Moduln W_i. $B \subseteq C_{K^{n\times n}}(C)$ ist die triviale Richtung. Andererseits: $K^{n\times 1}$ ist C-Modul. Als solcher ist $K^{n\times 1} \cong_C \bigoplus_{i=1}^{r} W_i^{n_i}$.

$$End_C(K^{n\times 1}) \cong \bigoplus_{i=1}^{r} D_i^{n_i\times n_i}$$

Aus Dimensionsvergleich folgt

$$B = C_{K^{n\times n}}(C)$$

(iv) B einfach $\Leftrightarrow$ $r = 1$ $\Leftrightarrow$ C einfach (aus (iii)).

Beispiel

(i)

$$B = \begin{pmatrix} K^{2\times 2} & 0 \\ 0 & K^{3\times 3} \end{pmatrix} \subseteq K^{5\times 5}$$

$$C = \left(\begin{array}{c|c} K\cdot I_2 & 0 \\ \hline 0 & K\cdot I_3 \end{array}\right)$$

(ii)

$$B = \left\{ \left(\begin{array}{cc|cc} a & b & & \\ c & d & \multicolumn{2}{c}{0} \\ \hline & & a & b \\ \multicolumn{2}{c|}{0} & c & d \end{array}\right) | a,b,c,d \in K \right\} \subseteq K^{4\times 4}$$

$$C = \left\{ \left(\begin{array}{c|c} xI_2 & yI_2 \\ \hline zI_2 & uI_2 \end{array}\right) | x,y,z,u \in K \right\}$$

5.1.2 Zentral einfache Algebren.

Bemerkung 5.4. *A_1, A_2 K-Algebren. Dann ist $A_1 \otimes_K A_2$ wieder K-Algebra mit $(a_1\otimes a_2)(a_1'\otimes a_2') = a_1a_1' \otimes a_2a_2'$.*

Beweis. Wohldefiniert: Betrachte $A_1 \times A_2 \times A_1 \times A_2 \to A_1 \otimes A_2 : (a_1, a_2, a_1', a_2') \mapsto a_1a_1' \otimes a_2a_2'$. Diese Abbildung ist multilinear, faktorisiert über $A_1 \otimes A_2$.

Beispiel

(i)

$$A_1 = K^{n\times n}, A_2 = K^{m\times m}$$
$$A_1 \otimes A_2 \cong K^{nm\times nm}$$
$$a \otimes b \mapsto a \otimes b$$

(ii)

$$D \otimes_K K^{n\times n} \cong D^{n\times n}$$

(iii) A/K endliche Galoiserweiterung vom Grad n.

$$A \otimes_K A \cong A \oplus \cdots \oplus A$$
$$a \otimes b \mapsto (a\sigma_1(b), \cdots, a\sigma_n(b))$$

wobei $Gal(A/K) = \{\sigma_1, \cdots, \sigma_n\}$.
z. B. $A = K[x]/(p(x))$

$$A \otimes A \cong A \otimes_K K[x]/(p(x)) \cong A[x]/(p(x)) \cong \bigoplus_i A[x]/(x - x_i)$$

falls $p(x) = \prod(x - x_i)$ in A.

Lemma 5.5. *A, B einfache K-Algebren, $Z(A) = K\cdot 1$ (d.h. A zentral einfach über K). Dann ist $A \otimes_K B$ eine einfache K-Algebra.*

Beweis. $0 \neq I < A \otimes_K B$. Sei $0 \neq u \in I$, dann ist $u = \sum_i a_i \otimes b_i$, o.B.d.A. b_i linear unabhängig über K. Die Länge von u sei die Anzahl der Summanden bez. dieser Darstellung. Wähle u von minimaler Länge. Seien $r, s \in A$, $(r \otimes 1)u(s \otimes 1) = \sum_i ra_is \otimes b_i \in I$, also existiert ein $u_1 \in I$ mit derselben Minimallänge:

$$u_1 = 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_m' \otimes b_m$$

Sei $a \in A$. $(a \otimes 1)u_1 - u_1(a \otimes 1)$ hat eine kürzere Länge als u_1, ist also $= 0$. Da die b_i linear unabhängig über K sind, sind die $1 \otimes b_i$ auch linear unabhängig über $A \otimes 1$.

$$\Rightarrow aa_i' - a_i'a = 0,\ i = 2, 3, \cdots, n$$

für alle $a \in A$.

$$\Rightarrow a_i' \in Z(A) = K \cdot 1$$
$$\Rightarrow a_i' = \alpha_i \cdot 1, \alpha_i \in K$$
$$\Rightarrow u_i = 1 \otimes (b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n) = 1 \otimes b \neq 0$$

Denn $(b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n) \neq 0$, da die b_i alle linear unabhängig sind.

$$\Rightarrow I \geq (1 \otimes B)u_1(1 \otimes B) = 1 \otimes BbB = 1 \otimes B$$
$$\Rightarrow A \otimes 1 \cdot 1 \otimes B = a \otimes B \leq I$$

d.h. $A \otimes B$ sind einfach.

Folgerung 5.6. *Ergänzung zum Doppelzentralisatorsatz Satz 5.3*
Sei $B \cong D^{\beta\times\beta} \subseteq K^{n\times n}$ einfach $C := C_{K^{n\times n}}(B) \cong (D^{op})^{\gamma\times\gamma}$, $Z := B \cap C = Z(B) = Z(D)$. Dann gilt

$$B \cdot C = \langle b \cdot c \mid b \in B, c \in C \rangle$$

ist eine einfache Teilalgebra von $K^{n\times n}$ mit $B \cdot C \cong Z^{k\times k}$ für ein $k \in \mathbb{N}$ ($k = \beta\gamma\ell^2$, wo $\ell^2 = \dim_Z(D)$).

Beweis. Seien B, C einfach zentral über Z. Nach Lemma 5.5 ist dann $B \otimes_Z C$ einfach.

$$B \otimes_Z C \to B \cdot C : b \otimes c \mapsto b \cdot c$$

ist ein K-Algebren-Epimorphismus, sogar ein Isomorphismus, da B und C einfache Z-Algebren sind. Also ist $B \cdot C$ eine einfache Z-Algebra.

$$dim_Z(B \otimes_Z C) = dim_Z B dim_Z C = \beta^2 dim_Z D \cdot \gamma^2 dim_Z D = (\beta\gamma\ell^2)^2 = k^2$$

Weiter liegt

$$B \cdot C \subseteq C_{K^{n\times n}}(Z) \cong Z^{m\times m}$$

Wie hängen β, γ, ℓ, m zusammen?

$K^{n\times 1}$	einfacher $K^{n\times n}$-Modul	
identisch		
$D^{\beta\times\gamma}$	als B- und C-Modul	Bilde jeweils die K-Dimension und sei dazu $d := \dim_K(Z)$:
identisch		
$Z^{1\times m}$	als Z-Modul	

$$\dim_K(K^{n\times 1}) = n = d\ell^2\beta\gamma = m \cdot d$$

Also $m = k$ und $\dim_Z BC = \dim_Z B \otimes_Z C = \dim_Z(B)\dim_Z(C) = (\ell^2\beta^2\ell^2\gamma^2) = k^2 = \dim_Z(Z^{m\times m})$ also $BC = C_{K^{n\times n}}(Z) = Z^{k\times k}$. □

5.1.3 Die Brauergruppe von K

Folgerung 5.7. *Sei D zentrale K-Divisionsalgebra (d.h. $Z(D) = K \cdot 1$). Dann gilt:*

$$D \otimes_K D^{op} \cong K^{n\times n}$$

Beweis. ${}_D D = V$, $D \subseteq End_K(V) \equiv K^{n\times n}$, $C := C_{K^{n\times n}}(D) \cong D^{op}$, $D \otimes_K D^{op} \cong D \cdot C = K^{n\times n}$ □

Folgerung 5.8. *Sei D zentrale K-Divisionsalgebra. Dann gilt :*
$dim_K D = n^2$ für ein $n \in \mathbb{N}$. n heißt **Index**.

Beweis. Sei $\overline{K}$ der algebraische Abschluß von K. Dann ist $\overline{K} \otimes_K D$ eine einfache $dim_K(D)$-dimensionale $\overline{K}$-Algebra, also isomorph zu $X^{n\times n}$ für ein n und eine endlich dimensionale $\overline{K}$-Divisionsalgebra X. Jede solche Divisionsalgebra ist aber isomorph zu $\overline{K}$ (jedes Minimalpolynom hat eine Nullstelle), also ist $\overline{K} \otimes_K D \cong \overline{K}^{n\times n}$ und $\dim_K(D) = n^2$. □

Es ist klar, dass für A zentral einfach $\dim_K A = n^2$ ist, denn $A = D^{k\times k}$ und $dim A = k^2(Index(D))^2$.

Satz 5.9. *Seien A, B zentral einfach K-Algebren. Dann gilt:*
$A \otimes_K B$ ist eine zentral einfache K-Algebra.

