Algebra

Lukas Pottmeyer

Vorwort

Dieses Skript entstand aus der Zusammensetzung von Skripten zu meinen Vorlesungen Algebra I an der TU Darmstadt WS13/14 und Algebra II an der TU Dortmund im WS14/15. Diese einzelnen Skripte dienten lediglich zur Nachbearbeitung zu den jeweiligen Vorlesungen. Das Skript orientiert sich weitestgehend an den Vorlesungen Algebra I+II von Prof. Dr. Walter Gubler an der Eberhardt-Karls-Universität Tübingen in den Semestern WS09/10+SS10. Die Abbildungen 3.1, 4.5, 5.2, 5.3, 7.1, 7.2, 7.4, A.2 sind der Oberwolfach Photo Collection [**MFO**] des MFO entnommen, die diese Bilder freundlicherweise unter der Creative Commons License Attribution-Share Alike 2.0 Germany zur Verfügung stellen. Die restlichen Abbildungen sind nach meinem bestem Wissen öffentliches Eigentum.
Für die Vollständigkeit und Fehlerfreiheit kann nicht garantiert werden. Fehler können gerne an meine aktuelle Email-Adresse gesendet werden.

Lukas Pottmeyer

Einleitung

Um das Jahr 825 verfasste der persische Gelehrte *Abū Ǧa'far Muḥammad b. Mūsā al-Ḫwārazmī* das Lehrbuch *Al-Kitāb al-muḫtaṣar fī ḥisāb al-ǧabr wa-'l-muqābala* (etwa: Das kurzgefasste Buch über die Rechenverfahren durch Ergänzen und Ausgleichen). Dieses Buch präsentiert allgemeine Verfahren zum Lösen von linearen und quadratischen Gleichungen in den positiven reellen Zahlen. Aus dem Wort *al-ǧabr* leitet sich das Wort *Algebra* ab. Die klassische Algebra beschäftigt sich also mit dem Lösen von polynomiellen Gleichungen. Der Fall der linearen Gleichungen wurde ausgiebig in der linearen Algebra behandelt. (Das Wort *Algorithmus* stammt übrigens vom Namen *al-Ḫwārazmī*). In der modernen Algebra beschäftigt man sich mit dem Studium von Verknüpfungen, wie sie zum Beispiel Gruppen definieren. Dieser abstrakte Zugang hat den Vorteil, dass er nicht auf einen konkreten Zahlbereich zum Lösen von Gleichungen beschränkt ist. Dadurch kann man Ergebnisse erlangen, die weit über das Lösen einer speziellen gegebenen Gleichung hinaus gehen. So werden wir unter anderem sehen, dass es eine algebraische Lösungsformel für polynomielle Gleichungen vom Grad n (wie die p,q-Formel falls $n = 2$) nur gibt, wenn $n \leq 4$ gilt. Ein weiteres Highlight ist der Beweis der Unmöglichkeit der Quadratur des Kreises. Das heißt, dass es nicht möglich ist nur mit Hilfe von Zirkel und Lineal aus einem gegebenen Kreis ein flächengleiches Quadrat zu konstruieren. Dies sind nur zwei der Anwendungen, die wir in diesem Skript betrachten.

Wir werden die Grundlagen der Gruppentheorie voraussetzen, da diese bereits in vorangegangenen Vorlesungen studiert wurden. Nichtsdestotrotz werden wir die wesentlichen Definitionen und Sätze ohne Beweise wiederholen. In diesem Skript studieren wir die Verknüpfungen in Ringen, Körpern und Moduln. Die ersten beiden Strukturen sind bereits aus der linearen Algebra bekannt. Ein Modul ist kurzgesagt ein Vektorraum der über einem Ring definiert ist. Bei Letzterem ist es erstaunlich festzustellen wie viel Allgemeiner diese Struktur im Vergleich zu den sehr zahlen Vektorräumen ist. Mit diesem Wissen werden wir einen anderen Aspekt der Gruppentheorie betrachten, die sogenannte Darstellungstheorie endlicher Gruppen. Diese erlaubt es abstrakte endliche Gruppen in einem geometrischen Kontext zu untersuchen. Zum Schluß geben wir eine (sehr) kurze Einführung in die algebraische Geometrie.

Notation

Mit $\mathbb{N}$ bezeichnen wir die natürlichen Zahlen, diese enthalten nicht die 0. Die Menge der natürlichen Zahlen mit 0 bezeichnen wir mit $\mathbb{N}_0$. Für eine Menge M bezeichnen wir mit $|M|$ die Kardinalität von M.

Inhaltsverzeichnis

KAPITEL 1

Gruppentheorie

1.1. Wiederholung

In diesem Abschnitt fassen wir die wesentlichen Definitionen und Sätze in der Gruppentheorie zusammen, die wir in dieser Vorlesung benutzen werden. Da der gesamte Inhalt aus der Vorlesung 'Einführung in die Algebra' bekannt seien sollte, werden wir auf Beweise weitestgehend verzichten.

DEFINITION 1.1.1. Sei G eine Menge mit einer inneren Verknüpfung $\cdot : G \times G \longrightarrow G$; $(a, b) \mapsto a \cdot b$. Wir definieren die folgenden Eigenschaften.

(G1) (Assoziativität) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(G2) (Neutralelement) $\exists e \in G$ mit $a \cdot e = e \cdot a = a$
(G3) (Inverse) $\forall a \in G : \exists a^{-1} \in G$ mit $a \cdot a^{-1} = a^{-1} \cdot a = e$

Ist die Eigenschaft (G1) erfüllt, so heißt $(G, \cdot)$ *Halbgruppe*. Eine Halbgruppe die auch (G2) erfüllt heißt *Monoid*. Schließlich heißt ein Monoid, das auch (G3) erfüllt *Gruppe*. Eine Gruppe heißt *abelsch*, genau dann, wenn sie kommutativ ist, d.h.

$$a \cdot b = b \cdot a \quad \forall a, b \in G.$$

Ist aus dem Zusammenhang klar welche Verknüpfung gemeint ist, dann schreiben wir kurz nur G für eine Halbgruppe, ein Monoid oder eine Gruppe.

BEMERKUNG 1.1.2. Für ein Monoid M definieren wir $M^* = \{a \in M | \exists a^{-1} \in M$, mit $a^{-1} \cdot a = a \cdot a^{-1} = e\}$. Es ist offensichtlich, dass M^* eine Gruppe bzgl. „$\cdot$“ bildet.

Ein *Homomorphismus* ist eine Abbildung $\varphi : G_1 \longrightarrow G_2$ zwischen zwei algebraischen Strukturen G_1 und G_2, die die Struktur von G_1 erhält. Unterobjekte sind Teilmengen eines gegebenen Objekts mit derselben „vererbten“ Verknüpfung. Für Gruppen heißt dies explizit:

DEFINITION 1.1.3. Sind G_1, G_2 Gruppen so ist ein Gruppen-Homomorphismus eine Abbildung $\varphi : G_1 \longrightarrow G_2$ mit $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
Wir definieren eine *Untergruppe* H einer Gruppe G als Teilmenge $H \subseteq G$ mit den folgenden 3 Axiomen:

(i) $e \in H$

(ii) $a, b \in H \Longrightarrow a \cdot b \in H$
(iii) $a \in H \Longrightarrow a^{-1} \in H$

Durch diese Axiome erreicht man wie gewünscht, dass H selbst eine Gruppe bezüglich der von G vererbten Verknüpfung ist.

DEFINITION/SATZ 1.1.4. *Sei $\varphi : G_1 \longrightarrow G_2$ ein Gruppen-Homomorphismus. Wir definieren den* Kern *von φ als*

$$\ker(\varphi) := \varphi^{-1}(e_2) = \{a \in G_1 \big| \varphi(a) = e_2\}.$$

Dann ist $\ker(\varphi)$ *eine Untergruppe von G_1 und $\varphi(G_1)$ ist eine Untergruppe von G_2. Weiter ist φ genau dann injektiv, wenn $ker(\varphi) = \{e_1\}$ ist.*
Ein Isomorphismus *ist ein Homomorphismus der eine beidseitige Umkehrabbildung besitzt, die selbst wieder ein Homomorphismus ist. Man kann sogar zeigen, dass eine Abbildung genau dann ein Gruppen-Isomorphismus ist, wenn sie ein bijektiver Gruppen-Homomorphismus ist.*

BEISPIEL 1.1.5. Sei X eine Menge. Wir definieren $M(X)$ als die Menge aller Abbildungen $f : X \longrightarrow X$ und wir benutzen die Hintereinanderausführung „$\circ$“ als Verknüpfung auf $M(X)$. Dann ist $M(X)$ ein Monoid mit Neutralelement id, und $M(X)^*$ ist die Menge der bijektiven Selbstabbildungen von X. Wir nennen $S(X) := M(X)^*$ die *symmetrische Gruppe* auf X. Ist X endlich, so können wir stets $X = \{1, \ldots, n\}$ annehmen. In diesem Fall wird $S(X)$ auch *Permutationsgruppe* genannt und wir schreiben hierfür kurz S_n. Jedes $\sigma \in S_n$ hat ein Signum $sig(\sigma) \in \{-1, 1\}$. Die Abbildung $sig : S_n \longrightarrow \{\pm 1\}$ ist ein Gruppen-Homomorphismus, dessen Kern nach 1.1.4 eine Untergruppe von S_n ist, die wir mit A_n bezeichnen und die *Alternierende Gruppe* heißt. Für $n \geq 4$ sind S_n und A_n keine abelschen Gruppen.

THEOREM 1.1.6 (Satz von Cayley). *Jede Gruppe G ist isomorph zu einer Untergruppe von $S(X)$ für eine geeignete Menge X. Falls $n = ord(G) < \infty$, dann kann man $S(X) = S_n$ wählen.*

BEWEIS. Sei $g \in G$ beliebig. Betrachte die Abbildung $\tau_g : G \to G; h \mapsto gh$. Da $\tau_{g^{-1}}$ ein beidseitiges Inverses zu τ_g ist, wissen wir dass τ_g bijektiv ist. Damit ist τ_g ein Element der symmetrischen Gruppe $S(G)$. Natürlich ist das Neutralelement in $S(G)$ gegeben durch τ_e. Die Abbildung $\varphi : G \to S(G)$; $g \mapsto \tau_g$ ist damit wohldefiniert. Weiter gilt für beliebige $g, g' \in G$:

$$\varphi(gg')(h) = \tau_{gg'}(h) = (gg')h = g(g'h) = \tau_g \circ \tau_{g'}(h) = (\varphi(g) \circ \varphi(g'))(h) \forall h \in G$$

Also ist φ ein Gruppen-Homomorphismus. Dieser ist injektiv, da aufgrund der Eindeutigkeit des Neutralelements der Kern von φ trivial ist. Also ist G

isomorph zu $\varphi(G)$. Letzteres ist als Bild einer Gruppe unter einem Homomorphismus wieder eine Gruppe, also eine Untergruppe von $S(G)$. □

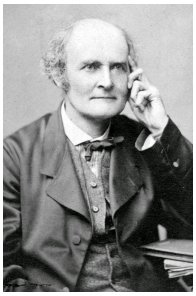


ABBILDUNG 1.1. Der englische Mathematiker *Arthur Cayley* (1821 - 1895) führte 1854 als erster die Definition und den Begriff einer abstrakten Gruppe ein. Von 1846 bis 1863 arbeitete er als Anwalt. Er gab die Mathematik jedoch nie auf und publizierte auch in dieser Zeit starke mathematische Arbeiten.

DEFINITION 1.1.7. Sei $(G_i)_{i\in I}$ eine Familie von Gruppen. Dann betrachten wir

$$\prod_{i\in I} G_i = \left\{(x_i)_{i\in I} \middle| x_i \in G_i\right\}$$

Wir definieren dann das *Produkt* der Gruppen $(G_i)_{i\in I}$ als $\prod_{i\in I} G_i$ versehen mit der Verknüpfung

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i \cdot y_i)_{i\in I}$$

Es folgt sofort, dass das Produkt von Gruppen wieder eine Gruppe ist.
Dieses direkte Produkt von Gruppen ist nicht zu verwechseln mit dem Produkt von Teilmengen einer gegebenen Gruppe. Ist G eine Gruppe und sind Y und Z beliebige Teilmengen von G so schreiben wir $YZ = \{yz|y \in Y, z \in Z\}$. Insbesondere ist $HH = H$ für jede Untergruppe H von G.

DEFINITION 1.1.8. Eine Untergruppe N der Gruppe G heißt *Normalteiler* von G, genau dann wenn $gNg^{-1} = N$ gilt für alle $g \in G$. Ist dies erfüllt so schreiben wir $N \triangleleft G$.
Für eine beliebige Untergruppe H von G sind die Mengen gH, $g \in G$, die *Linksnebenklassen von* H. Die Menge aller Linksnebenklassen von H bezeichnen wir mit G/H.
Die Anzahl der verschiedenen Linksnebenklassen von H ist der *Index von* H *in* G und wird mit $[G : H]$ bezeichnet.

BEMERKUNG 1.1.9. Jeder Linksnebenklasse von H in G können wir ein (nicht eindeutiges) Element g aus G zuordnen, so dass gH die gewählte Linksnebenklasse darstellt. Die Verknüpfung $(g_1H)(g_2H) = (g_1g_2H)$ ist wohldefiniert genau dann wenn $H \triangleleft G$ und dies ist genau dann der Fall wenn G/H eine Gruppe bzgl. dieser Verknüpfung bildet. G/H heißt dann *Faktorgruppe*.

In Linksnebenklassen zu rechnen ist dasselbe wie *modulo* einer Untergruppe H zu rechnen. Das heißt, wir schreiben $a \equiv b \mod H$ für $a, b \in G$ genau dann wenn $ab^{-1} \in H$ ist. Manchmal schreiben wir hierfür auch $a \sim_H b$. Beachte, dass $\sim_H$ eine Äquivalenzrelation ist und die Äquivalenzklasse von $g \in G$ genau die Linksnebenklasse $\overline{g} = gH$ ist.

BEMERKUNG 1.1.10. Die Quotientenabbildung $\pi : G \longrightarrow {}^{G}/_{N}$; $g \mapsto \overline{g}$ ist ein surjektiver Gruppen-Homomorphismus, weil wir in ${}^{G}/_{N}$ repräsentantenweise rechnen dürfen. Dann ist $ker(\pi) = N$.

PROPOSITION 1.1.11. *Sei $\varphi : G_1 \longrightarrow G_2$ ein Gruppen-Homomorphismus, dann ist $ker(\varphi)$ ein Normalteiler von G_1.*

THEOREM 1.1.12 (Homomorphiesatz). *Sei $\varphi : G_1 \longrightarrow G_2$ ein Gruppen-Homomorphismus und N_1 ein Normalteiler von G_1 mit $N_1 \subseteq ker(\varphi)$. Dann gibt es genau einen Homomorphismus $\overline{\varphi} : {}^{G_1}/_{N_1} \to G_2$ so, dass $\overline{\varphi}(\overline{x}) = \varphi(x)$. Weiter ist der Kern von $\overline{\varphi}$ gleich ${}^{ker(\varphi)}/_{N_1}$.*

KOROLLAR 1.1.13 (Isomorphiesatz). *Wir betrachten einen surjektiven Gruppen-Homomorphismus $\varphi : G_1 \to G_2$. Dann gibt es genau einen Isomorphismus $\overline{\varphi} : {}^{G_1}/_{ker(\varphi)} \to G_2$ so, dass $\overline{\varphi}(\overline{x}) = \varphi(x)$.*

THEOREM 1.1.14 (1. Isomorphiesatz). *Sei G eine Gruppe, H eine Untergruppe und $N \triangleleft G$. Dann gilt:*

(a) *HN ist eine Untergruppe von G mit Normalteiler $N \triangleleft HN$*
(b) *$H \cap N \triangleleft H$*
(c) *${}^{H}/_{H\cap N} \longrightarrow {}^{HN}/_{N}$; $\quad x(H \cap N) \mapsto xN$ ist ein Isomorphismus*

THEOREM 1.1.15 (2. Isomorphiesatz). *Sei $H \triangleleft G$, $N \triangleleft G$, $N \subseteq H \subseteq G$. Dann gilt*

(a) *$N \triangleleft H$*
(b) *${}^{H}/_{N} \triangleleft {}^{G}/_{N}$*
(c) *${}^{(G/N)}/_{(H/N)} \xrightarrow{\sim} {}^{G}/_{H}$, $\quad \overline{gN} \mapsto gH$ ist ein Gruppen-Isomorphismus.*

DEFINITION 1.1.16. Für eine endliche Gruppe G ist die *Ordnung* $\mathrm{ord}(G) \in \mathbb{N}$ die Anzahl der Elemente von G.

THEOREM 1.1.17 (Lagrange). *Sei H eine Untergruppe der Gruppe G. Dann gilt*

$$\mathrm{ord}(G) = \mathrm{ord}(H)[G : H]$$

KOROLLAR 1.1.18. $\mathrm{ord}(H)$ *ist ein Teiler von* $\mathrm{ord}(G)$.

Mit den üblichen Rechenregeln für das Symbol ∞, erweitert sich dieses Theorem auch auf unendliche Gruppen.

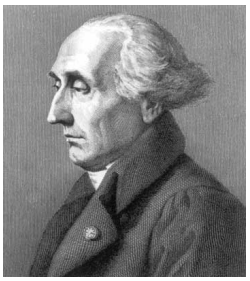


ABBILDUNG 1.2. *Joseph-Louis Lagrange* (1736 - 1813) war ein herausragender italienischer Mathematiker und Astronom. Er wurde als Giuseppe Lodovico Lagrangia geboren und war bereits mit 19 Jahren Mathematikprofessor in Turin.

DEFINITION 1.1.19. Für $g \in G$ definieren wir die Potenzen durch $g^0 := e$ und

$$g^m := \underbrace{g \cdot g \cdot \ldots \cdot g}_{m-mal}, \quad g^{-m} := (g^{-1})^m$$

für jedes $m \in \mathbb{N}$. Die *Ordnung von* g ist definiert als

$$\mathrm{ord}(g) := \min\{n \in \mathbb{N} | g^n = e\}$$

Wenn es kein $n \in \mathbb{N}$ gibt mit $g^n = e$, dann sei die Ordnung $\mathrm{ord}(g) := \infty$.

PROPOSITION 1.1.20. *Sei $Y \subseteq G$. Dann ist*

$$\langle Y \rangle := \{{g_1}^{\delta_1} \ldots {g_r}^{\delta_r} | r \in \mathbb{N}, g_j \in Y, \delta_j \in \{-1, 1\}\}$$

die kleinste Untergruppe von G, die Y enthält. Wir nennen $\langle Y \rangle$ die von Y erzeugte Untergruppe von G.

DEFINITION 1.1.21. Eine Gruppe die von einem Element erzeugt wird heißt *zyklische Gruppe* und hat nach 1.1.20 die Form

$$G = \{g^n | n \in \mathbb{Z}\}.$$

Beachte, dass eine zyklische Gruppe abelsch ist. Denn es gilt

$$g^n g^m = g^{n+m} = g^{m+n} = g^m g^n.$$

LEMMA 1.1.22. *Sei G eine Gruppe und $g \in G$. Dann ist die Ordnung der von g erzeugten Untergruppe $\langle g \rangle$ gleich der Ordnung von g. Sprich*

$$\mathrm{ord}(g) = \mathrm{ord}(\langle g \rangle).$$

PROPOSITION 1.1.23. *Sei G eine Gruppe. Dann gilt:*

(a) *G ist genau dann zyklisch, wenn es ein $m \in \mathbb{N}_0$ gibt mit $G \cong \mathbb{Z}/m\mathbb{Z}$.*
(b) *Falls G eine endliche zyklische Gruppe ist, gilt $G \cong \mathbb{Z}/\mathrm{ord}(G)\mathbb{Z}$.*
(c) *Eine unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$.*

BEMERKUNG 1.1.24. Sei $g \in G, \mathrm{ord}(g) < \infty, k \in \mathbb{Z}$. Dann gilt

$$g^k = e \Longleftrightarrow \mathrm{ord}(g) \mid k.$$

PROPOSITION 1.1.25. (a) *Jede Untergruppe von* $\mathbb{Z}$ *hat die Form* $m\mathbb{Z}$ *für geeignetes* $m \in \mathbb{N}$

(b) *Umgekehrt ist* $m\mathbb{Z}$ *eine Untergruppe von* $\mathbb{Z}$ *für alle* $m \in \mathbb{Z}$

(c) *Es ist* $m_1\mathbb{Z} = m_2\mathbb{Z}$ *genau dann wenn* $m_2 = \pm m_1$ *ist*

THEOREM 1.1.26. *Jede endliche abelsche Gruppe ist isomorph zu*

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

für gewisse $n_1, \ldots, n_r \in \mathbb{Z}$.

BEMERKUNG 1.1.27. Auf den ganzen Zahlen $\mathbb{Z}$ schreiben wir kurz $\mod m$ und meinen damit $\mod m\mathbb{Z}$.

THEOREM 1.1.28 (Satz von Euler). *Sei* $a \in \mathbb{Z}$, $m \in \mathbb{N}$ *und* $\mathrm{ggT}(a, m) = 1$. *Dann gilt:*

$$a^{\varphi(m)} \equiv 1 \mod m,$$

wober $\varphi(m) = |\{k \in \{1, \ldots, m\} | \, \mathrm{ggT}(k, m) = 1\}|$ *die —Eulersche* φ*-Funktion ist.*

ABBILDUNG 1.3. Der Schweizer *Leonhard Euler* (1707 - 1783) war einer der begabtesten und produktivsten Mathematiker aller Zeiten. Seine Werke wurden in mehr als 70 Bänden veröffentlicht und enthalten mehr als 800 Resultate. Seine Werke können auf der Seite `http://eulerarchive.maa.org` eingesehen werden.

THEOREM 1.1.29 (Kleiner Satz von Fermat). *Sei* p *eine Primzahl und* $a \in \mathbb{Z}$. *Dann gilt:*

$$a^p \equiv a \pmod p.$$

ABBILDUNG 1.4. *Pierre de Fermat* (1607 - 1665) war ein französischer Jurist und gilt als *König der Hobby-Mathematiker*. Besondere Bekanntheit erlangte er durch die Fermat Vermutung, ein Problem für das er behauptete eine Lösung zu besitzen, das aber erst 1994 von Andrew Wiles mit Hilfe modernster Mathematik gelöst werden konnte.

DEFINITION 1.1.30. Sei G eine Gruppe und X eine Menge. Die Gruppe G *operiert auf* X genau dann wenn es eine Abbildung gibt mit: G operiert auf $X \iff$ wir haben eine Abbildung
$G \times X \longrightarrow X$, $(g, x) \mapsto g \cdot x \in X$ mit:

(a) $e \cdot x = x$

(b) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \forall x \in X, g_1, g_2 \in G$

DEFINITION 1.1.31. Sei eine Gruppenoperation von G auf der Menge X gegeben. Für $x \in X$ heißt

$$G \cdot x = \{g \cdot x \big| g \in G\}$$

die *Bahn* von x. Eine Gruppenoperation heißt *transitiv*, wenn X nur aus einer Bahn besteht.

BEISPIEL 1.1.32. Wir definieren eine Relation $\sim$ auf X durch

$$x \sim y \iff \exists g \in G \text{ mit } x = g \cdot y$$

Man zeigt leicht, dass $\sim$ eine Äquivalenzrelation ist und die Äquivalenzklassen die Bahnen sind.

DEFINITION 1.1.33. Jede Gruppe G operiert auf sich selbst durch Konjugation. D.h.:

$$x \sim y \iff \exists g \in G \text{ mit } x = g^{-1} y g.$$

Die Äquivalenzklassen bezüglich $\sim$ heißen *Konjugationsklassen* von G.

SATZ 1.1.34. *Jedes $\sigma \in S_n$ lässt sich bis auf Vertauschen der Faktoren eindeutig schreiben als ein Produkt von Zyklen $\tau_1, \ldots, \tau_r$ der Länge mindestens 2. Bezeichnen wir mit m_i die Länge von τ_i, für alle $i \in \{1, \ldots, r\}$, und nehmen oBdA an, dass $m_1 \leq m_2 \leq \ldots \leq m_r$ ist, dann ist der* Zykeltyp *$(m_1, \ldots, m_r)$ von σ eindeutig bestimmt. Weiter sind zwei Elemente aus S_n in derselben Konjugationsklasse genau dann wenn sie denselben Zykeltyp besitzen.*

DEFINITION 1.1.35. Für $x \in X$ heißt

$$\text{Stab}(x) := \{g \in G \big| g \cdot x = x\}$$

der *Stabilisator* von $x \in X$. Offensichtlich ist $\text{Stab}(x)$ eine Untergruppe von G.

THEOREM 1.1.36 (Klassengleichung). *Sei G eine endliche Gruppe, X eine endliche Menge und G operiere auf X. Sei R ein Repräsentantensystem aus*

X bezüglich der äquivalenzrelation $\sim$ von oben, d.h. aus jeder Bahn wählen wir genau ein Element. Dann gilt:

$$|X| = \sum_{x \in R} \underbrace{[G : \mathrm{Stab}(x)]}_{|G|/|\mathrm{Stab}(x)|}$$

DEFINITION 1.1.37. Eine Gruppe G heißt *auflösbar* genau dann, wenn es eine *Normalreihe*

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

gibt, so dass die *Faktoren* G_j/G_{j-1} abelsch sind für alle $j = 1, \ldots, n$.

PROPOSITION 1.1.38. *Sei G auflösbar und H eine Untergruppe von G. Dann ist H auflösbar.*

PROPOSITION 1.1.39. *Sei N ein Normalteiler von G. Dann ist G auflösbar genau dann wenn N und G/N auflösbar sind.*

SATZ 1.1.40. *Die Gruppe G ist auflösbar genau dann wenn eine Normalreihe existiert, sodass alle Faktoren G_j/G_{j-1} zyklische Gruppen der Ordnung p_j sind für Primzahlen p_j.*

DEFINITION 1.1.41. Sei G eine Gruppe. Dann ist das *Zentrum von G* gegeben durch

$$Z(G) = \{a \in G | ab = ba \text{ für alle } b \in G\}.$$

Natürlich ist $Z(G)$ ein Normalteiler von G.

DEFINITION 1.1.42. Eine endliche Gruppe G ist eine *p-Gruppe*, für eine Primzahl p, genau dann wenn die Ordnung von G eine Potenz von p ist.

PROPOSITION 1.1.43. *Das Zentrum einer endlichen p- Gruppe ist nicht trivial.*

LEMMA 1.1.44. *Jede endliche p-Gruppe ist auflösbar.*

BEWEIS. Angenommen es existiert eine p-Gruppe G die nicht auflösbar ist. Es ist $|G| = p^n$ für ein $n \in \mathbb{N}$. Sei n minimal gewählt mit der Eigenschaft dass es eine p-Gruppe G mit p^n Elementen gibt, die nicht auflösbar ist. Das Zentrum $Z(G)$ von G ist nicht trivial (siehe Proposition 1.1.43). Weiter ist G auflösbar genau dann wenn $Z(G)$ und $G/Z(G)$ auflösbar sind. Da $Z(G)$ abelsch ist, ist $Z(G)$ insbesondere auflösbar. Also folgt nach Voraussetzung, dass $G/Z(G)$ nicht auflösbar ist und $|G/Z(G)| = p^m$, mit $m < n$. Dies ist ein Widerspruch zur Minimalität von n. Somit sind alle endlichen p-Gruppen auflösbar. □

SATZ 1.1.45. *Die symmetrische Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist.*

KAPITEL 2

Ringtheorie

2.1. Ringe

In einem Ring werden wir eine Gruppenstruktur um eine weitere innere Verknüpfung erweitern, wie z.B. bei einem Körper oder den ganzen Zahlen $\mathbb{Z}$. Beides sind grundlegende Beispiele für Ringe. Nun wollen wir einen Ring formal definieren.

DEFINITION 2.1.1. Ein *Ring* R ist eine Menge R mit zwei inneren Verknüpfungen $+$ und $\cdot$ so, dass

(R1) $(R, +)$ ist eine abelsche Gruppe,
(R2) $(R, \cdot)$ ist eine Halbgruppe,
(R3) es gelten die Distributivgesetze

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

und

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

Wenn nicht ausdrücklich anders gefordert werden wir in dieser Vorlesung stets annehmen, dass R ein Neutralelement (*Einselement*) 1 bzgl. „$\cdot$“ hat; d.h. dass $(R, \cdot)$ ein Monoid ist. Das Neutralelement bzgl. $+$ bezeichnen wir üblicherweise mit 0.

BEMERKUNG 2.1.2. Wir bezeichnen die Inverse von a bzgl. „$+$“ mit $-a$ und setzen $a - b := a + (-b)$. Wir benutzen folgende Rechenregeln:

(i) $a \cdot 0 = 0 = 0 \cdot a$
(ii) Das Einselement ist eindeutig.
(iii) $-a = (-1) \cdot a$
(iv) $R = \{0\}$ genau dann wenn $0 = 1$ gilt.

BEWEIS. Dies sind einfache Folgerungen aus den Axiomen. □

DEFINITION 2.1.3. Ein Ring heißt *kommutativ* falls die Multiplikation „$\cdot$“ kommutativ ist. Ein *Schiefkörper* ist ein Ring $K \neq \{0\}$ in dem jedes Element $a \neq 0$ ein Inverses bzgl. $\cdot$ besitzt. Ein *Körper* ist ein kommutativer Schiefkörper.

DEFINITION 2.1.4. Sei R ein kommutativer Ring. Wir wollen die aus $\mathbb{Z}$ bekannte Teilbarkeit auf R verallgemeinern. Wir nennen $a \in R$ *einen Teiler* von $b \in R$ genau dann, wenn es ein $c \in R$ gibt, mit $a \cdot c = b$. Wir nennen dann b *ein Vielfaches von* a und benutzen hierfür die Notation $a \mid b$.
Wenn $a \mid 1$, dann heißt a *eine Einheit* von R. Dies ist per Definition äquivalent dazu, dass a ein multiplikatives Inverses besitzt. Die Menge aller Einheiten in R ist gegeben durch R^*. Beachte, dass $(R^*, \cdot)$ eine (kommutative) Gruppe bildet. Wir nennen diese Gruppe *Einheitengruppe* von R.
Wenn es für $a \in R$ ein $c \in R \setminus \{0\}$ gibt, mit $a \cdot c = 0$, dann heißt a *Nullteiler* in R. Man darf diesen Begriff nicht mit den Teilern von Null verwechseln! Jedes $a \in R$ ist ein Teiler von Null im obigen Sinn, aber Nullteiler sind meist sehr spezielle Elemente in R.

DEFINITION 2.1.5. Ein *Integritätsbereich* ist ein kommutativer Ring R mit $0 \neq 1$, der keine Nullteiler verschieden von 0 hat.

BEISPIEL 2.1.6. Beispiele für Körper sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Z}/p\mathbb{Z}$, für eine Primzahl p.
Für $n \in \mathbb{N}$ und einen Körper K definieren wir die Menge aller $n \times n$-Matrizen mit einträgen aus K als $M_n(K)$. Weiter übernehmen wir die Notation aus Bemerkung 1.1.9 und schreiben die Elemente aus der Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ als $\overline{k} = k + m\mathbb{Z}$. Wir werden später sehen, dass auch $\mathbb{Z}/m\mathbb{Z}$ einen Ring mit der zusätzlichen Verknüpfung $\overline{l} \cdot \overline{k} = \overline{lk}$, für alle $l, k \in \mathbb{Z}$, ist.

Ring	komm.	Integritätsbereich	Einheitengruppe
$\mathbb{Z}$	✓	✓	$\{-1, 1\}$
Körper K	✓	✓ $(a \cdot c = 0 \overset{c \neq 0}{\Rightarrow} a = 0 \cdot c^{-1} = 0)$	$K \setminus \{0\}$
$M_n(K)$	$\Leftrightarrow n = 1$	-	$GL_n(K)$
$\mathbb{Z}/6\mathbb{Z}$	✓	- $(\overline{2} \cdot \overline{3} = \overline{0})$	$\{\overline{1}, \overline{5}\}$

TABELLE 1. Ein Paar Beispiele für Ringe und ihre Eigenschaften

DEFINITION 2.1.7. Eine Abbildung $\varphi : R_1 \longrightarrow R_2$ zwischen Ringen R_1 und R_2 heißt *Ring-Homomorphismus* genau dann wenn für alle $a, b \in R_1$ gilt

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(ii) $\varphi(a \cdot b) = \varphi(a)\varphi(b)$ und
(iii) $\varphi(1) = 1$.

Insbesondere ist also jeder Ring-Homomorphismus ein Gruppen-Homomorphismus zwischen den jeweiligen additiven Gruppen.

DEFINITION 2.1.8. Ein Ring-Homomorphismus $\varphi : R_1 \longrightarrow R_2$ heißt *Ring-Isomorphismus* genau dann wenn ein Ring-Homomorphismus $\Psi : R_2 \longrightarrow R_2$ existiert, mit

(i) $\varphi \circ \psi = \mathrm{id}_{R_2}$ und
(ii) $\psi \circ \varphi = \mathrm{id}_{R_1}$.

SATZ 2.1.9. *Die Abbildung φ ist ein Ring-Isomorphismus genau dann wenn φ ein bijektiver Ring-Homomorphismus ist.*

BEWEIS. Wie bei Gruppen. □

KONSTRUKTION 2.1.10. Für Ringe $R_1, R_2, \ldots, R_r$ definieren wir auf $R_1 \times \ldots \times R_r$ (analog zu Definition 1.1.7) eine Ringstruktur durch komponentenweise Verknüpfung. Das heißt:

$$(a_1, \ldots, a_r) + (b_1, \ldots, b_r) := (a_1 + b_1, \ldots, a_r + b_r)$$

und

$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) := (a_1 \cdot b_1, \ldots, a_r \cdot b_r)$$

Bis auf triviale Fälle ist dieses Produkt nie ein Integritätsbereich, da Elemente der Form $(0, \ldots 0, a_i, 0, \ldots 0)$ Nullteiler sind.
Analog können wir für beliebige Familien $(R_i)_{i \in I}$ von Ringen das *Produkt* $\prod_{i \in I} R_i$ konstruieren.

2.2. Ideale und Restklassenringe

In diesem Abschnitt seien R, R_1 und R_2 stets kommutative Ringe. Aus der Gruppentheorie kennen wir die Faktorgruppen G/N. Sie besteht aus allen Linksnebenklassen von N und ist genau dann eine wohldefinierte Gruppe wenn N ein Normalteiler von G ist (siehe Definition 1.1.8 und Bemerkung 1.1.9). Da $(R, +)$ abelsch ist, ist damit $(G/N, +)$ eine abelsche Gruppe für alle Untergruppen $H \subseteq (R, +)$.
Im Allgemeinen wird G/N jedoch kein Ring sein bezüglich der repräsentantenweise definierten Verknüpfungen. Wir wollen daher ein Analogon von Normalteilern für Ringe definieren.

DEFINITION 2.2.1. Eine additive Untergruppe I von R heißt *Ideal* in R genau dann wenn $a \cdot I \subseteq I$ gilt für alle $a \in R$. Analog zum Normalteiler in der Gruppentheorie besagt die Notation $I \lhd R$, dass I ein Ideal in R ist.

Sei I ein Ideal in R. Wie in Bemerkung 1.1.9 bezeichnen wir mit $\overline{a} = a + I$ die Nebenklasse von a bezüglich I in R.

PROPOSITION 2.2.2. *Sei I eine additive Untergruppe von R. Dann ist I genau dann ein Ideal in R wenn R/I bezüglich der repräsentantenweise definierten Verknüpfungen ein Ring ist.*

BEWEIS. Wir müssen zwei Implikationen beweisen.

$\Longrightarrow$ Wir wissen bereits, dass $(R/I, +)$ eine abelsche Gruppe ist. Wir wollen zeigen, dass die Multiplikation $(\overline{a} \cdot \overline{b} = \overline{a \cdot b})$ wohldefiniert ist auf R/I; d.h. unabhängig von der Wahl des Repräsentanten. Wir haben die Äuivalenzen

$$\overline{a_1} = \overline{a_2} \Longleftrightarrow \overline{a_1} - \overline{a_2} = \overline{0} \Longleftrightarrow a_1 - a_2 \in I.$$

Für $\overline{a_1} = \overline{a_2}$ und $b \in R$ beliebig folgt damit aus dem Idealaxiom $(a_1 - a_2) \cdot b = a_1 \cdot b - a_2 \cdot b \in I$. Wieder mit den äquivalenzen von oben haben wir damit $\overline{a_1 \cdot b} = \overline{a_2 \cdot b}$. Aufgrund der Kommutativität von R gilt auch $\overline{b \cdot a_1} = \overline{b \cdot a_2}$. Damit ist die Multiplikation auf R/I wohldefiniert.

Die Ringaxiome für R/I folgen sofort aus den entsprechenden Axiomen für R, weil wir nun repräsentantenweise rechnen dürfen.

$\Longleftarrow$ Für beliebige Elemente $a \in I$ und $r \in R$ gilt $\overline{a} \cdot \overline{r} = \overline{0} \cdot \overline{r} = \overline{0}$. Dies bedeutet nichts anderes als $a \cdot r \in I$. Also ist I ein Ideal.

□

DEFINITION 2.2.3. Sei $I \lhd R$.

(a) Wir nennen R/I *Faktorring*. Elemente aus dem Ring R/I heißen *Restklassen von R modulo I*.

(b) Wir sagen $a, b \in R$ sind *kongruent modulo I* genau dann wenn $\overline{a} = \overline{b} \in R/I$. Wir schreiben hierfür auch $a \equiv b \mod I$.

BEMERKUNG 2.2.4. Die kanonische Abbildung $\pi : R \longrightarrow R/I \; ; \; a \mapsto \overline{a}$, ist ein surjektiver Ring-Homomorphismus.

DEFINITION 2.2.5. Für einen Homomorphismus $\varphi : R_1 \longrightarrow R_2$ kommutativer Ringe definieren wir den Kern von φ als

$$\ker(\varphi) := \{a \in R_1 | \varphi(a) = 0\}.$$

Beachte, dass $\ker(\varphi)$ stets ein Ideal in R_1 ist. Denn für $a \in \ker(\varphi)$ und $r \in R$ beliebig gilt

$$\varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0 \quad .$$

Also ist auch $a \cdot r \in \ker(\varphi)$.
Wie üblich heißt $S \subseteq R$ *Teilring* des Ringes R genau dann wenn S mit den Verknüpfungen „$+$“ und „$\cdot$“ von R selbst ein Ring ist.

SATZ 2.2.6 (Isomorphiesatz). *Sei $\varphi : R_1 \longrightarrow R_2$ ein Homomorphismus kommutativer Ringe. Dann ist $\varphi(R_1)$ ein Teilring von R_2 und es gilt:*

$$R_1/\ker(\varphi) \xrightarrow{\sim} \varphi(R_1) \quad ; \quad \overline{a} \mapsto \varphi(a)$$

ist ein wohldefinierter Ring-Isomorphismus.

BEWEIS. Übung. □

PROPOSITION 2.2.7. *Sei $I \lhd R$. Dann ist $I = R$ genau dann wenn I eine Einheit enthält.*

BEWEIS. Wir zeigen die beiden Implikationen.

$\Longrightarrow$ $I = R \Longrightarrow 1 \in I \cap R^* \subseteq I$.

$\Longleftarrow$ Sei also $u \in I$ eine Einheit und $v \in R$ das multiplikative Inverse von u. Für $a \in R$ beliebig gilt nun

$$a = a \cdot 1 = a \cdot (v \cdot u) = \underbrace{(a \cdot v)}_{\in R} \cdot \underbrace{u}_{\in I} \quad .$$

Mit dem Idealaxiom aus 2.2.1 folgt sofort $a \in I$. Damit ist $I = R$.

□

KOROLLAR 2.2.8. *In einem Körper K sind $\{0\}$ und K die einzigen Ideale.*

BEWEIS. Wenn $I \neq \{0\}$ ein Ideal ist, dann enthält I eine Einheit und es folgt $I = K$ nach Proposition 2.2.7. □

KOROLLAR 2.2.9. *Sei K wieder ein Körper und $\varphi : K \longrightarrow R$ ein Ring-Homomorphismus. Wir nehmen weiter an, dass $R \neq \{0\}$ ist. Dann ist φ injektiv.*

BEWEIS. Wie in der Gruppentheorie gesehen ist die Injektivität von φ äquivalent zu $\ker(\varphi) = \{0\}$. Sei also $I = \ker\varphi$. Nach Korollar 2.2.8 gilt entweder $I = \{0\}$ oder $I = K$. Wegen $\varphi(1) = 1 \neq 0$ ist der zweite Fall ausgeschlossen und somit $\ker\varphi = \{0\}$ □

DEFINITION 2.2.10. Sei R ein Ring und I ein Ideal in R.

(a) I heißt *Maximalideal* genau dann wenn I ein maximales Element von $\{J \lhd R | J \neq R\}$ bzgl. der partiellen Ordnung $\subseteq$ ist.

(b) I heißt *Primideal* genau dann wenn $I \neq R$ und wenn gilt

$$ab \in I \Longrightarrow a \in I \text{ oder } b \in I.$$

PROPOSITION 2.2.11. *Sei $\{0\} \neq R \neq I \lhd R$. Dann gilt:*

(a) *I Primideal $\Longleftrightarrow$ R/I Integritätsbereich,*

(b) *I Maximalideal $\Longleftrightarrow$ R/I Körper.*

BEWEIS. Aussage (a) wird in den Übungen bewiesen. Zu (b):

$\Longrightarrow$ Da I ein Ideal ist, wissen wir nach Proposition 2.2.2, dass R/I ein kommutativer Ring ist. Weiter gilt $R/I \neq \{0\}$, da $I \neq R$.

Es bleibt also die Existenz von multiplikativen Inversen zu zeigen.

Sei dazu $\overline{a} \in R/I \setminus \{\overline{0}\}$ beliebig. Insbesondere ist also $a \notin I$. Die Menge $a \cdot R = \{a \cdot r | r \in R\}$ ist ein Ideal, denn es gilt für $r_1, r_2 \in R$

- $r_1 \cdot a - r_2 \cdot a = (r_1 - r_2) \cdot a$,
- $r_1 \cdot (r_2 \cdot a) = (r_1 \cdot r_2) \cdot a$.

Damit ist auch $J := I + aR$ ein Ideal (siehe Übungen). Offensichtlich gilt $I \subsetneq J$ und da I ein Maximalideal ist, folgt $J = R$.

Damit gibt es $x \in I$ und $y \in R$ mit $1 = x + ya$. Also gilt für die Restklassen modulo I, dass $\overline{1} = \overline{ya} = \overline{ay}$ und damit ist $\overline{a}$ invertierbar in R/I. Damit haben wir gezeigt, dass R/I ein Körper ist.

$\Longleftarrow$ Sei R/I ein Körper und $J \lhd R$ mit $J \supsetneq I$. Zu zeigen ist $J = R$. Wähle $a \in J \setminus I$. Dann ist $\overline{a}$ in R/I invertierbar. Also existiert ein $\overline{b} \in R/I$ mit $\overline{a \cdot b} = \overline{1}$. Daraus schließen wir $1 \in \underbrace{ab}_{\in J} + I \subseteq J$ und nach Proposition 2.2.7 folgt $J = R$.

□

KOROLLAR 2.2.12. *Jedes Maximalideal ist ein Primideal.*

BEWEIS. Folgt direkt aus Proposition 2.2.11. □

PROPOSITION 2.2.13. *Sei S ein Integritätsbereich und $\varphi : R \longrightarrow S$ ein Ring-Homomorphismus. Dann ist* $\ker(\varphi)$ *ein Primideal.*

BEWEIS. Wir wissen schon, dass $\ker(\varphi)$ ein Ideal ist. Seien also $a, b \in R$ mit $a \cdot b \in \ker(\varphi)$. Das heißt $0 = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Da S als Integritätsbereich keine nicht-trivialen Nullteiler besitzt ist $\varphi(a) = 0$ oder $\varphi(b) = 0$. Dies ist gleichbedeutend mit $a \in \ker(\varphi)$ oder $b \in \ker(\varphi)$, was zu zeigen war. □

Es ist leicht zu sehen (siehe Übungen), dass für zwei Ideale I, J von R auch $I \cap J$ und $I + J$ wieder Ideale von R sind.

SATZ 2.2.14 (Chinesischer Restsatz). *Seien $I_1, \ldots, I_n$ Ideale von R mit $I_k + I_l = R$ für alle $k \neq l$, wobei $k, l \in \{1, \ldots, n\}$. Dann ist die Abbildung*

$$\varphi : R \longrightarrow R/I_1 \times \ldots \times R/I_n \quad ; \quad a \mapsto (a + I_1, \ldots, a + I_n)$$

ein surjektiver Ring-Homomorphismus und $\ker(\varphi) = I_1 \cap \ldots \cap I_n$.

Mit dem Isomorphiesatz 2.2.6 induziert φ also einen kanonischen Isomorphismus

$$\overline{\varphi} : {}^{R}\!/_{(I_1 \cap \ldots \cap I_n)} \xrightarrow{\sim} {}^{R}\!/_{I_1} \times \ldots \times {}^{R}\!/_{I_n}.$$

Beweis. Wir führen den Beweis in vier Schritten.

1. Schritt: Es gilt $I_j + \bigcap_{k \neq j} I_k = R$ für alle $j \in \{1, \ldots, n\}$.

Für $k \neq j$ gibt es ein $a'_k \in I_k$ und ein $a_k \in I_j$ mit $1 = a_k + a'_k$. Ausmultiplizieren und Anwenden der Idealeigenschaft liefert

$$1 = \prod_{k \neq j} (a_k + a'_k) \in I_j + \bigcap_{k \neq j} I_k.$$

Aus Proposition 2.2.7 ergibt sich der 1. Schritt.

2. Schritt: φ ist surjektiv.

Wie im 1. Schritt gesehen gibt es Elemente $e_j \in I_j$ und $e'_j \in \bigcap_{k \neq j} I_k$ mit $1 = e_j + e'_j$. Sei $(a_1 + I_1, \ldots, a_n + I_n)$ aus ${}^{R}\!/_{I_1} \times \ldots \times {}^{R}\!/_{I_n}$ beliebig. Wir müssen zeigen, dass es im Bild von φ liegt. Es gilt

$$e'_j \equiv 1 \pmod{I_j} \quad \text{und} \quad e'_j \equiv 0 \pmod{I_k} \quad \forall k \neq j$$

und somit erhalten wir

$$a_j \equiv e'_j a_j \equiv e'_1 a_1 + \cdots + e'_n a_n \pmod{I_j}.$$

Für $a := e'_1 a_1 + \cdots + e'_n a_n$ gilt also

$$\varphi(a) = (a + I_1, \ldots, a + I_n) = (a_1 + I_1, \ldots, a_n + I_n) \in {}^{R}\!/_{I_1} \times \ldots \times {}^{R}\!/_{I_n},$$

wie gewünscht.

3. Schritt: φ ist ein Ring-Homomorphismus.

Dies folgt sofort aus der Tatsache, dass die Restklassenabbildungen $R \to {}^{R}\!/_{I_j}$ Ring-Homomorphismen sind.

4. Schritt: Es gilt $\ker(\varphi) = I_1 \cap \ldots \cap I_n$.

$a \in \ker(\varphi) \iff a \equiv 0 \pmod{I_j}\, \forall j \iff a \in \bigcap_{j=1}^{n} I_j$ □

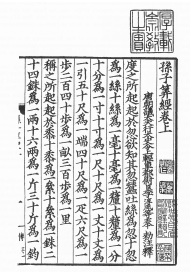


Abbildung 2.1. Die Schrift *Sunzi Suanjing* wurde im 5. Jahrhundert n.C. vom chinesischen Gelehrten Sun-Zi verfasst und enthält im dritten Kapitel die älteste bekannte Version des *chinesischen Restsatzes*.

2.3. Beispiele für Ringe

Wir werden drei wichtige Konstruktionen von Ringen kennenlernen.

2.3.1. Sei R ein kommutativer Ring und $n \in \mathbb{N}$. Dann bezeichnet $M_n(R)$ die Menge der $n \times n$-Matrizen mit Einträgen aus R. Mit der, aus der linearen Algebra bekannten Matrixaddition und -multiplikation wird $M_n(R)$ tatsächlich zu einem Ring.
Für $A = (a_{ij}) \in M_n(R)$ haben wir die Determinante

$$\det(A) := \sum_{\sigma \in S_n} \operatorname{sig}(\sigma) a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \in R$$

mit der Eigenschaft

$$\det(A \cdot B) = \det(A) \det(B). \tag{1}$$

für alle $A, B \in M_n(R)$. Dies folgt wie in der linearen Algebra, da dort in den Beweisen lediglich Ringeigenschaften benutzt wurden.
Mit $\operatorname{adj}(A)$ bezeichnen wir die *Adjunkte* von $A \in M_n(R)$. Da die Einträge dieser Matrix gerade Determinanten von Matrizen aus $M_{n-1}(R)$ sind, gilt auch $\operatorname{adj}(A) \in M_n(R)$. Analog zur linearen Algebra folgt

$$A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) E_n. \tag{2}$$

Hier bezeichnet wie üblich E_n die Einheitsmatrix in $M_n(R)$.

THEOREM 2.3.2. *Die Matrix A ist invertierbar in $M_n(R)$ genau dann wenn $\det(A)$ invertierbar in R ist.*

BEWEIS. Die Hinrichtung folgt aus (1) und $\det(E_n) = 1$. Die Rückrichtung folgt aus (2), da $A^{-1} = \det(A)^{-1} \cdot \operatorname{adj}(A) \in M_n(R)$ gilt. □

2.3.3. Die Menge $\mathbb{H} := \{A \in M_2(\mathbb{C}) | A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}, \text{ mit } w, z \in \mathbb{C}\}$ bildet einen Teilring von $M_2(\mathbb{C})$ und ihre Elemente heißen *Quaternionen*. Dass dies ein Teilring ist, sieht man leicht, bis auf die Abgeschlossenheit bzgl. „$\cdot$“. Es gilt aber:

$$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} \cdot \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -z_2 \overline{w_1} - \overline{w_2} z_1 & -\overline{w_1} w_2 + \overline{z_1} \overline{z_2} \end{pmatrix} \in \mathbb{H}.$$

Wir definieren die *Norm* auf $\mathbb{H}$ als

$$N(A) := \det(A) = |z|^2 + |w|^2.$$

Sei $A \in \mathbb{H}$, $A \neq 0$. Dann folgt aus (2)

$$\operatorname{adj}(A) = \begin{pmatrix} \overline{z} & -w \\ \overline{w} & z \end{pmatrix} \in \mathbb{H} \text{ und } A^{-1} = \frac{1}{N(A)} \operatorname{adj}(A) \in \mathbb{H}.$$

Also hat jedes Element in $\mathbb{H} \setminus \{0\}$ ein multiplikatives Inverses in $\mathbb{H}$. Damit sehen wir, dass die Quaternionen einen Schiefkörper bilden. Allerdings gilt

$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Damit ist $\mathbb{H}$ nicht kommutativ und insbesondere kein Körper.
Betrachte die Abbildung

$$\mathbb{C} \longrightarrow \mathbb{H} \quad ;$$

$$z = Re(z) + Im(z) \cdot i \mapsto Re(z) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + Im(z) \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

Dies ist offensichtlich ein injektiver Ring-Homomorphismus. Wir dürfen also $\mathbb{C}$ mit einem Teilring von $\mathbb{H}$ identifizieren in dem wir $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ setzen. Definieren wir weiter $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ so können wir $\mathbb{H}$ schreiben als

$$\mathbb{H} := \{x_0 + ix_1 + jx_2 + kx_3 \big| x_0, x_1, x_2, x_3 \in \mathbb{R}\}$$

Neben den üblichen Rechenregeln auf $\mathbb{R}$ gelten die folgenden Rechenregeln:

- $i^2 = j^2 = k^2 = -1$
- $ij = -ji = k$
- $jk = -kj = i$
- $ki = -ik = j$

2.3.4. Seien R, S kommutative Ringe. Der Ring $R[x]$ der Polynome in der Variablen x mit Koeffizienten in R wird analog zum in der linearen Algebra betrachteten Spezialfall definiert in dem R ein Körper ist. Das heißt, $R[x]$ besteht aus den formalen Summen $\sum_{i=0}^{n} a_i x^i$ mit $n \in \mathbb{N}_0$ und $a_i \in R$ für alle $i \in \{0, \ldots, n\}$. Mit den üblichen Rechenregeln für Addition und Multiplikation wird dies tatsächlich zu einem Ring.

LEMMA 2.3.5. *Sei $\varphi : R \longrightarrow S$ ein Ring-Homomorphismus und $s \in S$ beliebig. Dann existiert genau ein Ring-Homomorphismus $\varphi_s : R[x] \longrightarrow S$ mit $\varphi_s(x) = s$ und $\varphi_s|_R = \varphi$.*

BEWEIS. Für einen solchen Homomorphismus muss gelten $\varphi_s(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \varphi_s(a_i)\varphi_s(x)^i = \sum_{i=0}^{n} \varphi(a_i)s^i$. Daraus folgt sofort die Eindeutigkeit. Dass diese Zuordnung auch einen Homomorphismus beschreibt folgt sofort aus der Homomorphieeigenschaft von φ. □

Falls $R \subseteq S$ ein Teilring ist und φ als Inklusion gegeben ist so nennen wir den Homomorphismus φ_s *Einsetzhomomorphismus.*
Wir definieren für $f = \sum_k a_k x^k \in R[x] \setminus \{0\}$ den *Grad* von f durch

$$\operatorname{grad}(f) := \max\{k | a_k \neq 0\}$$

und setzen $\operatorname{grad}(0) := -\infty$.

PROPOSITION 2.3.6. *Sei R ein Integritätsbereich. Dann gilt*

(a) *die Gradformel:* $\operatorname{grad}(f \cdot g) = \operatorname{grad}(f) + \operatorname{grad}(g)$,
(b) $R[x]$ *ist ein Integritätsbereich,*
(c) $R[x]^* = R^*$.

BEWEIS. Seien $f, g \in R[x]$.

Zu (a): Falls $f = 0$ oder $g = 0$, ist die Aussage trivial. Sei also $f \neq 0 \neq g$ und schreibe

$$f = \sum_{i=0}^{n} a_i x^i \text{ mit } a_n \neq 0 \text{ und } g = \sum_{j=0}^{m} \text{ mit } a_m \neq 0 \quad .$$

Dann ist $f \cdot g = a_n \cdot a_m \cdot x^{n+m} +$*Terme kleinerer Ordnung.* Damit haben wir

$$\operatorname{grad}(f \cdot g) = n + m = \operatorname{grad}(f) + \operatorname{grad}(g),$$

wie gewünscht.

Zu (b): Sei $f \cdot g = 0$. Dann folgt nach a) $\operatorname{grad}(f) + \operatorname{grad}(g) = -\infty$. Insbesondere ist also $\operatorname{grad}(f) = -\infty$ oder $\operatorname{grad}(g) = -\infty$. Dies ist äquivalent zu $f = 0$ oder $g = 0$.

Zu (c): Dass R^* in $R[x]^*$ enthalten ist, ist klar. Für die andere Richtung sei $f \cdot g = 1$. Wieder mit (a) folgt dann $\operatorname{grad}(f) + \operatorname{grad}(g) = 0$. Damit muss sowohl f als auch g in R liegen und nach Annahme in R^*.

□

2.4. Lokalisierungen

Bekanntlich ist $\mathbb{Q}$ der kleinste Körper, der die ganzen Zahlen $\mathbb{Z}$ enthält. Diese Konstruktion des *Quotientenkörpers* verallgemeinern wir für beliebige Integritätsbereiche. Da es kaum mehr Aufwand ist, wollen wir die Gelegenheit nutzen und das Prinzip der Lokalisierung eines Ringes darstellen. Lokalisierungen werden besonders in der algebraischen Zahlentheorie und der algebraischen Geometrie zum Einsatz kommen. Für den Moment betrachten wir es lediglich als Konzept aus einem gegebenen Ring weitere Ringe zu konstruieren.
In diesem Abschnitt sei wieder R ein kommutativer Ring.

DEFINITION 2.4.1. Eine Teilmenge $T \subseteq R$ heißt *multiplikativ* falls $1 \in T$ und mit $a, b \in T$ auch $ab \in T$ ist.

BEISPIEL 2.4.2.
- Die Einheitengruppe R^* ist multiplikativ in R.
- Für ein Primideal $P \triangleleft R$ ist $R \setminus P$ eine multiplikative Teilmenge von R.
- Falls R ein Integritätsbereich ist erhalten wir als Spezialfall, dass $R \setminus \{0\}$ multiplikativ ist.

KONSTRUKTION 2.4.3. Sei $T \subseteq R$ multiplikativ. Auf $R \times T$ führen wir die Äquivalenzrelation

$$(a, b) \sim (c, d) :\Longleftrightarrow \exists t \in T \text{ , mit } t(ad - bc) = 0$$

ein. Dass diese tatsächlich eine Äquivalenzrelation ist, wird in den Übungen gezeigt. Die äquivalenzklasse von (a, b) bezeichnen wir wie bei Brüchen mit $\frac{a}{b}$ und den Raum aller Äquivalenzklassen bezeichnen wir mit $T^{-1}R$. Auf $T^{-1}R$ definieren wir die Verknüpfungen

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

Diese Verknüpfungen sind wohldefiniert. Denn: Gilt $\frac{a}{b} = \frac{a'}{b'}$ in $T^{-1}R$ dann existiert ein $t \in T$ mit $t(ab' - ba') = 0$. Für $c \in R$ und $d \in T$ beliebig gilt damit auch

$$t((ad + bc)b'd - (a'd + b'c)bd) = t(ab' - a'b)d^2 + t(bcb'd - b'cbd) = 0 \quad .$$

Somit haben wir $\frac{ad+bc}{bd} = \frac{a'd+b'c}{b'd}$ für alle $\frac{c}{d} \in T^{-1}R$. Folglich ist die Addition wohldefiniert. Die Wohldefiniertheit der Multiplikation funktioniert analog. Nun folgt leicht, dass $T^{-1}R$ mit obigen Verknüpfungen einen kommutativen Ring bildet. Als Einselement haben wir $\frac{a}{a} = \frac{1}{1} = 1$ und als Nullelement haben wir $\frac{0}{a} = 0$ für alle $a \in T$. Beachte dass beides identisch ist genau dann wenn $0 \in T$. D.h. nach Bemerkung 2.1.2(4)

$$T^{-1}R = \{0\} \Longleftrightarrow 0 \in T.$$

DEFINITION 2.4.4. Der in 2.4.3 konstruierte Ring $T^{-1}R$ heißt *Ring der Brüche von R bzgl. T.*

Der Ring der Brüche von R bzgl. T entsteht also grob gesagt dadurch, dass wir alle Elemente aus $T \subseteq R$ zu Einheiten in R machen. Insbesondere haben wir $(R^*)^{-1}R \cong R$. Der formale Beweis für diese Aussage folgt genau wie weiter unten in 2.4.7 und ist dem motivierten Leser überlassen.

DEFINITION 2.4.5. Ein Ring R heißt *lokal* genau dann wenn er nur ein einziges Maximalideal enthält.

Beispiel 2.4.6. Sei nun $P \triangleleft R$ ein Primideal und $T = R \setminus P$. In diesem Fall wollen wir $T^{-1}R =: R_P$ setzen und von der *Lokalisierung* von R an P sprechen. Die Idealeigenschaft von P impliziert sofort, dass die Menge $M_P = \{\frac{a}{b} | a \in P \text{ und } b \in R \setminus P\} \subsetneq R_P$ ein Ideal in R_P ist. Jedes Element $\frac{c}{d} \in R_P \setminus M_P$ ist eine Einheit in R_P, denn aus $c \notin P$ folgt $\frac{d}{c} \in R_P$. Weiter ist $\frac{d}{c} \cdot \frac{c}{d} = \frac{cd}{dc} = 1$. Aus Proposition 2.2.7 folgt damit, dass ein Ideal von R_P das nicht in M_P enthalten ist gleich R_P sein muss. Also ist R_P ein lokaler Ring mit eindeutigem Maximalideal M_P.

Konstruktion 2.4.7. Sei nun R ein Integritätsbereich. Dann ist $\{0\}$ ein Primideal in R. Als Spezialfall von 2.4.6 erhalten wir dass $\text{Quot}(R) := (R \setminus \{0\})^{-1}R$ ein Körper ist. Wir nennen $\text{Quot}(R)$ den *Quotientenkörper* von R. Betrachte den Ring-Homomorphismus $i : R \longrightarrow \text{Quot}(R)$; $r \mapsto \frac{r}{1}$. Da R ein Integritätsbereich ist, gilt

$$\begin{aligned} \ker(i) &= \{r \in R | \tfrac{r}{1} = 0 = \tfrac{0}{1}\} \\ &= \{r \in R | \exists t \in R \setminus \{0\} \text{ , mit } t(1 \cdot r - 1 \cdot 0) = 0\} = \{0\}. \end{aligned}$$

Also ist i injektiv und wir können R mit dem Teilring $i(R)$ von $\text{Quot}(R)$ identifizieren.

Fazit 2.4.8. Jeder Integritätsbereich R ist in einem Körper enthalten. Der kleinste Körper, der R enthält, ist nach Konstruktion $\text{Quot}(R)$. Dies entspricht exakt dem Fall $\mathbb{Z} \subset \mathbb{Q} = \text{Quot}(\mathbb{Z})$.

2.4.9. Wir wollen im Folgenden die Bezeichnung *Lokalisierung* erklären. Sei $R := \mathbb{R}[x]$ der Polynomring in einer Variablen über dem Körper $\mathbb{R}$. Ein beliebiges Polynom $f(x) \in R$ kann an jedem Element aus $\mathbb{R}$ ausgewertet werden. Wir erhalten eine (beliebig oft) differenzierbare Funktion

$$f(x) : \mathbb{R} \to \mathbb{R}; \qquad r \mapsto f(r)$$

Wenn wir Brüche von Polynomen $f(x)/g(x)$, mit $f(x), g(x) \in R$, betrachten ist dies nicht mehr beliebig möglich, da $g(r) = 0$ für manche $r \in \mathbb{R}$ gelten kann.
Sei $P = xR$. Wir behaupten, dass P ein Primideal ist.
Seien dazu $f(x) = \sum_{i=0}^{m} a_i x^i, g(x) = \sum_{j=0}^{n} b_j x^j \in R$ mit $f(x)g(x) \in P$. D.h. Der konstante Term von $f(x)g(x)$ ist gleich $0 = a_0 b_0$. Da a_0 und b_0 Elemente aus $\mathbb{R}$ sind, ist dies nur dann erfüllt wenn $a_0 = 0$ oder $b_0 = 0$ gilt. Dies bedeutet nichts anderes als $f(x) \in P$ oder $g(x) \in P$. Damit ist P ein Primideal und wir können die Lokalisierung R_P betrachten.
R_P besteht genau aus den Brüchen (Funktionen) $f(x)/g(x)$ mit $g(0) \neq 0$. Die Funktion $f(x)/g(x)$ lässt sich also an $x = 0$ auswerten. Es existiert sogar ein

$\epsilon > 0$, so dass

$$r \mapsto {}^{f(r)}\!/_{g(r)}$$

eine wohldefinierte und (beliebig oft) differenzierbare Funktion auf dem Intervall $(-\epsilon, \epsilon)$ beschreibt. Der Ring R_P besteht also aus genau denjenigen Brüchen von Polynomen, die *lokal* in einer Umgebung der Null definiert sind.

2.5. Teilbarkeit in Monoiden

In diesem Abschnitt wollen wir die Voraussetzungen schaffen um den *Fundamentalsatz der Arithmetik* zu verallgemeinern.

THEOREM 2.5.1 (wahrscheinlich im 3. Jahrhundert v. Chr.). *Jede ganze Zahl $a \in \mathbb{Z} \setminus \pm 1$ lässt sich als Produkt $\pm p_1 \cdots p_n$ schreiben, mit eindeutig bestimmten Primzahlen $p_1, \ldots, p_n$.*

Wir wollen also Teilbarkeit in Ringen studieren. Da hierfür nur die Multiplikation eine Rolle spielt, können wir allgemeiner Teilbarkeit in Monoiden M betrachen, die die *Kürzungsregel* erfüllen. D.h.:

$$ab = ac \Longrightarrow b = c \quad \text{für } a, b, c \in M.$$

Sei M im Folgenden stets ein solches Monoid. Als Beispiel kann man $M = R \setminus \{0\}$ setzen für einen Integritätsbereich R. Wie üblich bezeichnen wir die Menge aller Einheiten in M mit M^*.
Wir definieren Teiler, Vielfache und Einheiten von M analog zu 2.1.4.

DEFINITION 2.5.2. Zwei Elemente $a, b \in M$ heißen *assoziiert* genau dann wenn $a \mid b$ und $b \mid a$. Wir schreiben hierfür $a \sim b$.

Da Teilbarkeit transitiv ist, ist $\sim$ eine Äquivalenzrelation. Aus der Kürzungsregel folgt leicht

$$a \sim b \Longleftrightarrow \exists u \in M^* \text{ mit } a = ub.$$

Als Spezialfall erhalten wir

$$a \sim 1 \Longleftrightarrow a \in M^*.$$

DEFINITION 2.5.3. Ein Element $a \in M$ heißt *irreduzibel* genau dann, wenn die folgenden beiden Eigenschaften erfüllt sind:

(i) $a \notin M^*$
(ii) $b \mid a \Longrightarrow b \sim 1$ oder $b \sim a$

DEFINITION 2.5.4. Ein Element $a \in M$ heißt *prim* genau dann, wenn die folgenden beiden Eigenschaften erfüllt sind:

(i) $a \notin M^*$
(ii) $a \mid bc \Longrightarrow a \mid b$ oder $a \mid c$

Für $M = \mathbb{Z} \setminus \{0\}$ wissen wir, dass beide Definitionen identisch sind. Für allgemeine Monoide ist dies allerdings nicht der Fall. Jedoch gilt folgende Proposition.

PROPOSITION 2.5.5. *Für $a \in M$ gilt: a prim $\Longrightarrow$ a irreduzibel.*

BEWEIS. Sei $a \in M$ prim und $b \in M$ mit $b \mid a$. Es existiert also ein $c \in M$ mit $a = cb$. Insbesondere gilt also $a \mid cb$. Da a prim ist folgt $a \mid b$ oder $a \mid c$. Im ersten Fall gilt per Defintion $b \sim a$. Im zweiten Fall ist $ac' = c$ für ein $c' \in M$ und damit gilt mit der Kürzungsregel

$$bc'a = a \Leftrightarrow b \in M^* \Leftrightarrow b \sim 1 \quad .$$

Da a per Definition auch keine Einheit ist, ist a irreduzibel. □

DEFINITION 2.5.6. Gilt in einem Monoid M auch die Umkehrung von Proposition 5.4.5, dann sagen wir dass M die *Primbedingung* erfüllt.

DEFINITION 2.5.7.
- Ein Element $a \in M$ hat eine *Faktorisierung in irreduzible Elemente* genau dann wenn $a = p_1 \cdots p_s$ mit $p_1, \ldots, p_s$ irreduzibel in M.
- Eine solche Faktorisierung heißt *eindeutig*, falls $p_1, \ldots, p_s$ bis auf Permutation und Übergang zu assoziierten Elementen eindeutig bestimmt sind.
- M heißt *faktoriell* $\Longleftrightarrow$ jedes Element aus $M \setminus M^*$ hat eine eindeutige Faktorisierung in irreduzible Elemente.

Wie der Fundamentalsatz der Arithmetik besagt, ist $\mathbb{Z} \setminus \{0\}$ ein faktorielles Monoid.

DEFINITION 2.5.8. Das Monoid M genügt der *Teilerkettenbedingung*, genau dann wenn es keine unendliche Kette $\ldots \mid a_n \mid a_{n-1} \mid \ldots \mid a_1$ von paarweise nicht-assoziierten Elementen $a_i \in M$ gibt.

LEMMA 2.5.9. *Jedes faktorielle Monoid erfüllt die Teilerkettenbedingung.*

BEWEIS. Sei $a \in M$ beliebig. Falls $a \in M^*$ ist, ist jeder Teiler von a eine Einheit. Insbesondere besitzt a keinen nicht-assoziierten Teiler.
Sei also $a \in M \setminus M^*$. Dann haben wir die eindeutige Faktorisierung $a = p_1 \cdots p_r$ in irreduzible Elemente. Gilt nun $b \mid a$, dann folgt aus der eindeutigen Faktorisierung in irreduzible Elemente, dass b assoziiert ist zu $\prod_{i \in I} p_i$ für eine Teilmenge $I \subseteq \{1, \ldots, r\}$. Offensichtlich gilt $b \sim a$ genau dann wenn

$I = \{1, \dots, r\}$ gilt. Per Induktion folgt, dass jede Teilerkette von a nach spätestens r Schritten abbricht. Daraus folgt die Teilerettenbedingung. □

LEMMA 2.5.10. *Falls M die Teilerkettenbedingung erfüllt, dann hat jedes $a \in M \setminus M^*$ eine Faktorisierung in irreduzible Elemente.*

Diese Faktorisierung muss im Allgemeinen nicht eindeutig sein.

BEWEIS. Angenommen $a_i \in M \setminus M^*$ hat keine Faktorisierung in irreduzible Elemente. Es folgt, dass a_i nicht irreduzibel ist, da sonst $a_i = a_i$ eine Faktorisierung in irreduzible Elemente wäre. Da a_i nicht irreduzibel ist, existiert ein $b \in M \setminus M^*$ mit $b \mid a_i$ und b ist nicht assoziiert zu a_i. Damit gilt weiter $a_i = bc$ für ein $c \in M \setminus M^*$, das nicht assoziiert zu a_i ist. Hätten sowohl b als auch c eine Faktorisierung in irreduzible Elemente, so wäre deren Produkt eine Faktorisierung von a_i in irreduzible Elemente. Dies wurde ausgeschlossen.
Wir halten fest, dass a_i einen Teiler $a_{i+1} \in M \setminus M^*$ besitzt (nämlich b oder c), der nicht assoziiert zu a_i ist und keine Faktorisierung in irreduzible Elemente besitzt.
Für ein beliebiges Element $a = a_1 \in M \setminus M^*$ ohne Faktorisierung in irreduzible Elemente erhalten wir also eine unendliche Kette

$$\cdots \mid a_i \mid a_{i-1} \mid \cdots \mid a_2 \mid a_1.$$

Dies ist ein Widerspruch! Damit kann ein solches Element a nicht existieren und folglich hat jedes Element in $M \setminus M^*$ eine Faktorisierung in irreduzible Elemente. □

LEMMA 2.5.11. *Falls $a = p_1 \dots p_r = q_1 \dots q_s$ mit $p_1, \dots, p_r$ prim und $q_1, \dots, q_s$ irreduzibel, dann gilt $r = s$ und $\exists \pi \in S_r$ mit $p_i \sim q_{\pi(i)}$ $\forall i = 1, \dots, r$.*

BEWEIS. Per Induktion über r.
Induktionsanfang ($r = 1$): Es gilt $p_1 = q_1 \dots q_s$. Da p_1 prim ist, muss p_1 Teiler von einem q_i sein. Nach Umordnung darf man $p_1 \mid q_1$ annehmen. Weil q_1 irreduzibel ist und p_1 keine Einheit ist, gilt $p_1 \sim q_1$ also $p_1 = uq_1$ für eine Einheit $u \in M^*$. Nach der Kürzungsregel gilt dann $u = q_2 \dots q_s$. Damit ist $s = 1$, da sonst q_2 eine Einheit wäre, im Widerspruch zur Irreduzibilität.

Induktionsanfang für Puristen ($r = 0$): Das leere Produkt ist als 1 definiert, also hat man $1 = q_1 \dots q_s$. Das kann aber auch nur für $s = 0$ gelten, da sonst q_1 eine Einheit wäre im Widerspruch zu q_1 irreduzibel.

Induktionsschritt: Es sei also $r \geq 2$ und $p_1 \mid q_1 \dots q_s$. Weil p_1 prim ist, muss p_1 eines der q_i teilen. Wieder nach geeigneter Permutation dürfen wir $p_1 \mid q_1$ annehmen. Weil q_1 irreduzibel ist, folgt $p_1 \sim q_1$, d.h. $\exists u \in M^*$ mit $p_1 = uq_1$.

Somit gilt

$$uq_1p_2 \dots p_r = q_1 \dots q_s.$$

Es ist $up_2 \sim p_2$ und damit ist auch up_2 prim. Mit der Kürzungsregel folgt

$$(up_2)p_3 \dots p_r = q_2 \dots q_s.$$

Per Induktion folgt nun die Behauptung. □

THEOREM 2.5.12. *Der Modul M ist genau dann faktoriell wenn er der Prim- und der Teilerkettenbedingung genügt.*

BEWEIS. Wir müssen die beiden Implikationen beweisen.

$\Longrightarrow$ Sei also M faktoriell.

Zur Teilerkettenbedingung: folgt aus Lemma 2.5.9.

Zur Primbedingung: Sei $a \in M$ irreduzibel. Wir müssen zeigen, dass a prim ist. Seien dazu $b, c \in M$ mit $a \mid bc$. Weiter seien $b = p_1 \cdots p_r$ und $c = p_{r+1} \cdots p_s$ die eindeutigen Faktorisierungen von b und c in irreduzible Elemente. Es gilt $ad = bc = p_1 \cdots p_s$ für ein gewisses $d \in M$. Da M faktoriell ist, muss a in der Faktorisierung von bc vorkommen; d.h. es ist $a \sim p_i$ für ein $i \in \{1, \dots, s\}$. Damit gilt $a \mid b$ (falls $i \leq r$) oder $a \mid c$ (falls $i > r$). Damit ist a prim, und es folgt die Primbedingung.

$\Longleftarrow$ Die Existenz einer Faktorisierung in irreduzible Elemente folgt direkt aus Lemma 2.5.10, und aus der Primbedingung und Lemma 2.5.11 erhalten wir die Eindeutigkeit.

□

BEMERKUNG 2.5.13. Die Teilbarkeit „|“ definiert auf $M/\sim$ eine partielle Ordnung. Beachte, dass der Raum $M/\sim$ nichts anderes ist als der Raum M/M^*. Zur Erinnerung: Eine Ordnung heißt *partiell* genau dann wenn sie $\underbrace{\text{reflexiv}}_{a|a}$, $\underbrace{\text{transitiv}}_{a|b,b|c \Rightarrow a|c}$ und $\underbrace{\text{antisymmetrisch}}_{a|b,b|a \Rightarrow a=b}$ ist.

DEFINITION 2.5.14. Für $a, b \in M$ definieren wir

(a) Falls es bezüglich “ | “ ein größtes Element unter den gemeinsamen Teilern von a und b gibt, dann nennen wir es *größten gemeinsamen Teiler* von a und b und schreiben dafür $\mathrm{ggT}(a, b)$. D.h.: $d = \mathrm{ggT}(a, b)$ genau dann wenn
   (i) $d \mid a$ und $d \mid b$
   (ii) $c \mid a$ und $c \mid b \Longrightarrow c \mid d$

(b) Falls es bezüglich " | " ein kleinstes Element unter den gemeinsamen Vielfachen von a und b gibt, dann nennen wir es *kleinstes gemeinsames Vielfaches* von a und b und schreiben dafür $\mathrm{kgV}(a,b)$. D.h.: $d = \mathrm{kgV}(a,b)$ genau dann wenn
   (i) $a \mid d$ und $b \mid d$
   (ii) $a \mid c$ und $b \mid c \Longrightarrow d \mid c$

Falls ein ggT oder kgV existiert, ist es nur eindeutig in $M/\sim$ - also nur eindeutig bis auf Multiplikation mit Einheiten.

In einem allgemeinen Monoid muss weder ein ggT noch ein kgV zu zwei gegebenen Elementen aus diesem Monoid existieren. Allerdings gilt die folgende Proposition, die in den Übungen bewiesen wird.

PROPOSITION 2.5.15. *In einem faktoriellen Monoid M existieren zu je zwei Elemente $a, b \in M$ sowohl ein* $\mathrm{ggT}(a,b)$ *als auch ein* $\mathrm{kgV}(a,b)$.

2.6. Hauptideale

In diesem Abschnitt ist R ein kommutativer Ring. Wir werden Erzeugendensysteme von Idealen definieren. Besonders einfach sind Ideale, die nur von einem Element erzeugt sind. Sie heißen Hauptideale. Wir werden Teilbarkeitseigenschaften übersetzen in entsprechende Eigenschaften der Hauptideale.

PROPOSITION 2.6.1. *Sei S eine beliebige nicht leere Teilmenge von R. Mit $\langle S\rangle$ bezeichnen wir das kleinste Ideal von R welches S enthält. Es gilt*

$$\langle S\rangle = \{a_1 g_1 + \cdots + a_s g_s | s \in \mathbb{N}, a_i \in R, g_i \in S\} \quad .$$

BEWEIS. Die Existenz von $\langle S\rangle$ beweisen wir puristisch durch die offensichtliche Gleichung $\langle S\rangle = \cap J$, wobei dieser Schnitt über alle Ideale $J \lhd R$ läuft mit $S \subseteq J$. Nun wollen wir die explizite Form von $\langle S\rangle$ beweisen.
Sei J ein Ideal in R mit $S \subseteq J$. Aufgrund der Idealeigenschaft von J muss $ag \in J$ gelten, für alle $a \in R$ und $g \in S$. Weiter ist J eine additive Gruppe und enthält daher auch alle Elemente der Form $a_1 g_r + \cdots + a_r g_r$, $s \in \mathbb{N}$, $a_r \in R$ und $g_r \in S$. Es genügt also einzusehen, dass die rechte Seite in der Behauptung - nennen wir diese I - ein Ideal ist.
Die Menge I ist nach Konstruktion eine additive Gruppe (beachte $-1 \in R$). Die Idealeigenschaft folgt aus $a(a_1 g_1 + \cdots + a_s g_s) = (aa_1)g_1 + \cdots + (aa_s)g_s \in I$, für alle $a, a_i \in R$ und $g_i \in S$. □

DEFINITION 2.6.2. Gilt $\langle S\rangle = I$, dann heißt S *Erzeugendensystem* von I. Wenn $S = \{g_1, \ldots, g_s\}$ endlich ist, dann heißen die Elemente $g_1, \ldots, g_r$ *Erzeugende* des Ideals I. In diesem Fall gilt $I = Rg_1 + \cdots + Rg_s$.

DEFINITION 2.6.3. (a) $I \triangleleft R$ *Hauptideal* $:\Longleftrightarrow \exists a \in R$, mit $I = \langle a \rangle$.

(b) R heißt *Hauptidealbereich* (HIB) $:\Longleftrightarrow$ jedes Ideal ist Hauptideal und R ist ein Integritätsbereich.

BEISPIEL 2.6.4. $\mathbb{Z}$ ist ein Hauptidealbereich, da alle additiven Untergruppen die Form $n\mathbb{Z}$ haben (siehe Proposition 1.1.25 (a)).

LEMMA 2.6.5. *Seien $g, g' \in R$. Dann gilt:*

(a) $\langle g \rangle \subseteq \langle g' \rangle \Longleftrightarrow g' \mid g$

(b) *Falls R ein Integritätsbereich ist, dann gilt auch:* $\langle g \rangle = \langle g' \rangle \Longleftrightarrow g \in R^* g' \Longleftrightarrow g \sim g'$.

BEWEIS. Seien also $g, g' \in R$.

Zu (a): $\langle g \rangle \subseteq \langle g' \rangle \Longleftrightarrow g \in \langle g' \rangle \Longleftrightarrow \exists a \in R$, mit $g = ag' \Longleftrightarrow g' \mid g$.

Zu (b): Wenn $g = 0$ ist, ist offensichtlich auch $g' = 0$. Anderenfalls rechnen wir in $(R \setminus \{0\}, \cdot)$, also einem Monoid, das die Kürzungsregel erfüllt. Mit (a) und den Ergebnissen aus Abschnitt 2.5 folgt die Behauptung.

□

NOTATION 2.6.6. Ab jetzt ist R ein Integritätsbereich. Wir übertragen alle Bezeichnungen aus Abschnitt 2.5 auf das Monoid $M := R \setminus \{0\}$. Wir haben den Raum ${}^{M}/_{\sim}$ der Äquivalenzklassen von M modulo Assoziiertheit betrachtet. Definieren wir $\langle g_1 \rangle \cdot \langle g_2 \rangle = \langle g_1 g_2 \rangle$ so ist die Menge der Hauptideale verschieden von $\{0\}$ in R ein Monoid. Dieses ist nach Lemma 2.6.5 isomorph zu ${}^{M}/_{\sim}$.

Für alle $a \in R$ definieren wir, um den Sonderfall der Null besser einzubinden, $\mathrm{ggT}(a, 0) = \mathrm{ggT}(0, a) = a$ (wie immer bis auf Multiplikation mit Einheiten bestimmt) und $\mathrm{kgV}(a, 0) = \mathrm{kgV}(0, a) = 0$. Dies ist kompatibel mit der Definition von ggT und kgV aus 2.5.14.

Wir setzen weiter fest, dass 0 weder prim noch irreduzibel ist.

PROPOSITION 2.6.7. *Sei R ein Hauptidealbereich, $a, b \in R$. Dann gilt:*

(a) $\mathrm{ggT}(a, b)$ *existiert und* $\langle a, b \rangle = \langle a \rangle + \langle b \rangle = \langle \mathrm{ggT}(a, b) \rangle$.

