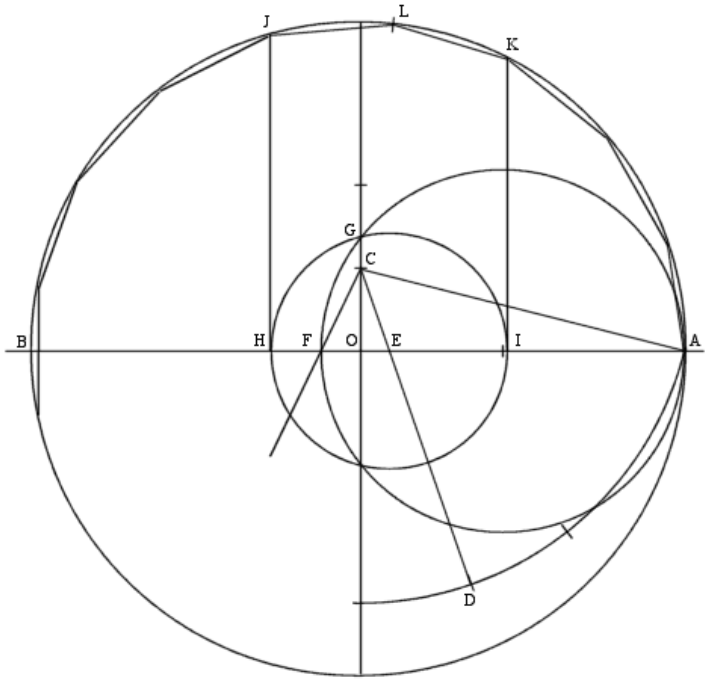
Skript zur Vorlesung

Algebra (4std.)



Wintersemester 2012/13
Frankfurt am Main

Prof. Dr. Martin Möller

Inhaltsverzeichnis

Vorwort

Dies ist ein Skript[1] zu einer Vorlesung „Algebra“ in Frankfurt/Main im WS 2012/13. Sie baut auf einer Vorlesung „Grundlagen der Algebra“ auf, in der Begriffe wie Gruppen, Gruppenoperationen, Bahnformel, Ringe, Ideale insbesondere der Polynomring, faktorielle Ringe und Hauptidealringe eingeführt wurden. Diese Begriffe werden vorausgesetzt und höchstens knapp wiederholt. Der Leser sei auf die Literatur, insbesondere das Skript von Philipp Habegger zur Vorlesung im SS 2012 verwiesen.

Quellen und Literatur: Literatur zur Algebra gibt es viel. Diese Vorlesung wurde zumeist folgenden Büchern entnommen:

- S.Bosch: „Algebra“ (Springer)
- M.Artin: „Algebra“ (Birkhäuser)
- J.Wolfart: „Einführung in die Zahlentheorie und Algebra“ (Viehweg)

Weiterführendes zu diesem Thema findet man z.B. bei

- S. Lang: „Algebra“ (Addison-Wesley)

[1] Titelbild: http://www.jimloy.com/geometry/17-gon.htm

1 Einführung

Algebra bedeutet Rechnen mit Gleichungen, heutzutage vielleicht das, was man mit Termumformungen übersetzen würde. Gleichungen sind dabei, in Abgrenzung zur Analysis, stets polynomielle Gleichungen wie z.B.

$$x^5 + 2x + 13 = 0$$

oder in 3 Veränderlichen

$$x^n + y^n = z^n$$

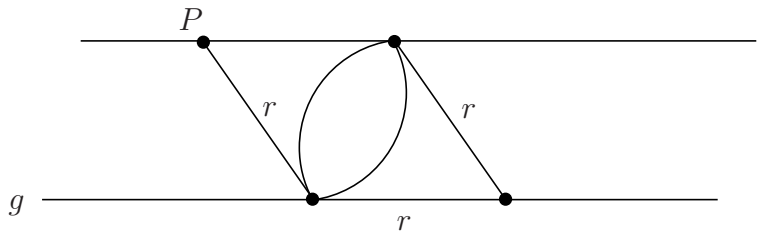
für ein festes $n \geqslant 0$. Lösen will man diese Gleichungen in einem Ring, z.B. ist die Lösbarkeit der zweiten Gleichung oben für $n \geqslant 3$ im Ring $\mathbb{Z}$ Fermats Problem, seit 1994 ein Satz von Wiles. Oder man sucht Lösungen in einem Körper. In der Tat gewinnt man aus jeder Lösung $(x, y, z) \in \mathbb{Z}^3$ der Fermat-Gleichung - mit Ausnahme von $x = y = z = 0$ eine Lösung von $x^n + y^n - 1 = 0$ in den rationalen Zahlen, nämlich $\left(\frac{x}{z}, \frac{y}{z}\right)$, falls $z \neq 0$ ist und analog in den anderen Fällen. Umgekehrt liefert jede Lösung $(q_1, q_2) \in \mathbb{Q}^2$ von $x^n + y^n - 1 = 0$ eine Lösung der Fermat-Gleichung in ganzen Zahlen, indem man mit dem Hauptnenner durchmultipliziert. Die Fermat-Gleichung wird uns noch häufig wiederbegegnen, auch wenn der Wiles'sche Beweis weit außer Reichweite dieser Vorlesung ist.

Konstruktionen mit Zirkel und Lineal. Das folgende Problem der Griechen hat über Jahrhunderte die Algebra, insbesondere die Körpertheorie motiviert. Es ist heutzutage kaum mehr wichtig, aber schön genug, um auch hier als Motivation zu dienen. Wir werden es im Rahmen der Vorlesung vollständig verstehen.
Die Griechen fragten sich, welche Punkte der Ebene man ausgehend von $(0, 0)$ und $(1, 0)$ mit Zirkel und Lineal konstruieren kann. Erlaubt sind dabei Geraden durch zwei bereits konstruierte Punkte, das Abtragen einer Strecke (zwischen konstruierten Punkten) auf einer Geraden, Kreise mit bereits konstruiertem Mittelpunkt und Radius, sowie Schnittpunkte solcher Geraden und Kreise.
Wir fassen die Punkte (x, y) der Ebene als komplexe Zahlen $z = x + iy$ auf und fragen, welche $z \in \mathbb{C}$ konstruierbar sind. Ist $\sqrt{\pi}$ konstruierbar (Quadratur des Kreises)? Ist $\sqrt[3]{2}$ konstruierbar, die Seite eines Würfels mit Volumen 2 (Delisches Problem)? Für welche n ist das regelmäßige n-Eck konstruierbar?
Den geometrischen Teil dieses Problems lösen wir vorweg.

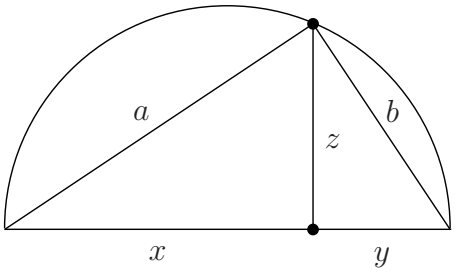
Satz 1.1 *Die konstruierbaren Punkte bilden einen Körper $F_{\sqrt{\ }} \subseteq \mathbb{C}$. Dies ist der kleinste Teilkörper von $\mathbb{C}$, der zu jedem $z \in F_{\sqrt{\ }}$ auch $\sqrt{z}$ enthält.*

Die Frage, welche der oben genannten Zahlen in $F_{\sqrt{}}$ liegen, beantworten wir im Hauptteil dieses Skripts, in dem auch alle Begriffe nochmals sorgfältig definiert werden.