Beweis. $A \otimes_K B$ einfach ist folgt aus Lemma 5.5. Sei $z = \sum a_i \otimes b_i \in Z(A \otimes B)$, b_i alle linear unabhängig über K. Sei $a \in A$ so dass

$$0 = (a \otimes 1)z - z(a \otimes 1) = \sum_i (aa_i - a_i a) \otimes b_i$$

Weil die b_i linear unabhängig sind, ist $aa_i - a_i a = 0$ für alle i. Da a beliebig war ist $a_i \in Z(A) = K \cdot 1$, d.h. $a_i = \alpha_i \cdot 1$ für $\alpha_i \in K$, also $Z = 1 \otimes \sum \alpha_i b_i \in 1 \otimes Z(B) = 1 \otimes K1$, d.h. $Z = \alpha 1 \otimes 1$. □

Definition 5.10. *Seien A, B zentral einfache K-Algebren.*
$A \sim B$ (d.h. **Braueräquivalent***) $\Leftrightarrow$ Es existieren $n, m \in N$ mit $A^{n \times n} \cong B^{m \times m}$*
($\Leftrightarrow$ A, B sind Matrixringe über isomorphen Divisionsalgebren.)
$[A]$ ist die Äquivalenzklasse von A.
Die Menge der Äquivalenzklassen ist die **Brauergruppe** *$B(K)$. Auf $B(K)$ existiert eine Multiplikation $[A][B] := [A \otimes_K B]$*

Satz 5.11. *Die Multiplikation in $B(K)$ ist wohldefiniert. $B(K)$ ist eine kommutative Gruppe mit*

$$[A^{-1}] = [A^{op}] \ , \ [K] = 1$$

Jedes Element von $B(K)$ wird eindeutig durch eine zentrale Divisionsalgebra repräsentiert.

Beweis. Wohldefiniert nachrechnen. Assoziativ und kommutativ, weil $\otimes$ assoziativ und kommutativ. $[A^{-1}] = [A^{op}]$, weil $A \otimes_K A^{op} = K^{n \times n}$

Satz 5.12. *Sei D zentrale K-Divisionsalgebra vom Index n. Jeder Teilkörper von D liegt in einem maximalen Teilkörper von D. Sei $L \leq D$ ein maximaler Teilkörper. Dann gilt*

(i) $C_D(L) = L$

(ii) $D \otimes_K L \cong_{L-Algebra} L^{n \times n}$ *(L Zerfällungskörper)*

(iii) $dim_K L = n$

Einen Erweiterungskörper F von K mit $F \otimes_K D \cong F^{n \times n}$ nennt man einen **Zerfällungskörper** *von D.*

Beweis.

(i) Sei $K \leq L_1$ Teilkörper von D. Dann ist $C_D(L_1) \supsetneq L_1$. Nehme $x \in C_D(L_1) - L_1$, $L_2 = L_1[x]$ etc. bis Gleichheit (muss kommen, da die Dimension endlich).

(ii) $D \otimes_K D^{op} \cong K^{n^2 \times n^2}$. O.B.d.A. L maximaler Teilkörper in D^{op}. Dann gilt :
$D \otimes_K L =: B \subseteq K^{n^2 \times n^2}$ ist einfache Teilalgebra. $C_{K^{n^2 \times n^2}}(B) = K \otimes_K L = L$ (wie in Beweis von Satz **??**). Also ist $B \cong_{L-Algebra} L^{s \times s}$ für ein s. $dim_L B = dim_K D = n^2$, daraus folgt: $n = s$.

(iii) Gehe über zu $L \otimes D \cong L^{n\times n}$. Also ist $\dim_L D = n$ und $dim_K D = dim_K L \cdot dim_L D$, also ist $dim_K L = n$.

Beispiel

(i). Sei K algebraisch abgeschlossen. Dann gilt: $|B(K)| = 1$.

(ii). $B(\mathbb{R}) \cong C_2$
Beweis: D sei $\mathbb{R}$-Divisionsalgebra, L maximaler Teilkörper. Dann ist $L \cong \mathbb{R}$ oder $L \cong \mathbb{C}$.
$L \cong \mathbb{R} \Rightarrow D = \mathbb{R}$
$L \cong \mathbb{C} \Rightarrow \mathbb{C} \otimes_{\mathbb{R}} D \cong \mathbb{C}^{2\times 2}$
Sei $L = \mathbb{R}[i] = \mathbb{C}$. Wähle $x \in D : x^{-1}ix = -i$, d.h. $xi = -ix$. Dann ist $x^2 \in C_D(L) \cap \mathbb{R}[x] = \mathbb{R}$ und $\mathbb{R}[x] \cong \mathbb{C}$. Da D eine Divisionsalgebra ist, ist $x^2 = -\alpha < 0$. Wähle x so, dass $x^2 = -1$. $D = L \oplus Lx$, also L-Vektorraum. $D = \mathbb{R}[i] \oplus \mathbb{R}[i]x$. $1, i \in \mathbb{R}[i]$ und $x, ix \in \mathbb{R}[i]x$ bilden die Basis der Quaternionen $\mathbb{H}$.

Satz 5.13. *(Skolem-Noether) A sei eine zentral einfache K-Algebra, B_1, B_2 einfache Teilalgebren von A (d. h. $1_A = 1_{B_1} = 1_{B_2}$), $\varphi : B_1 \to B_2$ ein Algebrenhomomorphismus. Dann gibt es ein $a \in A^*$, so dass $\varphi(b_1) = a^{-1}b_1a$* für alle $b_1 \in B_1$ *,d. h. φ setzt sich fort zu einem inneren Automorphismus von A.*

Beweis. Sei V ein einfacher A-Modul und $D^{op} = End_A(V)$. O.B.d.A. sei $V = D^{k\times 1}$, $\dim_K(D) = d$, $n = dk$, so dass $B_1 \subseteq A \hookrightarrow K^{n\times n}$. Definieren $C := C_{K^{n\times n}}(A) \cong D^{op}$. Dann ist V einfach als AC-Modul und $AC \cong K^{n\times n}$. Fasse V auf zwei Arten als B_1C-Modul auf:

(i). $(b_1c)v := b_1cv$ für alle $v \in V, b_1 \in B_1, c \in C$

(ii). $(b_1c)v := \varphi(b_1)cv$ für alle $v \in V, b_1 \in B_1, c \in C$

Da B_1C einfache Algebra ist, gibt es bis auf Isomorphie höchstens einen Modul gegebener Dimension, folglich gibt es ein $a \in K^{n\times n}$, so dass $a^{-1}b_1ca = \varphi(b_1)c$ für alle $b_1 \in B_1, c \in C$. Wählt man $b_1 = 1$, so folgt $a \in C_{K^{n\times n}}(C) = A$ und mit $c = 1$ erhält man $a^{-1}b_1a = \varphi(b_1)$ für alle $b_1 \in B_1$.

Satz 5.14. *(Wedderburn) $\mathcal{B}(\mathbb{F}_q) = C_1$, d.h. jede endlich dimensionale Divisionsalgebra über einem endlichen Körper ist ein Körper, d.h. alle zentral einfachen Algebren über $\mathbb{F}_q$ sind isomorph zu $\mathbb{F}_q^{n\times n}$ für ein $n \in \mathbb{N}$.*

Beweis. D sei zentrale Divisionsalgebra über $\mathbb{F}_q$ von Index n. Jedes Element von D liegt in einem maximalen Teilkörper (der Ordnung q^n). Je zwei dieser Teilkörper sind isomorph, also (Skolem-Noether) konjugiert in D. Also ist die multiplikative Gruppe D^* Vereinigung einer Konjugiertenklasse von Untergruppen. Allgemein gilt für eine Gruppe G: $G = \bigcup_{g\in G} H^g, H \leq G, [G : H] < \infty \Rightarrow G = H$. Denn es gibt $[G : N_G(H)]$ Konjugiertenklassen von H und $|\bigcup_{g\in G} H^g| \leq 1 + (|H| - 1)\frac{|G|}{|H|} = 1 + |G| - \frac{|G|}{|H|} < |G|$ für $H \neq G$. Also folgt $n = 1$. □

Satz 5.15. *Sei D eine zentrale K-Divisionsalgebra. Dann gibt es einen maximalen Teilkörper L von D, so dass L/K separabel ist. Insbesondere hat jede halbeinfache K-Algebra A mit $Z(A)/K$ separabel einen separablen Zerfällungskörper.*