(b) $\mathrm{kgV}(a, b)$ *existiert und* $\langle \mathrm{kgV}(a, b) \rangle = \langle a \rangle \cap \langle b \rangle$.

BEWEIS. Seien a, b Elemente des Hauptidealbereichs R.

Zu (a): Da R Hauptidealbereich, existiert ein $d \in R$, mit $\langle d \rangle = \langle a, b \rangle \Longrightarrow d \mid a$ und $d \mid b$. Falls es ein $c \in R$ gibt mit $c \mid a$ und $c \mid b$, dann folgt $\langle a, b \rangle = \langle d \rangle \subseteq \langle c \rangle$. Mit Lemma 2.6.5 erhalten wir $c \mid d$. Nach 2.6.6 gilt somit $\mathrm{ggT}(a, b) = d$ bis auf Multiplikation mit Einheiten.

Zu (b): Analog setzen wir $\langle d\rangle = \langle a\rangle \cap \langle b\rangle$. Dann haben wir $a \mid d$ und $b \mid d$. Gilt für ein $c \in R$ ebenfalls $a \mid c$ und $b \mid c$, so ist $c \in \langle d\rangle$. Also gilt $d \mid c$ und $\mathrm{kgV}(a,b) = d$ bis auf Multiplikation mit Einheiten.

□

BEMERKUNG 2.6.8. Insbesondere folgt für $a, b \in R$, dass es Elemente $x, y \in R$ gibt, mit $ax + by = \mathrm{ggT}(a,b)$. Diese Aussage ist als *Lemma von Bezout* bekannt.

PROPOSITION 2.6.9. *Sei R ein Integritätsbereich, $g \in R\setminus\{0\}$, $I = \langle g\rangle$. Dann gilt:*

$$I \text{ Primideal} \iff g \text{ prim}\ .$$

BEWEIS. Es gilt $I = R \iff g \in R^*$. Wir dürfen uns also auf den Fall $g \notin R^*$ beschränken.

$\Longrightarrow$ Sei I ein Primideal. Seien $a, b \in R$ mit $g \mid ab$. Dann folgt $ab \in I = \langle g\rangle \overset{I \text{ Primideal}}{\Longrightarrow} a \in I$ oder $b \in I \Longrightarrow g \mid a$ oder $g \mid b$. Somit ist g prim.

$\Longleftarrow$ Es sei g prim. Falls $ab \in I$ für $a, b \in R$, dann folgt $g \mid ab \overset{g \text{ prim}}{\Longrightarrow} g \mid a$ oder $g \mid b \Longrightarrow a \in I = \langle g\rangle$ oder $b \in I$. Somit ist I ein Primideal.

□

PROPOSITION 2.6.10. *Sei R ein Hauptidealbereich, $g \in R \setminus \{0\}$, $I = \langle g\rangle$. Dann gilt:*

$$I \text{ Maximalideal} \iff g \text{ irreduzibel}\ .$$

Hier ist Vorsicht geboten, da die Aussage – anders als Proposition 2.6.9 – nur gilt wenn R ein HIB ist.

BEWEIS. Wie eben dürfen wir annehmen, dass $a \notin R^*$ gilt.

$\Longrightarrow$ Sei I ein Maximalideal. Sei $a \in R$ mit $a \mid g$. Dann folgt $I = \langle g\rangle \subseteq \langle a\rangle \overset{I \text{ Maximalideal}}{\Longrightarrow} \langle a\rangle = I$ oder $\langle a\rangle = R = \langle 1\rangle \Longrightarrow a \sim g$ oder $a \sim 1$. Somit ist g irreduzibel.

$\Longleftarrow$ Es sei g irreduzibel und es sei J ein Ideal in R mit $\langle g\rangle \subsetneq J$. Wähle ein $b \in J \setminus \langle g\rangle$. Das heißt, $g \nmid b$. Insbesondere kann also g nicht assoziiert zu $\mathrm{ggT}(g,b)$ sein. Damit ist $\mathrm{ggT}(g,b) \sim 1$. Daraus folgt $R = \langle 1\rangle = \langle a, b\rangle \subseteq J \Longrightarrow R = J$. Damit ist I ein Maximalideal.

□

KOROLLAR 2.6.11. *In einem Hauptidealbereich R gilt:*

(a) $\{0\} \neq I$ *ist Primideal* $\iff \{0\} \neq I$ *ist Maximalideal.*

(b) a *ist prim* $\iff a$ *ist irreduzibel.*

BEWEIS. $\{0\} \neq \langle a \rangle$ Maximalideal $\overset{2.6.10}{\iff}$ a irreduzibel $\overset{2.5.5}{\iff}$ a prim $\overset{2.6.9}{\iff}$ $\{0\} \neq \langle a \rangle$ Primideal $\overset{2.2.12}{\iff}$ $\{0\} \neq \langle a \rangle$ Maximalideal $\iff$ a irreduzibel. □

BEISPIEL 2.6.12. $\mathbb{Z}$ hat die Ideale $n\mathbb{Z}$, $n \geq 0$. Diese sind nach Lemma 2.6.5 alle verschieden und es gilt: $I \lhd \mathbb{Z}$ Maximalideal $\iff I = p\mathbb{Z}$, p Primzahl.

SATZ 2.6.13 (Chinesischer Restsatz für Hauptidealbereiche). *Sei R ein Hauptidealbereich und seien $g_1, \ldots, g_r$ paarweise teilerfremde Elemente in $R \setminus \{0\}$. Dann gilt*

$$R/\langle g_1 \cdots g_r \rangle \xrightarrow{\sim} R/\langle g_1 \rangle \times \cdots \times R/\langle g_r \rangle.$$

BEWEIS. Für alle $k \neq l$ gilt nach Propositon 2.6.7 $\langle g_k \rangle + \langle g_l \rangle = \langle g_k, g_l \rangle = \langle \mathrm{ggT}(g_k, g_l) \rangle = R$. Weiter gilt $\mathrm{kgV}(g_k, g_l) \sim g_k g_l$ (siehe Übungen) für alle $k \neq l$. Wenden wir Proposition 2.6.7 induktiv an, so erhalten wir damit $\langle g_1 \rangle \cap \cdots \cap \langle g_r \rangle = \langle g_1 \cdots g_r \rangle$. Also folgt die Behauptung aus dem chinesischen Restsatz 2.2.14. □

2.7. Faktorielle Ringe

Die wichtigste Eigenschaft des Ringes $\mathbb{Z}$ ist die Gültigkeit des Fundamentalsatzes der Arithmetik 2.5.1 (eindeutige Primfaktorisierung). Wir werden in diesem Abschnitt diejenigen Ringe studieren, die diese Eigenschaft ebenfalls haben.

DEFINITION 2.7.1. Ein Integritätsbereich R heißt *faktoriell* genau dann wenn $R \setminus \{0\}$ ein faktorielles Monoid bezüglich der Multiplikation ist.

PROPOSITION 2.7.2 (Division mit Rest). *Sei R ein kommutativer Ring, $f(x) \in R[x]$ und $g = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in R[x]$, $a_d \in R^*$. Dann existieren eindeutige Elemente $q, r \in R[x]$, mit $f = qg + r$ und* $\mathrm{grad}(r) < \mathrm{grad}(g)$.

BEWEIS. Der, aus der Schule bekannte, Algorithmus zur Polynomdivision liefert die Existenz. Wir werden hier nur die Eindeutigkeit beweisen.
Seien also q', r' weitere Elemente in $R[x]$ mit $f = q'g + r'$ und $\mathrm{grad}(r') < \mathrm{grad}(g)$. Dann gilt $(q - q')g = r' - r$. Mit der Gradformel 2.3.6 folgt nun

$$\mathrm{grad}((q - q')g) = \mathrm{grad}(q - q') + \mathrm{grad}(g) = \mathrm{grad}(r' - r)$$

$$\leq \max\{\mathrm{grad}(r), \mathrm{grad}(r')\} < \mathrm{grad}(g).$$

Dies ist nur möglich für $\mathrm{grad}(q - q') < 0$, also für $q = q'$. Damit folgt unmittelbar auch $r = r'$, was zu zeigen war. Hier haben wir ausgenutzt, dass der höchste Koeffizient von g eine Einheit ist, also insbesondere kein Nullteiler. □

DEFINITION 2.7.3. Sei R ein Integritätsbereich. Falls eine Abbildung $d : R\setminus\{0\} \longrightarrow \mathbb{N}_0$ existiert mit der Eigenschaft:

$$\forall f, g \in R, g \neq 0 \, \exists q, r \in R \text{ mit } f = q \cdot g + r \text{ und } d(r) < d(g) \text{ oder } r = 0$$

Dann heißt R *euklidischer Ring* und d *Gradabbildung*. Das heißt, ein euklidischer Ring erlaubt die Division mit Rest.

Wir sagen auch R ist *euklidisch bezüglich* der Gradabbildung d.

BEISPIEL 2.7.4. (a) $\mathbb{Z}$ ist euklidisch bezüglich $d(m) = |m|$.

(b) Ein Körper K ist euklidisch bzgl. jeder Abbildung $d : K^* \to \mathbb{N}_0$.

(c) Für einen Körper K ist $K[x]$ euklidisch bezüglich $d(f) = \text{grad}(f)$.

(d) Der Ring $\mathbb{Z}[i] = \{a+bi | a, b \in \mathbb{Z}\}$ heißt *Ring der Gauß'schen Zahlen*. Er ist euklidisch bezüglich der Abbildung $N(a + bi) = a^2 + b^2$. Um dies zu zeigen stellen wir zunächst fest, dass $\mathbb{Z}[i]$ ein Teilring von $\mathbb{C}$ ist und dass $N(.) = |.|^2$ gilt, wobei $|.|$ den standard Betrag auf $\mathbb{C}$ beschreibt.

Seien nun $f, g \in \mathbb{Z}[i]$ beliebig mit $g \neq 0$. Dann gilt für eine Gleichung $f = qg + r$ mit $q, r \in \mathbb{Z}[i]$ gerade

$$N(r) < N(g) \Longleftrightarrow |r|^2 < |g|^2$$
$$\Longleftrightarrow |f - qg|^2 < |g|^2 \Longleftrightarrow |\frac{f}{g} - q| < 1.$$

Das Element $\frac{f}{g}$ ist ein Element aus $\mathbb{C}$. Es genügt also ein Element $q \in \mathbb{Z}[i]$ zu finden mit $|\frac{f}{g} - q| < 1$. Für dieses q und $r = f - gq \in \mathbb{Z}[i]$ folgt dann, dass wir Division mit Rest in $\mathbb{Z}[i]$ betreiben können.

Schreibe nun $\frac{f}{g} = x_1 + ix_2$ mit $x_1, x_2 \in \mathbb{R}$. Wähle $a, b \in \mathbb{Z}$ mit $|x_1 - a| \leq \frac{1}{2}$ und $|x_2 - b| \leq \frac{1}{2}$. Dann gilt für $q = a + bi \in \mathbb{Z}$,

$$|\frac{f}{g} - q| = \sqrt{(x_1 - a)^2 + (x_2 - b)^2} \leq \frac{1}{2}\sqrt{2} < 1.$$

Also sind die Gauß'schen Zahlen wie behauptet ein euklidischer Ring bzüglich $N(.)$.

THEOREM 2.7.5. *Jeder euklidische Ring R ist ein Hauptidealbereich.*

BEWEIS. Sei $\{0\} \neq I \lhd R$ beliebig und $a \in I \setminus \{0\}$ ein Element minimalen Grades. Wähle ein Element b aus I. Da R euklidisch ist, existieren $q, r \in R$ mit $b = qa+r$. Aufgrund der Idealeigenschaft von I muss $r \in I$ gelten, somit ist wegen der Minimalität von a der Fall $d(r) < d(a)$ nicht möglich. Es folgt $r = 0$ und $b \in \langle a \rangle = I$. □

THEOREM 2.7.6. *Jeder Hauptidealbereich ist faktoriell.*

BEWEIS. Sei R ein Hauptidealbereich. Wir werden zeigen, dass das Monoid $R \setminus \{0\}$ die Primbedingung und die Teilerkettenbedingung erfüllt. Dann können wir mit Theorem 2.5.12 schließen, dass R faktoriell ist.
Zur Primbedingung: Wurde bereits in Korollar 2.6.11 gezeigt.
Zur Teilerkettenbedingung: Sei also $\cdots \mid a_n \mid a_{n-1} \mid \cdots \mid a_1$ eine unendliche Teilerkette von nicht assoziierten Elementen in $R\setminus\{0\}$. $\overset{2.6.5}{\Longrightarrow} \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \langle a_3\rangle \subsetneq \ldots$ ist eine echte aufsteigende Kette von Idealen. In den übungen wurde gezeigt, dass $I := \bigcup_{j\in\mathbb{N}} \langle a_j\rangle$ ein Ideal ist. Weil R ein Hauptidealbereich ist, gibt es ein $a \in R\setminus\{0\}$ so, dass $\langle a\rangle = I$. Aufgrund der Definition von I existiert ein $j \in \mathbb{N}$ mit $a \in \langle a_j\rangle$. Daraus folgt

$$\langle a\rangle = \langle a_j\rangle = \langle a_{j+1}\rangle = \langle a_{j+2}\rangle = \ldots.$$

Dies ist allerdings ein Widerspruch dazu, dass die Elemente $\{a_i\}_{i\in\mathbb{N}}$ paarweise nicht-assoziiert sind. Damit folgt die Behauptung. □

Wir erhalten sofort:

KOROLLAR 2.7.7. *Jeder euklidische Ring ist faktoriell.*

BEISPIEL 2.7.8. $\mathbb{Z}$ ist euklidisch $\overset{2.7.7}{\Longrightarrow}$ $\mathbb{Z}$ ist faktoriell $\overset{\text{Def.}}{\Longrightarrow}$ Es gilt der Fundamentalsatz der Arithmetik 2.5.1.

BEMERKUNG 2.7.9. Die Inklusionen

$$\{\text{euklidische Ringe}\} \subset \{\text{Hauptidealbereiche}\} \subset \{\text{faktorielle Ringe}\}$$

sind strikt. Dass dies für die zweite Inklusion gilt, wird in den Übungen gezeigt. Die Aussage über die erste Inklusion ist viel schwieriger. Ein Beispiel für einen Ring der ein Hauptidealbereich aber kein euklidischer Ring bezüglich irgendeiner Gradabbildung d ist, ist der Ring

$$\begin{aligned} R := \mathbb{Z}\left[\tfrac{1+\sqrt{-19}}{2}\right] &= \left\{a + b\tfrac{1+\sqrt{-19}}{2} \middle| a, b \in \mathbb{Z}\right\} \\ &= \left\{a + \tfrac{b}{2} + (\tfrac{b}{2}\sqrt{-19}) \middle| a, b \in \mathbb{Z}\right\}. \end{aligned}$$

Dass dies ein Hauptidealbereich ist werden wir nicht zeigen können und verweisen dafür auf [**St**], Seite 17.
Wir werden im Folgenden zeigen, dass R nicht euklidisch ist bezüglich irgendeiner Gradabbildung $d : R \setminus \{0\} \to \mathbb{N}_0$.
Sei zunächst $N(.) = |.|$, mit dem standard Betrag $|.|$ auf $\mathbb{C}$ wie in Beispiel 5.6.4 (d). Da dieser Betrag multiplikativ ist, folgt für ein Element $0 \neq \alpha = a + \frac{b}{2} + (\frac{b}{2}\sqrt{-19}) \in R$:

$$\alpha \in R^* \Longleftrightarrow N(\alpha) = 1 \Longleftrightarrow \left(a + \frac{b}{2}\right)^2 + 19\left(\frac{b}{2}\right)^2 = 1. \tag{3}$$

Wäre α wie oben also eine Einheit, mit $b \neq 0$, so wäre $N(\alpha) \geq 19\left(\frac{b}{2}\right)^2 \geq \frac{19}{4} > 1$. Dies ist ausgeschlossen und somit folgt für eine Einheit α, dass $b = 0$ gilt. Wieder mit (3), erhalten wir sofort $R^* = \{\pm 1\}$.
Angenommen R ist euklidisch bezüglich einer Gradabbildung $d : R \setminus \{0\} \to \mathbb{N}_0$. Wähle dann ein Element $0 \neq x \in R \setminus R^*$ mit minimalem Grad $d(x)$ unter allen nicht-Einheiten in R. Für ein beliebiges $\beta \in R$ existieren also Elemente $q, r \in R$ mit $\beta = qx + r$ und $r = 0$ oder $d(r) < d(x)$. Letzteres kann nur erfüllt sein wenn gilt $r \in R^* = \{\pm 1\}$.
Dies bedeutet gerade, dass der Faktorring $R/\langle x\rangle$ aus maximal drei Elementen besteht. Weiter ist x keine Einheit und somit ist $\langle x\rangle \neq R$, was gleichbedeutend damit ist, dass $R/\langle x\rangle$ mindestens aus zwei Elementen besteht.
Da Ringe insbesondere abelsche Gruppen sind, folgt aus der Klassifikation der endlichen abelschen Gruppen (Theorem 1.1.36) gerade $R/\langle x\rangle \cong \mathbb{Z}/2\mathbb{Z}$ oder $R/\langle x\rangle \cong \mathbb{Z}/3\mathbb{Z}$.
Betrachten wir das Element $\omega = \frac{1+\sqrt{-19}}{2}$, so stellen wir fest, dass $\omega^2 - \omega + 5 = 0$ gilt. Diese Beziehung muss also auch für das Element $\omega + \langle x\rangle \in R/\langle x\rangle$ gelten. Allerdings finden wir durch Einsetzen:

- $\overline{1}^2 - \overline{1} + \overline{5} = \overline{1} \neq 0 \in \mathbb{Z}/2\mathbb{Z}$ und
- $\overline{0}^2 - \overline{0} + \overline{5} = \overline{1} \neq 0 \in \mathbb{Z}/2\mathbb{Z}$

und

- $\overline{1}^2 - \overline{1} + \overline{5} = \overline{2} \neq 0 \in \mathbb{Z}/3\mathbb{Z}$
- $\overline{2}^2 - \overline{2} + \overline{5} = \overline{1} \neq 0 \in \mathbb{Z}/3\mathbb{Z}$
- $\overline{0}^2 - \overline{0} + \overline{5} = \overline{2} \neq 0 \in \mathbb{Z}/3\mathbb{Z}$

Dies widerspricht der Beziehung $(\omega + \langle x\rangle)^2 - (\omega + \langle x\rangle) + (5 + \langle x\rangle) = 0 + \langle x\rangle \in R/\langle x\rangle$. Damit kann R nicht euklidisch bezüglich der Gradabbildung d sein. Da d beliebig gewählt war, folgt, dass R nicht euklidisch bezüglich irgendeiner Gradabbildung sein kann. Dies wollten wir beweisen.

Bemerkung 2.7.10. Ein Algorithmus ist eine Handlungsvorschrift für das Lösen eines Problems. Diese Handlungsvorschrift muss zwei Dinge erfüllen. Erstens muss sie das Problem tatsächlich lösen und zweitens muss diese Lösung in endlich vielen Schritten erreicht werden.

2.7.11 (Euklidischer Algorithmus). Für einen euklidischen Ring kann man einen ggT zweier Elemente mit dem euklidischen Algorithmus bestimmen. Sei R ein euklidischer Ring mit Gradabbildung $d : R\setminus\{0\} \longrightarrow \mathbb{N}_0$. Weiter seien $a, b \in R$ mit $b \neq 0$. Unser Ziel ist die Bestimmung von $\mathrm{ggT}(a, b)$.

- **Schritt 1:** Setze $a_1 := a$ und $a_2 := b$. Konstruiere eine Gleichung $a_1 = q_2 a_2 + a_3$ mit $q_2, a_3 \in R$ und $d(a_3) < d(a_2)$ oder $a_3 = 0$. Aufgrund der Summenregel gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_2, a_3)$.
- **Schritt 2:** Falls $a_3 = 0$, dann gilt $a_2 \mid a_1$ und damit $\mathrm{ggT}(a, b) = b$.
  Falls $a_2 \neq 0$, dann gehe zu Schritt 1 zurück mit (a_2, a_3) statt (a_1, a_2).

Wegen $d(a_2) > d(a_3) > d(a_4) > ... \geq 0$ terminiert der Algorithmus in endlich vielen Schritten. Das heißt, es gibt ein $n \in \mathbb{N}_0$ mit $a_{n+1} = 0$ und damit $\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, a_2) = \ldots = \mathrm{ggT}(a_{n-1}, a_n) = a_n$. Allerdings ist das Ergebnis wie immer nur eindeutig bis auf Multiplikation mit Einheiten!

Beispiel 2.7.12. Berechne zuerst $\mathrm{ggT}(42, 15)$ in $\mathbb{Z}$:

(a)
$$42 = 2 \cdot 15 + 12$$
$$15 = 1 \cdot 12 + 3$$
$$12 = 4 \cdot 3 + 0 \Longrightarrow \mathrm{ggT}(12, 3) = 3 \Longrightarrow \mathrm{ggT}(42, 15) = 3$$

(b)
$$42 = 3 \cdot 15 - 3$$
$$15 = (-5) \cdot (-3) + 0 \Longrightarrow \mathrm{ggT}(42, 15) = \mathrm{ggT}(15, -3) = -3$$

Als weiteres Beispiel berechnen wir $\mathrm{ggT}(x^4 - 2x^3 - 2x^2 - 2x - 3, x^4 - 3x^3 - 7x^2 + 15x + 18)$ in $\mathbb{Q}[x]$:

- $x^4 - 2x^3 - 2x^2 - 2x - 3 = 1 \cdot (x^4 - 3x^3 - 7x^2 + 15x + 18) + (x^3 + 5x^2 - 17x - 21)$
- $x^4 - 3x^3 - 7x^2 + 15x + 18 = (x - 8) \cdot (x^3 + 5x^2 - 17x - 21) + (50x^2 - 100x - 150)$
- $x^3 + 5x^2 - 17x - 21 = (\frac{1}{50}x + \frac{7}{50}) \cdot (50x^2 - 100x - 150) + 0 \Longrightarrow \mathrm{ggT}(x^4 - 2x^3 - 2x^2 - 2x - 3, x^4 - 3x^3 - 7x^2 + 15x + 18) = 50(x^2 - 2x - 3)$

Bemerkung 2.7.13. Der euklidische Algorithmus liefert uns stets *einen* ggT von zwei Elementen a, b. Wir werden im Fall der Ringe $\mathbb{Z}$ und $K[x]$, für einen Körper K, einen expliziten Repräsentanten auswählen und von *dem* ggT sprechen. Für $\mathbb{Z}$ wählen wir den positiven Repräsentanten und für $K[x]$ den normierten Repräsentanten als *den* ggT zweier Elemente. Dieser ist nun natürlich eindeutig bestimmt.
Haben wir einen $\mathrm{ggT}(a, b)$ für a, b in einem euklidischen Ring R mit dem Euklidischen Algorithmus berechnet, so können wir die Schritte in umgekehrter Reihenfolge betrachten. Dies führt zu einer Lösung der Gleichung $xa + yb = \mathrm{ggT}(a, b)$ für Elemente $x, y \in R$.

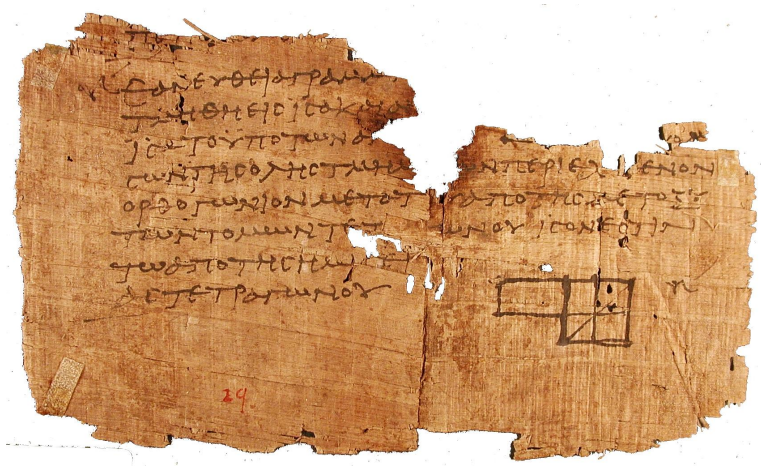


ABBILDUNG 2.2. Das Buch *die Elemente* von Euklid aus dem 3. Jahrhundert v.C. ist ohne Zweifel eine der bedeutendsten Schriften der Weltliteratur. Bis ins 19. Jahrhundert war es nach der Bibel das meist verbreitete Buch weltweit. Noch im 20. Jahrhundert war es ein gängiges Schulbuch für Mathematik. Auch heute noch (wie hoffentlich in diesem Skript) wird Euklids formale Struktur bestehend aus Axiomen, Definitionen und Postulaten, in mathematischen Texten verwendet.

2.8. Polynome über faktoriellen Ringen

Für einen faktoriellen Ring R werden wir zeigen, dass auch der Polynomring $R[x]$ faktoriell ist. Das bedeutet, dass jedes Polynom $f \in R[x] \setminus \{R^*, 0\}$ eine eindeutige Faktorisierung in irreduzible Elemente besitzt.

Wie immer nennen wir zwei Elemente a, b aus einem faktoriellen Ring assoziiert, genau dann wenn es eine Einheit $u \in R^*$ gibt mit $a \cdot u = b$. Wir schreiben hierfür $a \sim b$.

Sei R stets ein faktorieller Ring mit Quotientenkörper Q. Mit $\mathbb{P}$ bezeichnen wir ein Repräsentantensystem der irreduziblen Elemente in R. D.h.: Aus jeder Äquivalenzklasse modulo $\sim$ eines irreduziblen Elementes in R wählen wir genau eines als Element in $\mathbb{P}$ aus.

SATZ 2.8.1. *Sei $\alpha \in Q \setminus \{0\}$. Dann gibt es für jedes $p \in \mathbb{P}$ genau ein $v_p(\alpha) \in \mathbb{Z}$ so, dass $v_p(\alpha) = 0$ bis auf endlich viele $p \in \mathbb{P}$ und*

$$\alpha = u \prod_{p \in \mathbb{P}} p^{v_p(\alpha)}$$

für ein eindeutig bestimmtes $u \in R^*$.

BEWEIS. Folgt aus der eindeutigen Primfaktorzerlegung für Zähler und Nenner von α. □

BEISPIEL 2.8.2. Für $R = \mathbb{Z}$ und $\mathbb{P} = \{\text{positive Primzahlen}\}$ ist $-\frac{60}{49} = (-1) \cdot 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^{-2}$ und $v_p(-\frac{60}{49}) = 0$ für alle $p > 7$ in $\mathbb{P}$.

DEFINITION 2.8.3. Wir setzen $v_p(0) := \infty$ für alle $p \in \mathbb{P}$ und nennen $v_p(\alpha)$ die *p-adische Bewertung* von $\alpha \in Q$. Es gilt

$$v_p(\alpha \cdot \beta) = v_p(\alpha) + v_p(\beta). \tag{4}$$

DEFINITION 2.8.4. Für ein Polynom $f(x) = \sum_{i=0}^{n} a_i x^i \in Q[x]$ setzen wir

$$v_p(f) := \min_{i=0,\dots,n} \{v_p(a_i)\}.$$

BEMERKUNG 2.8.5. Es gelten folgende Eigenschaften:

(a) $v_p(f) = \infty \iff f = 0$.
(b) $v_p(f) \geq 0 \, \forall p \in \mathbb{P} \iff f \in R[x]$.

LEMMA 2.8.6 (Gauß-Lemma). *Seien $f, g \in Q[x]$ und $p \in \mathbb{P}$. Dann gilt $v_p(f \cdot g) = v_p(f) + v_p(g)$.*

(Beachte die Analogie zur Gradformel!)

BEWEIS. Falls $f = 0$ oder $g = 0$ ist die Aussage nach (4) klar. Seien also $f, g \in Q[x] \setminus \{0\}$ beliebig.
Nehmen wir für den Moment an, dass die Aussage für Polynome in $R[x]$ gilt. Wähle dann $a, b \in Q$ mit $af, bg \in R[x]$. Da die Aussage für Elemente aus Q gilt, erhalten wir

$$\begin{aligned} v_p(a) + v_p(b) + v_p(fg) &\overset{(4)}{=} v_p((af)(bg)) \overset{\text{Annahme}}{=} v_p(af) + v_p(bg) \\ &\overset{(4)}{=} v_p(a) + v_p(b) + v_p(f) + v_p(g). \end{aligned}$$

Damit gilt auch $v_p(fg) = v_p(f) + v_p(g)$. Es genügt also die Aussage für Polynome $f, g \in R[x] \setminus \{0\}$ zu beweisen. Analog zeigt man, dass es genügt Polynome mit teilerfremden Koeffizienten zu betrachten. Dann gilt $v_p(f) = v_p(g) = 0$, denn wäre $v_p(f) > 0$, dann gilt $v_p(a_i) > 0$ für alle Koeffizienten a_i von f. Damit wäre p ein gemeinsamer Teiler der Koeffizienten von f, was ausgeschlossen wurde.
Es bleibt also $v_p(f \cdot g) = 0$ zu zeigen. Für $p \in \mathbb{P}$ haben wir einen surjektiven Ring-Homomorphismus

$$\Phi_p : R[x] \longrightarrow {}^{R}\!/_{pR}[x], \quad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \overline{a_i} x^i.$$

Nach Proposition 2.6.9 ist $pR = \langle p \rangle$ ein Primideal in R. Es folgt mit Proposition 2.2.11, dass ${}^{R}\!/_{\langle p \rangle}$ ein Integritätsbereich ist. Insbesondere ist damit

$R/\langle p\rangle[X]$ ein Integritätsbereich (siehe 2.3.4). Aus Proposition 2.2.13 folgt, dass $\ker(\Phi_p)$ ein Primideal in $R[x]$ ist. Es gilt

$$\ker(\Phi_p) = \{\sum_{i=0}^{n} a_i x^i | p \mid a_i, \forall 0 \leq i \leq n\} = pR[x] = \{h \in R[x] \big| v_p(h) > 0\}.$$

Damit gilt nun

$$v_p(f) = 0 = v_p(g) \iff f, g \notin \ker(\Phi_p) \iff f \cdot g \notin \ker(\Psi_p) \iff v_p(f \cdot g) = 0.$$

Dies war zu zeigen. □

KOROLLAR 2.8.7. *Sei $h \in R[x]$ normiert, d.h. der höchste Koeffizient von h ist gleich 1. Weiter seien $f, g \in Q[x]$ ebenfalls normiert mit $h = f \cdot g$. Dann sind f, g bereits in $R[x]$.*

BEWEIS. Da $h \in R[x]$, gilt $v_p(h) \geq 0$ nach Bemerkung 2.8.5. Weil h normiert ist und $v_p(1) = 0$ gilt, erhalten wir $v_p(h) = 0$. Mit dem Gauß-Lemma folgt

$$0 = v_p(h) = v_p(f) + v_p(g).$$

Weil f, g ebenfalls normiert sind, folgt $v_p(f) \leq 0$ und $v_p(g) \leq 0$, somit folgt mit der Beziehung von oben $v_p(f) = v_p(g) = 0$ für alle $p \in \mathbb{P}$. □

ABBILDUNG 2.3. *Carl Friedrich Gauß* (1777 - 1855) lieferte in vielen Gebieten der Mathematik und Astronomie bedeutende Arbeit. U.A. war er der erste der einen Beweis für den Fundamentalsatz der Algebra (später) fand. Auch wenn er schon zu Lebzeiten ein gefeierter Mathematiker war, wurde sein ganzes Schaffen erst 1898 mit dem Fund seines Tagebuchs deutlich.

DEFINITION 2.8.8. Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in Q[x]$. Dann definieren wir den *Inhalt* von f als

$$\mu(f) := \prod_{p \in \mathbb{P}} p^{v_p(f)}.$$

Mit dem Gauß-Lemma folgt dann:

$$\mu(f \cdot g) = \mu(f) \cdot \mu(g) \tag{5}$$

Wenn $f \in R[x]$, dann gilt per Konstruktion $\mu(f) = \mathrm{ggT}(a_0, \ldots, a_n)$.

THEOREM 2.8.9. *Falls R ein faktorieller Ring ist, dann ist auch $R[x]$ ein faktorieller Ring.*

BEWEIS. Wir wollen im Folgenden ausnutzen, dass $Q[x]$ euklidisch, also insbesondere faktoriell, ist.

Schritt 1: Sei $f \in R[x]$ vom Grad ≥ 1. Dann ist f irreduzibel in $R[x]$ genau dann, wenn f irreduzibel in $Q[x]$ ist und wenn gleichzeitig $\mu(f) = 1$ ist.

$\Longrightarrow$ Angenommen $\mu(f) \neq 1$. Dann ist insbesondere $\mu(f)$ keine Einheit in R. Mit den Distributivgesetzen gilt $f = \mu(f)f'$, für ein $f' \in R[x]$ mit $\operatorname{grad}(f') = \operatorname{grad}(f) \geq 1$. Also ist f nicht irreduzibel in $R[x]$.

Sei also f irreduzibel in $R[x]$ und $f = gh$ für $g, h \in Q[x]$. Es bleibt zu zeigen, dass g oder h in $Q[x]^* = Q \setminus \{0\}$ ist. Wir nehmen an, dass alle Koeffizienten von g und h in gekürzter Form geschrieben sind. Sei γ das kgV aller Nenner der Koeffizienten von g und sei δ das kgV aller Nenner der Koeffizienten von h. Damit gilt $g' := \gamma g \in R[x]$ und $h' := \delta h \in R[x]$ und γ sowie δ sind minimal (bzgl Teilbarkeit) mit dieser Eigenschaft. Somit ist $\operatorname{ggT}(\gamma, \mu(g')) = 1$, denn wäre $p \in \mathbb{P}$ ein gemeinsamer irreduzibler Teiler, so wäre $\frac{\gamma}{p} g \in R[x]$ im Widerspruch zur Minimalität von γ. Ebenso ist $\operatorname{ggT}(\delta, \mu(f')) = 1$.

Aus $\gamma\delta f = g'h'$ und (5) erhalten wir

$$\mu(\gamma)\mu(\delta)\mu(f) = \mu(\gamma)\mu(\delta) \sim \gamma\delta \sim \mu(g')\mu(h').$$

Beachte, dass $\mu(f) = 1$ gilt, was wir zu Beginn des Beweises gezeigt haben.

Damit gilt nun $\mu(g') \sim \delta$ und $\mu(f') \sim \gamma$. Somit gilt $h'' := {}^{h'}/_{\gamma} \in R[x]$ und $g'' := {}^{g'}/_{\delta} \in R[x]$ und $f = g''h''$. Da f irreduzibel in $R[x]$ ist muss g'' oder h'' in $R[x]^* \subseteq Q[x]^*$ gelten. Es folgt, dass f irreduzibel in $Q[x]$ ist.

$\Longleftarrow$ Umgekehrt sei f irreduzibel in $Q[x]$ und $\mu(f) = 1$. Wir nehmen an, dass $f = gh$ mit $g, h \in R[x]$. Zu zeigen ist nun, dass g oder $h \in R[x]^*$.

Da f irreduzibel in $Q[x]$ ist, gilt g oder h in $Q[x]^* \cap R[x] = R \setminus \{0\}$. Sei oBdA $g \in R \setminus \{0\}$, dann ist $g \sim \mu(g)$. Aus (5) folgt, dass $1 = \mu(f) = \mu(g)\mu(h)$. Insbesondere muss dann $g \sim \mu(g) = \mu(h) = 1$ gelten. Also ist g eine Einheit in R. Es folgt, dass f irreduzibel in $R[x]$ ist. Dies beendet den Beweis von Schritt 1.

Schritt 2: Das Monoid $R[x] \setminus \{0\}$ erfüllt die Primbedingung. (D.h. jedes irreduzible Element in $R[x]$ ist prim in $R[x]$).

Sei also $f \in R[x]$ irreduzibel in $R[x]$. Dann folgt aus Schritt 1, dass $\mu(f) = 1$ und f irreduzibel in $Q[x]$ ist. Die Gleichung $\mu(f) = 1$ zusammen mit $f \in R[x]$ impliziert $v_p(f) = 0$ für alle $p \in \mathbb{P}$. Da $Q[x]$ faktoriell ist, ist f prim in $Q[x]$. Seien also $g, h \in R[x]$ mit $f \mid g \cdot h$. Dann existiert oBdA ein $d \in Q[x]$ mit $f \cdot d = g$. Es bleibt $d \in R[x]$ zu zeigen. Dies folg mit dem Gauß-Lemma und Bemerkung 2.8.5. Denn

$$v_p(f \cdot d) = v_p(f) + v_p(d) = v_p(d) = v_p(g) \geq 0, \text{ für alle } p \in \mathbb{P}.$$

Somit ist $d \in R[x]$ und f ist prim in $R[x]$. Dies beweist Schritt 2.

Schritt 3: Das Monoid $R[x]\setminus\{0\}$ erfüllt die Teilerkettenbedingung. (D.h. es existiert keine unendliche Teilerkette $\cdots \mid f_i \mid \cdots \mid f_2 \mid f_1$ mit paarweise nicht-assoziierten Elementen $f_i \in R[x]$.)

Sei $f \in R[x]\setminus\{0\}$ beliebig. Die Gradformel 2.3.6 und die Multiplikativität von $\mu(.)$ (5) liefern sofort, dass für $g \in R[x]$ mit $g \mid f$ sowohl $\mu(g) \mid \mu(f)$ als auch $\operatorname{grad}(g) \leq \operatorname{grad}(f)$ gilt.
Sei nun $g \in R[x]$ ein Teiler von f mit $\mu(g) = \mu(f)$ und $\operatorname{grad}(g) = \operatorname{grad}(f)$. Dann existiert ein $d \in R[x]$ mit $d \cdot g = f$ und $\mu(f) = 1$ (folgt aus (5)) und $\operatorname{grad}(d) = 0$ (folgt aus Proposition 2.3.6). Damit ist $d \in R^*$ und $g \sim f$.
Sei nun $r \in \mathbb{N}$ so gewählt, dass jede Kette nicht-assoziierter Teiler von $\mu(f)$ nach spätestens r Schritten abbricht. Es ist $r < \infty$, da $\mu(f) \in R$ und R faktoriell ist. Nach unseren Vorüberlegungen bricht nun jede Teilerkette von paarweise nicht-assoziierten Elementen von f nach spätestens $r + \operatorname{grad}(f)$ Schritten ab. Also erfüllt $R[x]\setminus\{0\}$ die Teilerkettenbedingung, was zu zeigen war.

Wir haben nun gesehen, dass $R[x]\setminus\{0\}$ ein Monoid ist, welches die Teilerkettenbedingung und die Primbedingung erfüllt. Aus Theorem 2.5.12 und der Definition eines faktoriellen Ringes folgt, dass $R[x]$ faktoriell ist. □

KOROLLAR 2.8.10. *Falls K ein Körper und $n \in \mathbb{N}$ ist, dann ist der Polynomring $K[x_1, \ldots, x_n]$ in den Variablen $x_1, \ldots, x_n$ ein faktorieller Ring.*

BEWEIS. Dies folgt aus Theorem 2.8.9 per Induktion, da in den Übungen bereits gezeigt wurde dass $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$ gilt. □

Wir interessieren uns für (die Faktorisierung in) irreduzible Elemente aus $K[x]$ für einen Körper K. Es ist eine komplexe Aufgabe für ein gegebenes Polynom zu entscheiden ob es irreduzibel ist oder nicht. Das *Kriterium von Eisenstein* liefert eine Klasse von irreduziblen Polynomen und ist in der Anwendung sehr einfach.

ABBILDUNG 2.4. *Gotthold Eisenstein* (1823 - 1852) war ein deutscher Mathematiker, dem bereits im dritten Semester ein Ehrendoktortitel verliehen wurde. Er starb bereits mit 29 Jahren an Tuberkolose.

THEOREM 2.8.11 (Eisensteinsches Irreduzibilitätskriterium). *Sei R ein faktorieller Ring und $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x]$ vom Grad $n \geq 1$. Weiter sei p ein irreduzibles Element aus R mit $p \nmid a_n$, $p \mid a_i \ \forall i < n$ und $p^2 \nmid a_0$. Dann ist $f(x)$ irreduzibel in $Q[x]$.*

BEWEIS. Da $p \nmid a_n$, gilt also auch $p \nmid \mu(f) = \text{ggT}(a_0, \ldots, a_n)$. Wir benutzen nun wieder die Gleichung $f = \mu(f) \cdot f'$ für ein $f' \in R[x]$ mit $\mu(f') = 1$ und $\operatorname{grad} f' = \operatorname{grad} f$. Da Multiplikation mit $\mu(f)$ die p-adische Bewertung der Koeffizienten nicht verändert, erfüllt auch f' die Vorraussetzungen des Theorems. Wir dürfen also $\mu(f) = 1$ annehmen. (Beachte hierzu, dass Multiplikation mit einem Element aus $Q \setminus \{0\}$ nichts an der Irreduzibilität eines Polynoms in $Q[x]$ ändert.)
Demnach genügt es nach Schritt 1 im Beweis von Theorem 2.8.9 zu zeigen, dass $f(x)$ irreduzibel in $R[x]$ ist. Angenommen dies wäre nicht der Fall und $f(x)$ wäre nicht irreduzibel in $R[x]$.
Dann gilt $f(x) = g(x) \cdot h(x)$ mit Elementen $g(x), h(x) \in R[x] \setminus R^*$. Es seien

$$g(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0, \quad h(x) = c_l x^l + \ldots + c_0$$

mit $b_k \neq 0 \neq c_l$ und $k + l = n$. Es ist weiter $k, l \geq 1$, denn wäre z.B. $k = 0$ so gilt

$$1 = \mu(f) \overset{(5)}{=} \mu(g)\mu(h) \sim b_0\mu(h).$$

Das bedeutet jedoch $g = b_0 \in R^*$ im Widerspruch zur Wahl von g.
Betrachte den surjektiven Ring-Homomorphismus

$$\Phi_p : R[x] \longrightarrow {}^{R}\!/_{pR}[x], \quad \sum \alpha_k x^k \mapsto \sum \overline{\alpha_k} x^k.$$

Wie bereits gesehen ist ${}^{R}\!/_{\langle p \rangle}$ ein Integritätsbereich nach den Propositionen 2.6.9 und 2.2.11. Sei $F := \text{Quot}({}^{R}\!/_{\langle p \rangle})$ der Quotientenkörper von ${}^{R}\!/_{\langle p \rangle}$. Dieser existiert nach 2.4.8 und der Ring $F[x]$ ist euklidisch also (nach Korollar 2.7.7) auch faktoriell.
Wenden wir nun Φ_p auf die Gleichung $f = g \cdot h$ an erhalten wir

$$\overline{a_n} x^n = \Phi_p(f) = \Phi_p(g)\Phi_p(h).$$

Da x irreduzibel in $F[x]$ ist und die Faktorisierung in irreduzible Elemente aus $F[x]$ eindeutig ist, müssen $\Phi_p(g)$ und $\Phi_p(h)$ Potenzen von x sein (bis

auf Multiplikation mit Konstanten). Somit gilt

$$\Phi_p(g) = \overline{b_k}x^k, \quad \Phi_p(h) = \overline{c_l}x^l.$$

Insbesondere gilt $\overline{b_0} = 0 = \overline{c_0}$ und damit $p \mid b_0$, $p \mid c_0$. Weil $a_0 = b_0c_0$ ist, muss $p^2 \mid a_0$ gelten. Dies ist ein Widerspruch zur Annahme und damit folgt dass f irreduzibel in $R[x]$ - und somit auch in $Q[x]$ - ist. □

Beispiel 2.8.12. Sei $K := k(t)$ der Körper der rationalen Funktionen über dem Körper k, d.h. K ist der Quotientenkörper von $k[t]$. Dann ist $x^n - t$ irreduzibel in $K[x]$ für jedes $n \in \mathbb{N}$. Denn $R := k[t]$ ist faktoriell und t ist irreduzibel in R. Das Kriterium von Eisenstein liefert nun die Behauptung.

KAPITEL 3

Körper

3.1. Grundlagen

In diesem Abschnitt sei K ein Körper. Wir werden sehen, dass die Körpertheorie eng mit der Theorie des Polynomringes verbunden ist. Wir halten daher die folgenden Aussagen aus dem letzten Kapitel fest.

FAKTEN 3.1.1.
(a) $K[x]$ ist ein euklidischer Ring bezüglich dem Grad (siehe Proposition 2.7.2) und damit ist $K[x]$ ein faktorieller Ring, d.h. für jedes $f \in K[x] \setminus K$ gibt es eine Faktorisierung in irreduzible Faktoren in $K[x]$ und die Faktorisierung ist bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig.
(b) Beachte, dass $K[x]^* = K^* = K \setminus \{0\}$ (siehe Proposition 2.3.6) gilt.
(c) Das Polynom $f(x) \in K[x]$ ist irreduzibel genau dann wenn eine der folgenden (äquivalenten) Bedingungen erfüllt ist:
   (i) $\operatorname{grad}(f) \geq 1$ und falls $f = g \cdot h$ mit $g, h \in K[x]$, dann muss $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$ gelten.
   (ii) $fK[x]$ ist ein Maximalideal in $K[x]$.
   (iii) ${}^{K[x]}/_{\langle f \rangle}$ ist ein Körper.

BEWEIS. Die Äquivalenz der Aussagen haben wir in Theorem 2.6.10 und den Propositionen 2.7.5 und 2.2.11 bewiesen. □

DEFINITION 3.1.2. Sei $f \in K[x]$. Wir sagen $\alpha \in K$ ist eine Nullstelle von f genau dann wenn für den Einsetzhomomorphismus $\varphi_\alpha : K[x] \longrightarrow K$ aus 2.3.4 gilt $\varphi_\alpha(f) = 0$.
Falls alle irreduziblen Faktoren von $f \in K[x] \setminus K$ den Grad 1 haben, dann sagen wir, dass f über K *in Linearfaktoren zerfällt*. Ist dies der Fall und gilt $f(x) = a_n x^n + \cdots + a_0$ so ist

$$f(x) = a_n(x - \alpha_1)^{v_1} \cdot \ldots \cdot (x - \alpha_r)^{v_r}$$

für paarweise verschiedenen $\alpha_1, \ldots \alpha_r \in K$ und $v_1, \ldots, v_r \in \mathbb{N}$ eindeutig bestimmt. Es ist durch einsetzen klar, dass $\alpha_1, \ldots, \alpha_r$ Nullstellen von f sind. Wir nennen v_j die *Multiplizität* der Nullstelle α_j. Weiter heißt α_j *mehrfache Nullstelle* von K falls $v_j > 1$.

PROPOSITION 3.1.3. *Sei $\alpha \in K$ eine Nullstelle von $f(x) \in K[x]$. Dann existiert genau ein $g(x) \in K[x]$ mit $f(x) = (x-\alpha)g(x)$.*

BEWEIS. Polynomdivision (2.7.2) liefert eindeutige Polynome $g(x), h(x) \in K[x]$ mit $f(x) = g(x)(x-\alpha) + h(x)$ mit $\text{grad}(h) < \text{grad}(x-\alpha) = 1$. Somit ist $h(x) = h \in K$ eine Konstante. Benutzen wir wieder den Einsetzhomomorphismus φ_α so erhalten wir

$$0 = \varphi_\alpha(f(x)) = \underbrace{\varphi_\alpha(x-\alpha)}_{=0}\varphi_\alpha(g(x)) + \varphi_\alpha(h) = h.$$

Dies beweist die Aussage. □

Dieses Verfahren nennen wir *Abspalten der Nullstelle $\alpha \in K$*. Im Folgenden werden wir Elemente aus K direkt in ein Polynom $f \in K[x]$ einsetzen ohne jedesmal formal den Einsetzhomomorphismus zu erwähnen. Wir schreiben dann kurz für $\beta \in K$ beliebig $f(\beta) = \varphi_\beta(f(x))$.

SATZ 3.1.4. *Sei $f(x) \in K[x]\setminus\{0\}$ vom Grad m. Dann hat $f(x)$ höchstens m verschiedene Nullstellen in K.*

BEWEIS. Wir beweisen dies mit vollständiger Induktion nach m, wobei für den Induktionsanfang $m = 0$ nichts zu zeigen ist.
Sei also $m > 0$. Da die Aussage trivialerweise erfüllt ist wenn f überhaupt keine Nullstelle in K hat, nehmen wir an dass f eine Nullstelle $\alpha \in K$ besitzt. Mit Proposition 3.1.3 können wir α abspalten und erhalten $f = (x-\alpha)g(x)$ für ein $g \in K[x]$ mit $\text{grad}(g) = m-1$. Nach Induktion hat $g(x)$ höchstens $m-1$ Nullstellen in K. Aus der Nullteilerfreiheit von K folgt, dass f höchstens m Nullstellen in K hat. □

KONSTRUKTION 3.1.5. Wir wollen einen Ring-Homomorphismus zwischen $\varphi : \mathbb{Z} \longrightarrow K$, für einen Körper K konstruieren.
Wir bezeichnen das Einselement in K mit $\mathbb{1}$. Da ein Ring-Homomorphismus die Einselemente aufeinander abbilden muss, gilt $\varphi(1) = \mathbb{1}$. Da φ ein Ring-Homomorphismus sein soll muss für $n \in \mathbb{N}$

$$\varphi(n) = \varphi(\underbrace{1+\ldots+1}_{n-mal}) = \underbrace{\varphi(1)+\ldots+\varphi(1)}_{n-mal} = \underbrace{\mathbb{1}+\ldots+\mathbb{1}}_{n-mal}$$

gelten. Weiter muss $\varphi(-n) = -\mathbb{1}\varphi(n)$ erfüllt sein. Damit ist φ eindeutig bestimmt und per Konstruktion auch ein Homomorphismus.
Da K insbesondere ein Integritätsbereich ist, muss $\ker(\varphi)$ ein Primideal in $\mathbb{Z}$ sein (siehe Proposition 2.2.13). Weiter ist $\mathbb{Z}$ ein Hauptidealbereich und somit ist $\ker(\varphi) = \{0\}$ oder $\ker(\varphi) = p\mathbb{Z}$ für eine positive Primzahl $p \in \mathbb{Z}$. Dies folgt aus Proposition 2.6.9.

Wir halten fest, dass es für jeden Körper K einen eindeutigen Ring-Homomorphismus $\varphi : \mathbb{Z} \longrightarrow K$ gibt. Der Kern von φ ist gleich $p\mathbb{Z}$ für ein eindeutiges $p \in \{0, \text{ positive Primzahlen}\}$.

DEFINITION 3.1.6. Die Zahl p aus 3.1.5 heißt *Charakteristik* von K und wird mit $\text{char}(K)$ bezeichnet.

Beispiele: Für $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ist φ die übliche Inklusion von $\mathbb{Z}$ in K. Also ist φ injektiv und es gilt $\text{char}(K) = 0$.
Wenn p eine Primzahl ist, dann ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper der Charakteristik p. Als φ hat man die Reduktionsabbildung $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ modulo p.

In jedem Körper können wir das Einselement mit $\varphi(1)$ identifizieren. Wir bezeichnen damit im Folgenden in jedem Körper das Einselement mit 1.
Wie immer ist ein Teilkörper $F \subseteq K$ eine Teilmenge, die bezüglich der Verknüpfungen "$+, \cdot$" in K wieder ein Körper ist. Ein *Körper-Homomorphismus* (bzw *Körper-Isomorphismus*) ist definiert als ein Ring-Homomorphismus (bzw Ring-Isomorphismus) zwischen zwei Körpern.

DEFINITION/SATZ 3.1.7. *Der* Primkörper *von K ist der (bezüglich der Inklusion) kleinste Teilkörper von K. Dieser existiert zu jedem Körper K.*

BEWEIS. Da der Duchschnitt von einer Familie von Teilkörpern von K offensichtlich wieder ein Teilkörper von K ist, setzen wir

$$P := \bigcap_{F \text{ Teilkörper von } K} F$$

als Primkörper von K. □

PROPOSITION 3.1.8. *Sei K ein Körper und $p \in \mathbb{Z}$ eine positive Primzahl. Dann gilt*

(a) $\text{char}(K) = p \iff$ *Primkörper* $P \cong \mathbb{Z}/p\mathbb{Z}$.
(b) $\text{char}(K) = 0 \iff$ *Primkörper* $P \cong \mathbb{Q}$.

BEWEIS. Mit φ bezeichnen wir die eindeutige Abbildung aus 3.1.5

Zu (a): $\Longrightarrow$ Sei $p = \text{char}(K) > 0$. Weil das Bild von φ als Ring von $1 \in K$ erzeugt wird (sogar als additive Gruppe), muss $\varphi(\mathbb{Z}) \subseteq P$ gelten. Nach dem Isomorphiesatz 2.2.6 gilt

$$\varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker(\varphi) \overset{\text{Def.}}{=} \mathbb{Z}/p\mathbb{Z}.$$

Somit ist $\varphi(\mathbb{Z})$ ein Teilkörper von K, der in P enthalten ist. Weil der Primkörper P der kleinste Teilkörper von K ist, folgt $P = \varphi(\mathbb{Z})$ und damit die Behauptung.

$\Longleftarrow$ folgt sofort.

Zu (b): Die Charakteristik von K ist gleich Null genau dann wenn φ injektiv ist. Damit ist $\varphi(\mathbb{Z}) \cong \mathbb{Z}$ ein Teilring von K. Der Ring $\varphi(\mathbb{Z})$ wird von $1 \in K$ erzeugt, ist also der kleinste Teilring von K. Der Homomorphismus φ erweitert sich eindeutig zu einem Körper-Homomorphismus $\overline{\varphi} : \mathbb{Q} \longrightarrow K$, durch $\overline{\varphi}(\frac{a}{b}) = \frac{\varphi(a)}{\varphi(b)}$. Da $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ ist, ist somit $\overline{\varphi}(\mathbb{Q})$ der Quotientenkörper von $\varphi(\mathbb{Z})$. Dieser Quotientenkörper muss gerade P sein, da er nach Konstruktion der kleinste Körper ist, der $\varphi(\mathbb{Z})$ enthält und somit als Körper von der 1 erzeugt wird. Also ist $P = \overline{\varphi}(\mathbb{Q}) \cong \mathbb{Q}$, da jeder Körper-Homomorphismus nach Korollar 2.2.9 injektiv ist.

Die Rückrichtung folgt wieder sofort.

□

KOROLLAR 3.1.9. *Jeder Teilkörper von K hat dieselbe Charakteristik wie K.*

BEWEIS. Dies folgt sofort aus Proposition 3.1.8, da jeder Teilkörper denselben Primkörper besitzt. □

SATZ 3.1.10. *Sei K ein Körper und p eine Primzahl. Die Abblidung $K \longrightarrow K$, mit $a \mapsto a^p$, ist ein Körper-Endomorphismus wenn* $\mathrm{char}(K) = p$ *ist.*

BEWEIS. Übung. □

3.2. Körpererweiterungen

Im Herzstück der Vorlesung werden wir Körpererweiterungen untersuchen. Die Hauptresultate werden in der Galoistheorie erreicht. In diesem Abschnitt werden wir die Grundlagen für diese bereitstellen.
Wie immer sei K ein Körper.

DEFINITION 3.2.1. Eine *Körpererweiterung* L von K ist ein Körper $L \supseteq K$ so, dass K ein Teilkörper von L ist. Wir nennen L auch *Oberkörper* von K und notieren solche Körpererweiterungen mit L/K. (Das hat nichts mit Faktorringen zu tun!)

BEISPIEL 3.2.2. $\mathbb{C}$ ist eine Körpererweiterung von $\mathbb{R}$, und $\mathbb{R}$ ist eine Körpererweiterung von $\mathbb{Q}$.

Sei L/K eine Körperereweiterung. Dann ist L ein K-Vektorraum mit der Addition aus L und der skalaren Multiplikation $K \times L \longrightarrow L$; $(\lambda, \beta) \mapsto \lambda \cdot \beta$. Hier ist die Multiplikation wieder die von L.

DEFINITION 3.2.3. Der *Grad* von L über K ist definiert als Dimension des K-Vektorraumes L. D.h.:

$$[L:K] := \begin{cases} \dim_K(L) & \text{falls diese endlich ist} \\ \infty & \text{sonst} \end{cases}.$$

Der Grad $[L:K]$ ist also genau dann gleich ∞, wenn wir beliebig viele K-linear unabhängige Elemente in L finden können.

BEISPIEL 3.2.4.
- $[\mathbb{C}:\mathbb{R}] = 2$, da $\{1, i\}$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist.
- $[\mathbb{R}:\mathbb{Q}] = \infty$, denn falls $[\mathbb{R}:\mathbb{Q}] = n < \infty$ wäre, so wäre $\mathbb{R} \cong \mathbb{Q}^n$ als $\mathbb{Q}$-Vektorraum. Aber: $\mathbb{Q}$ ist abzählbar, also ist auch $\mathbb{Q}^n$ abzählbar (Cantorsches Diagonalargument). Somit wäre dann auch $\mathbb{R}$ abzählbar, was bekannterweise nicht der Fall ist.

PROPOSITION 3.2.5 (Gradformel). *Seien $M \supseteq L \supseteq K$ Körpererweiterungen. Dann gilt*

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

BEWEIS. Falls $[L:K] = \infty$, so finden wir beliebig viele K-linear unabhängige Elemente in $L \subseteq M$. Also ist auch $[M:L] = \infty$. Da L-linear unabhängige Elemente erst recht K-linear unabhängig sind, folgt analog: $[M:K] = \infty$ falls $[M:L] = \infty$.
Es bleibt also die Aussage für $m := [M:L] < \infty$ und $l := [L:K] < \infty$ zu beweisen.
Seien dazu $\beta_1, \ldots, \beta_l$ eine K-Basis von L und $\gamma_1, \ldots, \gamma_m$ eine L-Basis von M. Wir wollen zeigen, dass die ml Elemente $\{\beta_i\gamma_j\}_{1\le i\le l, 1\le j\le m}$ eine K-Basis von M bilden.

Lineare Unabhängigkeit: Seien $\lambda_{ij} \in K$ mit $\sum\limits_{1\le i\le l, 1\le j\le m} \lambda_{ij}\beta_i\gamma_j = 0$. Wir müssen zeigen, dass dann $\lambda_{ij} = 0 \quad \forall i, j$ gilt. Ausklammern liefert

$$0 = \sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{l} \lambda_{ij}\beta_i\right)}_{\in L} \gamma_j \quad .$$

Nun sind die Elemente $\gamma_1, \ldots, \gamma_m$ aber L-linear unabhängig. Also folgt $\sum\limits_{i=1}^{l} \lambda_{ij}\beta_i = 0 \quad \forall j = 1, \ldots, m$. Die Elemente λ_{ij} liegen in K und $\beta_1, \ldots, \beta_l$ sind K-linear unabhängig. Damit gilt also $\lambda_{ij} = 0 \quad \forall i = 1, \ldots, l$ und $\forall j = 1, \ldots, m$, was zu zeigen war.

Erzeugendensystem: Dies zeigen wir auf eine ähnliche Art und Weise. Sei $\gamma \in M$ beliebig. Weil die Elemente $\gamma_1, \ldots, \gamma_m$ eine L-Basis von M bilden,

existieren $\mu_1, \ldots, \mu_m \in L$ mit $\gamma = \sum_{j=1}^{m} \mu_j \gamma_j$. Weiter ist $\beta_1, \ldots, \beta_l$ eine K-Basis von L, also gibt es $\lambda_{1j}, \ldots, \lambda_{lj} \in K$ mit $\mu_j = \sum_{i=1}^{l} \lambda_{ij} \beta_i$. Setzen wir dies in die erste Gleichung ein erhalten wir

$$\gamma = \sum_{j=1}^{m} \left(\sum_{i=1}^{l} \lambda_{ij} \beta_i \right) \gamma_j = \sum_{j=1}^{m} \sum_{i=1}^{l} \lambda_{ij} (\beta_i \gamma_j) \quad .$$

Also ist $\{\beta_i \gamma_j\}_{1 \leq i \leq l, 1 \leq j \leq m}$ eine K-Basis von M. Per Definition ist damit $[M : K] = ml = [M : L][L : K]$, was zu zeigen war. □

KONSTRUKTION 3.2.6 (Zur Konstruktion von Körpererweiterungen). Sei $f(x) \in K[x]$ irreduzibel. Wir konstruieren eine Körpererweiterung L/K, die eine Nullstelle von $f(x)$ enthält.
Wir setzen $L := {}^{K[x]}/_{\langle f(x) \rangle}$. Dass dies ein Körper ist hatten wir bereits in den Fakten 3.1.1 bemerkt. Es gibt einen natürlichen Körper-Homomorphismus $\varphi : K \longrightarrow L$, $\alpha \mapsto \overline{\alpha} := \alpha + \langle f(x) \rangle$. Dieser ist, wie jeder Körper-Homomorphismus injektiv (siehe Korollar 2.2.9). Identifizieren wir nun K mit $\varphi(K)$, so ist L tatsächlich eine Körpererweiterung von K.
Für $\beta := \overline{x} \in L$ gilt $f(\beta) = f(\overline{x}) = \overline{f(x)} = \overline{0} \in L$. Also besitzt f eine Nullstelle, nämlich β, in L.

Die Bestimmung von $[L : K]$ wird von großer Bedeutung sein.

PROPOSITION 3.2.7. *Mit den Bezeichnungen von oben gilt die schöne Formel* $[L : K] = \operatorname{grad}(f)$.

BEWEIS. Sei $g(x) \in K[x]$. Nach Divion mit Rest 2.7.2 existieren eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$ mit $g(x) = q(x)f(x) + r(x)$ und $\operatorname{grad}(r) < \operatorname{grad}(f)$. Gehen wir über zu den Restklassen modulo $\langle f \rangle$ so erhalten wir, dass jedes $\overline{g(x)} \in L$ die Form

$$\overline{g(x)} = \overline{r(x)} = a_{\operatorname{grad}(f)-1} \overline{x}^{\operatorname{grad}(f)-1} + \ldots + a_0,$$

mit eindeutig bestimmten $a_0, \ldots, a_{\operatorname{grad}(f)-1} \in K$, besitzt. Also bilden die Elemente $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{\operatorname{grad}(f)-1}$ eine K-Basis von L. Damit gilt $[L : K] = \operatorname{grad}(f)$. □

BEISPIEL 3.2.8. Das Polynom $f(x) := x^2 + 1$ ist irreduzibel in $\mathbb{R}[x]$, da es Grad 2 hat und keine Nullstelle in $\mathbb{R}$ besitzt. Die Körpererweiterung $L = {}^{\mathbb{R}[x]}/_{\langle x^2+1 \rangle}/\mathbb{R}$ ist also vom Grad 2 und es gilt $\overline{x}^2 = -1 \in L$. Somit ist die Abbildung $L \longrightarrow \mathbb{C}$; $\overline{g(x)} \mapsto g(i)$ ein Körper-Isomorphismus.

DEFINITION 3.2.9. Seien L/K und F/K zwei Körpererweiterungen. Ein *K-Homomorphismus* $\varphi : L \longrightarrow F$ ist ein Körper-Homomorphismus so, dass $\varphi|_K = id_K$ gilt. Ein *K-Isomorphismus* ist ein K-Homomorphismus mit einer beidseitigen Umkehrabbildung, die selbst ein K-Homomorphismus ist. Ein K-Isomorphismus mit $L = F$ heißt *K-Automorphismus*.
Die Abbildung aus Beispiel 3.2.8 ist also ein $\mathbb{R}$-Isomorphismus zwischen L und $\mathbb{C}$.

LEMMA 3.2.10. *Sei L/K eine endliche Körpererweiterung. Jeder K-Homomorphismus $\varphi : L \longrightarrow L$ ist ein K-Isomorphismus.*

BEWEIS. Dass φ injektiv ist, haben wir schon oft bemerkt. Damit ist $\varphi(L)$ isomorph zu L. Damit sind diese beiden Körper insbesondere isomorph als K-Vektorräume. Dies impliziert $[L : K] = [\varphi(L) : K]$. Weiter ist $\varphi(L) \subseteq L$ und somit gilt mit der Gradformel

$$[L : K] = [L : \varphi(L)] \cdot [\varphi(L) : K] = [L : \varphi(L)] \cdot [L : K].$$

Dies bedeutet $[L : \varphi(L)] = 1$ und $L = \varphi(L)$. Also ist φ auch surjektiv und somit, wie gewünscht, ein K-Isomorphismus. □

KONSTRUKTION 3.2.11. Sei L/K eine Körpererweiterung und sei $S \subseteq L$ eine beliebige Teilmenge. Dann gibt es einen kleinsten Teilring $K[S]$ von L, der K und S enthält. Wie immer zeigen wir die Existenz damit, dass $K \cup S \subseteq L$ gilt und der Durchschnitt einer beliebigen Familie von Teilringen wieder ein Teilring ist. Es gilt also

$$K[S] := \bigcap_{R \supseteq S \cup K} R.$$

Dabei läuft R im Index über alle Teilringe von L, die K und S enthalten. Wir sagen, dass der Ring $K[S]$ *von S über K erzeugt* ist.

In den Übungen wurde der Polynomring $K[x_1, \ldots, x_n]$ konstruiert. Hier ist die Indexmenge durch $\{1, \ldots, n\}$ gegeben. Ganz genau so erhält man für eine beliebige endliche Menge S den Polynomring $K[(x_s)_{s \in S}]$ in den Variablen x_s, $s \in S$. Wenn $S \subset T$ für eine endliche Menge T, dann ist $K[(x_s)_{s \in S}]$ ein Teilring von $K[(x_t)_{t \in T}]$. Für eine (unendliche) Menge S definieren wir den Polynomring in den Variablen $(x_s)_{s \in S}$ durch

$$K[(x_s)_{s \in S}] := \bigcup_T K[(x_t)_{t \in T}] \quad ,$$

wobei T über alle endlichen Teilmengen von S läuft.

PROPOSITION 3.2.12. *Sei L/K eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Dann gilt*

(a) *Es existiert genau ein Ring-Homomorphismus* $\varphi : K[(x_s)_{s\in S}] \longrightarrow L$ *mit* $\varphi|_K = \mathrm{id}_K$ *und* $\varphi(x_s) = s \quad \forall s \in S$.
(b) $K[S] = \mathrm{Bild}(\varphi) = \{p(s_1, \ldots, s_n) \big| n \in \mathbb{N}, p \in K[x_1, \ldots, x_n]$ *und* $s_1, \ldots, s_n \in S\}$.

BEWEIS. Um (a) zu beweisen genügt es festzustellen, dass wir uns nach Konstruktion auf den Fall einer endlichen Menge S beschränken können. Dieser wurde bereits in den Übungen bewiesen.
Aus Teil (a) folgt, dass Bild(φ) gleich der rechten Seite der Behauptung von (b) ist. Dies ist ein Teilring von L, der S und K enthält. Aufgrund der Abgeschlossenheit von Ringen bezüglich „+“ und „$\cdot$“ muss jeder Teilring von L, der K und S enthält, auch die Ausdrücke der Form $p(s_1, \ldots, s_n)$ enthalten. Also ist das Bild von φ gleich $K[S]$. □

PROPOSITION 3.2.13. *Sei L/K eine Körpererweiterung und $S \subseteq L$ eine beliebige Teilmenge. Wir bezeichen den Quotientenkörper von $K[S]$ mit $K(S)$. Der Körper $K(S)$ ist isomorph zum kleinsten Teilkörper von L, der K und S enthält. Dieser ist gegeben durch*

$$\bigcap_{F \supseteq K \cup S} F$$

wobei F über alle Teilkörper von L läuft, die K und S enthalten. $K(S)$ heißt die von S erzeugte Körpererweitungerung von K in L.

BEWEIS. Folgt leicht aus den Definitionen. □

Wir fassen $K(S)$ als Teilkörper von L auf und nennen $K(S)$ die *von S erzeugte Körpererweiterung von K*. Ist $S \subseteq L$ selbst ein Teilkörper, so gilt $K(S) = S(K) =: SK$ und wir nennen SK, das *Kompositum* von S und K in L.

ABBILDUNG 3.1. Die Konstruktion in 3.2.6 geht auf den deutschen Zahlentheoretiker und Algebraiker *Leopold Kronecker* (1823 - 1891) zurück. Er war Anhänger des Finitismus, in dem die Existenz eines mathematischen Objektes erst als bewiesen gilt, wenn man dieses Objekt explizit konstruiert hat.

3.3. Algebraische Zahlen

Wie immer sei K ein Körper. Wir wollen Nullstellen von Polynomen mit Koeffizienten in K betrachten. Diese Nullstellen nennen wir algebraisch über K. Wie der Name schon vermuten lässt, spielen diese Objekte eine zentrale Rolle in der modernen Algebra.

DEFINITION 3.3.1. Sei L/K eine Körpererweiterung.

- $\beta \in L$ heißt *algebraisch über* K genau dann wenn ein Polynom $p(x) \in K[x]\setminus\{0\}$ existiert, mit $p(\beta) = 0$.
- L/K heißt *algebraisch* genau dann wenn jedes $\beta \in L$ algebraisch über K ist.
- $\beta \in L$ heißt transzendent über K genau dann wenn es nicht algebraisch über K ist.

BEISPIEL 3.3.2.

- Die Zahl $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ und sogar über $\mathbb{Q}$, denn i ist Nullstelle von $p(x) = x^2 + 1 \in \mathbb{Q}[x]$.
- Die Elemente $\sqrt[n]{m} \in \mathbb{C}$, mit $n \in \mathbb{N}$ und $m \in \mathbb{Z}$ sind algebraisch über $\mathbb{Q}$, denn sie sind Nullstellen von $x^n - m$. Falls $m = 1$ ist, so nennen wir die Nullstellen von $x^n - 1$ die *n-ten Einheitswurzeln*. Nutzen wir die Polarkoordinatendarstellung auf $\mathbb{C}$ so stellen wir fest, dass $e^{2k\pi i/n}$, $k \in \mathbb{Z}$, n-te Einheitswurzeln in $\mathbb{C}$ sind.
- Zu zeigen, dass ein Element aus $\mathbb{C}$ transzendent über $\mathbb{Q}$ ist, ist schwierig. Das bedeutende Beispiel der Transzendenz von π wird im Anhang zu diesem Skript behandelt.
- Sei k ein Körper und setze $K = k(t) = \mathrm{Quot}(k[t])$, wobei $k[t]$ der Polynomring in der Variablen t ist. Dann ist t transzendent über k, da per Konstruktion des Polynomringes ein Element der Form $a_n t^n + \cdots + a_0$ mit $a_0, \ldots, a_n \in k$ genau dann gleich Null ist, wenn $a_0 = \cdots = a_n = 0$ gilt.

SATZ 3.3.3. *Sei L/K eine Körpererweiterung und $\beta \in L$ algebraisch. Dann gibt es ein eindeutig bestimmtes normiertes Polynom $m_{\beta,K} \in K[x]$ mit $m_{\beta,K}(\beta) = 0$ und mit minimalem Grad unter allen Polynomen $p \in K[x]\setminus\{0\}$ mit $p(\beta) = 0$.*

BEWEIS. Da β algebraisch über K ist, existiert ein Polynom in $K[x]$, das β als Nullstelle besitzt. Daraus folgt, dass es auch ein solches Polynom minimalen Grades geben muss. Weiter verändert die Multiplikation mit Elementen aus $K\setminus\{0\}$ nicht die Nullstellen des Polynoms. Damit können wir das Polynom normieren, was die Existenz von $m_{\beta,K}$ zeigt.

Sei nun $p \in K[x]\setminus\{0\}$ ein weiteres normiertes Polynom mit $p(\beta) = 0$ und minimalem Grad von allen diesen Polynomen (also $\operatorname{grad}(p) = \operatorname{grad}(m_{\beta,K})$). Dann gilt $\operatorname{grad}(m_{\beta,K} - p) < \operatorname{grad}(m_{\beta,K})$ und $m_{\beta,K}(\beta) - p(\beta) = 0$. Aufgrund der Minimalität des Grades gilt also $m_{\beta,K}(x) = p(x)$, was die Eindeutigkeit von $m_{\beta,K}$ zeigt. □

Das Polynom $m_{\beta,K}$ heißt *Minimalpolynom von β über K*. Die Menge $I = \{p(x) \in K[x] | p(\beta) = 0\}$ ist genau der Kern des Einsetzhomomorphismus $\varphi_\beta : K[x] \longrightarrow L \ ; \ p(x) \mapsto p(\beta)$ (siehe Lemma 2.3.5). Damit ist I nach Proposition 2.2.13 ein Primideal in $K[x]$.

LEMMA 3.3.4. *Es sei $p(x) \in K[x]$ ein normiertes Polynom mit $p(\beta) = 0$. Dann sind folgende Aussagen äquivalent:*

(i) $I = \{q(x) \in K[x] \big| q(\beta) = 0\} = \langle p(x)\rangle$
(ii) $q(x) \in K[x]\setminus\{0\}$, *mit* $q(\beta) = 0 \Longrightarrow p(x) \mid q(x)$
(iii) $p(x) = m_{\beta,K}(x)$ *ist das Minimalpolynom von β über K*
(iv) $p(x)$ *ist irreduzibel*

BEWEIS. Wir werden die Implikationskette $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$ zeigen.

$(i) \Rightarrow (ii)$ Sei $q(x) \in K[x]\setminus\{0\}$ mit $q(\beta) = 0$. D.h. $q(x) \in I = \langle p(x)\rangle$, also gilt $p(x) \mid q(x)$.

$(ii) \Rightarrow (iii)$ Es gilt $m_{\beta,K}(\beta) = 0$. Also gilt $p(x) \mid m_{\beta,K}(x)$. Mit der Gradformel muss also $\operatorname{grad}(p) \leq \operatorname{grad}(m_{\beta,K})$ sein. Die Minimalitätseigenschaft und die Eindeutigkeit von $m_{\beta,K}(x)$ zeigt gerade $p(x) = m_{\beta,K}(x)$.

$(iii) \Rightarrow (iv)$ Wir müssen zeigen, dass $m_{\beta,K}(x)$ irreduzibel ist in $K[x]$. Seien also $q, r \in K[x]$ mit $m_{\beta,K}(x) = q(x)r(x)$. Weil $m_{\beta,K}(x)$ normiert ist, können wir auch annehmen, dass $q(x)$ und $r(x)$ normiert sind. Weiter ist $0 = m_{\beta,K}(\beta) = q(\beta)r(\beta)$. Also gilt oBdA $q(\beta) = 0$. Also muss $\operatorname{grad}(q) = \operatorname{grad}(m_{\beta,K})$ gelten. Mit der Gradformel gilt also $\operatorname{grad}(r) = 0$, was gleichbedeutend ist mit $r \in K\setminus\{0\} = K[x]^*$. Also ist $m_{\beta,K}(x)$ tatsächlich irreduzibel in $K[x]$.

$(iv) \Rightarrow (i)$ Wir haben bereits gesehen, dass $I \neq \{0\}$ ein Primideal im Hauptidealbereich $K[x]$ ist. Also gilt $K[x] \neq I = \langle p_0\rangle$ für ein irreduzibles $p_0 \in K[x]$ (siehe Proposition 2.6.10 und Korollar 2.6.11). Da p ein Element in I ist, gilt also $p_0 \mid p$, und da p irreduzibel ist und p_0 keine Einheit ist, gilt sogar $p_0 \sim p$. Nach Lemma 2.6.5 folgt somit $\langle p\rangle = \langle p_0\rangle = I$.

□

Für eine Körpererweiterung L/K mit $\beta \in L$ haben wir mit $K[\beta]$ den kleinsten Teilring von L, der K und β enthält, bezeichnet. Nach Proposition 3.2.11 ist $K[\beta]$ das Bild des Einsetzhomomorphismus φ_β und somit gilt

$$K[\beta] = \{p(\beta) \big| p(x) \in K[x]\}.$$

Weiter war $K(\beta)$ der kleinste Teilkörper von L, der K und β enthält.

PROPOSITION 3.3.5. *Mit obigen Notationen gilt*

$$K[\beta] = K(\beta) \iff \beta \text{ ist algebraisch über } K.$$

BEWEIS. Die Gleichheit $K[\beta] = K(\beta)$ bedeutet gerade, dass $K[\beta]$ bereits ein Körper ist.

$\Longleftarrow$ Sei β algebraisch über K. Nach dem Isomorphiesatz 2.2.6 für den Einsetzhomomorphismus φ_β gilt

$$K[\beta] = \text{Bild}(\varphi_\beta) \cong {}^{K[x]}\!/_{\ker(\varphi_\beta)} = {}^{K[x]}\!/_{I}.$$

Wir wissen bereits, dass $I \neq \{0\}$ ein Primideal in $K[x]$ ist. Nach Korollar 2.6.11 ist I auch ein Maximalideal in $K[x]$. Also ist ${}^{K[x]}\!/_{I} \cong K[\beta]$ ein Körper (siehe Proposition 2.2.11). Insbesondere muss also $K[\beta] = K(\beta)$ gelten.

$\Longrightarrow$ Wir beweisen die Aussage durch Kontraposition und nehmen an, dass β transzendent über K ist. Wir müssen zeigen, dass $K[\beta]$ kein Körper ist. Zunächst bemerken wir, dass

$$\{0\} = \{p(x) \in K[x] | p(\beta) = 0\} = \ker(\varphi_\beta)$$

ist. Wieder mit dem Isomorphisatz erhalten wir nun

$$K[\beta] \cong {}^{K[x]}\!/_{\ker(\varphi_\beta)} \cong K[x].$$

Da $K[x]$ kein Körper ist (x ist keine Einheit) ist auch $K[\beta]$ kein Körper. Daher muss $K[\beta]$ ungleich $K(\beta)$ gelten.

□

Aus dem Beweis von Proposition 3.3.5 halten wir folgendes Resultat fest.

PROPOSITION 3.3.6. *Sei L/K eine Körpererweiterung, $\beta \in L$ und β algebraisch über K. Dann induziert der Einsetzhomomorphismus einen Isomorphismus*

$$K[x]/\langle m_{\beta,K}(x)\rangle \xrightarrow{\sim} K[\beta].$$

PROPOSITION 3.3.7. *Unter den Voraussetzungen von Proposition 3.3.6 gilt*

$$[K[\beta] : K] = \text{grad}(m_{\beta,K}).$$

BEWEIS. $[K[\beta] : K] \overset{3.3.6}{=} [K[x]/\langle m_{\beta,K}(x)\rangle : K] \overset{3.2.6}{=} \operatorname{grad}(m_{\beta,K})$ □

BEISPIEL 3.3.8. Sei p eine Primzahl und $n \in \mathbb{N}$ beliebig. Dann haben wir die Körpererweiterung $\mathbb{Q}[\sqrt[n]{p}]/\mathbb{Q}$ und $\mathbb{Q}[\sqrt[n]{p}]$ ist ein Teilkörper von $\mathbb{C}$. Es gilt, dass $x^n - p$ das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$ ist. Denn das Polynom ist offensichtlich normiert und hat die Nullstelle $\sqrt[n]{p}$. Weiter ist es irreduzibel nach Eisenstein (Theorem 2.8.11) und somit liefert uns Lemma 3.3.4, dass es tatsächlich das Minimalpolynom ist. Mit Proposition 3.3.7 erhalten wir somit

$$[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = \operatorname{grad}(x^n - p) = n.$$

DEFINITION 3.3.9. Sei L/K eine Körpererweiterung. Ein Zwischenkörper von L/K ist ein Körper F für den $K \subseteq F \subseteq L$ gilt.

PROPOSITION 3.3.10. *Sei L/K eine Körpererweiterung und $\beta \in L$. Dann ist β algebraisch über K genau dann wenn ein Zwischenkörper F von L/K existiert, mit $\beta \in F$ und $[F : K] < \infty$.*

BEWEIS. Wie immer bei 'genau dann wenn'-Aussagen müssen wir zwei Richtungen beweisen.

- $\Longrightarrow$ Sei β algebraisch über K. Setzte $F := K[\beta]$. Dies ist nach Proposition 3.3.5 tatsächlich ein Zwischenkörper mit $\beta \in F$. Weiter gilt $[F : K] = \operatorname{grad}(m_{\beta,K}) < \infty$, was wir in Proposition 3.3.7 bewiesen haben.
- $\Longleftarrow$ Sei F ein Körper wie in der Proposition beschrieben. Da $\beta \in F$ und $[F : K] = n < \infty$, müssen die $n + 1$ Elemente $1, \beta, \ldots, \beta^n$ nach Definition des Grades K-linear abhängig sein. Damit gibt es $a_0, \ldots, a_n \in K$, nicht alle 0, mit $a_0 + a_1\beta + \ldots + a_n\beta^n = 0$. Also ist β Nullstelle des Polynoms $a_0 + a_1x + \ldots + a_nx^n \in K[x]\setminus\{0\}$. Damit ist β algebraisch über K.

□

Insbesondere sind also alle endlichen Körpererweiterungen L/K (d.h. $[L : K] < \infty$) algebraisch.

THEOREM 3.3.11. *Sei L/K eine Körpererweiterung. Dann ist $M := \{\beta \in L | \beta$ algebraisch über $K\}$ ein Unterkörper von L mit $K \subseteq M$.*

BEWEIS. Für $\beta \in K$ ist $p(x) = x - \beta \in K[x]$ und hat die Nullstelle β. Somit gilt $\beta \in M$ und damit ist $K \subseteq M$ gezeigt. Insbesondere gilt $0, 1 \in M$.
Um zu zeigen, dass M ein Unterkörper von L ist, genügt es zu zeigen, dass $\beta \pm \gamma$, $\beta\gamma$ und $\gamma^{-1} \in M$ sind für beliebige Elemente $\beta, \gamma \in M$, $\gamma \neq 0$.