Beweis : Durch Abtragen kann man Streckenlängen addieren. Mit Zirkel und Lineal kann man Parallelen konstruieren. Mittels des Strahlensatzes kann man al-



so Gleichungen der Form $\frac{a}{b} = \frac{x}{y}$ bei drei gegebenen Größen lösen. Also ist $F_{\sqrt{}}$ ein Körper. Aus dem Thales-Kreis über eine Strecke der Länge $x + y$ folgt aus



$x^2 + z^2 = a^2,\ y^2 + z^2 = b^2$ und $a^2 + b^2 = (x + y)^2$ der Höhensatz

$$x \cdot y = z^2$$

und damit die Behauptung, dass $F_{\sqrt{}}$ die Wurzel aus allen $z \in F_{\sqrt{}}$ enthält.
Schließlich ist der Schnittpunkt von zwei Kreisen, von Geraden und Kreis oder zwei Geraden stets durch eine Gleichung vom Grad höchstens zwei (mit Koeffizienten in bereits konstruierten Längen) gegeben. Dies zeigt, dass $F_{\sqrt{}}$ nichts enthält, was nicht aus Quadratwurzeln und Körperoperation entsteht, also dass $F_{\sqrt{}}$ der kleinste Körper mit den genannten Eigenschaften ist. □

2 Körper und Körpererweiterungen

Ringe $(R, +, \cdot)$ haben in diesem Skript stets ein Einselement bzgl. der Multiplikation und sind kommutativ. Ein Ring heißt *nullteilerfrei*, falls aus $a \cdot b = 0$ folgt $a = 0$ oder

$b = 0$. Ein Ring heißt *Körper*, falls $(R \setminus \{0\},\ \cdot\ )$ eine Gruppe ist. Sind $L \subseteq K$ beides Körper, so nennen wir L einen *Teilkörper* von K und K eine *Körpererweiterung* von L. („Oberkörper“ und „Unterkörper“ sind unübliche Begriffe hierfür.)

2.1 Primkörper und Körperhomomorphismen

Da ein Ringhomomorphismus (per Definition) stets 1 auf 1 abbildet, gibt es zu jedem Körper K genau einen Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow K.$$

Der Kern von φ ist also ein Ideal und es ist $\mathbb{Z}/\ker(\varphi) \hookrightarrow K$, also ist $\mathbb{Z}/\ker(\varphi)$ nullteilerfrei. Folglich ist $\ker(\varphi)$ ein Primideal, also $\ker(\varphi) = \{0\}$ oder $\ker(\varphi) = (p)$, für eine Primzahl p. Wir nennen dementsprechend 0 oder p die *Charakteristik* des Körpers. Ein *Körperhomomorphismus* ist ein *Ringhomomorphismus* zwischen zwei Körpern. Ein solcher ist stets injektiv. Zwei Körper K_1, K_2 sind *isomorph*, wenn es Körperhomomorphismen $\varphi\colon K_1 \longrightarrow K_2$ und $\psi\colon K_2 \longrightarrow K_1$ mit $\psi \circ \varphi = \mathrm{id}_{K_1}$ und $\varphi \circ \psi = \mathrm{id}_{K_2}$ gibt. Man prüft leicht, dass dies äquivalent zur Existenz eines surjektiven Homomorphismus $\varphi\colon K_1 \longrightarrow K_2$ ist. Ist $K_1 = K_2$, so nennt man φ einen *Automorphismus*. Der Durchschnitt aller Teilkörper von K ist stets nichtleer (da $\{0, 1\}$ darin enthalten sind) und außerdem ein Körper. Er wird *Primkörper* von K genannt.

Proposition 2.1 *Sei $P \subseteq K$ der Primkörper von K. Dann gilt:*

i) Ist $\mathrm{char}(K) = p > 0$, so ist $P \cong \mathbb{F}_p$ (mit p prim).

ii) Ist $\mathrm{char}(K) = 0$, so ist $P \cong \mathbb{Q}$.

Zur Erinnerung: $\mathbb{F}_p = (\mathbb{Z}/(p), +,\ \cdot\ )$ ist ein Körper, da jedes $\overline{k} \neq \overline{0}$ ein Inverses besitzt, welches man mit dem erweiterten Euklid´schen Algorithmus findet.

Beweis : Für den kanonischen Homomorphismus $\varphi\colon \mathbb{Z} \longrightarrow K$ gilt $\mathrm{Im}(\varphi) \subseteq P$. Ist $\mathrm{char}(p) > 0$, so ist $\mathbb{Z}/(p) \cong \mathrm{Im}(\varphi)$ bereits ein Körper. Dies zeigt 2.1 i). Andernfalls ist φ injektiv und daher $P^0 = \left\{\frac{a}{b},\ a \in \mathrm{Im}(\varphi),\ b \in \mathrm{Im}(\varphi) \setminus \{0\}\right\} \subseteq K$ ein zu $\mathbb{Q}$ isomorpher Körper. Dies ist der kleinste Körper, der $\mathrm{Im}(\varphi)$ enthält und jeder Teilkörper enthält $\mathrm{Im}(\varphi)$ und damit P^0. Also ist $P = P^0 \cong \mathbb{Q}$. □

Beispiel 2.2 Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind aus der Vorlesung „Lineare Algebra“ bekannt. Wir betrachten die Menge (lies: $\mathbb{Q}$ adjungiert $\sqrt{2}$).

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b \cdot \sqrt{2} \colon a, b \in \mathbb{Q}\right\} \subseteq \mathbb{C}.$$

Diese Menge ist ein Körper, denn sie ist offenbar unter Addition und Multiplikation abgeschlossen und das Inverse von $a + b\sqrt{2}$ ist

$$\left(a + b\sqrt{2}\right)^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \cdot \sqrt{2}.$$

Wir hätten diesen Körper auch ohne das Wissen über $\mathbb{R}$ und $\mathbb{C}$ einführen können, indem wir $\sqrt{2}$ als formales Symbol betrachten, das uns daran erinnert, dass sein Quadrat $2 \in \mathbb{Q}$ ist. Diesen Standpunkt werden wir im folgenden Abschnitt ausführlich verwenden.
Wir bestimmen noch die Körperhomomorphismen $\varphi \colon \mathbb{Q}\left[\sqrt{2}\right] \longrightarrow \mathbb{Q}\left[\sqrt{2}\right]$. Eine Möglichkeit ist natürlich $\varphi = \mathrm{id}$. Eine weitere Möglichkeit ist durch $\varphi\left(\sqrt{2}\right) = -\sqrt{2}$ gegeben. In der Tat ist φ damit eindeutig festgelegt, denn $\varphi(1) = 1$, also $\varphi\left(a + b\sqrt{2}\right) = a + b\varphi\left(\sqrt{2}\right)$.
Dies sind alle Möglichkeiten, denn ist $\varphi\left(\sqrt{2}\right) = c + d\sqrt{2}$, so muss $2 = \varphi(2) = \varphi\left(\sqrt{2}\right) \cdot \varphi\left(\sqrt{2}\right) = c^2 + 2d^2 + 2cd\sqrt{2}$ sein. Ist $d = 0$, so $c^2 = 2$, was in $\mathbb{Q}$ keine Lösung hat und ist $c = 0$, so ist $d \in \{\pm 1\}$ und wir sind bei den oben genannten Fällen.

Übung 2.3 Ist $\mathrm{char}(K_1) \neq \mathrm{char}(K_2)$, so gibt es keine Körperhomomorphismen von K_1 nach K_2.

Ist die Charakteristik von K nicht Null, so gibt es einen Homomorphismus, der ganz anders aussieht als im obigen Beispiel. Er basiert auf dem folgenden Lemma.

Lemma 2.4 *Ist F ein Körper mit $\mathrm{char}(F) = p > 0$, so gilt für alle $a, b \in F$ und $r \in \mathbb{N}$:*

$$(a + b)^{p^r} = a^{p^r} + b^{p^r}, \ (a - b)^{p^r} = a^{p^r} - b^{p^r}.$$

Beweis : Per Induktion genügt es $r = 1$ zu betrachten. Es ist

$$(a + b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p \quad \text{und} \quad \binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Der Zähler ist durch p teilbar, der Nenner nicht, da p prim und $1 \leq i \leq p - 1$. Also sind alle mittleren Terme gleich Null in $\mathbb{F}$. □

Daher ist für alle F mit $\mathrm{char}(F) = p > 0$ die Abbildung

$$\tau_p \colon F \longrightarrow F, a \longmapsto a^p$$

ein Körperhomomorphismus, genannt *Frobenius-Homomorphismus*.