Beweis. Der Satz ist klar, falls $char(K) = 0$, da dann jede endliche Körpererweiterung separabel ist. Sei also $char(K) = p > 0$. Wir argumentieren mit Induktion über $dim_K(D) = n^2$. Ist $n = 1$, dann sind wir fertig. Sei also $n > 1$. Es genügt dann einen echten separablen Teilkörper $K \neq E \leq D$ zu finden. Denn dann ist $D' := C_D(E)$ eine zentrale E-Divisionsalgebra von Index m mit $m[E : K] = n$ und enthält nach Induktion einen maximalen Teilkörper L mit L/E separabel. Dann ist L aber auch maximaler Teilkörper von D und L/K ist separabel.
Angenommen es gibt keinen solchen echten separablen Teilkörper $K \neq E \leq D$. Dann ist jedes $x \in D \setminus K$ rein inseparabel, also $\mu_x(X) = X^{p^f} - a$ für ein $f \in \mathbb{N}$ und ein $a \in K$. Insbesondere ist dann p ein Teiler von n.
Sei jetzt F ein beliebiger maximaler Teilkörper von D und betrachte $F \otimes_K D = F^{n\times n}$. Dann ist $1 \otimes x \in F^{n\times n}$ ein Element mit $(1 \otimes x)^{p^f} = aI_n$. Also ist $Sp(1 \otimes x) = 0$ für jedes $x \in D$. Da die Elemente $1 \otimes x$ mit $x \in D$ aber $F^{n\times n}$ als F-Algebra erzeugen folgt daraus, dass $Sp(M) = 0$ für jede Matrix $M \in F^{n\times n}$, ein Widerspruch. □

5.2 Separable Algebren.

5.2.1 Reduzierte Norm und Spur.

Definition 5.16. *Sei A eine zentral einfache K-Algebra, L ein Zerfällungskörper von A. $p_a(x)$ das charakteristische Polynom von $1 \otimes a \in L \otimes_K A \cong L^{n\times n}$ über L heißt das* **reduzierte charakteristische Polynom von** *a.*

$$p_a(x) = x^n - \alpha_1 x^{n-1} + \ldots + (-1)^n \alpha_n$$

Dann heißt $\alpha_1 =: Sp_{(r)}(a)$ die **reduzierte Spur** *von a und $\alpha_n =: N_{(r)}(a)$ die* **reduzierte Norm** *von a.*

Satz 5.17. *Unter den Voraussetzungen der Definition sei zusätzlich angenommen, dass $L : K$ separabel ist.*

(i) $p_a(x) \in K[x]$ *und ist unabhängig von der Wahl von L.*

(ii) $Sp : A \to K$ *ist linear.*

(iii) $Sp : A \times A \to K : (a, b) \mapsto Sp(ab)$ *ist nichtausgeartete symmetrische Bilinearform.*

(iv) $N : A \to K$ *ist multiplikativ.*

Beweis.

(i) Δ sei die reguläre Darstellung von A. $\tilde{p}_a(x)$ sei das charakteristische Polynom von $\Delta(a)$. Dann ist $\tilde{p}_a(x) \in K[x]$ und $\tilde{p}_a(x) = \tilde{p}_{1\otimes a}(x) \in L[x]$. $\tilde{p}_{1\otimes a}(x) = (p_a(x))^n$, da die reguläre Darstellung von $L^{n\times n}$ (wie operiert $L^{n\times n}$ auf sich selbst) $= n\cdot$ natürliche Darstellung auf $L^{n\times 1}$ ist. Da L separabel über K ist $p_a(x) \in K[x]$ und unabhängig von L.

(ii) Klar!

(iii) Klar für $L^{n\times n}$, die Basis (e_{ij}) hat (e_{ji}) als duale Basis, also haben wir eine nichtausgeartete Bilinearform auf $L^{n\times n}$. Diese bleibt nichtausgeartet über A, da A eine L-Basis von $L^{n\times n}$ enthält.

(iv) Klar, da die Determinante multiplikativ ist.

Beispiel Betrachten die Quaternionendivisionsalgebra $\mathcal{Q} := \mathbb{R}[i,j,k]$ mit $i^2 = j^2 = (ij)^2 = -1$. Wir haben einen $\mathbb{R}$-Algebrenhomomorphismus: $\mathcal{Q} \to \mathbb{C}^{2\times 2}$:

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \; j \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \; k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

also ist $\mathbb{C}$ Zerfällungkörper von $\mathcal{Q}$ und $\mathbb{C} \otimes_{\mathbb{R}} \mathcal{Q} \cong \mathbb{C}^{2\times 2}$. Das reduzierte charakteristische Polynom von $q = a + bi + cj + dk$ ist das charakteristische Polynom von

$$\begin{pmatrix} a+ci & -b+di \\ b+di & a-ci \end{pmatrix}, \; x^2 - (2a)x + (a^2+b^2+c^2+d^2).$$

$2a$ ist die reduzierte Spur von q, $a^2+b^2+c^2+d^2$ ist die reduzierte Norm von q.

Definition 5.18. *Eine K-Algebra A heißt* **separabel** *über K, falls ein über K separabler Erweiterungskörper L von K existiert mit $L \otimes_K A \cong_{L-Algebra} \bigoplus_{i=1}^{k} L^{n_i\times n_i}$. In diesem Fall heißt $Sp : A \to L : a \mapsto \sum_{i=1}^{k} Sp(a_i)$ (wo a durch den Isomorphismus auf $\sum a_i$ mit $a_i \in L^{n_i\times n_i}$ abgebildet wird) die* **reduzierte Spur** *und $N : a \to L : a \mapsto \prod_{i=1}^{k} det(a_i)$ die* **reduzierte Norm**.

Übung: Reduzierte Norm und reduzierte Spur nehmen Werte in K an, den Grund dafür sehen Sie im folgenden Beispiel.

Beispiel A sei separabler Erweiterungskörper von K, L die normale Hülle von A (die kleinste Galoiserweiterung von K, in der L liegt). $L\otimes_K A \cong \oplus^{dim_K(A)} L : 1\otimes a \mapsto (\varphi_1(a), \ldots, \varphi_n(a))$, wo $\varphi_1, \ldots, \varphi_n$ Einbettungen von A in L sind. In diesem Fall ist die reguläre Spur gleich der reduzierten Spur und die reguläre Norm gleich der reduzierten Norm.

z. B. $K = \mathbb{Q}$, $A = \mathbb{Q}[\sqrt{2}]$, $L = \mathbb{Q}[\sqrt{2}]$ Dann ist $L \otimes_K A \cong L \oplus L$ vermöge $1 \otimes \sqrt{2} \mapsto (\sqrt{2}, -\sqrt{2})$.

Folgerung 5.19. *Ist A halbeinfach, $Z(A)$ separabel über K, so ist A separabel über K.*

Folgerung 5.20. *A separabel über $K \Rightarrow A$ ist halbeinfach.*

Beweis. $J(A)$ ist nilpotentes Ideal von A. Sei L separabler Zerfällungskörper für A. Falls $J(A) \neq 0$, so auch $0 \neq L \otimes_K J(A) \trianglelefteq L \otimes_K A$ und dieses Ideal ist nilpotent. Also ist $L \otimes_K A$ nicht halbeinfach. Widerspruch!

5.2.2 Assoziative Bilinearformen und das Casimirelement.

Bemerkung 5.21. *Sei c_{ij} die Standardbasis von $K^{n\times n}$ Dann folgt :*
Die bzgl. der Spur duale Basis ist $(e_{ij})_{1\leq i,j\leq n}$ mit $\sum_{i,j} e_{ij}e_{ji} = nI_n$.

Definition 5.22. *(i) Eine assoziative Bilinearform auf einer K-Algebra A ist eine bilineare Abbildung*

$$\Phi : A \times A \to K$$

die symmetrisch ist mit

$$\Phi(ab, c) = \Phi(a, bc)$$

für alle $a, b, c \in A$.

(ii) A separabel, Φ nicht ausgeartete assoziative Bilinearform. Das **Casimir-Element** *von A bez.Φ ist definiert als*

$$c_\Phi := \sum b_i b_i^*$$

wobei $(b_1, \cdots, b_n)$ eine Basis von A, $(b_1^*, \cdots, b_n^*)$ die bez. Φ duale Basis ist.

Bemerkung 5.23. *c_Φ ist unabhängig von der Basis. $c_\Phi \in Z(A)$, insbesondere induziert c_Φ einen Endomorphismus für jeden A-Modul.*

Beweis. $b_i' = \sum \alpha_{ij} b_j$ und $b_i'^* = \sum \beta_{ji} b_j^*$. Daraus folgt: $\sum \alpha_{ij}\beta_{jk} = \delta_{ik}$, also $\sum b_i' b_i'^* = \sum b_i b_i^*$, d.h. c_Φ ist unabhängig von der Basis.
Sei $u \in A^*$:

$$uc_\Phi u^{-1} = u(\sum b_i b_i^*)u^{-1} = \sum (ub_i)(b_i^* u^{-1})$$

$$\Phi(ub_i, b_j^* u^{-1}) = \Phi(b_j^* u^{-1}, ub_i) = \Phi(b_j^*, b_i) = \delta_{ij}$$

d.h. $(ub_1, \cdots, ub_n)$ und $(b_1^* u^{-1}, \cdots, b_n^* u^{-1})$ sind auch duale Basen. Sei o.B.d.A. $A = \bigoplus K^{n_i \times n_i}$. Daraus folgt $Z(A) = \{x \in A | uxu^{-1} = x, u \in A^*\}$, also $c_\Phi \in Z(A)$.