Weil β algebraisch über K ist, gibt es einen Unterkörper F_β von L mit $\beta \in F_\beta$ und $[F_\beta : K] < \infty$ (nach 3.3.10). Weil γ algebraisch über K ist, ist γ erst recht algebraisch über $F_\beta \supseteq K$. Wieder mit 3.3.10 gibt es einen Zwischenkörper F_γ mit $F_\beta \subseteq F_\gamma \subseteq L$ und $\gamma \in F_\gamma$ und $[F_\gamma : F_\beta] < \infty$. Mit der Gradformel 3.2.5 gilt $[F_\gamma : K] = [F_\gamma : F_\beta][F_\beta : K] < \infty$. Also ist F_γ ein Unterkörper von L, der $\beta \pm \gamma$, $\beta\gamma$ und γ^{-1} enthält, weil $\beta, \gamma \in F_\gamma$. Wieder mit 3.3.10 folgt, dass alle diese Elemente in M liegen. □

3.4. Zerfällungskörper

Sei K ein Körper. Für ein gegebenes Polynom $p(x) \in K[x]$ möchten wir einen Körper betrachten, der alle Nullstellen von p enthält. Dies wird in aller Regel nicht der Grundkörper K sein. In diesem Abschnitt werden wir die kleinste Körpererweiterung von K konstruieren, die alle Nullstellen von unserem gegebenen Polynom $p(x)$ enthält. Diese Erweiterung werden wir Zerfällungskörper nennen.
Wenn z.B. $p(x) = x^2 - 2$ ist und $K = \mathbb{Q}$, dann ist der Zerfällungskörper von $p(x)$ gleich $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \big| a, b, \in \mathbb{Q}\}$.

Proposition 3.4.1. *Seien L/K und L'/K Körpererweiterungen und sei $\varphi : L \longrightarrow L'$ ein K-Homomorphismus. Dann gilt $p(\varphi(\beta)) = \varphi(p(\beta))$ für alle $\beta \in L$. Insbesondere werden alle Nullstellen von $p(x)$ in L auf Nullstellen von $p(x)$ in L' abgebildet.*

Beweis. Sei $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ mit $a_i \in K$, $i = 1, \ldots, n$.

$$\begin{aligned} p(\varphi(\beta)) &= a_n\varphi(\beta)^n + a_{n-1}\varphi(\beta)^{n-1} + \ldots + a_0 \\ &= \varphi(a_n)\varphi(\beta)^n + \varphi(a_{n-1})\varphi(\beta)^{n-1} + \ldots + \varphi(a_0) \\ &= \varphi(a_n\beta^n) + \varphi(a_{n-1}\beta^{n-1}) + \ldots + \varphi(a_0) \\ &= \varphi(a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_0) = \varphi(p(\beta)) \end{aligned}$$

Sei nun $p(\beta) = 0$. Dann folgt aus dem ersten Teil

$$0 = \varphi(0) = \varphi(p(\beta)) = p(\varphi(\beta)).$$

Also ist $\varphi(\beta)$ eine Nullstelle von $p(x)$ in L' wie behauptet. □

Bemerkung 3.4.2. Wir erinnern daran, dass wir bereits gesehen haben dass es zu $p \in K[x] \setminus K$ eine Körpererweiterung L/K gibt, die eine Nullstelle von p enthält. Die Eigenschaft, dass ein Körper L' *alle* Nullstellen von p enthält ist gleichbedeutend damit, dass p über L' in Linearfaktoren zerfällt.

Proposition 3.4.3. *Sei $p(x)$ irreduzibel in $K[x]$. Dann gilt*

(a) *Es gibt eine Körpererweiterung L/K mit einer Nullstelle $\beta \in L$ von $p(x)$ so, dass $L = K[\beta]$.*
(b) *Sei $\varphi : K \longrightarrow L'$ ein Körper-Homomorphismus. Dann existiert genau ein Ring-Homomorphismus $\tilde{\varphi} : K[x] \longrightarrow L'[x]$, mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(x) = x$.*
(c) *Falls β' eine Nullstelle von $\tilde{\varphi}(p)$ in L' ist, dann gibt es genau einen Körper-Homomorphismus $\varphi' : L \longrightarrow L'$, mit $\varphi'|_K = \varphi$ und $\varphi'(\beta) = \beta'$*

BEWEIS. Die Aussage in (a) haben wir bereits in Beispiel 3.2.6 und Proposition 3.3.6 bewiesen.

Zu (b): Wie beim Einsetzhomomorphismus in Lemma 2.3.5 folgt, dass $\tilde{\varphi}$ durch $\tilde{\varphi}(\sum_{j=0}^{m} b_j x^j) = \sum_{j=0}^{m} \varphi(b_j)x^j$ eindeutig bestimmt und ein Ring-Homomorphismus ist.

Zu (c): Es ist $L = K[\beta] = \{q(\beta) | q \in K[x]\}$. Sei also $\gamma = q(\beta)$, mit $q(x) = a_n x^n + \cdots + a_0 \in K[x]$, beliebig. Da das gesuchte φ' ein Homomorphismus sein soll, muss gelten:

$$\varphi'(\gamma) = \varphi'(a_n)\varphi'(\beta)^n + \cdots + \varphi'(a_0) \overset{\text{Voraussetzung}}{=} \varphi(a_n)\beta'^n + \cdots + \varphi(a_0).$$

Dies zeigt die Eindeutigkeit. Wir müssen noch zeigen, dass diese Abbildung wohldefiniert ist. Sei also $q' \in K[x]$ ein weiteres Element mit $\gamma = q'(\beta)$. Da $p(x)$ irreduzibel ist, ist es bis auf Multiplikation mit Einheiten das Minimalpolynom von β. Also gilt nach Lemma 3.3.4 $p(x) \mid q'(x) - q(x)$. Insbesondere ist also $q'(x) = q(x) + r(x)p(x)$ für ein $r(x) \in K[x]$. Es folgt

$$\varphi'(q'(\beta)) = \varphi'(q(\beta)) + \underbrace{\varphi'(r(\beta)p(\beta))}_{=0} = \varphi'(q(\beta)).$$

Somit ist die Konstruktion von φ' tatsächlich wohldefiniert. Dass diese Konstruktion auch ein Körper-Homomorphismus ist folgt unmittelbar aus der homomorphie Eigenschaft von φ.

□

SATZ 3.4.4. *Sei $p(x) \in K[x]$ vom Grad $n \geq 1$. Dann gibt es eine Körpererweiterung L/K so, dass $p(x)$ in ein Produkt von Linearfaktoren in $L[x]$ zerfällt und $[L : K] \leq n!$ gilt.*

BEWEIS. Wir führen den Beweis per Induktion über n.
Wenn $n = 1$ ist, dann ist $p(x)$ selbst ein Linearfaktor in $K[x]$, also können wir $K = L$ wählen und es gilt $[L : K] = 1!$.

Sei nun also $n > 1$. Betrachte einen irreduziblen normierten Faktor $q(x) \in K[x]$ von $p(x)$. Nach Konstruktion 6.2.6 gibt es eine Körpererweiterung L'/K, die eine Nullstelle β von $q(x)$ enthält, und mit Proposition 3.2.5 gilt

$$[L' : K] = \text{grad}(q) \leq \text{grad}(p) = n \quad . \tag{6}$$

Insbesondere ist β auch eine Nullstelle von $p(x)$. Wir können die Nullstelle β von $p(x)$ abspalten, d.h. es gibt ein Polynom $q'(x) \in L'[x]$ so, dass $p(x) = (x - \beta)q'(x)$ und $\text{grad}(q') = n - 1$.
Nach Induktionsvoraussetzung existiert also eine Körpererweiterung L/L' so, dass $[L : L'] \leq (n-1)!$ und

$$q'(x) = a(x - \beta_1) \cdots (x - \beta_{n-1})$$

für geeignete $\beta_1, \ldots, \beta_{n-1} \in L$. Weiter gilt

$$[L : K] \overset{3.2.5}{=} [L : L'][L' : K] \overset{(6)}{\leq} (n-1)! \cdot n = n!$$

und $p(x)$ zerfällt über L in Linearfaktoren. □

THEOREM 3.4.5. *Sei $f(x) \in K[x]$. Dann gibt es eine Körpererweiterung L/K, mit $f(x) = a_n(x - \beta_1) \cdots (x - \beta_n)$ für Elemente $\beta_1, \ldots, \beta_n \in L$ und $L = K(\beta_1, \ldots, \beta_n)$. Diese Körpererweiterung L/K ist bis auf K-Isomorphie eindeutig.*

BEWEIS. *Existenz:* Nach Satz 3.4.4 existiert ein Körper L'/K mit $f(x) = a_n(x - \beta_1) \cdots (x - \beta_n)$ für Elemente $\beta_1, \ldots, \beta_n \in L'$. Der Teilkörper $L = K(\beta_1, \ldots, \beta_n)$ von L' erfüllt nun alle gewünschten Eigenschaften.
Eindeutigkeit: Seien L/K und L'/K zwei Körpererweiterungen, die die Voraussetzungen des Theorems erfüllen. D.h.: $L = K(\beta_1, \ldots, \beta_n)$, mit $f(x) = a_n(x - \beta_1) \cdots (x - \beta_n) \in L[x]$ und $L' = K(\beta'_1, \ldots, \beta'_n)$, mit $f(x) = a_n(x - \beta'_1) \cdots (x - \beta'_n) \in L'[x]$.
Sei F ein Zwischenkörper von L/K so, dass es einen K-Homomorphismus $\varphi : F \to L'$ gibt mit (siehe Proposition 3.4.3)

$$\tilde{\varphi}(f) = \varphi(a_n)(x - \beta'_1) \cdots (x - \beta'_n) \in L'[x].$$

Diese Voraussetzung ist zum Beispiel für $F = K$ und $\varphi = \text{id}$ erfüllt.
Behauptung: Es existiert ein Homomorphismus $\varphi' : L \longrightarrow L'$ so, dass $\varphi'|_F$ und $\varphi(\beta_i) = \beta'_i$ für alle $i = 1, \ldots, n$ nach geeigneter Permutation der Nullstellen $\beta'_1, \ldots, \beta'_n$.
Beweis der Behauptung: Mit Induktion nach n.
Für $n = 1$ gilt $f(x) = a_n(x - \beta_n) = a_n(x - \beta'_n) \in K[x]$. Also gilt $L = K = L'$.
Sein nun $n > 1$ und $p(x) \in K[x]$ der irreduzible Faktor von $f(x)$ mit $p(\beta_n) = 0 \in L$. Nach Voraussetzung besitzt $p(x)$ auch eine Nullstelle in L' und nach

Permutation der Nullstellen dürfen wir $p(\beta'_n) = 0 \in L'$ annehmen. Mit Proposition 3.4.3 (c) existiert ein K-Homomorphismus $\varphi_n : K(\beta_n) \to L'$ mit $\varphi_n(\beta_n) = \beta'_n$. Abspalten der Nullstelle $\beta_n \in L$ liefert

$$f(x) = (x - \beta_n)f_1(x) \text{ , für ein } f_1 \in (K(\beta_n))[x] \text{ mit } \operatorname{grad}(f_1) = n - 1.$$

Nach Induktionsvorraussetzung existiert also ein Homomorphismus $\varphi' : L \to L'$ mit $\varphi'|_{K(\beta_n)} = \varphi_n$, also ist φ' insbesondere ein K-Homomorphismus. Dies beweist die Behauptung. Das eben konstruierte φ' ist surjektiv, da $L' = K(\beta'_1, \ldots, \beta'_n)$ und $\varphi'(\beta_i) = \beta'_i$ für alle $i \in \{1, \ldots, n\}$. Da weiter jeder Körperhomomorphismus injektiv ist, ist φ' ein Isomorphismus, was zu zeigen war. □

Definition 3.4.6. Der Körper $L = K(\beta_1, \ldots, \beta_n)$ aus Theorem 3.4.5 heißt *Zerfällungskörper* von f. Es ist nach Konstruktion der kleinste Körper über dem f in Linearfaktoren zerfällt.

3.5. Algebraisch abgeschlossene Körper

Wir werden in diesem Abschnitt zwei wichtige Resultate beweisen. Erstens werden wir sehen, dass jedes Polynom über $\mathbb{C}$ in Linearfaktoren zerfällt und zweitens werden wir zeigen, dass jeder Körper eine algebraische Körpererweiterung $\overline{K}$ besitzt, so dass jedes Polynom aus $K[x]$ in Linearfaktoren aus $\overline{K}[x]$ zerfällt. Dies erlaubt uns für jeden Körper zu einer Körpererweiterung überzugehen, in der jede polynomielle Gleichung lösbar ist!

Definition 3.5.1. Ein Körper K heißt *algebraisch abgeschlossen*, genau dann wenn jedes Polynom in $K[x]$ vom Grad ≥ 1 mindestens eine Nullstelle in K besitzt.

Proposition 3.5.2. *In einem algebraisch abgeschlossenem Körper K zerfällt jedes $p(x) \in K[x] \setminus K$ in ein Produkt von Linearfaktoren aus $K[x]$.*

Beweis. Wir beweisen die Aussage mit Induktion nach $n = \operatorname{grad}(p)$. Der Fall $n = 1$ ist trivial. Falls $n > 1$, dann haben wir eine Nullstelle α von $p(x)$ nach Definition von algebraisch abgeschlossen. Wir spalten diese Nullstelle ab, wie in Proposition 3.1.3. Damit gilt $p(x) = (x - \alpha) \cdot q(x)$ für ein $q \in K[x]$ vom Grad $n - 1$. Mit Induktion folgt nun die Behauptung. □

Bemerkung 3.5.3. Ein algebraisch abgeschlossener Körper K kann keine echten algebraischen Erweiterungen besitzen. Denn für L/K algebraisch und $\alpha \in L$ muss nach Proposition 3.5.2 bereits $x - \alpha \in K[x]$, also $\alpha \in K$, gelten.

Satz 3.5.4 (Fundamentalsatz der Algebra). $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Es gibt viele verschiedene Beweise dieses Theorems. Der wohl eleganteste benutzt den folgenden Satz aus der Funktionentheorie (komplexen Analysis). Dorthin verweisen wir auch für einen Beweis.

THEOREM 3.5.5 (Satz von Liouville). *Sei $f : \mathbb{C} \longrightarrow \mathbb{C}$ eine holomorphe Funktion. Ist $|f(z)|$ beschränkt auf ganz $\mathbb{C}$, so ist f konstant.*

BEWEIS VON THEOREM 3.5.4. Sei $p(x) \in \mathbb{C}[x] \setminus \{0\}$, so dass p keine Nullstelle in $\mathbb{C}$ besitzt. Dann ist mit $p(x)$ auch $1/p(x)$ eine holomorphe Funktion auf ganz $\mathbb{C}$. Weiter ist $|1/p(z)|$ auf ganz $\mathbb{C}$ beschränkt, was aus der Stetigkeit von $1/p(x)$ folgt. Also gilt mit Theorem 3.5.5, $1/p(x) = c \in \mathbb{C} \setminus \{0\}$. Damit ist dann auch $p(x)$ konstant. Also besitzt jedes nicht konstante Polynom eine Nullstelle in $\mathbb{C}$. □

ABBILDUNG 3.2. Der herausragende französische Mathematiker *Joseph Liouville* (1809 - 1882) war höchst wahrscheinlich der erste der die Ideen Galois verstanden und ihre Bedeutung erkannt hat. Er veröffentlichte Galois Schriften 1846. Die Ideen Galois werden uns im nächsten Kapitel beschäftigen.

Wir benutzen im Folgenden das *Zorn'sche Lemma*. Dies ist eine Aussage in der Mathematik, die *nicht* (mit den Zermelo-Fraenkel-Axiomen) bewiesen werden kann. Es ist also ein Axiom und äquivalent zum sogenannten *Auswahl-Axiom*. Zunächst ein paar Vorüberlegungen:

Sei $M \neq \emptyset$ eine partiell geordnete Menge bezüglich der Relation $\leq$. (D.h. $\leq$ ist reflexiv, transitiv und antisymmetrisch, wie die Teilbarkeitsrelation aus Bemerkung 2.5.13). Eine Teilmenge $K \subseteq M$ heißt *total geordnet* genau dann wenn für alle $x, y \in K$ gilt $x \leq y$ oder $y \leq x$. Eine *obere Schranke* in einer solchen Menge K ist ein Element $z \in M$ mit $x \leq z$ für alle $x \in K$.

ZORN'SCHES LEMMA 3.5.6. *Falls jede total geordnete Teilmenge K von M eine obere Schranke in M hat, dann gibt es in M ein maximales Element x_{max}, d.h. $x \in M, x_{max} \leq x \Longrightarrow x_{max} = x$.*

LEMMA 3.5.7. *Jedes Ideal $I_0 \neq R$ in einem kommutativen Ring R ist in einem Maximalideal enthalten.*

BEWEIS. Sei $M = \{I \lhd R | I \neq R, I_0 \subseteq I\}$. Dann ist $M \neq \emptyset$, da $I_0 \in M$. Weiter ist M partiell geordnet bezüglich $\subseteq$. Wir zeigen nun, dass die Voraussetzungen des Zorn'schen Lemmas erfüllt sind.

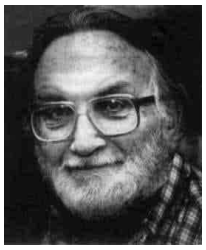


ABBILDUNG 3.3. Das Zorn'sche Lemma stammt von dem deutsch-amerikanischen Mathematiker *Max August Zorn* (1906 - 1993), der 1933 aufgrund der nationalsozialistischen Politik Deutschlands in die USA emigrierte. Ein weiteres wichtiges Resultat, das man mit Hilfe des Zorn'schen Lemmas erhält, ist die Existenz einer Basis in einem (nicht-endlich dimensionalen) Vektorraum.

Sei also K eine total geordnete Teilmenge von M, dann ist $J_0 := \bigcup_{J\in K} J$ auch ein Ideal, was in den übungen gezeigt wurde. Weil $1 \notin J \forall J \in K$, ist auch $1 \notin J_0$. Somit ist $I_0 \subseteq J_0 \neq R$. Also $J_0 \in M$ und J_0 ist eine obere Schranke von K in M. Nach dem Zorn'schen Lemma gibt es ein maximales Element J_{max} in M. Dieses ist offenbar ein Maximalideal von R welches I_0 enthält. □

In 3.2.9 haben wir für eine Menge T den Polynomring über einem Körper K in den Variablen x_t, $t \in T$, als $K[(x_t)_{t\in T}] := \bigcup_{S\subseteq T, |S|<\infty} K[(x_s)_{s\in S}]$ konstruiert. Hier ist $K[(x_s)_{s\in S}]$, für eine endliche Menge S, der übliche Polynomring in $|S|$ vielen Variablen, den wir schon aus den Übungen kennen.

THEOREM 3.5.8. *Jeder Körper K ist ein Teilkörper eines algebraisch abgeschlossenen Körpers.*

BEWEIS. Wir haben bereits gesehen, dass wir zu einem $f(x) \in K[x]$ einen Zerfällungskörper konstruieren können. Eine Körpererweiterung von K in der n Polynome $f_1, \ldots, f_n \in K[x]$, $n \in \mathbb{N}$, in Linearfaktoren zerfallen erhalten wir durch den Zerfällungskörper von $f_1 \cdots f_n \in K[x]$. Dies wollen wir nun mit Hilfe des Zorn'schen Lemmas 3.5.6 für unendlich viele Polynome erweitern.

1. Schritt: Es existiert eine Körpererweiterung K_1/K, so dass jedes $f(x) \in K[x]$ mindestens eine Nullstelle in K_1 besitzt.

Wir setzen $T := K[x]\backslash K$ und betrachten den Polynomring $R := K[(x_f)_{f\in T}]$. Insbesondere enthält R die Polynome $f(x_f)$ für alle $f \in T = K[x]\backslash K$. Diese Polynome erzeugen ein Ideal J_0 in R. Es ist also

$$J_0 = \langle \{ f(x_f) \big| f \in T \} \rangle \overset{2.6.1}{=} \{ \sum_{k=1}^{n} g_k f_k(x_{f_k}) | n \in \mathbb{N}, g_k \in R \}.$$

Wir wollen nun zeigen, dass J_0 nicht ganz R sein kann. Angenommen $J_0 = R$, dann wäre $1 \in J_0$ und damit hat man eine Darstellung

$$1 = g_1 f_1(x_{f_1}) + \ldots + g_n f_n(x_{f_n}) \text{ , mit } g_k \in R \text{ für } k \in \{1, \ldots, n\}.$$

Sei L ein Zerfällungskörper von $f_1 \cdots f_n \in K[x]$. Dann existieren für alle $k \in \{1, \ldots, n\}$ Elemente $\alpha_k \in L$, mit $f_k(\alpha_k) = 0$. Setzen wir diese Elemente $\alpha_1, \ldots, \alpha_n$ für $x_{f_1}, \ldots, x_{f_n}$ in obiger Gleichung ein, so erhalten wir $1 = 0$. Dies ist natürlich ein Widerspruch, also gilt $J_0 \neq R$.
Nach Lemma 3.5.7 gibt es ein Maximalideal J in R mit $J_0 \subseteq J$. Nach Proposition 2.2.11 ist $K_1 = {}^{R}\!/_{J}$ ein Körper. Es ist sogar eine Körpererweiterung von K, denn es ist

$$K \xrightarrow{\text{konst. Polyn.}} R \xrightarrow{\text{Proj.}} {}^{R}\!/_{J} = K_1.$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{=:\varphi}$$

Weil φ ein Ring-Homomorphismus zwischen Körpern ist, muss φ injektiv sein und damit dürfen wir K mit seinem Bild $\varphi(K)$ identifizieren und somit K als Teilkörper von K_1 auffassen. Sei nun $f \in T = K[x] \setminus K$ beliebig. Dann gilt für $\overline{x_f} = x_f + J \in K_1$ gerade $f(\overline{x_f}) = \overline{f(x_f)} = 0 \in K_1$ (analog zu 3.2.6). Damit besitzt jedes $f \in K[x] \setminus K$ eine Nullstelle in K_1.

2. Schritt: Schluss des Beweises.

Wir iterieren den ersten Schritt mit $K_0 = K$. Das heißt, für jedes $i \in \mathbb{N}_0$ konstruieren wir einen Körper K_{i+1} so, dass $K_i \subseteq K_{i+1}$ und jedes $f \in K_i[x] \setminus K_i$ eine Nullstelle in K_{i+1} besitzt.
Wir betrachten den Körperturm $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$. Genau wie bei Idealen sehen wir, dass $F := \cup_{i \in \mathbb{N}_0} K_i$ ein Körper ist mit $K \subseteq F$. Sei nun $g(x) \in F[x] \setminus F$ beliebig. Dann existiert ein $n \in \mathbb{N}$ mit $g(x) \in K_n[x] \setminus K_n$. Also besitzt $g(x)$ eine Nullstelle in $K_{n+1} \subseteq F$. Damit ist F ein algebraisch abgeschlossener Oberkörper von K. □

THEOREM 3.5.9. *Jeder Körper K besitzt eine algebraische Körpererweiterung $\overline{K}/K$, so dass $\overline{K}$ algebraisch abgeschlossen ist. Dadurch ist $\overline{K}$ bis auf K-Isomorphie eindeutig bestimmt.*

BEWEIS. *Existenz:* Wir haben in Theorem 3.5.8 bewiesen, dass es eine Körpererweiterung F/K gibt, so dass F algebraisch abgeschlossen ist. Setze nun $\overline{K} = \{\beta \in F | \beta \text{ algebraisch über } K\}$. In den übungen wird gezeigt, dass dies tatsächlich ein algebraisch abgeschlossener Körper ist und, dass $\overline{K}/K$ algebraisch ist.
Eindeutigkeit: Wir werden wieder das Zorn'sche Lemma benutzen. Seien $\overline{K}$ und $\overline{K}'$ zwei algebraisch abgeschlossene Oberkörper von K, die algebraisch über K sind. Definiere

$$M = \{(L, \tau) | L \text{ Zwischenkörper von } \overline{K}/K \text{ und } \tau : L \to \overline{K}' \text{ ein } K - \text{Hom.}\}.$$

Die Menge M ist nicht leer, da $(K, \mathrm{id}) \in M$. Die Relation

$$(L, \tau) \leq (L', \tau') \Longleftrightarrow L \subseteq L' \text{ und } \tau'|_L = \tau$$

ist eine partielle Ordung auf M (die hierfür nötigen Eigenschaften Reflexivität, Transitivität und Antisymmetrie sieht man sofort). Sei nun I eine beliebige Indexmenge und $\{(L_i, \tau_i)\}_{i \in I} \subseteq M$ eine totalgeordnete Teilmenge von M. Das bedeutet: Für $i, j \in I$ gilt $L_i \subseteq L_j$ und $\tau_j|_{L_i} = \tau_i$ oder andersherum. Dann ist $L = \cup_{i \in I} L_i$ ist ein Körper und jedes $\alpha \in L$ ist in einem L_i, für ein $i \in I$, enthalten. Dadurch wird $\tau : L \longrightarrow \overline{K}'$, durch $\alpha \mapsto \tau_i(\alpha)$, zu einem wohldefinierten K-Homomorphismus. Also ist das so erhaltene $(L, \tau) \in M$ eine obere Schranke von $\{(L_i, \tau_i)\}_{i \in I}$. Mit dem Zorn'schen Lemma 3.5.6 besitzt M ein maximales Element (Z, σ).
Nach Definition von M ist Z ein Teilkörper von $\overline{K}$. Angenommen $Z \neq \overline{K}$. Dann existiert ein $\alpha \in \overline{K} \setminus Z$. Da α algebraisch über K ist, ist α erst recht algebraisch über Z. Sei also $m_{\alpha,Z}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in Z[x]$ das Minimalpolynom von α. Dann besitzt

$$\tilde{\sigma}(m_{\alpha,Z}(x)) = x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_0) \in \overline{K}'$$

eine Nullstelle $\alpha' \in \overline{K}'$. Nach Proposition 3.4.3 existiert genau ein Körper-Homomorphismus $\sigma' : Z(\alpha) \longrightarrow \overline{K}'$ mit $\sigma'|_Z = \sigma$ und $\sigma'(\alpha) = \alpha'$. In der Sprache der eingeführten Relation $\leq$ bedeutet dies gerade $(Z, \sigma) \leq (Z(\alpha), \sigma')$ und aus $\alpha \notin Z$ folgt $(Z, \sigma) \neq (Z(\alpha), \sigma')$ im Widerspruch zur Maximalität von (Z, σ). Also gilt $Z = \overline{K}$ und $\sigma : \overline{K} \longrightarrow \overline{K}'$ ist ein K-Homomorphismus.
Wir müssen noch zeigen, dass σ sogar ein K-Isomorphismus ist. Wie immer wissen wir bereits, dass σ als Körper-Homomorphismus injektiv ist. Es bleibt die Surjektivität zu zeigen.
Der Körper $\sigma(\overline{K}) \subseteq \overline{K}'$ ist algebraisch abgeschlossen, denn: Sei $f \in \sigma(\overline{K})[x] \setminus \sigma(\overline{K})$ beliebig und $f' \in \overline{K}[x]$ mit $\tilde{\sigma}(f') = f$. Da $\overline{K}$ algebraisch abgeschlossen ist, existiert ein $\beta \in \overline{K}$ mit $f'(\beta) = 0$. Damit ist aber auch $\sigma(\beta) \in \sigma(\overline{K})$ eine Nullstelle von $\tilde{\sigma}(f') = f$ (siehe Proposition 3.4.1).
Nun ist $\overline{K}'$ eine algebraische Körpererweiterung des algebraisch abgeschlossenen Körpers $\sigma(\overline{K})$. Wie wir in Bemerkung 3.5.3 festgestellt haben, muss damit $\sigma(\overline{K}) = \overline{K}'$ gelten. Also ist σ ein K-Isomorphismus zwischen $\overline{K}$ und $\overline{K}'$. □

Definition 3.5.10. Sei K ein Körper. Ein algebraisch abgeschlossener Körper $\overline{K} \supseteq K$, der algebraisch über K ist, heißt *algebraischer Abschluss von* K. Wir haben in Theorem 3.5.9 gezeigt, dass jeder Körper einen bis auf K-Isomorphie eindeutigen algebraischen Abschluss besitzt.

Bemerkung 3.5.11. Ein Isomorphismus zwischen zwei algebraischen Abschlüssen, ist im Allgemeinen *nicht* eindeutig bestimmt, was in den Übungen gezeigt wird.

Beispiel 3.5.12. Der algebraische Abschluss von $\mathbb{R}$ ist $\overline{\mathbb{R}} = \mathbb{C}$. Da es jedoch viele über $\mathbb{Q}$ transzendente Elemente in $\mathbb{C}$ gibt, ist $\mathbb{C}$ kein algebraischer Abschluss von $\mathbb{Q}$.

Bemerkung 3.5.13. Endliche Körper können nicht algebraisch abgeschlossen sein. Um dies zu sehen müssen wir zu einem beliebigen endlichen Körper K ein Polynom $f(x) \in K[x] \setminus K$ konstruieren, dass keine Nullstellen in K besitzt. Ein solches Polynom ist zum Beispiel gegeben durch $f(x) = 1 + \prod_{\alpha \in K}(x - \alpha)$. Denn damit gilt $f(\alpha) = 1 \neq 0$ für alle $\alpha \in K$. Somit ist der endliche Körper K tatsächlich nicht algebraisch abgeschlossen.

KAPITEL 4

Galois-Theorie

4.1. Normale Körpererweiterungen

Wie immer sei K ein Körper. Für jedes Polynom $f(x) \in K[x]$ können wir den Zerfällungskörper konstruieren. In diesem Abschnitt wollen wir der Frage nachgehen für welche endlichen Körpererweiterungen L/K (d.h. $[L : K] < \infty$) der Körper L ein Zerfällungskörper für irgendein Polynom aus $K[x]$ ist.

DEFINITION 4.1.1. Die Körpererweiterung L/K heißt *normal* genau dann, wenn jedes irreduzible Polynom $p(x) \in K[x]$, welches eine Nullstelle in L besitzt, bereits in Linearfaktoren über $L[x]$ zerfällt.

Zur Erinnerung: Ist L/K eine Körpererweiterung und $\alpha \in L$, so ist $K(\alpha)$ der kleinste Teilkörper von L, der K und α enthält. Falls $[L : K] < \infty$, so ist α algebraisch über K und es gilt $K(\alpha) = K[\alpha]$, wobei $K[\alpha]$ der kleinste Teilring von L ist der K und α enthält.

LEMMA 4.1.2. *Seien L_1/K und L_2/K endliche Körpererweiterungen mit $L_1 = K(\alpha_1)$ und $L_2 = K(\alpha_2)$. Gilt $m_{\alpha_1,K}(x) = m_{\alpha_2,K}(x)$, dann gibt es genau einen K-Isomorphismus $\varphi : L_1 \longrightarrow L_2$ mit $\varphi(\alpha_1) = \alpha_2$.*

BEWEIS. Wir benutzen Proposition 3.3.6 und erhalten

$$K(\alpha_1) = K[\alpha_1] \underbrace{\xleftarrow{\sim}}_{\varphi_1} {}^{K[x]}\!/_{\langle m_{\alpha_1,K}(x)\rangle} = {}^{K[x]}\!/_{\langle m_{\alpha_2,K}(x)\rangle} \underbrace{\xrightarrow{\sim}}_{\varphi_2} K[\alpha_2] = K(\alpha_2).$$

Somit ist $\varphi = \varphi_2 \circ \varphi_1^{-1}$ der gesuchte K-Isomorphismus. Die Eindeutigkeit ist klar, da sich jedes Element aus $L_1 = K(\alpha_1)$ als Linearkombination von Elementen aus K und Potenzen von α_1 schreiben lässt. Damit ist φ eindeutig durch das Bild von α_1 bestimmt. □

LEMMA 4.1.3. *Seien L_1/K und L_2/K Körpererweiterungen und $\varphi : L_1 \longrightarrow L_2$ ein K-Homomorphismus. Für $p(x) \in K[x]$ werden die Nullstellen von $p(x)$ in L_1 durch φ injektiv auf die Nullstellen von $p(x)$ in L_2 abgebildet. Falls $L_1 = L_2$, dann permutiert φ die Nullstellen von $p(x)$ in $L_1 = L_2$*

BEWEIS. Folgt aus Proposition 3.4.1 und den Tatsachen, dass φ injektiv ist und eine Selbstinjektion einer endlichen Menge bereits bijektiv ist. □

PROPOSITION 4.1.4. *Die Körpererweiterung L/K sei endlich. Dann sind folgende Aussagen äquivalent:*

(a) *L/K ist normal*
(b) *L ist Zerfällungskörper eines Polynoms $f(x) \in K[x]$*

BEWEIS. Wir beweisen die beiden nötigen Inklusionen.

(a) $\Rightarrow$ (b): Weil L/K endlich ist, gibt es Elemente $\alpha_1, \ldots, \alpha_r \in L$ mit $L = K(\alpha_1, \ldots, \alpha_r)$. Wir können z.B. eine K-Basis des endlich dimensionalen (beachte die Definition von $[L : K]$) K-Vektorraumes L wählen.

Seien nun $f_i \in K[x]$ die Minimalpolynome der Elemente α_i für alle $i \in \{1, \ldots, r\}$. Jedes dieser $f_i \in K[x]$ hat eine Nullstelle in L und L/K ist normal. Also zerfallen alle f_i - und somit auch $f = f_1 \cdots f_r$ - in Linearfaktoren über $L[x]$. Sei Z der Zerfällungskörper von f über K. Wir wissen, dass L alle Nullstellen von f enthält. Somit gilt $Z \subseteq L$. Auf der anderen Seite wird L bereits von den Nullstellen $\alpha_1, \ldots, \alpha_r$ erzeugt. Somit gilt auch $L \subseteq Z$ und somit $L = Z$, was zu zeigen war.

(b) $\Rightarrow$ (a): Sei nun L der Zerfällungskörper von $f(x) \in K[x]$, d.h.

$$f(x) = a_n(x - \gamma_1) \cdot \ldots \cdot (x - \gamma_n)$$

für $\gamma_1, \ldots, \gamma_n \in L$ und $L = K(\gamma_1, \ldots, \gamma_n)$. Wähle ein beliebiges irreduzibles $p(x) \in K[x]$, welches eine Nullstelle in L enthält. Wir müssen zeigen, dass p über $L[x]$ in Linearfaktoren zerfällt.

Sei Z der Zerfällungskörper von p über L. Dann ist also $Z = L(\beta_1, \ldots, \beta_r)$, mit $p(x) = b_r(x - \beta_1) \cdots (x - \beta_r)$, und oBdA $\beta_1 \in L$. Um den Beweis zu beenden müssen wir zeigen, dass $\beta_i \in L$ für alle $i \in \{1, \ldots, r\}$. Multiplikation mit Einheiten in $K[x]$ verändert weder die Irredzibilität von p noch die Nullstellen von p. Damit wissen wir, dass $(x-\beta_1) \cdots (x-\beta_r)$ das Minimalpolynom von jedem β_i, $i \in \{1, \ldots, r\}$, ist. Also dürfen wir Lemma 4.1.2 anwenden. Dieses besagt, dass es für jedes β_i genau einen K-Isomorphismus

$$\varphi : K(\beta_1) \longrightarrow K(\beta_i) \text{ mit } \varphi(\beta_1) = \beta_i$$

gibt. Nun ist L der Zerfällungskörper von $f(x)$ als Polynom im Ring $K(\beta_1)[x]$. Weiter ist $L(\beta_i) = K(\gamma_1, \ldots, \gamma_n, \beta_i)$ der Zerfällungskörper von $f(x)$ als Polynom in $K(\beta_i)[x]$. Nach Satz 3.4.5 ist der Zerfällungskörper bis auf K-Isomorphie eindeutig bestimmt und damit gibt es eine Fortsetzung von φ zu einem K-Isomorphismus

$L = L(\beta_1) \xrightarrow{\sim} L(\beta_i)$. Nach der Gradformel gilt

$$[L : K] = [L(\beta_i) : K] = [L(\beta_i) : L][L : K]$$

und somit $[L(\beta_i) : L] = 1$. Dies bedeutet gerade $\beta_i \in L$.

□

KOROLLAR 4.1.5. *Sei L/K eine endliche Körpererweiterung. Dann existiert eine endliche Körpererweiterung F/L so, dass F/K normal ist.*

BEWEIS. Wie eben setzen wir $L = K(\alpha_1, \ldots, \alpha_r)$, $f_i(x) = m_{\alpha_i,K}(x)$ für alle $i \in \{1, \ldots, r\}$ und $f = f_1 \cdots f_r$. Wir betrachten den Zerfällungskörper F von $f := f_1 \cdots f_r$ über L. Damit haben wir die endlichen Körpererweiterungen

$$K \subseteq L \subseteq F.$$

Wir müssen zeigen, dass F auch der Zerfällungskörper von f über K ist. Seien dazu $\alpha_1, \ldots, \alpha_s$ alle Nullstellen von f in F. (Da $\alpha_1, \ldots, \alpha_r$ Nullstellen von f sind, dürfen wir tatsächlich dieselbe Notation benutzen). Damit gilt

$$F = L(\alpha_1, \ldots, \alpha_s) = L(\alpha_{r+1}, \ldots, \alpha_s) \tag{7}$$

$$= K(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_s) = K(\alpha_1, \ldots, \alpha_s). \tag{8}$$

Also ist F/K tatsächlich ein Zerfällungskörper und mit Proposition 4.1.4 ist F/K normal. □

KOROLLAR 4.1.6. *Sei L/K eine endliche normale Körpererweiterung und F ein Körper mit $K \subseteq F \subseteq L$. Dann ist auch L/F normal.*

BEWEIS. Mit Proposition 4.1.4 existiert ein Polynom $f \in K[x]$, so dass L der Zerfällungskörper von f über K ist. Natürlich ist f auch ein Element aus $F[x]$ und somit ist L erst recht der Zerfällungskörper von f über F. Wieder mit Proposition 4.1.4 schließen wir, dass L/F normal ist. □

4.2. Separable Körpererweiterungen

Wir wollen Polynome $f(x) \in K[x]$, wobei wie immer K ein Körper ist, klassifizieren hinsichtlich der Eigenschaft ob f eine mehrfache Nullstelle besitzt oder nicht. Ist dies nicht der Fall so nennen wir f separabel. Wir werden im folgenden sehen, dass diese unscheinbare Eigenschaft eines Polynoms tiefreichende Auswirkungen auf die Theorie der Körpererweiterungen hat.

DEFINITION 4.2.1. Sei L/K eine Körpererweiterung.

- Ein Polynom $f(x) \in K[x] \setminus K$ heißt *separabel* $\iff$ $f(x)$ hat nur einfache Nullstellen in seinem Zerfällungskörper über K.

- $\alpha \in L$ heißt *separabel* über $K \iff$ das Minimalpolynom von α über K ist separabel.
- L/K heißt *separabel* $\iff$ jedes $\alpha \in L$ ist separabel über K.
- Der Körper K heißt *vollkommen* $\iff$ jede algebraische Körpererweiterung von K ist separabel.

Die 'meisten' endlichen Körpererweiterungen sind separabel, wie wir bald sehen werden.
Für $f, g \in K[x]$ und eine beliebige Körpererweiterung L/K schreiben wir $\mathrm{ggT}_{L[x]}(f,g)$ für den normierten größten gemeinsamen Teiler von f und g im Ring $L[x]$.

LEMMA 4.2.2. *Mit obigen Notationen gilt* $\mathrm{ggT}_{L[x]}(f,g) = \mathrm{ggT}_{K[x]}(f,g)$.

BEWEIS. Da $K[x] \subseteq L[x]$, gilt natürlich $\mathrm{ggT}_{K[x]}(f,g) \mid \mathrm{ggT}_{L[x]}(f,g)$. Sowohl $K[x]$ als auch $L[x]$ ist ein Hauptidealbereich. Daher existieren $a, b \in K[x]$ mit $\mathrm{ggT}_{K[x]}(f,g) = \underbrace{af+bg}_{\in \mathrm{ggT}_{L[x]}(f,g)L[x]}$. Es ist also $\mathrm{ggT}_{K[x]}(f,g)$ ein Element in Hauptideal $\mathrm{ggT}_{L[x]}(f,g)L[x]$. Das bedeutet nichts anderes als dass $\mathrm{ggT}_{L[x]}(f,g) \mid \mathrm{ggT}_{K[x]}(f,g)$ gilt. Da beide ggT's normiert sind, folgt die gewünschte Gleichheit. □

Für ein Polynom $f(x) = a_d x^d + \ldots + a_0 \in K[x]$ ist die *formale Ableitung* gegeben durch das Polynom $f'(x) = da_d^{d-1} + (d-1)a_{d-1}^{d-2} + \ldots + a_1 \in K[x]$. Dies entspricht genau genau der Ableitung einer polynomiellen Funktion über $\mathbb{R}$, und es folgt genau wie in der Schule, dass für die formale Ableitung die Ketten- und Produktformel glt.

LEMMA 4.2.3. *Sei $f(x) \in K[x] \setminus K$ und f' die formale Ableitung von f. Dann gilt:*

(a) *f separabel $\implies f' \neq 0 \in K[x]$*
(b) *Falls f irreduzibel in $K[x]$, dann gilt auch die Umkehrung in (a). D.h.: f separabel $\iff f' \neq 0$.*

BEWEIS. Sei L/K der Zerfällungskörper von $f \in K[x]$. Dann können wir f schreiben als $f(x) = (x-\alpha_1)^{v_1} \cdots (x-\alpha_r)^{v_r}$ mit paarweise verschiedenen Elementen $\alpha_1, \ldots \alpha_r \in L$. Mit der Produktregel sehen wir sofort, dass α_i genau dann eine Nullstelle von f' ist falls $v_r > 1$ gilt. Insbesondere ist damit f separabel, genau dann wenn $\mathrm{ggT}_{L[x]}(f,f')$ keine Nullstellen besitzt. Nun gilt aber $\mathrm{ggT}_{L[x]}(f,f') \mid f$ und f zerfällt per Konstruktion von L in $L[x]$ in Linearfaktoren. Also gilt

$$f\text{separabel} \iff 1 = \mathrm{ggT}_{L[x]}(f, f') \overset{4.2.2}{=} \mathrm{ggT}_{K[x]}(f, f') \tag{9}$$

Also ist für ein separables $f \in K[x] \setminus K$, die Ableitung $f' \neq 0$, da sonst $1 = \mathrm{ggT}_{K[x]}(f, f') = \mathrm{ggT}_{K[x]}(f, 0) = f \notin K$ wäre. Dies beweist (a).
Es bleibt also zu zeigen, dass unter der Voraussetzung f irreduzibel auch $f' \neq 0 \Longrightarrow f$ *separabel* folgt. Sei also $f \in K[x] \setminus K$ irreduzibel und $f' \neq 0$. Aus der Irreduzibilität von f folgt dann, dass entweder $\mathrm{ggT}_{K[x]}(f, f') = 1$ oder $\mathrm{ggT}_{K[x]}(f, f') = a_d^{-1} f$ gilt, wobei a_d den Leitkoeffizienten von f bezeichnet (Beachte, dass der ggT stets normiert ist). Nun gilt

$$\mathrm{ggT}_{K[x]}(f, f') \overset{f' \neq 0}{\leq} \mathrm{grad}(f') < \mathrm{grad}(f).$$

Damit ist $\mathrm{ggT}_{K[x]}(f, f') = a_d^{-1} f$ nicht möglich. Es ist also $\mathrm{ggT}_{K[x]}(f, f') = 1$ und mit (9) folgt, dass f separabel ist. □

Proposition 4.2.4. *Der Körper K ist vollkommen falls*

(a) $\mathrm{char}(K) = 0$ *oder*
(b) $|K| < \infty$.

Beweis. Übung. □

Beispiel 4.2.5. Mit den intuitiven Rechenverfahren ist ein nicht-konstantes Polynom dessen Ableitung verschwindet schwer vorstellbar. Ist jedoch $K = \mathbb{Z}/p\mathbb{Z}$ und $f(x) = x^p + 1$, so ist $f'(x) = px = 0 \in K$. Wir wissen aus Proposition 4.2.4, dass K vollkommen ist. Also kann f nicht irreduzibel sein. Die Zerlegung von f in irreduzible Faktoren ist mit Hilfe des Frobenius-Homomorphismuses schnell gefunden. Es gilt $f(X) = x^p + 1 = (x + 1)^p$.

Definition 4.2.6. Eine Körpererweiterung L/K heißt *einfach* falls ein $\alpha \in L$ existiert mit $L = K(\alpha)$. Ein solches α heißt *primitives Element* von L/K.

Satz 4.2.7 (Satz vom primitiven Element). *Sei L/K eine endliche separable Körpererweiterung, dann ist L/K einfach. D.h. es existiert ein $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Wir betrachten zunächst den Fall, dass K endlich ist. Dann ist auch der endlich dimensionale K-Vektorraum L endlich. Genauer gilt: $|L| = |K|^{[L:K]}$. Also ist die multiplikative Gruppe L^* von L zyklisch, wie in den Übungen gezeigt wurde. Das heißt, es ist $L^* = \langle \alpha \rangle$ für ein $\alpha \in L$. Insbesondere ist somit $L = K(\alpha)$ was zu zeigen war.

Sei im Folgenden K ein Körper mit unendlich vielen Elementen. Da $[L : K] < \infty$, gilt $L = K(\alpha_1, \ldots, \alpha_r)$ für Elemente $\alpha_1, \ldots, \alpha_r \in L$ (wir können

zum Beispiel Basiselemente des endlichen K-Vektorraums L wählen). Wir benutzen Induktion nach r, wobei wir für $r = 1$ bereits fertig sind.
Für $r \geq 2$ gilt nach Induktionsvoraussetzung

$$L = K(\alpha_1, \ldots, \alpha_r) = K(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r) = K(\beta, \alpha_r).$$

Es genügt also den Fall $r = 2$ zu beweisen, mit $\alpha_1 = \beta, \alpha_2 = \gamma$.
Mit 4.1.5 existiert eine normale Körpererweiterung F/K mit $K(\beta, \gamma) \subseteq F$. Da *beta* und γ Elemente von F sind, zerfallen die jeweiligen Minimalpolynome in $F[x]$ in Linearfaktoren. D.h.:

$$m_{\beta,K}(x) = (x - \beta_1) \cdots (x - \beta_n) \in F[x] \text{ , mit } \beta_1 = \beta$$
$$m_{\gamma,K}(x) = (x - \gamma_1) \cdots (x - \gamma_m) \in F[x] \text{ , mit } \gamma_1 = \gamma.$$

Da L/K separabel ist, gilt $\beta_i \neq \beta_j$ und $\gamma_k \neq \gamma_l$ für alle $i \neq j$ und für alle $k \neq l$. Also besitzt die Gleichung $\beta_1 + z\gamma_1 = \beta_i + z\gamma_j$ für alle $i \in \{1, \ldots, n\}$ und alle $j \in \{2, \ldots, m\}$ genau eine Lösung. Wir wissen, dass $|K| = \infty$ gilt, also existiert ein $c \in K$ mit

$$\beta_i + c\gamma_j \neq \beta_1 + c\gamma_1 \qquad \forall i = 1, \ldots, n, \forall j = 2, \ldots, m. \tag{10}$$

Nun wollen wir zeigen, dass $\alpha = \beta + c\gamma$ ein primitives Element der Körpererweiterung $K(\beta, \gamma)/K$ ist. Dazu betrachten wir das Polynom $m_{\beta,K}(\alpha - cx) \in K(\alpha)[x]$. Für ein γ_i gilt

$$\begin{aligned} m_{\beta,K}(\alpha - c\gamma_i) = 0 &\iff \alpha - c\gamma_i = \beta_j \text{ für ein } j \in \{1, \ldots, n\} \\ &\iff \beta_1 + c\gamma_1 = \beta_j + c\gamma_i \text{ für ein } j \in \{1, \ldots, n\} \\ &\overset{(10)}{\iff} \beta_j = \beta_1 = \beta \text{ und } \gamma_i = \gamma_1 = \gamma \end{aligned}$$

Also gilt

$$\begin{aligned} x - \gamma &= \mathrm{ggT}_{F[x]}(m_{\beta,K}(\alpha - cx), m_{\gamma,K}(x)) \\ &\overset{4.2.2}{=} \mathrm{ggT}_{K(\alpha)[x]}(m_{\beta,K}(\alpha - cx), m_{\gamma,K}(x)) \in K(\alpha)[x]. \end{aligned}$$

Damit ist $\gamma \in K(\alpha)$. Weiter folgt $\beta = \alpha - c\gamma \in K(\alpha)$. Also ist $K(\beta, \gamma) \subseteq K(\alpha)$ und nach Konstruktion von α gilt auch die umgekehrte Inklusion. Damit ist tatsächlich $K(\beta, \gamma) = K(\alpha)$, wie gewünscht. □

Definition 4.2.8. Sei L/K eine endliche Körpererweiterung und $F \supseteq L$ mit F/K normal.

- Mit $\mathrm{Hom}_K(L, F)$ bezeichnen wir die Menge aller K-Homomorphismen $\sigma : L \longrightarrow F$.
- Die Zahl $[L : K]_s = |Hom_K(L, F)|$ heißt der *Separabilitätsgrad von* L/K.

BEMERKUNG 4.2.9. Um den Separabilitätsgrad in 4.2.8 zu definieren mussten wir einen Körper F wählen. Damit die Definition wohldefiniert ist, müssen wir noch begründen warum $[L:K]_s$ nicht von dieser Wahl abhängt. Es ist $L = K(\alpha_1, \ldots, \alpha_r)$ für gewisse $\alpha_1, \ldots, \alpha_r \in L$. Über jedem Körper F mit F/K normal und $L \subseteq F$ zerfallen die Minimalpolynome von $\alpha_1, \ldots, \alpha_r$ in Linearfaktoren. Weiter ist jeder K-Homomorphismus von $L \longrightarrow F$ eindeutig durch die Bilder von $\alpha_1, \ldots, \alpha_r$ bestimmt und diese Bilder sind wieder Nullstellen der jeweiligen Minimalpolynome (siehe Satz 3.4.1). Damit ist $[L:K]_s$ tatsächlich unabhängig von der Wahl des Körpers F. Man kann für F somit stets einen algebraischen Abschluss von L wählen.

SATZ 4.2.10. *Seien $K \subseteq L \subseteq E$ Körper mit E/K endlich. Dann gilt (wie wir es von einem 'Grad' erwarten)*

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

BEWEIS. Sei $I = \{1, \ldots, [L:K]_s\}$ und $J = \{1, \ldots, [E:L]_s\}$ und sei F/K normal mit $F \supseteq E$. Dann ist mit Korollar 4.1.6 auch F/L normal. Wir können also schreiben

$$\mathrm{Hom}_K(L,F) = \{\varphi_i | i \in I\} \text{ und } \mathrm{Hom}_L(E,F) = \{\psi_j | j \in J\}.$$

Sei nun $\varphi_i \in \mathrm{Hom}_K(L,F)$ beliebig und F der Zerfällungskörper von $f \in L[x] \setminus \{0\}$. Da F/L normal ist, dürfen wir dies nach Proposition 4.1.4 annehmen. Es ist also $F = L(\alpha_1, \ldots, \alpha_r)$ für $\alpha_1, \ldots, \alpha_r \in L$ mit $f(x) = a_r(x-\alpha_1)\cdots(x-\alpha_r)$. Durch sukzessives Anwenden von Proposition 3.4.3 lässt sich φ_i zu einem K-Homomorphismus $\overline{\varphi_i} : F \longrightarrow F$ fortsetzen. Mit Lemma 3.2.10 ist diese Abbildung sogar ein K-Isomorphismus. Im Allgemeinen ist eine solche Fortsetzung nicht eindeutig bestimmt. Für jedes $i \in I$ fixieren wir eine Fortsetzung $\overline{\varphi_i}$.
Wir stellen fest, dass die Abbildungen $\overline{\varphi_i} \circ \psi_j : L \longrightarrow F$ Elemente aus $\mathrm{Hom}_K(E,F)$ sind für alle Tupel $(i,j) \in I \times J$.

1. Schritt: Die Elemente $\overline{\varphi_i} \circ \psi_j$, $(i,j) \in I \times J$ sind paarweise verschieden.

Sei also $\overline{\varphi_i} \circ \psi_j = \overline{\varphi_{i'}} \circ \psi_{j'}$. Da die Abbildungen ψ_j und $\psi_{j'}$ Elemente aus L nicht verändern, gilt

$$\varphi_i = \overline{\varphi_i}|_L = \overline{\varphi_i} \circ \psi_j|_L = \overline{\varphi_{i'}} \circ \psi_{j'}|_L = \overline{\varphi_{i'}}|_L = \varphi_{i'}.$$

Also $\overline{\varphi_i} \circ \psi_j = \overline{\varphi_i} \circ \psi_{j'}$. Aus der Injektivität von $\overline{\varphi_i}$ folgt somit auch $\psi_j = \psi_{j'}$. Dies beweist den ersten Schritt.

2. Schritt: Jedes $\Phi \in \mathrm{Hom}_K(E,F)$ ist von der Form $\overline{\varphi_i} \circ \psi_j$ für ein $(i,j) \in I \times J$.

Sei $\Phi \in \mathrm{Hom}_K(E,F)$ beliebig. Es ist $\Phi|_L \in \mathrm{Hom}_K(L,F)$, also ist $\Phi|_L = \varphi_i$ für ein $i \in I$. Da $\overline{\varphi_i}$ ein K-Isomorphismus ist, gibt es eine Umkehrabbildung $\overline{\varphi_i}^{-1}$ von $\overline{\varphi_i}$, die ebenfalls ein K-Isomorphismus ist. Damit ist die Abbildung $\overline{\varphi_i}^{-1} \circ \Phi : E \to F$ offensichtlich ein wohldefinierter K-Homomorphismus. Es gilt sogar

$$a \in L \Longleftrightarrow \overline{\varphi_i}^{-1}(\Phi(a)) = \overline{\varphi_i}^{-1}(\varphi_i(a)) = \overline{\varphi_i}^{-1}(\overline{\varphi_i}(a)) = a.$$

Folglich ist $\overline{\varphi_i}^{-1} \circ \Phi = \psi_j$ für ein $j \in J$. Dies bedeutet gerade (wieder da $\overline{\varphi_i}$ ein Isomorphismus ist) $\Phi = \overline{\varphi_i} \circ \psi_j$, wie gewünscht. Damit ist auch der zweite Schritt bewiesen.

Wir haben also gezeigt, dass $\mathrm{Hom}_K(E,F) = \{\overline{\varphi_i} \circ \psi_j | (i,j) \in I \times J\}$ gilt und die Elemente $\overline{\varphi_i} \circ \psi_j$ paarweise verschieden sind. Es folgt

$$[E:K]_s = |I \times J| = |I| \cdot |J| [E:L]_s \cdot [l:K]_s.$$

Dies wollten wir zeigen. □

LEMMA 4.2.11. *Sei $K(\alpha)/K$ eine einfache algebraische Körpererweiterung. Dann gilt $[K(\alpha):K]_s \leq [K(\alpha):K]$. Gleichheit gilt genau dann wenn α separabel über K ist.*

Dieses Lemma wird in der nächsten Proposition weitreichend verallgemeinert.

BEWEIS. Der Beweis ist eine Anwendung von Satz 3.4.3. Sei $m_{\alpha,K}(x) \in K[x]$ das Minimalpolynom von α über K und sei $F/K(\alpha)$ eine endliche Körpererweiterung, so dass F/K normal ist. Damit zerfällt $m_{\alpha,K}(x)$ über F in Linearfaktoren. Sei β irgendeine Nullstelle von $m_{\alpha,K}(x)$ in F. Dann existiert ein $\varphi \in \mathrm{Hom}_K(K(\alpha),F)$ mit $\varphi(\alpha) = \beta$. Ist umgekehrt $\psi \in \mathrm{Hom}_K(K(\alpha),F)$ beliebig, so ist $\psi(\alpha)$ eine Nullstelle von $m_{\alpha,K}(x)$ in F. Natürlich ist jedes Element in $\mathrm{Hom}_K(K(\alpha),F)$ eindeutig durch das Bild von α bestimmt. Es gilt also

$$\begin{aligned}[K(\alpha):K]_s &\overset{\text{Def.}}{=} |\mathrm{Hom}_K(K(\alpha),F)| = |\{\beta \in F | m_{\alpha,K}(\beta) = 0\}| \\ &\leq \mathrm{grad}(m_{\alpha,K}) = [K(\alpha):K].\end{aligned}$$

Gleichheit gilt genau dann wenn $m_{\alpha,K}(x)$ genau $\mathrm{grad}(m_{\alpha,K})$ verschiedene Nullstellen besitzt. Dies ist genau dann der Fall wenn alle Nullstellen von $m_{\alpha,K}(x)$ verschieden sind, also genau dann wenn α separabel über K ist. □

PROPOSITION 4.2.12. *Sei L/K eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

(i) *L/K ist separabel.*

(ii) *Es gibt* $\alpha_1, \ldots, \alpha_r \in L$ *separabel über* K *mit* $L = K(\alpha_1, \ldots, \alpha_r)$.
(iii) $[L : K] = [L : K]_s$.

BEWEIS. Wir beweisen dies natürlich mit einem Ringschluss $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

(i) $\Rightarrow$ (ii) Nach Satz 4.2.7 gilt sogar $L = K(\alpha)$ mit α separabel über K.

(ii) $\Rightarrow$ (iii) Wir beweisen die Aussage per Induktion nach r, wobei wir den Induktionsanfang $r = 1$ bereits in Lemma 4.2.11 gezeigt haben. Sei für den Induktionsschritt also $r \geq 2$. Dass α_r separabel über K ist, bedeutet gerade, dass $m_{\alpha_r,K}(x)$ nur einfache Nullstellen besitzt. Weiter gilt $m_{\alpha_r,K(\alpha_1,\ldots,\alpha_{r-1})}(x) \mid m_{\alpha,K}(x)$. Also ist α_r auch separabel über $K(\alpha_1, \ldots, \alpha_{r-1})$. Also können wir Lemma 4.2.11 auch auf die Körpererweiterung $L = K(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r)/K(\alpha_1, \ldots, \alpha_{r-1})$ anwenden. Benutzen wir zusätzlich die Induktionsvoraussetzung so erhalten wir

$$\begin{aligned}[L : K] &= [K(\alpha_1, \ldots, \alpha_{r-1})(\alpha) : K(\alpha_1, \ldots, \alpha_{r-1})] \cdot [K(\alpha_1, \ldots, \alpha_{r-1}) : K] \\ &\overset{4.2.11+\mathrm{IV}}{=} [K(\alpha_1, \ldots, \alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})]_s \cdot [K(\alpha_1, \ldots, \alpha_{r-1}) : K]_s \\ &\overset{4.2.10}{=} [L : K]_s.\end{aligned}$$

Dies ist genau die Gleichung, die wir zeigen wollten.

(iii) $\Rightarrow$ (i) Wir beweisen die Kontraposition. Sei also $\alpha \in L$ inseparabel (d.h. nicht-separabel) über K. Mit Lemma 4.2.11 wissen wir $[K(\alpha) : K]_s < [K(\alpha) : K]$. Die Erweiterung $L/K(\alpha)$ ist endlich. Es existieren also $\alpha_1, \ldots, \alpha_r \in L$ mit $L = K(\alpha)(\alpha_1, \ldots, \alpha_r)$. Mit Hilfe der Gradformel schreiben wir

$$\begin{aligned}&[L : K] \\ &= \underbrace{[K(\alpha)(\alpha_1, \ldots, \alpha_r) : K(\alpha)(\alpha_1, \ldots, \alpha_{r-1})]}_{\geq [L:K(\alpha)(\alpha_1,\ldots,\alpha_{r-1})]_s} \cdots \underbrace{[K(\alpha) : K]}_{> [K(\alpha):K]_s} \\ &\overset{4.2.10}{>} [L : K]_s.\end{aligned}$$

Diese Ungleichung war zu zeigen.

□

KOROLLAR 4.2.13. *Seien* $K \subseteq L \subseteq E$ *Körper mit* E/K *endlich. Dann gilt*

$$E/K \text{ separabel} \iff L/K \text{ und } E/L \text{ sind separabel.}$$

BEWEIS. Übung. □

LEMMA 4.2.14. *Seien* L/K *eine separable Körpererweiterung und* F *ein Zwischenkörper von* L/K. *Dann sind auch* L/F *und* F/K *separabel.*

BEWEIS. Da $F \subseteq L$ ist, ist F/K separabel. Sei nun $\alpha \in L$ beliebg, dann ist $m_{\alpha,K}(x) \in F[x]$ ein Polynom mit $m_{\alpha,K}(\alpha) = 0$. Mit Proposition 3.3.4 folgt, $m_{\alpha,F}(x) \mid m_{\alpha,K}(x)$. Das Minimalpolynom von α über K hat nach Voraussetzung nur einfache Nullstellen. Damit hat auch jeder Teiler, insbesondere $m_{\alpha,F}(x)$ nur einfache Nullstellen. Das bedeutet α ist separabel über F. □

PROPOSITION 4.2.15. *Sei* $\mathrm{char}(K) = p > 0$ *und* L/K *eine endliche Körpererweiterung mit* $p \nmid [L : K]$. *Dann ist* L/K *separabel.*

BEWEIS. Sei L/K wie in den Voraussetzungen und $\alpha \in L$ beliebig. Wie in den Übungen gesehen existiert ein maximales $r \in \mathbb{N}_0$ mit $m_{\alpha,K}(x) = g(x^{p^r})$ für ein $g(x) \in K[x]$. Weiter wurde gezeigt, dass dieses (eindeutig bestimmte) g separabel ist. Mit der Gradformel sehen wir

$$[K(\alpha) : K] = \mathrm{grad}(m_{\alpha,K}) = p^r \,\mathrm{grad}(g) \mid [L : K].$$

Da p aber kein Teiler von $[L : K]$ ist, muss $r = 0$ gelten. D.h.: $m_{\alpha,K}(x) = g(x)$ ist separabel. □

4.3. Galois-Theorie

Sei ab jetzt stets L/K eine endliche Körpererweiterung. Im Allgemeinen ist es aufwendig alle Zwischenkörper dieser Körpererweiterung anzugeben, zumindest dann wenn die Körper unendlich viele Elemente besitzen. Unter milden Voraussetzungen an L/K werden wir in diesem Abschnitt das Problem darauf reduzieren alle Untergruppen der endlichen *Automorphismengruppe* von L/K zu finden. Dies ist deutlich einfacher und kann im Zweifelsfall sogar kombinatorisch gelöst werden. Diese Theorie hat viele Anwendungen und wir werden zwei der bekanntesten (Konstruierbarkeit mit Zirkel und Lineal, und Auflösbarkeit von polynomialen Gleichungen) in späteren Kapiteln studieren. Die Hauptidee der Theorie stammt von Evariste Galois.

ABBILDUNG 4.1. *Evariste Galois* (1811-1832) war ein französischer Mathematiker. Er scheiterte zweimal an der Aufnahmeprüfung der *École polytechnique* und war, als überzeugter Republikaner, zweimal im Gefängnis. Auch wurde seine Arbeit, aufgrund von mangelhafter Äußerer Form, nicht publiziert. Er starb unter rätselhaften Umständen (möglicherweise als passiver Selbstmord) im Duell mit einem bakannten französischen Schützen. Erst einige Jahre nach seinem Tod wurde die Bedeutung seiner Ideen erkannt.

DEFINITION 4.3.1. Eine endliche Körpererweiterung L/K heißt *Galoiserweiterung* $\iff L/K$ ist separabel und normal. In diesem Fall nennen wir $\mathrm{Aut}(L/K) = \{\varphi : L \longrightarrow L | \varphi \ K\text{-Isomorphismus }\} = \mathrm{Gal}(L/K)$ die *Galoisgruppe* von L/K. Die Gruppenstruktur ist hierbei durch die Hintereinanderausführung gegeben.

NOTATION 4.3.2. Sei L/K eine Körpererweiterung und S eine Teilmenge von $\mathrm{Aut}(L/K)$. Dann bezeichnet

$$L^S := \{\alpha \in L | \sigma(\alpha) = \alpha \ \forall \sigma \in S\}$$

den *Fixkörper* von S. Beachte, dass für jede solche Menge S die Menge L^S mit den von L vererbten Verknüpfungen tatsächlich einen Körper bildet.

LEMMA 4.3.3. *Sei L/K eine endliche Körpererweiterung. Dann gilt die Ungleichung $|\mathrm{Aut}(L/K)| \leq [L : K]$.*

BEWEIS. Sei F/K normal mit $L \subseteq F$. Dann ist $\mathrm{Aut}(L/K) \subseteq \mathrm{Hom}_K(L, F)$. Insbesondere gilt also $|\mathrm{Aut}(L/K)| \leq [L : K]_s \overset{\text{Übung}}{\leq} [L : K]$. □

THEOREM 4.3.4. *Sei L/K eine endliche separable Körpererweiterung. Dann sind folgende Aussagen äquivalent*

(i) *L/K ist normal*
(ii) $|\mathrm{Aut}(L/K)| = [L : K]$
(iii) $L^{\mathrm{Aut}(L/K)} = K$

BEWEIS. Wir beweisen dies per Ringschluss

(i) $\Rightarrow$ (ii) Nach Proposition 4.2.12 wissen wir bereits $[L : K]_s = |\mathrm{Hom}_K(L, L)| = [L : K]$. Mit Lemma 3.2.10 folgt Aussage (*ii*) unmittelbar.

(ii) $\Rightarrow$ (iii) Es gelte also $|\mathrm{Aut}(L/K)| = [L : K]$. Wir definieren den Zwischenkörper $F := L^{\mathrm{Aut}(L/K)}$. Da $K \subseteq F$, ist jeder F-Automporhismus von L insbesondere ein K-Automorphismus von L (d.h.: $\mathrm{Aut}(L/F) \subseteq \mathrm{Aut}(L/K)$). Wir wollen zeigen, dass auch die Rückrichtung gilt. Sei dafür $\varphi \in \mathrm{Aut}(L/K)$ beliebig. Dann ist $\varphi(\alpha) = \alpha \ \forall \alpha \in F = L^{\mathrm{Aut}(L/K)}$, nach der Definition des Fixkörpers. Also ist $\varphi|_F = \mathrm{id}_F$ und somit $\mathrm{Aut}(L/K) = \mathrm{Aut}(L/F)$. Es folgt

$$[L : K] \overset{\text{Vor.}}{=} |\mathrm{Aut}(L/K)| = |\mathrm{Aut}(L/F)| \overset{4.3.3}{\leq} [L : F]. \tag{11}$$

Dabei benutzen wir 4.3.3 für F statt K und beachten, dass L/F ebenfalls separabel ist nach 4.2.14. Benutzen wir die Gradformel, so erhalten wir $[L : K] = [L : F] \cdot [F : K]$. Aus (11) folgt somit $[L : K] = [L : F]$ und $[F : K] = 1$. Also folgt $L^{\mathrm{Aut}(L/K)} = F = K$. Dies zeigt (*iii*).

(iii) $\Rightarrow$ (i) Sei nun $L^{\mathrm{Aut}(L/K)} = K$. Der Satz vom primitiven Element liefert ein $\alpha \in L$ mit $L = K(\alpha)$. Wir wollen zeigen, dass L ein Zerfällungskörper vom Minimalpolynom $m_{\alpha,K}(x) \in K[x]$ ist. Natürlich ist L in diesem Zerfällungskörper enthalten.

Wir betrachten das Polynom $q(x) = \prod_{\sigma \in \mathrm{Aut}(L/K)}(x - \sigma(\alpha)) \in L[x]$. Das Polynom $q(x)$ zerfällt über L in Linearfaktoren und es gilt

$$n := \mathrm{grad}(q) = |\operatorname{Aut}(L/K)| \overset{4.3.3}{\leq} [L : K] \overset{3.3.7}{=} \mathrm{grad}(m_{\alpha,K}).$$

Sei $\tau \in \mathrm{Aut}(L/K)$ beliebig. Da $\mathrm{Aut}(L/K)$ eine Gruppe ist, permutiert die Verknüpfung mit τ die Elemente dieser Gruppe. Bezeichnen wir mit $\tilde{\tau}$ die eindeutige Fortsetzung von τ auf den Polynomring $L[x]$, mit $\tilde{\tau}(x) = x$, so erhalten wir

$$\tilde{\tau}(q(x)) = \prod_{\sigma \in \mathrm{Aut}(L/K)} (x - \tau \circ \sigma(\alpha)) = q(x) \in K[x].$$

Insbesondere bedeutet dies, dass τ alle Koeffizienten von q fixiert. Da τ beliebig gewählt war, ist q über $L^{\mathrm{Aut}(L/K)} \overset{\text{Vor.}}{=} K$ definiert. Damit ist $q(x) \in K[x] \setminus \{0\}$, $\mathrm{grad}(q) \leq \mathrm{grad}(m_{\alpha,K})$ und $q(\alpha) = 0$. Also ist $q(x)$ das Minimalpolynom von α.

Die Elemente $\sigma(\alpha)$, $\sigma \in \mathrm{Aut}(L/K)$, liegen alle in L. Damit ist $L = K(\alpha)$ ein Zerfällungskörper von $m_{\alpha,K}$ und nach Proposition 4.1.4 ist L/K normal. Dies beendet den Beweis.

□

Satz 4.3.5. *Sei L/K eine endliche und separable Körpererweiterung und sei H eine Untergruppe von* $\mathrm{Aut}(L/K)$. *Dann ist L/L^H eine Galoiserweiterung mit* $\mathrm{Gal}(L/L^H) = H$.

Beweis. Als Zwischenkörper von L/K ist auch L/L^H separabel (siehe Korollar 4.2.13). Mit dem Satz vom primitiven Element existiert ein $\alpha \in L$ mit $L = K(\alpha)$. Damit ist natürlich auch $L = L^H(\alpha)$. Im Beweis von Theorem 4.3.4 wurde gezeigt

$$q(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \in L^H[x] \text{ und } q(\alpha) = 0.$$

Es folgt, dass $m_{\alpha,L^H}(x) \mid q(x)$ gilt. Also ist

$$[L : L^H] = \mathrm{grad}(m_{\alpha,L^H}) \leq \mathrm{grad}(q) = |H|.$$

Andererseits gilt per Definition des Fixkörpers L^H, dass $H \subseteq \mathrm{Aut}(L/L^H)$ gilt. Damit erhalten wir

$$|H| \leq |\operatorname{Aut}(L/L^H)| \overset{4.3.3}{\leq} [L : L^H].$$

Es gilt also überall Gleichheit in dieser Ungleichungskette, woraus $H = \mathrm{Aut}(L/L^H)$ folgt. Nach Theorem 4.3.4 ist damit L/L^H normal und somit auch eine Galoiserweiterung. □

Beispiel 4.3.6. (a) $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, für $m \in \mathbb{Z}$, ist eine Galoiserweiterung, denn: $\mathbb{Q}(\sqrt{m})$ ist der Zerfällungskörper von $x^2 - m \in \mathbb{Q}[x]$, also ist $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ normal und die Separabilität folgt aus $\mathrm{char}(\mathbb{Q}) = 0$. Weiter ist $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] \leq \mathrm{grad}(x^2 - m) = 2$ und somit besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ aus maximal 2 Elementen und ist daher isomorph zu $\mathbb{Z}/2\mathbb{Z}$ oder trivial.

(b) Wir betrachten die Körpererweiterung $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Als endliche Körpererweiterung von $\mathbb{Q}$ ist $L/\mathbb{Q}$ separabel. Aus den übungen wissen wir bereits $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und $[L : \mathbb{Q}] = 4$. Für jeden $\mathbb{Q}$-Homomorphismus σ und jedes $m \in \mathbb{Q}$ gilt $\sigma(\sqrt{m})^2 = \sigma(\sqrt{m}^2) = \sigma(m) = m$. Also ist stets $\sigma(\sqrt{m}) \in \{\pm\sqrt{m}\}$. Die möglichen Bilder von $\sqrt{2}+\sqrt{3}$ unter einem Element aus $\mathrm{Aut}(L/\mathbb{Q})$ sind also $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ und $-\sqrt{2}-\sqrt{3}$. Wie im Beweis von Theorem 4.3.4 setzten wir

$$\begin{aligned} q(x) &= (x - (\sqrt{2} + \sqrt{3})) \cdot (x - (-\sqrt{2} - \sqrt{3})) \\ &\quad \cdot (x - (\sqrt{2} - \sqrt{3})) \cdot (x - (-\sqrt{2} + \sqrt{3})) \\ &= x^4 - 10x^2 + 1 \in \mathbb{Q}[x]. \end{aligned}$$

Das Polynom $q(x)$ ist also über $\mathbb{Q}$ definiert und besitzt $\sqrt{2} + \sqrt{3}$ als Nullstelle. Weiter ist $\mathrm{grad}(q) = 4 = [L : \mathbb{Q}] = \mathrm{grad}(m_{\sqrt{2}+\sqrt{3},\mathbb{Q}})$. Damit ist q das Minimalpolynom von $\sqrt{2}+\sqrt{3}$. Weiter ist jede Nullstelle von q enthalten in L und somit ist L der Zerfällungskörper von q. Als solcher ist $L/\mathbb{Q}$ auch eine normale also eine Galoiserweiterung.

Wir wollen in einer gegebenen endlichen Galoiserweiterung L/K (d.h. L/K ist normal und separabel) alle Zwischenkörper finden. Dieses Problem wird durch den nächsten Satz darauf reduziert alle Untergruppen der endlichen Gruppe $\mathrm{Gal}(L/K)$ zu finden.

Theorem 4.3.7 (Hauptsatz der Galoistheorie). *Sei L/K eine Galoiserweiterung. Dann bilden die folgenden Abbildungen eine bijektive Korrespondenz*

$$\{\textit{Untergruppen von } \mathrm{Gal}(L/K)\} \overset{H \mapsto L^H}{\longrightarrow} \{\textit{Zwischenkörper von } L/K\}$$

$$\{\textit{Zwischenkörper von } L/K\} \overset{F \mapsto \mathrm{Aut}(L/F)}{\longrightarrow} \{\textit{Untergruppen von } \mathrm{Gal}(L/K)\}$$

BEWEIS. Sei zunächst H eine Untergruppe von $\mathrm{Gal}(L/K)$. Dann ist L^H ein Zwischenkörper von L/K und somit ist die erste Abbildung wohldefiniert. Nach Satz 4.3.5 gilt wie gewünscht

$$H \mapsto L^H \mapsto \mathrm{Aut}(L/L^H) = H.$$

Umgekehrt sei F ein Zwischenkörper von L/K. Dann ist jedes Element in $\mathrm{Aut}(L/F)$ insbesondere ein Element in $\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$. Also ist $\mathrm{Aut}(L/F)$ tatsächlich eine Untergruppe von $\mathrm{Gal}(L/K)$. Nach Korollar 4.2.13 ist L/F separabel. Weiter ist mit L/K erst recht auch L/F normal und somit ist L/F eine Galoiserweiterung. Mit Theorem 4.3.4 gilt nun

$$F \mapsto \mathrm{Aut}(L/F) \mapsto L^{\mathrm{Aut}(L/F)} = F.$$

Wir haben also gezeigt, dass die Abbildungen aus dem Theorem gegenseitige Umkehrabbildungen sind. Insbesondere sind sie damit bijektiv. □

Die folgenden Eigenschaften folgen aus dem eben bewiesenen Hauptsatz.

PROPOSITION 4.3.8. *Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Seien weiter H, H_1, H_2 Untergruppen von G, und F ein Zwischenkörper von L/K. Dann gilt*

(a) $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$
(b) $|H| = [L : L^H]$ *und* $[G : H] = [L^H : K]$
(c) L/F *ist eine Galoiserweiterung*
(d) $\sigma \in G \implies \mathrm{Gal}(L/\sigma(F)) = \sigma\,\mathrm{Gal}(L/F)\sigma^{-1}$
(e) $\sigma \in G \implies L^{\sigma H \sigma^{-1}} = \sigma(L^H)$
(f) $H \lhd G \iff L^H/K$ *ist eine Galoiserweiterung*
(g) $H \lhd G \implies \mathrm{Gal}(L^H/K) \cong G/H$

BEWEIS. Übung. □

LEMMA 4.3.9. *Sei L/K eine Galoiserweiterung und $f \in K[x] \setminus K$ so, dass L der Zerfällungskörper von f über K ist. Dann ist* $\mathrm{Gal}(L/K)$ *isomorph zu einer Untergruppe der symmetrischen Gruppe S_n, mit $n = \mathrm{grad}(f)$.*

BEWEIS. Zunächst halten wir fest, dass ein solches Polynom f existiert, da L/K normal ist (siehe Theorem 4.1.4). Wir wissen bereits, dass jedes $\varphi \in \mathrm{Gal}(L/K)$ die Nullstellen von $f(x)$ permutiert. Da L/K separabel ist, gibt es genau $n = \mathrm{grad}(f)$ verschiedene Nullstellen von f in L. Bezeichne diese Menge von Nullstellen von f mit Z, dann gilt $L = K(Z)$. Bezeichnen wir mit $\mathrm{Per}(Z)$ die Permutationsgruppe der Elemente von Z (beachte $\mathrm{Per}(Z) \cong S_n$), so ist die Abbildung

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Per}(Z) \quad ; \quad \varphi \mapsto \varphi|_Z$$

ein wohldefinierter Gruppen-Homomorphismus. Dies ist klar, da die Verknüpfungen in beiden Gruppen die identische Hintereinanderausführung von Abbildungen ist. Weiterhin ist die Abbildung injektiv, da φ eindeutig durch die Bilder der Elemente aus Z bestimmt ist. Also lässt sich $\mathrm{Gal}(L/K)$ injektiv in $\mathrm{Per}(Z) \cong S_n$ einbetten, was zu zeigen war. □

Beispiel 4.3.10. Sei $K = \mathbb{Q}$ und L der Zerfällungskörper von $p(x) = x^3 - 5$. Wir wollen nun alle Zwischenkörper F von L/K bestimmen. Hierfür möchten wir Galoistheorie benutzen und stellen dazu zunächst fest, dass L/K tatsächlich eine Galoiserweiterung ist. Denn L/K ist als endliche Erweiterung eines Körpers der Charakteristik 0 separabel (siehe Proposition 4.2.4) und als Zerfällungskörper eines Polynoms in $K[x]$ ist L/K auch normal (siehe Proposition 4.1.4).
Die Nullstellen von $x^3 - 5$ sind gegeben durch $\alpha_1 = \sqrt[3]{5} \in \mathbb{R}$, $\alpha_2 = \zeta_3 \sqrt[3]{5}$ und $\alpha_3 = \zeta_3^2 \sqrt[3]{5}$, wobei $\zeta_3 = e^{2\pi i/3} \in \mathbb{C}$ eine 3-te Einheitswurzel ist. (D.h.: $\zeta_3 \notin \mathbb{R}$ und $\zeta_3^3 = 1$.)
Der Zerfällungskörper L von $x^3 - 5 \in \mathbb{Q}[x]$ ist also gegeben durch $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Wir wollen L schreiben als Körper der nur von zwei Elementen erzeugt wird. Dazu stellen wir fest, dass $\zeta_3 = \frac{\alpha_2}{\alpha_1} = \frac{\alpha_3}{\alpha_2} \in L$ gilt. Weiter sind α_1, α_2, $\alpha_3 \in \mathbb{Q}(\zeta_3, \sqrt[3]{5})$. Es folgt $L = \mathbb{Q}(\zeta_3, \sqrt[3]{5})$, denn es genügt zu zeigen, dass die jeweiligen Erzeugendenelemente im anderen Körper liegen.
Um den Hauptsatz der Galoistheorie anwenden zu können, müssen wir die Galoisgruppe $\mathrm{Gal}(L/K)$ bestimmen. Das Polynom $x^3 - 5 \in \mathbb{Q}[x]$ ist irreduzibel nach dem Eisensteinschen Irreduzibilitätskriterium. Damit folgt

$$[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = \mathrm{grad}(m_{\sqrt[3]{5},\mathbb{Q}}) = \mathrm{grad}(x^3 - 5) = 3.$$

Weiter ist $\mathbb{Q} \subseteq \mathbb{R}$ und $\sqrt[3]{5} \in \mathbb{R}$, also auch $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$. Da $\zeta_3 \notin \mathbb{R}$, folgt $\mathbb{Q}(\sqrt[3]{5}) \neq \mathbb{Q}(\sqrt[3]{5}, \zeta_3)$. Somit ist $[\mathbb{Q}(\sqrt[3]{5}, \zeta_3) : \mathbb{Q}(\sqrt[3]{5})] \geq 2$.
Da L der Zerfällungskörper von $x^3 - 5 \in \mathbb{Q}[x]$ ist, gilt nach Proposition 4.3.9 $[L : K] \leq 3! = 6$. Setzen wir diese Informationen zusammen, so liefert die Gradformel

$$6 \geq [L : K] = [\mathbb{Q}(\sqrt[3]{5}, \zeta_3) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{5}, \zeta_3) : \mathbb{Q}(\sqrt[3]{5})]}_{\geq 2} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]}_{=3} \geq 6.$$

Also gilt überall Gleichheit und es folgt

$$6 = [L : K] \overset{4.3.4}{=} |\mathrm{Gal}(L/K)|.$$

Nach Lemma 4.3.9 ist die Galoisgruppe $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe von $S(\{\alpha_1, \alpha_2, \alpha_3\}) \cong S_3$ und es gilt $|S_3| = 3! = 6$. Somit ist $\boxed{\mathrm{Gal}(L/K) \cong S_3}$.