2.2 Quotientenkörper

Das Verfahren, mit dem man aus dem Ring $\mathbb{Z}$ den Körper $\mathbb{Q}$ gewonnen hat, lässt sich auf beliebige nullteilerfreie Ringe R anwenden. Es wird wichtige Beispiele (und oft gute Gegenbeispiele) von Körpern definieren. Der Leser denke im Folgenden an $R = K[X]$ den Polynomring über dem Körper K und beobachte, was bei der Präsenz von Nullteilern (also z.B. bei $R = \mathbb{Z} \times \mathbb{Z}$) schiefgeht.
Auf der Menge der Paare $\{(a, b), a \in R, b \in R \setminus \{0\}\}$ führen wir die Relation

$$(a_1, b_1) \sim (a_2, b_2) \Longleftrightarrow a_1 b_2 - a_2 b_1 = 0$$

ein. Reflexivität und Symmetrie dieser Relation sind offensichtlich. Zur Transitivität betrachten wie 3 Paare auf $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$. Dann gibt $a_1 b_2 = a_2 b_1$ und $a_2 b_3 = a_3 b_2$, also $a_1 b_2 b_3 = b_1 a_3 b_2$ oder $b_2(a_1 b_3 - b_1 a_3) = 0$. Da nach Voraussetzung $b_2 \neq 0$ und R nullteilerfrei ist, folgt das gewünschte $a_1 b_3 - b_1 a_3 = 0$. Wir schreiben die Äquivalenzklassen von Paaren (a, b) sofort wie gewohnt als Brüche $\frac{a}{b}$.

Proposition 2.5 *Ist R nullteilerfrei, so bilden die Menge aller Äquivalenzklassen $\frac{a}{b}, a \in R, b \in R \setminus \{0\}$ mit der obigen Äquivalenzrelation $\sim$ und der üblichen Addition und Multiplikation*

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

einen Körper, genannt der Quotientenkörper *von R, Schreibweise $Q(R)$.*

In der obigen Konstruktion werden die „Nenner“ b_i stets multipliziert, nirgends wird die Addition benötigt. Erlaubt man als Nenner alle Ringelemente in einer Teilmenge $S \subseteq R$ mit $0 \notin S$, die multiplikativ abgeschlossen ist (Beispiele hierfür für $R = \mathbb{Z}$? Übung!), so ist $\sim$ wiederum eine Äquivalenzrelation. Man erhält aber im Allgemeinen keinen Körper, sondern nur einen Ring, die *Lokalisierung* von R nach S.

Übung 2.6 Wie kann man die Definition der Relation verallgemeinern, sodass sie auch in der Gegenwart von Nullteilern noch eine Äquivalenzrelation ist?

2.3 Endliche und algebraische Körpererweiterungen

Eine *Körpererweiterung* ist eine Inklusion von Körpern $K \hookrightarrow L$, die wir häufig als L/K schreiben. Insbesondere kann man die Multiplikation $L \times L \longrightarrow L$ im ersten

Argument auf K einschränken und erhält eine Abbildung $K \times L \longrightarrow L$, die L zu einem K-Vektorraum macht. Wir werden uns im Folgenden für *Zwischenkörper*, d.h. für Körper E mit $K \subseteq E \subseteq L$ interessieren.

Definition 2.7 *Wir nennen die Dimension von L als K-Vektorraum den* Grad *von L/K, in Zeichen $[L : K]$. Wir nennen L/K* endlich *bzw.* unendlich*, je nachdem ob $[L : K]$ endlich oder unendlich ist.*

Satz 2.8 *Sind $K \subseteq E \subseteq L$ Körpererweiterungen, so gilt*

$$[L : E] \cdot [E : K] = [L : K],$$

wobei der Fall unendlicher Körpererweiterungen mit den offensichtlichen Konventionen eingeschlossen ist.

Beweis : Es sei $B = \{x_i | i \in I\}$ und $C = \{y_j | j \in J \ldots\}$ eine Basis von L/E bzw. von E/K. Wir zeigen, dass die Menge $D = \{x_i y_j,\ i \in I,\ j \in J\}$ linear unabhängig ist und, im Falle $m = \#B < \infty$ und $n = \#C < \infty$, eine Basis von L/K.
Seien also endlich viele $c_{ij} \in K$ gegeben mit $\sum c_{ij}(x_i \cdot y_j) = 0$. Wir gruppieren um und erhalten

$$\sum_i \left(\sum_j (c_{ij} y_j) \right) x_i = 0$$

Die Koeffizienten vor den x_i liegen in E und die x_i sind E-linear unabhängig. Also ist für alle i

$$\sum_j c_{ij} y_j = 0.$$

Aus der K-linearen Unabhängigkeit der y_j folgt $c_{ij} = 0$ für alle i und j.
Um zu zeigen, dass die $x_i y_j$ den K-Vektorraum L aufspannen, nehmen wir $z \in L$ beliebig her. Dann gibt es $b_i \in E$ mit $\sum b_i x_i = z$. Die b_i wiederum können wir als $b_i = \sum_j c_{ij} \cdot y_j$ mit $c_{ij} \in K$ schreiben. Insgesamt ist $z = \sum c_{ij} x_i y_j$. □

Ist L/K eine Körpererweiterung und $\alpha \in L$, so gibt es genau einen Ringhomomorphismus

$$\varphi_\alpha : K[X] \longrightarrow L,\ \varphi_\alpha(X) = \alpha,$$

genannt der *Einsetzungshomomorphismus*. In der Tat erzwingt die Homomorphie, dass $\varphi_\alpha(X^n) = \alpha^n$ und damit $\varphi_\alpha \left(\sum_{n \geqslant 0} b_n X^n \right) = \sum_{n \geqslant 0} b_n \alpha^n$.

Definition 2.9 *Das Element $\alpha \in L$ heißt* algebraisch über K, *falls* $\mathrm{Ker}(\varphi_\alpha) \neq \{0\}$, *d.h. falls es eine Gleichung der Form*

$$\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0$$

mit $c_i \in K$ gibt. Andernfalls heißt α transzendent über K. *Wir nennen L/K* algebraisch, *falls jedes $\alpha \in L$ algebraisch über K ist.*

Zum Beispiel ist $\alpha = \sqrt[7]{5} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, denn es ist $\alpha^7 - 5 = 0$. Es ist nicht leicht zu zeigen, dass ein α transzendent über $\mathbb{Q}$ ist, d.h. dass eine Gleichung mit Koeffizienten in $\mathbb{Q}$ noch so hohen Grades niemals α annulliert. Wir werden später sehen, dass π und e in der Tat transzendent über $\mathbb{Q}$ sind.
Der Ring $K[X]$ ist nach [GA] eine Hauptidealring. Also ist $\mathrm{Ker}(\varphi_\alpha) = \langle f_\alpha \rangle$ von einem Element f_α erzeugt. Ist α algebraisch, so ist f_α nicht null und bis auf K^*-Vielfache eindeutig bestimmt. Wir normieren f_α immer so, dass der höchste Koeffizient gleich 1 ist. Offenbar ist f_α das Polynom kleinsten Grades (ungleich Null) mit der Eigenschaft $f_\alpha(\alpha) = 0$. Wir nennen f_α das *Minimalpolynom* von α. Es ist $K[X]/\langle f_\alpha \rangle \hookrightarrow L$ ein Teilkörper. Denn da L nullteilerfrei ist, ist auch $K[X]/\langle f_\alpha \rangle$ nullteilerfrei. Also ist f_α prim und somit irreduzibel nach [GA]. Wir halten fest:

Proposition 2.10 *Das Minimalpolynom eines algebraischen Elements $\alpha \in L$ ist irreduzibel und der von α erzeugte Unterring $\varphi_\alpha(K[X]) \subseteq L$ ist ein Körper, isomorph zu $K[X]/\langle f_\alpha \rangle$ und mit*

$$[K[\alpha] : K] = \deg(f_\alpha) =: n$$

Beweis : Jedes von Null verschiedene Primideal in $K[X]$ ist maximal, also ist $K[X]/\langle f_\alpha \rangle$ ein Körper, via φ_α zu $K[\alpha]$ isomorph. Die Dimensionsaussage zeigen wir für $K[X]/\langle f_\alpha \rangle$. Sei x die Restklasse von X. Offenbar erzeugt $\{1, x, x^2, \ldots, x^{n-1}\}$ diesen K-Vektorraum, denn ist $g \in K[X]$, so ist nach Polynomdivision

$$g = q \cdot f_\alpha + r \quad \text{mit } \deg(r) \leq n - 1,$$

also $g = r$ in $K[X]/\langle f_\alpha \rangle$. Andererseits ist diese Menge auch linear unabhängig, denn sonst gäbe es eine nichttriviale Linearkombination $\sum_{i=0}^{n-1} b_i X^i \in \langle f_\alpha \rangle$, im Widerspruch zu $\deg f_\alpha = n$. □