Beispiel Sei Sp die reduzierte Spur, $x \in Z(A)$. Dann folgt: $\Phi_x : A \times A \to K : (a, b) \mapsto Sp(\overline{axb})$ ist eine assoziative Bilinearform.

Übung: Sei Φ assoziative Bilinearform auf A. Dann gilt:
$Rad\Phi \trianglelefteq A$, allgemeiner $I \trianglelefteq A \Rightarrow I^\perp \trianglelefteq A$. $(Rad\Phi = A^\perp)$

5.2.3 Ordnungen in separablen Algebren.

Sei R ein Noetherscher Integritätsbereich mit Quotientenkörper K und A eine endlich dimensionale K-Algebra. Wir nehmen weiter an, dass R **ganz abgeschlossen** in K ist, also

$$R = \mathrm{Int}_R(K) = \{a \in K \mid a \text{ ist ganz über } R\} = \{a \in K \mid R[a] \text{ ist endlich erzeugter } R\text{−Modul}\}.$$

Z.B. K ein algebraischer Zahlkörper, $R = \mathbb{Z}_K$ der Ring der ganzen Zahlen in K.

Definition 5.24. *Eine R-***Ordnung** Λ *in A ist ein Teilring von A, der endlich erzeugt als R-Modul ist, und A als K-Vektorraum erzeugt.*
*Eine R-Ordnung Λ heißt R-***Maximalordnung***, falls für jede Ordnung Γ in A mit $\Lambda \leq \Gamma$ folgt, dass $\Lambda = \Gamma$ ist.*

Bemerkung 5.25. *Jede K-Algebra enthält R-Ordnungen, denn sei z.B. $B := (b_1, \ldots, b_n)$ eine K-Basis von A und $L := \langle b_1, \ldots, b_n \rangle_R$ das von ihr erzeugte R-Gitter. Dann ist die* **Linkssordnung**

$$O_l(L) := \{a \in A \mid aL \subseteq L\}$$

von L eine R-Ordnung in A. Ebenso die **Rechtsordnung** $O_r(L) := \{a \in A \mid La \subseteq L\}$.

Beweis. Klar ist $\Lambda := O_l(L)$ ein Teilring von A.
Wir zeigen, dass Λ eine K-Basis von A enthält. Dazu sei $(a_1, \ldots, a_n)$ eine beliebige K-Basis von A. Die $n \times n$-Matrix $X_i := {}^B(\rho(a_i))^B \in K^{n\times n}$ der linksregulären Darstellung von a_i bezüglich B hat einen Hauptnenner $h_i \in K^*$, so dass $h_i X_i \in R^{n\times n}$ liegt. Dann ist aber $h_i a_i \in O_l(L)$.
Wir wollen jetzt noch zeigen, dass Λ endlich erzeugter R-Modul ist. Da L eine K-Basis von A enthält, gibt es ein $s \in R$, so dass $s1_A \in L$. Also gilt $O_l(L)(s1_A) \subseteq L$, d.h. $\Lambda = O_l(L) \subseteq s^{-1}L$ ist ein Teilmodul eines e.e. R-Moduls. Da R Noethersch ist, ist auch Λ endlich erzeugt. □

Definition 5.26. *Ein Element $a \in A$ heißt* **ganz über** *R, wenn $R[a]$ ein endlich erzeugter R-Modul ist.*

Bemerkung 5.27. *Sei Λ eine R-Ordnung in A. Dann ist jedes $\lambda \in \Lambda$ ganz über R, denn $R[\lambda] \subseteq \Lambda$ ist als Teilmodul eines e.e. Moduls über einem Noetherschen Bereich wieder ein endlich erzeugter R-Modul.*

Satz 5.28. *(Lemma von Gauß) Sei R ganz abgeschlossen in seinem Quotientenkörper K und $f(X) \in R[X]$ ein normiertes Polynom. Gilt $f(X) = g(X)h(X)$ in $K[X]$ mit g, h normiert, so liegen g und h in $R[X]$.*

Beweis. Sei L ein Zerfällungskörper von f, also $f(X) = \prod(X - \alpha_i) \in L[X]$ und sein $S = \mathrm{Int}_R(L)$ der ganze Abschluss von R in L. Dann liegen alle Nullstellen von f in S, also auch die von g und h und somit auch die Koeffizienten. Also liegt $g(X) \in S[X]$ und $h(X) \in S[X]$. Dann aber $g, h \in (S \cap K)[X] = R[X]$. □

Satz 5.29. *Sei $\lambda \in A$. λ ist ganz über R genau dann wenn das Minimalpolynom von λ in $R[X]$ liegt.*

Beweis. Sei $R[\lambda] = \langle b_1, \ldots, b_n\rangle_R$ und $\lambda b_i = \sum_{j=1}^n a_{ij} b_j$ mit $M := (a_{ij}) \in R^{n\times n}$. Da $1 \in R[\lambda]$ ist, ist das Minimalpolynom von M gleich dem Minimalpolynom p von λ. Also teilt p das charakteristische Polynom f von M. f ist ein normiertes Polynom in $R[X]$, somit auch $p \in R[X]$.
Die Umkehrung ist trivial. □

Satz 5.30. *Sei A separabel. Dann hat A eine R-Maximalordnung. Allgemeiner gilt: Für jede R-Ordnung Λ in A gibt es eine R-Maximalordnung Γ in A, welche Λ enthält.*

Beweis. Sei Λ eine R-Ordnung in A. Dann sind alle Elemente aus Λ ganz über R, insbesondere liegen die reduzierten Spuren $Sp(\lambda)$ in R für alle $\lambda \in \Lambda$. Sei

$$\Lambda^{\#} := \{a \in A \mid Sp(ax) \in R \text{ für alle } x \in \Lambda\}.$$

Dann gilt $\Lambda \subseteq \Lambda^{\#}$.
Sei Δ irgendeine R-Ordnung, die Λ enthält. Dann sind auch die Elemente von Δ alle ganz über R und

$$\Lambda \subseteq \Delta \subseteq \Delta^{\#} \subseteq \Lambda^{\#}.$$

Also korrespondiert jede Oberordnung Δ zu einem R-Teilmodul Δ/Λ von $\Lambda^{\#}/\Lambda$. Dies ist ein endlich erzeugter R-Modul, besitzt also keine unendlich aufsteigenden Ketten, da R Noethersch ist. Also existiert eine R-Maximalordnung die Λ enthält. □

Beispiel. $A = \langle 1, i, j, k\rangle_{\mathbb{Q}}$ mit $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$. $\Lambda = \langle 1, i, j, k\rangle_{\mathbb{Z}}$, $\Lambda^{\#} = \frac{1}{2}\Lambda$, $\Gamma = \langle 1, i, j, \frac{1}{2}(1+i+j+k)\rangle$ ist (einzige) Maximalordnung von A, welche Λ enthält. Für diese Algebra A kann man zeigen, dass alle Maximalordnungen von A in A konjugiert sind, es gibt jedoch $\mathbb{Q}$-Divisionsalgebren vom Index 2, für die dies nicht der Fall ist. Ein Beispiel:
$A = \langle 1, \rho, i, \rho i\rangle_{\mathbb{Q}} \cong \mathbb{Q}[\rho] \oplus \mathbb{Q}[\rho]i$, wo $\rho^2 + \rho + 3 = 0$, $i^2 = -1$, $(i\rho)^2 = -3$. Diese Algebra enthält zwei Konjugiertenklassen von Maximalordnungen
$\Gamma_1 := \langle 1, \rho, i, \rho i\rangle_{\mathbb{Z}}$ ($\Gamma_1^* \cong C_4$) und
$\Gamma_2 := \langle 1, \rho + i, 2i, \frac{1+\rho i}{2}\rangle_{\mathbb{Z}}$ (mit Einheitengruppe C_6).
(Übungsaufgabe entsprechendes mit anderen Quaternionenalgebren.)

Ein Beispiel für eine nicht separable Algebra: Sei $A = \Delta_2(\mathbb{Q})$, die oberen Dreiecksmatrizen in $\mathbb{Q}^{2\times 2}$. Dann ist $J(A) = \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$. Die $\mathbb{Z}$-Ordnungen

$$\Lambda_n := \begin{pmatrix} \mathbb{Z} & \frac{1}{2^n}\mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix}$$

bilden eine echte unendlich aufsteigende Kette von Ordnungen in A, es gibt also keine Maximalordnung.

Beispiel. Sei $A = K^{n\times n}$. Dann ist $R^{n\times n}$ eine R-Maximalordnung in A.

Bemerkung 5.31. *Jede R-Maximalordnung in A enthält die eindeutig bestimmte R-Maximalordnung S der Zentrums von A, $S = \mathrm{Int}_R(Z(A)) = \{z \in Z(A) \mid \mu_z \in R[X]\}$. Insbesondere liegen die zentral primitiven Idempotente von A in jeder Maximalordnung von A.*

5.3 Gruppenalgebren.

In diesem Abschnitt sei G immer eine endliche Gruppe.