Wir wissen, dass es eine Bijektion zwischen den Zwischenkörpern von L/K und den Untergruppen von $\mathrm{Gal}(L/K)$ gibt. Daher müssen wir Untergruppen von S_3 bestimmen. Die Gruppe ist gegeben durch

$$S_3 = \{\underbrace{\mathrm{id}}_{\mathrm{ord}=1}, \underbrace{(12),(23),(13)}_{\mathrm{ord}=2}, \underbrace{(123),(132)}_{\mathrm{ord}=3}\}.$$

Weiter gilt für jede Untergruppe H von S_3 nach dem Satz von Lagrange 1.1.17 $|H|$ teilt $|S_3| = 6$. Sei also H eine Untergruppe von S_3. Dann gilt

$|H| = 1 \implies H = \{\mathrm{id}\}$
$|H| = 2 \implies H = \{\mathrm{id}, (12)\}$, $H = \{\mathrm{id}, (23)\}$ oder $H = \{\mathrm{id}, (13)\}$
$|H| = 3 \implies H = \{\mathrm{id}, (123), (132)\}$
$|H| = 6 \implies H = S_3$.

Damit haben wir alle Untergruppen der S_3 und somit von $\mathrm{Gal}(L/K)$ gefunden. Um „echte“ Untergruppen von $\mathrm{Gal}(L/K)$ (also nicht nur bis auf Isomorphie) anzugeben, gehen wir die bisher benutzten Isomorphismen zurück und identifizieren die Elemente aus $\mathrm{Gal}(L/K)$ mit den Elementen aus S_3. Das heißt

$$\sigma \in S_3 \mapsto \varphi_\sigma \in \mathrm{Gal}(L/K) \text{ mit } \varphi_\sigma(\alpha_i) = \alpha_{\sigma(i)} \forall i \in \{1,2,3\}.$$

Wir müssen nun die Fixkörper L^H für alle Untergruppen H von $\mathrm{Gal}(L/K)$ berechnen.

$|H| = 1$ $\boxed{L^H = L^{\mathrm{id}} = L}$.

$|H| = 2$ Sei also zunächst $H = \{\mathrm{id}, (12)\}$. Da id alle Elemente aus L fest lässt, gilt $L^H = L^{\varphi_{(12)}}$. Wir sehen sofort $\varphi_{(12)}|_{\mathbb{Q}} = \mathrm{id}$ und $\varphi_{(12)}(\alpha_3) = \alpha_3$. Somit ist $\mathbb{Q}(\alpha_3) \subseteq L^H$. Nun benutzen wir Galoistheorie und erhalten

$$[L^H : \mathbb{Q}(\alpha_3)] \cdot \underbrace{[\mathbb{Q}(\alpha_3) : \mathbb{Q}]}_{=3} = [L^H : K] \overset{4.3.8}{=} [\mathrm{Gal}(L/K) : H] \overset{1.1.17}{=} \frac{6}{2} = 3.$$

Somit ist $[L^H : \mathbb{Q}(\alpha_3)] = 1$ und $\mathbb{Q}(\alpha_3) \subseteq L^H$, also $\boxed{L^H = \mathbb{Q}(\alpha_3)}$.

Genauso erhalten wir $\boxed{L^{\{\mathrm{id},(13)\}} = \mathbb{Q}(\alpha_2)}$ und $\boxed{L^{\{\mathrm{id},(23)\}} = \mathbb{Q}(\alpha_1)}$.

$|H| = 3$ Es ist also $H = \{\mathrm{id}, \varphi_{(123)}, \varphi_{(132)}\} = \langle\varphi_{(123)}\rangle$. Damit ist $L^H = L^{\varphi_{(123)}}$, dann falls $\varphi_{(123)}(\alpha) = \alpha$, so ist auch $\varphi_{(132)}(\alpha) = \varphi_{(123)}(\varphi_{(123)}(\alpha)) = \varphi_{(123)}(\alpha) = \alpha$.

Wir sehen $\varphi_{(123)}(\zeta_3) = \varphi_{(123)}(\frac{\alpha_2}{\alpha_1}) = \frac{\alpha_3}{\alpha_2} = \zeta_3$. Daraus folgt wieder $\mathbb{Q}(\zeta_3) \subseteq L^H$. Es ist

$$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \mathrm{grad}(m_{\zeta_3,\mathbb{Q}}) = \mathrm{grad}(x^2 + x + 1) = 2$$

und

$$[L^H : \mathbb{Q}] \overset{4.3.8}{=} [\mathrm{Gal}(L/K) : H] \overset{1.1.17}{=} \frac{6}{3} = 2.$$

Wie im Fall $|H| = 2$ folgt somit $\boxed{L^H = \mathbb{Q}(\zeta_3)}$.

$|H| = 6$ Dann ist H gleich $\mathrm{Gal}(L/K)$ und nach Proposition 4.3.4 gilt damit $\boxed{L^H = \mathbb{Q}}$.

Fazit: Die paarweise verschiedenen Körper

$$\mathbb{Q} = K, \mathbb{Q}(\zeta_3), \mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}(\zeta_3\sqrt[3]{5}), \mathbb{Q}(\zeta_3^2\sqrt[3]{5}), \mathbb{Q}(\zeta_3, \sqrt[3]{5}) = L$$

sind alle Zwischenkörper von L/K.

$$\begin{aligned} \text{Es ist } L^H/\mathbb{Q} \text{ normal} &\iff H \triangleleft \mathrm{Gal}(L/K) \cong S_3 \\ &\iff |H| \in \{1, 3, 6\} \\ &\iff L^H \in \{L, \mathbb{Q}(\zeta_3), K\} \end{aligned}$$

Wir wollen ein weiteres wichtiges Beispiel einer Galoiserweiterung geben. Dieses Beispiel ist sehr allgemein und bedarf einer weiteren Definition.

Definition 4.3.11. Sei K ein Körper und $x_1, \ldots, x_n$ Variablen. Ein Polynom $p \in K[x_1, \ldots, x_n]$ heißt *symmetrisch* genau dann wenn $p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ gilt, für alle σ in der symmetrischen Gruppe S_n. Offensichtliche Beispiele sind

$$s_r(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_r \le n} x_{i_1} \cdots x_{i_r} \text{ , für } r \in \{0, \ldots, n\}.$$

Das heißt:

$$\begin{aligned} s_0 &= 1 \\ s_1 &= x_1 + \cdots + x_n \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

Diese Polynome s_r heißen *elementare symmetrische Polynome.*

Beispiel 4.3.12. Wir benutzen die Notationen der Definition einfach weiter und betrachten die Körpererweierung $K(x_1, \ldots, x_n)/K(s_1, \ldots, s_n)$. Wir behaupten, dass dies eine Galoiserweiterung mit Galoisgruppe S_n ist. Hierfür führen wir eine weitere Variable T ein. Dann erhalten wir

$$(T - x_1) \cdots (T - x_n) = \sum_{i=0}^{n} (-1)^i s_i(x_1, \ldots, x_n) T^{n-i} \in (K(s_1, \ldots, s_n))[T].$$

Dies sieht man leicht durch Ausmultiplizieren, oder man kennt den Satz von Vieta. Es folgt, dass $K(x_1, \ldots, x_n)$ der Zerfällungskörper eines Polynoms

vom Grad n aus $(K(s_1,\dots,s_n))[T]$ ist. Insbesondere ist die Körpererweiterung $K(x_1,\dots,x_n)/K(s_1,\dots,s_n)$ nach Proposition 4.1.4 normal. Weiter sind die Elemente $x_1,\dots,x_n$, welche exakt die Nullstellen des Polynoms sind, nach Konstruktion paarweise verschieden. Somit ist die Körpererweiterung $K(x_1,\dots,x_n)/K(s_1,\dots,s_n)$ auch separabel nach Proposition 4.2.12. Es bleibt zu zeigen, dass die Galoisgruppe von $K(x_1,\dots,x_n)/K(s_1,\dots,s_n)$ isomorph zu S_n ist.
Für jedes $\sigma \in S_n$ betrachten wir den Einsetzhomomorphismus

$$\varphi_\sigma : K[x_1,\dots,x_n] \longrightarrow K[x_1,\dots,x_n], \text{ mit } x_i \mapsto x_{\sigma(i)} \text{ für alle } i \in 1,\dots,n.$$

Diese Abbildung ist offensichtlich sogar ein Ring-Isomorphismus, der sich kanonisch zu einem K-Automorphismus von $K(x_1,\dots,x_n)$ fortsetzt. Diese Fortsetzung bezeichnen wir wieder mit φ_σ. Da $K(s_1,\dots,s_n)$ von symmetrischen Polynomen erzeugt wird, sind alle Elemente dieses Körpers symmetrisch in $x_1,\dots,x_n$. Das bedeutet gerade $\varphi_\sigma|_{K(s_1,\dots,s_n)} = \mathrm{id}$. Damit gilt $\varphi_\sigma \in \mathrm{Gal}(K(x_1,\dots,x_n)/K(s_1,\dots,s_n))$.
Offensichtlich gilt $\varphi_\sigma \neq \varphi_\tau$ für $\sigma \neq \tau$ in S_n. Wir haben also gezeigt

$$|\mathrm{Gal}(K(x_1,\dots,x_n)/K(s_1,\dots,s_n))| \leq |S_n|.$$

In Lemma 4.3.9 haben wir gesehen, dass die Galoisgruppe in jedem Fall isomorph zu einer Untergruppe von S_n ist. Damit gilt wie behauptet

$$\mathrm{Gal}(K(x_1,\dots,x_n)/K(s_1,\dots,s_n)) \cong S_n.$$

4.4. Kreisteilungskörper

Kreisteilungskörper sind wichtige Beispiele für Galoiserweiterungen. Es sind diejenigen Körper, die über $\mathbb{Q}$ von Einheitswurzeln erzeugt werden. In diesem Abschnitt werden wir Kreisteilungskörper rein formal studieren. Im nächsten Abschnitt werden wir dann ihre geometrische Bedeutung erkennen.
Sei ab jetzt K ein Körper mit algebraischem Abschluss $\overline{K}$.

Definition 4.4.1. Für $n \in \mathbb{N}$, heißt ein Element $\zeta \in \overline{K}$ *n-te Einheitswurzel*, genau dann wenn $\zeta^n = 1$ gilt. Die Menge aller n-ten Einheitswurzeln in $\overline{K}$ bezeichnen wir mit U_n.

Lemma 4.4.2. *Sei* $\mathrm{char}(K) \nmid n$. *Dann ist* $(U_n,\cdot)$ *eine zyklische Gruppe der Ordnung* n.

Beweis. Seien $\zeta,\zeta' \in U_n$. Dann ist $(\zeta\cdot\zeta')^n = \zeta^n\cdot\zeta'^n = 1\cdot 1 = 1$ und $\zeta\cdot\zeta^{n-1} = 1$. Also ist $(U_n,\cdot)$ tatsächlich eine Gruppe. Als endliche Untergruppe von $\overline{K}^*$ ist U_n damit eine zyklische Gruppe.

Die Elemente in U_n sind genau die verschiedenen Nullstellen von $x^n - 1$. Für die Ableitung dieses Polynoms gilt, da $\mathrm{char}(K)$ kein Teiler von n ist, $(x^n-1)' = nx^{n-1} \neq 0$. Somit ist 0 die einzige Nullstelle von $(x^n-1)'$, aber keine Nullstelle von x^n-1. Nach (9) aus Lemma 4.2.3 ist x^n-1 also separabel und hat daher n verschiedene Nullstellen. Damit gilt auch $|U_n| = n$. □

DEFINITION 4.4.3. Eine n-te Einheitswurzel ζ_n heißt *primitiv*, genau dann wenn $U_n = \langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \dots\}$ gilt. Da U_n zyklisch ist, existiert zu jedem n, mit $\mathrm{char}(K) \nmid n$, eine primitive n-te Einheitswurzel.

Sei wieder $\mathrm{char}(K) \nmid n$ und ζ_n eine primitive n-te Einheitswurzel in $\overline{K}$. Die Abbildung

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow U_n \quad ; \quad \overline{m} \mapsto \zeta_n^m \tag{12}$$

ist wohldefiniert, denn für irgendeinen Repräsentanten $m + kn$ von $\overline{m}$ gilt $\zeta_n^{m+kn} = \zeta_n^m \cdot \zeta_n^{nk} = \zeta_n^m$. Es ist weiter sehr leicht zu sehen, dass die Abbildung aus (12) ein Gruppen-Isomorphismus zwischen $\mathbb{Z}/n\mathbb{Z}$ und U_n ist.
Wir erinnern an die Euler'sche φ-Funktion aus den Übungen. Sie ist gegeben durch

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |\{a \in \{1, \dots, n\} \,|\, \mathrm{ggT}(a, n) = 1\}.$$

LEMMA 4.4.4. *Sei* $\mathrm{char}(K) \nmid n$ *und* ζ_n *eine primitive* n*-te Einheitswurzel. Dann ist* $\zeta \in U_n$ *genau dann primitiv, wenn* $\zeta = \zeta_n^m$*, mit* $\mathrm{ggT}(m, n) = 1$*. Insbesondere existieren genau* $\varphi(n)$ *primitive* n*-te Einheitswurzeln.*

BEWEIS. Die Umkehrabbildung des Isomorphismus aus (12) ist gegeben durch $U_n = \langle \zeta_n \rangle \longrightarrow \mathbb{Z}/n\mathbb{Z}$; $\zeta_n^m \mapsto \overline{m} = m + n\mathbb{Z}$. Dieser Isomorphismus bildet primitive Einheitswurzeln, als Erzeuger von U_n, genau auf die Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ ab. Es genügt also Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ zu studieren. Es gilt

$$\begin{aligned} \langle \overline{m} \rangle = \mathbb{Z}/n\mathbb{Z} &\iff \overline{1} \in \langle \overline{m} \rangle \iff \exists k \in \mathbb{Z} \text{ mit } \overline{1} = \overline{m}\overline{k} \\ &\iff \overline{m} \in (\mathbb{Z}/n\mathbb{Z})^* \iff \mathrm{ggT}(m, n) = 1. \end{aligned}$$

Dies war zu zeigen. □

SATZ 4.4.5. *Sei* $n \in \mathbb{N}$ *und* $\mathrm{char}(K) \nmid n$*. Weiter sei* ζ_n *eine primitive* n*-te Einheitswurzel in* $\overline{K}$*. Dann gilt*

(a) $K(\zeta_n)/K$ *ist eine Galoiserweiterung.*
(b) *Für alle* $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$ *existiert genau ein* $\overline{k(\sigma)} \in (\mathbb{Z}/n\mathbb{Z})^*$ *mit* $\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$*.*
(c) *Die Abbildung*

$$\Psi : \mathrm{Gal}(K(\zeta_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \quad ; \quad \sigma \mapsto \overline{k(\sigma)}$$

ist ein kanonischer injektiver Gruppen-Homomorphismus.

Insbesondere ist also $\mathrm{Gal}(K(\zeta_n)/K)$ *abelsch.*

BEWEIS. Wir beweisen die drei Aussagen.

Zu (a): Da $\mathrm{char}(K) \nmid n$, ist mit Lemma 4.4.2 $n = |U_n|$ gleich der Anzahl der verschiedenen Nullstellen von $x^n - 1 \in K[x]$. Insbesondere ist also $x^n - 1 \in K[x]$ separabel. Damit ist nach Proposition 4.2.12 auch $K(\zeta_n)/K$ separabel.

Weiter ist der Zerfällungskörper von $x^n - 1 \in K[x]$ gegeben durch $K(U_n) = K(\zeta_n, \zeta_n^2, \dots) = K(\zeta_n)$. Also ist $K(\zeta_n)/K$ auch normal (siehe Theorem 4.1.4) und endlich (Proposition 3.3.7) und somit Galois.

Zu (b): Zunächstchst stellen wir fest

$$\sigma(\zeta_n)^n = \sigma(\zeta_n^n) = \sigma(1) = 1$$

für alle $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$. Also ist $\sigma(\zeta_n)$ eine n-te Einheitswurzel und da ζ_n primitiv ist, existiert genau ein $\overline{k(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ mit $\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$. Wir müssen noch zeigen, dass $\overline{k(\sigma)}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ ist. (Dies ist nach Lemma 4.4.4 äquivalent dazu, dass $\zeta_n^{k(\sigma)}$ eine primitive n-te Einheitswurzel ist.)

Für die Identität $\mathrm{id} \in \mathrm{Gal}(K(\zeta_n)/K)$ gilt natürlich $\overline{k(\mathrm{id})} = \overline{1} \in (\mathbb{Z}/n\mathbb{Z})^*$. Weiter gilt für $\sigma, \tau \in \mathrm{Gal}(K(\zeta_n)/K)$ beliebig:

$$\zeta_n^{k(\tau\circ\sigma)} = (\tau \circ \sigma)(\zeta_n) = \tau(\sigma(\zeta_n)) = \tau(\zeta_n^{k(\sigma)}) = \tau(\zeta_n)^{k(\sigma)} = \zeta_n^{k(\tau)k(\sigma)}. \tag{13}$$

Es folgt $\overline{k(\tau \circ \sigma)} = \overline{k(\tau)k(\sigma)}$. Setzen wir nun $\tau = \sigma^{-1}$ so erhalten wir $\overline{1} = \overline{k(\mathrm{id})} = \overline{k(\sigma)k(\sigma^{-1})}$. Also ist $\overline{k(\sigma)} \in (\mathbb{Z}/n\mathbb{Z})^*$ wie gewünscht.

Zu (c): Nach (13) ist $\Psi : \mathrm{Gal}(K(\zeta_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$; $\sigma \mapsto \overline{k(\sigma)}$ ein wohldefinierter Gruppen-Homomorphismus. Wir beweisen die Injektivität dadurch, dass wir die Trivialität von $\ker(\Psi)$ beweisen. Sei also $\sigma \in \ker(\Psi)$. Dann ist $\overline{k(\sigma)} = \overline{1}$ und somit $\sigma(\zeta_n) = \zeta_n^{k(\sigma)} = \zeta_n$. Da ζ_n die Körpererweiterung $K(\zeta_n)/K$ erzeugt und $\sigma|_K = \mathrm{id}$ nach Voraussetzung, muss σ die Identität auf ganz $K(\zeta_n)$ sein. Damit besteht der Kern von Ψ aus nur einem Element und Ψ ist injektiv.

Dass die Abbildung Ψ kanonisch ist, bedeutet, dass Ψ nicht von der Wahl der primitiven Einheitswurzel ζ_n abhängt. Sei also $\zeta \in U_n$ irgendeine andere primitive n-te Einheitswurzel. Dann gilt $\zeta_n \in \langle\zeta\rangle$ und daher $K(\zeta_n) = K(U_n) = K(\zeta)$. Weiter ist $\zeta = \zeta_n^k$ für ein $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k, n) = 1$ (nach Lemma 4.4.4). Wegen

$$\sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = (\zeta_n^{k(\sigma)})^k = (\zeta_n^k)^{k(\sigma)} = \zeta^{k(\sigma)}$$

hängt $\overline{k(\sigma)}$ tatsächlich nicht von der Wahl von ζ_n ab.

□

DEFINITION 4.4.6. Für $K = \mathbb{Q}$ und ζ_n eine primitive n-te Einheitswurzel, nennen wir $\mathbb{Q}(\zeta_n)$ den *n-ten Kreisteilungskörper* (oder den *n-ten zyklotomischen Körper*). In diesem Fall können wir stets $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ setzen.

THEOREM 4.4.7. *Im Fall $K = \mathbb{Q}$ ist der Homomorphismus*

$$\Psi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \quad ; \quad \sigma \mapsto \overline{k(\sigma)}$$

aus Satz 4.4.5 sogar ein Isomorphismus. Damit gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

BEWEIS. Wir wissen aus Satz 4.4.5 bereits, dass Ψ ein injektiver Gruppen-Homomorphismus ist. Es genügt also die Surjektivität von Ψ zu beweisen. Dies tun wir in drei Schritten

1.Schritt: Sei $p \nmid n$ ein Primzahl. Dann gilt $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) = 0$. (Hierbei ist wie immer $m_{\zeta_n,\mathbb{Q}}(x) \in \mathbb{Q}[x]$ das Minimalpolynom von ζ_n über $\mathbb{Q}$.)

Es ist ζ_n eine Nullstelle von $x^n - 1 \in \mathbb{Q}[x]$. Mit Lemma 3.3.5 gilt daher $m_{\zeta_n,\mathbb{Q}}(x)h(x) = x^n - 1$, für ein $h(x) \in \mathbb{Q}[x]$. Weiter muss dieses $h(x)$ normiert sein. Es gilt also sogar $h(x) \in \mathbb{Z}[x]$ (siehe Korollar 2.8.7).
Wir nehmen nun an, dass $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) \neq 0$. Da ζ_n^p eine Nullstelle von $x^n - 1$ ist, muss $h(\zeta_n^p) = 0$ gelten. Damit ist ζ_n eine Nulltelle von $h(x^p) \in \mathbb{Z}[x]$ es folgt

$$m_{\zeta_n,\mathbb{Q}}(x)g(x) = h(x^p)$$

für ein $g(x) \in \mathbb{Z}[x]$. Wir wenden den surjektiven Ring-Homomorphismus

$$\Phi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x] \quad ; \quad \sum_{i=0}^{r} a_i x^i \mapsto \sum_{i=0}^{r} \overline{a_i} x^i$$

an. Damit gilt $\Phi_p(m_{\zeta_n,\mathbb{Q}}(x))\Phi_p(g(x)) = \Phi_p(h(x^p))$. Weiter ist mit dem kleinen Satz von Fermat 1.1.29 $a^p = a$ für alle $a \in \mathbb{Z}/p\mathbb{Z}$. Mit dem Frobenius-Homomorphismus angewendet auf $\mathrm{Quot}(\mathbb{Z}/p\mathbb{Z}[x])$ sehen wir $\Phi_p(h(x^p)) = \Phi_p(h(x))^p$. Also sind die Nullstellen von $\Phi_p(h(x^p))$ genau die Nullstellen von $\Phi_p(h(x))$. Nach Voraussetzung existiert eine gemeinsame Nullstelle von $\Phi_p(h(x^p))$ und $\Phi_p(m_{\zeta_n,\mathbb{Q}}(x))$, also auch von $\Phi_p(h(x))$ und $\Phi_p(m_{\zeta_n,\mathbb{Q}}(x))$. Aus

$$\Phi_p(h(x))\Phi_p(m_{\zeta_n,\mathbb{Q}}(x)) = \Phi_p(x^n - 1) = x^n - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[x]$$

folgt somit, dass $x^n - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ eine mehrfache Nullstelle besitzt, im Widerspruch zur Separabilität von $x^n - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$. (Beachte $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p \nmid n$.) Also war unsere Annahme $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) \neq 0$ falsch. Es gilt also wie gewünscht $m_{\zeta_n,\mathbb{Q}}(\zeta_n^p) = 0$.

2. Schritt: Sei ζ eine primitive n-te Einheitswurzel. Dann ist $m_{\zeta_n,\mathbb{Q}}(\zeta) = 0$.

Sei also ζ eine primitive n-te Einheitswurzel. Aus Lemma 4.4.4 folgt $\zeta = \zeta_n^k$ mit $\mathrm{ggT}(n,k) = 1$. Es ist also $k = p_1 \cdots p_r$ mit Primzahlen $p_1, \ldots, p_r$ teilerfremd zu n. Setze $\zeta_{n,0} = \zeta_n$ und $\zeta_{n,i} = \zeta_{n,i-1}^{p_i}$ für $i \in \{1, \ldots, r\}$. D.h.:

$$\zeta_{n,1} = \zeta_n^{p_1}, \zeta_{n,2} = \zeta_n^{p_1 p_2}, \ldots, \zeta_{n,r} = \zeta_n^k = \zeta.$$

Nach dem 1. Schritt ist nun $m_{\zeta_n,\mathbb{Q}}(\zeta_{n,1}) = 0$. Daraus folgt $m_{\zeta_{n,1},\mathbb{Q}}(x) = m_{\zeta_n,\mathbb{Q}}(x)$. Wieder mit dem 1. Schritt ist damit $m_{\zeta_{n,1},\mathbb{Q}}(\zeta_{n,2}) = 0$, und somit auch $m_{\zeta_{n,2},\mathbb{Q}}(x) = m_{\zeta_n,\mathbb{Q}}(x)$. Wiederholen wir dies r-mal, so erhalten wir

$$m_{\zeta_n,\mathbb{Q}}(\zeta) = m_{\zeta_n,\mathbb{Q}}(\zeta_{n,r}) = m_{\zeta_{n,r-1},\mathbb{Q}}(\zeta_{n,r}) = 0.$$

Das war für den 2. Schritt zu zeigen.

3. Schritt: Beweisende.

Das Polynom $m_{\zeta_n,\mathbb{Q}}(x)$ ist irreduzibel und es gilt $\mathrm{char}(\mathbb{Q}) = 0$. Folglich ist $m_{\zeta_n,\mathbb{Q}}(x)$ separabel und daher ist der Grad von $m_{\zeta_n,\mathbb{Q}}(x)$ gegeben durch die Anzahl der verschiedenen Nullstellen von $m_{\zeta_n,\mathbb{Q}}(x)$. Da wir eben gezeigt haben, dass jede primitive n-te Einheitswurzel eine Nullstelle dieses Polynoms ist, gilt nach Lemma 4.4.4

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \mathrm{grad}(m_{\zeta_n,\mathbb{Q}}(x)) \geq \varphi(n).$$

Weiter gilt nach Theorem 4.3.4 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})|$. Da die Abbildung $\Psi : \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ injektiv ist, erhalten wir auch

$$|\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| \leq |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n).$$

Zusammen liefert dies also

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n).$$

Der Homomorphismus Ψ ist also eine injektive Abbildung zwischen endlichen Mengen gleicher Kardinalität. Damit ist Ψ bijektiv, also ein Isomorphismus. □

Definition 4.4.8. Für eine primitive n-te Einheitswurzel $\zeta_n \in \mathbb{C}$, nennen wir das Polynom $F_n(x) = m_{\zeta_n,\mathbb{Q}}(x)$ das *n-te Kreisteilungspolynom*. Die Wohldefiniertheit und weitere Eigenschaften werden in den Übungen gezeigt.

Beispiel 4.4.9.

- $F_1(x) = x - 1$
- $F_2(x) = x + 1$
- $F_3(x) = x^2 + x + 1$
- $F_4(x) = x^2 + 1$

- $F_5(x) = x^4 + x^3 + x^2 + x + 1$

Allgemein gilt $F_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1$ für jede Primzahl p. Wenn man diese Liste weiterführt könnte man meinen, dass alle Kreisteilungspolynome Koeffizienten in $\{-1, 0, 1\}$ haben. Aber: $F_{105}(x) = x^{48} + \cdots - 2x^{41} + \ldots$.

ABBILDUNG 4.2. *David Hilbert* (1862 - 1943) war einer der bedeutendsten Mathematiker des 19. und 20. Jahrhunderts. Er war einer der letzten universellen Mathematiker, der in fast allen Bereichen der Mathematik, bis hin zur theoretischen Physik, forschte. Seine im Jahr 1900 vorgestellte Liste mit 23 Problemen beschäftigt die Mathematik bis heute.

Eine kurze Exkursion: Inverse Galoitheorie. David Hilbert bewies, dass es zu jeder symmetrischen Gruppe S_n eine Galoiserweiterung $F/\mathbb{Q}$ gibt mit $\mathrm{Gal}(F/\mathbb{Q}) \cong S_n$. (Der interessierte Leser sei auf [**Vo**], Kapitel 1, verwiesen). Damit folgt leicht, dass es zu jeder endlichen Gruppe G eine Galoiserweiterung L/K, mit $L/\mathbb{Q}$ endlich, gibt mit $\mathrm{Gal}(L/K) \cong G$. Denn: Wir wissen, dass G isomorph zu einer Untergruppe einer S_n ist (Satz von Cayley). Sei nun $F/\mathbb{Q}$ Galois, mit $\mathrm{Gal}(F/\mathbb{Q}) \cong S_n$. Wir können also G mit einer Untergruppe von $\mathrm{Gal}(F/\mathbb{Q})$ identifizieren. Mit Satz 4.3.5 ist F/F^G eine Galoiserweiterung mit Galoisgruppe G.
Folgende Frage ist allerdings noch immer (200 Jahre nach Galois!) ungelöst:

FRAGE. Existiert zu jeder endlichen Gruppe G eine Galoiserweiterung $K/\mathbb{Q}$ mit $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

Wie bereits erwähnt gilt dies für alle symmetrischen Gruppen. Im Folgenden wollen wir beweisen, dass die Antwort auf diese Frage auch für alle abelschen Gruppen „Ja“ ist. Dazu benutzen wir ein berühmtes Theorem der Zahlentheorie, welches wir in dieser Vorlesung leider nicht beweisen können. Der funktionentheoretische Beweis findet sich etwa in [**Br**], Abschnitt 1.6.

THEOREM 4.4.10 (Dirichet'scher Primzahlsatz). *Seien a und n teilerfremde ganze Zahlen. Dann existieren unendlich viele Primzahlen p mit $p \equiv a \mod m$.*

KOROLLAR 4.4.11. *Sei G eine endliche abelsche Gruppe, dann existiert eine ganze Zahl n, so dass es einen surjektiven Gruppen-Homomorphismus $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow G$ gibt.*

BEWEIS. Nach dem Strukturssatz für endliche abelsche Gruppen ist

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

ABBILDUNG 4.3. Der deutsche Mathematiker *Johann Peter Gustav Lejeune Dirichlet* (1805 - 1859) arbeitete hauptsächlich in der Zahlentheorie. Z.B. bewies er mit 20Jahren, zusammen mit Legendre, die Fermat-Vermutung für den Fall $n = 5$. Später trat er die Nachfolge von Gauß an der Universität Göttingen an.

für gewisse $n_1, \ldots, n_r \in \mathbb{Z}$. Nach Theorem 4.4.10 können wir paarweise verschiedene Primzahlen $p_1, \ldots, p_r$ wählen mit $p_i \equiv 1 \mod n_i$ für alle $i \in \{1, \ldots, r\}$. Betrachten wir die kanonischen Abbildungen

$$\varphi_i : \mathbb{Z}/(p_i-1)\mathbb{Z} \longrightarrow \mathbb{Z}/n_i\mathbb{Z} \quad ; \quad a + (p_i - 1)\mathbb{Z} \mapsto a + n_i\mathbb{Z}$$

für alle $i \in \{1, \ldots, r\}$. Nach Wahl der Primzahlen p_i gilt $n_i \mid p_i - 1$ für alle $i \in \{1, \ldots, r\}$. Somit sind die Abbildungen $\varphi_1, \ldots, \varphi_r$ wohldefinierte surjektive Gruppen-Homomorphismen. Es folgt, dass damit auch die Abbildung

$$\begin{aligned} \varphi : \mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_r-1)\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \cong G \\ (a_1, \ldots, a_r) &\mapsto (\varphi_1(a_1), \ldots, \varphi_r(a_r)) \end{aligned}$$

ein wohldefinierter surjektiver Gruppen-Homomorphismus ist. Um den Beweis zu schließen müssen wir noch zeigen, dass $\mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_r-1)\mathbb{Z}$ isomorph ist zu $(\mathbb{Z}/n\mathbb{Z})^*$ für ein $n \in \mathbb{N}$. Setzen wir $n = p_1 \cdots p_r$ so liefert uns der Chinesische Restsatz:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^* \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \mathbb{Z}/(p_r-1)\mathbb{Z}.$$

Beachte für die letzte Isomorphie, dass für eine Primzahl p der Ring $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, und somit $(\mathbb{Z}/p\mathbb{Z})^*$ eine zyklische Gruppe mit $p - 1$ Elementen sein muss. □

THEOREM 4.4.12. *Sei G eine endliche abelsche Gruppe, dann existiert eine Galoiserweiterung $K/\mathbb{Q}$ mit* $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

BEWEIS. Sei $n \in \mathbb{N}$ wie in Korollar 4.4.11 und $\varphi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow G$ der surjektive Gruppen-Homomorphismus. Dann gilt

$$(\mathbb{Z}/n\mathbb{Z})^*/\ker(\varphi) \cong G. \tag{14}$$

Mit Theorem 4.4.7 ist $)\mathbb{Z}/n\mathbb{Z})^*$ isomorph zu $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, für eine primitive n-te Einheitswurzel ζ_n. Wir bezeichnen mit H eine Untergruppe von $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $H \cong \ker(\varphi)$. Da die Gruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ abelsch ist, ist H sogar ein Normalteiler. Proposition 4.3.8 liefert uns also, dass die Erweiterung $\mathbb{Q}(\zeta_n)^H/\mathbb{Q}$ Galois ist und die zugehörige Galoisgruppe isomorph ist zu

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/H \cong (\mathbb{Z}/n\mathbb{Z})^*/\ker(\varphi) \overset{(14)}{\cong} G.$$

Das war zu zeigen. □

4.5. Konstruierbarkeit mit Zirkel und Lineal

In diesem Abschnitt werden wir vollständig klären, welche Konstruktionen mit Hilfen von Zirkel und Lineal (kein Geodreieck!) durchführbar sind. Wir setzen hier elementare Schulgeometrie voraus.

4.5.1. Unter *Konstruktion mit Zirkel und Lineal* verstehen wir folgendes. Es seien zwei Punkte P_1 und P_2 in der Ebene gegeben.

- Zu zwei konstruierten (gegebenen) Punkten lässt sich eine Gerade konstruieren, die durch die beiden Punkte verläuft.
- Zu zwei konstruierten (gegebenen) Punkten Q_1, Q_2 lässt sich ein Kreis konstruieren, mit Mittelpunkt Q_1 der durch Q_2 verläuft.
- Zu konstruierten Geraden und Kreisen lassen sich die Schnittpunkte dieser (falls sie existieren) konstruieren.

Probleme 4.5.2. Wir werden folgende antike Probleme lösen.

(A) (Winkeldreiteilung) Kann man zu einem beliebigen gegebenem Winkel α, den Winkel $\alpha/3$ konstruieren?
(B) (Das Delische Problem) Lässt sich zu einem gegebenen Würfel ein Würfel doppelten Volumens konstruieren?
(C) (Quadratur des Kreises) Kann man zu einem gegebenen Kreis ein flächengleiches Quadrat konstruieren?
(D) (reguläre n-Ecke) Es ist ganz einfach aus zwei Punkten P_1, P_2 ein reguläres 3-Eck zu konstruieren. Welche anderen regulären n-Ecke lassen sich konstruieren?

Lemma 4.5.3. *Seien P_1, P_2, P Punkte in der Ebene und sei g die Gerade durch P_1 und P_2. Dann sind die folgenden Operationen mit Zirkel und Lineal möglich.*

(a) *Der Mittelpunkt der Strecke von P_1 nach P_2 ist konstruierbar.*
(b) *Es ist eine zu g senkrechte Gerade durch P_1 konstruierbar.*
(c) *Es ist eine zu g parallele Gerade durch P konstruierbar.*
(d) *Jeder gegebene Winkel lässt sich halbieren.*

Beweis. Wir geben die jeweiligen Konstruktionen an.

Zu (a) Zeichne die Kreise um P_1 durch P_2 und andersherum. Verbinde nun die beiden Schnittpunkte dieser Kreise. Die entstandene Gerade schneidet die Strecke von P_1 nach P_2 im Mittelpunkt.

Zu (b) Zeichne einen Kreis um P_1 der durch P_2 geht. Dieser schneidet g in einem Punkt P_3, so dass P_1 der Mittelpunkt der Strecke von P_3 nach P_4 ist. Nun starten wir die Konstruktion aus a) mit P_1 ersetzt durch P_3.

Zu (c) Übung.

Zu (d) Sei h eine Gerade die g im Winkel α schneidet. Sei oBdA P_1 der Schnittpunkt von h und g. Zeichne einen Kreis um P_1 durch P_2. Wähle einen Schnittpunkt P_3 dieses Kreises mit h. Nach (c) können wir nun eine zu g parallele Gerade durch P_3 und eine zu h parallele Gerade durch P_2 konstruieren. Diese beiden Geraden schneiden sich in einem Punkt P_4. Nach Konstruktion bildet P_1, P_2, P_4, P_3 eine Raute. Damit halbiert die Gerade durch P_1 und P_4 genau unseren Winkel α.

□

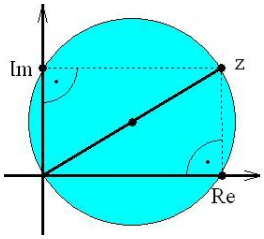
BEMERKUNG 4.5.4. Wir schaffen nun den Übergang zur modernen Algebra. Dazu identifizieren wir unsere Zeichenebene mit der Ebene der komplexen Zahlen $\mathbb{C}$ und die Punkte P_1 und P_2 mit den Zahlen 0 und 1. Sei ab jetzt Z die Menge aller aus $\{0, 1\}$ mit Hilfe von Zirkel und Lineal konstruierbaren Zahlen in $\mathbb{C}$. Dann gilt

(i) $\mathbb{Z} \subseteq Z$ durch „Abtragen“ der Strecke von 0 nach 1.

(ii) $i \in Z$ als Schnittpunkt eines Kreises um 0 mit Radius 1 und der Senkrechten zur geraden durch 0 und 1 durch den Punkt 0.

(iii) $z = Re(z) + Im(z)i \in Z \iff Re(z), Im(z) \in Z$.

ABBILDUNG 4.4. Die Richtung $\Longleftarrow$ ist nach Lemma 4.5.3 trivial. Für die andere Richtung können wir zum Beispiel den *Thaleskreis* der Strecke von 0 nach z zeichen. Dessen Schnittpunkte mit den (konstruierbaren) reellen und imaginären Achsen sind genau der Realteil bzw. der Imaginärteil von z.



SATZ 4.5.5. *Die Menge Z bildet einen Teilkörper von $\mathbb{C}$.*

BEWEIS. Offensichtlich ist mit $a \in Z$ auch $-a \in Z$. Wir wollen zunächst zeigen, dass Z abgeschlossen ist bezüglich Addition und Multiplikation.

Addition: Nach 4.5.4 (*iii*) genügt es zu zeigen, dass für $z_1, z_2 \in Z \cap \mathbb{R}$ auch $z_1 + z_2 \in \mathbb{Z}$ ist. Sei oBdA $z_1 \leq z_2$. Der Mittelpunkt m der Verbindungsstrecke von z_1 und z_2 ist konstruierbar und gleich $\frac{z_1+z_2}{2}$. Ein weiteres Abtragen der Strecke zwischen 0 und m liefert $z_1 + z_2$.

Multiplikation: Seien also $z_1, z_2 \in Z$. Nach 4.5.4 (iii) ist zu zeigen, dass

$$Re(z_1 z_2) = Re(z_1)Re(z_2) - Im(z_1)Im(z_2) \in Z \text{ und}$$
$$Im(z_1 z_2) = Re(z_1)Im(z_2) + Re(z_2)Im(z_1) \in Z \text{ gilt.}$$

Es genügt also zu zeigen, dass für $a, b \in Z \cap \mathbb{R}$ auch $ab \in Z$ gilt. Aufgrund der Abgeschlossenheit bezüglich Multiplikation mit -1 dürfen wir sogar a und b als positiv annehmen.
Natürlich sind ai und bi konstruierbar. Wir ziehen die Verbindungsgerade von i und a, und die dazu Parallele durch den Punkt bi. Diese Gerade ist nach Lemma 4.5.3 konstruirbar und schneidet die reelle Achse in einem Punkt c (der damit konstruierbar - also in Z - ist). Mit dem Strahlensatz gilt nun

$$b = \frac{|bi|}{|i|} = \frac{c}{a}.$$

Daraus folgt, $c = ab \in Z$.

Wir haben bis jetzt gezeigt, dass Z ein Teilring von $\mathbb{C}$ ist. Es bleibt zu zeigen, dass jedes $z \in Z \setminus \{0\}$ ein multiplikatives Inverses besitzt. Sei also $z \in Z \setminus \{0\}$, dann ist

$$z^{-1} = \frac{\overline{z}}{\overline{z}z} = \frac{Re(z)}{|z|^2} - \frac{Im(z)}{|z|^2}i.$$

Wir wissen bereits, dass $Re(z), Im(z), \overline{z}, \overline{z}z, \pm i \in Z$ gilt. Es genügt also nach 4.5.4 (iii) wieder zu zeigen, dass $\frac{a}{b} \in Z$ für $a, b \in Z \cap \mathbb{R}_{>0}$. Wieder konstruieren wir zunachst ai und bi. Wir ziehen die Verbindungsgerade zwischen bi und 1 und eine dazu parallele Gerade durch den Punkt ai. Diese Gerade schneidet die reelle Achse in einem Punkt c, der nach Lemma 4.5.3 konstruierbar ist. Mit dem Strahlensatz folgt nun

$$\frac{a}{b} = \frac{|ai|}{|bi|} = \frac{c}{1} = c \in Z.$$

Somit ist Z tatsächlich ein Zwischenkörper von $\mathbb{C}$. □

LEMMA 4.5.6. *Ist $z \in Z$, so ist auch $\pm\sqrt{z} \in Z$.*

BEWEIS. Wir schreiben $z = |z|e^{i\alpha}$ in Polarkoordinaten. Dann ist $\pm\sqrt{z} = \pm\sqrt{|z|}e^{i\alpha/2}$ und sowohl $|z|$ als auch $e^{i\alpha}$ ist konstruierbar. Da wir Winkel halbieren dürfen (siehe Lemma 4.5.3) ist auch $e^{i\alpha/2}$ konstruierbar. Es bleibt also zu zeigen, dass $\sqrt{|z|} \in Z$ ist. Konstruiere den Thaleskreis zu den (konstruierbaren) Punkten $-i$ und $|z|i$. (D.h.: einen Kreis der durch die Verbindungsstrecke zwischen $-i$ und $|z|i$ halbiert wird.) Dieser schneidet die reelle Achse in einem Punkt h, der damit konstruierbar ist. Wende nun den

Höhensatz auf das rechtwinklige Dreieck $|z|i$, h, $-i$ an. Dann erhalten wir

$$|z| = ||z|i| \cdot |-i| = h^2.$$

Somit ist $h = \sqrt{|z|} \in Z$, wie gewünscht. □

PROPOSITION 4.5.7. *Sei L/K eine Galoiserweiterung und $\overline{K}$ ein gemeinsamer algebraischer Abschluss von K und L. Weiter sei $\alpha \in L$ beliebig. Dann gilt*

$$\beta \in \overline{K} \text{ ist Nullstelle von } m_{\alpha,K}(x) \iff \beta = \sigma(\alpha) \text{ für ein } \sigma \in \mathrm{Gal}(L/K).$$

BEWEIS. Wir haben im Beweis von Satz 4.3.4 gesehen, dass das Polynom

$$q(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \sigma(\alpha))$$

Koeffizienten in $L^{\mathrm{Gal}(L/K)} \overset{4.3.4}{=} K$ besitzt. Da auch $q(\alpha) = 0$ gilt, folgt $m_{\alpha,K}(x) \mid q(x)$. Insbesondere ist jede Nullstelle von $m_{\alpha,K}(x)$ in $\overline{K}$ auch eine Nullstelle von $q(x)$ und somit gegeben durch $\sigma(\alpha)$, für ein $\sigma \in \mathrm{Gal}(L/K)$. Die Umkehrung ist klar nach 3.4.1. □

DEFINITION 4.5.8. Seien L und K Körper der Charakteristik 0. Wir sagen, dass L aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht, falls eine Körperkette

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = L \tag{15}$$

existiert, so dass $L_{i+1} = L_i(\sqrt{\omega_i})$, für ein $\omega_i \in L_i$, für alle $i \in \{0, \ldots, r-1\}$.

PROPOSITION 4.5.9. *Seien L und K Körper der Charakteristik 0, so dass L aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht. Dann existiert eine Galoiserweiterung F/K mit $L \subseteq F$ und $[F : K] = 2^n$ für ein $n \in \mathbb{N}_0$.*

BEWEIS. Sei also $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = L$ eine Körperkette wie in (15). Wir beweisen die Aussage durch Induktion über r.

Induktionsanfang, $r = 1$: Dann ist $L = K(\sqrt{\omega_0})$ mit $\omega_0 \in K$. Also ist $[L : K] \in \{1, 2\}$ und L/K eine Galoiserweiterung. (L ist der Zerfällungskörper von $x^2 - \omega_0 \in K[x]$.)

Induktionsschritt, $r \geq 2$: Nach Induktionsvoraussetzung existiert eine Galoiserweiterung F'/K mit $L_{r-1} \subseteq F'$ und $[F' : K] = 2^{n'}$ mit $n' \in \mathbb{N}_0$. Weiter ist $L = L_{r-1}(\sqrt{\omega_{r-1}})$ für ein $\omega_{r-1} \in L_{r-1} \subseteq F'$. Sei M der Zerfällungskörper von $m_{\sqrt{\omega_{r-1}},K}(x) \in K[x]$ über K. Wie immer ist M/K eine Galoiserweiterung und somit ist auch das Kompositum $F'M/K$ (gebildet in einem algebraischen Abschluss $\overline{K}$ von K) eine Galoiserweiterung. Nach Proposition

4.5.7 sind alle Nullstellen von dem Polynom $m_{\sqrt{\omega_{r-1}},K}(x)$ gegeben durch $\{\tau(\sqrt{\omega_{r-1}})|\tau \in \mathrm{Gal}(F'M/K)\}$. Schreibe $\mathrm{Gal}(F'M/K) = \{\tau_1, \ldots, \tau_k\}$, dann ist $F'M = F'(\tau_1(\sqrt{\omega_{r-1}}), \ldots, \tau_k(\sqrt{\omega_{r-1}}))$ und es gilt

$$\tau_i(\sqrt{\omega_{r-1}})^2 = \tau_i(\underbrace{\omega_{r-1}}_{\in F'}) = \tau_i|_{F'}(\omega_{r-1}) \in F'$$

für alle $i \in \{1, \ldots, k\}$. Damit ist also $[F'M : K]$ gleich

$$\underbrace{[F'M : F'(\tau_1(\sqrt{\omega_{r-1}}), \ldots, \tau_{k-1}(\sqrt{\omega_{r-1}}))]}_{\in\{1,2\}} \cdots \underbrace{[F'(\tau_1(\sqrt{\omega_{r-1}}) : F']}_{\in\{1,2\}} \cdot \underbrace{[F' : K]}_{=2^{n'}}.$$

Insbesondere ist $[F'M : K] = 2^n$ für ein $n \in \mathbb{N}$. Somit erfüllt $F = F'M$ alle Bedingungen des gesuchten Körpers. □

THEOREM 4.5.10. *Die Zahl $z \in \mathbb{C}$ ist genau dann in Z, wenn es eine Galoiserweiterung $L/\mathbb{Q}$ gibt mit $z \in L$ und $[L : \mathbb{Q}] = 2^n$ für ein $n \in \mathbb{N}$.*

BEWEIS. Wir beweisen die beiden Richtungen.

$\Longrightarrow$ Sei also $z \in Z$. Nach Proposition 4.5.9 genügt es zu zeigen, dass z in einem Körper liegt, der durch sukzessive Adjunktion von Quadratwurzeln aus $\mathbb{Q}$ entsteht.

Dass z konstruierbar ist bedeutet, dass es Elemente $z_1, z_2, \ldots, z_r$ gibt, mit $z_r = z$ und so dass z_j ein Schnittpunkt von

(i) zwei Geraden,
(ii) zwei Kreisen oder
(iii) einer Geraden und einem Kreis ist,

die je durch zwei Punkte in $\{0, 1, z_1, z_2, \ldots, z_{j-1}\}$ definiert sind, für alle $j \leq r$.

Wir wissen bereits, dass $i = \sqrt{-1} \in Z$, wir dürfen also die Menge der gegebenen Punkte (0 und 1) um die Punkte i und $-i$ erweitern. Weiter möchten wir alle Konstruktionen symmetrisch zur reellen Achse durchführen. D.h.: $z = z_r$ lässt sich durch eine der Operationen $(i), (ii), (iii)$ aus $\{0, 1, i, -i, z_1, \overline{z_1}, \ldots, z_{r-1}, \overline{z_{r-1}}\}$ konstruieren. Wir beweisen die Behauptung nun per Induktion über r.

Induktionsanfang, $r = 0$: Das heißt, dass z in 0 Schritten konstruierbar ist - also gegeben. Demnach ist $z \in \{0, 1, i, -i\}$, und somit $z \in \mathbb{Q}(i)$. Da $\mathbb{Q}(i)$ aus $\mathbb{Q}$ durch Adjunktion einer Quadratwurzel entsteht, ist der Induktionsanfang bewiesen.

Induktionsschritt, $r \geq 1$: Nach Induktionsvoraussetzung existiert ein Körper $L/\mathbb{Q}$, der aus sukzessiver Adjunktion von Quadratwurzeln entsteht und mit $i, -i, z_1, \overline{z_1}, \ldots, z_{r-1}, \overline{z_{r-1}} \in L$. Damit enthält L auch $Re(z_j) = {}^{(z_j+\overline{z_j})}/_2$ und $Im(z_j) = {}^{(z_j-\overline{z_j})}/_{2i}$ für alle $j \in \{1, \ldots, r-1\}$.

Wir betrachten nur den schwierigsten Fall (ii), dass z_r der Schnitt zweier Kreise ist. Seien die Mittelpunkte dieser Kreise gegeben durch x_1, x_2 und die Punkte, durch die die Kreise verlaufen, seien y_1, y_2, wobei $x_1, x_2, y_1, y_2 \in \{0, 1, i, -i, z_1, \overline{z_1}, \ldots, z_{r-1}, \overline{z_{r-1}}\}$ gilt. Also gilt

$$(Re(z_r) - Re(x_j))^2 + (Im(z_r) - Im(x_j))^2 = R_j^2 \text{ für } j \in \{1, 2\}. \tag{16}$$

Beachte, dass $Re(x_j), Im(x_j), R_j^2 = (x_j - y_j)(\overline{x_j} - \overline{y_j}) \in L$ gilt für $j \in \{1, 2\}$. Da sich die Kreise nicht trivial schneiden, gilt $x_1 \neq x_2$. Sei also oBdA $Re(x_1) \neq Re(x_2)$. Subtrahieren der beiden Gleichungen aus (16) liefert

$$\begin{aligned}(Im(z_r) - \underbrace{Im(x_1)}_{\in L})^2 - (Im(z_r) - \underbrace{Im(x_2)}_{\in L})^2 \\ = \underbrace{R_1^2 - R_2^2 + Re(x_2)^2 - Re(x_1)^2}_{\in L} + \underbrace{2(Re(x_1) - Re(x_2))}_{\in L} Re(z_r).\end{aligned} \tag{17}$$

Es folgt $Re(z_r) \in L(Im(z_r))$ und, da $i \in L$, folgt $L(z_r) \subseteq L(Im(z_r))$. Lösen wir nun (17) nach $Re(z_r)$ auf und setzen dies in eine der Gleichungen aus (16) ein, so sehen wir, dass $Im(z_r)$ Lösung einer quadratischen Gleichung über L ist. Also ist $[L(z_r) : L] \mid [L(Im(z_r)) : L] \in \{1, 2\}$. Insbesondere gilt also $L(z_r) = L(\sqrt{\alpha})$ für ein $\alpha \in L$. Also liegt z_r in einem Körper $L(\sqrt{\alpha})$, der aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln entsteht.

$\Longleftarrow$ Sei also $L/\mathbb{Q}$ eine Galoiserweiterung mit $[L : \mathbb{Q}] = 2^k$ und $z \in L$. Nach Proposition 4.3.4 gilt $|\operatorname{Gal}(L/\mathbb{Q})| = 2^k$. Damit ist $\operatorname{Gal}(L/\mathbb{Q})$ eine 2-Gruppe und somit existiert nach Lemma 1.1.44 eine Normalenreihe

$$\{\mathrm{id}\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = \operatorname{Gal}(L/\mathbb{Q}) \tag{18}$$

mit ${}^{G_i}/_{G_{i-1}} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ für alle $i \in \{1, \ldots, k\}$. Wenden wir den Hauptsatz der Galoistheorie 4.3.7 auf die Kompositionsreihe (18) an, so erhalten wir eine Körperkette

$$\mathbb{Q} = L^{G_k} \subset L^{G_{k-1}} \subset \cdots \subset L^{G_0} = L \ni z. \tag{19}$$

Mit Proposition 4.3.8 erhalten wir $[L^{G_{i-1}} : L^{G_i}] = |G_i/G_{i-1}| = 2$, für alle $i \in \{1, \dots, k\}$. Also ist $L^{G_{i-1}} = L^{G_i}(\sqrt{\omega_i})$ mit $\omega_i \in L^{G_i}$.

Da Z ein Körper ist und nach Lemma 4.5.6 Wurzeln aus konstruierten Zahlen konstruierbar sind, gilt damit

$$L^{G_i} \subseteq Z \Longrightarrow L^{G_{i-1}} \subseteq Z.$$

Da $L^{G_k} = \mathbb{Q} \subset Z$ gilt, folgt induktiv $L^{G_0} = L \subseteq Z$. Damit ist insbesondere z mit Zirkel und Lineal konstruierbar.

□

Wir können natürlich auch mehr als zwei Punkte vorgeben und Zahlen aus $\{0, 1, z_1, \dots, z_r\}$, mit $z_1, \dots, z_r \in \mathbb{C}$ beliebig, mit Zirkel und Lineal konstruieren. Damit erhalten wir analog zum vorherigen Theorem:

THEOREM 4.5.11. *Seien $z_1, \dots, z_r \in \mathbb{C}$ beliebig. Dann ist $z \in \mathbb{C}$ aus den Elementen $0, 1, z_1, \dots, z_r$ mit Hilfe von Zirkel und Lineal konstruierbar, genau dann wenn eine Galoiserweiterung $L/\mathbb{Q}(z_1, \overline{z_1}, \dots, z_r, \overline{z_r})$ existiert mit $z \in L$ und $[L : \mathbb{Q}(z_1, \overline{z_1}, \dots, z_r, \overline{z_r})] = 2^k$.*

4.5.12. Wir wollen nun die Probleme aus 4.5.2 lösen.

Zur Winkeldreiteilung: Kann jeder Winkel α mit Zirkel und Lineal gedrittelt werden?

Algebraische Übersetzung: Lässt sich aus $0, 1, e^{i\alpha}$ die Zahl $e^{i\alpha/3}$ konstruieren?

Antwort: Nein! Wählen wir etwa $\alpha = \frac{2\pi}{3}$, dann ist $e^{i\alpha} = \zeta_3$ eine primitive dritte Einheitswurzel und $e^{i\alpha/3} = \zeta_9$ eine primitive neunte Einheitswurzel. Die Winkeldreiteilung von α ist nach Theorem 4.5.11 genau dann möglich, wenn eine Galoiserweiterung $L/\mathbb{Q}(\zeta_3, \overline{\zeta_3}) = \mathbb{Q}(\zeta_3)$ existiert mit $\zeta_9 \in L$ und $[L : \mathbb{Q}(\zeta_3)] = 2^k$. Beachte, dass $\zeta_3 = \zeta_9^3 \in \mathbb{Q}(\zeta_9)$ liegt. Mit Theorem 4.4.4 gilt

$$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \varphi(3) = 2 \text{ und } [\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6.$$

Die Gradformel liefert uns somit

$$[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_3)] = \frac{[\mathbb{Q}(\zeta_9) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_3) : \mathbb{Q}]} = 3.$$

Sei nun F irgendeine endliche Körpererweiterung von $\mathbb{Q}(\zeta_3)$ mit $\zeta_9 \in F$. Dann gilt

$$[F : \mathbb{Q}(\zeta_3)] = [F : \mathbb{Q}(\zeta_9)] \cdot [\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_3)] = 3 \cdot [F : \mathbb{Q}(\zeta_9)].$$

Insbesondere ist $[F : \mathbb{Q}(\zeta_3)]$ keine 2er Potenz. Es gibt also keinen Körper L mit den geforderten Eigenschaften. Damit ist ζ_9 nicht aus $0, 1, \zeta_3$ konstruierbar. Dies bedeutet gerade, dass der Winkel $\alpha = \frac{2\pi}{3}$ nicht mit Zirkel und Lineal gedrittelt werden kann.

Zum Delischen Problem: Übung.

Zur Quadratur des Kreises: Lässt sich aus einem gegebenen Kreis ein flächengleiches Quadrat konstruieren?

Algebraische Übersetzung: Der Flächeninhalt des Einheitskreises ist gleich π. Die Kantenlänge eines flächengleichen Quadrates ist also $\sqrt{\pi}$. Damit gilt

$$\begin{aligned} & \text{Die Quadratur des Kreises ist möglich} \\ \iff\ & \sqrt{\pi} \text{ ist mit Zirkel und Lineal konstruierbar} \\ \overset{4.5.5,4.5.6}{\iff}\ & \pi \text{ ist mit Zirkel und Lineal konstruierbar} \\ \overset{4.5.10}{\iff}\ & \exists L/\mathbb{Q} \text{ Galois (endlich!) mit } \pi \in L \text{ und } [L:\mathbb{Q}] = 2^k \end{aligned}$$

Dies ist aber nicht möglich, da π transzendent über $\mathbb{Q}$ ist und somit in keiner endlichen Körpererweiterung von $\mathbb{Q}$ liegt. Es folgt, dass die Quadratur des Kreises unmöglich ist!

Zu den regulären n-Ecken: Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $e^{i2\pi/n} = \zeta_n$ konstruierbar ist.

LEMMA 4.5.13. *ζ_n ist konstruierbar $\iff \varphi(n) = 2^k$.*

BEWEIS. Der Beweis ist eine einfache Folgerung aus Theorem 4.5.10.

- $\Longleftarrow$ $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist mit Satz 4.4.3 eine Galoiserweiterung und es gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ (siehe Theorem 4.4.7). Ist nun $\varphi(n) = 2^k$, so ist ζ_n nach Theorem 4.5.10 konstruierbar.
- $\Longrightarrow$ Sei ζ_n konstruierbar. Dann existiert also eine Galoiserweiterung L/K mit $[L:\mathbb{Q}] = 2^m$ und $\mathbb{Q}(\zeta_n) \subseteq L$. Mit der Gradformel gilt

  $$2^m = [L:\mathbb{Q}(\zeta_n)] \cdot [\mathbb{Q}(\zeta_n):\mathbb{Q}] \overset{4.4.7}{=} [L:\mathbb{Q}(\zeta_n)] \cdot \varphi(n).$$

  Also ist $\varphi(n)$ ein Teiler von 2^m, und somit ebenfalls eine 2er Potenz.

□

Sei nun $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von n. Dann gilt

$$\varphi(n) = p_1^{e_1-1}(p_1-1) \cdots p_r^{e_r-1}(p_r-1).$$

Dies ist eine 2er Potenz, genau dann wenn $n = 2^e p_1 \cdots p_r$, mit $e \in \mathbb{N}_0$ beliebig und paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ mit $p_i - 1 = 2^{k_i}$ für alle $i \in \{1, \ldots, r\}$. Solche Primzahlen heißen *Fermat-Primzahlen.* Fermat-Primzahlen sind z.B.: 3, 5, 17, 257, 65537. Dies sind die einzigen bekannten Beispiele!

4.6. Auflösbarkeit algebraischer Gleichungen

Sei K ein Körper der Charakteristik 0 und $\overline{K}$ ein algebraischer Abschluss von K. Für eine quadratische Gleichung $ax^2+bx+c \in K[x]$ gilt bekanntlich,

dass die Nullstellen gegeben sind durch

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Wir haben also eine algebraische Lösungsformel für quadratische Gleichungen in einer Variablen über dem Körper K. In diesem Abschnitt werden wir zeigen, dass eine solche Formel für $f(x) = 0$, $f(x) \in K[x]$, nur existiert wenn $\text{grad}(f) \leq 4$ ist.

DEFINITION 4.6.1. Sei $f(x) \in K[x]$, $\text{char}(K) = 0$. Dann heißt die Gleichung $f(x) = 0$ *durch Radikale auflösbar*, genau dann wenn sich alle Nullstellen von $f(x)$ in $\overline{K}$ aus K durch die Operationen $+$, $-$, $\cdot$, $\div$ und $\sqrt[n]{\cdot}$, $n \in \mathbb{N}$, darstellen lassen.

Diese Definition ist äquivalent zur Folgenden.

DEFINITION 4.6.1.' Sei $f(x) \in K[x]$, $\text{char}(K) = 0$, und $L \subseteq \overline{K}$ ein Zerfällungskörper von $f(x) \in K[x]$. Dann ist $f(x) = 0$ *durch Radikale auflösbar*, genau dann wenn es einen Körper E_n mit $L \subseteq E_n$ gibt und eine Körperkette

$$K = E_0 \subseteq E_1 = E_0(\omega_1) \subseteq E_2 = E_1(\omega_2) \subseteq \cdots \subseteq E_{n-1}(\omega_n) = E_n$$

so, dass für alle $i \in \{1, \ldots, n\}$ ein $k_i \in \mathbb{N}$ existiert mit $\omega_i^{k_i} \in E_{i-1}$.

Die Äquivalenz beider Aussagen sehen wir so: Gilt 6.1' so lässt sich per Konstruktion jedes Element in L (insbesondere also alle Nullstellen von $f(x)$) durch die Operationen $+$, $-$, $\cdot$, $\div$ und $\sqrt[n]{\cdot}$ ($\sqrt[k_i]{\cdot}$) darstellen. Damit gilt auch Definition 6.1.
Gilt auf der anderen Seite 6.1 so lässt sich jede Nullstelle von $f(x)$ schreiben als z.B.

$$\sqrt[7]{\frac{\sqrt[5]{a + \sqrt{bc}} \pm b \cdot 8}{\sqrt[3]{a+b} \mp 5}}, \text{ mit } a, b, c \in K$$

so erhalten wir einen Körperturm

$$K = E_0 \subseteq E_1 = E_0(\sqrt{bc}) \subseteq E_2 = E_1(\sqrt[3]{a+b}) \subseteq E_3 = E_2(\sqrt[5]{a + \sqrt{bc}})$$
$$\subseteq E_4 = E_3(\sqrt[7]{\frac{\sqrt[5]{a + \sqrt{bc}} \pm b \cdot 8}{\sqrt[3]{a+b} \mp 5}}).$$

Der Körper E_4 enthält K und alle Nullstellen von $f(x)$. Damit enthält E_4 auch den Zerfällungskörper L von $f(x) \in K[x]$ - also gilt tatsächlich auch 6.1'.

DEFINITION 4.6.2. Seien $T, y_1, \ldots, y_n$ Variablen über dem Körper K. Wir definieren das Polynom

$$P_n(T) = T^n + y_1 T^{n-1} + \ldots + y_n \in K(y_1, \ldots, y, n)[T]. \tag{20}$$

Die Gleichung $P_n(T) = 0$ heißt *allgemeine Gleichung n-ten Grades.*

BEMERKUNG 4.6.3. Es gibt eine allgemeine algebraische Lösungsformel für Nullstellen eines beliebigen Polynoms vom Grad n über einem gegebenen Körper K mit $\mathrm{char}(K) = 0$ genau dann, wenn die Nullstellen eines beliebigen Polynoms vom Grad n immer auf dieselbe Art mit den Operationen aus 6.1 ausgedrückt werden können. Dies ist genau dann der Fall, wenn die allgemeine Gleichung n-ten Grades $P_n(T) = 0$ aus (20) durch Radikale auflösbar ist.

NOTATION 4.6.4. Sei $f \in K[x]$, $\mathrm{char}(K) = 0$, und $L \subseteq \overline{K}$ ein Zerfällungskörper von $f \in K[x]$. Dann ist L/K separabel ($\mathrm{char}(K) = 0$) und normal nach Proposition 4.1.4. Also ist L/K eine Galoiserweiterung. Wir schreiben dann $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$ und sprechen von der *Galoisgruppe von* f.

SATZ 4.6.5. *Sei* $P_n(T) \in K(y_1, \ldots, y, n)[T]$ *das Polynom aus* (20)*, wobei* K *ein Körper ist und* $y_1, \ldots, y_n$ *Variablen sind. Weiter bezeichnen wir mit* L *den Zerfällungskörper von* $P_n(T)$ *über* $K(y_1, \ldots, y, n)$*. Dann ist die Erweiterung* $L/K(y_1, \ldots, y, n)$ *Galois und es gilt* $\mathrm{Gal}(P_n(T)) \cong S_n$*.*

BEWEIS. Seien $\beta_1, \ldots, \beta_n$ sämtliche Nullstellen von $P_n(T)$ in einem algebraischen Abschluss von $K(y_1, \ldots, y_n)$. Sei $x_1, \ldots, x_n$ eine weitere Menge von Variablen über K, und seien $s_0, \ldots, s_n \in K[x_1, \ldots, x_n]$ die elementaren symmetrischen Polynome aus Definition 4.3.11. Dann gilt

$$P_n(T) = (T - \beta_1) \cdots (T - \beta_n) = \sum_{i=0}^{n} (-1)^i s_i(\beta_1, \ldots, \beta_n) T^{n-i}.$$

Dies sehen wir wieder durch den Satz von Vieta. Koeffizientenvergleich liefert nun

$$y_i = (-1)^i s_i(\beta_1, \ldots, \beta_n) \text{ für alle } i \in 1, \ldots, n. \tag{21}$$

Sei $\varphi' : K[x_1, \ldots, x_n] \longrightarrow K[\beta_1, \ldots, \beta_n]$ der Einsetzhomomorphismus zur Menge $\{\beta_1, \ldots, \beta_n\}$. Schränken wir φ' auf den Ring $K[s_1, \ldots, s_n]$ ein, so erhalten wir einen Homomorphismus $\varphi : K[s_1, \ldots, s_n] \longrightarrow K[y_1, \ldots, y_n]$. Die Gleichung in (21) induziert eine Umkehrabbildung von φ. Damit ist φ sogar ein Ring-Isomorphismus welcher sich kanonisch zu einem K-Isomorphismus der zugehörigen Quotientenkörper fortsetzt - diese Fortsetzung bezeichnen wir weiterhin mit φ.
Die Fortsetzung von φ^{-1} auf $(K[y_1, \ldots, y_n])[T]$ bildet das Polynom $P_n(T)$ auf das Polynom $g(T) = \sum_{i=0}^{n} (-1)^i s_i(x_1, \ldots, x_n) T^{n-i}$ ab. Damit müssen auch die jeweiligen Zerfällungskörper isomorph sein. Der Zerfällungskörper

von $g(T)$ ist gerade $K(x_1, \ldots, x_n)$. Aus Beispiel 4.3.12 folgt somit

$$\mathrm{Gal}(P_n(T)) \cong \mathrm{Gal}(K(x_1, \ldots, x_n)/K(s_1, \ldots, s_n)) \cong S_n.$$

Das war zu zeigen. □

Ist G eine Gruppe und F ein Körper, so bildet die Menge gegeben durch $\{f : G \to F | f$ Abbildung$\}$ einen F-Vektorraum, bezüglich der Verknüpfungen

- $(f + g)(a) = f(a) + g(a)$
- $(\lambda f(a)) = \lambda(f(a))$

für alle $a \in G$, alle $f, g : G \to F$ und alle $\lambda \in F$.
Solche Abbildungen sind Spezialfälle von *Charakteren*, die wir intensiv in Kapitel 6 studieren werden.

LEMMA 4.6.6 (Artinsches Lemma). *Sind $\chi_1, \ldots, \chi_n : G \longrightarrow F^*$ paarweise verschiedene Gruppen-Homomorphismen, dann sind $\chi_1, \ldots, \chi_n$ sogar F-linear unabhängig im Vektorraum $\{f : G \to F | f$ Abbildung$\}$.*

BEWEIS. Wir führen einen Widerspruchsbeweis. Angenommen es existieren paarweise verschiedene Gruppen-Homomorphismen $\chi_1, \ldots, \chi_n : G \longrightarrow F^*$, die F-linear abhängig sind. Sei dann n kleinstmöglich mit dieser Eigenschaft. Dann ist $n \geq 2$ und nach Annahme existieren Elemente $a_1, \ldots, a_n \in F$, nicht alle gleich Null, mit

$$a_1\chi_1 + \ldots + a_n\chi_n = 0. \tag{22}$$

Weil n minimal ist, folgt sogar dass $a_i \neq 0$ für alle $i \in \{1, \ldots, n\}$. Es ist $\chi_1 \neq \chi_2$, also existiert ein $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Aus (22) folgt für jedes $h \in G$

$$0 = a_1\chi_1(gh) + \cdots + a_n\chi_n(gh) = a_1\chi_1(g)\chi_1(h) + \ldots + a_n\chi_n(g)\chi_n(h).$$

Also gilt

$$a_1\chi_1(g)\chi_1 + \ldots + a_n\chi_n(g)\chi_n = 0. \tag{23}$$

Multiplizieren wir (22) mit $\chi_1(g)$ und subtrahieren (23) so erhalten wir

$$a_2\underbrace{(\chi_1(g) - \chi_2(g))}_{\neq 0}\chi_2 + \ldots + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0 \tag{24}$$

Dies ist eine nicht triviale F-Linearkombination von $\chi_2, \ldots, \chi_n$, die 0 ergibt. Also sind $\chi_2, \ldots, \chi_n$ paarweise verschieden und F-linear abhängig. Dies ist ein Widerspruch zur Minimalität von n. □

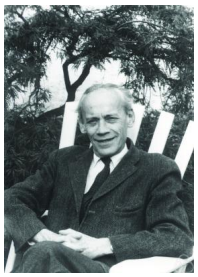


ABBILDUNG 4.5. Der östereichische Mathematiker *Emil Artin* (1898-1962) war einer der bedeutendsten Algebraiker des 20.Jahrhunderts und somit in weiten Teilen mitverantwortlich für die moderne Algebra wie wir sie heute kennen(lernen). Zu seinen Schülern zählt unter anderem Max Zorn.

KOROLLAR 4.6.7. *Seien M, L Körper und $\sigma_1, \ldots, \sigma_n : L \longrightarrow M$ paarweise verschiedene Körper-Homomorphismen. Dann sind $\sigma_1, \ldots, \sigma_n$ bereits M-linear unabhängig.*

BEWEIS. Für jedes $i \in \{1, \ldots, n\}$ ist $\sigma_i|_{L^*}$ ein Gruppen-Homomorphismus. Die Aussage folgt nun sofort aus dem Artinschen Lemma 4.6.6. □

SATZ 4.6.8. *Sei $n \in \mathbb{N}$ und K ein Körper mit $\mathrm{char}(K) \nmid n$ und $U_n \subset K$. Ist L/K eine Galoiserweiterung vom Grad n mit zyklischer Galoisgruppe, dann existiert ein $a \in K$ so, dass $L = K(\omega)$ für eine beliebige Nullstelle ω von $x^n - a \in K[x]$ in $\overline{K}$. Ist umgekehrt $\omega \in \overline{K}$, so dass $\omega^n \in K$ ist, dann ist $K(\omega)/K$ eine zyklische Galoiserweiterung.*

BEWEIS. Aus $\mathrm{char}(K) \nmid n$ folgt mit Lemma 4.4.2, dass $|U_n| = n = |\langle \zeta_n \rangle|$, für eine primitive n-te Einheitswurzel ζ_n, gilt. Weiter ist nach Voraussetzung

$$\mathrm{Gal}(L/K) = \langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma \circ \sigma = \sigma^2, \ldots, \sigma^{n-1}\}.$$

Die n Elemente $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ sind nach Korollar 4.6.7 L-linear unabhängig. Also gibt es ein $\alpha \in L$ mit

$$L \ni \Theta = \alpha + \zeta_n \sigma(\alpha) + \zeta_n^2 \sigma^2(\alpha) + \cdots + \zeta_n^{n-1} \sigma^{n-1}(\alpha) \neq 0.$$

Wir berechnen nun $\sigma(\Theta)$. Es gilt $\zeta_n \in U_n \subset K$, $\sigma^n = \mathrm{id}$ und $\zeta_n^n = 1$. Damit erhalten wir

$$\begin{aligned} \sigma(\Theta) &= \sigma(\alpha) + \sigma(\zeta_n)\sigma^2(\alpha) + \cdots + \sigma(\zeta_n^{n-1})\sigma^n(\alpha) \\ &= \sigma(\alpha) + \zeta_n \sigma^2(\alpha) + \cdots + \zeta_n^{n-1}\alpha = \zeta_n^{-1}\Theta. \end{aligned}$$

Induktiv folgt

$$\sigma^2(\Theta) = \sigma(\sigma(\Theta)) = \sigma(\zeta_n^{-1}\Theta) = \sigma(\zeta_n^{-1})\sigma(\Theta) = \zeta_n^{-1}\zeta_n^{-1}\Theta = \zeta_n^{-2}\Theta,$$

und allgemein

$$\sigma^j(\Theta) = \zeta_n^{-j}\Theta. \tag{25}$$

für alle $j \in \{1, \ldots, n\}$. Das Element ζ_n hat Ordnung n und mit (25) folgt

$$\sigma^j(\Theta) \neq \sigma^i(\Theta) \text{ für alle } i \neq j \in \{1, \ldots, n\}. \tag{26}$$

Damit folgt

$$\begin{aligned} n = [L : K] \geq [K(\Theta) : K] &\overset{4.2.12}{=} |\operatorname{Hom}_K(K(\Theta), \overline{K})| \\ &\geq |\{\tau|_{K(\Theta)} | \tau \in \operatorname{Gal}(L/K)\}| \geq n. \end{aligned}$$

Es ist also $n = [L : K] = [K(\Theta) : K]$ und mit der Gradformel folgt $[L : K(\Theta)] = 1$, also $L = K(\Theta)$.
Wir haben also ein primitives Element Θ von L/K gefunden. Wir müssen noch zeigen, dass $a = \Theta^n$ ein Element aus K ist. (Denn damit ist dann Θ eine Nullstelle von $x^n - a \in K[x]$). Es ist

$$\sigma^j(a) = \sigma^j(\Theta)^n \overset{(25)}{=} (\zeta_n^{-j}\Theta)^n \overset{\zeta_n^n=1}{=} \Theta^n = a \text{ für alle } j \in \{1, \ldots, n\}.$$

Somit gilt $a \in L^{\operatorname{Gal}(L/K)} \overset{4.3.4}{=} K$. Somit gilt die Behauptung mit $\omega = \Theta$ und wegen $U_n \subset K$ folgt die Behauptung auch für alle anderen Nullstellen von $x^n - a \in K[x]$.
Die Rückrichtung wird in den Übungen behandelt. □

Definition 4.6.9. Sei L/K eine Galoiserweiterung. Dann heißt L/K *zyklisch*, *abelsch* oder *auflösbar*, genau dann wenn die jeweilige Eigenschaft auf die Galoisgruppe $\operatorname{Gal}(L/K)$ zutrifft.

Lemma 4.6.10. *Sei* $\operatorname{char}(K) = 0$ *und* L *ein Zerfällungskörper von* $f(x) \in K[x]$. *Weiter sei* F/K *ein Zerfällungskörper von* $g(x) \in K[x]$ *mit* $F \subseteq \overline{K} = \overline{L}$ *und* LF *das Kompositum von* L *und* F *in* $\overline{K}$. *Dann gilt*

(a) LF/K *auflösbar* $\iff$ LF/F *und* F/K *sind auflösbar.*
(b) $f(x) \cdot g(x) = 0$ *ist durch Radikale auflösbar* $\iff$ $f(x) = 0$, $f(x) \in F[x]$ *und* $g(x) = 0$ *sind durch Radikale auflösbar.*

Insbesondere gilt, falls $g(x) = 0$ *durch Radikale auflösbar ist, dann ist*

$f(x) = 0$, $f(x) \in K[x]$, *durch Radikale auflösbar* $\iff$ $f(x) = 0$, $f(x) \in F[x]$, *durch Radikale auflösbar.*

Beweis. In dem wir $\operatorname{char}(K) = 0$ und Proposition 4.1.4 benutzen sehen wir, dass F/K, L/K, LF/F und LF/K tatsächlich Galoiserweiterungen sind (das wird auch teilweise in den Übungen gezeigt).

Zu (a): Es ist $\operatorname{Gal}(LF/F) \subseteq \operatorname{Gal}(LF/K)$ und mit Theorem 4.3.7 gilt $F = (LF)^{\operatorname{Gal}(LF/F)}$. Da F/K eine Galoiserweiterung ist, folgt mit Proposition 4.3.8 (f), dass $\operatorname{Gal}(LF/F)$ ein Normalteiler von $\operatorname{Gal}(LF/K)$ ist. Also erhalten wir mit Proposition 4.3.8 (g)

$$\operatorname{Gal}(LF/K)/\operatorname{Gal}(LF/F) \cong \operatorname{Gal}(F/K).$$

Nach Proposition 1.1.39 wissen wir, dass eine Gruppe G genau dann auflösbar ist, wenn für einen Normalteiler N von G sowohl N als auch G/N auflösbar sind. Wenden wir dies auf unsere Vorüberlegungen an so erhalten wir, dass $\mathrm{Gal}(LF/K)$ genau dann auflösbar ist wenn $\mathrm{Gal}(LF/F)$ und $\mathrm{Gal}(F/K)$ auflösbar sind. Das war zu zeigen.

Zu (b): Wir beweisen zunächst die Richtung von Links nach Rechts. Sei also $f(x) \cdot g(x) = 0$ durch Radikale auflösbar. Das bedeutet, dass sich die Nullstellen von $f(x)\cdot g(x)$, also die Nullstellen von $f(x)$ und die Nullstellen von $g(x)$, aus K durch die Operationen $+$, $-$, $\cdot$, $\div$ und $\sqrt[n]{\cdot}$ ausdrücken lassen. Damit ist $g(x) = 0$ über K auflösbar. Da $F \supseteq K$ gilt, ist insbesondere auch $f(x) = 0$ über F durch Radikale auflösbar.

Für die Rückrichtung nehmen wir Körperketten wie in 4.6.1'

$$K = E_0 \subseteq E_1 = E_0(\omega_1) \subseteq \cdots \subseteq E_{r-1}(\omega_r) = E_r$$

mit $F \subseteq E_r$, und

$$F = F_r \subseteq F_{r+1} = F_r(\omega_{r+1}) \subseteq \cdots \subseteq F_{s-1}(\omega_s) = F_s$$

mit $LF \subseteq F_s$, und so dass $\omega_i^{k_i} \in E_{i-1}$, bzw. $\in F_{i-1}$, für gewisse $k_1, \ldots, k_s \in \mathbb{N}$. Beachte, dass LF gerade der Zerfällungskörper von $f(x) \in F[x]$ ist.

Bilden wir nun in der zweiten Kette das Kompositum mit E_r so erhalten wir

$$K = E_0 \subseteq \cdots \subseteq E_r \overset{F\subseteq E_r}{=} F_rE_r(\omega_{r+1}) = F_{r+1}E_r \subseteq \cdots \subseteq F_sE_r$$

mit derselben Bedingung für die ω_i, $i \in \{1, \ldots, s\}$, wie oben und mit $LF \subseteq F_sE_r$. Per Konstruktion ist LF der Zerfällungskörper von $f(x) \cdot g(x) \in K[x]$. Damit ist wie gewünscht $f(x) \cdot g(x) = 0$ durch Radikale auflösbar.

□

THEOREM 4.6.11. *Sei $f(x) \in K[X]$, $\mathrm{char}(K) = 0$. Dann ist $f(x) = 0$ auflösbar durch Radikale, genau dann wenn $\mathrm{Gal}(f)$ eine auflösbare Gruppe ist.*

BEWEIS. Wir zeigen zunächst, dass wir, um die Aussage zu beweisen, $U_n \subset K$ für beliebiges n annehmen dürfen. Sei dazu $n \in \mathbb{N}$ beliebig. Nach Lemma 4.4.2 ist $|U_n| = n$ und $U_n = \langle \zeta_n \rangle$ ist zyklisch. Der Zerfällungskörper von $x^n - 1 \in K[x]$ ist also gegeben durch $K(\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}) = K(\zeta_n)$. Wie immer ($\mathrm{char}(K) = 0$ + Zerfällungskörper) ist $K(\zeta_n)/K$ eine Galoiserweiterung. Wir

werden im nächsten Abschnitt sehen, dass $K(\zeta_n)/K$ abelsch, also auflösbar, ist.
Sei L der Zerfällungskörper von $f(x) \in K[x]$, dann ist mit Lemma 4.6.10 (a)

$$L(\zeta_n) = L(K(\zeta_n))/K \text{ auflösbar } \iff L(\zeta_n)/K(\zeta_n) \text{ auflösbar.} \tag{27}$$

(Die Bedingung $K(\zeta_n)/K$ auflösbar ist ohnehin immer erfüllt). Weiter ist $x^n - 1 \in K[x]$ offensichtlich durch Radikale auflösbar. Mit Lemma 4.6.10 (b) folgt also auch

$$f(x) = 0, f(x) \in K[x], \text{ durch Radikale auflösbar} \iff$$
$$f(x) = 0, f(x) \in K(\zeta_n)[x], \text{ durch Radikale auflösbar.} \tag{28}$$

Fassen wir (27) und (28) zusammen, so erhalten wir, dass wir oBdA annehmen dürfen, dass $U_n \subset K$ für belibiges $n \in \mathbb{N}$.