Proposition 2.11 *Jede endliche Körpererweiterung L/K ist algebraisch.*

Beweis : Es sei $n = [L : K]$ und $\alpha \in L$. Dann sind die $(n+1)$ Elemente $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^n$ linear abhängig über K. Folglich gibt es eine nichttriviale Relation

$$\sum_{i=0}^{n} c_i \alpha^i = 0,$$

was zu zeigen war. □

Es ist nicht richtig, dass jede algebraische Erweiterung endlich ist. Bevor wir dies zeigen, einige Zwischenschritte.
Sei L/K eine Körpererweiterung und $A = \{\alpha_i, i \in I\}$ eine Teilmenge von L. Wir bezeichnen mit $K(A)$ den kleinsten Teilkörper von L, der K und alle α_i enthält, genannt der von A erzeugte Körper. Er enthält alle Ausdrücke der Form

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \quad \text{mit } f, g \in K[X_1, \ldots, X_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \quad \text{und } \alpha_1, \ldots, \alpha_n \in A.$$

Definition 2.12 *Die Körpererweiterung L/K heißt* endlich erzeugt, *falls es eine endliche Menge A gibt mit $L = K(A)$.*

Proposition 2.13 *Sei $L = K(\alpha_1, \ldots, \alpha_n)$ endlich erzeugt. Sind $\alpha_1, \ldots, \alpha_n$ algebraisch über K, so ist $L = K[\alpha_1, \ldots, \alpha_n]$ eine endliche und damit algebraische Erweiterung von K.*

Beweis : Wir schließen per Induktion nach n. Für $n = 1$ ist die Aussage in Proposition 2.10 enthalten. Per Induktion können wir annehmen, dass $K[\alpha_1, \ldots, \alpha_{n-1}]$ eine endliche Körpererweiterung von K ist und dass $K[\alpha_1, \ldots, \alpha_n]$ ein Körper und endlich über $K[\alpha_1, \ldots, \alpha_{n-1}]$ ist, folgt wiederum aus Proposition 2.10. Nach Satz 2.8 ist also $K[\alpha_1, \ldots, \alpha_n]$ endlich über K. □

Als Übung überlege man, wie man algorithmisch das Minimalpolynom von $\alpha + \beta$ über $\mathbb{Q}$ bestimmt, wenn man die Minimalpolynome von α und β kennt. Die obige Proposition besagt, dass dies möglich ist!

2.4 Irreduzibilitätskriterien

Zur Bestimmung von Körpergraden muss man regelmäßig testen, ob ein Kandidat für ein Minimalpolynom wirklich das Minimalpolynom ist, also irreduzibel ist. Dazu hier zwei nützliche Tests.

Sei hierzu R ein faktorieller Ring. Dann besitzt jedes Element $\frac{a}{b} \in Q(R) \setminus \{0\}$ eine eindeutige Darstellung

$$\frac{a}{b} = u \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdots p_n^{\varepsilon_n},$$

wobei $u \in R^*$ ist $n \geqslant 0$, $p_1, \ldots, p_n$ paarweise verschiedene irreduzible Element und $\varepsilon_i \in \mathbb{Z} \setminus \{0\}$. Ist p irreduzibel, so definieren wir die *p-Bewertung* von $\frac{a}{b}$ als $\nu_p\left(\frac{a}{b}\right) = \varepsilon_i$, falls $p = p_i$, $\nu_p\left(\frac{a}{b}\right) = 0$ sonst.
Wir erweitern diese Definition auf Polynome, indem wir für $f = \sum a_i x^i \in Q(R)[X]$ definieren

$$\nu_p(f) = \min_i \ \nu_p(a_i).$$

Offenbar ist $f \in R[X]$, falls $\nu_p(f) \geqslant 0$ für alle irreduziblen p. Wir nennen $f \in R[X] \setminus R$ primitiv, falls $\nu_p(f) = 0$ für alle irreduziblen p. Jedes $f \in Q(R)[X]$ lässt sich durch Durchmultiplizieren mit dem „Hauptnenner“ als $f = a \cdot \widetilde{f}$ mit $f \in R[X]$ primitiv schreiben. Die Zahl

$$a = \prod_{p \text{ irreduzibel}} p^{\nu_p(f)}$$

und $\widetilde{f} = a^{-1} \cdot f$ leisten offenbar das Verlangte. Unser Ziel ist folgender Satz von Gauß.

Satz 2.14 *Sei R faktoriell. Dann ist auch $R[X]$ faktoriell. Ein Polynom $q \in R[X]$ ist genau dann irreduzibel, wenn entweder $q \in R$ ist und irreduzibel in R oder q primitiv in $R[X]$ ist und irreduzibel in $Q(R)[X]$. Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann irreduzibel in $R[X]$, wenn es irreduzibel in $Q(R)[X]$ ist.*

Vor dem Beweis zeigen wir die Nützlichkeit des Satzes im Fall $R = \mathbb{Z}$ anhand des folgenden sogenannten Eisenstein-Kriteriums.

Satz 2.15 *Sei R ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv. Sei $p \in R$ irreduzibel mit*

$$p \nmid a_n, \ p \mid a_i \quad \textit{für} \quad i < n \quad \textit{und} \quad p^2 \nmid a_0$$

Dann ist f irreduzibel in $R[X]$ und (nach dem Satz von Gauß) auch in $Q(R)[X]$.

Beispiel 2.16 Sei p eine Primzahl. Das Polynom $f(X) = X^{p-1} + X^{p-2} + \ldots + 1$ ist irreduzibel in $\mathbb{Q}[X]$, denn $f(X) = (X^p - 1)/(X - 1)$, also ist

$$\begin{aligned} f(X+1) &= \left((X+1)^p - 1\right)/X \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1}. \end{aligned}$$

und dieses Polynom genügt den Voraussetzungen des Eisenstein-Kriteriums.

Beweis von Satz 2.15 : Angenommen $f = g \cdot h$ mit $g = \sum_{i=0}^{r} b_i x^i$ und $h = \sum_{i=0}^{s} c_i x^i$ mit $r > 0$ und $s > 0$. Dann ist offenbar $r + s = n$. Es folgt

$$\begin{aligned} a_n &= b_r \cdot c_s, \quad p \nmid b_r, \qquad p \nmid c_s \\ a_0 &= b_0 \cdot c_0, \quad p \mid b_0 \cdot c_0, \quad p^2 \nmid b_0 \cdot c_0. \end{aligned}$$

Nach eventueller Vertauschung der Rollen von g und h können wir annehmen, dass $p \mid b_0$ und $p \nmid c_0$. Sei t der maximale Index, sodass $p \mid b_\tau$ für alle $0 \leqslant \tau \leqslant t$. Nach dem oben gesagten gibt es ein solches t und $t < r$. Es ist

$$a_{t+1} = b_{t+1} \cdot c_0 + b_t \cdot c_1 + \ldots + b_0 \cdot c_{t+1},$$

wobei wir $c_i = 0$ für $i > s$ der einfacheren Schreibweise wegen definieren. Nach Definition von t sind $b_0 \cdot c_{t+1}, b_1 \cdot c_t, \ldots, b_t c_1$ alle durch p teilbar, aber $b_{t+1} \cdot c_0$ nicht. Also ist a_{t+1} nicht durch p teilbar, folglich $t + 1 = n$, also $r = n$ und $s = 0$, im Widerspruch zur Annahme über g und h. □

Wir kommen zurück zum Beweis des Satzes von Gauß und starten mit folgender Hilfsaussage.