Definition 5.32. *Sei G eine endliche Gruppe und K ein kommutativer Ring. Dann wird der freie K-Modul auf der Menge G,*

$$KG := \{\sum_{g\in G} a_g g \mid a_g \in K\}$$

zu einer K-Algebra durch $\sum_{g\in G} a_g g \sum_{h\in G} b_h h := \sum_{g,h} a_g b_h gh$. Diese K-Algebra heißt der **Gruppenring** *von G über K.*

Die Darstellungstheorie endlicher Gruppen studiert Gruppenhomomorphismen $\Delta : G \to \mathrm{GL}\, n(K)$ der Gruppe G in volle lineare Gruppen über einem Körper K. In Analogie zum Hauptsatz über transitive G-Mengen, welcher eine Klassifikation aller Homomorphismen von G in symmetrische Gruppen liefert, wollen wir in der Darstellungstheorie alle K-Matrixdarstellungen,

also Homomorphismen von G in volle lineare Gruppen über K, klassifizieren. Bei den G-Mengen benötigten wir dazu die Untergruppenstruktur von G, bei den Darstellungen die Algebrenstruktur von KG.

Bemerkung 5.33. *Sei $\Delta : G \to \mathrm{GL}_n(K)$ ein Gruppenhomomorphismus. Dann wird K^n zu einem KG-Modul V_Δ durch*

$$(\sum_{g\in G} a_g g)v = \sum_{g\in G} a_g \Delta(g)v \text{ für alle } v \in K^n.$$

Ist $\Gamma : G \to \mathrm{GL}_m(K)$ eine weitere K-Matrixdarstellung von G, so ist

$$V_\Delta \cong V_\Gamma \Leftrightarrow m = n \text{ und es gibt } A \in \mathrm{GL}_n(K) \text{ mit } A\Delta(g)A^{-1} = \Gamma(g) \text{ für alle } g \in G.$$

Dann nennt man die Darstellungen Δ und Γ **äquivalent**. *Die Darstellung Δ heißt* **irreduzibel**, *falls V_Δ einfach ist und* **unzerlegbar**, *wenn V_Δ unzerlegbar ist. Umgekehrt liefert jeder e.e. KG-Modul V durch Einschränkung auf G einen Gruppenhomomorphismus $\Delta_V : G \to \mathrm{GL}(V)$ (also nach Basiswahl eine K-Matrixdarstellung von G).*

In der Darstellungstheorie unterscheidet man zwei wesentlich verschiedene Fälle, je nachdem ob die Charakteristik des Körpers die Gruppenordnung teilt oder nicht.

Satz 5.34. *(Maschke) Sei G eine endliche Gruppe und K ein Körper. Dann ist die Gruppenalgebra KG eine halbeinfache K-Algebra genau dann wenn $|G| \in K^*$.*

Beweis. $\Leftarrow$: Wir zeigen, dass KG ein halbeinfacher KG-Linksmodul ist. Dazu genügt es zu zeigen, dass jeder KG-Teilmodul von KG ein G-invariantes Komplement hat. Sei also $U \leq_{KG} KG$ und wähle einen Teilraum $U' \leq KG$ so dass $KG = U \oplus U'$ als K-Vektorraum. Seien $\pi, \pi' = 1 - \pi \in \mathrm{End}_K(KG)$ die zu dieser Zerlegung gehörigen Projektionen, also $\pi(KG) = U$. Setze

$$\rho := \frac{1}{|G|} \sum_{g\in G} g^{-1}\pi g$$

also $\rho(a) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(ga)$ für alle $a \in KG$. Dann ist ρ wohldefiniert, da $|G|$ in K invertierbar ist.
Behauptung: $\rho \in \mathrm{End}_{KG}(KG)$.
Denn für $h \in G$, $a \in KG$ ist

$$\rho(ha) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gha) = h\frac{1}{|G|}\sum_{g\in G}(gh)^{-1}\pi(gha) = h\rho(a).$$

Weiter ist $\mathrm{Bild}(\rho)$ enthalten in U, da U ein KG-Teilmodul ist. Für $a \in U$ ist

$$\rho(a) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(ga) = \frac{1}{|G|}\sum_{g\in G} g^{-1}ga = a$$

also ist ρ eine G-invariante Projektion auf U. Der Kern von ρ ist ein G-invariantes Komplement von U in KG. Also ist KG halbeinfach.
$\Rightarrow$: Sei $I := \{\sum a_g g \in KG \mid \sum a_g = 0\}$ (das sogenannte Augmentationsideal in KG). Dann

ist I ein Ideal in KG. Da KG halbeinfach ist hat I also ein G-invariantes Komplement $KG = I \oplus U$ mit $U \leq_{KG} KG$. Dann ist $U \cong KG/I \cong K$ der triviale KG-Modul, d.h. es ist $U = \langle u \rangle_K$ für jedes $0 \neq u \in U$ und es gilt $gu = u$ für alle $g \in G$. Schreibt man $u = \sum_{g\in G} u_g g$ so gilt für $h \in G$, dass

$$hu = \sum_{g\in G} u_g(hg) = \sum_{g\in G} u_{h^{-1}g} g = u$$

und somit $u_g = u_h$ für alle $g, h \in G$. Also ist $u = a\sum_{g\in G} g$ für ein $a \in K$, insbesondere $\sum_{g\in G} g \in U$ und somit $\sum_{g\in G} g \notin I$ d.h. $|G| \neq 0$ in K. □

Im folgenden setzen wir immer voraus, dass die Charakteristik von K gleich 0 ist. Dann ist KG eine halbeinfache K-Algebra, also nach dem Satz von Wedderburn

$$KG = \bigoplus_{i=1}^{h'} D_i^{n_i' \times n_i'}$$

für geeignetes $h' \in \mathbb{N}$, $n_i' \in \mathbb{N}$ und Schiefkörper $D_i = \mathrm{End}_{KG}(M_i)$. Die Gruppenalgebra hat genau h' Isomorphieklassen von einfachen Moduln $M_1, \ldots, M_{h'}$ und jeder endlich erzeugte KG-Modul ist direkte Summe einfacher Moduln. Die D_i sind endlich dimensionale Divisionsalgebren über K. Es gibt also eine endliche Erweiterung L von K, so dass

$$LG = \bigoplus_{i=1}^{h} L^{n_i \times n_i}.$$

Jedes solche L nennen wir **Zerfällungskörper** von G über K. Die Anzahl h der Isomorphieklassen einfacher LG-Moduln ist dann genau die Dimension von $Z(LG)$ über L.
Klar ist

$$\sum_{g\in G} a_g g \in Z(LG) \Leftrightarrow h\sum_{g\in G} a_g g h^{-1} = \sum_{g\in G} a_g g \text{ für alle } h \in G \Leftrightarrow a_g = a_{hgh^{-1}} \text{ für alle } h, g \in G.$$

Bezeichnung 5.35. *Im folgenden werden wir annehmen, dass K ein Zerfällungskörper von G ist, der Charakteristik 0 hat.*
$M_1, \ldots, M_h$ bezeichnen die einfachen KG-Moduln.
Dann ist $M_i \cong K^{n_i \times 1}$ nach Basiswahl und $\Delta_i : G \to \mathrm{GL}_{n_i}(K)$ eine zugehörige Matrixdarstellung (bis auf Konjugation in $\mathrm{GL}_{n_i}(K)$ eindeutig).
Sei $\chi_i : G \to K, g \mapsto \mathrm{Spur}(\Delta_i(g))$ der Charakter der Darstellung Δ_i.
Dann ist χ_i schon durch den KG-Modul M_i eindeutig festgelegt und es gilt

$$\chi_i(ghg^{-1}) = \chi_i(h) \text{ für alle } g, h \in G.$$

χ_i ist also konstant auf den Konjugiertenklassen von G.

Definition 5.36. *Seien G, g_i, χ_j wie in Bezeichnung 5.35; $K = \mathbb{C}$. Die Matrix*

$$(\chi_i(g_j))_{1\leq i,j\leq h}$$

heißt die **Charaktertafel** *von G.*

Beispiel Sei $G = C_2 = \langle a \rangle$. Dann ist G abelsch, also sind alle irreduziblen Darstellungen von G eindimensional und deshalb gleich den irreduziblen Charakteren. Die Charaktertafel von G ist

C_2	1	a
χ_1	1	1
χ_2	1	-1

Bemerkung 5.37. *Sei ρ der Charakter der regulären Darstellung von G. Dann ist*

$$\rho(g) = \begin{cases} |G| & g = 1 \\ 0 & sonst \end{cases}$$

$\rho = \sum_{i=1}^{h} \chi_i(1)\chi_i$.

Beweis. $\rho(1) = |G| = dim_K(KG)$. Sei $g \neq 1, G = \{g_1, \dots g_n\}$ eine Basis von KG. Dann ist $gg_i \neq g_i$, also $Spur(D_\rho(g)) = 0 = \rho(g)$ als Spur einer Permutationsmatrix (=Anzahl der Fixpunkte). □

Beispiel Die Charaktertafel der S_3:

S_3	(.)	(..)	(...)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1
ρ	6	0	0

Satz 5.38. *Sei G eine endliche Gruppe K Zerfällungskörper von G der Charakteristik 0.*

(0) $\dim_K(KG) = \sum_{i=1}^{h} \chi_i(1)^2 = |G|$.