Mit Hilfe dieser Vorüberlegungen beweisen wir nun das Theorem.

$\Longleftarrow$ Sei also $\mathrm{Gal}(f)$ auflösbar. Das bedeutet L/K ist auflösbar. Es existiert also eine Normalreihe

$$\{\mathrm{id}\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_r = \mathrm{Gal}(f) = \mathrm{Gal}(L/K) \tag{29}$$

mit zyklischen Faktoren ${}^{G_i}/_{G_{i-1}} \cong {}^{\mathbb{Z}}/_{p_i\mathbb{Z}}$, wobei p_i eine Primzahl ist für alle $i \in \{1, \ldots, r\}$.

Bilden wir nun die Fixkörper von der Kompositionsreihe (29), so erhalten wir nach Proposition 4.3.8 einen Körperturm

$$L = L^{G_0} \supseteq L^{G_1} \supseteq \cdots \supseteq L^{G_r} = K \tag{30}$$

so, dass $L^{G_{i-1}}/L^{G_i}$ eine Galoiserweiterung für alle $i \in \{1, \ldots, r\}$ ist, mit

$$\mathrm{Gal}(L^{G_{i-1}}/L^{G_i}) \overset{4.3.8(g)}{\cong} {}^{\mathrm{Gal}(L/L^{G_i})}/_{G_{i-1}} \overset{4.3.5}{\cong} {}^{G_i}/_{G_{i-1}} \overset{\text{Vor.}}{\cong} {}^{\mathbb{Z}}/_{p_i\mathbb{Z}}.$$

Nach dem Satz von Lagrange 1.1.17 gilt $p_i = |{}^{G_i}/_{G_{i-1}}|$ ist ein Teiler von $|\mathrm{Gal}(f)| =: n$. Wir dürfen nach dem Beginn des Beweises annehmen, dass $U_n \subset K$ ist. Da $p_i | n$ für alle $i \in \{1, \ldots, r\}$, gilt damit $U_{p_i} \subseteq U_n \subset K \subseteq L^{G_i}$. Nach Lemma 4.6.8 existiert also für alle $i \in \{1, \ldots, r\}$ ein $\omega_i \in L^{G_{i-1}}$ mit $\omega_i^{p_i} \in L^{G_i}$ und $L^{G_{i-1}} = L^{G_i}(\omega_i)$. Damit lässt sich (30) schreiben als

$$K = L^{G_r} \subseteq L^{G_{r-1}} = L^{G_r}(\omega_i) \subseteq \cdots \subseteq L^{G_1}(\omega_1) = L^{G_0} = L.$$

Dies bedeutet nichts anderes als, dass $f(x) = 0$ durch Radikale auflösbar ist, was wir zeigen wollten.

$\Longrightarrow$ Sei also $f(x) = 0$ durch Radikale auflösbar. Dann existiert eine Körperkette

$$K = E_0 \subseteq E_1 = E_0(\omega_1) \subseteq \cdots \subseteq E_r = e_{r-1}(\omega_r) = E_r \tag{31}$$

mit $L \subseteq E_r$ für einen Zerfällungskörper L von $f(x) \in K[x]$ und so, dass für alle $i \in \{1, \ldots, r\}$ ein $k_i \in \mathbb{N}$ existiert mit $\omega_i^{k_i} \in E_{i-1}$.

Sei $m = \prod_{i=1}^{r} k_i$, dann dürfen wir wieder annehmen, dass $U_m \subset K$ ist. Mit Satz 4.4.8 wissen wir nun, dass $E_{i-1}(\omega_i) = E_i/E_{i-1}$ eine Galoiserweiterung mit zyklischer Galoisgruppe ist.

Nachdem wir die Kette (31) ähnlich wie im Beweis von Proposition 4.5.9 um endlich viele Schritte erweitern, dürfen wir auch E_r/K als Galoiserweiterung annehmen.

Mit dem Hauptsatz der Galoistheorie 4.3.7 existieren nun Untergruppen $G_i \subseteq \mathrm{Gal}(E_r/K)$ mit

$$K = E_0 = E_r^{G_r} \subseteq \underbrace{E_r^{G_{r-1}}}_{=E_1} \subseteq \underbrace{E_r^{G_{r-2}}}_{=E_2} \subseteq \cdots \subseteq E_r^{G_0} = E_r^{\{\mathrm{id}\}} = E_r \supseteq L.$$

Jede Erweiterung $E_r^{G_{i-1}}/E_r^{G_i}$, $i \in \{1, \ldots, r\}$, ist Galois. Proposition 4.3.8 (f) liefert uns nun

$$\{\mathrm{id}\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = \mathrm{Gal}(E_r/K)$$

und wie eben gilt ${}^{G_i}\!/_{G_{i-1}} \cong \mathrm{Gal}(E_r^{G_{i-1}}/E_r^{G_i})$ für alle $i \in \{1, \ldots, r\}$. Also ist ${}^{G_i}\!/_{G_{i-1}}$ zyklisch, und somit abelsch, für alle $i \in \{1, \ldots, r\}$. Dies bedeutet gerade, dass $\mathrm{Gal}(E_r/K)$ auflösbar ist. Wir müssen die Auflösbarkeit von $\mathrm{Gal}(L/K)$ zeigen. Da Quotienten von auflösbaren Gruppen auflösbar sind, folgt dies aus

$$\mathrm{Gal}(L/K) \overset{4.3.7}{=} \mathrm{Gal}(E_r^{\mathrm{Gal}(E_r/L)}/K) \overset{4.3.8(f)+(g)}{\cong} {}^{\mathrm{Gal}(E_r/K)}\!/_{\mathrm{Gal}(E_r/L)}.$$

Somit ist $\mathrm{Gal}(L/K) = \mathrm{Gal}(f)$ auflösbar, was zu zeigen war.

□

KOROLLAR 4.6.12. *Sei* $\mathrm{char}(K) = 0$ *und* $f(x) \in K[X]$ *mit* $\mathrm{grad}(f) \leq 4$. *Dann ist* $f(x) = 0$ *durch Radikale auflösbar.*

BEWEIS. Die Gruppe $\mathrm{Gal}(f)$ ist nach Lemma 4.3.9 isomorph zu einer Untergruppe von der symmetrischen Gruppe S_4 und S_4 ist auflösbar (siehe 1.1.45). Da Untergruppen von auflösbaren Gruppen wieder auflösbar sind, ist also $\mathrm{Gal}(f)$ auflösbar. Mit Theorem 4.6.11 ist somit $f(x) = 0$ durch Radikale auflösbar. □

KOROLLAR 4.6.13. *Sei* $\mathrm{char}(K) = 0$. *Dann ist die allgemeine Gleichung n-ten Grades* $P_n(T) = 0$ *genau dann durch Radikale auflösbar, wenn* $n \leq 4$ *ist. Insbesondere gibt es nur für Polynome vom Grad* ≤ 4 *allgemeine algebraische Lösungsformeln!*

BEWEIS. Die Gleichung $P_n(T) = 0$ ist nach Theorem 4.6.11 genau dann durch Radikale auflösbar wenn die Gruppe $\mathrm{Gal}(P_n(T))$ auflösbar ist. In Satz 4.3.5 haben wir gesehen, dass diese Gruppe isomorph zur symmetrischen Gruppe S_n ist. Aus der Gruppentheorie (siehe Satz 1.1.45) wissen wir, dass S_n genau dann auflösbar ist, wenn $n \leq 4$ gilt.
Dass hieraus die zweite Behauptung des Korollars folgt haben wir in 4.6.3 bemerkt. □

BEMERKUNG 4.6.14. Für explizite Formeln in den Fällen $n = 3, 4$ verweisen wir auf [**Bo**], 6.2. Diese komplizierten Formeln werden Cardano zugeschrieben, stammen aber eigentlich von del Ferro, Tartaglia und Ferrari (16. Jahrhundert).

ABBILDUNG 4.6. *Nils Hendrik Abel* (1802-1829) bewies als erster, dass sich eine allgemeine Gleichungen fünften Grades nicht durch Radikale auflösen lässt. Er lebte in seinen letzten Jahren von Schulden und Zuwendungen befreundeter Mathematiker. Trotz seines kurzen Lebens fand er auch bedeutende Resultate und Konzepte in anderen mathematischen Disziplinen. Hermite meinte: *„Abel hat den Mathematikern genug hinterlassen um sie für 500 Jahre zu beschäftigen.“*

KAPITEL 5

Modultheorie

5.1. Grundlagen

In der linearen Algebra wurden intensiv Vektorräume über einem Körper K studiert. Dies sind abelsche Gruppen mit einer zusätzlichen Skalarmultiplikation mit K. Wir wollen unter anderem untersuchen welche Resultate über Vektorräume sich verallgemeinern lassen, wenn wir K durch einen Ring R ersetzen. Sei also stets $R \neq \{0\}$ ein Ring (mit Einselement).

DEFINITION 5.1.1. Ein *R-Linksmodul* ist eine abelsche Gruppe $(M, +)$ mit einer Verknüpfung

$$. : R \times M \longrightarrow M \quad ; \quad (r, m) \mapsto r.m,$$

so dass für alle $m, m_1, m_2 \in M$ und $a, b \in R$ gilt

(i) $1.m = m$
(ii) $a.(m_1 + m_2) = a.m_1 + a.m_2$
(iii) $(a + b).m = a.m + b.m$
(iv) $(ab).m = a.(b.m)$

Analog definiert man einen *R-Rechtsmodul* als abelsche Gruppe $(M, +)$ mit einer Verknüpfung

$$. : M \times R \longrightarrow M \quad ; \quad (m, r) \mapsto m.r,$$

so dass die zu $(i) - (iv)$ analogen Eigenschaften gelten.

Wir werden einen R-Links-, beziehungsweise R-Rechtsmodul, $(M, +, .)$ oft nur mit M bezeichnen. Die Verknüpfung $R \times M$, beziehungsweise $M \times R$, wird wie bei Vektorräumen *R-Skalarmultiplikation* genannt.
Wie bei Ringen folgt sofort aus der Definition 5.1.1, dass $0.m = 0$, $(-1).m = -m$ und $r.0 = 0$ für alle $m \in M$ und alle $r \in R$ gilt.

DEFINITION 5.1.2. Für einen Ring $R = (R, +, \cdot)$ definieren wir den *entgegengesetzten Ring* zu R durch $R^{op} = (R, +, *)$, wobei $a * b = b \cdot a$ für alle $a, b \in R^{op}$ gilt.

LEMMA 5.1.3. *Es existiert eine bijektive Korrespondenz zwischen R-Linksmoduln und R^{op}-Rechtsmoduln. Diese ist gegeben durch*

$$\{M \ R\text{-Linksmodul}\} \overset{(M,+,.)\mapsto(M,+,*)}{\longleftrightarrow} \{M \ R^{op}\text{-Rechtsmodul}\},$$

wobei $m_* r = r.m$ für alle $m \in M$ und für alle $r \in R$ gilt.

BEWEIS. Übung. □

NOTATION 5.1.4. Lemma 5.1.3 sagt uns, dass wir jedem Rechtsmodul einen eindeutigen Linksmodul zuordnen können. Damit können wir Resultate über Rechtsmoduln auf Resultate über Linksmoduln zurückführen. Wir werden im Folgenden R-Linksmoduln betrachten und kurz *R-Moduln* nennen.

BEISPIEL 5.1.5. (i) Sei $(M,+)$ irgendeine abelsche Gruppe. Die Abbildung

$$\mathbb{Z} \times M \longrightarrow M \quad ; \quad (n,m) \mapsto n.m = \begin{cases} \underbrace{m + \cdots + m}_{n \text{ mal}} \text{ falls } n \geq 0 \\ -(\underbrace{m + \cdots + m}_{-n \text{ mal}}) \text{ sonst} \end{cases} \tag{32}$$

erfüllt alle Eigenschaften aus 5.1.1. Also ist jede abelsche Gruppe auf kanonische Weise ein $\mathbb{Z}$-Modul. Beachte, dass die leere Summe als Null definiert ist und somit auch $0.m$ durch (32) definiert ist.

(ii) Ist R ein Körper, so gilt

$$M \text{ ist ein } R\text{-Modul} \Longleftrightarrow M \text{ ist ein } R\text{-Vektorraum}$$

(iii) Jeder Ring ist selbst ein R-Modul mit der gegebenen Addition und der Multiplikation auf R als R-Skalarmultiplikation.

(iv) Sei K ein Körper und V ein K-Vektorraum. Dann ist $R = \mathrm{End}(V) = \{f : V \to V | f \text{ Gruppen-Hom.}\}$ ein Ring bezüglich $(f_1 + f_2)(v) = f_1(v) + f_2(v)$ und $(f_1 \circ f_2)(v) = f_1(f_2(v))$ für alle $f_1, f_2 \in R$ und alle $v \in V$. Dieser Ring ist im Allgemeinen nicht kommutativ (nie für $\dim(V) > 1$).

Den Vektorraum V können wir nun als R-Modul auffassen, durch die Abbildung

$$R \times V \to V \quad ; \quad (\varphi, v) \mapsto \varphi.v = \varphi(v).$$

Wir überprüfen die nötigen Eigenschaften aus 5.1.1. Seien dazu v, v_1, v_2 aus V und $\varphi, \varphi_1, \varphi_2$ aus R beliebig.

- id ist das Einselement in R und es gilt $\mathrm{id}\,.v = \mathrm{id}(v) = v$.
- $\varphi.(v_1 + v_2) = \varphi(v_1 + v_2) \overset{\text{Hom}}{=} \varphi(v_1) + \varphi(v_2)$.
- $(\varphi_1 + \varphi_2).v \overset{\text{Def.}}{=} \varphi_1(v) + \varphi_2(v)$.

– $(\varphi_1 \circ \varphi_2).v = \varphi_1(\varphi_2(v)) = \varphi_1.(\varphi_2.v)$.

Somit ist V tatsächlich ein R-Modul.

DEFINITION/SATZ 5.1.6. Sei A eine abelsche Gruppe, dann ist $\mathrm{End}(A)$ wie in Beispiel 5.1.5 *iv*) ein Ring, genannt der *Endomorphismenring* von A. Für einen Ring R und einen R-Modul M definieren wir den Endomorphismenring von R, beziehungsweise von M, als $\mathrm{End}(R) = \mathrm{End}(R,+)$, beziehungsweise $\mathrm{End}(M) = \mathrm{End}(M,+)$. Wir fassen also R und M als abelsche Gruppe auf.

BEWEIS. ganz einfach. □

Das Beispiel 5.1.5 *iv*) ist in gewisser Weise „fundamental“, wie die folgende Proposition zeigt.

PROPOSITION 5.1.7. *Sei $(M,+)$ eine abelsche Gruppe und R ein Ring. Dann gibt es eine bijektive Korrespondenz zwischen R-Modulstrukturen auf M und Ring-Homomorphismen von R nach* $\mathrm{End}(M)$. *Genauer:*

(a) *Wenn M ein R-Modul ist, so ist die Abbildung*

$$\varphi : R \longrightarrow \mathrm{End}(M) \quad ; \quad r \mapsto \mu_r,$$

wobei $\mu_r(m) = r.m$ für alle $m \in M$ gilt, ein Ring-Homomorphismus.

(b) *Ist umgekehrt $\varphi : R \longrightarrow \mathrm{End}(M)$ ein Ring-Homomorphismus, so ist M ein R-Modul, durch die Verknüpfung*

$$R \times M \quad ; \quad (r,m) \mapsto r.m = (\varphi(r))(m).$$

BEWEIS. Die Konstruktionen in (a) und (b) sind offensichtlich invers zueinander. Der Beweis besteht also alleine darin, die Eigenschaften eines Ring-Homomorphismus, beziehungsweise eines R-Moduls, nachzuprüfen.

Zu (a): Sei also M ein R-Modul. Als erstes zeigen wir, dass die Abbildung φ wohldefiniert ist. D.h.: $\mu_r \in \mathrm{End}(M)$ für alle $r \in R$.

Für $r \in R$ und $m_1, m_2 \in M$ beliebig, gilt $\mu_r(m_1+m_2) = r.(m_1+m_2) \overset{5.1.1(ii)}{=} r.m_1 + r.m_2 = \mu_r(m_1) + \mu_r(m_2)$. Also ist tatsächlich $\mu_r \in \mathrm{End}(M)$.

Weiter gilt $\varphi(1) = \mu_1$ und $\mu_1(m) = 1.m \overset{5.1.1(i)}{=} m$ für alle $m \in M$. Damit ist $\varphi(1) = \mathrm{id}$, und id ist wie bereits gesehen, dass Einselement in $\mathrm{End}(R)$.

Sind nun $r_1, r_2 \in R$ beliebig, so gilt $\varphi(r_1 + r_2) = \mu_{r_1+r_2}$ und es ist $\mu_{r_1+r_2}(m) = (r_1+r_2).m \overset{5.1.1(iii)}{=} r_1.m + r_2.m = \mu_{r_1}(m) + \mu_{r_2}(m)$ für alle $m \in M$. Dies zeigt $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$.

Zuletzt gilt $\varphi(r_1 r_2) = \mu_{r_1 r_2}$ und es ist $\mu_{r_1 r_2}(m) = (r_1 r_2).m \overset{5.1.1iv)}{=} r_1.(r_2.v) = \mu_{r1} \circ \mu_{r_2}(m)$ für alle $m \in M$. Also gilt auch $\varphi(r_1 r_2) =$

$\varphi(r_1) \circ \varphi(r_2)$. Dies zeigt, dass φ wie behauptet ein Ring-Homomorphismus ist.

Zu (b): Sei also $\varphi : R \longrightarrow \mathrm{End}(M)$ ein Ring-Homomorphismus. Wir müssen die Eigenschaften aus 5.1.1 überprüfen. Es gilt

- $1.m = (\varphi(1))(m) = \mathrm{id}(m) = m$ für alle $m \in M$.
- $(r_1 r_2).m = \varphi(r_1 r_2)(m) = \varphi(r_1) \circ \varphi(r_2)(m) = r_1.(r_2.m)$ für alle $r_1, r_2 \in R$ und alle $m \in M$.

Die anderen beiden Punkte folgen analog. Somit ist M ein R-Modul.

□

Ein R-Modul M ist also eine abelsche Gruppe zusammen mit einem Ring-Homomorphismus $R \longrightarrow \mathrm{End}(M)$. Insbesondere stellen wir wieder fest, dass jede abelsche Gruppe M eine eindeutige (!) Struktur als $\mathbb{Z}$-Modul besitzt, da es genau einen Ring-Homomorphismus $\mathbb{Z} \longrightarrow \mathrm{End}(M)$ gibt.

DEFINITION 5.1.8. Sei M ein R-Modul. Ein *Untermodul* von M ist eine Untergruppe $(N, +)$ von $(M, +)$ so, dass $r.n \in N$, für alle $n \in N$ und alle $r \in R$, gilt.
Sei M' ein weiterer R-Modul. Eine Abbildung $\varphi : M \longrightarrow M'$ heißt *R-Modul-Homomorphismus*, genau dann wenn

(i) φ ist ein Gruppen-Homomorphismus, und
(ii) $\varphi(r.m) = r.\varphi(m)$ für alle $r \in R$, $m \in M$.

Ein R-Modul-Homomorphismus $\varphi : M \longrightarrow M'$ heißt *R-Modul-Isomorphismus*, genau dann wenn es eine beidseitige Umkehrfunktion gibt, die selbst ein R-Modul-Homomorphismus ist.

Genau wie bei Gruppen und Ringen gilt, dass ein R-Modul-Homomorphismus ein Isomorphismus ist genau dann wenn er bijektiv ist.

BEMERKUNG 5.1.9. Wir fassen den Ring R als Linksmodul über sich selbst auf. Dann sind die Untermoduln von R genau die *Linksideale* von R. Analoges gilt für die *Rechtsideale* von R. Eine Teilmenge I von R die sowohl Links- als auch Rechtsideal ist, heißt *zweiseitiges Ideal* von R.

LEMMA 5.1.10. *Sei M ein R-Modul und N ein Untermodul von M. Dann ist M/N mit der Abbildung*

$$R \times M/N \longrightarrow M/N \quad ; \quad (r, m + N) \mapsto r.m + N$$

ein R-Modul, genannt Faktormodul.

BEWEIS. Wir wissen bereits, dass M/N eine abelsche Gruppe ist. Weiter ist die Abbildung $(r, m+N) \mapsto r.m+N$ wohldefiniert. Denn für $m+N = m'+N$ gilt $m' = m + n$ für ein $n \in N$. Daraus folgt, wie erforderlich,

$$r.m' + N = r.(m + n) + N = r.m + \underbrace{r.n}_{\in N} + N = r.m + N.$$

Nun können wir repräsentantenweise rechnen. Daraus folgen die R-Modul Axiome für M/N sofort aus denen von M. □

THEOREM 5.1.11 (Isomorphiesatz). *Seien M, M' R-Moduln und $\varphi : m \longrightarrow M'$ ein R-Modul-Homomorphismus. Dann ist $\varphi(M)$ ein Untermodul von M' und $\ker(\varphi)$ ein Untermodul von M. Weiter ist die Abbildung*

$$\Psi : M/\ker(\varphi) \xrightarrow{\sim} \varphi(M) \quad ; \quad m + \ker(\varphi) \mapsto \varphi(m)$$

ein wohldefinierter R-Modul-Isomorphismus.

BEWEIS. Die Aussagen sind alle bereits für Gruppen bekannt. Wir müssen also nur noch die R-Linearität nachpr$\ddot{}$fen.
$\varphi(M)$ ist Untermodul von M': Sei also $m' \in \varphi(M)$. Dann existiert ein $m \in M$ mit $\varphi(m) = m'$. Es ist somit für beliebiges $r \in R$

$$r.m' = r.\varphi(m) = \varphi(\underbrace{r.m}_{\in M}) \in \varphi(M).$$

$\ker(\varphi)$ ist Untermodul von M: Sei $m \in \ker(\varphi)$ und $r \in R$. Dann ist $\varphi(r.m) = r.\varphi(m) = r.0 = 0$. Also ist auch $r.m \in \ker(\varphi)$.
Ψ ist ein R-Modul-Isomorphismus: Wie bereits erwähnt ist nur noch die R-Linearität zu überprüfen. Für $m + \ker(\varphi) \in M/\ker(\varphi)$ und $r \in R$ beliebig, gilt

$$\Psi(r.(m+\ker(\varphi))) = \Psi(r.m+\ker(\varphi)) = \varphi(r.m) = r.\varphi(m) = r.\Psi(m+\ker(\varphi)).$$

Damit ist der Isomorphisatz bewiesen. □

5.2. Freie Moduln

Sei wieder $R \neq 0$ ein Ring. Wir wissen, dass jeder Vektorraum eine Basis besitzt. Dies können wir für beliebige R-Moduln sicher nicht erwarten. Wir werden hier studieren, wann und wie das Konzept einer Basis auf R-Moduln übertragbar ist.

KONSTRUKTION 5.2.1. Sind M_1, M_2 zwei R-Moduln, so ist auch$M_1 \times M_2$ ein R-Modul mit der R-Skalarmultiplikation $r.(m_1, m_2) = (r.m_1, r.m_2)$ für alle $r \in R$ und $(m_1, m_2) \in M_1 \times M_2$. Diese Konstruktion wollen wir auf beliebig viele R-Moduln erweitern.

Sei dazu I irgendeine Indexmenge und sei $(M_i)_{i\in I}$ eine Familie von R-Moduln. Das *direkte Produkt* der R-Moduln $(M_i)_{i\in I}$ ist gegeben durch

$$\prod_{i\in I} M_i = \{(a_i)_{i\in I} | a_i \in M_i \text{ für alle } i \in I\}.$$

Mit der komponentenweise definierten Addition und R-Skalarmultiplikation ist $\prod_{i\in I} M_i$ selbst ein R-Modul. Es gilt $r.0 = 0$ für alle $r \in R$, damit ist

$$\oplus_{i\in I} M_i = \{(a_i)_{i\in I} \in \prod_{i\in I} M_i | a_i \neq 0 \text{ für nur endlich viele } i \in I\}$$

ein Untermodul von $\prod_{i\in I} M_i$. Diesen nennen wir die *direkte Summe* der R-Moduln $(M_i)_{i\in I}$. Ist die Menge I endlich, so gilt natürlich $\prod_{i\in I} M_i = \oplus_{i\in I} M_i$.

PROPOSITION 5.2.2. *Sei $(N_i)_{i\in I}$ eine Familie von Untermoduln eines R-Moduls M.*

(a) *Es ist*

$$\sum_{i\in I} N_i = \{\sum_{i\in I_0} a_i | I_0 \subseteq I \text{ endlich, und } a_i \in N_i \text{ für alle } i \in I_0\}$$

ein Untermodul von M, genannt die Summe *der $(N_i)_{i\in I}$.*

(b) *Folgende Aussagen sind äquivalent*

(i) $\varphi : \oplus_{i\in I} N_i \longrightarrow M;\ (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i$ *ist ein R-Modul-Isomorphismus.*

(ii) *Jedes $a \in M$ besitzt eine eindeutige Darstellung $a = \sum_{i\in I} a_i$ mit $a_i \in N_i$ für alle $i \in I$ und $a_i \neq 0$ nur endlich oft.*

(iii) *Es gilt $\sum_{i\in I} N_i = M$ und $N_j \cap \sum_{i\in I\setminus\{j\}} N_i = \{0\}$ für alle $j \in I$.*

BEWEIS. Übung. □

DEFINITION 5.2.3. Gilt eine der drei äquivalenten Aussagen in 5.2.2 (b), so nennen wir M die *innere direkte Summe* der $(N_i)_{i\in I}$ und schreiben dafür $M = \oplus_{i\in I} N_i$.

DEFINITION 5.2.4. Sei M ein R-Modul und $X \subseteq M$ eine Teilmenge. Eine *R-Linearkombination* aus X ist eine Summe $\sum_{i=1}^{n} r_i.x_i$, mit $n \in \mathbb{N}$ und $r_i \in R$, $x_i \in X$ für alle $i \in \{1, \ldots, n\}$. Sei $\langle X\rangle$ die Menge aller R-Linearkombinationen aus X, dann sieht man, dass $\langle X\rangle$ der kleinste Untermodul von M ist, der X enthält. Er heißt der *von X erzeugte Untermodul* von M. Wenn $\langle X\rangle = M$ gilt, so heißt X *Erzeugendensystem* von M. Besitzt M ein endliches Erzeugendensystem $x_1, \ldots, x_n$, so nennen wir M *endlich erzeugt*. Mit den Notationen in Proposition 5.2.2 gilt dann $M = R.x_1 + \cdots + R.x_n$.

BEMERKUNG 5.2.5. Sei M ein endlich erzeugter R-Modul und N ein Untermodul von M. Dann ist N nicht notwendigerweise endlich erzeugt!
Sei $R \neq \{0\}$ irgendein Ring. Betrachte den Polynomring $S = R[x_1, x_2, \dots]$ in abzählbar unendlich vielen Variablen. Dann ist S als Modul über sich selbst endlich erzeugt (vom Einselement). Allerdings ist der Untermodul $N = \langle x_1, x_2, \dots \rangle$ nicht endlich erzeugt. Dies sehen wir wie folgt.
Angenommen es gibt $f_1, \dots, f_n \in N$ mit $\langle f_1, \dots, f_n \rangle = \langle x_1, x_2, \dots \rangle = N$. Die Elemente $f_1, \dots, f_n$ liegen im Teilring $R[x_1, \dots, x_r]$ von S, für ein $r \in \mathbb{N}$. Da diese Elemente N erzeugen, gibt es $a_1, \dots, a_n \in S$ mit

$$x_{r+1} = a_1 f_1 + \cdots + a_n f_n. \tag{33}$$

Wieder liegen alle Elemente $a_1, \dots, a_n$ in einem Ring $R[x_1, \dots, x_m]$ für ein $m \in \mathbb{N}$ und wir dürfen oBdA annehmen, dass $m \geq r+1$ gilt. Wir wenden nun den Einsetzhomomorphismus

$$\varphi : R[x_1, \dots, x_m] \longrightarrow R \quad ; \quad x_i \mapsto \begin{cases} 0 \text{ falls } i \neq r+1 \\ 1 \text{ falls } i = r+1 \end{cases}$$

auf die Gleichung (33) an. Dann gilt

$$1 = \varphi(x_{r+1}) = \varphi(a_i) \underbrace{\varphi(f_1)}_{=0} + \cdots + \varphi(a_n) \underbrace{\varphi(f_n)}_{=0} = 0.$$

(Beachte, dass die Polynome $f_1, \dots, f_n$ keinen konstanten Term haben). Dies ist natürlich ein Widerspruch, also ist N nicht endlich erzeugt.

DEFINITION 5.2.6. Sei M ein R-Modul und $X \subseteq M$ eine Teilmenge. Die Menge X heißt *R-linear unabhängig*, falls für jede R-Linearkombination $\sum_{i=1}^n r_i.x_i$ aus X mit $\sum_{i=1}^n r_i.x_i = 0$ bereits $r_1 = \cdots = r_n = 0$ gilt.
Eine Menge $X \subseteq M$ heißt *Basis von M*, genau dann wenn X ein R-linear unabhängiges Erzeugendensystem von M ist. Besitzt M eine Basis, so nennen wir M einen *freien* R-Modul.

BEMERKUNG 5.2.7. Die Definition einer Basis ist vollkommen analog zum bekannten Fall eines Vektorraumes. Der große Unterschied ist, dass nicht jeder R-Modul eine Basis besitzt. Wir wissen beispielsweise, dass die abelsche Gruppe $\mathbb{Z}/g\mathbb{Z}$, $g > 1$, ein $\mathbb{Z}$-Modul ist. Es gilt

$$g.\overline{m} = \overline{gm} = \overline{0} \in \mathbb{Z}/g\mathbb{Z} \text{ für alle } \overline{m} \in \mathbb{Z}/g\mathbb{Z}.$$

Somit ist jede einelementige Teilmenge von $\mathbb{Z}/g\mathbb{Z}$ bereits $\mathbb{Z}$-linear abhängig. Insbesondere kann es keine Basis von $\mathbb{Z}/g\mathbb{Z}$ geben.

FRAGE. Ist jeder Untermodul eines freien R-Moduls M frei?

Auch das gilt leider nicht. Der Ring $\mathbb{Z} \times \mathbb{Z}$ ist frei als Modul über sich selbst (Das Einselement $(1,1)$ ist eine Basis). Offensichtlich ist $\mathbb{Z} \times \{0\}$ ein Untermodul von $\mathbb{Z}\times\mathbb{Z}$. Wieder gilt, dass jede einelementige Teilmenge $\mathbb{Z}\times\mathbb{Z}$-linear abhängig ist. Denn für jedes $(n,0) \in \mathbb{Z} \times \{0\}$ gilt

$$(0,1).(n,0) = (0,0) = 0 \in \mathbb{Z} \times \{0\}.$$

Also ist $\mathbb{Z} \times \{0\}$ kein freier $\mathbb{Z} \times \mathbb{Z}$-Modul.

DEFINITION 5.2.8. Sei S eine Menge und R ein Ring. Dann heißt $F(S) = \oplus_{s\in S} R$ *der freie Modul über* S.

Um zu zeigen, dass diese Definition sinnvoll ist, müssen wir zeigen, dass $F(S)$ tatsächlich ein freier R-Modul ist. Jedes Element in $F(S)$ hat die Form $(r_s)_{s\in S}$ mit $r_s \in R$ für alle $s \in S$ und $r_s \neq 0$ nur endlich oft.
Wir definieren für alle $s \in S$ Elemente $e_s \in F(S)$ durch

$$e_s = (e_{s,t})_{t\in S} \text{ , mit } e_{s,t} = \begin{cases} 1 \text{ falls } t = s \\ 0 \text{ sonst} \end{cases}$$

Diese Elemente bilden (analog zur Standardbasis eines Vektorraumes) eine Basis von $F(S)$. Die Abbildung von S nach $F(S)$, die jedes $s \in S$ auf das zugehörige e_s schickt, ist offensichtlich injektiv. Damit können wir die Elemente e_s mit s identifizieren und somit stets S als kanonische Basis von $F(S)$ betrachten. Dies dient in erster Linie der einfacheren Notation.

PROPOSITION 5.2.9. *Sei M ein R-Modul. Dann sind die folgenden Aussagen äquivalent.*

(i) *M ist ein freier R-Modul.*
(ii) *$M \cong F(S)$ für eine geeignete Menge S.*

BEWEIS. Übung. □

BEMERKUNG 5.2.10. In der Linearen Algebra wurde gezeigt, dass je zwei Basen eines Vektorraums dieselbe Kardinalität haben. Damit konnte die wichtige Invariante $\dim(V)$ definiert werden. Leider funktioniert auch das nicht in beliebigen R-Moduln.
Sei K ein Körper und $R = \mathrm{End}_K(K[x])$ der Ring aller K-linearer Endomorphismen des Polynomringes $K[x]$. Wieder betrachten wir R als Modul über sich selbst und stellen fest, dass 1 eine R-Basis ist. Der K-Vektorraum $K[x]$ hat die Basis $\{1 = x^0, x, x^2, \dots\}$. Damit ist ein $f \in R$ eindeutig durch die Bilder $f(x^i)$, $i \in \mathbb{N}$, bestimmt. Weiter können wir die Bilder $f(x^i)$, $i \in \mathbb{N}$, wie beim Einsetzhomomorphismus beliebig vorgeben.

Wir definieren nun f_1 und f_2 in R durch

$$f_1(x^i) = \begin{cases} x^{i/2} \text{ falls } i \text{ gerade} \\ 0 \text{ falls } i \text{ ungerade} \end{cases} ; f_2(x^i) = \begin{cases} 0 \text{ falls } i \text{ gerade} \\ x^{i-1/2} \text{ falls } i \text{ ungerade} \end{cases}$$

Also folgt für alle $g_1, g_2 \in R$

$$(g_1 \circ f_1 + g_2 \circ f_2)(x^i) = \begin{cases} g_1(x^{i/2}) \text{ für } i \text{ gerade} \\ g_2(x^{i-1/2}) \text{ für } i \text{ ungerade} \end{cases} \tag{34}$$

Also ist $g_1 \circ f_1 + g_2 \circ f_2$ die Nullabbildung, genau dann wenn g_1 und g_2 auf allen x^i, $i \in \mathbb{N}$, verschwinden. Dies ist genau dann der Fall wenn $g_1 = g_2 = 0 \in R$ gilt. Somit sind f_1 und f_2 R-linear unabhängig. Sei nun $g \in R$ beliebig, dann wähle $g_1, g_2 \in R$ so, dass $g_1(x^i) = g(x^{2i})$ und $g_2(x^i) = g(x^{2i+1})$ für alle $i \in \mathbb{N}$. Aus (34) folgt sofort $g_1 \circ f_1 + g_2 \circ f_2(x^i) = g(x^i)$ und somit $g_1 \circ f_1 + g_2 \circ f_2 = g$. Damit ist f_1, f_2 auch ein Erzeugendensystem von R. Wir stellen also fest, dass R die Basen $\{1\}$ und $\{f_1, f_2\}$ besitzt.

Diese Bemerkung lässt Modultheorie zwar sehr interassant, allerdings auch vollkommen unintuitiv, wirken. Wir können dieses verhalten etwas kontrollieren, wenn wir zu kommutativen Ringen übergehen.

PROPOSITION 5.2.11. *Sei R ein kommutativer Ring und M ein endlich erzeugter freier R-Modul. Dann haben alle R-Basen von M dieselbe Länge $n < \infty$. Diese Zahl n nennen wir den* Rang *des R-Moduls M und bezeichnen sie mit* $\mathrm{rk}(n)$.

BEWEIS. Sei $\mathcal{M}$ ein Maximalideal von R, dies existiert nach Lemma 3.5.7. Die Menge

$$\mathcal{M}.M = \{\lambda_1.m_1 + \cdots + \lambda_k.m_k | k \in \mathbb{N}, \lambda_i \in \mathcal{M}, m_i \in M \ \forall \ i \in \{1, \ldots, k\}\}$$

ist ein Untermodul von M. Die Abgeschlossenheit bezüglich „+“ ist klar und die Abgeschlossenheit bezüglich der R-Skalarmultiplikation ist genau die Idealeigenschaft von $\mathcal{M}$ (die Maximalität wird hierfür nicht benötigt). Wir betrachten den Faktormodul ${}^{M}\!/_{\mathcal{M}.M}$. Die R-Skalarmultiplikation ist gegeben durch $r.(m + \mathcal{M}.M) = r.m + \mathcal{M}.M$, und es gilt $\lambda.(m + \mathcal{M}.M) = 0$ für alle $\lambda \in \mathcal{M}$. Damit folgt, dass ${}^{M}\!/_{\mathcal{M}.M}$ sogar ein ${}^{R}\!/_{\mathcal{M}}$-Modul ist, mit der Skalarmultiplikation $(r + \mathcal{M}).(m + \mathcal{M}.M) = r.m + \mathcal{M}.M$.
Nun ist aber ${}^{R}\!/_{\mathcal{M}}$ ein Körper und damit ist ${}^{M}\!/_{\mathcal{M}.M}$ ein ${}^{R}\!/_{\mathcal{M}}$-Vektorraum. Sei $(b_i)_{i \in I}$ ein Erzeugendensystem des R-Moduls M. Jedes Element aus dem ${}^{R}\!/_{\mathcal{M}}$-Vektorraum ${}^{M}\!/_{\mathcal{M}.M}$ lässt sich dann schreiben als

$$m + \mathcal{M}.M = \sum_{i \in I} r_i.b_i + \mathcal{M}.M = \sum_{i \in I} (r_i + \mathcal{M}).(b_i + \mathcal{M}.M) + \mathcal{M}.M$$

für gewisse $r_i \in R$ mit $r_i \neq 0$ für nur endlich viele $i \in I$. Somit ist auch $(b_i + \mathcal{M}.M)_{i\in I}$ ein Erzeugendensystem des ${}^{R}/_{\mathcal{M}}$-Vektorraumes ${}^{M}/_{\mathcal{M}.M}$. Nach Voraussetzung existiert ein endliches Erzeugendensystem von M und somit existiert auch ein endliches Erzeugendensystem des ${}^{R}/_{\mathcal{M}}$-Vektorraumes ${}^{M}/_{\mathcal{M}.M}$. Dies ist natürlich nur möglich wenn dieser Vektorraum endlich dimensional ist.
Insbesondere gilt weiter, dass für jede R-Basis $(b_i)_{i\in I}$ von M, die Elemente $(b_i + \mathcal{M}.M)_{i\in I}$ ein Erzeugendensystem des ${}^{R}/_{\mathcal{M}}$-Vektorraumes ${}^{M}/_{\mathcal{M}.M}$ bilden. Sei im Folgenden $B = (b_i)_{i\in I}$ eine R-Basis von M.
Es bleibt zu zeigen, dass $(b_i + \mathcal{M}.M)_{i\in I}$ auch ${}^{R}/_{\mathcal{M}}$-linear unabhängig sind. Sei dazu $0 = \sum_{i\in I}(r_i + \mathcal{M}).(b_i + \mathcal{M}.M) + \mathcal{M}.M$ für $r_i \in R$ nur endlich oft nicht in $\mathcal{M}$. Per Definition der Skalarmultiplikation folgt

$$0 = \sum_{i\in I} r_i.b_i + \mathcal{M}.M \text{ also } \sum_{i\in I} r_i.b_i \in \mathcal{M}.M.$$

Da B eine R-Basis von M ist, ist diese Linearkombination eindeutig. Es folgt per Definition von $\mathcal{M}.M$, dass $r_i \in \mathcal{M}$ für alle $i \in I$ gilt. Dies bedeutet nichts anderes als $r_i + \mathcal{M} = 0 \in {}^{R}/_{\mathcal{M}}$ für alle $i \in I$. Also ist $(b_i + \mathcal{M}.M)_{i\in I}$ auch ${}^{R}/_{\mathcal{M}}$-linear abhängig.
Wir haben also gezeigt, dass $(b_i + \mathcal{M}.M)_{i\in I}$ eine Basis des endlich demensionalen ${}^{R}/_{\mathcal{M}}$-Vektorraumes ${}^{M}/_{\mathcal{M}.M}$ ist. Damit gilt $|I| = |B| = \dim({}^{M}/_{\mathcal{M}.M}) = n$. Insbesondere haben alle R-Basen von M dieselbe Länge. □

DEFINITION 5.2.12. Seien $R \subseteq R'$ kommutative Ringe, $1_{R'} = 1 \in R$. Ein Element $\alpha \in R'$ heißt *ganz* über R, genau dann wenn ein normiertes Polynom $f(x) \in R[x] \setminus \{0\}$ existiert mit $f(\alpha) = 0$.

BEISPIEL 5.2.13.
- Mit den Bezeichnungen aus 5.2.12 ist jedes $\alpha \in R$ ganz über R, denn α ist Nullstelle des normierten Polynoms $f(x) = x - \alpha \in R[x]$.
- Falls $R = K$ und $R' = L$ Körper sind, so ist $\alpha \in L$ ganz über K genau dann wenn α algebraisch über K ist.

SATZ 5.2.14. *Seien $R \subseteq R'$ kommutative Ringe mit demselben Einselement und sei $\alpha \in R'$. Dann sind die folgenden Aussagen äquivalent:*

(i) *α ist ganz über R.*
(ii) *es existiert ein endlich erzeugter R-Modul $M \subseteq R'$ mit $1 \in M$ und $\alpha M \subseteq M$.*

BEWEIS. Da beide Aussagen trivialerweise für die Null erfüllt sind, nehmen wir ab jetzt $\alpha \neq 0$ an.

$(i) \Rightarrow (ii)$ Sei also $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in R[x]$ mit $f(\alpha) = 0$. Setze $M = R + R\alpha + R\alpha^2 + \ldots + R\alpha^{d-1}$. Es ist $1 \in R \subseteq M$. Weiter gilt auch

$$\begin{aligned}\alpha M &= R\alpha + R\alpha^2 + \ldots + R\alpha^d \\ &= R\alpha + R\alpha^2 + \ldots + R(-a_{d-1}\alpha^{d-1} - \ldots - a_0) \subseteq M.\end{aligned}$$

Also gilt die Aussage (ii).

$(ii) \Rightarrow (i)$ Seien nun $\beta_1, \ldots, \beta_n \in R'$ mit $M = R\beta_1 + \cdots + R\beta_n$, so dass $1 \in M$ und $\alpha M \subseteq M$ gilt. Wir wollen zeigen, dass α Nullstelle eines charakteristischen Polynoms einer gewissen Matrix $A \in M_n(R)$ ist.

Da $\alpha M \subseteq M$ gilt, existieren zu jedem β_i, $i \in \{1, \ldots, n\}$, Elemente $\alpha_{i1}, \ldots, \alpha_{in} \in R$ mit $\alpha\beta_i = \sum_{j=1}^n \alpha_{ij}\beta_i$. Bezeichnen wir mit $E_n \in M_n(R)$ die Einheitsmatrix, so gilt für $A = (a_{ij}) \in M_n(R)$ also

$$A \cdot \begin{pmatrix}\beta_1 \\ \vdots \\ \beta_n\end{pmatrix} = \alpha E_n \cdot \begin{pmatrix}\beta_1 \\ \vdots \\ \beta_n\end{pmatrix} \quad ; \text{d.h.} \quad (\alpha E_n - A) \cdot \begin{pmatrix}\beta_1 \\ \vdots \\ \beta_n\end{pmatrix} = 0 \tag{35}$$

Wir erinnern an die Adjunkte Matrix $\operatorname{adj}(\alpha E_n - A) \in M_n(R)$ von $\alpha E_n - A$. Diese Matrix hat die Eigenschaft

$$\operatorname{adj}(\alpha E_n - A) \cdot (\alpha E_n - A) = \det(\alpha E_n - A) E_n = f(\alpha) E_n$$

für das (normierte) charakteristische Polynom $f(x) \in R[x]$ von A. (Diese Aussage wurde in der linearen Algebra nur für Körper bewiesen, im Beweis werden aber nur Ringeigenschaften benutzt.)

Aus (35) folgt sofort

$$\begin{pmatrix}f(\alpha)\beta_1 \\ \vdots \\ f(\alpha)\beta_n\end{pmatrix} = \operatorname{adj}(\alpha E_n - A) \cdot \underbrace{(\alpha E_n - A) \cdot \begin{pmatrix}\beta_1 \\ \vdots \\ \beta_n\end{pmatrix}}_{=0} = \begin{pmatrix}0 \\ \vdots \\ 0\end{pmatrix}.$$

Die Elemente $\beta_1, \ldots, \beta_n$ sind gerade die Erzeugenden von M, daher gilt $f(\alpha)\beta = 0$ für alle $\beta \in M$. Insbesondere also $f(\alpha) = f(\alpha) \cdot 1 = 0$. Somit ist α ganz über R.

□

5.3. Artinsche und noethersche Moduln

Sei wieder R ein Ring. Wir wollen die Theorie von endlich dimensionalen Vektorräumen möglichst weit verallgemeinern. Dazu benötigen wir einen Dimensionsbegriff für eine möglichst große Klasse von Moduln. Wenn wir

nur diejenigen Moduln betrachten, die frei von endlichem Rang sind, ist dies zu restriktiv. Weiter muss ein Untermodul eines freien R-Moduls M, mit $\mathrm{rk}(M) = n < \infty$, nicht frei vom Rang $\leq n$ sein. Dies ist jedoch eine fundamentale Eigenschaft der Dimension eines Vektorraumes.
Wir werden in diesem Abschnitt noethersche und artinsche Moduln betrachten. Für einen R-Modul der beide Eigenschaften erfüllt, werden wir die Länge des Moduls definieren können. Dies verallgemeinert den Begriff der Dimension eines endlich dimensionalen Vektorraumes.

DEFINITION 5.3.1. Ein R-Modul M heißt *noethersch*, genau dann wenn jede echt aufsteigende Kette von Untermoduln $N_1 \subsetneq N_2 \subsetneq \cdots$ endlich ist.

DEFINITION 5.3.2. Ein R-Modul M heißt *artinsch*, genau dann wenn jede echt absteigende Kette von Untermoduln $N_1 \supsetneq N_2 \supsetneq \cdots$ endlich ist.

ABBILDUNG 5.1. *Amalie Emmy Noether* (1882-1935) war eine deutsche Mathematikerin, die besonders in der abstrakten Algebra und der theoretischen Physik tätig war. Sie war die erste deutsche Professorin, auch wenn dies zunächst nur ein Titel war für den Sie keine Bezahlung erhielt.

In beiden Definitionen können wir auch sagen, dass jede aufsteigende, bzw. absteigende (nicht notwendiger weise *echt*) Kette von Untermoduln *stationär* wird. Das bedeutet, dass ein $k_0 \in \mathbb{N}$ existiert, mit $N_k = N_{k+1}$ für alle $k \geq k_0$.

DEFINITION 5.3.3. Ein Ring R heißt noethersch, bzw. artinsch, genau dann wenn R als R-Modul noethersch, bzw. artinsch, ist.

Genauer müsste es in Definition 5.3.3 *linksartinsch* und *linksnoethersch* heißen, da wir R als R-**Links**modul betrachten. Analog definiert man die Begriffe *rechtsartinsch* und *rechtsnoethersch*.

BEISPIEL 5.3.4.
(a) Jeder Hauptidealbereich R ist noethersch. (Übung)
(b) Wenn R ein Körper ist, dann gilt für einen R-Modul (also einen R-Vektorraum) M:

$$M \text{ noethersch} \iff M \text{ artinsch} \iff \dim(M) = n < \infty$$

Dies sehen wir folgendermaßen: Sei $\dim(M) = n < \infty$ und sei $N_1 \subsetneq N_2 \subsetneq \cdots$ eine echt aufsteigende Kette von Untermoduln. Da R ein Körper ist, sind dies Untervektorräume und somit folgt

$$\dim(N_1) < \dim(N_2) < \cdots < \dim(M) = n.$$

Also kann eine solche Kette maximal $n+1$ Glieder haben. Es folgt, dass M noethersch ist. Das selbe Argument für eine echt absteigende Kette liefert uns auch, dass M artinsch ist.

Sei andererseits $\dim(M) = \infty$. Das bedeutet, dass es eine Folge $\{b_i\}_{i\in\mathbb{N}}$ in M von linearunabhängigen Elementen gibt. Dann ist jedoch $N_1 = \langle b_1\rangle \subsetneq N_2 = \langle b_1, b_2\rangle \subsetneq \cdots$ eine unendlich lange echt aufsteigende Kette von Untermoduln und $N_1' = \langle b_1, b_2, \dots\rangle \supsetneq N_2' = \langle b_2, b_3, \dots\rangle \supsetneq \cdots$ eine unendlich lange echt absteigende Kette von Untermoduln von M. Somit ist M weder noethersch noch artinsch.

PROPOSITION 5.3.5. *Ein R-Modul M ist genau dann noethersch, wenn jeder Untermodul von M endlich erzeugt ist.*

BEWEIS. Wir müssen die beiden Implikationen zeigen.

$\Longrightarrow$ Sei also M noethersch und N ein Untermodul von M. Falls $N = \{0\}$, so ist N offensichtlich endlich erzeigt. Wir nehmen also an, dass $N \neq \{0\}$ gilt. Dann existiert ein $a_1 \in N \setminus \{0\}$ und wir können $N_1 = \langle a_1\rangle = R.a_1$ betrachten. Natürlich ist $N_1 \subseteq N$. Wenn $N_1 = N$, so ist N endlich erzeugt (durch a_1). Wenn $N_1 \neq N$, so finden wir ein $a_2 \in N \setminus N_1$ und es ist $N_1 \subsetneq N_2 = \langle a_1, a_2\rangle \subseteq N$. Wieder gilt, dass N endlich erzeugt ist, falls $N_2 = N$ gilt. Wir wiederholen dieses Prinzip und erhalten eine echt aufsteigende Kette von Untermoduln $N_1 \subsetneq N_2 \subsetneq \cdots \subseteq N$. Da M noethersch ist, muss diese Kette abbrechen; d.h. es existiert ein $k \in \mathbb{N}$ mit $N_k = \langle a_1, \dots, a_k\rangle = N$. Das war zu zeigen.

$\Longleftarrow$ Sei also jeder Untermodul von M endlich erzeugt. Angenommen M ist nicht noethersch. Dann existiert eine unendlich lange echt aufsteigende Kette von Untermoduln $N_1 \subsetneq N_2 \subsetneq \cdots$ von M. Damit ist auch $N = \cup_{j\in\mathbb{N}} N_j$ ein Untermodul von M (das zeigt man genau wie bei Idealen auch). Nach Voraussetzung gilt $N = \langle a_1, \dots, a_r\rangle$ für gewisse $a_1, \dots, a_r \in M$. Nach Definition von N existiert ein $k \in \mathbb{N}$, mit $a_1, \dots, a_r \in N_k$. Damit gilt nun

$$N \overset{\text{Def.}}{\supseteq} N_{k+1} \supsetneq N_k \overset{a_1,\dots,a_r\in N_j}{\supseteq} \langle a_1, \dots, a_r\rangle = N.$$

Dies ist ein Widerspruch und somit ist M tatsächlich noethersch.

□

PROPOSITION 5.3.6. *Sei M ein R-Modul und N ein Untermodul von M. Dann gilt*

(a) *M noethersch $\Longleftrightarrow$ N und M/N noethersch*

(b) *M artinsch $\iff$ N und ${}^{M}/_{N}$ artinsch*

BEWEIS. Wir beweisen nur Teil (a). Der Beweis von (b) funktioniert genauso, wenn man „$\subseteq$“ durch „$\supseteq$“ ersetzt.

$\Longrightarrow$ Offensichtlich ist mit M auch N noethersch, da jede Kette von Untermoduln von N insbesondere eine Kette von Untermoduln von M ist. Sei nun $M'_1 \subseteq M'_2 \subseteq \cdots$ eine aufsteigende Kette von Untermoduln von ${}^{M}/_{N}$. Bezeichnen wir mit $\pi : M \longrightarrow {}^{M}/_{N}$ die kanonische Projektion $m \mapsto m+N$, so sind $M_1 = \pi^{-1}(M'_1), M_2 = \pi^{-1}(M'_2), \ldots$ Untermoduln von M und es gilt $M_1 \subseteq M_2 \subseteq \cdots$. Da M noethersch ist, wird diese Kette stationär; d.h. es existiert ein $k_0 \in \mathbb{N}$ mit $M_k = M_{k+1}$ für alle $k \geq k_0$. Daraus folgt aber

$$M'_k = \pi(M_k) = \pi(M_{k+1}) = M'_{k+1} \text{ für alle } k \geq k_0.$$

Beachte, dass dies nur gilt, da π surjektiv ist. Also wird auch die Kette $M'_1 \subseteq M'_2 \subseteq \cdots$ stationär. Also ist ${}^{M}/_{N}$ noethersch.

$\Longleftarrow$ Seien N und ${}^{M}/_{N}$ noethersch und $M_1 \subseteq M_2 \subseteq \cdots$ eine aufsteigende Kette von Untermoduln von M. Wir betrachten die beiden Ketten

$$(M_1 \cap N) \subseteq (M_2 \cap N) \subseteq \cdots \text{ und} \tag{36}$$

$$\begin{aligned} &{}^{M_1+N}/_{N} \subseteq {}^{M_2+N}/_{N} \subseteq \cdots \\ \Longleftrightarrow\ &M_1 + N \subseteq M_2 + N \subseteq \cdots \end{aligned} \tag{37}$$

Die Kette (36) ist eine Kette von Untermoduln von N und (37) ist eine Kette von Untermoduln von ${}^{M}/_{N}$. Sowohl N als auch ${}^{M}/_{N}$ sind noethersch. Also werden (36) und (37) stationär. Es existiert also ein $k_0 \in \mathbb{N}$ mit

$$M_k \cap N = M_{k+1} \cap N \text{ und } M_k + N = M_{k+1} + N \text{ für alle } k \geq k_0.$$

Sei nun $k \geq k_0$ und $m \in M_{k+1}$. Insbesondere ist also $m \in M_{k+1} + N = M_k + N$. Es existieren somit Elemente $x \in M_k$ und $y \in N$ mit

$$\underbrace{m - x}_{\in M_{k+1}} = y \in N \cap M_{k+1} = N \cap M_k.$$

Da also x und y in M_k liegen, gilt auch $m = x + y \in M_k$. Es gilt also $M_{k+1} \subseteq M_k$ und nach Voraussetzung auch $M_k \subseteq M_{k+1}$. Zusammen ergibt dies $M_k = M_{k+1}$ für alle $k \geq k_0$. Also wird die Kette $M_1 \subseteq M_2 \subseteq \cdots$ stationär. Das bedeutet nichts anderes, als dass M noethersch ist.

□

PROPOSITION 5.3.7. *Sei M ein endlich erzeugter R-Modul. Dann gilt:*

(a) *R noethersch $\Longrightarrow$ M noethersch.*
(b) *R artinsch $\Longrightarrow$ M artinsch.*

BEWEIS. Diesmal beweisen wir nur Teil (b) und (a) folgt analog. Sei also $a_1, \ldots, a_n$ ein Erzeugendensystem von M und setze $S = \{a_1, \ldots, a_n\}$. Dann ist, wie in 5.2.9 gesehen, S eine Basis des freien Moduls $F(S) \cong R^n = \underbrace{R \oplus \ldots \oplus R}_{n\text{-mal}}$.
Nach Voraussetzung ist R artinsch und in den Übungen wurde gezeigt, dass die direkte Summe von artinschen Moduln wieder artinsch ist. Induktiv folgt, dass $R^n \cong F(S)$ artinsch ist.
Genau wie beim Einsetzhomomorphismus aus 2.3.5 oder wie bei K-linearen Abbildungen von K-Vektorräumen, erhalten wir einen (eindeutigen) R-Modul-Homomorphismus

$$\varphi : F(S) \longrightarrow M \quad ; \quad \underbrace{a_i}_{\in S} \mapsto a_i \text{ für alle } i \in \{1, \ldots, n\}.$$

Dann ist $\varphi(F(S))$ ein Untermodul von M, der die Elemente $a_1, \ldots, a_n$ enthält. Da aber bereits $M = \langle a_1, \ldots, a_n \rangle$ gilt, ist $\varphi(F(S)) = M$. Also ist φ surjektiv. Mit dem Isomorphiesatz 5.1.11 erhalten wir ${}^{F(S)}/_{\ker(\varphi)} \cong M$. Nach Proposition 5.3.6 ist M als Faktor des artinschen Moduls $F(S)$ selbst artinsch. Das war zu zeigen. □

BEMERKUNG 5.3.8. Jede Kette $\{0\} = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_m = M$ eines R-Moduls M ist insbesondere eine *Normalreihe* ($M_i \triangleleft M_{i+1}$; vgl. Gruppen.1.39), denn jedes M_i ist eine abelsche Gruppe. Eine *Verfeinerung* einer Normalreihe, ist eine Erweiterung der Normalenreihe um endlich viele Untermoduln und eine *Kompositionsreihe* ist eine Normalenreihe, die keine Verfeinerungen mehr ermöglicht. Wir sagen, dass zwei Normalreihen

$$\{0\} = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_m = M \text{ und } \{0\} = N_0 \subseteq N_1 \subsetneq \cdots \subsetneq N_n = M$$

äquivalent sind, wenn sie dieselbe Länge $m = n$ haben, und wenn es eine Permutation $\pi \in S_n$ gibt mit

$${}^{M_i}/_{M_{i-1}} \cong {}^{N_{\pi(i)}}/_{N_{\pi(i)-1}} \text{ für alle } i \in \{1, \ldots, n\}.$$

BEISPIEL 5.3.9. Sei K ein Körper, $n \in \mathbb{N}$ und $e_1, \ldots, e_n$ die Standardbasis von K^n. Dann ist

$$\{0\} \subsetneq e_1K \subsetneq e_1K + e_2K \subsetneq \cdots \subsetneq e_1K + \cdots + e_nK = K^n$$

eine Kompositionsreihe der Länge $n = \dim(K^n)$.

Im Folgenden wollen wir zeigen, dass Kompositionsreihen, wenn Sie denn existieren, bis auf Äquivalenz eindeutig bestimmt sind.

LEMMA 5.3.10 (Zassenhaus-Lemma). *Seien $P' \subseteq P$ und $N' \subseteq N$ Untermoduln des R-Moduls M. Dann gilt*

$$L := {}^{[(N\cap P)+N']}\!/_{[(N\cap P')+N']} \cong {}^{[(N\cap P)+P']}\!/_{[(N'\cap P)+P']}.$$

BEWEIS. Betrachte die Abbildung $\varphi : N \cap P \longrightarrow L$, definiert durch $a \mapsto \overline{a} = a + (N \cap P') + N'$. Es ist nicht schwierig zu sehen, dass φ ein R-Modul-Homomorphismus ist und dass

$$\ker(\varphi) = [(N \cap P') + N'] \cap (N \cap P) = (N \cap P') + (N' \cap P)$$

gilt. Weiter existieren für ein beliebiges $\overline{a} \in L$ Elemente $b \in N \cap P$ und $c \in N'$ mit $a = b + c$. Das bedeutet nichts anderes als $\overline{a} = \overline{b} = \varphi(b)$. Also ist φ surjektiv. Wieder mit dem Isomorphiesatz folgt $L \cong {}^{N\cap P}\!/_{(N'\cap P)+(N\cap P')}$. Dies ist natürlich isomorph zu ${}^{(N\cap P)+P'}\!/_{(N'\cap P)+P'}$. Das war zu zeigen. □

THEOREM 5.3.11 (Verfeinerungssatz von Schreier). *Seien*

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n = M \tag{38}$$

$$\{0\} = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_p = M \tag{39}$$

zwei Reihen von Untermoduln des R-Moduls M. Dann existieren äquivalente Verfeinerungen von (38) *und* (39).

BEWEIS. Setze $N_{jk} = (N_j \cap P_k) + N_{j-1}$ und $P_{kj} = (P_k \cap N_j) + P_{k-1}$ für alle $j \in \{1, \ldots, n\}$ und $k \in \{1, \ldots, p\}$. Dann ist

$$\{0\} \subseteq N_{11} \subseteq N_{12} \subseteq \cdots \subseteq \underbrace{N_{1p}}_{N_1} \subseteq N_{21} \subseteq N_{22} \subseteq \cdots \subseteq N_{np} = M$$

eine Kette von Untermoduln, die jedes Glied aus (38) enthält, und

$$\{0\} \subseteq P_{11} \subseteq P_{12} \subseteq \cdots \subseteq \underbrace{P_{1n}}_{P_1} \subseteq P_{21} \subseteq P_{22} \subseteq \cdots \subseteq P_{pn} = M$$

eine Kette von Untermoduln, die jedes Glied aus (39) enthält. Weiter haben beide Reihen dieselbe Länge pn und nach dem Zassenhaus-Lemma 5.3.10 gilt auch

$${}^{N_{jk}}\!/_{N_{j,k-1}} \cong {}^{P_{kj}}\!/_{P_{k,j-1}}. \tag{40}$$

Damit sehen wir, dass $N_{jk} = N_{j,k-1}$ genau dann wenn $P_{kj} = P_{k,j-1}$ gilt. Entfernen wir nun alle mehrfachen Einträge aus beiden Ketten, so erhalten wir wieder mit (40) äquivalente Verfeinerungne von (38) und (39). □



ABBILDUNG 5.2. Theorem 5.3.12 ist benannt nach *Marie Ennemond Camille Jordan* (1838-1922; Bild links) und *Otto Ludwig Hölder* (1859-1937; Bild mitte) und gilt für Normalreihen von Gruppen und Moduln gleichermaßen. Der ursprüngliche Beweis wurde zunächst von *Otto Schreier* (1901-1929) dann von *Hans Julius Zassenhaus* (1921-1991; Bild rechts) auf die hier gegebene Form vereinfacht.

THEOREM 5.3.12 (Jordan-Hölder Theorem). *Sei M ein R-Modul, der eine Kompositionsreihe besitzt. Dann sind alle Kompositionsreihen von M äquivalent. Insbesondere haben alle Kompositionsreihen von M dieselbe Länge.*

BEWEIS. Seien zwei Kompositionsreihen von M gegeben (diese existieren nur nach Voraussetzung!). Dann besitzen diese äquivalente Verfeinerungen. Allerdings besitzen Kompositionsreihen keine Verfeinerungen, also müssen sie bereits äquivalent sein. Die zweite Aussage folgt unmittelbar. □

THEOREM 5.3.13. *Sei M ein R-Modul. Dann besitzt M eine Kompositionsreihe, genau dann wenn M artinsch und noethersch ist.*

BEWEIS. Wir beweisen die beiden Implikationen.

$\Longrightarrow$ Sei also

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_r = M \tag{41}$$

eine Kompositionsreihe von M. Sei weiter $\{0\} \subseteq P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_s \subseteq M$ irgendeine Reihe von Untermoduln von M. Dann besitzen diese beiden Ketten äquivalente Verfeinerungen. Allerdings ist (41) eine Kompositionsreihe und besitzt daher keine echte Verfeinerung. Es muss also $s \leq r$ gelten. Insbesondere ist jede solche Reihe endlich. Somit ist M artinsch und noethersch.

$\Longleftarrow$ Sei nun M artinsch und noethersch. Wenn $M = \{0\}$, dann besitzt M die triviale Kompositionsreihe. Sei also $M \neq \{0\}$. Da M noethersch ist, existiert ein maximaler Untermodul M_1 von M mit $M_1 \neq M$. Als Untermodul von M ist auch M_1 noethersch, also gilt entweder $M = \{0\}$ oder es existiert ein maximaler Untermodul M_2 von M_1 mit $M_2 \neq M_1$. Auf diese Weise erhalten wir eine

echt absteigende Kette $\cdots \subsetneq M_2 \subsetneq M_1 \subsetneq M$. Da M auch artinsch ist, bricht diese Kette nach endlich vielen Schritten ab. Es gilt also $\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M$ für ein $r \in \mathbb{N}$ und nach Konstruktion gibt es keine echte Verfeinerung dieser Kette. Damit haben wir eine Kompositionsreihe konstruiert.

□

DEFINITION 5.3.14. Sei M ein artinscher und noetherscher R-Modul. Dann ist die *Länge von M* gegeben durch die Länge einer Kompositionsreihe von M. Wir schreiben dafür $l(M)$.

Beachte, dass diese Definition nach den Theoremen 5.3.13 und 5.3.12 wohldefiniert ist.

PROPOSITION 5.3.15. *Sei M ein artinscher und noetherscher R-Modul und N ein Untermodul von M. Dann gilt die Formel $l(M) = l(N) + l(M/N)$. Insbesondere folgt aus $N \subsetneq M$ auch $l(N) < l(M)$.*

BEWEIS. Übung. □

Wir können Polynomringe natürlich auch für nicht kommutative Ringe R definieren/konstruieren. Diese Ringe sind etwas sperrig, da wir unter anderem keinen Einsetzhomomorphismus mehr haben. Es gilt die Rechenregel $x \cdot a = ax$ für alle $a \in R$ und die Unbestimmte x des Polynomrings $R[x]$.
Wir schließen dieses Kapitel nun mit einem Satz, der besonders für die algebraische Geometrie eine wichtige Rolle spielt. Der Name wird sich im letzten Teil der Vorlesung erklären.

THEOREM 5.3.16 (Hilberts Basissatz). *Sei R ein noetherscher Ring, dann ist auch der Polynomring $R[x]$ noethersch.*

BEWEIS. Wir wollen Proposition 5.3.5 benutzen. Sei also $I \subseteq R[x]$ ein beliebiges Linksideal von $R[x]$. Wir müssen zeigen, dass I endlich erzeugt ist. Für alle $n \in \mathbb{N}$ definieren wir die R-Moduln

$$I_n = \{f \in I \,|\, \operatorname{grad}(f) \leq n\} \subseteq I.$$

Dass dies tatsächlich R-Moduln sind, folgt unmittelbar aus der R-Modulstruktur von I. Für jedes $n \in \mathbb{N}$ betrachten wir die (wohldefinierte) Abbildung

$$b_n : I_n \longrightarrow R \quad ; \quad f = \sum_{i=0}^{n} a_i x^i \mapsto a_n.$$

Die Rechenregeln des Polynomrings $R[x]$ implizieren sofort, dass b_n für alle $n \in \mathbb{N}$ ein R-Modul-Homomorphismus ist. Damit sind die Bilder $b_n(I_n)$ ebenfalls R-Moduln. Es gilt sogar

$$b_1(I_1) \subseteq b_2(I_2) \subseteq \cdots \subseteq R, \text{ denn } b_n(\underbrace{f}_{\in I_n}) = b_{n+1}(\underbrace{x \cdot f}_{\in I_{n+1}}).$$

Da R als noethersch vorausgesetzt wurde, muss diese aufsteigende Kette von Linksidealen in R stationär werden. Es existiert also ein $N \in \mathbb{N}$, so dass

$$b_m(I_m) = b_N(I_N) \text{ für alle } m \geq N. \tag{42}$$

Der R-Modul $\oplus_{i=0}^{N} Rx^i$ ist endlich erzeugt und R ist noethersch. Damit folgt aus Proposition 5.3.7, dass $\oplus_{i=0}^{N} Rx^i$ noethersch ist. Nach Proposition 5.3.6 ist somit auch der Untermodul $I_N \subseteq \oplus_{i=0}^{N} Rx^i$ noethersch. Also existieren $g_1, \ldots, g_r \in I_N$ mit $I_N = \sum_{i=1}^{r} Rg_i$. Wir wollen zeigen, dass diese $g_1, \ldots, g_r$ auch Erzeugende von I sind. Dann ist I wie gewünscht endlich erzeugt und das Theorem bewiesen. Wir zeigen also im Folgenden $I = R[x]I_N$.
Nach Konstruktion der I_n, $n \in \mathbb{N}$, gilt $I = \cap_{n\in\mathbb{N}} I_n$. Wir müssen also $I_m \subseteq R[x]I_N$ zeigen, für alle $m \in \mathbb{N}$.
Wir benutzen Induktion über m, wobei der Induktionsanfang $m \leq N$ trivial ist.
Sei also $m > N$ und $f \in I_m$ beliebig. Dann ist $b_m(f) \in b_m(I_m) \overset{(42)}{=} b_N(I_N)$. Somit existiert ein $f_1 \in I_N$ mit $b_m(f) = b_N(f_1) = b_m(x^{m-N} f_1)$. Das bedeutet gerade $\operatorname{grad}(f - x^{m-N} f_1) \leq m - 1$. Die Induktionsvoraussetzung liefert uns nun

$$f = (\underbrace{f - x^{m-N} f_1}_{\in I_{m-1}}) + \underbrace{X^{m-N} f_1}_{\in R[x]I_N} \in R[x]I_N.$$

Es folgt $I = R[x]I_N = \sum_{i=0}^{N} R[x]g_i$ ist endlich erzeugt. □

KOROLLAR 5.3.17. *Sei R ein noetherscher Ring, dann ist auch $R[x_1, \ldots, x_n]$ noethersch.*

BEWEIS. Das folgt sofort per Induktion aus Theorem 5.3.16. □

5.4. Moduln über Hauptidealbereichen

In diesem Abschnitt werden wir endlich erzeugte Moduln über Hauptidealbereichen studieren. Im Gegensatz zu allgemeinen Moduln über beliebigen Ringen, verhalten sich diese recht zahm. Am Ende werden wir den Elementarteilersatz formulieren, der unter anderem eine Verallgemeinerung der Klassifikation endlicher abelscher Gruppen darstellt.

LEMMA 5.4.1. *Sei R ein Integritätsbereich und M ein R-Modul. Weiter sei M/N frei für einen Untermodul N von M. Dann gilt $M \cong N \oplus M/N$.*

BEWEIS. Sei $(\overline{m_i})_{i\in I}$ eine R-Basis von M/N, für Elemente $m_i \in M$, für alle $i \in I$. (Wie immer bezeichnet $\overline{m_i}$ die Restklasse $m_i + N$). Für jedes $m \in M$ existieren damit eindeutige $\lambda_i \in R$, $i \in I$, mit $\lambda_i \neq 0$ nur endlich oft, so dass $\overline{m} = \sum_{i\in I} \lambda_i \overline{m_i}$. Damit ist $m - \sum_{i\in I} \lambda_i m_i \in N$. Also ist die Abbildung

$$\varphi : M \longrightarrow N \oplus M/N \quad ; \quad m \mapsto (m - \sum_{i\in I} \lambda_i m_i, \overline{m})$$

wohldefiniert und man zeigt leicht, dass φ ein R-Modul-Homomorphismus ist. Weiter gilt

$$\ker(\varphi) = \{m \in M | \overline{m} = \sum_{i\in I} \lambda_i \overline{m_i} = \overline{0} \text{ und } m = \sum_{i\in I} \lambda_i m_i\} = \{0\}.$$

Also ist φ injektiv. Es bleibt die Surjektivität von φ zu zeigen. Sei dazu $(g, \overline{m}) \in N \oplus M/N$ beliebig. Seien wie eben $\lambda_i \in R$ mit $\overline{m} = \sum_{i\in I} \lambda_i \overline{m_i}$. Da $g \in N$ ist, gilt $\overline{g + \sum_{i\in I} \lambda_i m_i} = \overline{m}$. Also gilt $\varphi(g + \sum_{i\in I} \lambda_i m_i) = (g, \overline{m})$, und φ ist surjektiv. Wir haben gezeigt, dass φ ein bijektiver R-Modul-Homomorphismus ist. Dies beweist das Lemma. □

DEFINITION 5.4.2. Sei R ein Ring und M ein R-Modul. Für eine Teilmenge $S \subseteq M$ definieren wir den *Annulator* von S durch $\mathrm{Ann}(S) = \{\lambda \in R | \lambda.m = 0 \ \ \forall m \in S\}$. Das Element $m \in M$ heißt *Torsionselement*, wenn $\mathrm{Ann}(m) \neq \{0\}$. Die Menge aller Torsionselemente in M bezeichnen wir mit $T(M)$. Dann heißt M

$$\textit{torsionsfrei} \iff T(M) = \{0\}$$
$$\textit{Torsionsmodul} \iff T(M) = M$$

BEISPIEL 5.4.3.
- Der $\mathbb{Z}$-Modul $\mathbb{Z}$ ist torsionsfrei, da $\mathbb{Z}$ nullteilerfrei ist.
- Der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ ist für alle $n \geq 2$ ein Torsionsmodul (vergleiche 5.2.7).

LEMMA 5.4.4. *Sei R ein Ring und M ein R-Modul. Dann gilt*

(a) $\mathrm{Ann}(S)$ *ist ein Linksideal in R für alle Teilmengen $S \subseteq M$.*
(b) $\mathrm{Ann}(M)$ *ist ein zweiseitiges Ideal in R.*

Sei ab jetzt R ein Integritätsberich. Dann gilt

(c) $T(M)$ *ist ein Untermodul von M, mit $T(T(M)) = T(M)$.*
(d) $M/T(M)$ *ist torsionsfrei.*

BEWEIS. Übung. Beachte, dass es für die Teile (c) und (d) tatsächlich notwendig ist, R als Integritätsbereich vorauszusetzen. □

SATZ 5.4.5. *Sei R ein Hauptidealbereich und M ein freier R-Modul vom Rang $n < \infty$. Dann ist jeder Untermodul von M frei vom Rang kleiner oder gleich n.*

BEWEIS. Es ist mit Proposition 5.2.9 $M \cong R^n$. Es genügt also den Beweis für $M = R^n$ zu führen. Dies tun wir durch Induktion über n.
Induktionsanfang: $n = 1$: Sei also $M = R$ und N ein Untermodul von M. Insbesondere ist also N ein Ideal in R, und es gilt $N = \langle a \rangle$ für ein a in R. Falls $a = 0$, so ist N frei vom Rang 0, sonst ist $\{a\}$ eine R-Basis von N (da R nullteilerfrei) und es gilt $\mathrm{rk}(N) = 1 \leq 1$.
Induktionsschritt: $n > 1$: Betrachte den surjektiven R-Modul-Homomorphismus

$$p_n : R^n \longrightarrow R \quad ; \quad (a_1, \ldots, a_n) \mapsto a_n.$$

Sei N ein Untermodul von R^n, dann ist die Einschränkung $p_n|_N : N \longrightarrow R$ noch immer ein R-Modul-Homomorphismus. Es gilt $p_n(N) \triangleleft R$ und wie im Fall $n = 1$ ist $\mathrm{rk}(p_n(N)) \leq 1$. Weiter ist $\ker(p_n|_N)$ ein Untermodul von $\underbrace{R \oplus \cdots \oplus R}_{(n-1)\text{-mal}} \oplus \{0\} \cong R^{n-1}$. Nach Induktionsvoraussetzung gilt damit $\mathrm{rk}(\ker(p_n|_N)) \leq n - 1$. Mit dem Isomorphiesatz erhalten wir ${}^{N}\!/_{\ker(p_n|_N)} \cong p_n(N)$. Wie oben gesehen ist damit $\mathrm{rk}({}^{N}\!/_{\ker(p_n|_N)}) \leq 1$. Mit Lemma 5.4.1 gilt weiter $N \cong {}^{N}\!/_{\ker(p_n|_N)} \oplus \ker(p_n|_N)$. Somit ist

$$\mathrm{rk}(N) = \mathrm{rk}({}^{N}\!/_{\ker(p_n|_N)}) + \mathrm{rk}(\ker(p_n|_N)) \leq 1 + n - 1 \leq n.$$

Dies war zu zeigen. (Beachte, dass für eine Basis $a_1, \ldots, a_r$ eines R-Moduls E und eine Basis $b_1, \ldots, b_s$ eines R-Moduls F, der R-Modul $E \oplus F$ die Basis $(a_1, 0), \ldots, (a_r, 0), (0, b_1), \ldots, (0, b_s)$ besitzt.) □

THEOREM 5.4.6. *Sei R ein Hauptidealbereich und M ein endlich erzeugter R-Modul. Dann ist M frei, genau dann wenn M torsionsfrei ist.*

BEWEIS. Wie immer beweisen wir die beiden nötigen Implikationen.

- $\Longrightarrow$ Sei M also ein freier R-Modul und $m \in M$ ein Torsionselement. Schreibe $m = \sum_{i=1}^{k} \lambda_i.m_i$, mit $\lambda_i \in R$ und einer Basis $m_1, \ldots, m_k$ von M. Sei nun $\lambda \in R \setminus \{0\}$ so dass $\lambda.m = 0$. Dann gilt auch $\sum_{i=1}^{k} (\lambda\lambda_i).m_i = 0$. Es muss also $\lambda\lambda_i = 0$ für alle $i \in \{1, \ldots, k\}$ gelten. Da $\lambda \neq 0$ und R ein Integritätsbereich ist, gilt bereits $\lambda_i = 0$ für alle $i \in \{1, \ldots, k\}$, und somit $m = 0$. Wir haben gezeigt, dass 0 das einzige Torsinselement in M ist. Dies ist gleichbedeutend damit, dass M torsionsfrei ist.
- $\Longleftarrow$ Sei $m_1, \ldots, m_r$ ein Erzeugendensystem von M. Dann existiert eine maximale R-linear unabhängige Teilmenge von $\{m_1, \ldots, m_r\}$. Sei

diese oBdA gegeben durch $m_1, \dots, m_s$. Aufgrund der Maximalität sind die Elemente $m_1, \dots, m_s, m_j$ linear abhängig für alle $j > s$. Dies bedeutet, es existiert eine R-Linearkombination

$$\lambda_{j_1}.m_1 + \cdots + \lambda_{j_s}.m_s + \lambda_j.m_j = 0 \text{ mit } \lambda_j \neq 0. \tag{43}$$

Nach Wahl von $m_1, \dots, m_s$ ist $F = \langle m_1, \dots, m_s \rangle$ ein freier R-Modul. Definiere $\lambda = \prod_{j=s+1}^{r} \lambda_j \neq 0$ (beachte, dass das leere Produkt als 1 definiert ist) und betrachte die Abbildung

$$\varphi : M \longrightarrow F \quad ; \quad m \mapsto \lambda.m.$$

Diese ist wohldefiniert, da nach (43) $\lambda.m_j \in F$ für alle $j \in \{1, \dots, r\}$ gilt, und da $m_1, \dots, m_r$ ein Erzeugendensystem von M ist, gilt tatsächlich $\lambda.m \in F$ für alle $m \in M$. Weiter ist φ ein R-Modul-Homomorphismus, da R kommutativ ist, und es gilt $\ker(\varphi) \subseteq T(M) \overset{\text{Vor.}}{=} \{0\}$. Die Abbildung φ ist also insbesondere injektiv. Wir können somit M als Untermodul von F auffassen. Aus Satz 5.4.5 folgt, dass M ein freier Modul ist.

□

THEOREM 5.4.7. *Sei R ein Hauptidealbereich und M ein endlich erzeugter R-Modul. Dann existiert ein freier R-Modul F mit $M \cong F \oplus T(M)$.*

BEWEIS. Ist $m_1, \dots, m_r$ ein Erzeugendensystem von M, so ist $\overline{m_1}, \dots, \overline{m_r}$ ein Erzeugendensystem von $M/T(M)$. Nach Lemma 5.4.4 ist $M/T(M)$ torsionsfrei und somit, nach Theorem 5.4.6, ein freier R-Modul. Mit Lemma 5.4.1 folgt nun $M \cong M/T(M) \oplus T(M)$. □

Der Beweis des nächsten Satzes ist sehr technisch und wird in dieser Vorlesung nicht geführt. Wir verweisen für den Beweis auf [**JS**], VII. Satz 8.4.

THEOREM 5.4.8 (Elementarteilersatz). *Sei R ein Hauptidealbereich und M ein freier R-Modul vom Rang $r < \infty$. Sei weiter N ein Untermodul von M. Dann existiert eine Basis $m_1, \dots, m_r$ von M und $\lambda_1, \dots, \lambda_r \in R$, so dass $\{\lambda_1.m_1, \dots, \lambda_r.m_r\} \setminus \{0\}$ eine Basis von N ist und $\lambda_1 \mid \lambda_2 \mid \cdots \mid \lambda_r$ gilt. Die Elemente $\lambda_1, \dots, \lambda_r$ sind bis auf Multiplikation mit Einheiten eindeutig bestimmt durch N und heißen* Elementarteiler von N in M.