Lemma 2.17 *Sei R faktoriell und p irreduzibel. Dann gilt für $f, g \in Q(R)[X]$ die Gleichheit der p-Bewertungen*

$$\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g).$$

Beweis : Für $f \in Q(R)$ ein konstantes Polynom und $g \in Q(R)[X]$ beliebig ist die Aussage offenbar richtig, ebenso für $f = 0$ oder $g = 0$, wobei man die übliche Konvention $\min(\{\}) = \infty$ benutze.
Mit dieser Vorüberlegung kann man den allgemeinen Fall nach Durchmultiplizieren mit dem Hauptnenner auf $f, g \in R[X]$ reduzieren. Man kann nun noch statt f und g die Polynome $f/p^{\nu_p(f)}$ und $g/p^{\nu_p(g)}$ betrachten, welche $\nu_p(f) = 0 = \nu_p(g)$ haben. Wir müssen $\nu_p(f \cdot g) = 0$ zeigen. Hierzu betrachten wir den Homomorphismus

$$\chi : R[X] \longrightarrow (R/pR)[X],$$

welcher jeden Koeffizienten des Polynoms auf seine Restklasse modulo p abbildet. Es ist

$$\ker(\chi) = \{f \in R[X] : \quad \nu_p(f) > 0\}.$$

Es ist also $\chi(f) \neq 0$ und $\chi(g) \neq 0$ und wenn $0 = \chi(f \cdot g) = \chi(f) \cdot \chi(g)$ wäre, so wäre $(R/pR)[X]$ nicht nullteilerfrei, im Widerspruch zu [GA, Lemma 2.6]. □

Beweis des Satzes 2.14 : Im Fall i) eines irreduziblen Elements q in R ist R/qR integer und damit auch $(R/qR)[X] \cong R[X]/qR[X]$ ein Integritätsring. Also ist q prim in $R[X]$. Wir wissen noch nicht, dass $R[X]$ faktoriell ist, also folgt in $R[X]$ dass ‚prim' die Eigenschaft ‚irreduzibel' hat, aber die Umkehrung ist erst am Ende des Beweises klar.
Im Fall ii) ist nachzuweisen, dass ein primitives $q \in R[X]$, prim in $Q(R)[X]$ auch prim in $R[X]$ ist. Seien $f, g \in R[X]$ und es gelte $q \mid f \cdot g$. Dann gilt diese Teilbarkeit auch in $Q(R)[X]$, also folgt, dass (ohne Einschränkung) $q \mid f$ gilt. Dies besagt, dass es $h \in Q(R)[X]$ gibt mit $f = q \cdot h$. Wir müssen zeigen, dass $h \in R[X]$. Dabei hilft uns das vorangegangene Lemma. Für jedes Primelement $p \in R$ gilt

$$0 \leq \nu_p(f) = \nu_p(q) + \nu_p(h) = \nu_p(h),$$

wobei die letzte Gleichheit verwendet, dass q primitiv ist. Damit ist $h \in R[X]$ und eine Implikation der zweiten Aussage ist bewiesen.
Der Beweis der umgekehrten Implikation sowie der ersten Aussage folgt, wenn wir zeigen, dass ein $0 \neq f \in R[X] \setminus R[X]^*$ in ein Produkt von Elementen wie in i) und ii) zerfällt, denn von diesen haben wir bereits nachgewiesen, dass sie prim in $R[X]$ sind und so müssen wir Eindeutigkeit der Zerlegung nicht explizit zeigen.
Sei dazu $f = a \cdot \widetilde{f}$ mit $a \in R$ und $\widetilde{f}$ primitiv.
Da R faktoriell ist, können wir a als Produkt von Primelementen vom Typ i) schreiben und müssen uns nur noch um $\widetilde{f}$ kümmern. Sei

$$\widetilde{f} = c\widetilde{f_1} \cdot \ldots \cdot \widetilde{f_r}$$

eine Zerlegung in Primelemente in $Q(R)[X]$ und $c \in Q(R)^*$, was wir im faktoriellen Ring $Q(R)[X]$ immer erreichen können. Wir können durch geeignete Wahl von c erreichen, dass alle $\widetilde{f_i} \in R[X]$ liegen und dort primitiv sind. Es bleibt zu zeigen, dass bei dieser Wahl $c \in R^*$ ist. Aufgrund des vorangehenden Lemmas gilt für alle $p \in R$

$$\nu_p(\widetilde{f}) = \nu_p(c) + \nu_p(\widetilde{f_1}) + \ldots + \nu_p(\widetilde{f_r})$$

und die Voraussetzung ‚primitiv' impliziert

$$\nu_p(\widetilde{f}) = \nu_p(\widetilde{f_1}) = \ldots = \nu_p(\widetilde{f_r}) = 0.$$

Also ist $\nu_p(c) = 0$ für alle p und damit ist $\widetilde{f} = (c\widetilde{f_1}) \cdot \widetilde{f_2} \cdot \ldots \cdot \widetilde{f_r}$ die gewünschte Zerlegung. Die letzte Behauptung folgt unmittelbar aus ii). □

Nach dem Ende des Exkurses in die Ringtheorie kommen wir noch einmal auf Irreduzibilitätskriterien zurück.

Im Beweis des Satzes von Gauß und damit implizit beim Eisensteinkriterium haben wir die Reduktionsabbildung modulo p verwendet. Wir halten diese nützliche Idee nochmal fest.

Proposition 2.18 *Sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ primitiv und $p \in \mathbb{Z}$ prim mit $p \nmid a_n$. Ist $\overline{f} \in \mathbb{F}_p[X]$, die koeffizientenweise Reduktion von f, in $\mathbb{F}_p[X]$ irreduzibel, so ist f in $\mathbb{Q}[X]$ irreduzibel.*

Beweis : Koeffizientenreduktion ist ein Homomorphismus

$$\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p)\mathbb{Z}[X] = \mathbb{F}_p[X].$$

Ist also $f = g \cdot h$ reduzibel, so ist $\overline{f} = \overline{g} \cdot \overline{h}$. Die Irreduzibilität von $\overline{f}$ impliziert, dass ohne Einschränkung $\overline{g} \in \mathbb{F}_p$ ein konstantes Polynom ist. Dann aber ist jeder Koeffizient von g außer dem Konstantglied durch p teilbar, insbesondere der führende Koeffizient. Dann ist auch a_n durch p teilbar, im Widerspruch zur Voraussetzung. □

Beispiel 2.19 Das Polynom $f = X^3 + 3X^2 - 4X - 1 \in \mathbb{Q}[X]$ ist irreduzibel, denn seine Reduktion modulo 3 ist $\overline{f} = X^3 - X - 1$ und dieses Polynom ist irreduzibel in $\mathbb{F}_3[X]$. Man beachte, dass es zum Nachweis der Irreduzibilität bei Polynomen von Grad 3 genügt zu prüfen, dass das Polynom keine Nullstelle besitzt.

2.5 Der algebraische Abschluss

Wir beantworten zunächst die Frage aus Abschnitt 2.3 nach einer nicht-endlichen algebraischen Erweiterung. Sei dazu

$$\mathbb{Q}^{\text{alg}} = \{\alpha \in \mathbb{C} : \alpha \text{ ist algebraisch über } \mathbb{Q}\}.$$

Die Menge $\mathbb{Q}^{\text{alg}}$ ist offenbar ein Körper, der $\mathbb{Q}$ enthält. Wir nennen $\mathbb{Q}^{\text{alg}}$ den algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$, einem Körper, dessen Existenz wir aus der linearen Algebra voraussetzen. Per Definition ist $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ algebraisch. Angenommen $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = n < \infty$. Dann betrachten wir das Polynom $f = X^{n+1} - p \in \mathbb{Q}[X]$. Nach dem Eisensteinkriterium ist es irreduzibel. Der Körper $L = \mathbb{Q}[X]/\langle f \rangle$ hat Grad $n+1$ über $\mathbb{Q}$ und vermöge des Homomorphismus mit $X \longmapsto \sqrt[n+1]{p}$ ist L ein Teilkörper von $\mathbb{Q}^{\text{alg}}$. Dies steht im Widerspruch zur Gradvoraussetzung. Dabei haben wir den „Fundamentalsatz der Algebra“verwendet, der besagt, dass jedes Polynom in $\mathbb{Q}[X]$ über $\mathbb{C}$ eine Nullstelle hat.

Ziel dieses Abschnitts ist die allgemeine Konstruktion eines Körpers, der zum einen das leistet, was $\mathbb{C}$ für Polynome in $\mathbb{Q}[X]$ leistet -nämlich dass jedes Polynom eine Nullstelle besitzt- und der zum anderen minimal unter solchen Körpern ist. $\mathbb{C}$ leistet dies nicht, sondern der oben beschriebene Körper $\mathbb{Q}^{\text{alg}}$, wie wir weiter unten sehen werden.

Definition 2.20 *Ein Körper K heißt* algebraisch abgeschlossen, *falls jedes Polynom $f \in K[X] \setminus K$ eine Nullstelle besitzt.*

Offenbar kann man die Definition induktiv nach Abdividieren eines Linearfaktors anwenden und erhält, dass jedes nicht konstante Polynom über einem algebraisch abgeschlossenen Körper in Linearfaktoren zerfällt. Die Bezeichnung rechtfertigt die folgende Proposition.