(i) *$Z(KG)$ hat die zentral primitiven Idempotente e_i als Basis, $e_i^2 = e_i,\ e_i e_j = 0,$ falls $i \neq j$.*

$$Z(KG) = \bigoplus_{i=1}^{h} Z(KG)e_i = \bigoplus_{i=1}^{h} Ke_i \tag{5.3.1}$$

(ii) *$Z(KG)$ hat die Klassensummen $\overline{c}$ als Basis. (Ist C eine Konjugiertenklasse von G, so sei $\overline{c} := \sum_{g \in C} g$.)*

(iii) *$dim_K(Z(KG)) = h =$ Anzahl der Konjugiertenklassen von G. Also ist die Anzahl der Äquivalenzklassen irreduzibler Darstellungen von G genau die Anzahl der Konjugiertenklassen von Elementen von G.*

(iv) *Seien $g_1, \dots g_h$ Vertreter der Konjugiertenklassen $C_1, \dots, C_h$, $\overline{c}_i = \sum_{l=1}^{h} \omega_l(\overline{c}_i)e_l$. Dann gilt*

(i). *$\omega_l : Z(KG) \to K$ sind Algebrenhomomorphismen. Sie heißen* **zentrale Charaktere**.

(ii). Ist χ_l der Charakter der irreduziblen Darstellung mit $\chi_l(e_l KG) \neq 0$, so gilt

$$|C_i|\chi_l(g_i) = \omega_l(\overline{c}_i)\chi_l(1).$$

Insbesondere ist χ_l konstant auf den Konjugiertenklassen.

(iii). Ist $\overline{c}_i\overline{c}_j = \sum_{k=1}^{h} \alpha_{ijk}\overline{c}_k$, so ist $\alpha_{ijk} = 1 \cdot |\{(a,b) \in C_i \times C_j \mid ab = g_k\}|$

Beweis.

(0) und (i) Klar! Beachte: $KG \cong \bigoplus_{i=1}^{h} K^{n_i \times n_i}$ und $Z(KG) \cong \bigoplus KI_{n_i}$.

(ii) Sei $\sum \alpha_g g \in Z(KG)$, $h \in G$. Dann ist $h^{-1}(\sum \alpha_g g)h = \sum \alpha_g g$ und $h^{-1}(\sum \alpha_g g)h = \sum \alpha_g h^{-1}gh = \sum \alpha_{hxh^{-1}} x$. Also α konstant auf den Konjugiertenklassen, also $\sum \alpha_g g = \sum \alpha_{\overline{c}_i}\overline{c}_i$. Klar ist: $\overline{c}_i \in Z(KG)$.

(iii) folgt aus (i) und (ii).

(iv) (i). Die ω_i sind Homomorphismen, da $e_i e_j = \delta_{ij} e_i$, also $(\sum \alpha_i e_i)(\sum \beta_i e_i) = \sum \alpha_i \beta_i e_i$.

(ii). Seien $g, h \in C_i$. Dann existiert also ein $x \in G$ mit $x^{-1}gx = h$. Δ_i sei die zu χ_i gehörige Darstellung. Dann ist

$$\Delta_i(h) = \Delta_i(x)^{-1}\Delta_i(g)\Delta_i(x).$$

Also gilt $\chi_i(g) = \chi_i(h)$. $\sum_{g \in C_j} \Delta_i(g) = \Delta_i(\overline{c}_j) = \omega_i(\overline{c}_j) I_{n_i}$ Spur nehmen auf beiden Seiten liefert die Behauptung.

(iii). $\overline{c}_i\overline{c}_j = (\sum_{g \in C_i} g)(\sum_{h \in C_j} h) = \sum_{g \in C_i, h \in C_j} gh = \sum_k \alpha_{ijk} \sum_{s \in C_k} s$.

□

Bemerkung

Die Gleichung

$$\overline{c}_i\overline{c}_j = \sum_{k=1}^{h} \alpha_{ijk}\overline{c}_k$$

liefert

$$\omega_l(\overline{c}_i)\omega_l(\overline{c}_j) = \sum_{k=1}^{h} \alpha_{ijk}\omega_l(\overline{c}_k).$$

In Matrixschreibweise:

$$\omega_l(\overline{c}_i) \begin{pmatrix} \omega_l(\overline{c}_1) \\ \vdots \\ \omega_l(\overline{c}_h) \end{pmatrix} = (\alpha_{ijk})_{1 \leq j,k \leq h} \begin{pmatrix} \omega_l(\overline{c}_1) \\ \vdots \\ \omega_l(\overline{c}_h) \end{pmatrix}$$

Die Bestimmung der $\omega_l(\overline{c}_i)$ ist also ein Eigenwertproblem. Diese Gleichung kann auch algorithmisch verwendet werden (Burnside-Dixon-Algorithmus). Die Matrix $(\alpha_{ijk})_{j,k} \in \mathbb{Z}^{h \times h}$ ist die der regulären Darstellung von $Z(KG)$ bzgl. der Basis $(\overline{c}_1, \ldots, \overline{c}_h)$.

Folgerung 5.39. *Die $\omega_l(\overline{c}_i)$ sind als Eigenwerte einer ganzzahligen Matrix ganz algebraische Zahlen.*

5.3.1 Die Orthogononalitätsrelationen

Satz 5.40. *(i)*

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g^{-1})g = \frac{\chi_i(1)}{|G|}\sum_j \chi_i(g_j^{-1})\overline{c}_j$$

(ii) Orthogonalitätsrelationen:

$$\frac{1}{|G|}\sum_{i=1}^{h}\chi_j(g_i)\chi_k(g_i^{-1})|C_i| = \delta_{jk}(1.OR)$$

$$\sum_{i=1}^{h}\chi_i(g_j)\chi_i(g_k^{-1}) = \delta_{jk}|C_G(g_j)|(2.OR)$$

Beweis.

(i) Sei $e_i = \sum \alpha_g g$. Dann ist $\alpha_g|G| = \rho(e_i g^{-1}) = \sum^j \chi_j(1)\chi_j(e_i g^{-1}) = \chi_i(1)\chi_i(g^{-1})$.

(ii) Es ist $e_i e_j = \delta_{ij}$, also

$$(\frac{\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g^{-1})g)(\frac{\chi_j(1)}{|G|}\sum_{h\in G}\chi_j(h^{-1})h) = (\frac{\chi_i(1)\chi_j(1)}{|G|}\sum_{k\in G}(\sum_g \chi_i(g^{-1})\chi_j(k^{-1}g))k$$

Also $\delta_{ij}e_i = \delta_{ij}\frac{\chi_i(1)}{|G|}\sum_{k\in G}\chi_i(k^{-1})k$. Koeffizientenvergleich für $k = 1$ liefert die erste Orthogonalitätsrelation (1.OR). Sei $X := (\chi_i(g_j))_{i,j}$ die Charaktertafel von G, $\tilde{X} := (\chi_i(g_j^{-1}))_{i,j}$ und $D = diag(|C_1|, \ldots, |C_h|)$. Dann ist $XD\tilde{X} = I$, also $X^{-1} = D\tilde{X}$ und $(D\tilde{X})X = I$, also $\tilde{X}X = D^{-1}$. Dies ist die zweite Orthogonalitätsrelation.

□

Bemerkung 5.41. *Ist χ der Charakter einer komplexen irreduziblen Darstellung Δ der endlichen Gruppe G und $g \in G$ ein Element der Ordnung d, so ist $\Delta(g)$ diagonalisierbar und $\chi(g)$ die Summe der Eigenwerte von $\Delta(g)$, also die Summe von d-ten Einheitswurzeln. Es gilt $|\chi(g)| \leq \chi(1)$ mit Gleichheit genau dann wenn $\Delta(g) \in \mathbb{C}^* I_n$ eine Skalarmatrix ist.*

Bemerkung 5.42. *Das Zentrum $Z(G)$ operiert auf der Menge der Konjugiertenklassen von G, ist nämlich C eine Konjugiertenklasse von G und $z \in Z(G)$, so ist $\{zg \mid g \in C\} = zC$ wieder eine Konjugiertenklasse von G. Es gilt $\chi_i(zg) = \omega_i(z)\chi_i(g)$. Ist also insbesondere $g \sim zg$, so gilt $\omega_i(z) = 1$ oder $\chi_i(g) = 0$.*

Folgerung 5.43. *Für $1 \leq i \leq h$ gilt $\chi_i(1) \mid [G : Z(G)]$.*

Beweis. Sei Œ χ_i ein treuer Charakter, d.h. Δ_i injektiv. Dann gilt $\omega_i(z) \neq 1$ für $1 \neq z \in Z(G)$. Also ist $\chi_i(g) \neq 0$ nur dann wenn die Bahn der Konjugiertenklasse C von g unter $Z(G)$ genau $|Z(G)|$ Elemente hat. Seien $C_1, \ldots, C_k$ die Vertreter der Bahnen der Länge $|Z(G)|$ unter der