THEOREM 5.4.9. *Sei R ein Hauptidealbereich und M ein endlich erzeugter R-Modul. Dann existieren $\lambda_1, \dots, \lambda_s \in R \setminus \{R^* \cup \{0\}\}$ mit $\lambda_1 \mid \cdots \mid \lambda_s$ und*

$$M \cong R/\langle \lambda_1 \rangle \times \cdots \times R/\langle \lambda_s \rangle \times R^{s'}.$$

Die Elemente $\lambda_1, \ldots, \lambda_s$ heißen Elementarteiler von M *und sind bis auf Multiplikation mit Einheiten eindeutig bestimmt. Weiter ist auch $s' \in \mathbb{N}$ eindeutig bestimmt.*

BEWEIS. Sei $M = \langle m_1, \ldots, m_r \rangle$ und sei $e_1, \ldots, e_r$ die Standardbasis von $R^r = R.e_1 \oplus \cdots \oplus R.e_r$ aus 5.2.9. Wir erhalten einen surjektiven R-Modul-Homomorphismus $\varphi : R^r \longrightarrow M$ durch $\varphi(e_i) = m_i$ für alle $i \in \{1, \ldots, r\}$. Wenden wir den Elementarteilersatz 5.4.8 auf $N = \ker(\varphi)$ an, so erhalten wir eine Basis $b_1, \ldots, b_r$ von R^r und Elemente $\lambda_1 \mid \cdots \mid \lambda_r$, so dass die Menge $\{\lambda_1.b_1, \ldots, \lambda_r.b_r\} \setminus \{0\}$ eine Basis von N ist. Mit dem Isomorphiesatz folgt

$$M = \varphi(R^r) \cong {}^{R^r}\!/_N = {}^{\oplus_{i=1}^r R.b_i}\!/_{\oplus_{i=1}^r R.(\lambda_i.b_i)} \cong {}^{R}\!/_{\langle\lambda_1\rangle} \oplus \cdots \oplus {}^{R}\!/_{\langle\lambda_r\rangle}.$$

Falls $\lambda_i \in R^*$, so ist ${}^{R}\!/_{\langle\lambda_i\rangle}$ trivial. Falls $\lambda_i = 0$ so ist ${}^{R}\!/_{\langle\lambda_i\rangle} \cong R$. Sei nun $\lambda_1' \mid \cdots \mid \lambda_s'$ die Sequenz, die wir aus $\lambda_1 \mid \cdots \mid \lambda_r$ durch weglassen aller Einheiten und Nullen erhalten. Dann gilt

$$M \cong {}^{R}\!/_{\langle\lambda_1'\rangle} \times \cdots \times {}^{R}\!/_{\langle\lambda_s'\rangle} \times R^{s'},$$

wobei $s' = \mathrm{rk}({}^{M}\!/_{T(M)})$ durch die Anzahl der $\lambda_i = 0$ gegeben ist. Aus dem Elementarteilersatz erhalten wir auch die Eindeutigkeit (bis auf Multiplikation mit Einheiten) der Elemente λ_i', $i \in \{1, \ldots, s\}$. □

BEISPIEL 5.4.10. Sei M ein $\mathbb{Z}$-Modul mit $\mathrm{rk}({}^{M}\!/_{T(M)}) = 1$ und $|T(M)| = 36 = 2^2 \cdot 3^2$. Dann ist $T(M)$ isomorph zu

$M_1 = {}^{\mathbb{Z}}\!/_{2^2 \cdot 3^2 \mathbb{Z}}$ oder
$M_2 = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2 \cdot 3^2 \mathbb{Z}}$ oder
$M_3 = {}^{\mathbb{Z}}\!/_{2 \cdot 3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2 \cdot 3\mathbb{Z}}$ oder
$M_4 = {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2^2 \cdot 3\mathbb{Z}}$.

Weiter ist M isomorph zu $M_i \oplus \mathbb{Z}$ für genau ein $i \in \{1, 2, 3, 4\}$.

THEOREM 5.4.11 (Elementarteilersatz für Matrizen). *Sei R ein Hauptidealbereich und $A \in M_n(R)$ eine $n \times n$-Matrix mit Einträgen aus R. Dann existieren invertierbare Matrizen $S \in GL_n(R)$ und $T \in GL_n(R)$, so dass SAT eine Diagonalmatrix D ist, mit Diagonalelementen $\lambda_1 \mid \lambda_2 \mid \cdots \mid \lambda_n$. Diese Diagonalelemente sind bis auf Multiplikation mit Einheiten eindeutig bestimmt.*

BEWEIS. Sei $\underline{e} = \{e_1, \ldots, e_n\}$ die Standardbasis von R^n. Die Matrix A beschreibt durch Multiplikation eine R-lineare Abbildung $\varphi_A : R^n \longrightarrow R^n$. Also ist $\varphi_A(R^n) \subseteq R^n$ ein Untermodul von R^n. Nach Theorem 5.4.8 existiert eine Basis $e_1', \ldots, e_n'$ von R^n und $\lambda_1, \ldots, \lambda_s \in R \setminus \{0\}$ mit $\lambda_1 \mid \lambda_2 \mid \cdots \mid \lambda_s$, so dass $\lambda_1 e_1', \ldots, \lambda_s e_s'$ eine Basis von $\varphi_A(R^n)$ ist.

Wähle $S \in GL_n(R)$ mit $Se'_i = e_i$ für alle $i \in \{1, \ldots, n\}$. Seien weiter $f_1, \ldots, f_s \in R^n$ mit $\varphi_A(f_i) = \lambda_i e'_i$ für alle $i \in \{1, \ldots, s\}$. Da $\lambda_1 e'_1, \ldots, \lambda_s e'_s$ eine Basis von $\varphi_A(R^n)$ ist, gilt

$$N = \langle f_1, \ldots, f_s \rangle = Rf_1 \oplus \cdots \oplus Rf_s.$$

Weiter existiert zu jedem $m \in R^n$ genau ein $a \in N$ mit $\varphi_A(m) = \varphi_A(a)$. Damit lässt sich jedes $m \in R^n$ eindeutig als Summe $m = a + b$ mit $a \in N$ und $b = m - a \in \ker(\varphi_A)$ schreiben. (Denn für jedes $b' \in \ker(\varphi_A)$ ist $\varphi_A(m - b') = \varphi_A(m)$.) Nach Proposition 5.2.2 (b) ist also

$$R^n = Rf_1 \oplus \cdots \oplus Rf_s \oplus \ker(\varphi_A).$$

Da $\ker(\varphi_A)$ als Untermodul von R^n frei ist (siehe Satz 5.4.5), existieren $f_{s+1}, \ldots, f_n \in \ker(\varphi_A)$, so dass $f_1, \ldots, f_n$ eine Basis von R^n ist. Sei nun $T \in GL_n(R)$ die Transformationsmatrix, mit $Te_i = f_i$ für alle $i \in \{1, \ldots, n\}$. Dann gilt

$$SATe_i = SAf_i = S(\lambda_i e'_i) = \lambda_i (Se'_i) = \lambda_i e_i \text{ für alle } i \in \{1, \ldots, n\},$$

wobei wir $\lambda_i = 0$ für $i > s$ setzen. Also ist $D = SAT$ eine Diagonalmatrix mit Diagonalelementen $\lambda_1, \ldots, \lambda_n$. Die Eindeutigkeit der λ_i's folgt aus der Eindeutigkeit der Elementarteiler aus Theorem 5.4.8. □

Definition 5.4.12. Die Diagonalmatrix D aus Theorem 5.4.11 heißt *Smith-Normalform* von A.

Beispiel 5.4.13. Sei wieder R ein Hauptidealbereich. Matrix-Multiplikation mit Matrizen aus $GL_n(R)$ bedeutet nichts anderes als elementare Zeilen- und Spaltenumformungen durchzuführen. D.h.:

(1) Vertauschen von Spalten/Zeilen.
(2) Spalten/Zeilen mit Einheiten multiplizieren.
(3) Das r-fache einer Spalte/Zeile, $r \in R$, zu einer anderen Spalte/Zeile addieren.

Wir fassen $M = \mathbb{Z}^3$ als $\mathbb{Z}$-Modul auf und betrachten den Untermodul

$$N = \mathbb{Z} \cdot \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 8 \\ 4 \\ 10 \end{pmatrix}.$$

Die Elementarteiler von N in M sind nun gegeben durch die Elemente der Smith-Normalform von

$$A = \begin{pmatrix} 2 & 8 & 0 \\ 5 & 4 & 0 \\ 3 & 10 & 0 \end{pmatrix}.$$

Diese bestimmen wir nun durch Aktionen der Form (1), (2) und (3).

$$A \to \begin{pmatrix} 2 & 8 & 0 \\ 5 & 4 & 0 \\ 1 & 2 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 \\ 5 & 4 & 0 \\ 2 & 8 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 \\ 0 & -6 & 0 \\ 0 & 4 & 0 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 4 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Somit sind die Elementarteiler von N in M gegeben durch $1 \mid 2 \mid 0$. Mit den Notationen aus dem Beweis von Theorem 5.4.11 gilt dann

$$S = \begin{pmatrix} -1 & 0 & 1 \\ 11 & 1 & -9 \\ -19 & -2 & 16 \end{pmatrix} \quad , \quad T = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Damit erhalten wir die Basis

$$e_1' = \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} \quad , \quad e_2' = \begin{pmatrix} 2 \\ -3 \\ 2 \end{pmatrix} \quad , \quad e_3' = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

von M, so dass $\{1e_1', 2e_2', 0e_3'\} \setminus \{0\}$ eine Basis von N ist.

5.5. Einfache und halbeinfache Moduln

Moduln sind besonders leicht zu studieren wenn sie nur triviale Untermoduln besitzen. Wie in der Gruppentheorie nennen wir solche Moduln einfach. Halbeinfache Moduln sind aus einfachen zusammengesetzt. In diesem Abschnitt ist wie immer $R \neq \{0\}$ ein Ring.

Definition 5.5.1. Ein R-Modul $M \neq \{0\}$ heißt *einfach*, genau dann wenn $\{0\}$ und M die einzigen Untermoduln von M sind.

Beispiel 5.5.2.
(a) $\mathbb{Z}$-Moduln sind genau die abelschen Gruppen. Also ist ein $\mathbb{Z}$-Modul M einfach genau dann wenn $M \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.
(b) Sei $R = K$ ein Körper und V ein endlich dimensionaler K-Modul (=K-Vektorraum). Dann ist V einfach genau dann wenn $\dim(V) = 1$.
(c) Der K-Vektorraum V aus (b) ist auch stets ein $\mathrm{End}_K(V)$-Modul (siehe Proposition 5.1.7). Auf diese Weise ist V stets einfach, denn zu allen $v, w \in V$ existiert ein $\varphi \in \mathrm{End}_K(V)$ mit $\varphi.v = \varphi(v) = w$.

Lemma 5.5.3. *Sei $I \subsetneq R$ ein Linksideal. Dann existiert ein maximales Linksideal $J \subsetneq R$ mit $I \subseteq J$.*

BEWEIS. Dies zeigt man genau wie bei kommutativen Ringen mit Hilfe des Zorn'schen Lemmas (siehe 3.5.6). □

DEFINITION 5.5.4. Ein Untermodul N eines R-Moduls M besitzt ein *Komplementmodul* P in M, genau dann wenn $M = N \oplus P$ gilt für einen Untermodul P von M.

LEMMA 5.5.5 (Lemma von Schur). *Jeder R-Modul-Homomorphismus zwischen einfachen R-Moduln ist entweder die Nullabbildung oder ein Isomorphismus.*

BEWEIS. Seien M, N einfache R-Moduln und $\varphi \in \mathrm{Hom}_R(M, N)$ nicht die Nullabbildung. Dann ist $\ker(\varphi) \subsetneq M$ ein Untermodul des einfachen Moduls M. Somit ist $\ker(\varphi) = 0$ und φ injektiv. Genauso ist $\varphi(M) \subseteq N$ ein von $\{0\}$ verschiedener Untermodul des einfachen Moduls N. Damit ist $\varphi(M) = N$ und φ surjektiv. Zusammen ergibt dies, dass φ wie gewünscht ein R-Modul-Isomorphismus ist. □

ABBILDUNG 5.3. Der deutsche Mathematiker *Issai Schur* (1875-1941) leistete bedeutende Arbeit in der Darstellungstheorie. Auch das eben kennengelernte Lemma ist in diesem Kontext entstanden. Schur soll zudem ein ausgezeichneter Dozent gewesen sein.

LEMMA 5.5.6. *Seien $\{N_i\}_{i \in I}$ einfache Untermoduln des R-Moduls M, so dass $M = \sum_{i \in I} N_i$ ist. (Hier ist I irgendeine Indexmenge). Dann existiert zu jedem Untermodul N von M eine Teilmenge $J \subseteq I$, so dass $M = N \oplus (\bigoplus_{j \in J} N_j)$ gilt.*

BEWEIS. Sei also N ein beliebiger Untermodul von M und sei

$$S = \{J \subseteq I | N + \sum_{j \in J} N_j = N \oplus (\bigoplus_{j \in J} N_j)\}.$$

Die Menge S ist partiell geordnet bezüglich der Inklusion von Mengen. Wir wollen das Zorn'sche Lemma auf S anwenden und prüfen daher die Voraussetzungen.

Es ist $S \neq \emptyset$, da die leere Menge selbst in S enthalten ist. Sei nun K eine total geordnete Teilmenge von S. Das heißt: für $I_1, I_2 \in K$ gilt entweder $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$. Wir müssen zeigen, dass K eine obere Schranke in S besitzt. Ein vielversprechender Kandidat ist $I_K = \cup_{J \in K} J$.

Offensichtlich ist I_K eine obere Schranke von K, es bleibt also $I_K \in S$ zu zeigen. Es muss also

$$N + \sum_{j \in I_K} N_j = N \oplus (\bigoplus_{j \in I_K} N_j) \tag{44}$$

gelten. Sei $a \in N + \sum_{j \in I_K} N_j$ und seien

$$a = b + \sum_{j \in I_K} a_j = b' + \sum_{j \in I_K} a'_j \text{ mit } b, b' \in N,\ a_j, a'_j \in N_j\ \forall j \in I_K$$

zwei Darstellungen von a. Die obigen Summen sind endlich und K ist total geordnet. Es gibt also ein $I' \in K \subseteq S$, so dass $a_j, a'_j \in I'$ für alle $j \in I_K$. Da $I' \in S$, gilt

$$N + \sum_{j \in I'} N_j = N \oplus (\bigoplus_{j \in I'} N_j).$$

Mit Proposition 5.2.2 wissen wir, dass die Darstellungen von a gleich seien müssen. Es folgt, $b = b'$ und $a_j = a'_j$ für alle $j \in I_K$. Wieder aus Proposition 5.2.2 folgt damit auch die Gleichung (44).
Wir dürfen also tatsächlich das Zorn'sche Lemma auf S anwenden und erhalten ein maximales Element $J_{\max}$ in S. Unser Ziel ist es $M = N \oplus (\bigoplus_{j \in J_{\max}} N_j)$ zu zeigen. Aus $J_{\max} \in S$ wissen wir bereits, dass die Summe direkt ist. Sei nun $i \in I$ beliebig. Falls $N_i \cap (N \oplus (\bigoplus_{j \in J_{\max}} N_j)) = \{0\}$ gilt, so ist (wieder mit 5.2.2)

$$N + (\sum_{j \in J_{\max}} N_j) + N_i = N \oplus (\bigoplus_{j \in J_{\max}} N_j) \oplus N_i = N \oplus (\bigoplus_{j \in J_{\max} \cup \{i\}} N_j)$$

und $J_{\max} \subsetneq J_{\max} \cup \{i\} \in S$. Dies ist natürlich ein Widerspruch zur Maximalität von $J_{\max}$.
Es ist also $N_i \cap (N \oplus (\bigoplus_{j \in J_{\max}} N_j)) \neq \{0\}$ ein Untermodul des einfachen Moduls N_i. Daraus folgt $N_i \cap \oplus(\bigoplus_{j \in J_{\max}} N_j) = N_i$ für alle $i \in I$. Dies liefert nun

$$M = \sum_{i \in I} N_i \subseteq N \oplus (\bigoplus_{j \in J_{\max}} N_j) \subseteq M.$$

Es gilt also überall Gleichheit, was den Beweis des Lemmas schließt. □

Definition 5.5.7. Ein R-Modul M heißt *halbeinfach*, genau dann wenn $M = \bigoplus_{j \in I} M_j$ für einfache Untermoduln M_j von M.

Beispiel. Jeder Vektorraum V über einem Körper K ist halbeinfach. Denn für eine K-Basis $\{e_i\}_{i \in I}$ von V (die bekanntlich immer existiert) ist $V = \bigoplus_{i \in I} Ke_i$ und die eindimensionalen Unterräume Ke_i sind einfach für alle $i \in I$.

THEOREM 5.5.8. *Sei M ein R-Modul, dann sind folgende Aussagen äuivalent:*

(i) $M = \sum_{i \in I} M_i$ *für einfache Untermoduln* M_i *von* M.
(ii) M *ist halbeinfach.*
(iii) *Jeder Untermodul von* M *besitzt ein Komplementmodul in* M.

BEWEIS. Wir beweisen das Theorem mit einem Ringschluss.

(i) $\Rightarrow$ (ii) Dies ist genau die Aussage von Lemma 5.5.6 für den Untermodul $N = \{0\}$.

(ii) $\Rightarrow$ (iii) Dies ist ebenfalls in Lemma 5.5.6 bewiesen worden.

(iii) $\Rightarrow$ (i) Wir beweisen diese Implikation in drei Schritten.

1. Schritt: Seien $P \subseteq N$ Untermoduln von M. Dann besitzt P auch einen Komplementmodul in N.

Nach Voraussetzung existiert ein Komplementmodul Q von P in M. Es gilt also $M = P \oplus Q$. Wir setzen $Q' = N \cap Q$. Natürlich gilt

$$P \cap Q = \{0\} \Longrightarrow P \cap Q' = \{0\}. \tag{45}$$

Sei weiter $a \in N \subseteq M$ beliebig, dann existieren $p \in P$ und $q \in Q$ mit $a = p + q$. Damit erhalten wir auch

$$q = \underbrace{a}_{\in N} - \underbrace{p}_{\in N} \in N \cap Q = Q' \implies N = P + Q'. \tag{46}$$

Mit Proposition 5.2.2 folgt aus (45) und (46) sofort $N = P \oplus Q'$, und somit der erste Schritt.

2. Schritt: Jeder Untermodul $N \neq \{0\}$ von M besitzt einen einfachen Untermodul.

Sei also $N \neq \{0\}$ ein Untermodul von M und sei $a \in N \setminus \{0\}$ beliebig. Es genügt zu zeigen, dass $\langle a \rangle = Ra \subseteq N$ einen einfachen Untermodul besitzt. Wir nehmen daher oBdA $N = Ra$ an. Dann ist der R-Modul-Homomorphismus

$$\varphi : R \longrightarrow N \quad ; \quad r \mapsto ra$$

surjektiv. Nach Lemma 5.5.3 existiert ein maximales Linksideal $\mathcal{M}$ in R mit $\ker(\varphi) \subseteq \mathcal{M}$. Nach dem 1. Schritt angewendet auf die Untermoduln $\varphi(\mathcal{M}) \subseteq N$ von M existiert ein Untermodul Q mit

$$N = \varphi(\mathcal{M}) \oplus Q \implies Q \cong {}^{N}\!/_{\varphi(\mathcal{M})}. \tag{47}$$

Wenden wir den Homomorphiesatz auf φ und $\varphi|_{\mathcal{M}}$ an, so erhalten wir

$$N \cong {}^{R}\!/_{\ker(\varphi)} \text{ und } \varphi(\mathcal{M}) \cong {}^{\mathcal{M}}\!/_{\varphi(\mathcal{M})\cap\ker(\varphi)} = {}^{\mathcal{M}}\!/_{\ker(\varphi)}.$$

Setzen wir dies in (47) ein, so sehen wir

$$Q \cong {}^{R}\!/_{\ker(\varphi)}\!/_{{}^{\mathcal{M}}\!/_{\ker(\varphi)}} \cong {}^{R}\!/_{\mathcal{M}}.$$

Da $\mathcal{M}$ ein maximales Linksideal folgt aus den Übungen, dass ${}^{R}\!/_{\mathcal{M}} \cong Q \subseteq N$ einfach ist.

3. Schritt: Sei $\{P_j\}_{j\in J}$ die Menge aller einfachen Untermoduln von M. Dann gilt $M = \sum_{j\in J} P_j$.

Angenommen es wäre $\sum_{j\in J} P_j \neq M$. Dann existiert nach Voraussetzung ein Untermodul $Q \neq \{0\}$ von M, mit $(\sum_{j\in J} P_j) \oplus Q = M$. Allerdings enthält Q nach dem 2. Schritt einen einfachen Untermodul. Es gilt also $P_i \subseteq Q$ für ein $i \in J$. Daraus folgt

$$\{0\} \neq P_i \subseteq (\sum_{j\in J} P_j) \cap Q$$

was natürlich ein Widerspruch ist zur Direktheit der Summe. Also gilt $M = \sum_{j\in J} P_j$. Dies beweist den 3. Schritt und somit das Theorem.

□

KOROLLAR 5.5.9. *Jeder Untermodul N und jeder Faktormodul ${}^{M}\!/_{N}$ eines halbeinfachen R-Moduls M ist halbeinfach.*

BEWEIS. Die Aussage ist trivial für $N = \{0\}$. Sei also $N \neq \{0\}$. Dann besitzt, nach dem 2. Schritt im Beweis von Theorem 5.5.8, jeder Untermodul von N einen Komplementmodul. Theorem 5.5.8 liefert nun, dass N halbeinfach ist.
Das gleiche Theorem liefert auch die existenz eines Komplementmoduls P in M mit $M = N \oplus P$. Somit ist ${}^{M}\!/_{N} \cong P$, und P ist als Untermodul von M halbeinfach. □

5.6. Einfache und halbeinfache Ringe

Wir betrachten nun einen „Spezialfall“ des letzten Abschnittes, nämlich Ringe als Moduln über sich selbst. Wir werden diese halbeinfachen Ringe vollständig klassifizieren. Die dabei entstandene Theorie werden wir im nächsten Kapitel über Darstellungstheorie benutzen. Sei weiterhin $R \neq \{0\}$ ein Ring.

DEFINITION 5.6.1. Sei R ein Ring und I ein Linksideal in R.

- R heißt *halbeinfach* $\iff$ R ist halbeinfach als R-(Links)modul.
- I heißt *einfach* $\iff$ I ist einfach als R-Modul.
- R heißt *einfacher Ring* $\iff$ R besitzt keine zweiseitigen Ideale ausser $\{0\}$ und R.

Achtung! Dass ein Ring R ein einfacher Ring ist, ist nicht äquivalent dazu, dass R ein einfacher R-Modul ist! Jeder Ring, der einfach als R-Modul ist, ist auch ein einfacher Ring. Denn jedes zweiseitige Ideal ist erst recht ein Linksideal. Die Umkehrung ist im Allgemeinen jedoch nicht richtig. Trotz dieser möglichen Konfusion haben sich diese Bezeichnungen durchgesetzt.

DEFINITION 5.6.2. Ein Schiefkörper ist ein Ring D in dem jedes von Null verschiedene Ideal ein multiplikatives Inverses besitzt.

Natürlich ist jeder Körper ein Schiefkörper. Das prominenteste Beispiel eines nicht kommutativen Schiefkörpers sind die Quaternionen.

LEMMA 5.6.3. *Sei D ein Schiefkörper und $n \in \mathbb{N}$. Dann ist der Matrizenring $M_n(D)$ ein einfacher Ring. Weiter ist $M_n(D)$ sowohl artinsch als auch noethersch.*

BEWEIS. Übung. □

PROPOSITION 5.6.4. *Sei M ein einfacher R-Modul, dann ist* $\mathrm{End}_R(M)$ *ein Schiefkörper.*

BEWEIS. Man zeigt ganz einfach (vergleiche 5.1.6), dass $\mathrm{End}_R(M) = \{f : M \to M | f \ R\text{-Modul-Homomorphismus}\}$ ein Ring ist. Für $f_1, f_2 \in \mathrm{End}_R(M)$ und $m \in M$ ist die Addition gegeben durch $(f_1+f_2)(m) = f_1(m)+f_2(m)$ und die Multiplikation durch $(f_1 \circ f_2)(m) = f_1(f_2(m))$. Nach dem Lemma von Schur 5.5.5 ist jedes $f \in \mathrm{End}_R(M) \setminus \{0\}$ ein Isomorphismus. Somit existiert eine Umkehrabbildung $f^{-1} \in \mathrm{End}_R(M)$. Diese ist offensichtlich das gesuchte multiplikative Inverse. □

NOTATION 5.6.5. Zwei Linksideale I_1, I_2 von R nennen wir isomorph, wenn sie isomorph als R-Moduln sind. Für eine Teilmenge $S \subseteq M$ eines R-Moduls M, schreiben wir $I_1.S$ für den kleinsten Untermodul von M der alle Elements $\lambda.a$, $\lambda \in I_1$ und $a \in S$, enthält. Man sieht leicht

$$I_1.S = \{\sum_{i=1}^{n} \lambda_i.a_i | n \in \mathbb{N}_0, \lambda_i \in I_1, a_i \in S \text{ für alle } i \in \{1, \ldots, n\}\}.$$

Diese Konstruktion hatten wir bereits im Beweis von Proposition 5.2.11 benutzt.

LEMMA 5.6.6. *Sei R ein halbeinfacher Ring, I ein einfaches Linksideal und M ein einfacher R-Modul. Für jedes $m \in M$ sei $T_m : I \longrightarrow M$ gegeben durch $T_m(\lambda) = \lambda.m$. Dann gilt*

(a) $\mathrm{Hom}_R(I, M) = \{T_m | m \in M\}$.
(b) $I \cong M \iff I.m = M$ *für ein* $m \in M$.
(c) $I \ncong M \iff I.M = \{0\}$.

BEWEIS. Wir beweisen nun die Aussagen, wobei (b) und (c) direkte Folgerungen aus (a) sind.

Zu (a): Die R-Modulstruktur von M impliziert sofort, dass für alle $m \in M$ gilt $T_m \in \mathrm{Hom}_R(I, M)$. Sei nun $\varphi \in \mathrm{Hom}_R(I, M)$ beliebig. Nach dem Lemma von Schur 5.5.5 ist φ entweder die Nullabbildung oder ein Isomorphismus. Die Nullabbildung ist natürlich gegeben durch φ_0. Sei also φ ein Isomorphismus.

Da R halbeinfach ist, existiert nach Theorem 5.5.8 ein Linksideal I' von R mit $R = I \oplus I'$. Jedes $\lambda \in R$ lässt sich also eindeutig schreiben als $\lambda = a + b$ mit $a \in I$ und $b \in I'$. Betrachte nun die Projektion auf die erste Komponente

$$\pi_1 : R \longrightarrow I \quad ; \quad \lambda = a + b \mapsto a.$$

Diese Projektion ist ein surjektiver R-Modul-Homomorphismus. Somit ist auch $\psi = \varphi \circ \pi_1 : R \longrightarrow M$ ein surjektiver R-Modul-Homomorphismus. Für $a \in I$ beliebig gilt

$$\varphi(a) = \varphi(\pi_1(a)) = \psi(a) = \psi(a \cdot 1) = a\psi(1).$$

Also ist tatsächlich $\varphi = T_m$ mit $m = \psi(1)$.

Zu (b): Es gilt

$$\begin{aligned} I \cong M &\overset{5.5.5}{\iff} \exists \varphi \in \mathrm{Hom}_R(I, M) \text{ mit } \varphi(I) = M \\ &\overset{(a)}{\iff} \exists m \in M \text{ mit } T_m(I) = I.m = M \end{aligned}$$

Zu (c): Es gilt

$$\begin{aligned} I \ncong M &\overset{5.5.5}{\iff} \mathrm{Hom}_R(I, M) = \{0\} \overset{(a)}{\iff} T_m(a) = a.m = 0 \ \forall m \in M, \forall a \in I \\ &\overset{5.6.5}{\iff} I.M = \{0\} \end{aligned}$$

□

KOROLLAR 5.6.7. *Sei R ein halbeinfacher Ring, dann ist jeder einfache R-Modul isomorph zu einem einfachen Linksideal von R.*

BEWEIS. Sei M ein einfacher R-Modul. Da R halbeinfach ist, gilt $R = \sum_{I \subseteq R} I$, wobei die Summe über alle einfachen Linksideale von R läuft. Damit ist

$$\{0\} \neq 0 = M = R.M = \sum_{I \subseteq R} I.R.$$

Somit existiert ein einfaches Linksideal I von R mit $I.M \neq \{0\}$. Mit Lemma 5.6.6 folgt $M \cong I$. □

THEOREM 5.6.8. *Sei R ein halbeinfacher Ring. Dann gibt es nur endlich viele paarweise nicht isomorphe einfache Linksideale $I_1, \ldots, I_s$ von R. Ist $I_1, \ldots, I_s$ eine vollständige Liste solcher Linksideale, dann gilt für alle $j \in \{1, \ldots, s\}$*

(a) *$R_j = \sum_{I \cong I_j} I$ ist ein zweiseitiges Ideal, wobei die Summe über alle Linksideale I von R mit $I \cong I_j$ läuft.*
(b) *R_j ist ein Teilring von R (mit Einselement) und es ist $R = \prod_{i=1}^{s} R_j$.*

BEWEIS. Wir berachten die Menge $S = \{I \subseteq R | I \text{ einfaches Linksideal}\}$ aller einfacher Linksideale von R. Auf dieser Menge bildet Isomorphie offensichtlich eine Äquivalenzrelation. Bezeichnen wir mit S_j, $j \in J$, die zugehörigen Äquivalenzklassen, so erhalten wir $S = \dot{\cup}_{j \in J} S_j$ und für $I \in S_j$, $I' \in S_i$ mit $i, j \in J$ gilt genau dann $I \cong I'$ wenn $i = j$ gilt.
Wir wollen zunächst (a) beweisen ohne uns um die Endlichkeit von J zu kümmern. Setze also $R_j = \sum_{I \in S_j} I$. Als Summe von Linksidealen ist auch R_j ein Linksideal von R für alle $j \in J$. Falls $i \neq j \in J$ und $I \in S_i$, $I \in S_j$, dann gilt nach Lemma 5.6.6 $I \cdot I' = 0$. Also gilt auch

$$R_i \cdot R_j = (\sum_{I \in S_i} I) \cdot (\sum_{I' \in S_j} I') = \sum_{(I,I') \in S_i \times S_j} I \cdot I' = 0 \ \forall i \neq j. \tag{48}$$

Der Ring R ist halbeinfach, also eine Summe von einfachen Linksidealen. Insbesondere ist R somit Summe aller einfacher Linksideale. Das heißt

$$R = \sum_{I \in S} I = \sum_{j \in J} \sum_{I \in S_j} I = \sum_{j \in J} R_j. \tag{49}$$

Zusammen erhalten wir

$$R_i \subseteq R_i \cdot R \overset{(49)}{=} R_i \cdot \sum_{j \in J} R_j = \sum_{j \in J} R_i \cdot R_j \overset{(48)}{\subseteq} R_i \ \forall i \in J.$$

Also gilt überall Gleichheit und wir erhalten $R_i = R_i \cdot R$ für alle $i \in J$. Damit ist R_i auch ein Rechtsideal, also ein beidseitiges Ideal. Damit ist Teil (a) bewiesen.

Als nächstes zeigen wir die Endlichkeit von J. Aus (49) wissen wir, dass $R \ni 1 = \sum_{j\in J} e_j$ gilt, mit $e_j \in R_j$ für alle $j \in J$. Wie immer ist dies eine endliche Summe. Es gibt also eine endliche Teilmenge $J' \subseteq J$ mit

$$j \in J' \Longleftrightarrow e_j \neq 0.$$

Wir setzen $|J'| = s$. Sei $\lambda \in R$ beliebig mit $\lambda \overset{(49)}{=} \sum_{i\in J} \lambda_i$ mit $\lambda_i \in R_i$ für alle $i \in J$. Dann gilt für $i \in J$

$$\lambda_i = 1 \cdot \lambda_i = (\sum_{j\in J'} e_j) \cdot \lambda_i = \sum_{j\in J'} (e_j \cdot \lambda_i) \overset{(48)}{=} \begin{cases} e_i \cdot \lambda_i \text{ falls } i \in J' \\ 0 \text{ sonst} \end{cases} \tag{50}$$

Für ein $i \in J \backslash J'$ wäre somit $R_i = \{0\}$, was nicht sein kann, da $\{0\} \neq I_i \subseteq R_i$ ist. Somit gilt $J = J' \overset{oBdA}{=} \{1, \ldots, s\}$. Wir wählen für jedes $i \in \{1, \ldots, s\}$ ein Element $I_i \in S_i$. Dies ist die gesuchte Menge von Idealen $I_1, \ldots, I_s$ aus der Formulierung des Theorems.
Bewisen wir nun Teil (b). Sei wieder $\lambda = \sum_{i\in J} \lambda_i$, mit $\lambda_i \in R_i$ für alle $i \in J$, ein beliebiges Element aus R. Aus (50) folgt, dass diese Darstellung eindeutig ist. Denn:

$$e_j \cdot \lambda = e_j \cdot \sum_{i=1}^{s} \lambda_i = \sum_{i=1}^{s} e_j \cdot \lambda_i \overset{(48)}{=} e_j \cdot \lambda_j \overset{(50)}{=} \lambda_j \ \forall j \in \{1, \ldots, s\}. \tag{51}$$

Also gilt $R = \bigoplus_{i=1}^{s} R_i = \prod_{i=1}^{s} R_i$ als R-Moduln. Gleichung (51) zeigt auch, dass e_j das Einselement in R_j ist, für alle $j \in \{1, \ldots, s\}$. Somit sind alle zweiseitigen Ideale $R_1, \ldots, R_j$ auch Ringe mit Einselement. Da die Ringmultiplikation auf den Ringen $R, R_1, \ldots, R_s$ genau die R-Skalarmultiplikation ist, ist R auch als Ring das direkte Produkt der Ringe $R_1, \ldots, R_s$. □

THEOREM 5.6.9. *Die Ringe $R_1, \ldots, R_s$ aus Theorem 5.6.8 sind einfache Ringe. Weiter ist jedes R_i eine endliche direkte Summe von einfachen Linksidealen, die alle isomorph (zu I_i) sind.*

BEWEIS. Wir übernehmen die Notation aus Theorem 5.6.8. Sei $j \in \{1, \ldots, s\}$ beliebig. Jedes Linksideal I von R mit $I \subseteq R_j$ ist natürlich auch ein Linksideal des Ringes R_j. Ist umgekehrt I ein Linksideal in R_j, so folgt aus (48), dass I auch ein Linksideal in R ist. Denn für $\lambda = \sum_{i=1}^{s} \lambda_i \in R$ beliebig (mit $\lambda_i \in R_i$ fr alle $i \in \{1, \ldots, s\}$) gilt

$$\lambda \cdot I = \sum_{i=1}^{s} \lambda_i \cdot I \overset{(48)}{=} \lambda_j \cdot I \subseteq I.$$

Wir haben also gezeigt, dass alle einfachen Linksideale I von R mit $I \subseteq R_j$ einfache R_j-Moduln sind. Somit ist R_j nach Theorem 5.5.8 halbeinfach. Es existieren also einfache Linksideale $\{I_k\}_{k\in K}$ von R_j mit $R_j = \bigoplus_{k\in K} I_K$.

Wir bezeichnen das Einselement in R_j wieder mit e_j. Dann existiert eine endliche Tilmenge $K_0 \subset K$, so dass $e_j \in \bigoplus_{k\in K_0} I_k$. Es folgt

$$\bigoplus_{k\in K} I_k = R_j = R_j \cdot e_j \subseteq R \cdot \bigoplus_{k\in K_0} I_k \subseteq \bigoplus_{k\in K_0} I_k \subseteq \oplus_{k\in K} I_k.$$

Also ist $R = \bigoplus_{k\in K_0} I_k$ für die endliche Menge K_0. Weiter sind nach Konstruktion von R_j alle I_k, $k \in K_0$, isomorph.
Es bleibt zu zeigen, dass R_j ein einfacher Ring ist. Sei dazu $I \subseteq R_j$ ein von Null verschiedenes zweiseitiges Ideal. Als Linksideal von R_j ist I nach Korollar 5.5.9 halbeinfach. Insbesondere existiert ein einfaches Linksideal J von R_j mit $J \subseteq I$. Da I auch ein Rechtsideal von R_j ist, gilt $I \cdot \lambda \subseteq I$ für alle $\lambda \in R_j$. Nach Lemma 5.6.6 liegen also alle einfachen Linksideale I' von R_j mit $I' \cong J$ in I. Da R_j jedoch genau die Summe all dieser I' ist, ist $R_j \subseteq I$. Somit gilt $I = R_j$ und R_j ist wie behauptet ein einfacher Ring. □

Proposition 5.6.10. *Sei R halbeinfach und M ein R-Modul. Dann ist auch M halbeinfach.*

Beweis. Sei M ein R-Modul. Der freie R-Modul $F(M)$ mit Basis M (siehe 5.2.8) ist als direkte Summe von halbeinfachen R-Moduln (nämlich R) selbst auch halbeinfach. Da $\{m \in M\}$ eine Basis von $F(M)$ ist, existiert ein (notwendigerweise) surjektiver R-Modul-Homomorphismus $\varphi : F(M) \longrightarrow M$ mit $\varphi(m) = m$. Der Homomorphisatz liefert nun $M \cong {}^{F(M)}/_{\ker(\varphi)}$, was als Faktormodul eines halbeinfachen Moduls wieder halbeinfach ist (siehe Korollar 5.5.9). □

Beispiel 5.6.11. Sei D ein Schiefkörper und $n \in \mathbb{N}$. Wir betrachten den Matrizenring $M_n(D)$. Nach Lemma 5.6.3 ist $M_n(D)$ ein einfacher Ring. Wir werden zeigen, dass $M_n(D)$ auch halbeinfach ist. Dazu sei für jedes $k \in \{1, \ldots, n\}$

$$L_k = \{B = (b_{ij}) \in M_n(D) | b_{ij} = 0 \text{ für } j \neq k\}.$$

Jedes dieser L_k ist ein Linksideal, da Multiplikation von rechts mit einem Element B aus L_k alles ausser die k-te Spalte eliminiert. Weiter ist jedes dieser L_k sogar ein einfaches Linksideal in $M_n(D)$, denn:
Sei $\{0\} \neq I \subseteq L_k$ und $B = (b_{ij}) \in I \setminus \{0\}$ beliebig. Wir nehmen oBdA $b_{1k} \neq 0$ an. Für $l, m \in \{1, \ldots, n\}$ definieren wir

$$E_{ml} = (e_{ij}) \text{ mit } e_{ij} = \begin{cases} 1 \text{ falls } i = m \text{ und } j = l \\ 0 \text{ sonst} \end{cases}$$

Dann ist $E_{1k} = (b_{1k}^{-1})E_{11} \cdot B \in I$. Weiter ist $E_{lk} = E_{l1} \cdot E_{1k} \in I$ für alle $l \in \{1, \ldots, n\}$. Da die Matrizen $E_{1k}, \ldots, E_{nk}$ offensichtlich Erzeugende von ganz L_k sind, ist $I = L_k$ und L_k ist ein einfaches Linksideal.
Weiter gilt $M_n(D) = L_1 \oplus \cdots \oplus L_n$. Nach Theorem 5.6.9 sind alle $L_1, \ldots, L_n$ isomorph und nach Lemma 5.6.6 existiert daher zu jedem Paar $(i, j) \in \{1, \ldots, n\}^2$ ein $\lambda \in M_n(D)$ mit $L_i = L_j \cdot \lambda$. Dies gilt zum Beispiel für $\lambda = E_{ij}$.

KONSTRUKTION 5.6.12. Sei M ein R-Modul, wobei diesmal R ein beliebiger Ring ist. In Proposition 5.1.7 haben wir gesehen, dass M durch $\varphi.m = \varphi(m)$ auch ein $R' = \mathrm{End}_R(M)$-Modul ist. Wiederholen wir dieses Prinzip so sehen wir, dass M auch ein $R'' = \mathrm{End}_{R'}(M)$-Modul ist.
Für $\lambda \in R$ beliebig, betrachten wir die R-Skalarmultiplikation auf M

$$ {}_\lambda T : M \longrightarrow M \quad ; \quad m \mapsto \lambda.m. $$

Seien $\varphi \in R' = \mathrm{End}_R(M)$ und $\lambda \in R$ beliebig, dann gilt

$$ {}_\lambda T(\varphi.m) = {}_\lambda T(\varphi(m)) = \lambda.\varphi(m) = \varphi(\lambda.m) = \varphi({}_\lambda T(m)) = \varphi.{}_\lambda T(m) $$

für alle $m \in M$. Da ${}_\lambda T$ auch offensichtlich ein Gruppen-Homomorphismus ist, gilt ${}_\lambda T \in \mathrm{End}_{R'}(M) = R''$. Wir erhalten eine Abbildung

$$ T : R \longrightarrow R'' \quad ; \quad \lambda \mapsto {}_\lambda T. $$

PROPOSITION 5.6.13. *Sei R ein einfacher Ring und $I \neq \{0\}$ ein Linksideal in R. Weiter setzen wir $R' = \mathrm{End}_R(I)$ und $R'' = \mathrm{End}_{R'}(I)$. Dann ist die eben konstruierte Abbildung T aus 5.6.12 ein Ring-Isomorphismus.*

BEWEIS. Aus der R-Modulstruktur von I folgt sofort, dass T ein Ring-Homomorphismus ist. Für $\lambda \in \ker(T)$ und $\mu \in R$ beliebig gilt

$$ {}_{(\lambda\mu)}T = {}_\lambda T \circ {}_\mu T = 0 \circ {}_\mu T = 0 = {}_\mu T \circ {}_\lambda T = {}_{(\mu\lambda)}T. $$

Also ist $\ker(T) \subseteq R$ ein zweiseitiges Ideal im einfachen Ring R. Da $1 \notin \ker(T)$, muss daher $\ker(T) = 0$ sein. Somit ist T injektiv.
Es bleibt die Surjektivität von T zu zeigen. Da $\lambda \cdot I \subseteq I$ und $R \cdot \lambda R$ für alle $\lambda \in R$, ist auch $I \cdot R$ ein zweiseitiges Ideal in R. Weiter ist $I \subseteq I \cdot R$ und $I \neq \{0\}$, also $I \cdot R = R$ (wieder da R ein einfacher Ring ist). Somit gilt auch

$$ T(I) \circ T(R) = T(R). \tag{52} $$

Wir betrachten die Rechtsmultiplikation $T_\lambda : I \longrightarrow I$, $T_\lambda(\mu) = \mu\lambda$, aus Lemma 5.6.6. Wir wissen bereits, dass $T_\lambda \in R'$ gilt für alle $\lambda \in I$. Für $f \in R''$ gilt also

$$ f(\mu\lambda) = f(T_\lambda(\mu) \overset{f \ R'\text{-linear}}{=} T_\lambda(f(\mu)) = f(\mu)\lambda \ \forall \lambda, \mu \in I. $$

Dies bedeutet $f \circ {}_\mu T = {}_{f(\mu)}T$ für alle $\mu \in I$,also $f \circ T(I) \in T(I)$. Somit ist $T(I)$ ein Linksideal in R''. Dies liefert nun

$$R'' = R'' \circ T(R) \overset{(52)}{=} R''\theta(I)\theta(R) \overset{T(I)\ \text{Linksideal}}{=} T(I) \circ T(R) = T(R).$$

Also ist T auch surjektiv und daher ein Ringisomorphismus. □

THEOREM 5.6.14 (Satz von Artin-Wedderburn). *Für einen Ring $R \neq \{0\}$ sind folgende Aussagen äquivalent:*

(i) *R ist ein einfacher (links)artinscher Ring.*
(ii) *$R \cong M_n(D)$ für einen Schiefkörper D und $n \in \mathbb{N}$.*

BEWEIS. Die Implikation $(ii) \Longrightarrow (i)$ ist die Aussage in Lemma 5.6.3. Es bleibt also $(i) \Longrightarrow (ii)$ zu zeigen.
Da R artinsch ist wird jede absteigende Kette von Linksidealen in R stationär. Es existiert also ein einfaches Linksideal I in R. Nach Proposition 5.6.4 ist $\mathrm{End}_R(I) = D$ ein Schiefkörper. Seien $x_1, \ldots, x_k \in I$ D-linear unabhängig. Dann existiert ein $\varphi : I \longrightarrow I$ in $\mathrm{End}_D(I)$ mit $\varphi(x_1) = \cdots = \varphi(x_{k-1}) = 0$ und $\varphi(x_k) = x_k$. Weiter ist nach Proposition 5.6.13 $\varphi = {}_\lambda T$ für ein $\lambda \in R$. Das heißt

$$\lambda x_1 = \cdots \lambda x_{k-1} = 0 \text{ und } \lambda x_k = x_k \neq 0.$$

Also ist $\lambda \in \mathrm{Ann}(x_1, \ldots, x_{k-1}) \setminus \mathrm{Ann}(x_1, \ldots, x_k)$. Nach Lemma 5.4.4 haben wir also ein echt absteigende Kette von Linksidealen

$$\mathrm{Ann}(x_1) \supsetneq \mathrm{Ann}(x_1, x_2) \supsetneq \cdots \mathrm{Ann}(x_1, \ldots, x_k). \tag{53}$$

Falls ein $x_{k+1} \in I$ existiert, so dass $x_1, \ldots, x_{k+1}$ D-linear unabhängig sind, erweitern wir die Kette (53) um ein Glied. Da R artinsch ist, bricht dieses Verfahren irgendwann ab und wir erhalten eine maximale D-linear unabhängige Teilmenge $\{x_1, \ldots, x_n\}$ von I. Also ist I ein n-dimensionaler D-Vektorraum und es gilt

$$R \overset{5.6.13}{\cong} \mathrm{End}_D(I) \overset{LinA}{\cong} M_n(D).$$

Das war zu zeigen. □

KOROLLAR 5.6.15 (Wedderburns Struktursatz). *Ein Ring R ist halbeinfach, genau dann wenn Schiefkörper $D_1, \ldots, D_r$ und Zahlen $n_1, \ldots, n_r$ existieren so dass*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).$$

BEWEIS. Übung. □

.

ABBILDUNG 5.4. Der schottische Mathematiker *Joseph Henry Maclagan Wedderburn* (1882-1948) war lange Zeit herausgeber der Zeitschrift *Annals of Mathematics*, einem der renomiertesten mathematischen Journals.

5.7. Das Tensorprodukt

Wir setzen in diesem Abschnitt R als kommutativen Ring voraus. Für zwei gegebene R-Moduln M und N kennen wir bereits das direkte Produkt und die direkte Summe von M und N. Wir werden in diesem kurzen Abschnitt eine weitere, bilineare, Konstruktion kennenlernen um aus M und N einen neuen R-Modul zu erhalten. Diese Konstruktion kommt neben der Algebra auch in der Differenzialgeometrie und der Physik vor.

DEFINITION 5.7.1. Seien M, N, P drei R-Mduln. Eine Abbildung $f : M \times N \longrightarrow P$ heißt *bilinear*, genau dann wenn für alle $a, a' \in M$, $b, b' \in N$ und $\lambda \in R$ gilt:

- $f(a + a', b) = f(a, b) + f(a', b)$ und
- $f(a, b + b') = f(a, b) + f(a, b')$ und
- $f(\lambda.a, b) = \lambda.f(a, b) = f(a, \lambda.b)$.

KONSTRUKTION 5.7.2. Seien wieder M und N zwei R-Moduln. Wir betrachten die Menge $M \times N$, wobei wir die Modulstruktur von $M \times N$ vergessen. Nun bilden wir den freien R-Modul $F(M \times N)$ mit $M \times N$ als R-Basis. Die Elemente aus $F(M \times N)$ sind also R-Linearkombinationen der Elemente $(a, b) \in M \times N$. Sei $E \subseteq F(M \times N)$ der Untermodul, das von den folgenden Elementen erzeugt ist

$$\left.\begin{array}{l} (a, b) + (a', b) - (a + a', b) \\ (a, b) + (a, b') - (a, b + b') \\ \lambda(a, b) - (\lambda a, b) \\ \lambda(a, b) - (a, \lambda b) \end{array}\right\} a, a' \in M,\ b, b' \in N,\ \lambda \in R$$

Der R-Modul ${}^{F(M\times N)}/_{E}$ heißt *Tensorprodukt von M und N über R* und wird mit $M \otimes_R N$ bezeichnet. Das *Tensorprodukt von $a \in M$ und $b \in N$ über R* ist gegeben als

$$a \otimes_R b = (a, b) + E \in {}^{F(M\times N)}/_{E} = M \otimes_R N.$$

Per Konstruktion ist klar, dass sich jedes Element in $M \otimes_R N$ als Linearkombination $\sum_{(a,b)\in M\times N} \lambda_{(a,b)}(a \otimes_R b)$ mit $\lambda_{(a,b)} \in R$ nur endlich oft ungleich

Null schreiben lässt. Beachte, dass nicht jedes Element in $M \otimes_R N$ die Form $a \otimes_R b$ hat!
Wenn klar ist über welchem Ring wir arbeiten, schreiben wir schlicht $\otimes$ anstatt $\otimes_R$.

PROPOSITION 5.7.3. *Mit den Notationen aus 5.7.2 gelten die folgenden Rechenregeln in $M \otimes N$:*

(i) $(a + a') \otimes b = a \otimes b + a' \otimes b$
(ii) $a \otimes (b + b') = a \otimes b + a \otimes b'$
(iii) $\lambda(a \otimes b) = (\lambda.a) \otimes b$
(iv) $\lambda(a \otimes b) = a \otimes (\lambda.b)$.

BEWEIS. Dies folgt sofort aus der Konstruktion von E aus 5.7.2. Denn für alle $a_1, a_1', a_2, a_2' \in M$, $b_1, b_1', b_2, b_2' \in N$ und $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in R$ gilt:

$$\begin{aligned}
&\lambda_1(a_1 + a_1') \otimes \lambda_2(b_1 + b_1') = \lambda_3(a_2 + a_2') \otimes \lambda_4(b_2 + b_2') \\
\iff &\lambda_1(a_1 + a_1') \otimes \lambda_2(b_1 + b_1') - \lambda_3(a_2 + a_2') \otimes \lambda_4(b_2 + b_2') \\
\overset{\text{Def.}}{\iff} &(\lambda_1.(a_1 + a_1'), \lambda_2.(b_1 + b_1')) - (\lambda_3.(a_2 + a_2'), \lambda_4.(b_2 + b_2')) + E = 0 \\
\iff &(\lambda_1.(a_1 + a_1'), \lambda_2.(b_1 + b_1')) - (\lambda_3.(a_2 + a_2'), \lambda_4.(b_2 + b_2')) \in E
\end{aligned}$$

Dies ist per Definition von E für alle Gleichungen (i)-(iv) erfüllt. □

Die nächste Proposition zeigt, dass das Tensorprodukt bis auf Isomorphie eindeutig durch eine einzige Eigenschaft bestimmt ist. Wir sprechen in einem solchen Fall von einer *universellen* Eigenschaft.

PROPOSITION 5.7.4. *Das Tensorprodukt $M \otimes_R N$ der R-Moduln M und N erfüllt zusammen mit der Abbildung*

$$i : M \times N \longrightarrow M \otimes_R N \quad ; \quad (a, b) \mapsto a \otimes_R b$$

folgende universelle Eigenschaft[1]*:*

(a) *Sei P ein R-Modul und $f : M \times N \longrightarrow P$ bilinear. Dann existiert genau ein R-Modul-Homomorphismus $\varphi : M \otimes_R N \longrightarrow P$ so, dass $\varphi \circ i = f$.*
(b) *Falls T ein R-Modul ist und $\tau : M \times N \longrightarrow T$ eine bilineare Abbildung, so dass es für jede bilineare Abbildung $f : M \times N \longrightarrow P$ genau einen R-Modul-Homomorphismus $\varphi : T \longrightarrow P$ gibt mit $\varphi \circ \tau = f$, dann existiert genau ein R-Modul-Isomorphismus $\psi : T \longrightarrow M \otimes_R N$ mit $\psi \circ i = \tau$.*

[1]Dies ist ein Konzept aus der *Kategorientheorie*. In dieser Sprache ist das Tensorprodukt streng genommen gegeben durch das Paar $(M \otimes N, i)$.

BEWEIS. Übung. □

KOROLLAR 5.7.5. *Seien M_1, M_2, N_1, N_2 R-Moduln und $\varphi_i : M_i \longrightarrow N_i$, $i \in \{1, 2\}$, R-Modul-Homomorphismen. Dann existiert genau ein R-Modul-Homomorphismus $\varphi = \varphi_1 \otimes \varphi_2 : M_1 \otimes M_2 \longrightarrow N_1 \otimes N_2$ mit $\varphi(a_1 \otimes a_2) = \varphi_1(a_1) \otimes \varphi_2(a_2)$ für alle $a_i \in M_i$.*

BEWEIS. Da φ_1, φ_2 R-Modul-Homomorphismen sind, ist die Abbildung

$$f : M_1 \times M_2 \longrightarrow N_1 \otimes N_2 \quad ; \quad (a_1, a_2) \mapsto \varphi_1(a_1) \otimes \varphi_2(a_2)$$

bilinear. Mit Proposition 5.7.4 erhalten wir sofort die gewünschte Aussage. □

KOROLLAR 5.7.6. *Für jeden R-Modul M gilt $R \otimes_R M \cong M \cong M \otimes_R R$.*

BEWEIS. Wir beweisen nur die erste Isomorphie, die zweite folgt analog. Die Abbildung

$$f : R \times M \longrightarrow M \quad ; \quad (\lambda, a) \mapsto \lambda.a$$

ist bilinear. Nach Proposition 5.7.4 existiert also genau ein R-Modul-Homomorphismus $\varphi : R \otimes_R M \longrightarrow M$ mit $\varphi(\lambda \otimes (a) = \lambda.a$ für alle $\lambda \in R$ und für alle $a \in M$. Mit Proposition 5.7.3 gilt $\lambda \otimes a = 1 \otimes (\lambda.a)$. Somit ist $\psi : M \longrightarrow R \otimes_R M$, $a \mapsto 1 \otimes a$, als R-Modul-Homomorphismus (wieder Proposition 5.7.3) eine Umkehrabbildung von φ. Also ist φ ein Isomorphismus und es gilt $M \cong R \otimes_R M$. □

PROPOSITION 5.7.7. *Seien $(M_i)_{i \in I}$ und $(N_j)_{j \in J}$ Familien von R-Moduln. Dann gibt es einen Isomorphismus*

$$(\bigoplus_{i \in I} M_i) \otimes_R (\bigoplus_{j \in J} N_j) \xrightarrow{\sim} \bigoplus_{(i,j) \in I \times J} (M_i \otimes N_j) = T.$$

BEWEIS. Wir setzen $M = \bigoplus_{i \in I} M_i$ und $N = \bigoplus_{j \in J} N_j$ und zeigen, dass T die Bedingung aus Proposition 5.7.4 (b) erfüllt. Sei dazu

$$\tau : M \times N \longrightarrow T \quad ; \quad ((a_i)_{i \in I}, (b_j)_{j \in J}) \mapsto (a_i \otimes b_j)_{(i,j) \in I \times J}$$

die benötigte bilineare Abbildung. Wir müssen also zeigen, dass für einen beliebigen R-Modul P und eine beliebige bilineare Abbildung $f : M \times N \longrightarrow P$, ein eindeutiger R-Modul-Homomorphismus $\varphi : T \longrightarrow P$ existiert mit $\varphi(\tau((a, b))) = f((a, b))$ für alle $(a, b) \in M \times N$.
Für alle Tupel $(i, j) \in I \times J$ ist $f_{ij} = f|_{M_i \times N_j} : M_i \times N_j \longrightarrow P$ bilinear. Wir dürfen also Proposition 5.7.4 anwenden und erhalten einen eindeutigen R-Modul-Homomorphismus $\varphi_{ij} : M_i \otimes N_j \longrightarrow P$ mit $\varphi_{ij}(\tau((a_i, b_j))) =$

$f_{ij}((a_i, b_j))$ für alle $a_i \in M_i$ und alle $b_j \in N_j$. Diese R-Modul-Homomorphismen φ_{ij} können wir nun zu unserem gesuchten R-Modul-Homomorphismus φ zusammensetzen, durch:

$$\varphi(\tau((a_i)_{i\in I}, (b_j)_{j\in J})) = (\varphi_{ij}(a_i \otimes b_j))_{(i,j)\in I\times J}.$$

Die Eindeutigkeit von φ folgt unmittelbar aus der Eindeutigkeit der $\varphi_{i,j}$'s. Somit erfüllt T die Voraussetzung aus Proposition 5.7.4 und es folgt, dass T isomorph zu $M \otimes N$ ist. □

KOROLLAR 5.7.8. *Ist M ein freier R-Modul mit Basis $(e_i)_{i\in I}$ und ist N ein freier R-Modul mit Basis $(f_j)_{j\in J}$, dann ist $M \otimes_R N$ ein freier R-Modul mit Basis $(e_i \otimes_R f_j)_{(i,j)\in I\times J}$.*

BEWEIS. Es gilt

$$M\otimes N = (\bigoplus_{i\in I} Re_i)\otimes(\bigoplus_{j\in J} Rf_j) \overset{5.7.7}{\cong} \bigoplus_{(i,j)\in I\times J} (Re_i\otimes Rf_j) = \bigoplus_{(i,j)\in I\times J} R(e_i\otimes f_j).$$

□

KAPITEL 6

Darstellungstheorie

Oft kommen Gruppen in einem starken Geometrischen Zusammenhang vor. Zum Beispiel ist die n-te Diedergruppe $D_n = \langle x, y | \operatorname{ord}(x) = n,\ \operatorname{ord}(y) = 2,\ yxy^{-1} = x^{-1} \rangle$ *darstellbar* als Symmetriegruppe eines regelmässigen n-Ecks. Solch eine Beschreibung einer Gruppe heißt *Darstellung*. Unter anderem spielen Darstellungen von Galoisgruppen eine wichtige Rolle in Wiles Beweis von Fermat's letztem Satz. Wir werden (komplexe) Darstellungen von endlichen Gruppen studieren und dabei die Modultheorie des letzen Kapitel benutzen.

6.1. Die Gruppenalgebra und weitere Grundlagen

In diesem Abschnitt werden wir den Zusammenhang von Darstellungen und Moduln herleiten. Sei dazu G eine Gruppe und K ein Körper.

Definition 6.1.1. Eine *Darstellung der Gruppe G auf einen K-Vektorraum V* ist ein Gruppen-Homomorphismus $\rho : G \longrightarrow GL_K(V)$. Wir sprechen auch kurz von *Darstellung* von G. Die *Dimension einer Darstellung* ist die Dimension des Vektorraumes V.

Bemerkung 6.1.2. Sei ρ eine Darstellung von G. Wir bezeichnen das Bild von g unter ρ mit $\rho_g \in GL_K(V)$. Zu jedem K-Vektorraum V haben wir die triviale Darstellung von G auf V, gegeben durch $\rho_g = \mathrm{id}_V$ für alle $g \in G$. Jede eindimensionale Darstellung von G können wir auffassen als Gruppen-Homomorphismus $\rho : G \longrightarrow K^*$ und jeder solche Gruppen-Homomorphismus ist eine eindimensionale Darstellung von G.

Wiederholung. Eine *K-Algebra* ist ein Ring mit einer K-Skalarmultiplikation, so dass die Ringmultiplikation K-bilinear ist. Ein *K-Algebren-Homomorphismus* ist ein K-linearer Ring-Homomorphismus.

Konstruktion 6.1.3. Sei G eine Gruppe und K ein Körper. Wir definieren den freien K-Modul (=K-Vektorraum) $F(G)$ mit kanonischer Basis G. Wie in 5.6.9 sehen wir hier G als Menge an. Es lässt sich jedes Element in $F(G)$ eindeutig schreiben als $\alpha = \sum_{g \in G} \lambda_g . g$, mit $\lambda_g \in K$ nur endlich oft verschieden von Null.

Wir wollen auf $F(G)$ eine (Ring-)Multiplikation definieren. Da diese die Distributivgesetze erfüllen muss, genügt es $(\lambda.g) \cdot (\lambda'.h)$ zu definieren für $\lambda, \lambda' \in K$ und $g, h \in G$. Wir setzen (natürlich) $(\lambda.g) \cdot (\lambda'.h) = (\lambda\lambda').(gh)$. Damit gilt für beliebige $\alpha_1 = \sum_{g\in G} \lambda_g.g, \alpha_2 = \sum_{g\in G} \lambda'.g \in F(G)$

$$\alpha_1 \cdot \alpha_2 = (\sum_{g\in G} \lambda_g.g) \cdot \sum_{g\in G} \lambda'.g = \sum_{g\in G} (\sum_{g_1 g_2 = g} \lambda_{g_1}\lambda'_{g_2}).g$$

Wir haben also einen K-Vektorraum $F(G)$ der zusätzlich ein Ring bezüglich „$\cdot$“ ist, also ist $(F(G), \cdot)$ eine K-Algebra. Um diese K-Algebra vom Modul $F(G)$ zu unterscheiden bezeichnen wir Sie mit $K[G]$ und nennen sie die *Gruppenalgebra* von G über K. Per Konstruktion ist $\dim_K(K[G]) = |G|$.
Die kanonischen Einbettungen

$$i_G : G \longrightarrow (K[G])^* \quad ; \quad g \mapsto 1.g \quad \text{und}$$

$$i_K : K \longrightarrow K[G] \quad ; \quad \lambda \mapsto \lambda.e$$

sind offensichtlich injektive Gruppen-Homomorphismen, wodurch wir $G \subseteq K[G]$ und $K \subseteq K[G]$ annehmen dürfen.

PROPOSITION 6.1.4. *Die Gruppenalgebra $K[G]$ erfüllt zusammen mit der Abbildung i_G folgende universelle Eigenschaft:*

(a) *Für jeden Gruppen-Homomorphismus $f : G \longrightarrow \mathcal{A}^*$, für eine K-Algebra $\mathcal{A}$, existiert genau ein K-Algebren-Hom. $\varphi : K[G] \longrightarrow \mathcal{A}$ mit $\varphi \circ i_G = f$.*

(b) *Falls (a) für eine K-Algebra $\mathcal{B}$ und einen Gruppen-Homomorphismus $j : G \longrightarrow \mathcal{B}^*$ anstelle von $K[G]$ und i_G gilt. Dann existiert genau ein K-Algebren-Isomorphismus $\psi : K[G] \longrightarrow \mathcal{B}$ mit $\psi \circ i_G = j$.*

BEWEIS. Genau wie bei Proposition 5.7.4, was in den Übungen gezeigt wurde. □

KOROLLAR 6.1.5. *Sei $f : G \longrightarrow G'$ ein Gruppen-Homomorphismus. Dann existiert genau ein K-Algebren-Homomorphismus $\varphi : K[G] \longrightarrow K[G']$ mit $\varphi|_G = f$.*

BEWEIS. Die Abbildung $f : G \longrightarrow K[G']^*$ mit $g \mapsto f(g)$ ist ein Gruppen-Homomorphismus. Proposition 6.1.4 (a) liefert nun den gewünschten K-Algebren-Homomorphismus φ. □

PROPOSITION 6.1.6. *Sei V ein K-Vektorraum und G eine Gruppe. Es gibt eine Bijektion zwischen den Darstellungen von G auf V und den $K[G]$-Linksmodulstrukturen auf V, die die K-Skalarmultiplikation auf V fortsetzen. Genauer:*

(a) *Falls* $\rho : G \longrightarrow GL_K(V)$ *eine Darstellung ist, so liefert*

$$K[G] \times V \longrightarrow V \quad ; \quad (\sum_{g\in G} \lambda_g g, v) \mapsto (\sum_{g\in G} \lambda_g g).v = \sum_{g\in G} \lambda_g \rho_g(v)$$

eine $K[G]$*-Modulstruktur auf* V*.*

(b) *Falls* V *ein* $K[G]$*-Modul ist, so dass die* $K[G]$*-Skalarmultiplikation eingeschränkt auf* K *mit der* K*-Skalarmultiplikation des Vektorraumes* V *übereinstimmt so ist*

$$\rho : G \longrightarrow GL_K(V) \quad ; \quad g \mapsto \rho_g \text{ mit } \rho_g(v) = g.v \ \forall v \in V$$

eine Darstellung von G *auf* V*.*

Beweis. Dies kann ohne große Mühen nachgerechnet werden. Wir wollen diese Aussage jedoch als eine Anwendung der Bijektion zwischen R-Moduln M und abelschen Gruppen M mit einem Ring-Homomorphismus $\varphi : R \longrightarrow \mathrm{End}(M)$ herleiten. Hier setzen wir $R = K[G]$ und $M = V$. Dann bilden nach Proposition 5.1.7 die Abbildungen

$$\{K[G]\text{-Modulstruktur von } V\} \overset{\varphi(\alpha)(v)=\alpha.v}{\longmapsto} \left\{ \begin{smallmatrix} \varphi:K[G]\longrightarrow \mathrm{End}(V) \\ \text{Ring-Homomorphismus} \end{smallmatrix} \right\}$$

$$\left\{ \begin{smallmatrix} \varphi:K[G]\longrightarrow \mathrm{End}(V) \\ \text{Ring-Homomorphismus} \end{smallmatrix} \right\} \overset{\alpha.v=\varphi(\alpha)(v)}{\longmapsto} \{K[G]\text{-Modulstruktur von } V\}$$

eine bijektive Korrespondenz. Schränken wir uns auf Modulstrukturen von V ein, die die K-Linearität von V respektieren so erhalten wir dieselbe bijektive Korrespondenz zwischen den Mengen

$$\left\{ \begin{smallmatrix} K[G]\text{-Modulstruktur von } V, \\ \text{die } K\text{-Skalarmult. fortsetzt} \end{smallmatrix} \right\} \text{ und } \left\{ \begin{smallmatrix} \varphi:K[G]\longrightarrow \mathrm{End}_K(V) \\ K\text{-Algebren-Hom.} \end{smallmatrix} \right\}.$$

Mit Proposition 6.1.4 ist auch die Korrespondenz

$$\left\{ \begin{smallmatrix} \varphi:K[G]\longrightarrow \mathrm{End}_K(V) \\ K\text{-Algebren-Hom.} \end{smallmatrix} \right\} \overset{\rho=\varphi|_G}{\longmapsto} \left\{ \begin{smallmatrix} \rho:G\longrightarrow \mathrm{End}_K(V) \\ \text{Darstellung} \end{smallmatrix} \right\}$$

$$\left\{ \begin{smallmatrix} \rho:G\longrightarrow \mathrm{End}_K(V) \\ \text{Darstellung} \end{smallmatrix} \right\} \overset{\varphi(\sum_{g\in G} \lambda_g g)(v)=\sum_{g\in G} \lambda_g \rho_g(v)}{\longmapsto} \left\{ \begin{smallmatrix} \varphi:K[G]\longrightarrow \mathrm{End}_K(V) \\ K\text{-Algebren-Hom.} \end{smallmatrix} \right\}$$

bijektiv. Beachte, dass $G \subseteq K[G]^*$ ist, und somit der Ring-Homomorphismus φ tatsächlich auf $\mathrm{End}_K(V)^* = GL_K(V)$ abgebildet wird. Damit folgt die Proposition. □

Definition 6.1.7. Die Darstellung, die zu $K[G]$ aufgefasst als $K[G]$-Modul korrespondiert, heißt *reguläre Darstellung* von G.

Definition 6.1.8. Seien V und W zwei K-Vektorräume und σ eine Darstellung von G auf V und ρ eine Garstellung von G auf W.

(a) Ein $\varphi \in \mathrm{Hom}_K(V, W)$ heißt G*-äquivariant* genau dann wenn $\varphi \circ \sigma_g = \rho_g \circ \varphi$ für alle $g \in G$ gilt.

(b) Die Darstellungen σ und ρ heißen *äquivalent* genau dann wenn ein G-äquivarianter K-Vektorraum-Isomorphismus $\varphi : V \longrightarrow W$ existiert.

(c) Ein Unterraum P von V heißt *G-invariant* genau dann wenn $\sigma_g(P) \subseteq P$ für alle $g \in G$ gilt.

(d) Die Darstellung σ heißt *irreduzibel* genau dann wenn 0 und V die einzigen G-invarianten K-Vektorräume von V sind.

DEFINITION 6.1.9. Sei $(V_i)_{i\in I}$ eine Familie von K-Vektorräumen und sei σ_i eine Darstellung von G auf V_i für jedes $i \in I$.

(a) Die *direkte Summe* $\bigoplus_{i\in I} \sigma_i$ ist eine Darstellung von G auf $\bigoplus_{i\in I} V_i$ gegeben durch

$$(\bigoplus_{i\in I} \sigma_i)_g((v_i)_{i\in I}) = ((\sigma_i)_g(v_i))_{i\in I} \text{ für alle } (v_i)_{i\in I} \in \bigoplus_{i\in I} V_i.$$

(b) Eine Darstellung σ von G auf V heißt *vollreduzibel* genau dann wenn σ die direkte Summe einer Familie von irreduziblen Darstellungen ist.

All diese Definitionen spiegeln bekannte Definitionen aus der Modultheorie wieder. Die Brücke zwischen Darstellungen und $K[G]$-Moduln schlägt gerade Proposition 6.1.6.

PROPOSITION 6.1.10. *Sei G eine Gruppe, K ein Körper, V, W zwei K-Vektorräume und σ und ρ seien Darstellungen von G auf V beziehungsweise auf W. Mit Proposition 6.1.6 können wir V und W auch als $K[G]$-Moduln auffassen. Dann gilt*

(a) *$\varphi : V \longrightarrow W$ ist G-äquivariant genau dann wenn φ ein $K[G]$-Modul-Homomorphismus ist.*

(b) *σ und ρ sind äquivalent genau dann wenn V und W isomorph als $K[G]$-Moduln sind.*

(c) *Ein Unterraum $P \subseteq V$ ist G-invariant genau dann wenn P ein $K[G]$-Untermodul von V ist.*

(d) *σ ist irreduzibel genau dann wenn V ein einfacher $K[G]$-Modul ist.*

(e) *σ ist vollreduzibel genau dann wenn V ein halbeinfacher $K[G]$-Modul ist.*

BEWEIS. Die $K[G]$-Modulstruktur auf V ist gegeben durch die Vorschrift $(\sum_{g\in G} \lambda_g g).v = \sum_{g\in G} \lambda_g \sigma_g(v)$. Die $K[G]$-Modulstruktur von W ist analog definiert.

Zu (a): Definitionsgemäß sind G-invariante Abbildungen und $K[G]$-Modul-Homomorphismen beides Gruppen-Homomorphismen. Es bleibt zu

zeigen, dass die Eigenschaft $\varphi \circ \sigma_g = \rho_g \circ \varphi$ für alle $g \in G$ gerade die $K[G]$-Linearität wiederspiegelt.

Sei zunächst $\varphi : V \longrightarrow W$ eine G-äquivariante Abbildung. Dann gilt für alle $v \in V$:

$$\varphi((\sum_{g\in G} \lambda_g g).v) = \varphi(\sum_{g\in G} \lambda_g \sigma_g(v)) \overset{\text{Hom.}}{=} \sum_{g\in G} \lambda_g \varphi(\sigma_g(v))$$
$$\overset{\text{Def.}}{=} \sum_{g\in G} \lambda_g \rho_g(\varphi(v)) = (\sum_{g\in G} \lambda_g g).\varphi(v)$$

Also ist φ ein $K[G]$-Modul-Homomorphismus.

Ist umgekehrt $\varphi : V \longrightarrow W$ ein $K[G]$-Modul-Homomorphismus. Dann gilt

$$\varphi(\sigma_g(v)) = \sigma(g.v) \overset{\text{Hom.}}{=} g.\varphi(v) = \rho_g(v) \text{ für alle } g \in G, v \in V.$$

Somit ist φ auch G-äquivariant.

Zu (b): Dies ist klar nach (a), da ein Modul-Homomorphismus genau dann ein Isomorphismus ist, wenn er bijektiv ist.

Die Aussagen (c)-(e) werden in den Übungen bearbeitet. □

KOROLLAR 6.1.11. *Seien σ und ρ irreduzible Darstellungen von G auf die K-Vektorräume V und W. Dann ist jede G-äquivariante Abbildung $\varphi : V \longrightarrow W$ entweder ein Isomorphismus oder die Nullabbildung.*

BEWEIS. Eine G-äquivariante Abbildung $\varphi : V \longrightarrow W$ ist nach Proposition 6.1.10 (a) ein $K[G]$-Modul-Homomorphismus der durch σ und ρ induzierten $K[G]$-Moduln V und W. Da σ und ρ irreduzibel sind, folgt mit Proposition 6.1.10 (d), dass V und W einfach sind. Nun folgt die Aussage aus dem Lemma von Schur 5.5.5. □

LEMMA 6.1.12. *Sei G eine endliche Gruppe und ρ eine irreduzible Darstellung von G auf einen K-Vektorraum V. Dann ist ρ endlich-dimensional.*

BEWEIS. Wir betrachten V als $K[G]$-Modul mit der durch ρ induzierten Skalarmultiplikation. Da ρ irreduzibel ist, ist V einfach. Sei nun $v \in V \setminus \{0\}$ beliebig, dann ist

$$T_v : K[G] \longrightarrow V \quad ; \quad \alpha \mapsto \alpha.v$$

ein $K[G]$-Modul-Homomorphismus. Da die $K[G]$-Skalarmultiplikation gerade eine Fortsetzung der K-Skalarmultiplikation auf V ist, ist T_v erst recht ein K-Vektorraum-Homomorphismus. Es ist $e.v = v \in T_v(K[G]) \setminus \{0\}$. Da V einfach ist, folgt somit $T_v(K[G]) = V$. Damit ist $\dim_K(V) \leq \dim_K(K[G]) = |G| < \infty$. □

Unter zwei weiteren Annahmen lässt sich dieses Lemma noch verschärfen.

LEMMA 6.1.13. *Sei K algebraisch abgeschlossen, G eine endliche abelsche Gruppe und ρ eine irreduzible Darstellung von G auf einen K-Vektorraum V. Dann ist ρ eindimensional.*

BEWEIS. Für $\lambda \in K$ sei wie immer ${}_\lambda T$ die Skalarmultiplikation mit λ. D.h.: ${}_\lambda T(v) = \lambda v$ für alle $v \in V$. Die K-Linearität von Abbildungen $\varphi \in \mathrm{End}_K(V)$ bedeutet nun nichts anderes als $\varphi \circ {}_\lambda T = {}_\lambda T \circ \varphi$. Insbesondere gilt dies für alle ρ_g, $g \in G$. Also ist ${}_\lambda T$ für alle $\lambda \in K$ eine G-äquivariante Abbildung.
Wir wollen als erstes zeigen, dass jede G-äquivariante Abbildung diese Form besitzt. Sei dazu $\varphi \in \mathrm{End}_K(V)$ G-äquivariant. Nach Lemma 6.1.12 ist V endlich-dimensional, somit besitzt φ ein charakteristisches Polynom. Die Nullstellen dieses Polynoms sind genau die Eigenwerte von φ. Da K algebraisch abgeschlossen ist, liegen also alle Eigenwerte von φ in K. Sei $\lambda \in K$ ein Eigenwert von φ und $v \neq 0$ ein Eigenvektor zu λ. Dann ist $({}_\lambda T - \varphi)(v) = 0$, also ist $({}_\lambda T - \varphi)$ nicht injektiv und insbesondere kein Isomorphismus.
Natürlich ist $({}_\lambda T - \varphi)$ als Summe von G-äquivarianten Abbildungen selbst G-äquivariant. Da ρ irreduzibel ist, folgt aus Korollar 6.1.11, dass $({}_\lambda T - \varphi)$ die Nullabbildung ist. Das bedeutet gerade ${}_\lambda T = \varphi$.
Insbesondere ist für jedes $g \in G$ die Abbildung ρ_g gleich ${}_\lambda T$ für ein $\lambda \in K$. Denn für alle $g, h \in G$ gilt

$$\rho_g \circ \rho_h = \rho_{gh} \overset{G \text{ abelsch}}{=} \rho_{hg} = \rho_h \circ \rho_g.$$

Somit ist ρ_g tatsächlich G-äquivariant. Sei nun W ein Unterraum von V. Dann gilt für alle $g \in G$

$$\rho_g(W) = {}_\lambda T(W) = \lambda W = W.$$

Also ist jeder Unterraum von V bereits G-invariant. Da ρ irreduzibel ist, ist dies nur möglich wenn V keine echten Unterräume besitzt. Also muss V, und somit ρ, eindimensional sein. □

BEMERKUNG 6.1.14. Sei $n \geq 3$ und ρ die natürliche irreduzible Darstellung der Diedergruppe D_n auf $\mathbb{R}^2$ aus den Übungen. Fassen wir $\mathbb{Z}/n\mathbb{Z}$ als Untergruppe von D_n auf so erhalten wir eine Darstellung $\rho|_{\mathbb{Z}/n\mathbb{Z}}$ von G auf $\mathbb{R}^2$. Genau wie in den Übungen sieht man, dass auch diese Darstellung irreduzibel ist. Also ist Lemma 6.1.13 falsch für nicht algebraisch abgeschlossene Körper!

THEOREM 6.1.15 (Satz von Maschke). *Sei G eine endliche Gruppe und* $\mathrm{char}(K) \nmid |G|$. *Dann ist $K[G]$ halbeinfach.*

BEWEIS. Wir wollen die Beschreibung aus Theorem 5.5.8 benutzen, dass ein Modul halbeinfach ist, genau dann wenn jeder Untermodul ein Komplementmodul besitzt.
Sei also $N \subseteq K[G]$ ein beliebiger $K[G]$-Untermodul. Dann ist N insbesondere ein Unterraum des K-Vektorraumes $K[G]$. Aus der linearen Algebra ist bekannt, dass ein Unterraum U von $K[G]$ mit $N \oplus U = K[G]$ existiert. Wir können nicht erwarten, dass dieses U auch ein Untermodul von $K[G]$ ist, aber wir erhalten eine K-lineare Projektion

$$\pi : K[G] \longrightarrow N \quad ; \quad \alpha = \underbrace{n}_{\in N} + \underbrace{u}_{\in U} \mapsto n.$$

Daraus basteln wir eine $K[G]$-lineare Abbildung mit folgendem Trick: Sei $\rho : G \longrightarrow GL_K(K[G])$ die reguläre Darstellung von G. Setze nun

$$\pi_G : K[G] \longrightarrow N \quad ; \quad \alpha \mapsto \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} \circ \underbrace{\pi \circ \rho_g(\alpha)}_{\in N}.$$

Hier fassen wir $|G| \in K$ auf indem wir $\mathbb{Z}$ mit dem Bild $\varphi(\mathbb{Z})$ des eindeutigen Ring-Homomorphismuses $\varphi : \mathbb{Z} \longrightarrow K$ identifizieren. Dann ist $|G|^{-1}$ definiert, da $\mathrm{char}(K) \nmid |G|$ gilt. Die Abbildung π_G ist wohldefiniert, da N ein $K[G]$-Modul ist. Weiter ist π_G, als Verknüpfung von K-linearen Abbildungen, selbst K-linear. Weiter gilt für beliebiges $h \in G$

$$\rho_h \circ \pi_G = \frac{1}{|G|} \sum_{g \in G} \rho_h \circ \rho_{g^{-1}} \circ \pi \circ \rho_g = \frac{1}{|G|} \sum_{\substack{g' = hg^{-1} \\ g \in G}} \rho_{g'} \circ \pi \circ \rho_{g'^{-1}h}$$

$$= \frac{1}{|G|} \sum_{g' \in G} \rho_{g'} \circ \pi \circ \rho_{g'^{-1}} \rho_h = \pi_G \circ \rho_g.$$

Wir haben also gezeigt, dass π_G ein G-äquivariante Abbildung ist. Aus Proposition 6.1.10 folgt, dass π_G auch $K[G]$-linear ist. Somit ist $\ker(\pi_G)$ ein Untermodul von $K[G]$.
Wir behaupten, dass $N \oplus \ker(\pi_G) = K[G]$ gilt. Dafür zeigen wir zunächst, dass der Schnitt von N und $\ker(\pi_G)$ trivial ist. Dies folgt unmittelbar, da für alle $n \in N$ gilt:

$$\pi_G(n) = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ \pi \circ \underbrace{\rho_g(n)}_{\in N} = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ \rho_g(n) = \frac{1}{|G|} \sum_{g \in G} n = n \tag{54}$$

Weiter ist für $\alpha \in K[G]$ beliebig $\pi_G(\alpha - \pi_G(\alpha)) = \pi_G(\alpha) - \pi_G(\pi_G(\alpha)) \overset{(54)}{=} 0$. Also ist $\alpha - \pi_G(\alpha) \in \ker(\pi_G)$, was gerade $K[G] = \ker(\pi_G) + N$ bedeutet.
Damit ist die Behauptung gezeigt, und $\ker(\pi_G)$ ist der gesuchte Komplementmodul von N. Da N beliebig war, folgt dass $K[G]$ halbeinfach ist. □

ABBILDUNG 6.1. Der deutsche Mathematiker *Heinrich Maschke* (1853-1908) arbeitete zunächst als Lehrer in Berlin und später als Arbeiter in einer Firma in New Jersey, bevor er 1896 Professor an der University of Chicago wurde. Ab 1907 war er Vizepräsident der American Mathematical Society.

KOROLLAR 6.1.16. *Sei G eine endliche Gruppe mit* $\mathrm{char}(K) \nmid |G|$*, dann ist jede Darstellung von G auf einen K-Vektorraum V vollreduzibel.*

BEWEIS. Eine Darstellung von G auf V ist nach Proposition 6.1.10 genau dann vollreduzibel, wenn V ein halbeinfacher $K[G]$-Modul ist. Wir haben gerade gesehen, dass unter unserer Voraussetzung an $\mathrm{char}(K)$ der Ring $K[G]$ halbeinfach ist. Somit ist nach Theorem 5.6.9 auch jeder $K[G]$-Modul halbeinfach. Damit folgt die Aussage sofort. □

BEMERKUNG 6.1.17. Unter der Voraussetzung $\mathrm{char}(K) \nmid |G| < \infty$ haben wir gesehen, dass alle Darstellungen von G vollreduzibel, also durch die irreduziblen Darstellungen bestimmt, sind. Die irreduziblen Darstellungen wiederum sind nach Proposition 6.1.10 bestimmt durch die einfachen $K[G]$-Moduln. Jeder einfache $K[G]$-Modul ist jedoch isomorph zu einem einfachen Linksideal von $K[G]$ (siehe Korollar 5.6.7). Somit sind alle Darstellungen von G in der Modulstruktur von $K[G]$, oder äquivalent in der regulären Darstellung von G, codiert!