Proposition 2.21 *Ein Körper K ist genau dann algebraisch abgeschlossen, wenn für jede algebraische Körpererweiterung L/K gilt $L = K$.*

Beweis : Nehmen wir an, K sei algebraisch abgeschlossen und $\alpha \in L \setminus K$. Dann zerfällt das Minimalpolynom von α über K in Linearfaktoren $f_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i)$. Also ist $n = 1$ und $\alpha_1 = \alpha \in K$, da f_α irreduzibel ist. Zur Umkehrung sei $f \in K[X]$ irreduzibel. Wir würden gerne eine algebraische Erweiterung L/K konstruieren, in der f eine Nullstelle α hat. Dies leistet die folgende Proposition. Dann aber ist wegen $L = K$ die Nullstelle α bereits in K und die Bedingung für K algebraisch abgeschlossen geprüft. □

Die folgende Konstruktion von algebraischen Erweiterungen, in denen wir erzwingen, dass ein gegebenes Polynom f eine Nullstelle hat, wird auch als Kronecker-Verfahren oder „Adjunktion einer Nullstelle von f“ bezeichnet.

Proposition 2.22 *Sei K ein Körper und $f \in K[X]$ irreduzibel vom Grad $\geqslant 1$. Dann gibt es eine endliche algebraische Erweiterung L/K, sodass f eine Nullstelle in L hat. Konkret leistet $L = K[X]/\langle f \rangle$ das Verlangte.*

Beweis : Da f irreduzibel ist, ist $\langle f \rangle \subseteq K[X]$ ein maximales Ideal und damit L ein Körper. Dieser enthält offenbar K und X (oder genauer gesagt, die Restklasse $\overline{X}$ von X modulo $\langle f \rangle$) ist eine Nullstelle von f in L, denn $f(\overline{X}) = \overline{f(X)} = \overline{0}$). Außerdem ist $\{1, X, X^2, \ldots, X^{\deg(f)-1}\}$ eine K-Basis von L, was die Endlichkeit der Erweiterung zeigt. □

Um einen algebraischen Abschluss eines gegebenen Körpers K zu konstruieren, müssten wir also nacheinander das Verfahren von Kronecker auf alle irreduziblen Polynome anwenden. Dabei müssen wir auch noch kontrollieren, dass die Elemente, die in Erweiterungskörpern hinzukommen zur Konstruktion von anderen irreduziblen Polynomen verwendet werden können. Darauf müssen wir wieder das Kronecker-Verfahren anwenden usw. Die Konstruktion eines algebraischen Abschlusses ist also in der Hauptsache ein mengentheoretisches Problem.

Satz 2.23 *Jeder Körper K besitzt einen algebraisch abgeschlossenen Erweiterungskörper L.*

Vor dem Beweis erinnern wir an das Zorn'sche Lemma (siehe [LA]): Ist M eine (partiell) geordnete Menge und hat jede total geordnete Teilmenge von M eine obere Schranke, so besitzt M ein maximales Element. Damit zeigen wir:

Proposition 2.24 *Sei R ein Ring und $a \subsetneqq R$ ein echtes Ideal. Dann besitzt R ein maximales Ideal $m \supseteq a$.*

Beweis : Sei M die Menge aller Ideale, die a enthalten, geordnet bezüglich Inklusion. $M \neq \emptyset$, da $a \in M$. Ist $N \subseteq M$ total geordnet, so zeigen wir, dass $c = \bigcup_{b \in N} b$ ein Ideal ist. Dies folgt daraus, dass alle Idealaxiome nur endlich viele Elemente involvieren. Konkret sei $\gamma_1, \gamma_2 \in c$, also $\gamma_1 \in b_1$ und $\gamma_2 \in b_2$ für $b_1, b_2 \in N$. Dann gibt es wegen der Totalordnung ein b_3, das b_1 und b_2 enthält. Also ist $\gamma_1 \in b_3, \gamma_2 \in b_3, \gamma_1 + \gamma_2 \in b_3$ wegen des ersten Idealaxioms und damit $\gamma_1 + \gamma_2 \in c$. Die anderen Axiome zeigt man genauso. Das Zorn'sche Lemma liefert also ein maximales Element, notwendigerweise das gesuchte maximale Ideal. □

Beweis des Satzes 2.23 : Um auf alle irreduziblen Polynome in K gleichzeitig das Verfahren von Kronecker anzuwenden, benutzen wir einen Polynomring in unendlich vielen Variablen. Seien $\mathcal{X} = (X_f)_{f \in I}$ eine Menge von Variablen, indiziert durch

$$I = \{f \in K[X] : \deg(f) \geqslant 1\}$$

und sei $K[\mathcal{X}]$ der Polynomring in diesen Variablen. Darin liegt das Ideal (erzeugt von unendlich vielen Elementen)

$$a = \langle f(X_f) : f \in I \rangle,$$

erzeugt von den Polynomen $f \in I$, angewandt jeweils auf die „eigene" Variable X_f. Zur Anwendung der vorigen Proposition müssen wir zeigen, dass $a \subsetneqq K[\mathcal{X}]$ ist.

Wäre das nicht der Fall, also $1 \in a$, so gäbe es $f_1, \ldots, f_n \in I$ und $g_1, \ldots, g_n \in K[\mathcal{X}]$ mit

$$\sum_{i=1}^{n} g_i f_i(X_{fi}) = 1. \tag{1}$$

Wir wenden nun das Kronecker-Verfahren (endlich oft!) auf die Polynome $f_1, \ldots, f_n$ an, so dass diese Polynome in einem Erweiterungskörper L Nullstellen $\alpha_i, i = 1, \ldots, n$ haben. Da 1 eine Gleichheit von Polynomen $\in K[\mathcal{X}]$ ist, können wir sie auch als Gleichheit von Polynomen in $L[\mathcal{X}]$ auffassen. Es folgt, dass beide Seiten auch noch gleich sind, wenn wir für die Variablen beliebige Konstanten in L einsetzen, also α_i für X_{f_i}. Dann aber erhalten wir $0 = 1$, der gewünschte Widerspruch.

Sei $m \subseteq K[\mathcal{X}]$ ein maximales Ideal, das a enthält, welches nach der vorigen Proposition existiert. Dann ist $L_1 = K[\mathcal{X}]/m$ ein Erweiterungskörper von $K = L_0$ und alle Polynome in $K[X] \backslash K$ haben eine Nullstelle in L_1. Wir iterieren dieses Verfahren und konstruieren L_{i+1} wie oben aus L_i, sodass alle Polynome in $L_i[X]$ eine Nullstelle in L_{i+1} haben. Schließlich definieren wir

$$L = \bigcup_{n=0}^{\infty} L_n$$

und müssen noch zeigen, dass L in der Tat algebraisch abgeschlossen ist. Sei dazu $f \in L[X] \setminus L$. Das Polynom hat nur endlich viele Koeffizienten, die folglich allesamt in einem L_n liegen, also $f \in L_n[X]$. Also hat f eine Nullstelle in L_{n+1} und damit in L. □

Korollar 2.25 *Sei K ein Körper. Dann gibt es eine algebraische Körpererweiterung $\overline{K}/K$, sodass $\overline{K}$ algebraisch abgeschlossen ist.*

Beweis : Wir konstruieren mit dem vorigen Satz eine algebraisch abgeschlossene Körpererweiterung L/K und setzen (wie im Fall $L = \mathbb{C}$)

$$\overline{K} = \{\alpha \in L \colon \alpha \text{ ist algebraisch über } K\}.$$

Dann ist $\overline{K}$ ein Körper, da für α und β algebraisch auch $-\alpha, \alpha^{-1}, \alpha + \beta$ und $\alpha \cdot \beta$ algebraisch über K sind. Außerdem ist $\overline{K}$ algebraisch abgeschlossen, denn wenn $f \in \overline{K}[X] \setminus \overline{K}$ ist, so hat f eine Nullstelle $\alpha \in L$. α ist also algebraisch über $\overline{K}$, also algebraisch über der endlichen Körpererweiterung von K, die man durch Adjunktion der Koeffizienten von f erhält und damit algebraisch über K, also $\alpha \in \overline{K}$. □

Ein algebraischer Abschluss von $\mathbb{Q}$ ist nicht $\mathbb{C}$, sondern ein echter Teilkörper $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Das liegt daran, dass z.B. $\pi \in \mathbb{C}$ transzendent über $\mathbb{Q}$ ist, wie wir später sehen werden. Bereits jetzt kann man sich leicht überlegen, dass der algebraische Abschluss eines abzählbaren Körpers abzählbar ist (Übung!), aber $\mathbb{C}$ ist überabzählbar.
Zu Beginn des vorigen Abschnitts haben wir bewusst den unbestimmten Artikel gewählt. Wir wissen noch nicht, dass der algebraische Abschluss von K eindeutig ist, in dem Sinne, dass je zwei solche Abschlüsse zu einander isomorph sind. Dazu müssen wir einen Isomorphismus zwischen diesen Abschlüssen konstruieren und dazu wiederum versuchen Körperhomomorphismen auf Körpererweiterungen fortzusetzen.