Operation von $Z(G)$ auf der Menge der Konjugiertenklassen von G und $g_i \in G_i$. Dann gilt für $\chi = \chi_i$:

$$|G| = \sum_{g\in G} \chi(g)\chi(g^{-1}) = |Z(G)| \sum_{i=1}^{k} |C_i|\chi(g_i)\chi(g_i^{-1}) = |Z(G)|\chi(1) \sum_{i=1}^{k} \frac{|C_i|\chi(g_i)}{\chi(1)}\chi(g_i^{-1}) = |Z(G)|\chi(1)a$$

mit $a = \sum_{i=1}^{k} \omega_\chi(C_i)\chi(g_i^{-1})$ ganz algebraisch. □

Im allgemeinen gilt für eine K-Algebra A: Sind M_1, M_2 zwei A-Moduln, so ist ihr Tensorprodukt $M_1 \otimes_K M_2$ ein $A \otimes A$-Modul. Für Gruppenalgebren $A = KG$, kann man das Tensorprodukt wieder zu einem A-Modul machen: Seien M_1, M_2 KG-Moduln. Dann ist $M_1 \otimes_K M_2$ wieder ein KG-Modul durch $g(m_1 \otimes m_2) := gm_1 \otimes gm_2$ für alle $g \in G m_i \in M_i$. In Matrizen: $(\Delta_1 \otimes \Delta_2)(g) := \Delta_1(g) \otimes \Delta_2(g)$. Der zugehörige Charakter ist $(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g)$.

Beispiel Die Charaktertafel der A_5:

$\lvert C_G(g_i)\rvert$	1	15	20	12	12
A_5	(.)	(..)(..)	(...)	(.....)	$(.....)^{-1}$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	x	$1-x$
χ_5	3	-1	0	$1-x$	x
p	5	1	2	0	0
p'	6	2	0	1	1

mit $x = \frac{1+\sqrt{5}}{2}$ p ist der Permutationscharakter der A_5 auf 5 Punkten, $\chi_2 = p - \chi_1$ ein irreduzibler Charakter (da $(\chi_2, \chi_2) = 1$). Die Operation auf den 5-Sylowgruppen gibt eine Permutationscharakter der Ordnung 6: p'. $\chi_3 := p' - \chi_1$ ist ein irreduzibler Charakter. Die letzten beiden Zeilen ergeben sich aus den Orthogonalitätrelationen.

5.3.2 Eine Anwendung: Der p^aq^b Satz von Burnside

Satz 5.44. *(Burnside) Seien p, q Primzahlen und G eine endliche Gruppe der Ordnung $|G| = p^aq^b$. Dann ist G auflösbar.*

Ein einfacher Beweis ergibt sich mithilfe der Darstellungstheorie: Sei zunächst G eine beliebige endliche Gruppe und K ein Zerfällungskörper von G der Charakteristik 0.

Satz 5.45. *Sei $\Delta : G \to \mathrm{GL}_n(K)$ eine irreduzible Darstellung mit Charakter χ. Sei C eine Konjugiertenklasse von G mit $\mathrm{ggT}(|C|, n) = 1$. Dann gilt entweder $\chi(g) = 0$ für alle $g \in C$ oder $\Delta(g) \in K^*I_n$ für alle $g \in C$.*

Beweis. Sei $\mathbb{E}\, K = \mathbb{C}$. Sei ω der zu χ gehörende zentrale Charakter. Dann ist nach Folgerung 5.39

$$\omega(\overline{C}) = \omega(\sum_{g\in C} g) = \frac{|C|\chi(g)}{\chi(1)}$$

eine ganz algebraische Zahl, also wegen $\mathrm{ggT}(|C|, \chi(1)) = 1$ auch $\frac{\chi(g)}{\chi(1)}$ ganz. Da ganze Zahlen $\neq 0$ Betrag ≥ 1 haben, folgt dass entweder $\chi(g) = 0$ oder $|\chi(g)| = |\chi(1)|$ und somit $\Delta(g) = \zeta I_n$ für eine komplexe Einheitswurzel ζ. □

Satz 5.46. *Sei G eine nichtabelsche einfache Gruppe. Dann hat G keine Konjugiertenklasse $\neq \{1\}$ von Primzahlpotenzordnung.*

Beweis. Sei $|C| = p^a$ mit $a \geq 1$ und einer Primzahl p. Sei $\Delta : G \to \mathrm{GL}_n(\mathbb{C})$ eine irreduzible Darstellung, $\Delta \neq 1$. Dann ist $G \cong \Delta(G)$ und $Z(\Delta(G)) = 1$ da G einfach ist. Sei χ der Charakter von Δ. Ist der Charaktergrad $\chi(1)$ nicht durch p teilbar, so gilt also nach obigem Satz, dass $\chi(g) = 0$ für $g \in C$. Für die komplex irreduziblen Charaktere $\{1 = \chi_1, \chi_2, \ldots, \chi_h\}$ gilt also

$$0 = \sum_{i=1}^{h} \chi_i(g)\chi_i(1) == 1 + \sum_{p|\chi_i(1)} \chi_i(g)\chi_i(1)$$

woraus sich ein Widerspruch ergibt, da die Summe durch p teilbar ist, 1 jedoch nicht. □

Zum Beweis des p^aq^b-Satzes von Burnside, sei $|G| = p^aq^b$ mit $a+b \geq 1$ (sonst G zyklisch von Primzahlordnung). Zeigen: G hat einen echten Normalteiler. Dies ist klar, sobald $ab = 0$ gilt, denn dann ist G eine p-Gruppe. Seien also a und b größer als 0 und P eine p-Sylowgruppe von G. Dann ist $Z(P) \neq 1$. Wähle also $1 \neq z \in Z(P)$. Dann ist $P \leq C_G(z)$ und somit $|z^G| = \frac{|G|}{|C_G(z)|}$ eine Potenz von q. Der letzte Satz sagt dann aus, dass G nicht einfach ist.

5.3.3 Die Frobenius Reziprozität

Definition 5.47. *Seien χ, ψ Klassenfunktionen auf G (d. h. χ und ψ sind konstant auf den Konjugiertenklassen von G). Definieren ein Skalarprodukt:*

$$(\chi, \psi) := \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}) = \frac{1}{|G|} \sum_{i=1}^{h} \chi(g_i)\psi(g_i^{-1})|C_i|$$

Klar: Die irreduziblen Charaktere bilden eine Orthonormalbasis. Ist χ eine beliebige Klassenfunktion, so ist $\chi = \sum_{i=1}^{h} (\chi_i, \chi)\chi_i$.

Eine Anwendung: Das Burnsidesche Fixpunktlemma.
Sei M eine endliche G-Menge. Dann ist die Anzahl der Bahnen von G auf M gleich $\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}_M(g)$ wobei $\mathrm{fix}_M(g)$ die Anzahl der Fixpunkte von g auf M bezeichnet.
Jede G-Menge M liefert einen KG-Modul V_M der Dimension $|M|$ mit Basis M und $\Delta : G \to \mathrm{GL}_{|M|}(K), \Delta(g)(m) := gm$, die sogenannte Permutationsdarstellung. Dann ist $\mathrm{Spur}(\Delta(g)) = \chi(g) = \mathrm{fix}_M(g)$. Der Fixraum von G in V_M also

$$\{v \in V_M \mid \Delta(g)v = v \text{ für alle } g \in G\}$$

hat die Bahnsummen als K-Basis, seine Dimension ist also gleich der Anzahl a der Bahnen von G auf M. Dies ist auch die Vielfachheit des trivialen KG-Moduls (mit Charakter 1) in dem Modul V_M also

$$a = (1, \chi) = \frac{1}{|G|} \sum_{g \in G} 1\chi(g).$$

Bemerkung 5.48. *Seien A, B K-Algebren, M ein A-B-Bimodul, N ein B-Linksmodul.*

$$M \otimes_B N := M \otimes_K N / \langle (mb \otimes n - m \otimes bn | b \in B, m \in M, n \in N \rangle$$

ist wieder ein A-Linksmodul.