PROPOSITION 6.1.18. *Sei G eine endliche Gruppe und K algebraisch abgeschlossen mit* $\mathrm{char}(K) \nmid |G|$*. Dann ist $K[G] \cong M_{n_1}(K) \times \ldots \times M_{n_r}(K)$ für gewisse $n_1, \ldots, n_r \in \mathbb{N}$, und es ist $|G| = n_1^2 + \ldots + n_r^2$.*

BEWEIS. Der Ring $K[G]$ ist nach dem Satz von Maschke halbeinfach. Mit dem Struktursatz von Wedderburn gilt also

$$K[G] \cong M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r) \tag{55}$$

für gewisse $n_1, \ldots, n_r \in N$ und Schiefkörper $D_1, \ldots, D_r$. Aus dem Beweis des Satzes von Artin-Wedderburn wissen wir, dass wir $D_i = \mathrm{End}_{R_i}(I_i)$ wählen können für einen einfachen Teilring R_i von $K[G]$ und ein einfaches Linksideal I_i von R_i. Aus Theorem 5.6.8 wissen wir sogar, dass R_i ein zweiseitiges Ideal in $K[G]$ ist. Insbesondere ist R_i also eine K-Algebra. Weiter ist $\dim_K(R_i) \leq \dim_K(K[G]) = |G| < \infty$. In den Übungen wird gezeigt, dass daraus bereits $D_i \cong K$, für alle $i \in \{1, \ldots, r\}$, folgt. Somit folgt aus (55) die erste Behauptung.

Weiter gilt damit

$$|G| = \dim_K(K[G]) = \dim_K(M_{n_1}(K) \times \ldots \times M_{n_r}(K))$$
$$= \sum_{i=1}^{r} \dim_K(M_{n_i}(K)) = \sum_{i=1}^{r} n_i^2.$$

Damit gilt auch die zweite Behauptung. □

6.2. Charaktere

Sei in diesem Abschnitt stets G eine endliche Gruppe und K ein Körper mit $\mathrm{char}(K) \nmid |G|$. Im letzten Abschnitt haben wir gesehen, dass unter diesen Voraussetzungen sämtliche Darstellungen von G in der Gruppenalgebra $K[G]$ stecken und, dass die „relevanten“ (die irreduziblen) Darstellungen endlichdimensional sind. Wir wollen diese Darstellungen von G durch noch einfachere Objekte klassifizieren.

Wiederholung. Die *Spur* Tr einer K-linearen Abbildung eines endlichdimensionalen K-Vektorraumes V ist die Summe der Diagonalelemente einer Darstellungsmatrix der Abbildung. Diese Definition ist unabhängig von der Basiswahl und damit wohldefiniert.

Definition 6.2.1. Sei $\rho : G \longrightarrow GL_K(V)$ eine Darstellung von G. Die Abbildung

$$\chi_\rho : G \longrightarrow K \quad ; \quad g \mapsto Tr(\rho_g)$$

heißt *Charakter* der Darstellung ρ.

Proposition 6.2.2. *Seien $\sigma : G \longrightarrow GL_K(V)$ und $\rho : G \longrightarrow GL_K(W)$ Darstellungen von G (nach globaler Voraussetzung sind sie endlichdimensional). Dann gilt*

(a) $\chi_\sigma(g) = \chi_\sigma(hgh^{-1})$ *für alle* $g, h \in G$.
(b) $\chi_{\sigma\oplus\rho} = \chi_\sigma + \chi_\rho$
(c) *Wenn σ und ρ äquivalent sind, ist* $\chi_\sigma = \chi_\rho$

Beweis. Wir erinnern daran, dass die Spuren von äquivalenten Matrizen $A, B \in M_n(K)$ (d.h.: es ist $A = C^{-1}BC$ für ein $C \in (M_n(K))^*$) gleich sind.

Zu (a): Für alle $g, h \in G$ gilt $\sigma_{hgh^{-1}} \overset{\text{Hom.}}{=} \sigma_h \circ \sigma_g \circ \sigma_{h^{-1}} \overset{\text{Hom.}}{=} \sigma_h \circ \sigma_g \circ \sigma_h^{-1}$. Also gilt auch wie gewünscht

$$\chi_\sigma(hgh^{-1}) = Tr(\sigma_{hgh^{-1}}) = Tr(\sigma_g) = \chi_\sigma(g) \ \forall g, h \in G.$$

Zu (b): Die direkte Summe $\sigma \oplus \rho$ ist die Darstellung von G auf $V \oplus W$ mit $g \mapsto (\sigma_g, \rho_g)$. Sei B eine K-Basis von V und B' eine K-Basis von W, und für alle $g \in G$ seine A_g und A'_g die Darstellungsmatrizen

von σ_g bezüglich B beziehungsweise von ρ_g bezüglich B'. Dann ist die Darstellungsmatrix von $(\sigma_g, \rho_g) = \sigma_g \oplus \rho_g$ bezüglich der Basis $\{(b,0)|b \in B\} \cup \{(0,b')|b' \in B'\}$ von $V \oplus W$ gegeben durch

$$\begin{pmatrix} A_g & 0 \\ 0 & A'_g \end{pmatrix}$$

Damit sieht man sofort $\chi_{\sigma\oplus\rho}(g) = Tr(A_g)+Tr(A'_g) = \chi_\sigma(g)+\chi_\rho(g)$ für alle $g \in G$.

Zu (c): Dass σ und ρ äquivalent sind heißt, dass es einen K-Vektorraum-Isomorphismus $\varphi : V \longrightarrow W$ gibt mit $\varphi \circ \sigma_g = \rho_g \circ \varphi$ für alle $g \in G$. Das bedeutet also $\sigma_g = \varphi^{-1} \circ \rho_g \circ \varphi$ für alle $g \in G$. Somit sind wie in (a) auch die Charaktere von σ und ρ gleich.

□

NOTATION 6.2.3. Sei $K[G]$ die Gruppenalgebra von G über K. Da $K[G]$ halbeinfach ist (Satz von Maschke), können wir die Theorie über halbeinfache Ringe anwenden und erhalten

$$K[G] = R_1 \times \ldots \times R_r$$

für einfache Ringe $R_1, \cdots, R_r$. Es ist sogar $R_i \cong M_{n_i}(D_i)$ für $n_i \in \mathbb{N}$ und einen Schiefkörper D_i. Die Einselemente der Ringe R_i nennen wir e_i, dann gilt

$$1 = e_1 + \ldots + e_r \text{ und } e_i e_j = e_j e_i = \begin{cases} e_i \text{ falls } i = j \\ 0 \text{ sonst} \end{cases}.$$

Aus Beispiel 5.6.11 wissen wir, dass es für jedes $i \in \{1, \ldots, r\}$ einfache $K[G]$-Linksideale $L_{i1}, \ldots, L_{in_i}$ gibt mit

$$R_i = L_{i1} \oplus \ldots \oplus L_{in_i}$$

und nach Theorem 5.6.8 gilt $L_{ik} \cong L_{jl}$ genau dann wenn $i = j$ ist. Weiter ist jeder einfache $K[G]$-Modul isomorph zu genau einem Linksideal aus $\{L_{11}, L_{21}, \ldots, L_{r1}\}$. Die $K[G]$-Linksideale L_{ik} sind insbesondere K-Vektorräume. Sei ρ_{ik} die assoziierte Darstellung von G auf L_{ik} aus Proposition 6.1.5 ($\rho_{ik}(g)(v) = g.v$). Aus Proposition 6.2.2 (c) folgt für die zugehörigen Charaktere $\chi_{ik} = \chi_{il}$ für alle $l, k \in \{1, \ldots, r\}$. Wir setzen $\chi_i = \chi_{i1}$ und nennen $\chi_1, \ldots, \chi_r$ die *elementaren Charaktere* von G über K. Den Charakter der regulären Darstellung von G nennen wir χ_{reg}.

LEMMA 6.2.4. *Mit den Bezeichnungen von oben gilt*

$$\chi_{\text{reg}}(g) = n_1\chi_1(g) + \ldots + n_r\chi_r(g) = \begin{cases} |G| \textit{ falls } g = e \\ 0 \textit{ sonst} \end{cases}.$$

BEWEIS. Da Darstellungen genau dann äquivalent sind wenn ihre zugehörigen Vektorräume isomorph als $K[G]$-Moduln sind, folgt die erste Gleichheit sofort aus Proposition 6.2.2 und

$$K[G] = \bigoplus_{i=1}^{r} R_i = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} L_{ij} \cong \bigoplus_{i=1}^{r} L_{i1}^{n_i}.$$

Kommen wir nun zur zweiten Gleichheit. Die Elemente aus G bilden per Konstruktion eine K-Basis von $K[G]$. Wir betrachten die Darstellungsmatrizen von $\rho_{\text{reg}}(g)$, $g \in G$, in dieser Basis. Natürlich ist dann $\rho_{\text{reg}}(e) = \text{id}$ die Einheitsmatrix. Also gilt $\chi_{\text{reg}}(e) = \dim_K(K[G]) = |G|$.
Die Abbildung $\rho_{\text{reg}}(g)$ bildet $h \in G$ auf gh ab. Also sind in der Darstellungsmatrix von $\rho_{\text{reg}}(g)$ die Einheitsvektoren permutiert. Für $g \neq e$ ist $gh \neq h$ für alle $h \in G$. Also kann der i-te Einheitsvektor nicht in der i-ten Spalte der Matrix stehen. Somit sind alle Diagonaleinträge gleich Null, insbesondere also $\chi_{\text{reg}}(g) = 0$. □

BEMERKUNG 6.2.5. Sei $\rho : G \longrightarrow GL_K(V)$ eine Darstellung von G mit Charakter χ. Diese induziert durch $\alpha.v = (\sum_{g\in G} \lambda_g g).v = \sum_{g\in G} \lambda_g \rho_g(v)$ eine $K[G]$-Modulstruktur auf V und $\chi(g)$ ist gegeben als Spur der K-linearen Abbildung ${}_gT : V \longrightarrow V$ mit $v \mapsto g.v$. Diese Abbildungen ${}_\alpha T$ sind jedoch K-linear für alle $\alpha \in K[G]$. Auf diese Weise können wir χ eindeutig K-linear auf ganz $K[G]$ fortsetzen durch $\chi(\alpha) = Tr({}_\alpha T)$.

PROPOSITION 6.2.6. *Sei* $\text{char}(K) = 0$*, dann sind zwei Darstellungen der Gruppe G äquivalent, genau dann wenn ihre Charaktere gleich sind.*

BEWEIS. Dass äquivalente Darstellungen dieselben Charaktere haben, haben wir bereits gezeigt (Proposition 6.2.2). Es bleibt also die Rückrichtung zu beweisen.
Sei ρ eine Darstellung von G auf V mit Charakter χ. Wieder wird V damit zu einem $K[G]$-Modul. Da $K[G]$ halbeinfach ist, ist nach Proposition 5.6.10 auch V halbeinfach. Nun wissen wir, dass alle einfachen $K[G]$-Moduln isomorph zu einem der Linksideale $L_{11}, \ldots, L_{r1}$ sind. Damit ist

$$V \cong L_{11}^{m_1} \oplus \ldots \oplus L_{r1}^{m_r}$$

für gewisse $m_1, \ldots, m_r \in \mathbb{N}_0$ (beachte, dass V nach Voraussetzung endlichdimensional ist). Mit Proposition 6.2.2 (c) ist der Charakter der Darstellung, die durch $L_{11}^{m_1} \oplus \ldots \oplus L_{r1}^{m_r}$ induziert ist, ebenfalls gleich χ. Genau wie in Lemma 6.2.4 gilt somit $\chi(g) = \sum_{i=1}^{r} m_i \chi_i(g)$ für alle $g \in G$.
Betrachten wir nun die Fortsetzungen von $\chi, \chi_1, \ldots, \chi_r$ auf $K[G]$, so gilt aufgrund der K-Linearität und der Tatsache, dass G eine Basis von $K[G]$

ist sogar

$$\chi(\alpha) = m_1\chi_1(\alpha) + \ldots + m_r\chi_r(\alpha) \text{ für alle } \alpha \in K[G]. \tag{56}$$

Für die Einselemente e_i der Ringe R_i ist die Linksmultiplikation ${}_{e_i}T$ eingeschränkt auf L_{j1} die Identität falls $i = j$ oder die Nullabbildung sonst. Es folgt

$$\begin{aligned}\chi(e_j) \overset{(56)}{=} \sum_{i=1}^{r} m_i\chi_i(e_j) &\overset{\text{Def.}}{=} \sum_{i=1}^{r} m_i Tr({}_{e_j}T|_{L_{i1}}) \\ &= m_j Tr({}_{e_j}T|_{L_{j1}}) = m_j \dim_K(L_{j1}).\end{aligned}$$

Dies ist eine Gleichung im Körper K, und da $\text{char}(K) = 0$ vorausgesetzt wurde, gilt

$$m_j = \frac{\chi(e_j)}{\dim_K(L_{j1})} \text{ für alle } j \in \{1, \ldots, r\}.$$

Ist nun ρ' irgendeine Darstellung von G auf V' ebenfalls mit Charakter χ, so ist wieder

$$V' \cong L_{11}^{m'_1} \oplus \ldots \oplus L_{r1}^{m'_r}$$

und genau wie eben sehen wir

$$m'_j = \frac{\chi(e_j)}{\dim_K(L_{j1})} = m_j \text{ für alle } j \in \{1, \ldots, r\}.$$

Somit sind V und V' isomorph als $K[G]$-Moduln, was gerade bedeutet, dass ρ und ρ' äquivalent sind. □

KOROLLAR 6.2.7. *Sei wieder* $\text{char}(K) = 0$*, und mit* $\chi_1, \ldots, \chi_r$ *bezeichnen wir die elementaren Charaktere der Gruppe* G*. Dann ist jeder Charakter einer irreduziblen Darstellung von* G *gleich* χ_i *für genau ein* $i \in \{1, \ldots, r\}$*.*

BEWEIS. Dies folgt aus der soeben bewiesenen Proposition, da irreduzible Darstellungen durch einfache $K[G]$-Moduln bis auf Äquivalenz durch eine Darstellung ρ_{ik} zu einem einfachen Linksideal L_{ik} gegeben ist (vergleiche 6.2.3). □

6.3. Skalarprodukte von Charakteren

Wir haben Darstellungen einer endlichen Gruppe studiert. Dabei haben sich Charaktere von irreduziblen Darstellungen als Klassifikation von Darstellungen angeboten. Dies wollen wir weiter spezialisieren. An manchen Stellen mussten wir Einschränkungen an den Körper K stellen ($\text{char}(K) = 0$, K algebraisch abgeschlossen). Für den konkreten Fall $K = \mathbb{C}$ erhalten wir ein weiters Hilfsmittel für das Studium von Charakteren - nämlich Skalarprodukte.

Sei jetzt also $K = \mathbb{C}$, G eine endliche Gruppe und jede Darstellung sei endlichdimensional. Wir sprechen hierfür kurz von komplexen Darstellungen von G.

DEFINITION 6.3.1. Sei V ein komplexer endlichdimensionaler Vektorraum mit einem (hermiteschen) Skalarprodukt $\langle .,. \rangle$, und sei ρ eine Darstellung von G auf V. Dann heißt ρ *unitär* bezüglich $\langle .,. \rangle$, genau dann wenn $\langle v, w \rangle = \langle \rho_g(v), \rho_g(w) \rangle$ für alle $g \in G$ und alle $v, w \in V$ gilt.

SATZ 6.3.2. *Sei $(.,.)$ ein beliebiges Skalarprodukt auf dem $\mathbb{C}$-Vektorraum V, und sei ρ eine Darstellung von G auf V. Setze*

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho_g(v), \rho_g(w)) \text{ für alle } v, w \in V.$$

Dann ist $\langle .,. \rangle$ ein Skalarprodukt auf V und ρ ist unitär bezüglich $\langle .,. \rangle$.

BEWEIS. Dass $\langle .,. \rangle$ ein Skalarprodukt ist, folgt sofort aus der Tatsache, dass ρ_g ein Homomorphismus und $(.,.)$ ein Skalarprodukt ist. Es ist unitär, da für jedes $h \in G$ die Zuordnung $g \mapsto gh$ eine Bijektion auf G ist. □

KOROLLAR 6.3.3. *Sei ρ eine Darstellung von G auf V mit Charakter χ. Dann ist $\chi(g^{-1}) = \overline{\chi(g)}$ für alle $g \in G$. Hier bezeichnet $\bar{\cdot}$ komplexe Konjugation.*

BEWEIS. Sei ρ unitär bezüglich des Skalarproduktes $\langle .,. \rangle$ (dies existiert nach Satz 6.3.2). Es existiert bekanntlich eine Orthonormalbasis von V bezüglich $\langle .,. \rangle$. Weiter ist aus der linearen Algebra bekannt, dass mit der linearen Abbildung ρ_g auch die zugehörige Darstellungsmatrix A_g bezüglich dieser Orthonormalbasis unitär ist. Also gilt $A_g^{-1} = \overline{A_g}^t$ für alle $g \in G$, wobei B^t die transponierte Matrix zu einer Matrix B beschreibt. Es folgt

$$\chi(g^{-1}) = Tr(A_{g^{-1}}) = Tr(A_g^{-1}) = Tr(\overline{A_g}^t) = \overline{Tr(A_g)} = \overline{\chi(g)}$$

und somit das Korollar. □

NOTATION 6.3.4. Wie immer benutzen wir folgende Bezeichnungen:

- $\mathbb{C}[G] = R_1 \times \ldots \times R_r$ für einfache Ringe $R_1, \ldots, R_r$
- $R_i \cong M_{n_i}(\mathbb{C})$ für gewisse $n_i \in \mathbb{N}$
- $|G| = n_1^2 + \ldots n_r^2$
- e_i ist das Einselement in R_i und $e_i R_j = \begin{cases} R_i \text{ falls i=j} \\ 0 \text{ sonst} \end{cases}$
- $R_i = L_{i1} \oplus \ldots \oplus L_{in_i}$ für einfache Linksideale L_{ij}
- $L_{ij} \cong L_{kl} \iff i = k$
- $\dim_{\mathbb{C}}(L_{ij}) = n_i$

- $\chi_1, \ldots, \chi_r$ sind die elementaren Charaktere von G (d.h.: χ_i ist der irreduzible Charakter der von L_{i1} induziert wird)
- $\chi_{\text{reg}} = n_1\chi_1 + \ldots + n_r\chi_r$ ist der reguläre Charakter von G
- Jeder Charakter χ lässt sich eindeutig $\mathbb{C}$-linear auf $\mathbb{C}[G]$ fortsetzen. Diese Abbildung nennen wir wieder χ.

Dies wurde alles in Proposition 6.1.18, Theorem 5.6.8, Theorem 5.6.9, Korollar 6.2.4 und Bemerkung 6.2.5 gezeigt.

NOTATION 6.3.5. Die Menge $\mathbb{C}^G = \{f : G \longrightarrow \mathbb{C} | f \text{ Abbildung}\}$ ist bezüglich

$$(f_1 + f_2)(g) = f_1(g) + f_2(g) \text{ und } (\lambda f_1)(g) = \lambda f_1(g)$$

für alle $f_1, f_2 \in \mathbb{C}^G$, alle $\lambda \in K$ und alle $g \in G$ ein $\mathbb{C}$-Vektorraum. Eine Basis von $\mathbb{C}^G$ ist offensichtlich gegeben durch die Elemente δ_g, $g \in G$, mit

$$\delta_g(h) = \begin{cases} 1 \text{ falls } g = h \\ 0 \text{ sonst} \end{cases} .$$

Insbesondere gilt $\mathbb{C}^G \cong \mathbb{C}^{|G|} \cong \mathbb{C}[G]$ als $\mathbb{C}$-Vektorräume. Die Teilmenge

$$\Gamma(G, \mathbb{C}) = \{f \in \mathbb{C}^G | f(ghg^{-1}) = f(h) \text{ für alle} g, h \in G\}$$

ist ein Unterraum von $\mathbb{C}^G$ und heißt Raum der *Klassenfunktionen* von G. Der Name erklärt sich dadurch, dass in $\Gamma(G, \mathbb{C})$ genau die Funktionen liegen, die konstant auf den Konjugationsklassen von G sind. Auf $\mathbb{C}^G$ und $\Gamma(G, \mathbb{C})$ haben wir das hermitesche Skalarprodukt $\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}$.

SATZ 6.3.6. *Der Raum der Klassenfunktionen $\Gamma(G, \mathbb{C})$ und das Zentrum $Z(\mathbb{C}[G])$ von $\mathbb{C}[G]$ sind isomorph als $\mathbb{C}$-Vektorräume. Wir erinnern daran, dass $Z(\mathbb{C}[G]) = \{\alpha \in \mathbb{C}[G] | \alpha\beta = \beta\alpha$ für alle $\beta \in \mathbb{C}[G]\}$ ist.*

BEWEIS. Übung. □

PROPOSITION 6.3.7. *Die Einselemente $e_1, \ldots, e_r$ liegen in $Z(\mathbb{C}[G])$ und in der Basisdarstellung $e_i = \sum_{g \in G} \lambda_g g$ sind die Koeffizienten gegeben durch $\lambda_g = \frac{n_i}{|G|}\chi_i(g^{-1})$.*

BEWEIS. Für $\alpha \in \mathbb{C}[G]$ beliebig, existiert eine eindeutige Darstellung $\alpha = \sum_{j=1}^{r} \lambda_j$, mit $\lambda_j \in R_j$ für alle $j \in \{1, \ldots, r\}$. Wir erhalten

$$e_i\alpha = \sum_{j=1}^{r} e_i\lambda_j = \lambda_i = \sum_{j=1}^{r} \lambda_j e_i = \alpha e_i.$$

Damit ist e_i tatsächlich im Zentrum von $\mathbb{C}[G]$ für alle $i \in \{1, \ldots, r\}$. Insbesondere ist damit für jedes $\alpha \in \mathbb{C}[G]$ die Abbildung

$${}_\alpha T|_{L_{i1}} \longrightarrow L_{i1} \quad ; \quad \beta \mapsto \alpha\beta$$

gleich ${}_{e_i\alpha}T|_{L_{i1}}$. Daraus folgt

$$\chi_i(\alpha) = Tr({}_{\alpha}T|_{L_{i1}}) = Tr({}_{e_i\alpha}T|_{L_{i1}}) = \chi_i(e_i\alpha). \tag{57}$$

Mit dieser Gleichung erhalten wir

(58)

$$\chi_{\text{reg}}(e_ig^{-1}) = \sum_{j=1}^{r} n_j\chi_j(e_ig^{-1}) \overset{(57)}{=} \sum_{j=1}^{r} n_j\chi_j(\underbrace{e_je_i}_{=0 \text{ für } i\neq j} g^{-1}) = n_i\chi_i(e_ig^{-1}).$$

Andererseits gilt mit Korollar 6.2.4

(59)

$$\chi_{\text{reg}}(e_ig^{-1}) = \chi_{\text{reg}}(\sum_{h\in G} \lambda_h hg^{-1}) = \sum_{h\in G} \lambda_h\chi_{\text{reg}}(hg^{-1}) = \lambda_g\chi_{\text{reg}}(e) = \lambda_g|G|.$$

Setzen wir die Gleichungen (58) und (59) gleich und benutzen (57) so erhalten wir wie gewünscht $\lambda_g = \frac{n_i}{|G|}\chi_i(g^{-1})$. □

PROPOSITION 6.3.8. *Seien χ und χ' Charaktere von irreduziblen komplexen Darstellungen ρ und ρ' von G, dann gilt*

$$\langle\chi,\chi'\rangle = \begin{cases} 1 \textit{ falls } \rho \textit{ und } \rho' \textit{ äquivalent sind} \\ 0 \textit{ sonst} \end{cases}$$

BEWEIS. Nach Korrollar 6.2.7 gilt $\chi = \chi_i$ und $\chi' = \chi_j$ für gewisse $i, j \in \{1,\dots,r\}$. Genau wie gerade im Beweis von Proposition 6.3.7 sehen wir

$$\chi_i(e_j) = \chi_i(e_ie_j) = \begin{cases} Tr(\text{id}\,|_{L_{i1}}) \\ Tr(0|_{L_{i1}}) \end{cases} = \begin{cases} \dim_K(L_{i1}) = n_i \text{ falls } i = j \\ 0 \text{ falls } i \neq j \end{cases}.$$

Weiter gilt

$$\chi_i(e_j) \overset{6.3.7}{=} \chi_i(\sum_{g\in G} \frac{n_j}{|G|}\chi_j(g^{-1})g) \overset{K\text{-lin.}}{=} \sum_{g\in G} \frac{n_j}{|G|}\chi_j(g^{-1})\chi_i(g) \overset{6.3.3}{=} n_j\langle\chi_j,\chi_i\rangle.$$

Fügen wir diese beiden Gleichungen zusammen so erhalten wir

$$\langle\chi,\chi'\rangle = \langle\chi_i,\chi_j\rangle = \begin{cases} 1 \text{ falls } i = j \\ 0 \text{ falls } i \neq j \end{cases}.$$

Da mit Proposition 6.2.6 genau dann $i = j$ gilt, wenn die Darstellungen ρ, ρ' äquivalent sind, folgt sofort die Behauptung. □

THEOREM 6.3.9. *Die elementaren Charaktere $\chi_1,\dots,\chi_r$ von G bilden eine Orthonormalbasis von $\Gamma(G,\mathbb{C})$ bezüglich $\langle .,. \rangle$. Insbesondere ist r gleich der Anzahl verschiedener Konjugationsklassen von G.*

BEWEIS. In Proposition 6.2.2 haben wir gesehen, dass $\chi_1, \ldots, \chi_r$ tatsächlich Klassenfunktionen sind. Die Orthonormalitätseigenschaft haben wir bereits in Proposition 6.3.8 gesehen. Damit folgt auch unmittelbar die $\mathbb{C}$-lineare Unabhängigkeit von $\chi_1, \ldots, \chi_r$. Es bleibt zu zeigen, dass die elementaren Charaktere auch ganz $\Gamma(G, \mathbb{C})$ erzeugen, beziehungsweise dass die Dimension von $\Gamma(G, \mathbb{C})$ gleich r ist.
Nach Satz 6.3.6 ist $\Gamma(G, \mathbb{C})$ isomorph zu $Z(\mathbb{C}[G])$. Für dieses Zentrum gilt
(60)
$$Z(\mathbb{C}[G]) \cong Z(\underbrace{M_{n_1}(\mathbb{C})}_{R_1} \times \ldots \times \underbrace{M_{n_r}(\mathbb{C})}_{R_r}) = Z(M_{n_1}(\mathbb{C})) \times \ldots \times Z(M_{n_r}(\mathbb{C})).$$

Wir behaupten, dass für jedes $n \in N$ die Gleichung $Z(M_n(\mathbb{C})) = \{\lambda E_n | \lambda \in \mathbb{C}\}$ gilt. Offensichtlich ist jedes Element der rechten Seite auch im Zentrum. Die andere Inklusion sehen wir durch einfaches Rechnen: Sei dazu $A \in Z(M_n(\mathbb{C}))$ beliebig, und seien $E_{ij} = (e_{kl})_{1 \leq k,l \leq n}$ die Matrizen mit $e_{ij} = 1$ und $e_{kl} = 0$ für $(k, l) \neq (i, j)$ aus 5.6.11. Dann folgt aus der Bedingung $E_{ij}A = AE_{ij}$ für alle $i, j \in \{1, \ldots, n\}$ sofort, dass A eine Diagonalmatrix ist. Weiter ist für A das Vertauschen der $i$ten und der $j$ten Spalte dasselbe wie Vertauschen der $i$ten und $j$ten Zeile. Damit sind auch alle Diagonalelemente von A identisch. Damit ist die Behauptung gezeigt.
Insbesondere gilt somit $\dim_{\mathbb{C}}(Z(M_{n_i}(\mathbb{C})) = 1$ für alle $i \in \{1, \ldots, r\}$. Damit erhalten wir

$$\dim_{\mathbb{C}}(\Gamma(G, \mathbb{C})) = \dim_{\mathbb{C}}(Z(\mathbb{C}[G])) \overset{(60)}{=} \sum_{i=1}^{r} \dim_{\mathbb{C}}(Z(M_{n_i}(\mathbb{C}))) = r.$$

Aus unseren Vorüberlegungen folgt, dass $\chi_1, \ldots, \chi_r$ eine Basis von $\Gamma(G, \mathbb{C})$ bilden. Da $\dim_{\mathbb{C}}(\Gamma(G, \mathbb{C}))$ auch gleich der Anzahl von verschiedenen Konjugationsklassen ist, ist das Theorem bewiesen. □

DEFINITION 6.3.10. Sei ρ eine beliebige komplexe Darstellung von G mit Charakter χ, dann heißt $\langle \chi, \chi_i \rangle$ der *i-te Fourierkoeffizient von χ*.

PROPOSITION 6.3.11. *Seien $\rho_1, \ldots, \rho_r$ komplexe Darstellungen von G deren Charaktere gerade die elementaren Charaktere $\chi_1, \ldots, \chi_r$ sind. Weiter sei ρ eine komplexe Darstellung mit Charakter χ. Dann sind die Fourierkoeffizienten $\langle \chi, \chi_1 \rangle$ in $\mathbb{N}_0$ und ρ ist äquivalent zu*

$$\underbrace{(\rho_1 \oplus \ldots \oplus \rho_1)}_{\langle \chi, \chi_1 \rangle\text{-mal}} \oplus \ldots \oplus \underbrace{(\rho_r \oplus \ldots \oplus \rho_r)}_{\langle \chi, \chi_r \rangle\text{-mal}}.$$

BEWEIS. Nach dem Satz von Maschke 6.1.15 ist ρ vollreduzibel und nach 6.2.6 und 6.2.7 ist jede irreduzible Darstellung von G äquivalent zu genau

einer Darstellung $\rho_1, \ldots, \rho_r$. Also ist ρ äquivalent zu

$$\underbrace{(\rho_1 \oplus \ldots \oplus \rho_1)}_{m_1\text{-mal}} \oplus \ldots \oplus \underbrace{(\rho_r \oplus \ldots \oplus \rho_r)}_{m_r\text{-mal}}$$

für gewisse $m_1, \ldots, m_r \in \mathbb{N}_0$. Da äquivalente Darstellungen denselben Charakter haben (siehe 6.2.2 (c)), folgt aus Proposition 6.2.2 (c)

$$\chi = m_1\chi_1 + \ldots + m_r\chi_r.$$

Nun ist aber $\chi_1, \ldots, \chi_r$ eine Orthonormalbasis von $\Gamma(G, \mathbb{C})$ und $\chi \in \Gamma(G, \mathbb{C})$. Somit gilt auch $\chi = \sum_{i=1}^{r} \langle \chi, \chi_i \rangle \chi_i$. Koeffizientenvergleich liefert nun die gewünschte Aussage. □

Durch Berechnen der Fourierkoeffizienten eines Charakters erhalten wir also die Zerlegung der zugehörigen Darstellung in irreduzible Darstellungen!

PROPOSITION 6.3.12. *Eine komplexe Darstellung ρ von G mit Charakter χ ist genau dann irreduzibel wenn $\langle \chi, \chi \rangle = 1$ gilt.*

BEWEIS. Es gilt

$$\begin{aligned}
\langle \chi, \chi \rangle &= \langle \sum_{i=1}^{r} \langle \chi, \chi_i \rangle \chi_i, \sum_{j=1}^{r} \langle \chi, \chi_j \rangle \chi_j \rangle \\
&= \sum_{i=1}^{r} \langle \chi, \chi_i \rangle \langle \chi_i, \sum_{j=1}^{r} \langle \chi, \chi_j \rangle \chi_j \rangle \\
&= \sum_{i=1}^{r} \sum_{j=1}^{r} \langle \chi, \chi_i \rangle \overline{\langle \chi, \chi_j \rangle} \langle \chi_i, \chi_j \rangle \qquad = \sum_{i=1}^{r} \langle \chi, \chi_i \rangle^2
\end{aligned}$$

Somit ist $\langle \chi, \chi \rangle = 1$ genau dann wenn $\langle \chi, \chi_i \rangle = 1$ für ein $i \in \{1, \ldots, r\}$ und $= 0$ für alle anderen. Dies ist genau dann erfüllt wenn $\chi = \chi_i$ ist, was wiederum genau dann der Fall ist wenn ρ irreduzibel ist. □

LEMMA 6.3.13. *Sei ρ eine komplexe Darstellung von G auf V mit Charakter χ. Dann ist $\chi(g)$ ganz über $\mathbb{Z}$ für alle $g \in G$.*

BEWEIS. Sei also $g \in G$ beliebig. Wir betrachten die zyklische Untergruppe $C = \langle g \rangle$ von G. Schränken wir nun ρ auf C ein, so erhalten wir eine Darstellung von C auf V. Diese hat den Charakter $\chi|_C$. Wir dürfen also oBdA annehmen, dass G zyklisch ist. Seien $\chi_1, \ldots, \chi_r$ die elementaren Charaktere von G. Da G abelsch ist, folgt aus Lemma 6.1.12 dass die Darstellungen assoziiert zu χ_i eindimensional sind. Also ist $\chi_i : G \longrightarrow \mathbb{C}^*$ ein Gruppen-Homomorphismus. Also gilt

$$\chi_i(g)^{|G|} = \chi_i(g^{|G|}) \overset{\text{Fermat}}{=} \chi_i(e) = 1.$$

Das Element $\chi_i(g)$ ist also eine $|G|$-te Einheitswurzel und somit ganz über $\mathbb{Z}$. Mit Proposition 6.3.11 erhalten wir $\chi(g) = \sum_{i=1}^{r} m_i\chi_i(g)$ für gewisse $m_1, \ldots, m_r \in \mathbb{N}_0$. Da Summe und Produkte von ganzen Elementen (dies folgt aus der Charakterisierung in Satz 5.2.14), wieder ganz sind ist auch $\chi(g)$ ganz über $\mathbb{Z}$. □

THEOREM 6.3.14. *Sei ρ eine irreduzible komplexe Darstellung von G auf V. Dann ist $\dim_{\mathbb{C}}(V)$ ein Teiler von $|G|$. Mit den üblichen Bezeichnungen bedeutet dies $n_i \mid |G|$ für alle $i \in \{1, \ldots, r\}$.*

BEWEIS. Die Idee des Beweises ist es, zu zeigen dass $|G|/\dim_{\mathbb{C}}(V) \in \mathbb{Q}$ ganz über $\mathbb{Z}$ ist. Denn dann folgt aus dem Gauß-Lemma 2.8.6 bereits $|G|/\dim_{\mathbb{C}}(V) \in \mathbb{Z}$, was zu zeigen ist.
Sei $\Gamma(G, \mathbb{C})_{\mathbb{Z}}$ die Menge aller Klassenfunktionen mit ganzzahligen Werten. Dies ist natürlich eine Untergruppe von $\Gamma(G, \mathbb{C})$. Wir haben einen $\mathbb{C}$-Vektorraum-Isomorphismus von $\Gamma(G, \mathbb{C})$ nach $Z(\mathbb{C}[G])$ durch die Abbildung $f \mapsto \sum_{g\in G} f(g)g$. Schränken wir diesen Isomorphismus auf $\Gamma(G, \mathbb{C})_{\mathbb{Z}}$ ein, so erhalten wir einen $\mathbb{Z}$-Modul-Isomorphismus

$$\varphi : \Gamma(G, \mathbb{C})_{\mathbb{Z}} \longrightarrow Z(\mathbb{C}[G])_{\mathbb{Z}} = \{\alpha \in Z(\mathbb{C}[G]) | \alpha = \sum_{g\in G} \lambda_g g, \lambda_g \in \mathbb{Z}\ \forall g \in G\}.$$

Wie immer ist für beliebiges $f \in \Gamma(G, \mathbb{C})$ die Abbildung

$$_{\varphi(f)}T : V \longrightarrow V \quad ; \quad v \mapsto \varphi(f).v = \sum_{g\in G} f(g)\rho_g(v)$$

ein $\mathbb{Z}$-Modul-Homomorphismus und es gilt für alle $\alpha \in \mathbb{C}[G]$

$$_{\varphi(f)}T(\alpha.v) = \varphi(f)(\alpha.v) = (\varphi(f)\alpha).v) \overset{\varphi(f)\in Z(\mathbb{C}[G])}{=} \alpha(\varphi(f).v) = \alpha(_{\varphi(f)}T(v))$$

Das bedeutet gerade, dass $_{\varphi(f)}T$ ein $\mathbb{C}[G]$-Modul-Homomorphismus ist. Die Darstellung ρ ist irreduzibel und daher existiert genau wie im Beweis von Lemma 6.1.13 ein $\lambda_f \in \mathbb{C}$ mit $_{\varphi(f)}T = {}_{\lambda_f}T$. Diese Eigenschaft zeigt sofort, dass dieses λ_f eindeutig ist.

Behauptung: Die Abbildung

$$\psi : Z(\mathbb{C}[G])_{\mathbb{Z}} \longrightarrow \mathbb{C} \quad ; \quad \sum_{g\in G} \lambda_g g = \varphi(f) \mapsto \lambda_f$$

ist ein wohldefinierter Ring-Homomorphismus.

Die Wohldefiniertheit haben wir bereits eingesehen. Weiter ist $_1T = {}_{1_e}T$, was gerade $\psi(1) = 1$ bedeutet. Wir prüfen nun die Additivität und Multiplikativität von ψ nach. Seien dafür $f_1, f_2 \in \Gamma(G, \mathbb{C})_{\mathbb{Z}}$ beliebig und sei $\varphi(f_1)\varphi(f_2) = \varphi(f)$. Dann gilt für alle $v \in V$:

$$\lambda_{f_1+f_2}T(v) = \lambda_{f_1+f_2}.v = \varphi(f_1+f_2).v = \varphi(f_1).v+\varphi(f_2).v = {}_{\lambda_{f_1}}T(v)+{}_{\lambda_{f_2}}T(v)$$

$$\lambda_f T(v) = {}_{\varphi(f)}T(v) = \varphi(f).v = \varphi(f_1)\varphi(f_2).v = {}_{\lambda_{f_1}}T({}_{\lambda_{f_2}}T(v)) = \lambda_{f_1}\lambda_{f_2}.v$$

Dies beweist die Behauptung.

Der $\mathbb{Z}$-Modul $Z(\mathbb{C}[G])_{\mathbb{Z}}$ ist ein Untermodul des endlich erzeugten $\mathbb{Z}$-Moduls $\bigoplus_{g\in G}\mathbb{Z}.g$. Da $\mathbb{Z}$ als Hauptidealbereich noethersch ist, ist $Z(\mathbb{C}[G])_{\mathbb{Z}}$ auch selbst endlich erzeugt (siehe Propositionen 5.3.7 + 5.3.5). Somit ist auch der Ring $\psi(Z(\mathbb{C}[G])_{\mathbb{Z}})$ als $\mathbb{Z}$-Modul endlich erzeugt. Mit Proposition 5.2.14 folgt, dass jedes Element aus $\psi(Z(\mathbb{C}[G])_{\mathbb{Z}})$ ganz über $\mathbb{Z}$ ist.
Seien $K_1,\dots,K_r \subseteq G$ die verschiedenen Konjugationsklassen von G und seien $g_i \in K_i$, $i \in \{1,\dots,r\}$, beliebige Repräsentanten dieser Klassen. Die Funktionen

$$\delta_{K_i}(h) = \begin{cases} 1 \text{ falls } h \in K_i \\ 0 \text{ sonst} \end{cases}$$

sind offensichtlich in $\Gamma(G,\mathbb{C})_{\mathbb{Z}}$ für alle $\{1,\dots,r\}$. Insbesondere gilt also

(61) die Elemente $\lambda_i := \psi(\varphi(\delta_{K_i}))$ sind ganz über $\mathbb{Z}$.

Kommen wir nun zum Schluss des Beweises:

$$\begin{aligned} |G| &\overset{6.3.12}{=} |G|\langle\chi,\chi\rangle = \sum_{g\in G}\overline{\chi(g)}\chi(g) \\ &\overset{6.2.2}{=} \sum_{i=1}^{r}\overline{\chi(g_i)}\sum_{g\in G}\delta_{K_i}(g)\chi(g) \overset{6.3.3}{=} \sum_{i=1}^{r}\chi(g_i^{-1})Tr({}_{\psi(\delta_{K_i})}T) \\ &= \sum_{i=1}^{r}\chi(g_i^{-1})Tr({}_{\lambda_i}T) = \sum_{i=1}^{r}\chi(g_i^{-1})\lambda_i \dim_{\mathbb{C}}(V) \end{aligned}$$

Teilen wir diese Gleichung durch $\dim_{\mathbb{C}}(V)$ so erhalten wir

$$\frac{|G|}{\dim_{\mathbb{C}}(V)} = \sum_{i=1}^{r}\chi(g_i^{-1})\lambda_i.$$

Nach Lemma 6.3.13 ist $\chi(g_i^{-1})$ ganz über $\mathbb{Z}$ und nach (61) ist auch λ_i ganz über $\mathbb{Z}$ für alle $i \in \{1,\dots,r\}$. Also ist auch $\frac{|G|}{\dim_{\mathbb{C}}(V)} = \sum_{i=1}^{r}\chi(g_i^{-1})\lambda_i$ ganz über $\mathbb{Z}$. Wie zu Beginn des Beweises argumentiert folgt daraus, dass $\dim_{\mathbb{C}}(V)$ ein Teiler von $|G|$ ist. □

LEMMA 6.3.15. *Seien ρ_1,ρ_2 komplexe Darstellungen der Gruppe G auf die $\mathbb{C}$-Vektorräume V beziehungsweise W. Dann gibt es eine Darstellung ρ von G auf $V\otimes W$ mit $\chi_\rho(g) = \chi_{\rho_1}(g)\cdot\chi_{\rho_2}(g)$ für alle $g \in G$.*

BEWEIS. Dies folgt aus der Übungsaufgabe 40. Dort wurde eine Darstellung $\rho_1 \otimes \rho_2$ von $G \times G$ auf $V \otimes W$ konstruiert mit $\chi_{\rho_1 \otimes \rho_2}((g_1, g_2)) = \chi_{\rho_1}(g_1) \cdot \chi_{\rho_2}(g_2)$ für alle $(g_1, g_2) \in G \times G$. Schränken wir die Darstellung $\rho_1 \otimes \rho_2$ auf die diagonale Untergruppe $\{(g, g) | g \in G\}$ von $G \times G$, die offensichtlich isomorph ist zu G, ein so erhalten wir das gewünschte Resultat. □

6.4. Die Charaktertafel

Sei wieder G eine endliche Gruppe. Wir wollen für G alle elementaren Charaktere $\chi_1, \ldots, \chi_r$ der komplexen irreduziblen Darstellungen von G bestimmen. Wir wissen nach Theorem 6.3.9, dass r gleich der Anzahl der verschiedenen Konjugationsklassen von G ist. Seien $[e] = [g_1], [g_2], \ldots, [g_r]$ die verschiedenen Konjugationsklassen von G. Dann beschreiben wir $\chi_1, \ldots, \chi_r$ durch eine Tabelle der Form

G	$[g_1]$	$[g_2]$	$\cdots$	$[g_r]$
χ_1	$\chi_1(g_1)$	$\chi_1(g_2)$	$\cdots$	$\chi_1(g_r)$
χ_2	$\chi_2(g_1)$	$\chi_2(g_2)$	$\cdots$	$\chi_2(g_r)$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
χ_r	$\chi_r(g_1)$	$\chi_r(g_2)$	$\cdots$	$\chi_r(g_r)$

Diese Tabelle heißt *Charaktertafel* der Gruppe G. Wir stellen fest, dass es immer die triviale irreduzible eindimensionale Darstellung von G gibt, die jedes Gruppenelement auf $1 \in \mathbb{C}^*$ abbildet. Somit kann χ_1 immer als der zugehörige triviale Charakter gewählt werden.
Weiter benutzen wir die üblichen Notationen aus 6.3.4. Dann gilt insbesondere

$$\chi_i(e) = \dim_{\mathbb{C}}(L_i) = n_i \text{ für alle } i \in \{1, \ldots, r\}.$$

BEISPIEL 6.4.1. Für eine zyklische Gruppe $G = \langle g \rangle$ der Ordnung n ist natürlich jedes Element aus G eine eigene Konjugationsklasse. Die Charaktertafel von G wurde bereits in den Übungen bestimmt. Sei ζ_n eine primitive n-te Einheitswurzel. Dann gilt:

$\langle g \rangle$	$[e]$	$[g]$	$[g^2]$	$\cdots$	$[g^{n-1}]$
χ_1	1	1	1	$\cdots$	1
χ_2	1	ζ_n	ζ_n^2	$\cdots$	ζ_n^{n-1}
χ_3	1	ζ_n^2	ζ_n^4	$\cdots$	$\zeta_n^{2(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
χ_n	1	ζ_n^{n-1}	$\zeta_n^{2(n-1)}$	$\cdots$	$\zeta_n^{(n-1)(n-1)}$

BEISPIEL 6.4.2. Wir wollen die Charaktertafel der symmetrischen Gruppe S_4 bestimmen. Es ist $|S_4| = 24$. Als erstes müssen wir wissen, wie viele

elementare Charaktere es überhaupt gibt. Dazu müssen wir die Konjugationsklassen von S_4 bestimmen. Dies ist mit Satz 1.1.34 besonders einfach. Es gilt:

Konjugationsklasse	Anzahl der Elemente
[id]	1
[(12)]	6
[(123)]	8
[(1234)]	6
[(12)(34)]	3

Somit gibt es 5 irreduzibele Darstellungen von S_4 mit den Dimensionen $n_1, \ldots, n_5$, wobei wir bereits wissen, dass oBdA $n_1 = 1$ ist. Die Anzahl der Elemente in einer Konjugationsklasse ist wichtig für die Berechnung von Skalarprodukten von Charakteren, daher nehmen wir diese Information mit in die Charaktertafel der S_4 auf. Diese hat die folgende Gestalt

S_4	1 Element [id]	6 Elemente [(12)]	8 Elemente [(123)]	6 Elemente [(1234)]	3 Elemente [(12)(34)]
χ_1	1	1	1	1	1
χ_2	n_2				
χ_3	n_3				
χ_4	n_4				
χ_5	n_5				

Das Signum ist ein Gruppen-Homomorphismus von S_4 nach $\mathbb{C}^*$, also eine eindimensionale (irreduzible) Darstellung. Dadurch erhalten wir auch χ_2. Weiter ist nach Proposition 6.1.18 und Theorem 6.3.14

$$2 + n_3^2 + n_4^2 + n_5^2 = |G| = 24 \quad \text{und} \quad n_i | 24 \ \forall i \in \{1, \ldots, 5\}.$$

Eine kurze Fallunterscheidung liefert nun $n_3 = 2$ und $n_4 = n_5 = 3$. Diese Informationen füllen wir in die Charaktertafel ein und erhalten

S_4	1 Element [id]	6 Elemente [(12)]	8 Elemente [(123)]	6 Elemente [(1234)]	3 Elemente [(12)(34)]
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2				
χ_4	3				
χ_5	3				

Die S_4 opperiert offensichtlich auf $GL_4(\mathbb{C}^4)$ durch Permutation der Spaltenvektoren. D.h. für $\sigma \in S_4$ und $(v_1 v_2 v_3 v_4) \in GL_4(\mathbb{C}^4)$ ist $\sigma.(v_1 v_2 v_3 v_4) = (v_{\sigma(1)} v_{\sigma(2)} v_{\sigma(3)} v_{\sigma(4)})$. Sei E_4 die Einheitsmatrix in $GL_4(\mathbb{C}^4)$. Dann liefert die Zuordnung $\sigma \mapsto \sigma.E_4$ eine 4dimensionale Darstellung von S_4. Der Charakter

χ dieser Darstellung ist gegeben durch

$$\chi(\sigma) = Tr(\sigma.E_4) = |\{\text{Fixpunkte von } \sigma\}|.$$

Also durch

S_4	1 Element [id]	6 Elemente [(12)]	8 Elemente [(123)]	6 Elemente [(1234)]	3 Elemente [(12)(34)]
χ	4	2	1	0	0

Die Darstellung der Permutationen der Einheitsvektoren ist nicht irreduzibel, da wir bereits wissen, dass es keine 4dimensionale irreduzible Darstellung von S_4 gibt. Alternativ sehen wir dies durch die Rechnung

$$\langle \chi, \chi \rangle = \frac{1}{24}(4^2 + 6 \cdot 2^2 + 8 \cdot 1^2 + 6 \cdot 0^2 + 3 \cdot 0^2) = 2 \neq 1.$$

Beachte, dass wir im Skalarprodukt die Elemente in derselben Konjugationsklasse zusammengefasst haben. Dadurch entstehen die *Gewichte* im Skalarprodukt.
Wir suchen mit Hilfe der Fourierkoeffizienten die Zerlegung in irreduzible Darstellungen. Es gilt

$$\langle \chi, \chi_1 \rangle = \frac{1}{24}(4 \cdot 1 + 6 \cdot 1 \cdot 2 + 8 \cdot 1 \cdot 1 + 6 \cdot 0 + 3 \cdot 0) = 1.$$

Mit Proposition 6.3.11 wissen wir, dass χ_1 in der Zerlegung von χ mit Vielfachheit 1 vorkommt. Somit erhalten wir nach Proposition 6.2.2 eine Darstellung mit Charakter $\chi' = \chi - \chi_1$. Also

S_4	1 Element [id]	6 Elemente [(12)]	8 Elemente [(123)]	6 Elemente [(1234)]	3 Elemente [(12)(34)]
χ'	3	1	0	-1	-1

Für diesen Charakter gilt

$$\langle \chi', \chi' \rangle = \frac{1}{24}(3^2 + 6 \cdot 1^2 + 6 \cdot (-1)^2 + 3 \cdot (-1)^2) = 1.$$

Somit ist die zugehörige Darstellung irreduzibel und es gilt oBdA $\chi_4 = \chi'$. Weiter erhalten wir mit Lemma 6.3.15 eine Darstellung von S_4 mit Charakter $\chi'' = \chi_2 \cdot \chi_4$. Eine einfache Rechnung zeigt, dass auch $\langle \chi'', \chi'' \rangle = 1$ gilt und somit ist $\chi_5 = \chi''$.
Es fehlt lediglich noch die Bestimmung von χ_3. Dies ist nun aber dank Lemma 6.2.4 besonders einfach. Denn es gilt

$$\chi_1(\sigma) + \chi_2(\sigma) + 2\chi_3(\sigma) + 3\chi_4(\sigma) + 3\chi_5(\sigma) = \begin{cases} 24 \text{ falls } \sigma = \text{id} \\ 0 \text{ sonst} \end{cases}.$$

Damit können wir die Charaktertafel der S_4 vervollständigen und erhalten

S_4	1 Element [id]	6 Elemente [(12)]	8 Elemente [(123)]	6 Elemente [(1234)]	3 Elemente [(12)(34)]
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

KAPITEL 7

Kommutative Algebra

In diesem Kapitel werden wir uns ausschließlich kommutativen Strukturen widmen. Daher ist ab jetzt **jeder Ring als kommutativ vorausgesetzt!** Unser Hauptaugenmerk liegt af dem Polynomring $K[x_1, \ldots, x_n]$ über einem Körper K. Dies führt zu einer kurzen Einführung in die algebraische Geometrie. Wir werden wieder Elemente in Polynome einsetzen und dabei implizit den Einsetzhomomorphismus benutzen.

7.1. Algebraische Unabhängigkeit

Wir wollen den bekannten Begriff der linearen Unabhängigkeit erweitern. Dies lässt sich darauf anwenden endlich erzeugte Körpererweiterungen zu studieren, die nicht notwendig algebraisch sind. Insbesondere werden wir einen Grad für transzendente Erweiterungen einführen.

DEFINITION 7.1.1. Sei R ein Ring. Eine *Ringerweiterung* von R ist ein Ring R' mit $R \subseteq R'$ und $1_R = 1_{R'}$. Eine Ringerweiterung $R \subseteq R'$ heißt *ganz*, genau dann wenn jedes Element aus R' ganz über R ist.

Ist eine Ringerweiterung $R \subseteq R'$ gegeben, so ist R' durch Einschränkung der Ringmultiplikation ein R-Modul. Insbesondere liefert Satz 5.2.14, dass $R \subseteq R'$ ganz ist, falls R' ein endlich erzeugter R-Modul ist.

LEMMA 7.1.2. *Sei K ein Körper und R ein Ring, so dass $R \subseteq K$ eine Ringerweiterung ist, und K ein endlich erzeugter R-Modul ist. Dann ist R selbst ein Körper.*

BEWEIS. Es ist nur zu zeigen, dass jedes Element $a \in R \setminus \{0\}$ ein multiplikatives Inverses in R besitzt. Da K ein Körper ist, existiert sicher ein multiplikatives Inverses $a^{-1} \in K$. Nun ist aber $R \subseteq K$ eine ganze Ringerweiterung und somit existieren Elemente $\lambda_0, \ldots, \lambda_{n-1} \in R$ mit

$$a^{-n} + \lambda_{n-1}a^{-(n-1)} + \ldots + \lambda_0$$
$$\implies a^{-n} = -\lambda_{n-1}a^{-(n-1)} - \ldots - \lambda_0.$$

Multiplizieren wir diese Gleichung mit a^{n-1} erhalten wir

$$a^{-1} = -\lambda_{n-1} - \lambda_{n-2}a - \ldots - \lambda_0 a^{n-1} \in R.$$

Es ist a^{-1} tatsächlich in R, da $a^r \in R$ gilt für alle $r \in \mathbb{N}_0$. □

LEMMA 7.1.3. *Seien $R \subseteq R'$ und $R' \subseteq R''$ Ringerweiterungen, so dass R' ein endlich erzeugter R-Modul und R'' ein endlich erzeugter R'-Modul ist. Dann ist R'' ein endlich erzeugter R-Modul.*

BEWEIS. Sei $\alpha_1, \ldots, \alpha_s \in R'$ ein Erzeugendensystem des R-Moduls R' und sei $\beta_1, \ldots, \beta_r \in R''$ ein Erzeugendensystem des R'-Moduls R''. Dann lässt sich jedes $\beta \in R''$ schreiben als

$$\sum_{i=1}^{r} \lambda_i \beta_i, \tag{62}$$

mit $\lambda_i \in R$ für alle $i \in \{1, \ldots, r\}$. Weiter existieren Elemente $\mu_{ij} \in R$, so dass $\lambda_i = \sum_{j=1}^{s} \mu_{ij}\alpha_j$ gilt, für alle $i \in \{1, \ldots, r\}$. Setzen wir dies in (62) ein, so erhalten wir

$$\beta = \sum_{i=1}^{r} \left(\sum_{j=1}^{s} \mu_{ij}\alpha_j \right) \beta_i = \sum_{(i,j) \in \{1,\ldots,r\} \times \{1,\ldots,s\}} \mu_{ij}(\alpha_j \beta_i).$$

Somit ist $\{\alpha_j\beta_i\}_{(i,j)\in\{1,\ldots,r\}\times\{1,\ldots,s\}}$ ein endliches Erzeugendensystem des R-Moduls R''. □

BEMERKUNG 7.1.4. Sei K ein Körper und A eine K-Algebra. Es gibt zwei Arten A als „endlich erzeugt über K“ aufzufassen. Die erste ist, dass A *endlich erzeugt als K-Modul* ist, es also Elemente $a_1, \ldots, a_r \in A$ gibt, so dass jedes $a \in A$ von der Form $\lambda_1 a_1 + \cdots + \lambda_n a_n$, mit $\lambda_1, \ldots, \lambda_n \in K$, ist.
Bei der zweiten Variante erlauben wir auch die Ringstruktur auf A bei der Erzeugung von Elementen. Das heißt A ist *endlich erzeugt als K-Algebra*, falls es Elemente $a_1, \ldots, a_n \in A$ gibt, so dass jedes Element in A von der Form $f(a_1, \ldots, a_n)$, für ein $f \in K[x_1, \ldots, x_n]$ ist.
Diese beiden Definitionen sind natürlich nicht äquivalent. Zum Beispiel ist der Polynomring $K[x]$ per Konstruktion endlich erzeugt als K-Algebra, aber nicht endlich erzeugt als K-Modul. Jedoch ist jede K-Algebra, die endlich erzeugt als K-Modul ist, auch endlich erzeugt als K-Algebra.

DEFINITION 7.1.5. Sei K ein Körper und A eine K-Algebra. Elemente $a_1, \ldots, a_n \in A$ heißen *algebraisch abhängig über K*, falls es ein Polynom $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ gibt mit $f(a_1, \ldots, a_n) = 0$. Existiert kein solches Polynom, dann heißen $a_1, \ldots, a_n$ *algebraisch unabhängig über K*. Eine beliebige Teilmenge $S \subseteq A$ nennen wir algebraisch unabhängig über K, genau dann wenn alle endlichen Teilmengen von S algebraisch unabhängig über K sind.

BEISPIEL 7.1.6. Sei wieder K ein Körper.

- Der Polynomring $K[x_1, \ldots, x_n]$ in den Variablen $x_1, \ldots, x_n$ ist eine K-Algebra. Per Definition sind die Elemente $x_1, \ldots, x_n$ algebraisch unabhängig über K. (Es ist $f(x_1, \ldots, x_n) = 0$ genau dann wenn $f = 0$).
- Ist L/K eine Körpererweiterung und ist $\alpha \in L$ algebraisch über K, dann ist für alle Elemente $\alpha_1, \ldots, \alpha_n \in L$ die Menge $\alpha_1, \ldots, \alpha_n, \alpha$ algebraisch abhängig über K. Hierzu wählen wir einfach das $f \in K[x_1, \ldots, x_n, x_{n+1}] \setminus \{0\}$ mit $f(x_1, \ldots, x_{n+1}) = m_{\alpha,K}(x_{n+1})$.

NOTATION 7.1.7. Sei K ein Körper und A eine K-Algebra. Für eine Teilmenge $S \subseteq A$ bezeichnen wir mit $K[S]$ den kleinsten Teilring von A, der K und S enthält. Dann ist $K[S]$ auch eine K-Algebra und es gilt

$$K[S] = \{f(a_1, \ldots, a_n) | n \in \mathbb{N},\ f \in K[x_1, \ldots, x_n],\ a_1, \ldots, a_n \in S\}.$$

Falls A ein Integritätsbereich ist, bezeichnen wir mit $K(S)$ den Quotientenkörper von $K[S]$. Für algebraisch unabhängige Elemente $a_1, \ldots, a_n$ ist somit $K[a_1, \ldots, a_n]$ isomorph zum Polynomring $K[x_1, \ldots, x_n]$, denn der Einsetzhomomorphismus

$$\varphi : K[x_1, \ldots, x_n] \longrightarrow K[a_1, \ldots, a_n] \quad ; \quad f \mapsto f(a_1, \ldots, a_n)$$

ist nach Definition von algebraisch unabhängig injektiv und nach Konstruktion von $K[a_1, \ldots, a_n]$ auch surjektiv.

PROPOSITION 7.1.8. *Seien $b_1, \ldots, b_n$ über K algebraisch abhängige Elemente in einer K-Algebra A. Dann existiert ein $t \in \mathbb{N}$ so, dass b_n ganz über $K[b_1 - b_n^t, b_2 - b_n^{t^2}, \ldots, b_{n-1} - b_n^{t^{n-1}}]$ ist.*

BEWEIS. Nach Annahme gibt es ein Polynom $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ mit $f(b_1, \ldots, b_n) = 0$. das bedeutet, dass es eine endliche Teilmenge $I \subseteq \mathbb{N}_0^n$ gibt, mit

$$0 = \sum_{\nu=(\nu_1,\ldots,\nu_n)\in I} \lambda_\nu b_1^{\nu_1} \cdots b_n^{\nu_n} \text{ wobei } \lambda_\nu \in K^* \text{ für alle } \nu \in I. \tag{63}$$

Sei $t \in \mathbb{N}$ beliebig mit $t > \max\{\max\{\nu_1, \ldots, \nu_n\} | (\nu_1, \ldots, \nu_n) \in I\}$. Wir schreiben $b_i' = b_i - b_n^{t^i}$ für alle $i \in \{1, \ldots, n-1\}$ und setzen dies in (63) ein. Wir erhalten

$$\begin{aligned} 0 = h(b_n) &= \sum_{\nu\in I} \lambda_\nu (b_1' + b_n^t)^{\nu_1} \cdots (b_{n-1}' + b_n^{t^{n-1}})^{\nu_{n-1}} b_n^{\nu_n} \\ &= \sum_{\nu\in I} \lambda_\nu b_n^{t\nu_1 + t^2\nu_2 + \ldots + t^{n-1}\nu_{n-1} + \nu_n} + g(b_n) \end{aligned} \tag{64}$$

für Polynome $h, g \in (K[b'_1, \ldots, b'_{n-1}])[x]$, wobei

$$\text{grad}(g) < \max\{t\nu_1 + \ldots + t^{n-1}\nu_{n-1} + \nu_n | (\nu_1, \ldots, \nu_n) \in I\} =: N.$$

Es bleibt nur zu zeigen, dass wir h als normiert annehmen dürfen. Wir haben t gerade so gewählt, dass alle Zahlen in $\{t\nu_1 + \ldots + t^{n-1}\nu_{n-1} + \nu_n | (\nu_1, \ldots, \nu_n) \in I\}$ verschieden sind (Darstellungen im t-adischen Zahlsystem sind eindeutig). Insbesondere ist somit $\text{grad}(h) = N$ und es ist $h(x) = \lambda_\nu x^N +$ *Terme kleinerer Ordung* für geeignetes $\nu \in I$. Es ist $\lambda_\nu \in K^*$ und somit ist $\lambda_\nu^{-1} h(x)$ ein normiertes Polynom in $(K[b'_1, \ldots, b'_{n-1}])[x]$ mit b_n als Nullstelle. Daher ist b_n wie gewünscht ganz über $K[b'_1, \ldots, b'_{n-1}]$. □

THEOREM 7.1.9 (Noetherscher Normalisierungssatz). *Sei K ein Körper und A eine K-Algebra, die als Algebra endlich erzeugt über K ist. Dann existieren über K algebraisch unabhängige Elemente $a_1, \ldots, a_r \in A$, so dass A ein endlich erzeugter $K[a_1, \ldots, a_r]$-Modul ist.*

BEWEIS. Nach Voraussetzung existieren Elemente $b_1, \ldots, b_n \in A$ mit $A = K[b_1, \ldots, b_n]$. Wir führen den Beweis per Induktion über n.
Induktionsanfang: $n = 1$: Es ist also $A = K[b_1]$. Falls b_1 algebraisch unabhängig über K ist, sind wir fertig, da A ein endlich erzeugter A-Modul ist. Falls b_1 algebraisch abhängig über K ist, existiert ein $f \in K[x] \setminus \{0\}$ mit $f(b_1) = 0$. Da K ein Körper ist, können wir oBdA annehmen, dass f normiert ist. Somit ist b_1 ganz über K, und mit Satz 5.2.14 ist A ein endlich erzeugter K-Modul.
Induktionsschritt: $n \geq 2$: Wie eben sind wir fertig, falls bereits $b_1, \ldots, b_n$ algebraisch unabhängig über K sind. Seien also $b_1, \ldots, b_n$ algebraisch abhängig über K. Mit Proposition 7.1.8 folgt, dass für gewisses $t \in \mathbb{N}$ b_n ganz über $K[\underbrace{b_1 - b_n^t}_{=b'_1}, \ldots, \underbrace{b_{n-1} - b_n^{t^{n-1}}}_{=b'_{n-1}}]$ ist. Benutzen wir die Gleichung

$$A = K[b_1, \ldots, b_n] = K[b'_1, \ldots, b'_{n-1}, b_n] = (K[b'_1, \ldots, b'_{n-1}])[b_n],$$

so folgt dass A ein endlich erzeugter $K[b'_1, \ldots, b'_{n-1}]$-Modul ist. Nach Induktionsvoraussetzung existieren $a_1, \ldots, a_r \in A$, algebraisch unabhängig über K, so dass $K[b'_1, \ldots, b'_{n-1}]$ ein endlich erzeugter $K[a_1, \ldots, a_r]$-Modul ist. Zusammen schließen wir mit Lemma 7.1.3, dass A ein endlich erzeugter $K[a_1, \ldots, a_r]$-Modul ist. Das war zu zeigen. □

KOROLLAR 7.1.10. *Sei L/K eine Körpererweiterung, so dass L endlich erzeugt als K-Algebra ist. Dann ist L/K eine endliche Körpererweiterung, und somit insbesondere algebraisch.*

BEWEIS. L erfüllt die Voraussetzungen vom Noetherschen Normalisierungssatz. Somit existieren über K algebraisch unabhängige Elemente $a_1, \ldots, a_r \in L$, so dass L endlich erzeugt als $K[a_1, \ldots, a_r]$-Modul ist. Mit Lemma 7.1.2 folgt, dass $K[a_1, \ldots, a_r]$ ein Körper ist. Dies ist aber nur für $r = 0$, also $K[a_1, \ldots, a_r] = K$ erfüllt. Also ist L/K endlich und mit Proposition 3.3.10 auch algebraisch. □

DEFINITION 7.1.11. Sei L/K eine Körpererweiterung. Eine Menge $B \subseteq L$ heißt *Transzendenzbasis von* L/K, genau dann wenn B algebraisch unabhängig über K ist und die Erweiterung $L/K(B)$ algebraisch ist.

PROPOSITION 7.1.12. *Sei L/K eine Körpererweiterung. Dann existiert eine Transzendenzbasis von L/K. Weiter gilt, dass eine Teilmenge $B \subseteq L$ genau dann eine Transzendenzbasis von L/K ist, wenn B eine maximale über K algebraisch unabhängige Teilmenge von L ist.*

BEWEIS. Angenommen es gibt eine Transzendenzbasis B von L/K. Dann ist $L/K(B)$ algebraisch. Sei also $\alpha \in L \setminus B$ beliebig und $f \in K(B)[x] \setminus \{0\}$ mit $f(\alpha) = 0$. Jedes Element in $K(B)$ ist von der Form $g(a_1,\ldots,a_r)/\widehat{g}(a_1,\ldots,a_r)$ für gewisse $a_1, \ldots, a_r \in B$ und $g, \widehat{g} \in K[x_1, \ldots, x_r]$. Wenden wir dies auf die Koeffizienten von f an und vergrössern möglicherweise r, so erhalten wir

$$0 = \frac{g_d(a_1, \ldots, a_r)}{\widehat{g}_d(a_1, \ldots, a_r)}\alpha^d + \ldots + \frac{g_0(a_1, \ldots, a_r)}{\widehat{g}_0(a_1, \ldots, a_r)}.$$

Multiplizieren wir diese Gleichung mit $\prod_{i=0}^{d} \widehat{g}_i(a_1, \ldots, a_r) \neq 0$, so erhalten wir eine nichttriviale polynomielle Gleichung in $a_1, \ldots, a_r, \alpha$, die Null ergibt. Somit ist $B \cup \{\alpha\}$ algebraisch abhängig über K. Da $\alpha \in L \setminus B$ beliebig war, bedeutet dies gerade, dass B eine maximale algebraisch unabhängige Teilmenge von L ist.

Im Folgenden zeigen wir, dass eine maximale über K algebraisch unabhängige Teilmenge $B \subseteq L$ existiert und, dass so eine Menge B eine Transzendenzbasis von L/K ist. Dies ist wiedermal eine Anwendung des Zornschen Lemmas 3.5.6. Sei also $C = \{B \subseteq L | B \text{ algebraisch unabhängig}\}$. Wie immer ist C nicht leer und partiell geordnet bezüglich Inklusion. Weiter ist für eine total geordnete Teilmenge $\{B_i\}_{i \in I} \subseteq C$ die Menge $\cup_{i \in I} B_i$ eine obere Schranke in C. Dass dies eine obere Schranke ist, ist offensichtlich. Diese liegt in C, da jede endliche Teilmenge von $\cup_{i \in I} B_i$ in einem B_j, $j \in I$, liegt und damit algebraisch unabhängig ist.

Das Zornsche Lemma liefert uns also die Existenz einer maximalen algebraisch unabhängigen Teilmenge $B \subseteq L$. Es bleibt zu zeigen, dass $L/K(B)$ algebraisch ist. Natürlich ist jedes Element aus $K(B)$ algebraisch über $K(B)$.

Sei also $\alpha \in L \setminus K(B)$. Die Maximalität von B besagt, dass $a_1, \ldots, a_r, \alpha$ algebraisch abhängig über K ist für gewisse $a_1, \ldots, a_r \in B$. Somit existiert ein $f \in K[x_1, \ldots, x_r, x] \setminus \{0\} = K[x_1, \ldots, x_r][x] \setminus \{0\}$ mit

$$f(a_1, \ldots, a_r, \alpha) = f_d(a_1, \ldots, a_r)\alpha^d + \ldots + f_0(a_1, \ldots, a_r) = 0.$$

Da $f \neq 0$ ist, sind nicht alle $f_0, \ldots, f_d$ gleich Null. Die algebraische Unabhängigkeit von $a_1, \ldots, a_r$ garantiert, dass damit auch nicht alle Koeffizienten $f_0(a_1, \ldots, a_r), \ldots, f_d(a_1, \ldots, a_r)$ gleich Null sind. Es folgt, dass

$$f_d(a_1, \ldots, a_r)\alpha^d + \ldots f_0(a_1, \ldots, a_r) \in K(B)[x] \setminus \{0\}$$

ein nicht-triviales Polynom mit Nullstelle α ist. Das bedeutet, dass $\alpha \in L$ algebraisch über $K(B)$ ist. □

Beispiel 7.1.13. Sei $K[x_1, \ldots, x_n]$ der Polynomring in r Variablen über einem Körper K. Dann bilden die Elemente $x_1, \ldots, x_r$ eine Transzendenzbasis von $K(x_1, \ldots, x_r)/K$. Hier ist wie üblich $K(x_1, \ldots, x_r)$ der Quotientenkörper des zugehörigen Polynomringes.
Für eine algebraische Körpererweiterung L/K ist $\emptyset$ eine Transzendenzbasis von L/K.

Satz 7.1.14. *Sei L/K eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in L$ eine Transzendenzbasis von L/K. Dann besitzen alle Transzendenzbasen von L/K genau n Elemente.*

Beweis. Dies folgt aus Proposition 7.1.12 und dem folgendem Satz, genau wie die entsprechende Aussage über Basen von Vektorräumen. □

Satz 7.1.15 (Steinitzscher Austauschsatz). *Seien $\alpha_1, \ldots, \alpha_n$ eine Transzendenzbasis von L/K und sei $\beta \in L$ transzendent über K. Dann ist nach möglicher Umnummerierung $\beta, \alpha_2, \ldots, \alpha_n$ eine Transzendenzbasis von L/K.*

Beweis. Da $\alpha_1, \ldots, \alpha_n$ eine Transzendenzbasis von L/K ist, ist β algebraisch über $K(\alpha_1, \ldots, \alpha_n)$. Es existiert also eine $f \in K(\alpha_1, \ldots, \alpha_n)[x] \setminus \{0\}$ mit $f(\beta) = 0$. Dies impliziert sofort die Existenz eines Elementes $g \in K(x_1, \ldots, x_n, x) \setminus \{0\}$ mit $g(\alpha_1, \ldots, \alpha_n, \beta) = 0$. Wie im Beweis von Proposition 7.1.12 dürfen wir nach Multiplikation mit den Nennern der Koeffizienten von g sogar $g \in K[x_1, \ldots, x_n, x] \setminus \{0\}$ annehmen.
Da β transzendent über K ist, muss mindestens eine der Variablen $x_1, \ldots, x_n$ in g vor. Sei dies oBdA x_1. Das bedeutet gerade, dass g aufgefasst als Polynom in $(K[x_2, \ldots, x_n, x])[x_1]$ positiven Grad hat.

$$\implies \alpha_1 \text{ ist algebraisch über } K(\alpha_2, \ldots, \alpha_n, \beta). \tag{65}$$

Sei nun $\beta' \in L$ beliebig. Dann ist β' algebraisch über $K(\alpha_1, \ldots, \alpha_n, \beta) = K(\alpha_2, \ldots, \alpha_n, \beta)(\alpha_1)$. Damit muss β' nach (65) bereits algebraisch über $K(\alpha_2, \ldots, \alpha_n, \beta)$ ist.
Es bleibt zu zeigen, dass $\alpha_2, \ldots, \alpha_n, \beta$ algebraisch unabhängig über K sind. Angenommen dies wäre nicht der Fall. Da $\alpha_2, \ldots, \alpha_n$ nach Voraussetzung algebraisch unabhängig sind, muss dann β algebraisch über $K(\alpha_2, \ldots, \alpha_n)$ sein. Dann folgt aber mit (65), dass auch α_1 algebraisch über $K(\alpha_2, \ldots, \alpha_n)$ ist. Dies ist ein Widerspruch zur algebraischen Unabhängigkeit der Elemente $\alpha_1, \ldots, \alpha_n$. Also ist $\alpha_2, \ldots, \alpha_n, \beta$ auch algebraisch unabhängig über K und somit eine Transzendenzbasis von L/K. □

Definition 7.1.16. Der *Transzendenzgrad* einer Körpererweiterung L/K ist gegeben durch

$$tr.\deg(L/K) = \begin{cases} n \text{ falls } L/K \text{ eine Tr'basis mit } n < \infty \text{ Elementen besitzt} \\ \infty \text{ sonst} \end{cases}$$

Beachte, dass diese Definition nach Satz 7.1.14 wohldefiniert ist.

Beispiel 7.1.17. Sei wieder $K[x_1, \ldots, x_n]$ der Polynomring in n Variablen mit Quotientenkörper L. Dann ist $x_1, \ldots, x_n$ eine Transzendenzbasis und es gilt $tr.\deg(L/K) = n$. Die n Elemente $x_1^2, \ldots, x_n^2$ sind natürlich ebenfalls algebraisch unabhängig über K und somit bilden auch diese Elemente nach Satz 7.1.14 eine Transzendenzbasis. Aber es ist $L \neq K(x_1^2, \ldots, x_n^2)$.
Dies zeigt, dass ausser im Fall $tr.\deg(L/K) = 0$ Transzendenzbasen und von ihnen erzeugte Körper niemals eindeutig bestimmt sind.

Proposition 7.1.18. *Seien M/L und L/K Körpererweiterungen, dann gilt*

$$tr.\deg(M/K) = tr.\deg(M/L) + tr.\deg(L/K).$$

Beweis. Übung. □

Abbildung 7.1. In seiner Arbeit „Algebraische Theorie der Körper“ (1910) führte der deutsche Mathematiker *Ernst Steinitz* (1871-1928) die Begriffe Primkörper, perfekte Körper und Transzendenzgrad ein, und bewies den uns bekannten Satz, dass jeder Körper in einem algebraisch abgeschlossenen Körper enthalten ist.

Beispiel 7.1.19. Sei K ein Körper. Wir betrachten die K-Algebra

$$A = {}^{K[x,y]}\!/_{\langle y^2 - x^3 + x \rangle}.$$

Diese ist über K als K-Algebra erzeugt von den Elementen $\overline{x} = x+\langle y^2-x^3+x\rangle$ und $\overline{y} = y+\langle y^2-x^3+x\rangle$. Das Polynom $f(X,Y) = Y^2-X^3+X \in K[X,Y]$ ist ein nicht-triviales Polynom mit $f(\overline{x},\overline{y}) = \overline{f(x,y)} = \overline{y^2-x^3+x} = \overline{0} \in A$. Somit sind $\overline{x}$ und $\overline{y}$ algebraisch abhängig über K. Weiter ist $\overline{x} \in A$ algebraisch unabhängig über K, da $f(x) \notin \langle y^2 - x^3 + x\rangle$ ist für alle $f \in K[X] \setminus \{0\}$. Also bedeutet $f(\overline{x}) = \overline{0}$ auch $f(X) = 0$.
Es ist $A = (K[\overline{x}])[\overline{y}]$ und $\overline{y}$ ist ganz über $K[\overline{x}]$, da es Nullstelle des normierten Polynoms $f(X) = X^2-\overline{x}^3+\overline{x} \in (K[\overline{x}])[X]$ ist. Das bedeutet gerade, dass die gesamte Ringerweiterung $A \supseteq K[\overline{x}]$ ganz ist. Das Element $\overline{x}$ bildet also eine mit dem Noetherschen Normalisierungssatz 7.1.9 vorausgesagte algebraisch unabhängige Teilmenge von A.
Es ist $x^3 - x$ kein Quadrat in $K(x)$, da es ungeraden Grad besitzt. Somit besitzt $y^2 - x^3 + x$ aufgefasst als Polynom in y über $K(x)$ keine Nullstelle in $K(x)$. Da der Grad in y gleich 2 ist, folgt sofort, dass $y^2 - x^3 + x$ irreduzibel in $(K(x))[y]$ ist. Insbesondere ist es also irreduzibel in $K[x,y]$.
Es ist also $\langle y^2 - x^3 + x\rangle$ ein Primideal in $K[x,y]$. Folglich ist A ein Integritätsbereich und wir können den Quotientenkörper $L = Quot(A)$ bilden. Wie gerade gesehen, ist $\overline{x} \in L$ transzendent über K und A ist eine ganze Ringerweiterung von $K[\overline{x}]$. Da offensichtlich L eine ganze Ringerweiterung von A ist, ist L eine ganze Ringerweiterung von $K[\overline{x}]$ und insbesondere von $K(\overline{x})$. Das heißt nichts anderes, als dass $L/K(\overline{x})$ algebraisch ist. Also ist $\overline{x}$ eine Transzendenzbasis von L/K und es gilt $tr.\deg(L/K) = 1$.

7.2. Grundbegriffe der algebraischen Geometrie

In der lineraen Algebra werdeen Lösungsmengen von Systemen linearer Gleichungen über einem Körper studiert. In der algebraischen Geometrie werden Lösungsmengen von Systemen polynomieller Gleichungen über (meist algebraisch abgeschlossenen) Körpern studiert. Der Begriff *Geometrie* kommt daher, dass solche Lösungsmengen zumindest über $\mathbb{R}$ oder $\mathbb{C}$ und in kleinen Dimensionen anschaulische geometrische Formen liefern. Zum Beispiel beschreiben die Nullstellen von $x^2 + y^2 - 1$ den Einheitskreis in $\mathbb{R}^2$.
Wir wollen unter Anderem die Verbindung solcher Lösungsmengen zu Idealen in Polynomringen studieren. Im Folgenden sei K stets ein Körper.

Definition 7.2.1. Sei $K[x_1,\dots,x_n]$ der Polanomring in n Variablen über K. Für eine Teilmenge $T \subseteq K[x_1,\dots,x_n]$ bezeichnen wir die *Nullstellenmenge* von T in K^n mit

$$V(T) = \{\underline{a} = (a_1,\dots,a_n) \in K^n | f(\underline{a}) = 0 \text{ für alle } f \in T\}.$$

Eine *algebraische Menge* in K^n ist eine Menge der Form $V(T)$ für eine Teilmenge $T \subseteq K[x_1, \ldots, x_n]$.

BEMERKUNG 7.2.2. Sei $T \subseteq K[x_1, \ldots, x_n]$ eine Teilmenge und $\langle T \rangle$ das von T erzeugte Ideal in $K[x_1, \ldots, x_n]$, dann ist $V(T) = V(\langle T \rangle)$. Dies ist offensichtlich, da mit $f_1(\underline{a}) = f_2(\underline{a}) = 0$ und $g \in K[x_1, \ldots, x_n]$ beliebig auch $(f_1 + f_2)(\underline{a}) = f_1(\underline{a}) + f_2(\underline{a}) = 0$ und $(gf_1)(\underline{a}) = g(\underline{a})f_1(\underline{a}) = 0$ gilt. Wir können also alle Mengen T, deren Nullstellen algebraische Mengen definieren, stets als Ideal betrachten.

BEISPIEL 7.2.3. Wir geben ein paar einfache Beispiele für algebraische Mengen in K^n.

- Jeder Punkt $\underline{a} = (a_1, \ldots, a_n) \in K^n$ ist eine algebraische Menge. Denn es ist

$$V(x_1 - a_1, \ldots, x_n - a_n) = \{\underline{b} \in K^n | b_1 = a_1, \ldots, b_n = a_n\} = \{\underline{a}\}.$$

- Der ganze Raum K^n ist eine algebraische Menge, denn es ist $V(0) = V(\emptyset) = K^n$.
- Auch die leere Menge ist eine algebraische Menge, denn offensichtlich ist $V(1) = V(K[x_1, \ldots, x_n]) = \emptyset$. Für $K = \mathbb{R}$ gibt es auch echte Ideale A von $K[x_1, \ldots, x_n]$ mit $V(A) = \emptyset$. Zum Beispiel ist dies für $A = \langle x^2+y^2+1 \rangle$ der Fall. Das Hauptresultat dieses Abschnittes impliziert, dass für algebraisch abgeschlossenes K nur dann $V(A) = \emptyset$ gilt wenn $A = K[x_1, \ldots, x_n]$ gilt.