Ist $\sigma\colon K \longrightarrow L$ ein Körperhomomorphismus und $f \in K[X]$, so schreiben wir $f^\sigma \in L[X]$ für das Polynom, das entsteht, wenn wir σ auf jeden Koeffizienten anwenden. Ist $\alpha \in K$ eine Nullstelle von f, so ist $\sigma(\alpha)$ offenbar eine Nullstelle von f^σ.

Lemma 2.26 *Sei $L = K(\alpha)/K$ eine algebraische Körpererweiterung und f das Minimalpolynom von α. Weiter sei $\sigma\colon K \longrightarrow F$ ein Körperhomomorphismus.*

i) Ist $\sigma_L\colon L \longrightarrow F$ ein Körperhomomorphismus, der σ fortsetzt (d.h. $\sigma_L|_K = \sigma$), so ist $\sigma_L(\alpha)$ eine Nullstelle von f^σ.

ii) Umgekehrt gibt es zu jeder Nullstelle $\beta \in F$ von f^σ eine Fortsetzung σ_L von σ mit $\sigma_L(\alpha) = \beta$.

Insbesondere ist die Anzahl der Fortsetzungen von σ beschränkt durch den Grad von f.

Beweis : Aus $f(\alpha) = 0$ folgt für jede Fortsetzung σ_L

$$0 = f^{\sigma_L}(\sigma_L(\alpha)) = f^\sigma(\sigma_L(\alpha)) \text{ und damit i).}$$

Um ii) zu zeigen, betrachten wir die Homomorphismen, die durch Einsetzen von α bzw. von β in ein Polynom bzw. sein σ-Bild entstehen.

$$\begin{aligned} \varphi_\alpha\colon K[X] &\longrightarrow K[\alpha], \quad g \longmapsto g(\alpha) \\ \Psi\colon K[X] &\longrightarrow F, \qquad g \longmapsto g^\sigma(\beta). \end{aligned}$$

Letztere Abbildung ist als Verkettung des Homomorphismus $K[X] \longmapsto F[X]$, $g \longmapsto g^\sigma$ und des Einsetzungshomomorphismus β in der Tat ein Homomorphismus. Es gilt $\mathrm{Ker}(\varphi_\alpha) = \langle f \rangle$ nach Definition des Minimalpolynoms. Da φ_α surjektiv ist, gibt

es einen inversen Homomorphismus $\overline{\varphi}_\alpha^{-1}\colon K[\alpha] \longrightarrow K[X]/\langle f\rangle$. Wegen $f^\sigma(\beta) = 0$ ist $\langle f\rangle \subseteq \mathrm{Ker}\Psi$. Nach dem Homomorphiesatz gibt es also eine Abbildung $\overline{\Psi}$, sodass $\Psi = \overline{\Psi} \circ \pi$ ist, wobei $\pi\colon K[X] \longrightarrow K[X]/\langle f\rangle$ die Abbildung auf den Quotientenring ist. Die gesuchte Fortsetzung ist nun

$$\overline{\Psi} \circ \overline{\varphi}_\alpha^{-1} : K[\alpha] \longrightarrow K[X]/\langle f\rangle \longrightarrow F.$$

□

Satz 2.27 *Sei L/K eine algebraische Körpererweiterung, F algebraisch abgeschlossen und $\sigma\colon K \hookrightarrow F$ ein Homomorphismus. Dann besitzt σ eine Fortsetzung $\sigma_L\colon L \longrightarrow F$. Ist L ebenfalls algebraisch abgeschlossen und $F/\sigma(K)$ algebraisch, so ist σ_L ein Isomorphismus.*

Des Satz besagt also insbesondere, dass alle algebraischen Abschlüsse eines Körpers K zueinander isomorph sind.

Beweis : Um das vorige Lemma sukzessive anzuwenden, bis wir σ bis auf L fortgesetzt haben, benötigen wir wieder das Zorn'sche Lemma. Sei also M die Menge aller Paare (E, τ), bestehend aus einem Zwischenkörper $K \subseteq E \subseteq L$ und einer Fortsetzung $\tau\colon E \longrightarrow F$ von σ. Dann ist M partiell bzgl. der Relation $\subseteq'$ geordnet, wobei $(E_1, \tau_1) \subseteq' (E_2, \tau_2)$, falls $E_1 \subseteq E_2$ und $\tau_2|_{E_1} = \tau_1$. Ist $(E_i, \tau_i),\ i \in I$ eine Kette, so ist $(E = \bigcup E_i, \tau)$ mit $\tau(x) = \tau_i(x)$, falls $x \in E_i$, eine obere Schranke. Man beachte, dass wir die Kompatibilität der τ_i benötigen, um einzusehen, dass dieses τ wohldefiniert ist. Sei also (E_∞, τ_∞) ein maximales Element von M. Wir sind fertig, wenn wir gezeigt haben, dass $E_\infty = L$ ist. Falls nicht, wählen wir $\alpha \in L \setminus E_\infty$ und wenden das vorige Lemma auf dieses α an. Wir erhalten eine Fortsetzung von τ_∞ nach $E_\infty[\alpha]$, im Widerspruch zur Maximalität von (E_∞, τ_∞).
Ist L algebraisch abgeschlossen, so ist auch $\sigma_L(L)$ algebraisch abgeschlossen: Körperhomomorphismen sind auf ihrem Bild stets invertierbar. Ist $f \in \sigma_L(L)[X]$, so ist $f^{\sigma_L^{-1}} \in L[X]$, besitzt also eine Nullstelle α und $\sigma_L(\alpha)$ ist die gesuchte Nullstelle von f. Da $F/\sigma(K)$ algebraisch ist, also erst recht $F/\sigma_L(L)$ algebraisch, muss $F = \sigma_L(L)$ sein und damit σ_L eine Isomorphismus. □

2.6 Zerfällungskörper

Dieser Abschnitt ist eine Vorbereitung in Richtung Galoistheorie. Bisher haben wir zu einem Polynom eine Nullstelle adjungiert. Im vorigen Abschnitt haben wir

gesehen, dass Körperhomomorphismen Nullstellen von f auf (andere) Nullstellen von f^σ abbilden. Wenn wir also alle Körperautomorphismen eines Körpers $L = K[X]/\langle f\rangle$ bestimmen wollen, so klappt das gut, wenn alle Nullstellen von f gleichberechtigt auftreten. Betrachten wir zum Beispiel $f = X^3 - 2 \in \mathbb{Q}[X]$. Das Polynom besitzt eine reelle Nullstelle $\alpha = \sqrt[3]{2}$. Also ist $\mathbb{Q}[\alpha] \subseteq \mathbb{R}$. Die anderen beiden Nullstellen von f sind $\xi_3 \cdot \sqrt[3]{2}$ und $\xi_3^2 \cdot \sqrt[3]{2}$, wobei $\xi_3 = e^{2\pi i/3} \in \mathbb{C} \setminus \mathbb{R}$ eine dritte Einheitswurzel ist, d.h. eine Nullstelle von $x^3 - 1$. Der Körper $\mathbb{Q}[\alpha]$ enthält also genau eine der drei komplexen Nullstellen von f.

Definition 2.28 *Sei $\mathcal{F} = (f_i)_{i\in I}$ mit $f_i \in K[X]$ eine Menge von Polynomen. Eine Körpererweiterung L/K heißt* Zerfällungskörper *von $\mathcal{F}$, falls*

i) jedes $f_i \in \mathcal{F}$ über L in Linearfaktoren zerfällt und

ii) die Körpererweiterung L/K von den Nullstellen der f_i erzeugt wird.