Definition 5.49. *Sei $H \leq G$, M ein KH-Modul. Dann heißt $M^G := KG \otimes_{KH} M$ der* **induzierte Modul**. *(ist wieder ein KG-Modul)*

Bemerkung 5.50. *Sei $G = \bigcup_{i=1}^n g_i H$. Dann ist $KG = \oplus_{i=1}^n g_i KH$ als KH-Rechtsmodul und $M^G \cong \oplus_{i=1}^n g_i KH \otimes_{KH} M = \oplus_{i=1}^n g_i \otimes_{KH} M \cong_K \oplus_{i=1}^n M$. $\dim_K(M^G) = \dim_K(M)|G : H| = \dim_K(M)n$. Ist $g \in G$ mit $gg_i = g_j h$ $h \in H$, so ist $g(g_i \otimes m) = g_j h \otimes m = g_j \otimes hm$. In Matrizen gilt: Ist $\Delta : H \to \mathrm{GL}_m(K)$ die Matrixdarstellung von H auf M bezüglich der Basis $(b_1, \ldots, b_m)$, so ist die Matrixdarstellung Δ^G von G auf M^G bezüglich der Basis*

$$(g_1 \otimes b_1, \ldots, g_1 \otimes b_m, g_2 \otimes b_1, \ldots, g_n \otimes b_m)$$

gegeben als die Blockmatrix

$$\Delta^G(g) = [\Delta^\circ(g_j g g_i^{-1})]_{i,j} \text{ wobei } \Delta^\circ(x) = \begin{cases} 0 & x \notin H \\ \Delta(x) & x \in H \end{cases}$$

Für den Charakter χ^G von Δ^G gilt

$$\chi^G(g) = \sum_{i=1}^n \chi^\circ(g_i g g_i^{-1}) \text{ wobei } \chi^\circ(x) = \begin{cases} 0 & x \notin H \\ \chi(x) & x \in H \end{cases}$$

und χ der Charakter von M ist.

Beispiel $M = K$, $h1 = h$ für alle $h \in H$ (triviale Darstellung). M^G ist ein Permutationsmodul, $\chi_{M^G}(g) =$ Anzahl der Fixpunkte von g auf G/H.

Beispiel $G = S_4$, $H = S_3$,

$$\langle (1,2), (1,2,3,4) \rangle = S_4 = S_3 \dot\cup (1,4) S_3 \dot\cup (2,4) S_3 \dot\cup (3,4) S_3$$

Setze man $g_1 = 1$, $g_2 = (1,4)$, $g_3 = (2,4)$, $g_4 = (3,4)$, $g = (1,2)$, $h = (1,2,3,4)$ so berechnet man

$g_1 g g_1^- 1 = g_2 g g_3^{-1} = g_3 g g_2^{-1} = g_4 g g_4^{-1} = (1,2) \in U$ und
$g_1 h g_2^{-1} = (1,2,3), g_2 h g_3^{-1} = (2,3), g_3 h g_4^{-1} = (1,2), g_4 h g_1^{-1} = (1,2,3) \in U.$

Für $W = \mathbb{C}$ mit der Signumsdarstellung erhält man also die induzierte Darstellung

$$g \mapsto \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \; h \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

(Zeilenkonvention). Ist $W = \mathbb{C}^2$ mit der 2-dimensionalen Darstellung (an Tafel).

Definition 5.51. *Ist φ eine Klassenfunktion von H, so definieren wir die Klassenfunktion φ^G von G durch*

$$\varphi^G(g) = \sum_{i=1}^{n} \varphi^\circ(g_i g g_i^{-1}) \text{ wobei } \varphi^\circ(x) = \begin{cases} 0 & x \notin H \\ \varphi(x) & x \in H \end{cases}$$

Dann ist φ^G unabhängig von der Wahl der Nebenklassenvertreter g_i.

Satz 5.52. *(Frobenius Reziprozität) Ist χ eine Klassenfunktion von G und φ eine Klassenfunktion von H, so gilt*

$$(\varphi^G, \chi)_G = (\varphi, \chi_{|H})_H$$

Beweis.

$$\begin{array}{l} (\varphi^G, \chi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) \sum_{i=1}^{n} \varphi^\circ(g_i g g_i^{-1}) = \\ \frac{1}{|G|} \sum_{i=1}^{n} \sum_{g \in g_i^{-1} H g_i} \chi(g^{-1}) \varphi(g_i g g_i^{-1}) = \\ \frac{1}{|G|} \sum_{i=1}^{n} \sum_{h \in H} \chi((g_i^{-1} h g_i)^{-1}) \varphi(h) = \\ \frac{n}{|G|} \sum_{h \in H} \chi(h^{-1}) \varphi(h) = (\varphi, \chi_{|H})_H \end{array}$$

□

Die Frobenius Reziprozität ist eine numerische Folgerung aus der konzeptionelleren Frobeinus-Nakayama Reziprozität, die einen Isomorphismus zwischen $\mathrm{Hom}_{KG}(W^G, V)$ und $\mathrm{Hom}_{KH}(V_{|H}, W)$ für jeden KG-Modul V und KH-Modul W herstellt. Ist φ der Charakter des KH-Moduls W und χ der Cahrakter des KG-Moduls V so gilt

$$(\varphi^G, \chi)_G = \dim(\mathrm{Hom}_{KG}(W^G, V)) \text{ und } (\varphi, \chi_{|H})_H = \dim(\mathrm{Hom}_{KH}(V_{|H}, W)).$$

Index

A-Modul, 57
K-Divisionsalgebra, 77
R-Maximalordnung, 86
R-Ordnung, 86
Ω-(zulässige) Untergruppe, 29
Ω-Gruppe, 29
Ω-Homomorphismus, 29
Ω-Kompositionsreihe, 30
Ω-Subnormalreihe, 30
Ω-einfach, 30
n-te Kreisteilungspolynom, 45
äquivalent, 71, 89

abelsch, 44
Ableitung, 17
algebraisch, 10
algebraisch abgeschlossen, 14
algebraisch abhängig, 11
algebraisch unabhängig, 11
algebraische Abschluss von K in L, 14
algebraischen Abschluss von K in L, 10
algebraischer Abschluss, 14
algebraischer Zahlkörper, 53
Algebrenhomomorphismus, 77
Annihilator, 58
Artinsch, 63
auflösbar, 33, 44, 50
auflösbar durch Radikale, 50
Automorphismengruppe, 21

Braueräquivalent, 82
Brauergruppe, 82

Casimir-Element, 86
Charakter, 39
charakteristisch, 21
charakteristische Reihen, 33
Charaktertafel, 90

Darstellung, 77
direkte Produkt, 24, 59
direkte Summe, 59
Diskriminante, 54
divisibel, 76

einfach, 57, 78
einfache, 10
elementar aus M konstruierbar, 51
endlich, 8
Erweiterungskörper, 8
exakt, 73
exakte Folge von A-Moduln, 73

Faktorgruppe, 22
Familie, 4
Fermatsche Primzahl, 52
frei, 59
Frobeniusautomorphismus, 16

Galoisgruppe, 41
galoissch, 41
ganz über $\mathbb{Z}$, 53
ganz über R, 87
ganz abgeschlossen, 86
ganzen Abschluß von $\mathbb{Z}$ in R, 53
Ganzheitsbasis, 54
Gerade, 51
Grad, 8
Grammatrix, 54
Gruppenring, 88

halbeinfach, 60, 61
Hauptreihen, 33
Homomorphismus, 21

Idempotent, 66, 70
Index, 81
induktiv geordnet, 4

induzierte Modul, 96
injektiver, 74
inneren Automorphismen, 21
inneres direktes Produkt, 24
inverse Differente, 54
irreduzibel, 89
Isomorphismus, 21

Jacobsonradikal, 64

Körperautomorphismus, 12
Körperhomomorphismus, 12
Körper, 8, 57
Körpererweiterung, 8
Körperhomomorphismus über K, 12
kleinste obere Schranke, 24
kommutativ, 57
Kommutatorreihe, 33
Kommutatoruntergruppe, 21
Komplement, 36
Kompositionsreihen, 33
Kompositum, 43
Kreis, 51
kurze exakte Folge, 73

Linksideale, 57
Linksnoethersch, 63
Linkssordnung, 86
lokal, 67

maximales Element, 4
maximales Ideal, 6
Minimalpolynom, 10

Noethersch, 62, 63
Norm, 47
normal, 19
normale Hülle, 20
Normalteiler, 21

obere Schranke, 4
opposite Ring, 58
Ordnung, 4
orthogonal, 70

partiell geordnete Menge, 24
perfekt, 18, 33
PIM, 74
primitive n-te Einheitswurzel, 44
primitives Element, 17, 18, 43
primitives Idempotent, 70
Primkörper, 9
projektiver, 73

Rang, 59
Rechtsordnung, 86
reduzierte charakteristische Polynom von a, 84
reduzierte Norm, 84, 85
reduzierte Spur, 84, 85
reguläre A-Modul, 57
rein transzendent, 11
Ring, 57
Ring der ganzen Zahlen in K, 53

Schiefkörper, 57
Segment, 4
separabel, 17, 85
Separabilitätsgrad, 19
spaltet, 73
Spur, 47
Spurbilinearform, 48

Teilkörper, 8
Teilverband, 25
transzendent, 10
Transzendenzbasis, 11
Transzendenzgrad, 11

unzerlegbar, 67, 89

Verband, 25
Verbandshomomorphismus, 25
vollständig geordnet, 4

wohlgeordnet, 4
Wurzelkörper, 13

zentral primitiv, 70
zentrale Charaktere, 91
Zentralisator, 77
Zentrum, 21, 57
Zerfällungskörper, 13, 82, 90
Zirkel und Lineal konstruierbar, 51

zyklisch, 44
zyklischer Modul, 58