PROPOSITION 7.2.4. *Sei $T \subseteq K[x_1, \ldots, x_n]$ eine beliebige Teilmenge. Dann existieren $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ mit $V(T) = V(f_1, \ldots, f_r)$.*

BEWEIS. Wir wissen, dass $V(T) = V(\langle T \rangle)$ gilt. Weiter ist K als Körper trivialerweise noethersch, also ist mit dem Hilbertschen Basissatz 5.3.16 auch $K[x_1, \ldots, x_n]$ noethersch. Also existieren nach Proposition 5.3.5 endlich viele Polynome $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ mit $\langle T \rangle = \langle f_1, \ldots, f_r \rangle$. Damit erhalten wir $V(T) = V(\langle T \rangle) = V(\langle f_1, \ldots, f_r \rangle) = V(f_1, \ldots, f_r)$. □

LEMMA 7.2.5. *Sei J eine Indexmenge und seien A, B, A_j, $j \in J$, Ideale vom Polynomring $K[x_1, \ldots, x_n]$. Dann gilt*

(a) $A \subseteq B \Longrightarrow V(B) \subseteq V(A)$.
(b) $V(A \cap B) = V(A) \cup V(B)$.
(c) $V(\sum_{j \in J} A_j) = \bigcap_{j \in J} V(A_j)$.

BEWEIS. Dies sind einfache Folgerungen aus der Definition der Nullstellenmenge.

Zu (a): Sei $\underline{a} \in V(B)$. Dann ist $f(\underline{a}) = 0$ für alle $f \in B$, insbesondere also für alle $f \in A \subseteq B$. Somit ist per Definition auch $\underline{a} \in V(A)$.

Zu (b): Wir wissen nach (a) bereits $V(A) \cap V(B) \subseteq V(A \cap B)$. Angenommen es gäbe ein $\underline{a} \in V(A \cap B) \setminus \{V(A) \cup V(B)\}$. Dann existieren $g \in A$ und $h \in B$ mit $g(\underline{a}) \neq 0 \neq h(\underline{a})$. Damit ist natürlich auch $(gh)(\underline{a}) \neq 0$. Andererseits ist $gh \in A \cap B$ und es gilt $f(\underline{a}) = 0$ für alle $f \in A \cap B$. Das ist ein Widerspruch, daher kann ein solches $\underline{a}$ nicht existieren.

Zu (c): Dies folgt wie in (a).

$$\begin{aligned} V(\sum_{j \in J} A_j) &= \{\underline{a} \in K^n | f(\underline{a}) = 0 \ \forall f \in \sum_{j \in J} A_j\} \\ &= \{\underline{a} \in K^n | f(\underline{a}) = 0 \ \forall f \in A_j \ \forall j \in J\} \\ &= \bigcap_{j \in J} \{\underline{a} \in K^n | f(\underline{a}) = 0 \ \forall f \in A_j\} = \bigcap_{j \in J} V(A_j) \end{aligned}$$

□

WIEDERHOLUNG. Ein *topologischer Raum* (X, Ω) ist eine Menge X zusammen mit einer Teilmenge Ω der Potenzmenge von X, die die drei folgenden Axiome erfüllt. Die Elemente in Ω werden *offene* Teilmengen von X genannt.

(i) $\emptyset$ und X sind offen.
(ii) Schnitte von endlich vielen offenen Mengen sind offen.
(iii) Vereinigungen von beliebig vielen offenen Mengen sind offen.

Teilmengen von X heißen *abgeschlossen* genau dann wenn ihr Komplement in X offen ist. Somit sind die Axiome $i), ii), iii)$ äquivalent zu:

(i') X und $\emptyset$ sind abgeschlossen.
(ii') Vereinigungen von endlich vielen abgeschlossenen Mengen sind abgeschlossen.
(iii') Schnitte von beliebig vielen abgeschlossenen Mengen sind abgeschlossen.

Für eine Teilmenge $Y \subseteq X$ ist der *Abschluss* $\overline{Y}$ von Y in X gegeben als Schnitt aller abgeschlossener Mengen, die Y enthalten. Eine Teilmenge Y heißt *dicht* in X falls $\overline{Y} = X$ gilt.

SATZ 7.2.6. *Nennen wir die algebraischen Mengen auf K^n abgeschlossen (und die Komplemente algebraischer Mengen offen) so wird damit K^n zu einem topologischen Raum.*

BEWEIS. Die Axiome $(i'), (ii'), (iii')$ haben wir in 7.2.3 und 7.2.4 nachgeprüft. □

DEFINITION 7.2.7. Die in Satz 7.2.6 definierte Topologie heißt *Zariski-Topologie* auf K^n. Den topologischen Raum $(K^n, \{K^n \backslash V(T) | T \subseteq K[x_1, \ldots, x_n]\})$ nennen wir affinen Raum und bezeichnen ihn mit $\mathbb{A}^n_K$, oder $\mathbb{A}^n$ falls der zugrunde liegende Körper klar ist. Die abgeschlossenen Mengen in $\mathbb{A}^n_K$ heißen *(affine) Varietäten* über K.

Achtung: Auf $\mathbb{R}^n$. oder auch $\mathbb{C}^n$, gibt es noch die „übliche“ Topologie, die gegeben ist durch die euklidische Metrik auf $\mathbb{R}$ beziehungsweise $\mathbb{C}$. Diese Topologie ist grundverschieden zur Zariski-Topologie!
Auf $\mathbb{R}$ ist eine offene Umgebung des Punktes 0 in der metrischen Topologie gegeben durch ein Intervall $(-\varepsilon, \varepsilon)$, $\varepsilon > 0$. Diese offenen Mengen sind also „relativ klein“ im Vergleich zu ganz $\mathbb{R}$. In der Zariski-Topologie ist eine offene Umgebung der 0 gegeben durch $\mathbb{R} \setminus \{\text{Nullstellen von } f(x) \cdot x\}$ für ein Polynom $f \in K[x] \setminus \{0\}$, also bis auf endlich viele Punkte ganz $\mathbb{R}$ und somit „riesen groß“.

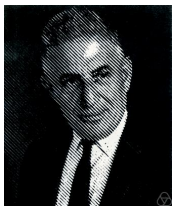


ABBILDUNG 7.2. Der amerikanische Mathematiker *Oscar Zariski* (1899-1986; Geburtsname: Ascher Zaritsky) war ein Pionier der heutigen algebraischen Geometrie. Er formalisierte die Geometrie in dem er Sie in eine algebraische Sprache übersetzte.

KONSTRUKTION 7.2.8. Das Bilden der Nullstellenmenge liefert eine Abbildung von den Idealen von $K[x_1, \ldots, x_n]$ in die Teilmengen von $\mathbb{A}^n$. Wir wollen eine Abbildung in die andere Richtung konstruieren. Sei also $X \subseteq \mathbb{A}^n$ eine Teilmenge. Dann setzen wir

$$I(X) = \{f \in K[x_1, \ldots, x_n] | f(\underline{a}) = 0 \text{ für alle } \underline{a} \in X\}.$$

Wie in 7.2.2 sehen wir sofort, dass $I(X)$ ein Ideal in $K[x_1, \ldots, x_n]$ ist. Es heißt das *Verschwindungsideal* von X.

LEMMA 7.2.9. *Seien X und Y Teilmengen von $\mathbb{A}^n_K$ und A ein Ideal in $K[x_1, \ldots, x_n]$. Dann gilt*

(a) $X \subseteq Y \Longrightarrow I(Y) \subseteq I(X)$.
(b) $A \subseteq I(V(A))$.
(c) $V(I(Y)) = \overline{Y}$, *wobei* $\overline{Y}$ *der Abschluss von* Y *in der Zariski-Topologie ist.*

BEWEIS. Die Aussagen in (a) und (b) folgen unmittelbar aus der Definition. Ebenfalls ist sofort klar, dass $Y \subseteq V(I(Y))$ gilt. Da $V(I(Y))$ als algebraische

Menge abgeschlossen ist, muss damit auch $\overline{Y} \subseteq V(I(Y))$ gelten. Umgekehrt existiert ein Ideal A in $K[x_1, \ldots, x_n]$ mit $\overline{Y} = V(A)$. Damit erhalten wir

$$I(Y) \overset{(a)}{\supseteq} I(\overline{Y}) = I(V(A)) \overset{(b)}{\supseteq} A.$$

Bilden wir auf beiden Seiten die Nullstellenmenge so sehen wir mit Lemma 7.2.5 $V(I(Y)) \subseteq V(A) = \overline{Y}$. Also gilt Gleichheit. □

Beispiel 7.2.10. Die Inklusion in Teil (b) des eben bewiesenen Lemmas ist im Allgemeinen strikt. Betrachte das Ideal $\langle x^2 \rangle \lhd K[x_1, \ldots, x_n]$. Dann gilt

$$I(V(\langle x^2 \rangle)) = I(\{a \in K | a^2 = 0\}) = I(\{0\}) = xK[x] = \langle x \rangle \neq \langle x^2 \rangle.$$

Definition 7.2.11. Sei R ein Ring und I ein Ideal in R. Dann heißt

$$\sqrt{I} = \{\lambda \in R | \lambda^k \in I \text{ für ein } k \in \mathbb{N}\}$$

das *Radikal von* I. Ein Ideal $I \lhd R$ heißt *reduziert* falls $\sqrt{I} = I$ gilt.

Lemma 7.2.12. *Sei R ein Ring und I ein Ideal in R. Dann ist $\sqrt{I}$ ein reduziertes Ideal in R.*

Beweis. Übung. □

Proposition 7.2.13. *Sei R ein Ring und I ein Ideal in R. Dann ist $\sqrt{I}$ gleich dem Schnitt aller I umfassenden Primideale von R.*

Beweis. Sei P ein Primideal mit $I \subseteq P$ und $a \in \sqrt{I}$. Dann ist $a^k \in P$ für ein $k \in \mathbb{N}$. Da P ein Primideal ist, folgt damit auch $a \in P$. Somit ist $\sqrt{I}$ im Schnitt aller Primideale, die I enthalten.
Wir beweisen nun die andere Inklusion in dem wir zeigen, dass es zu jedem $a \notin \sqrt{I}$ ein Primideal P gibt mit $I \subseteq I$ und $a \notin P$. Dann kann dieses a nicht im Schnitt aller Primideale liegen, die I enthalten. Die Negation dieser Aussage liefert das gewünschte Resultat.
Sei also $a \in R \setminus \sqrt{I}$. Wir wenden das Zornsche Lemma 3.5.6 auf die Menge

$$S = \{J \lhd R | I \subseteq J \text{ und } a^k \notin J \text{ für alle } k \in \mathbb{N}_0\}.$$

Die Menge S ist nicht leer, da nach Wahl von a das Ideal I in S ist. Die restlichen Vorraussetzungen zeigt man mit den üblichen Argumenten. Wir erhalten ein maximales Element P in S. Natürlich ist $a \notin P$ und $I \subseteq P$. Wir müssen also nur noch zeigen, dass P ein Prmideal ist.
Seien also $b, c \in R \setminus P$. Dann gilt

$$P \subsetneq P + \langle b \rangle \quad \text{und} \quad P \subsetneq P + \langle c \rangle.$$

Da P maximal in S ist, existieren also $k, l \in \mathbb{N}$ mit $a^k \in P \subsetneq P + \langle b \rangle$ und $a^l \in P \subsetneq P + \langle c \rangle$. Daraus folgt

$$a^{k+l} \in (P \subsetneq P + \langle b \rangle)(P \subsetneq P + \langle c \rangle) \subseteq P \subsetneq P + \langle bc \rangle.$$

Es ist also $P \subsetneq P + \langle bc \rangle$ nicht in S, und somit $bc \not\in nP$. Damit ist gezeigt, dass P ein Primideal ist. □

THEOREM 7.2.14 (Hilberts Nullstellensatz). *Sei K ein algebraisch abgeschlossener Körper. Dann gilt*

(a) *Ein Ideal $M \subseteq K[x_1, \ldots, x_n]$ ist genau dann maximal, wenn es ein $\underline{a} = (a_1, \ldots, a_n) \in K^n$ gibt mit $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.*
(b) *Für jedes Ideal $A \subsetneq K[x_1, \ldots, x_n]$ gilt $V(A) \neq \emptyset$.*
(c) *Für jedes Ideal $A \subseteq K[x_1, \ldots, x_n]$ gilt $I(V(A)) = \sqrt{A}$.*

BEWEIS. Die Hauptzutat für den Beweis ist der Noethersche Normalisierungssatz.

Zu (a): $\Leftarrow$ (Für diese Richtung wird die Voraussetzung *algebraisch unabhängig* nicht benötigt.) Seien also $\underline{a} = (a_1, \ldots, a_n) \in K^n$ und $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Offensichtlich gilt $x_i \equiv a_i \mod M$ für alle $i \in \{1, \ldots, n\}$. Damit gilt

$$f(x_1, \ldots, x_n) \equiv f(a_1, \ldots, a_n) \mod M \ \forall f \in K[x_1, \ldots, x_n].$$

Insbesondere gilt also

$$f(a_1, \ldots, a_n) = 0 \Longleftrightarrow f \in M.$$

Das bedeutet gerade, dass M der Kern des Einsetzhomomorphismuses $\varphi_{\underline{a}} : K[x_1, \ldots, x_n] \longrightarrow K$, mit $f \mapsto f(\underline{a})$, ist. Da konstante Polynome auf sich selbst abgebildet werden, ist $\varphi_{\underline{a}}$ surjektiv. Der Homomorphiesatz liefert nun

$$K[x_1, \ldots, x_n]/M \cong K.$$

Somit ist M ein Maximalideal.

$\Rightarrow$ Sei nun M ein beliebiges Maximalideal von $K[x_1, \ldots, x_n]$, dann ist

$$L = K[x_1, \ldots, x_n]/M$$

ein Körper, der als K-Algebra endlich erzeugt ist. Nach Korollar 7.1.10 wissen wir, dass damit L/K eine algebraische Erweiterung des algebraisch abgeschlossenen Körpers K ist. Somit ist mit Bemerkung 3.5.3 $L \cong K$. Ein expliziter Isomorphismus ist gegeben durch $\pi|_K$, die Einschränkung der kanonischen Projektion $\pi : K[x_1, \ldots, x_n] \longrightarrow L$ auf den Körper K. (Es ist

offensichtlich, dass π_K ein injektiver Ring-Homomorphismus ist. Die Surjektivität folgt, da $\pi(K) \subseteq L$ algebraisch abgeschlossen ist.)

Dies bedeutet gerade, dass es zu jedem $f \in K[x_1, \dots, x_n]$ genau ein $a \in K$ gibt mit $\pi(f) = \pi(a)$. Seien $a_1, \dots, a_n \in K$ diejenigen Elemente mit

$$\pi(x_i) = \pi(a_i) \text{ für alle } i \in \{1, \dots, n\}.$$

Es folgt, dass $x_i - a_i \in \ker(\pi) = M$ gilt, für alle $i \in \{1, \dots, n\}$. Somit gilt

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq M.$$

In der Rückrichtung haben wir aber gesehen, dass bereits das Ideal $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ ein Maximalideal ist. Somit folgt wie gewünscht

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq M.$$

Zu (b): Sei $A \neq K[x_1, \dots, x_n]$ ein Ideal. Dann existiert ein Maximalideal M mit $A \subseteq M \overset{(a)}{=} \langle x_1 - a_1, \dots, x_n - a_n \rangle$ für gewisse $a_1, \dots, a_n \in K$. Insbesondere ist also

$$(a_1, \dots, a_n) \overset{7.2.3}{=} V(M) \overset{7.2.5}{\subseteq} V(A) \neq \emptyset.$$

Zu (c): Für ein $f \in \sqrt{A}$, gilt $f^k \in A$ für ein $k \in \mathbb{N}$. Mit Lemma 7.2.9 ist somit $f^k \in I(V(A))$. Allerdings besitzen f und f^k dieselben Nullstellen, und somit ist auch $f \in I(V(A))$.

Es bleibt zu zeigen, dass jedes $f \in I(V(A))$ auch in $\sqrt{A}$ liegt. Da dies ohne Frage für die Null gilt, sei $f \in I(V(A)) \setminus \{0\}$ beliebig. Da $K[x_1, \dots, x_n]$ noethersch ist, existieren nach Proposition 5.3.5 Elemente $g_1, \dots, g_r \in K[x_1, \dots, x_n]$ mit

$$A = \langle g_1, \dots, g_r \rangle.$$

Nun benutzen wir den *Rabinowitsch-Trick* indem wir eine weitere Variable t einführen und die Elemente $g_1, \dots, g_r$ als Elemente im Ring $K[x_1, \dots, x_n, t]$ auffassen. Wir setzen nun $B = \langle g_1, \dots, g_r, tf - 1 \rangle \lhd K[x_1, \dots, x_n, t]$. Es ist dann

$$V(B) = \{(\underline{a}, b) \in K^n \times K \mid \underbrace{g_1(\underline{a}) = \dots = g_r(\underline{a}) = 0}_{\Leftrightarrow \underline{a} \in V(A)} \text{ und } bf(\underline{a}) = 1\}$$

Angenommen es existiert ein $(\underline{a}, b) \in V(B)$. Dann muss $\underline{a} \in V(A)$ gelten, aber $f(\underline{a}) \neq 0$. Da $f \in I(V(A))$, kann ein solches $\underline{a}$ nicht

existieren. Damit ist $V(B) = \emptyset$ und mit Teil (b) schließen wir

$$B = K[x_1, \ldots, x_n, t].$$

Insbesondere existieren also $h_0, h_1, \ldots, h_r \in K[x_1, \ldots, x_n, t]$ mit

$$1 = h_1 g_1 + \ldots + h_r g_r + h_0[tf - 1]. \tag{66}$$

Wir fassen (66) als Gleichung in $(K(x_1, \ldots, x_n))[t]$ auf. Dies ist ein Polynomring in einer Variablen über einem Körper, also können wir sehr vertraut in diesem Ring rechnen. Da $f \in K(x_1, \ldots, x_n)^*$ ist, können wir auf (66) den Einsetzhomomorphismus

$$\varphi_{1/f} : (K(x_1, \ldots, x_n))[t] \longrightarrow K(x_1, \ldots, x_n) \quad ; \quad F(t) \mapsto F(1/f)$$

anwenden. Dadurch erhalten wir

$$1 = \sum_{i=1}^{r} h_i(x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}) g_i(x_1, \ldots, x_n). \tag{67}$$

Sei nun $m \in \mathbb{N}$ der größte Exponent von t, der in einem der Polynome $h_1, \ldots, h_r$ vorkommt. Dann ist $h_i(x_1, \ldots, x_n, 1/f) f^m \in K[x_1, \ldots, x_n]$ für alle $i \in \{1, \ldots, r\}$. Multiplizieren wir (67) mit f^m so erhalten wir

$$f^m = \sum_{1=1}^{r} \underbrace{h_i(x_1, \ldots, x_n, 1/f) f^m}_{\in K[x_1, \ldots, x_n]} \underbrace{g_i}_{\in A} \in A.$$

Das bedeutet gerade $f \in \sqrt{A}$, was zu zeigen war.

□

KOROLLAR 7.2.15. *Für einen algebraisch abgeschlossenen Körper K liefern die Zuordnungen I und V eine bijektive inklusionsumkehrende Korrespondenz:*

$$\{X \subseteq \mathbb{A}^n_K \textit{ Varietät}\} \underset{A \mapsto V(A)}{\overset{X \mapsto I(X)}{\rightleftarrows}} \{A \subseteq K[x_1, \ldots, x_n] \textit{reduziertes Ideal}\}.$$

BEWEIS. Per Definition ist $V(A)$ eine Varietät für alle Ideale A im Ring $K[x_1, \ldots, x_n]$. Somit ist die Abbildung V wohldefiniert. Für eine beliebige Varietät $X \subseteq \mathbb{A}^n$, ist $X = V(A)$ für ein Ideal A in $K[x_1, \ldots, x_n]$. Damit ist

$$I(X) = I(V(A)) \overset{7.2.14}{=} \sqrt{A} \tag{68}$$

nach Lemma 7.2.12 ein reduziertes Ideal. Also ist auch die Abbildung I wohldefiniert. Gleichung (68) zeigt auch, dass $I(V(A)) = A$ gilt für alle reduzierten Ideale A. In Lemma 7.2.9 wurde bereits $V(I(X)) = X$ für alle Varietäten X gezeigt. Damit ist die Aussage bewiesen. □

ABBILDUNG 7.3. Der Beweis von Hilberts Nullstellensatz mit Hilfe des Rabinowitsch-Tricks wurde vom mathematischen Physiker *George Yuri Rainich* (1886-1968) entdeckt und 1929 unter dem Pseudonym J.L. Rabinowitsch veröffentlicht.

BEMERKUNG 7.2.16. Durch Einschränkung der Abbildungen I und V aus Korollar 7.2.15 erhalten wir nach Hilberts Nullstellensatz 7.2.14 eine bijektive Korrespondenz zwischen Punkten in $\mathbb{A}_K^n$ und Maximalidealen in $K[x_1, \ldots, x_n]$.

DEFINITION 7.2.17. Sei (X, Ω) ein topologischer Raum und $Y \subseteq X$ eine Teilmenge von X.

- Dann ist Y ein topologischer Raum durch die *von X induzierte Topologie*, in der die offenen Mengen von Y genau die Mengen $\{Y \cap U | U \in \Omega\}$ sind.
- X heißt *irreduzibel*, genau dann wenn es keine echten abgeschlossenen Teilmengen $X_1, X_2 \subsetneq X$ gibt mit $X = X_1 \cup X_2$.
- X heißt *noethersch*, genau dann wenn jede echt absteigende Kette $X_1 \supsetneq X_2 \supsetneq \ldots$, von abgeschlossenen Teilmengen von X, endlich ist.

Bei noeterschen Moduln/Ringen, bricht jede echt *aufsteigende* Kette von Untermoduln/Idealen ab. Auf den ersten Blick erscheint die Definition für topologische Räume daher verwirrend. Das nächste Beispiel zeigt, dass diese Definition aus unserer Sicht doch sehr sinnvoll ist.

BEISPIEL 7.2.18. (a) Sei K ein Körper und

$$V_1 \supseteq V_2 \supseteq \ldots \tag{69}$$

eine absteigende Kette von Varietäten in $\mathbb{A}_K^n$. Mit Lemma 7.2.9 erhalten wir duch bilden der Verschwindungsideale eine aufsteigende Kette von Idealen

$$I(V_1) \subseteq I(V_2) \subseteq \ldots$$

in $K[x_1, \ldots, x_n]$. Da dieser Ring noethersch ist, wird die Kette stationär. Das heißt es existiert ein $N \in \mathbb{N}$ so dass $I(V_m) = I(V_N)$ für alle $m \geq N$ gilt. Damit ist aber auch

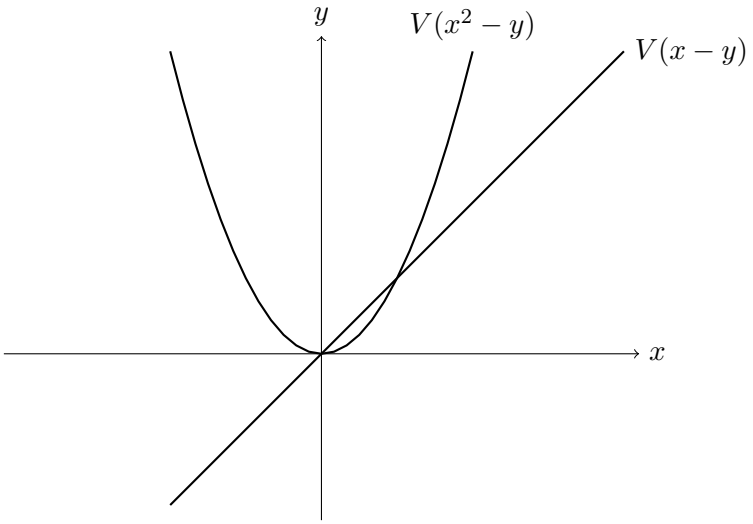
$$V_m \overset{7.2.9}{=} V(I(V_m)) = V(I(V_N)) \overset{7.2.9}{=} V_N \text{ für alle } m \geq N.$$

Damit wird auch (69) stationär und $\mathbb{A}_K^n$ ist noethersch. Dies impliziert auch sofort, dass jede Varietät X noethersch ist.

(b) Es ist $V(y^2 - x^2y - xy + x^3) \subseteq \mathbb{A}^2_{\mathbb{R}}$ nicht irreduzibel. Denn es gilt

$$\begin{aligned} V(y^2 - x^2y - xy + x^3) &= V(y(y - x^2) - x(y - x^2)) \\ &= V((y - x)(y - x^2)) = V(y - x) \cap V(y - x^2). \end{aligned}$$

Man sieht auch geometrisch, dass dass diese Varietät irreduzibel sein muss. Denn sie besteht gerade aus einer geraden und einer Parabel, wie im folgenden Bild.



(c) Für jeden Körper K ist $\mathbb{A}^n_K$ irreduzibel, wie aus der folgenden Proposition folgt. Beachte dabei, dass $I(\mathbb{A}^n_K) = I(V(0)) \overset{7.2.14}{=} \sqrt{\{0\}} = 0$. Die Bedingung *algebraisch abgeschlossen* wird in den Übungen deutlich abgeschwächt.

PROPOSITION 7.2.19. *Sei K ein Körper und $X \subseteq \mathbb{A}^n_K$ eine Varietät. Dann ist X irreduzibel genau dann wenn $I(X)$ ein Primideal ist.*

BEWEIS. Wir werden beweisen, dass X reduzibel ist, genau dann wenn $I(X)$ kein Primideal ist.

$\Longrightarrow$ Sei also $X = X_1 \cup X_2$, mit $X_1, X_2 \subsetneq X$ abgeschlossen. Dann ist mit 7.2.9 $I(X_1), I(X_2) \supsetneq I(X)$. Wir wählen nun $f \in I(X_1) \setminus I(X)$ und $g \in I(X_2) \setminus I(X)$. Dann ist auch $\langle f \rangle \subseteq I(X_1)$ und $\langle g \rangle \subseteq I(X_2)$. Insbesondere ist also $fg \in I(X_1) \cap I(X_2) = I(X_1 \cup X_2) = I(X)$. Also ist $I(X)$ kein Primideal.

$\Longleftarrow$ Sei nun $I(X)$ kein Primideal. Dann existieren $f, g \in K[x_1, \ldots, x_n] \setminus I(X)$ mit $fg \in I(X)$. Betrachte die Ideale $I(X) + \langle f \rangle$ und $I(X) + \langle g \rangle$. Es ist mit Lemma 7.2.5

$$V(I(X) + \langle f \rangle) \cup V(I(X) + \langle g \rangle) \subseteq V(I(X)) = X. \tag{70}$$

Andersherum gilt für $a \in X$ auch $(fg)(a) = f(a)g(a) = 0$, also $f(a) = 0$ oder $g(a) = 0$. Somit ist

$$a \in \begin{cases} V(I(X) + \langle f \rangle) \text{ falls } f(a) = 0 \\ V(I(X) + \langle g \rangle) \text{ falls } g(a) = 0 \end{cases}.$$

Also gilt $X \subseteq V(I(X)+\langle f\rangle)\cup V(I(X)+\langle g\rangle) \overset{(70)}{=} X$. Nach Definition sind $V(I(X) + \langle f\rangle)$ und $V(I(X) + \langle g\rangle)$ abgeschlossen. Weiter ist $V(I(X) + \langle f\rangle) \neq X \neq V(I(X) + \langle g\rangle)$, da f (beziehungsweise g) in $I(V(I(X)+\langle f\rangle))$ (beziehungsweise $I(V(I(X)+\langle g\rangle))$) aber nicht in $I(X)$ liegt. Damit ist X reduzibel.

□

KOROLLAR 7.2.20. *Für einen algebraisch abgeschlossenen Körper K liefern die Zuordnungen I und V eine bijektive Korrespondenz*

$$\{X \subseteq \mathbb{A}^n_K \textit{irreduzibel}\} \underset{A \mapsto V(A)}{\overset{X \mapsto I(X)}{\rightleftarrows}} \{A \subseteq K[x_1, \ldots, x_n] \textit{Primideal}\}.$$

BEWEIS. Wir schränken die Korrespondenz aus Korollar 7.2.15 ein und benutzen Proposition 7.2.19. □

KONSTRUKTION 7.2.21. Sei $V \subseteq \mathbb{A}^n_K$ eine Varietät. Durch Einschränken des Einsetzhomomorphismus auf V liefert jedes $f \in K[x_1, \ldots, x_n]$ eine Abbildung $f_V : V \longrightarrow K$. Für $f, g \in K[x_1, \ldots, x_n]$ gilt

$$\begin{aligned} f_V = g_V &\iff f_V - g_V = 0_V \iff (f - g)_V = 0_V \\ &\overset{Def.}{\iff} f - g \in I(V) \iff f \equiv g \mod I(V). \end{aligned}$$

Also liefern alle Elemente in ${}^{K[x_1,\ldots,x_n]}/_{I(V)}$ wohldefinierte paarweise verschiedene Abbildungen von V auf K. Der Ring $K[V] = {}^{K[x_1,\ldots,x_n]}/_{I(V)}$ heißt *Koordinatenring von V*. Mit Proposition 7.2.19 gilt

$$V \text{ irreduzibel} \iff I(V) \text{ Primideal} \iff K[V] \text{ Integritätsbereich.}$$

Für irreduzible Varietäten V haben wir also stets den *Funktionenkörper von V* gegeben durch $K(V) = Quot(K[V])$. Ist K algebraisch abgeschlossen, so ist $I(\mathbb{A}^n_K) = 0$ (siehe 7.2.18 (c)) und somit gilt $K[\mathbb{A}^n_K] = K[x_1, \ldots, x_n]$.

7.3. Dimensionstheorie

Sei **K ab jetzt** stets ein **algebraisch abgeschlossener Körper**. Im letzten Abschnitt haben wir eine Verbindung zwischen Varietäten und Idealen von Polynomringen kennengelernt. Die algebraische Geometrie beschäftigt sich unter Anderem mit der Übersetzung von geometrischen/topologischen Eigenschaften von $\mathbb{A}^n_K$ in algebraische Eigenschaften des Ringes $K[x_1, \ldots, x_n]$.

Wir werden im Folgenden Dimensionsbegriffe für topologische Rüme und für Ringe kennenlernen und zeigen, dass $\dim_{\text{top}}(\mathbb{A}^n_K) = \dim(K[x_1, \ldots, x_n]) = n$ gilt.

DEFINITION 7.3.1. Sei (X, Ω) ein topologischer Raum mit $X \neq \emptyset$. Die Dimension von X ist definiert als das Supremun aller Zahlen $n \in \mathbb{N}_0$, so dass eine Kette $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$ existiert, mit X_i abgeschlossen, irreduzibel und nicht leer für alle $i \in \{1, \ldots, n\}$. Wir bezeichnen dieses Supremum mit $\dim_{\text{top}}(X)$.

BEMERKUNG 7.3.2.

- Ist (X, Ω) ein topologischer Raum und seien U_1, $U_2 \in \Omega$ mit $U_1 \cap U_2 = \emptyset$. Dann ist $(X \setminus U_1) \cup (X \setminus U_2) = X$. Also kann X nur dann irreduzibel sein, wenn der Schnitt von zwei beliebigen nicht trivialen offenen Mengen nicht leer ist. Insbesondere kann ein Hausdorffraum nicht irreduzibel sein. Dasselbe Argument zeigt sogar, dass in einem Hausdorffraum die irreduziblen Teilmengen genau durch die einelementigen Teilmengen gegeben sind. Damit hat jeder Hausdorffraum die Dimension Null.
- Sei $Y \subsetneq X$ eine abgeschlossene Teilmenge des topologischen Raumes (X, Ω). Wir versehen Y mit der durch X induzierten Topologie. Ist nun $Y' \subseteq Y$ abgeschlossen in dieser Topologie, so ist $Y \setminus Y' = Y \cap U$ mit einem $U \in \Omega$. Damit ist dann

$$X \setminus Y' = (X \setminus Y) \cup (Y \setminus Y') = (X \setminus Y) \cup (Y \cap U) = \underbrace{(X \setminus Y)}_{\in \Omega} \cup \underbrace{U}_{\in \Omega}.$$

  Also ist Y' auch abgeschlossen in X. Damit folgt insbesondere, dass eine Teilmenge von Y irreduzibel im topologischen Raum Y ist, genau dann wenn Sie irreduzibel im topologischen Raum X ist.

  Sei nun $\dim_{\text{top}}(X) < \infty$ und X irreduzibel. Dann ist $\dim_{\text{top}}(Y) < \dim_{\text{top}}(X)$. Denn jede Kette $Y_0 \subsetneq Y_1 \subsetneq \ldots Y_n$ von abgeschlossenen irreduziblen nicht leeren Teilmengen von Y ist eine Kette von Teilmengen in X mit denselben Eigenschaften (wie gerade gezeigt). Da X irreduzibel ist, ist $Y_0 \subsetneq Y_1 \subsetneq \ldots Y_n \subsetneq X$ eine solche Kette mit einem Glied mehr. Nach Vorraussetzung ist $\dim_{\text{top}}(X)$ endlich und somit ist die Dimension von Y echt kleiner als die von X.
- Sei X noethersch. In den Übungen wird gezeigt, dass eindeutige irreduzible abgeschlossene $X_1, \ldots, X_r \subseteq X$ existieren mit $X = X_1 \cup X_2 \cup \cdots \cup X_r$. Ist nun $Y \subseteq X$ irreduzibel, so ist

$$Y = X \cap Y = (X_1 \cap Y) \cup \cdots \cup (X_r \cap Y).$$

Aus der Irreduzibilität von Y folgt, dass $Y \subseteq X_i$ für ein $i \in \{1, \dots, r\}$ gilt. Somit gilt

$$\dim_{\text{top}}(X) = \max_{1 \leq i \leq r} \{\dim_{\text{top}}(X_i)\}.$$

Wir wollen $\dim_{\text{top}}(V)$ für Varietäten V bestimmen. Dafür definieren wir eine ganz ähnliche Dimension für Ringe.

DEFINITION 7.3.3. Sei R ein Ring und P ein Primideal in R. Dann ist die *Höhe* von P, bezeichnet mit $\text{ht}(P)$, gegeben durch das Supremum aller $n \in \mathbb{N}_0$, so dass eine Kette $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$ existiert von Primidealen $P_0, \dots, P_n$ von R. Die *Krulldimension* von R ist nun $\dim(R) = \sup\{\text{ht}(P) | P \text{ Primideal in } R\}$.

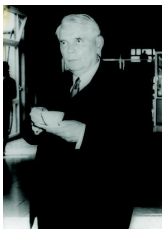


ABBILDUNG 7.4. *Wolfgang Krull* (1899 - 1971) war ein detscher Algebraiker, der Topologien auf algebraischen Strukturen einführte. Damit lässt sich unter anderem der Hauptsatz der Galoistheorie auf beliebige (nicht notwendigerweise endliche) normale und separable Körpererweiterungen verallgemeinern.

BEISPIEL 7.3.4.

- Sei R ein Hauptidealbereich, dann ist jedes Primideal auch ein Maximalideal. Damit gilt $\dim(R) \leq 1$. Es gilt für einen Hauptidealbereich genau dann $\dim(R) = 0$ wenn R ein Körper ist.
- Jede Kette von nicht leeren Varietäten in $\mathbb{A}^n_K$

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r \tag{71}$$

liefert nach Korollar 7.2.20 Eine Kette

$$I(V_0) \supsetneq I(V_1) \supsetneq \cdots \supsetneq I(V_r) \tag{72}$$

von Primidealen in $K[x_1, \dots, x_r]$. Andersherum liefert jede Kette wie in (72) durch bilden der Nullstellenmengen eine Kette von nicht leeren Varietäten in $\mathbb{A}^n_K$. Damit gilt

$$\dim_{\text{top}}(\mathbb{A}^n_K) = \dim(K[\mathbb{A}^n_K]) = \dim(K[x_1, \dots, x_n]) \geq n.$$

Um dies zu verifizieren müssen noch eine Kette von Primidealen aus $K[x_1, \dots, x_n]$ mit $n+1$ Gleidern finden. Es ist ${}^{K[x_1,\dots,x_n]}\!/_{\langle x_1,\dots,x_i \rangle} \cong K[x_{i+1}, \dots, x_n]$ ein Integritätsbereich für alle $i \in \{1, \dots, n\}$. Damit ist

$$\{0\} \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \cdots \subsetneq \langle x_1, \dots, x_n \rangle$$

eine solche Kette von Primidealen.

LEMMA 7.3.5. *Sei R ein Ring und I ein Ideal in R. Weiter sei $\pi : R \longrightarrow {}^{R}/_{I}$ die kanonische Projektion. Dann gibt es eine bijektive Korrespondenz*

$$\{P \text{ Primideal in } {}^{R}/_{I}\} \underset{Q \mapsto \pi(Q)}{\overset{P \mapsto \pi^{-1}(P)}{\rightleftarrows}} \{Q \supseteq I \text{ Primideal in } R\}.$$

BEWEIS. Sei P ein Primideal in ${}^{R}/_{I}$. Für $a, b \in R$ mit $ab \in \pi^{-1}(P)$ ist $\pi(ab) = \pi(a)\pi(b) \in P$. Da P ein Primideal ist, gilt $\pi(a) \in P$ oder $\pi(b) \in P$. Insbesondere also $a \in \pi^{-1}(P)$ oder $b \in \pi^{-1}(P)$. Es ist damit $\pi^{-1}(P)$ ein Primideal mit $I = \pi^{-1}(0) \subseteq \pi^{-1}(P)$ und die Abbildung von links nach rechts ist wohldefiniert. Weiter gilt aufgrund der Surjektivität von π auch $\pi(\pi^{-1}(P)) = P$.
Sei nun Q ein Primideal in R mit $I \subseteq Q$. Für $a, b \in {}^{R}/_{I}$ mit $ab \in \pi(Q)$ wählen wir Elemente $a', b' \in R$ mit $\pi(a') = a$ und $\pi(b') = b$. Es ist dann $ab = \pi(a')\pi(b') = \pi(a'b') \in \pi(Q)$. Es existiert also ein $q \in Q$ mit $\pi(a'b') = \pi(q)$. Das bedeutet gerade

$$a'b' - \underbrace{q}_{\in Q} \in \ker(\pi) = I \subseteq Q. \tag{73}$$

Also ist auch $a'b' \in Q$ und nach Annahme ist a' oder b' in Q. Damit gilt auch $a = \pi(a')$ oder $b = \pi(b')$ in $\pi(Q)$, somit ist $\pi(Q)$ ein Primideal und auch die Abbildung von rechts nach links ist wohldefiniert. Weiter ist natürlich $Q \subseteq \pi^{-1}(\pi(Q))$. Andererseits gilt für ein $a \in \pi^{-1}(\pi(Q))$ per Definition $\pi(a) \in \pi(Q)$ und genau wie in (73) folgt $a \in Q$. Damit gilt tatsächlich $\pi^{-1}(\pi(Q)) = Q$. □

PROPOSITION 7.3.6. *Sei V eine Varietät in $\mathbb{A}^n_K$. Dann gilt* $\dim_{\text{top}}(V) = \dim(K[V])$.

BEWEIS. Sei wieder π die kanonische Projektion von $K[x_1, \ldots, x_n]$ auf $K[V]$ und sei

$$V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_n (\subseteq V)$$

eine Kette von irreduziblen Varietäten. Dann ist mit Proposition 7.2.19 und Lemma 7.3.5

$$\pi(I(V_0)) \supsetneq \pi(I(V_1)) \supsetneq \ldots \supsetneq \pi(I(V_n)) (\supseteq \pi(I(V)) = 0)$$

eine Kette von Primidealen von $K[V]$. Damit ist $\dim_{\text{top}}(V) \leq \dim(K[V])$. Ist umgekehrt

$$(\{0\} \subseteq) P_0 \subsetneq P_1 \subsetneq \ldots P_n$$

eine Kette von Primidealen von $K[V]$ so ist mit Korollar 7.2.21 und Lemma 7.3.5

$$(V = V(I(V)) \supseteq) V(\pi^{-1}(P_0)) \supsetneq V(\pi^{-1}(P_1)) \supsetneq \ldots \supsetneq V(\pi^{-1}(P_n))$$

eine Kette von irreduziblen Varietäten in V. Damit ist auch $\dim_{\text{top}}(V) \geq \dim(K[V])$ und die Proposition folgt. □

BEMERKUNG 7.3.7. Wir wollen nun die Verbindung zwischen der Krulldimension und dem Transzendenzgrad herstellen. Sei $R \supseteq K$ ein Integritätsbereich, der als K-Algebra endlich erzeugt ist. Der Einfachheit halber werden wir im Folgenden $tr.\deg(R)$, den Transzendenzgrad von R, schreiben und damit $tr.\deg(\text{Quot}(R)/K)$ meinen. Da jede über K algebraisch unabhängige Menge $\alpha_1, \ldots, \alpha_r \in \text{Quot}(R)$ durch Multiplikation mit einem $\lambda \in R \setminus \{0\}$ zu einer über K algebraisch unabhängigen Menge in R wird, stimmt $tr.\deg(R)$ mit der Anzahl der algebraisch unabhängigen Elemente in R aus dem Noetherschen Normalisierungssatz überein.

PROPOSITION 7.3.8. *Sei R wie in 7.3.7 und $P \neq \{0\}$ ein Primideal in R. Dann ist $tr.\deg(R) > tr.\deg(R/P)$.*

BEWEIS. Da P ein Primideal ist, ist R/P ein Integritätsbereich. Weiter ist mit R auch R/P eine endlich erzeugte K-Algebra. Somit ist $tr.\deg(R/P)$ wie in 7.3.7 wohldefiniert.
Sei $\beta \in P \setminus \{0\}$ beliebig. Angenommen β wäre ganz über K. Dann ist $K[\beta]$ eine endliche Körpererweiterung von K. Insbesondere ist dann β eine Einheit in R, woraus $R = P$ folgt. Dies widerspricht der Voraussetzung, dass P ein Primideal ist. Es folgt

(74) Jedes $\beta \in P \setminus \{0\}$ ist algebraisch unabhängig über K.

Jede Menge $\alpha_1, \ldots, \alpha_r \in R$ aus algebraisch abhängigen Elementen, liefert eine algebraisch abhängige Menge der Restklassen $\overline{\alpha_1}, \ldots, \overline{\alpha_r} \in R/P$. Die Kontraposition dieser Aussage liefert sofort $tr.\deg(R) \geq tr.\deg(R/P)$.
Wir führen nun einen Widerspruchsbeweis und nehmen an, dass $tr.\deg(R) = tr.\deg(R/P) = n$ gilt. Sei dann $\overline{\alpha_1}, \ldots, \overline{\alpha_n} \in R/P$ eine Transzendenzbasis von $\text{Quot}(R/P)/K$, und $\beta \in P \setminus \{0\}$ beliebig. Dann sind die $n+1$ Elemente $\beta, \alpha_1, \ldots, \alpha_n \in R$ algebraisch abhängig über K. Es existiert also ein $f \in K[y, x_1, \ldots, x_n] \setminus \{0\}$ mit $f(\beta, \alpha_1, \ldots, \alpha_n) = 0$. Mit (74) muss mindestens eines der $x_1, \ldots, x_n$ in f vorkommen. Weiter dürfen wir damit annehmen, dass $f(y, x_1, \ldots, x_n)$ kein Vielfaches von y ist (wir dürfen f schließlich sogar als irreduzibel voraussetzen). Damit ist

$$F(x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \setminus \{0\}.$$

Nun ist aber

$$\overline{0} = \overline{f(\beta, \alpha_1, \ldots, \alpha_n)} = f(\overline{\beta}, \overline{\alpha_1}, \ldots, \overline{\alpha_n}) \overset{\beta \in P}{=} F(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) \in R/P$$

im Widerspruch zur algebraischen Unabhängigkeit von $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$. Damit folgt wie gewünscht $tr.\deg(R/P) < tr.\deg(R)$. □

KOROLLAR 7.3.9. *Sei R wie in 7.3.7, dann ist* $\dim(R) \leq tr.\deg(R)$.

BEWEIS. Unter der Voraussetzung, dass R ein Integritätsbereich ist, ist genau dann $\dim(R) = 0$ wenn $\{0\}$ das einzige Primideal - und somit auch das einzige Maximalideal - in R ist. Dies ist genau dann der Fall wenn R ein Körper ist, der nach Voraussetzung endlich erzeugt als K-Algebra ist. Mit Korollar 7.1.10 ist dies äquivalent dazu, dass R/K algebraisch ist, was wiederum gleichbedeutend mit $tr.\deg(R) = 0$ ist. Wir haben also gezeigt

$$\dim(R) = 0 \iff tr.\deg(R) = 0. \tag{75}$$

Wir beweisen das Korrolar nun per Induktion über $n = tr.\deg(R)$, wobei wir den *Induktionsanfang* $n = 0$ gerade bereits geführt haben.

Induktionsschritt: $n \geq 1$: Sei also $\{0\} = P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_m$ eine Kette von Primidealen in R. Wir dürfen nach dem Beginn des Beweises oBdA $m \neq 0$ annehmen. Sei wieder $\pi : R \longrightarrow R/P_1$ die kanonische Projektion. Nach Lemma 7.3.5 ist dann $\{\overline{0}\} = \pi(P_1) \subsetneq \pi(P_2) \subsetneq \ldots \subsetneq \pi(P_m)$ eine Kette von Primidealen in R/P_1. Damit erhalten wir

$$tr.\deg(R) \overset{7.3.8}{>} tr.\deg(R/P_1) \overset{\text{IV}}{\geq} \dim(R/P_1) \geq m - 1.$$

Das bedeutet gerade $m \leq tr.\deg(R)$. Somit besitzt jede Kette von Primidealen in R maximal $tr.\deg(R) + 1$ verschiedene Glieder (wenn wir $\{0\}$ mitzählen). Das heißt $\dim(R) \leq tr.\deg(R)$. □

THEOREM 7.3.10. *Es gilt* $\dim_{\text{top}}(\mathbb{A}^n_K) \dim(K[x_1, \ldots, x_n]) = n$.

BEWEIS. Wir haben in Beispiel 7.3.4 bereits gesehen, dass $\dim_{\text{top}}(\mathbb{A}^n_K) = \dim(K[x_1, \ldots, x_n]) \geq n$ gilt. Die Aussage folgt nun aus Korollar 7.3.9, da wir in 7.1.13 schon $tr.\deg(K[x_1, \ldots, x_n]) = n$ gesehen haben. □

Unser Ziel ist es $\dim_{\text{top}}(V) = \dim(K[V])$ für eine Varietät V zu bestimmen. Nach dem Noetherschen Normalisierungssatz ist $K[V]$ isomorph zu einer ganzen Erweiterung eines Polynomringes. Da wir die Dimension des Polynomringes gerade bestimmt haben, studieren wir im Weiteren wie sich die Dimension in ganzen Ringerweiterungen verhält.

LEMMA 7.3.11. *Sei $R \subseteq S$ eine Ringerweiterung und sei J ein (Prim-) Ideal in S. Dann ist $I = J \cap R$ ein (Prim-) Ideal von R und*

$$\varphi : R/I \longrightarrow S/J \quad ; \quad r + I \mapsto r + J$$

ist ein injektiver Ring-Homomorphismus. Damit können wir S/J stets als Ringerweiterung von R/I auffassen.

BEWEIS. Die Idealeigenschaft von J in S und die Abgeschlossenheit von R bezüglich Multiplikation, liefern sofort die Idealeigenschaft von I in R. Offensichtlich vererbt sich auch die Primidealeigenschaft von J auf I. Da $I \subseteq J$, ist $\varphi(r+i+I) = r+i+J = r+J$ für alle $i \in I$. Damit ist φ wohldefiniert und, da wir representantenweise Rechnen dürfen, folgt dass φ ein Homomorphismus ist. Weiter ist

$$\ker(\varphi) = \{r + I \in R/I | r \in J\} = \{0 + I\}$$

und damit ist φ injektiv. □

LEMMA 7.3.12. *Sei $S \supseteq R$ eine ganze Ringerweiterung, J ein Ideal in S und $I = J \cap R$. Dann ist $S/J \supseteq R/I$ eine ganze Ringerweiterung. Weiter ist $I \neq \{0\}$ falls J einen nicht-Nullteiler enthält.*

BEWEIS. Sei $a + J \in S/J$ beliebig und $\lambda_0, \ldots, \lambda_{n-1} \in R$ mit

$$0 = a^n + \lambda_{n-1}a^{n-1} + \ldots + \lambda_0. \tag{76}$$

Reduzieren wir (76) modulo J so erhalten wir eine Ganzheitsgleichung von $a + J$ mit Koeffizienten in R/I. Also ist $S/J \supseteq R/I$ ganz. Sei nun $a \in J$ kein Nullteiler und (76) die zugehörige Ganzheitsgleichung. Da a kein Nullteiler ist, ist mindestens einer der Koeffizienten $\lambda_0, \ldots, \lambda_{n-1}$ ungleich Null. Sei m kleinstmöglich mit $\lambda_m \neq 0$. Dann ist

$$0 = a^m(a^{n-m} + \lambda_{n-1}a^{n-m-1} + \ldots + \lambda_m).$$

Wir können also, wieder da a kein Nullteiler ist, oBdA $\lambda_0 \neq 0$ annehmen. Dann gilt

$$\underbrace{\lambda_0}_{\in R} = -a^n - \lambda_{n-1}a^{n-1} - \ldots - \lambda_1 a = \underbrace{a}_{\in J}(-a^{n-1} - \lambda_{n-1}a^{n-2} - \ldots - \lambda_1).$$

Insbesondere ist $0 \neq \lambda_0 \in J \cap R = I$. □

DEFINITION 7.3.13. Sei R ein Ring. Eine Teilmenge $T \subseteq R$ heißt *multiplikativ abgeschlossen*, genau dann wenn $1 \in T$ und mit $a, b \in T$ auch $ab \in T$ gilt.

BEISPIEL 7.3.14.

- Sei $a \in R$ beliebig. Dann ist $\{a^k\}_{k \in \mathbb{N}_0}$ multiplikativ abgeschlossen.
- Sei $P \subseteq R$ ein Primideal. Dann ist $R \setminus P$ multiplikativ abgeschlossen. Dies ist gerade die Definition eines Primideals. Genauso gilt für eine beliebige Menge $\{P_i\}_{i \in I}$ von Primidealen in R, dass $R \setminus (\bigcap_{i \in I} P_i)$ multiplikativ abgeschlossen ist.

LEMMA 7.3.15 (Krull-Lemma). *Sei R ein Ring, $I \subseteq R$ ein Ideal und $T \subseteq R$ multiplikativ abgeschlossen mit $I \cap T = \emptyset$. Dann existiert ein Primideal P von R mit $I \subseteq P$ und $P \cap T = \emptyset$.*

BEWEIS. In Proposition 7.2.13 haben wir den Spezialfall $T = \{a^k\}_{k\in\mathbb{N}_0}$ für $a \in R$ bewiesen. Den allgemeinen Fall beweist man wörtlich genauso. □

LEMMA 7.3.16. *Sei wieder $R \subseteq S$ eine ganze Ringerweiterung und $P \subseteq R$ ein Primideal. Für jedes $a \in P \cdot S$ existiert eine Gleichung*

$$a^n + \lambda_{n-1}a^{n-1} + \ldots + \lambda_0 = 0 \quad \textit{mit} \quad \lambda_0, \ldots, \lambda_{n-1} \in P.$$

BEWEIS. Sei $a \in P \cdot S$, dann existieren definitionsgemäß $\pi_1, \ldots, \pi_r \in P$ und $s_1, \ldots, s_r \in S$ mit $a = \sum_{i=1}^{r} \pi_i s_i$. Wir setzen $S' = R[s_1, \ldots, s_r]$. Da alle s_i ganz über R sind, ist S' nach Satz 5.2.14 ein endlich erzeugter R-Modul. Weiter ist natürlich $a \in R \cdot S'$.
Sei nun $\{\omega_1, \ldots, \omega_n\}$ ein Erzeugendensystem von S' als R-Modul. Dann ist

$$P \cdot S' = P \cdot (R\omega_1 + \ldots + \omega_n) \overset{R\cdot P=P}{=} P\omega_1 + \ldots P\omega_n.$$

Wir haben also für jedes $i \in \{1, \ldots, n\}$ eine Darstellung

$$a\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ mit } a_{ij} \in P \text{ für alle } (i,j) \in \{1, \ldots, n\}^2.$$

Ab jetzt können wir genauso argumentieren wie in 5.2.14 und zeigen, dass a Nullstelle des charakteristischen Polynoms $f(x)$ von $A = (a_{ij})$ ist. Da alle $a_{ij} \in P$ sind, liegen auch alle Koeffizienten von f in P. Damit ist das Lemma bewiesen. □

PROPOSITION 7.3.17. *Sei $R \subseteq S$ eine ganze Ringerweiterung und $P \subseteq R$ ein Primideal. Dann existiert ein Primideal $\mathfrak{P}$ von S mit $\mathfrak{P} \cap R = P$.*

BEWEIS. Sei also P ein Primideal in R und $T = R \setminus P$. Angenommen es gäbe ein $a \in P \cdot S \cap T (\subseteq R)$. Seien dann $\lambda_0, \ldots, \lambda_{n-1} \in P$ aus Lemma 7.3.16 mit

$$a^n = \underbrace{-\lambda_{n-1}a^{n-1}}_{\in P} - \ldots - \underbrace{\lambda_0}_{\in P} \in P.$$

Dann ist aber, da P als Primideal reduziert ist, auch $a \in P$ im Widerspruch zu $a \in T = R \setminus P$.
Es ist also $P \cdot S \cap T = \emptyset$ und $P \cdot S$ ein Ideal in S. Mit dem Krull-Lemma 7.3.15 existiert ein Primideal $\mathfrak{P}$ von S mit (1) $P \cdot S \subseteq \mathfrak{P}$ und (2) $\mathfrak{P} \cap T = \emptyset$. Für dieses Primideal gilt

$$P \overset{(1)}{\subseteq} \mathfrak{P} \cap R \overset{(2)}{\subseteq} P.$$

Es gilt also wie gewünscht $\mathfrak{P} \cap R = P$. □

THEOREM 7.3.18. *Sei $R \subseteq S$ eine ganze Ringerweiterung. Dann gilt für die Krulldimensionen* $\dim(R) = \dim(S)$.

BEWEIS. Sei $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_n$ eine Kette von Primidealen in S. Dann ist

$$(\mathfrak{P}_0 \cap R) \subseteq (\mathfrak{P}_1 \cap R) \subseteq \ldots \subseteq (\mathfrak{P}_n \cap R) \tag{77}$$

eine Kette von Primidealen in R. Angenommen es gilt $\mathfrak{P}_i \cap R = \mathfrak{P}_{i+1} \cap R = P$ für ein $i \in \{0 \ldots, n-1\}$. Nach Lemma 7.3.12 ist ${}^{S}\!/_{\mathfrak{P}_i} \supseteq {}^{R}\!/_{P}$ eine ganze Ringerweiterung und mit Lemma 7.3.5 ist ${}^{\mathfrak{P}_{i+1}}\!/_{\mathfrak{P}_i}$ $(= \pi(\mathfrak{P}_{i+1}))$ ein Primideal in ${}^{S}\!/_{\mathfrak{P}_i}$. Weiter ist nach Annahme

$${}^{\mathfrak{P}_{i+1}}\!/_{\mathfrak{P}_i} \cap {}^{R}\!/_{P} = {}^{\mathfrak{P}_{i+1} \cap R}\!/_{\mathfrak{P}_i \cap R} = \{0\}.$$

Also kann ${}^{\mathfrak{P}_{i+1}}\!/_{\mathfrak{P}_i}$ nach Lemma 7.3.12 nur aus Nullteilern von ${}^{S}\!/_{\mathfrak{P}_i}$ bestehen. Da letzteres ein Integritätsbereich ist, ist ${}^{\mathfrak{P}_{i+1}}\!/_{\mathfrak{P}_i} = \{0\}$, also $\mathfrak{P}_{i+1} = \mathfrak{P}_i$. Dies ist offensichtlich ein Widerspruch. Somit sind alle Inklusionen in (77) strikt und es gilt $\boxed{\dim(R) \geq \dim(S)}$.
Sei umgekehrt $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ eine Kette von Primidealen in R und $\mathfrak{P}_0$ ein Primideal in S mit $\mathfrak{P}_0 \cap R = P_0$ (existiert nach Proposition 7.3.17). Da ${}^{S}\!/_{\mathfrak{P}_0}$ ganz über ${}^{R}\!/_{P_0}$ ist, folgt wiederum mit 7.3.17 dass es ein Primideal ${}^{\mathfrak{P}_1}\!/_{\mathfrak{P}_0}$ in ${}^{S}\!/_{\mathfrak{P}_0}$ gibt, mit

$${}^{\mathfrak{P}_1}\!/_{\mathfrak{P}_0} \cap {}^{R}\!/_{P_0} = {}^{P_1}\!/_{P_0}.$$

Mit Lemma 7.3.5 folgt damit $\mathfrak{P}_1 \cap R = P_1$ und damit $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1$. Wir führen dieses Verfahren induktiv fort und erhalten eine Kette $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_n$ von Primidealen in S mit $\mathfrak{P}_i \cap R = P_i$ für alle $i \in \{1, \ldots, n\}$. Damit gilt auch $\boxed{\dim(R) \leq \dim(S)}$. Zusammen erhalten wir die Gleichheit dieser Dimensionen. □

BEMERKUNG 7.3.19. Beachte, dass ohne die Voraussetzung *S ganz über R* weder $\dim(R) \leq \dim(S)$ noch $\dim(R) \geq \dim(S)$ gilt. Dies sehen wir zum Beispiel in den Ringerweiterungen $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}[x]$, da $\mathbb{Z}$ und $\mathbb{Q}[x]$ als Hauptidealbereiche Dimension 1 haben und $\mathbb{Q}$ als Körper Dimension 0.

THEOREM 7.3.20. *Sei $V \subseteq \mathbb{A}^n_K$ eine Varietät. Dann gilt*

$$\dim_{\text{top}}(V) = \dim(K[V]) = tr.\deg(K(V)/K).$$

BEWEIS. Die erste Gleichung kennen wir bereits aus Proposition 7.3.6. Nach dem Noetherschen Normalisierungssatz 7.1.9 ist $K[V]$ isomorph zu einer ganzen Ringerweiterung eines Polynomringes $K[x_1, \ldots, x_t]$, wobei t gleich $tr.\deg(K(V)/K)$ ist. Es gilt also

$$\dim(K[V]) \overset{7.3.18}{=} \dim(K[x_1, \ldots, x_t]) \overset{7.3.10}{=} t = tr.\deg(K(V)/K).$$

□

BEISPIEL 7.3.21. Sei $V = V(y^2 - x^3 + x) \subseteq \mathbb{A}^n_{\mathbb{C}}$. Es ist $I(V) = \langle y^2 - x^3 + x \rangle$ und $\mathbb{C}[V] = {}^{\mathbb{C}[x,y]}/_{\langle y^2 - x^3 + x \rangle}$. Mit Theorem 7.3.20 ist $\dim_{\text{top}}(V) = tr.\deg K[V] \overset{7.1.19}{=} 1$. Irreduzible Varietäten von Dimension 1 heißen (erwartungsgemäß) *Kurven*.

ANHANG A

Transzendente Elemente

Hier wollen wir beweisen, dass π transzendent über den rationalen Zahlen $\mathbb{Q}$ ist. Sei stets $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von $\mathbb{Q}$, den wir als Teilkörper der komplexen Zahlen betrachten. Der Körper $\overline{\mathbb{Q}}$ besteht genau aus den Nullstellen von Polynomen aus $\mathbb{Q}[x]$. Nun gibt es aber nur abzählbar viele solche Polynome und jedes Polynom hat nur endlich viele Nullstellen. Damit besteht $\overline{\mathbb{Q}}$ aus abzählbar unendlich vielen Elementen. Da $\mathbb{C}$ bekanntermaßen überabzählbar ist, sind fast alle Elemente aus $\mathbb{C}$ transzendent über $\mathbb{Q}$. Jedoch ist es sehr schwierig ein explizites Beispiel einer transzendenten komplexen Zahl zu geben. Bevor wir uns der Transzendenz von π widmen geben wir zunächst ein einfacheres Beispiel einer über $\mathbb{Q}$ transzendenten Zahl aus $\mathbb{R}$ an.

A.1. Die Liouvillekonstante

THEOREM A.1.1 (Approximationssatz von Liouville). *Sei $\alpha \in \overline{\mathbb{Q}}$ mit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n \geq 2$. Dann existiert eine positive Konstante $c \in \mathbb{R}$, so dass $|\alpha - \frac{p}{q}| \geq \frac{c}{q^n}$ für alle $p, q \in \mathbb{Z} \setminus \{0\}$ gilt.*

BEWEIS. Nach Voraussetzung existiert ein irreduzibles Polynom $f(x) \in \mathbb{Z}[x]$ mit $\text{grad}(f) = n$ und $f(\alpha) = 0$. Wir spalten die Nullstelle α von f ab und erhalten $f(x) = (x - \alpha)g(x)$ für ein $g(x) \in \mathbb{C}[x] \setminus \mathbb{C}$. Da $g(x)$, als Funktion $\mathbb{R} \longrightarrow \mathbb{C}$; $t \mapsto g(t)$, stetig ist, existieren positive Konstanten ε und δ, so dass

$$|\alpha - t| < \varepsilon \Longrightarrow 0 \neq |g(t)| < \delta.$$

Hier haben wir neben der Stetigkeit von g auch benutzt, dass $g(x)$ nur endlich viele (genau $n - 1$) Nullstellen besitzt. Setze nun $c = \min\{\varepsilon, \delta^{-1}\}$. Angenommen es gäbe $p, q \in \mathbb{Z} \setminus \{0\}$ mit $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$. Dann ist insbesondere $|g(\frac{p}{q})| < \delta$ und somit

$$|f(\frac{p}{q})| = |\alpha - \frac{p}{q}| \cdot |g(\frac{p}{q})| < \frac{c}{q^n} \cdot \delta \leq \frac{1}{q^n}.$$

Damit ist $q^n f(\frac{p}{q}) \in \mathbb{Z}$ mit $|q^n f(\frac{p}{q})| < 1$. Dies ist nicht möglich, da nach Voraussetzung $f(\frac{p}{q}) \neq 0$ ist. Also war unsere Annahme falsch und somit ist das Theorem bewiesen. □

KOROLLAR A.1.2. *Die reelle Zahl* $L = \sum_{k=1}^{\infty} 10^{-k!}$ *ist transzendent über* $\mathbb{Q}$.

BEWEIS. Wir setzen $s_m = \sum_{k=1}^{m} 10^{-k!}$ für alle $m \in \mathbb{N}$. Dann ist s_m eine rationale Zahl mit Nenner $q = 10^{m!}$. Wäre nun L algebraisch vom Grand n, so existiert nach dem Approximationssatz A.1.1 eine Konstante $c > 0$ mit

$$|L - s_m| \geq \frac{c}{q^n} \tag{78}$$

für alle $m \in \mathbb{N}$. Wähle nun irgendein $N \in \mathbb{N}$ mit $q^{N-n+1} > c$. Dann folgt

$$\begin{aligned} |L - s_N| = \sum_{k=N+1}^{\infty} 10^{-k!} &< \sum_{k=(N+1)!}^{\infty} 10^{-k} \overset{\text{geo.R}}{=} \frac{1}{9 \cdot 10^{(N+1)!-1}} \\ &< \frac{1}{q^{N+1}} = \frac{1}{q^{N-n+1}} \cdot \frac{1}{q^n} < \frac{c}{q^n}. \end{aligned}$$

Dies ist ein Wiederspruch zu (78). Also kann L nicht algebraisch über $\mathbb{Q}$ sein. □

BEMERKUNG A.1.3. Die reelle Zahl L aus Korrolar A.1.2 heißt *Liouvillekonstante* und war die erste relle Zahl von der man die Transzendenz über $\mathbb{Q}$ beweisen konnte.

A.2. Die Kreiszahl π

ABBILDUNG A.1. Der erste Beweis der Transzendenz von π stammt von *Carl Louis Ferdinand von Lindemann* (1852 - 1939). Sein Beweis basierte auf Ideen von Charles Hermite. Angeblich soll Lindemann, nachdem er den Beweis fand, einen Freund (Oberst-Lieutenant von dem Busche) getroffen haben, der ihn mit den Worten „Sie sehen ja aus als hätten Sie die Quadratur des Kreises gelöst“ begrüßt hat. In 4.5.12 haben wir gesehen wie treffend diese Bemerkung war.

Wir werden hier einem Beweis von David Hilbert für die Transzendenz von π folgen.

LEMMA A.2.1. *Sei* $S \supseteq R$ *eine Ringerweiterung und seien* $a \in S$ *und* $\lambda_0, \ldots, \lambda_n \in R$ *mit* $\lambda_n \neq 0$ *und* $\lambda_n a^n + \cdots + \lambda_0 = 0$. *Dann ist* $\lambda_n a$ *ganz über* R.

BEWEIS. Aus $\lambda_n a^n + \cdots + \lambda_0 = 0$ folgt sofort

$$\begin{aligned} 0 &= \lambda_n^{n-1}\lambda_n a^n + \lambda_n^{n-1}\lambda_{n-1}a^{n-1} + \ldots + \lambda_n^{n-1}\lambda_0 \\ &= (\lambda_n a)^n + \lambda_{n-1}(\lambda_n a)^{n-1} + \lambda_{n-2}\lambda_n(\lambda_n a)^{n-2} + \ldots + \lambda_0\lambda_n^{n-1}. \end{aligned}$$

Also ist $\lambda_n a$ ganz über R. □

LEMMA A.2.2. *Seien $a_1, \ldots, a_n$ sämtliche Nullstellen eines Polynoms aus $\mathbb{Q}[x]$. Weiter sei $g(x) \in \mathbb{Q}(a_1, \ldots, a_n)[x]$ symmetrisch in $a_1, \ldots, a_n$ (d.h.: Schreiben wir $g(x) = \widehat{g}(a_1, \ldots, a_n, x)$, mit $\widehat{g} \in \mathbb{Q}[x_1, \ldots, x_n, x]$, dann ist $g(x) = \widehat{g}(a_{\sigma(1)}, \ldots, a_{\sigma_n}, x)$ für alle $\sigma \in S_n$). Dann ist $g(x) \in \mathbb{Q}[x]$.*

BEWEIS. Es ist $g(x) = f_k(a_1, \ldots, a_n)x^k + \ldots + f_0(a_1, \ldots, a_n)$ mit $f_0, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]$. Dann ist nach Voraussetzung

$$f_i(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) = f_i(a_1, \ldots, a_n) \text{ für alle } \sigma \in S_n \text{ und alle } i \in \{0, \ldots, k\}.$$

Weiter ist $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}$ als Zerfällungskörper eine Galoiserweiterung (beachte $\mathrm{char}(\mathbb{Q}) = 0$) und es gilt mit Lemma 4.3.9, $\mathrm{Gal}(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}) \subseteq S_n$. Insbesondere ist also jedes $f_i(a_1, \ldots, a_n)$ invariant unter allen Elementen aus $\mathrm{Gal}(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q})$. Theorem 4.3.4 liefert nun wie gewünscht $f_i(a_1, \ldots, a_n) \in \mathbb{Q}$ für alle $i \in \{0, 1 \ldots, k\}$. □

LEMMA A.2.3. *Sei $f \in \mathbb{R}[x]$ mit $\mathrm{grad}(f) = m$ und sei $z \in \mathbb{C}$ beliebig. Dann gilt*

$$I(f; z) = \int_0^1 z e^{z(1-u)} f(zu) \mathrm{d}u = e^z \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z).$$

Weiter gilt $|I(f; z)| \leq |z|e^{|z|} \sup_{u \in [0,1]} |f(uz)|$. Hier und im Folgenden bezeichnet $f^{(j)}$ die j-te Ableitung von f.

BEWEIS. Die Betragsabschätzung ist trivial. Die andere Aussage beweisen wir per Induktion über m, wobei für $f = 0$ nichts zu zeigen ist. Für den Induktionsanfang $m = \mathrm{grad}(f) = 0$, also $f = c \in \mathbb{R}^*$ rechnen wir leicht nach

$$\int_0^1 z e^{z(1-u)} f(zu) \mathrm{d}u = cze^z \int_0^1 e^{-zu} \mathrm{d}u = ce^z - c.$$

Für $\mathrm{grad}(f) \geq 1$ liefert partielle Integration

$$\begin{aligned} I(f; z) &= \left[-e^{z(1-u)} f(zu) \right]_0^1 + \int_0^1 e^{z(1-u)} z f^{(1)}(zu) \mathrm{d}u \\ &= -f(z) + e^z f(0) + I(f^{(1)}; z). \end{aligned}$$

Da $\mathrm{grad}(f^{(1)}) = m - 1 < m$ gilt, können wir die Induktionsvoraussetzung anwenden, woraus die Behauptung folgt. □

LEMMA A.2.4. *Ist $f \in \mathbb{Z}[x]$ ein Polynom und $n \in \mathbb{N}$. Dann existiert ein $f_1 \in \mathbb{Z}[x]$ mit $f^{(n)}(x) = n! f_1(x)$.*

BEWEIS. Die Ableitung ist linear. Daher genügt es die Behauptung für Monome $f(x) = x^k$, $k \in \mathbb{N}_0$, zu beweisen. Für $n > k$ ist $f^{(n)} = 0$ und somit

können wir $f_1 = 0$ wählen. Für $n \leq k$ gilt

$$f^{(n)} = k(k-1)\cdots(k-n+1)x^{k-n} = \frac{k!}{(k-n)!}x^{k-n} = n!\underbrace{\binom{k}{n}}_{\in\mathbb{Z}}x^{k-n}.$$

Damit hat $f_1(x) = \binom{k}{n}x^{k-n} \in \mathbb{Z}[x]$ die gewünschte Eigenschaft. □

THEOREM A.2.5. *Die Kreiszahl π ist transzendent.*

BEWEIS. Wir führen einen Widerspruchsbeweis und nehmen an, dass π algebraisch über $\mathbb{Q}$ ist. Dann ist auch $a_1 := i\pi$ algebraisch über $\mathbb{Q}$.
Seien $a_1, \ldots, a_s \in \mathbb{C}$ sämtliche Nullstellen des Minimalpolynoms $m_{a_1,\mathbb{Q}}(x) \in \mathbb{Q}[x]$. Mit der Eulergleichung $e^{i\pi} + 1 = 0$ erhalten wir

$$0 = \prod_{j=1}^{s}(1 + e^{a_j}) = \sum_{\epsilon_1=0}^{1}\cdots\sum_{\epsilon_s=0}^{1} e^{\epsilon_1 a_1 + \cdots + \epsilon_s a_s}.$$

Bezeichne mit $b_1, \ldots, b_r$ die von Null verschiedenen Exponenten der rechten Seite, dann gilt

$$0 = e^{b_1} + \cdots + e^{b_r} + c, \text{ mit } c \in \mathbb{N}. \tag{79}$$

Da mindestens einer der Exponenten gleich Null ist ($\epsilon_1 = \cdots = \epsilon_n = 0$), ist c tatsächlich ungleich 0, also insbesondere $c \geq 1$. Die Elemente $0, b_1, \ldots, b_r$ sind genau die Nullstellen des Polynoms

$$g(x) = \prod_{\epsilon_1=0}^{1}\cdots\prod_{\epsilon_s=0}^{1}(x - (\epsilon_1 a_1 + \cdots + \epsilon_s a_s)) \in \mathbb{Q}[a_1, \ldots, a_s, x].$$

Dieses Polynom ist offensichtlich symmetrisch in $a_1, \ldots, a_s$. Somit folgt aus Lemma A.2.2 $g(x) \in \mathbb{Q}[x]$. Wähle nun ein $d \in \mathbb{Z}$ so, dass $d \cdot g(x) \in \mathbb{Z}[x]$. (z.B. können wir d als ein kgV aller Nenner der Koeffizienten von $g(x)$ wählen). Per Definition ist 0 genau eine c-fache Nullstelle von $d \cdot g(x)$ (siehe (79)). Spalten wir die Nullstelle 0 also c-mal ab, so stellen wir fest, dass die Elemente $b_1, \ldots, b_r$ genau die Nullstellen sind von

$$h(x) = \frac{d \cdot g(x)}{x^c} = c_r x^r + \cdots + c_1 x + c_0 \in \mathbb{Z}[x] \text{ mit } c_r = d > 0 \text{ und } c_0 \neq 0.$$

Für ein beliebiges $n \in \mathbb{N}$ definieren wir nun das Polynom

$$f_n(x) = \frac{c_r^{rn-1}}{(n-1)!}x^{n-1}(h(x))^n \in \mathbb{Q}[x].$$

Es ist $\operatorname{grad}(f_n) = rn + n - 1$. Wenden wir nun Lemma A.2.3 an für $f = f_n$ und $z = b_k$, $k \in \{1, \dots, r\}$, so erhalten wir

$$\begin{aligned}\sum_{k=1}^{r} I(f_n; b_k) &= \sum_{k=1}^{r} r \int_0^1 b_k e^{b_k(1-u)} f_n(b_k u)\mathrm{d}u \\ &= \sum_{k=1}^{r} e^{b_k} \sum_{j=0}^{rn+n-1} f_n^{(j)}(0) - \sum_{k=1}^{r} \sum_{j=0}^{rn+n-1} f_n^{(j)}(b_k) \\ &= -c \sum_{j=0}^{rn+n-1} f_n^{(j)}(0) - \sum_{k=1}^{r} \sum_{j=0}^{rn+n-1} f_n^{(j)}(b_k). \qquad (80)\end{aligned}$$

Diese Gleichung wollen wir für ein geeignet gewähltes $n \in \mathbb{N}$ auf einen Widerspruch führen. Untersuchen wir zunächst die rechte Seite von (80). Betrachten wir die konstanten Terme von den Ableitungen von f_n, so erhalten wir

$$f_n^{(l)}(0) = \begin{cases} 0 & \text{für } l \in \{0, \dots, n-2\} \\ c_r^{rn-1} c_0^n & \text{für } l = n-1 \\ c_r^{rn-1} n m_l & \text{für } l \geq n \end{cases}$$

für gewisse $m_l \in \mathbb{Z}$ für alle $l \geq n$ (es ist m_l ein ganzzahliges Vielfaches eines Koeffizientens von $h(x)^n$). Insbesondere ist damit

$$\sum_{j=0}^{rn+n-1} f_n^{(j)}(0) = c_r^{rn-1} c_0 + n \underbrace{\sum_{j=n}^{rn+n-1} c_r^{rn-1} m_j}_{=:m \in \mathbb{Z}}. \qquad (81)$$

Weiter ist $f_n^{(l)}(b_k) = 0$ für alle $k \in \{1, \dots, r\}$ und alle $l \in \{0, \dots, n-1\}$, da b_k eine n-fache Nullstelle von f_n ist.

Für $l \geq n$ ist nach Lemma A.2.4 die l-te Ableitung von $x^{n-1}(h(x))^n$ durch $l!$, also auch durch $n!$, teilbar. Zu jedem $l \geq n$ existiert also ein Polynom $\tilde{f}_{n,l}(x) \in \mathbb{Z}[x]$ mit $f_n^{(l)}(x) = n \cdot c_r^{rn-1} \tilde{h}_{n,l}(x)$. Wir setzen

$$\tilde{h}_n = \sum_{j=n}^{rn+n-1} \tilde{f}_{n,j} \in \mathbb{Z}[x] \text{ mit } \operatorname{grad}(\tilde{h}_n) = nr - 1.$$

Damit gilt

$$\sum_{k=1}^{r} \sum_{j=0}^{rn+n-1} f_n^{(j)}(b_k) = \sum_{k=1}^{r} \sum_{j=n}^{rn+n-1} f_n^{(j)}(b_k) = n \sum_{k=1}^{r} c_r^{nr-1} \tilde{f}_n(b_k). \qquad (82)$$

Die Summe auf der rechten Seite von (82) ist symmetrisch in $b_1, \dots, b_r$, also insbesondere $\operatorname{Gal}(\mathbb{Q}(b_1, \dots, b_r)/\mathbb{Q})$-invariant. Mit Theorem 4.3.4 ist also $\sum_{k=1}^{r} c_r^{nr-1} \tilde{f}_n(b_k) \in \mathbb{Q}$. Da $\operatorname{grad}(\tilde{f}_n) = rn - 1$ ist, ist diese Summe auch ein Element in $\mathbb{Z}[c_r b_1, \dots, c_r b_k]$. Weiter ist jedes b_k Nullstelle von $h(x)$, und

c_r war genau der Leitkoeffizient von $h(x)$. Mit Lemma A.2.1 sind somit $c_r b_1, \ldots, c_r b_r$ ganzüber $\mathbb{Z}$. Insbesondere ist

$$\sum_{k=1}^{r} c_r^{nr-1} \tilde{f}_n(b_k) =: \tilde{m} \in \mathbb{Z}. \tag{83}$$

Setzen wir nun die Gleichungen (81), (82) und (83) in (80) ein, so erhalten wir

$$\begin{aligned}
\sum_{k=1}^{r} I(f_n; b_k) &\overset{(80)}{=} -c \sum_{j=0}^{rn+n-1} f_n^{(j)}(0) - \sum_{k=1}^{r} \sum_{j=0}^{rn+n-1} f_n^{(j)}(b_k) \\
&\overset{(81)}{=} -cc_r^{rn-1} c_0 - cnm - \sum_{k=1}^{r} \sum_{j=0}^{rn+n-1} f_n^{(j)}(b_k) \\
&\overset{(82)}{=} -cc_r^{rn-1} c_0 - cnm - n \sum_{k=1}^{r} c_r^{nr-1} \tilde{f}_n(b_k) \\
&\overset{(83)}{=} \underbrace{-cc_r^{rn-1} c_0}_{\neq 0} - n(cm + \tilde{m}) \in \mathbb{Z}.
\end{aligned}$$

Für jedes $n \in \mathbb{N} \setminus \{1\}$ mit $\mathrm{ggT}(cc_r c_0, n) = 1$ ist somit

$$\left| \sum_{k=1}^{r} I(f_n; b_k) \right| \geq 1. \tag{84}$$

Auf der anderen Seite liefert uns die Abschätzung aus Lemma A.2.3 eine Konstante $M > 0$, die nicht von n abhängt, mit $|I(f_n; b_k)| \leq {}^{M^n}/_{(n-1)!}$ für alle $k \in \{1, \ldots, r\}$. Dies sehen wir in dem wir $R = \max_{1 \leq k \leq r} |b_k| e^{|b_k|}$ und $C = \sup_{|z| \leq R} \{|zh(z)|\}$ setzen. Dann gilt die Behauptung für $M = c_r^r CR$. Damit gilt aber

$$\left| \sum_{k=1}^{r} I(f_n; b_k) \right| \leq \sum_{k=1}^{r} |I(f_n; b_k)| \leq \frac{rM^n}{(n-1)!} \xrightarrow{n \to \infty} 0.$$

Wir können also $n \in \mathbb{N}$ mit $\mathrm{ggT}(cc_r c_0, n) = 1$ genügend groß wählen mit $|\sum_{k=1}^{r} I(f_n; b_k)| < 1$. Dies ist ein Widerspruch zu (84). Somit kann $i\pi$ nicht algebraisch über $\mathbb{Q}$ sein. Somit ist π transzendent über $\mathbb{Q}$. □

Mit ganz ähnlichen Argumenten kann man allgemeiner das folgende Theorem beweisen, was unter anderem auch die Transzendenz von e impliziert. Für einen Beweis verweisen wir auf [**Ja**], Kapitel 4.12.

THEOREM A.2.6 (Lindemann-Weierstraß Theorem). *Seien $a_1, \ldots, a_n$ algebraisch über $\mathbb{Q}$ und linear unabhängig über $\mathbb{Q}$. Dann sind die Elemente $e^{a_1}, \ldots, e^{a_n}$ algebraisch unabhängig über $\mathbb{Q}$.*

ABBILDUNG A.2. Den Beweis von Theorem A.2.6 skizzierte von Lindemann bereits in seiner Arbeit über die Transzendenz von π. Er schloss diese Arbeit mit „Eine genauere Darlegung der hier nur angedeuteten Beweise behalte ich mir für eine spätere Veröffentlichung vor“. Da dies nicht passierte, vervollständigte *Karl Weierstraß* (1815-1897) (den alle aus der Analysis kennen) den Beweis.

Literaturverzeichnis

[Bo] Bosch, S.; *Algebra*. 4. überarbeitete Auflage; Springer-Verlag Berlin (2001)

[Br] Brüdern, J.; *Einführung in die analytische Zahlentheorie*; Springer-Verlag Berlin Heidelberg (1995)

[Ja] Jacobson, N.; *Basic Algebra I*, Second Edition; W.H. Freeman and Company San Francisco (1985)

[JS] Jantzen, J. und Schwermer, J.; *Algebra*; Springer-Verlag Berlin Heidelberg (2006)

[MFO] `http://owpdb.mfo.de/` (Stand: 12.11.2014)

[St] Stroth, G.: *Algebra: Einführung in die Galoistheorie*; Berlin, New York: de Gruyter (1998)

[Vo] Völklein, H.; *Groups as Galois groups: an introduction*. Cambridge Studies in Advanced Mathematics **53**; Cambridge University Press (1996)