Die Existenz eines Zerfällungskörpers zu einer beliebigen Menge $\mathcal{F}$ folgt leicht aus der bereits bewiesenen Existenz des algebraischen Abschlusses. Man wählt einen algebraischen Abschluss $\overline{K}$ von K und nimmt für L den kleinsten Teilkörper von $\overline{K}$, der alle Nullstellen der Polynome in $\mathcal{F}$ enthält.

Proposition 2.29 *Sind L_1 und L_2 zwei Zerfällungskörper von $\mathcal{F} = (f_i)_{i\in I}$ mit $f_i \in K[X]$. Dann lässt sich jeder $K-$Homomorphismus $\overline{\tau} : L_1 \longrightarrow \overline{L_2}$ faktorisieren als $\overline{\tau} = i \circ \tau$, wobei $\tau : L_1 \longrightarrow L_2$ ein Isomorphismus ist und $i : L_2 \hookrightarrow \overline{L_2}$ die Inklusion.*

Insbesondere sind je zwei Zerfällungskörper von $\mathcal{F}$ isomorph über K.

Beweis : Wir betrachten zuerst den Fall, dass $\mathcal{F} = (f)$ aus nur einem Polynom besteht. Sind $a_1, \ldots, a_n$ die Nullstellen von f in L_1 und $b_1, \ldots, b_n$ die Nullstellen von f in $L_2 \subseteq \overline{L_2}$, so ist

$$f^{\overline{\tau}} = \prod_{i=1}^{n} \big(X - \overline{\tau}(a_i)\big) = f = \prod_{i=1}^{n} (X - b_i).$$

Also ist, nach geeigneter Umordnung $\overline{\tau}(a_i) = b_i$ und daher

$$L_2 = K(b_1, \ldots, b_n) = K\big(\overline{\tau}(a_1), \ldots, \overline{\tau}(a_n)\big) = \overline{\tau}(L_1).$$

Für endliche Mengen $\mathcal{F} = (f_i)_{i\in I}$ ist der Zerfällungskörper von $\mathcal{F}$ offenbar der Zerfällungskörper von $\prod_{i\in I} \cdot f_i$, womit wir diesen Fall soeben mitbewiesen haben.

Für den allgemeinen Fall schreiben wir $L_1 = \langle \bigcup_{j\in J} L_{1,j} \rangle$, wobei $L_{1,j}$ der Zerfällungskörper von $\mathcal{F}_j = (f_i)_{i\in I_j}$ ist und I_j endliche Teilmengen mit $I_{j+1} \supseteq I_j$ für und $\bigcup_{j\in J} I_j = I$. Dabei bezeichnen die spitzen Klammern das Körper-Erzeugnis in einem algebraischen Abschluss $\overline{L}_1$ von L_1 der $L_{1,j}$, also den kleinsten Teilkörper von $\overline{L}_1$, der alle $L_{1,j}$ enthält.

Wir wenden nun den ersten Teil auf $L_{1,j}$ für alle $j \in J$ an und erhalten $\overline{\tau}_j : L_j \longrightarrow L_2$ mit der Eigenschaft $\overline{\tau}_j|_{L_{1,j-1}} = \overline{\tau}_{j-1}$. Da jedes $x \in L_1$ in einem $L_{1,j}$ für j genügend groß enthalten ist, definiert dies den gesuchten Homomorphismus $\overline{\tau} : L_1 \longrightarrow L_2$.

Für die zweite Aussage müssen wir nur die Inklusion $K \to \overline{L}_2$ in einen Homomorphismus $\overline{\tau} : L_1 \longrightarrow \overline{L}_2$ fortsetzen und erhalten aus dem ersten Teil den gewünschten Isomorphismus $\tau : L_1 \longrightarrow L_2$. □

Der Körper $\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ ist also nach dem Eingangsbeispiel ein Zerfällungskörper, zum Polynom $x^3 - 2$. Sind die Zwischenkörper $\mathbb{Q}[\sqrt[3]{2}]$ und $\mathbb{Q}[\zeta_3]$ auch Zerfällungskörper ? Das folgende Kriterium hilft, diese Art von Fragen zu beantworten.

Satz 2.30 *Sei L/K eine algebraische Körpererweiterung und ein algebraischer Abschluss $\overline{L}$ von L fixiert. Dann sind äquivalent:*

i) Jeder $K-$Homomorphismus $L \to \overline{L}$ ist ein Automorphismus von L, verkettet mit der gegebenen Inklusion $L \hookrightarrow \overline{L}$.

ii) L ist Zerfällungskörper einer Familie von Polynomen aus $K[X]$.

iii) Jedes irreduzible Polynom $f \in K[X]$, das in L eine Nullstelle besitzt, zerfällt über L in Linearfaktoren.

Eine Körpererweiterung L/K, die eine der Bedingungen des Satzes erfüllt, heißt normal.

Beweis : Wir starten mit $i)$ impliziert $iii)$. Sei $a \in L$ eine Nullstelle des irreduziblen Polynoms $f \in K[X]$ und $b \in \overline{L}$ eine weitere Nullstelle. Dann gibt es nach Lemma 2.26 einen Homomorphismus $\tau : K(a) \longrightarrow I$ mit $\tau(a) = b$. Diesen können wir auf die algebraische Körpererweiterung $L/K(a)$ zu $\overline{\tau} : L \longrightarrow \overline{L}$ fortsetzen. Nach $i)$ ist $\overline{\tau}(L) \subseteq L$ und damit $b = \tau(a) = \overline{\tau}(a) \in L$. Da b beliebig war, folgt $iii)$.

Es gelte nun $iii)$ und es seien $(a_i)_{i\in I}$ Elemente, die L/K erzeugen. Sei f_i das Minimalpolynom von a_i. Da die f_i nach Voraussetzung in Linearfaktoren zerfallen, ist L der Zerfällungskörper von $(f_i)_{i\in I}$.

Für die fehlende Implikation bemerken wir, dass bei einem $K-$Homomorphismus $\tau : L \longrightarrow \overline{L}$ mit L auch $\tau(L)$ Zerfällungskörper von $\mathcal{F} = (f_i)_{i\in I}$ ist. Die Behauptung folgt aus der vorangehenden Proposition. □

Aus diesem Satz folgt, dass in einer Kette $K \subset L \subset M$ von Körpern M/K normal auch M/L normal impliziert, man verwende $ii)$ und betrachte $f_i \in K[X] \subseteq L[X]$. Aber aus M/K normal folgt *nicht* L/K normal. Man verwendet dazu das Anfangsbeispiel und den Körper $L = \mathbb{Q}(\sqrt[3]{2}) \subseteq M = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$. Ist eine Körpererweiterung nicht normal, aber man wünscht in einer normalen Erweiterung zu arbeiten — was wir in der Galoistheorie ständig werden —, so hilft folgender Satz.

Proposition 2.31 *Sei L/K algebraisch. Dann gibt es eine minimale (bezüglich Inklusion) Erweiterung L'/K, die normal ist und sodass $L' \supseteq L$. Diese wird* normale Hülle *von L/K genannt und ist bis auf Isomorphie über L eindeutig. Die Erweiterung L'/K ist endlich, falls L/K endlich ist.*

Beweis : Sei $L = K(\mathcal{A})$, wobei $\mathcal{A} = (a_i)_{i\in I}$ mit $a_i \in L$ ein Erzeugendensystem der Erweiterung ist. Sei f_i das Minimalpolynom von a_i und L' der von den Nullstellen der f_i erzeugte Teilkörper in einem algebraischen Abschluss $\overline{L}$ von L. Dann ist offenbar L'/K normal, $L' \supseteq L$ und L' minimal mit dieser Eigenschaft.

Ist $L = K(a)$, so ist $[L' : L] \leq (\deg f_a)!$ Hieraus folgt die Endlichkeitsaussage. Für die Eindeutigkeitsaussage seien L'_1 und L'_2 zwei normale Hüllen und somit Zerfällungskörper der obigen $f_i, i \in \mathcal{I}$. Wir können auch $f_i \in L[X]$ auffassen und L'_1 und L'_2 sind Zerfällungskörper auch dieser Polynome. Die Eindeutigkeit folgt nun aus Proposition 2.29. □

2.7 Separable Körpererweiterungen

Körperhomomorphismen werden fortgesetzt, indem man Nullstellen auf Nullstellen abbildet, sagt grob gesprochen das Lemma 2.26. Dabei passieren viele ungewöhnliche Dinge, wenn das Minimalpolynom mehrfache Nullstellen hat. Wir wollen diese Situation charakterisieren und dann von den weiteren Betrachtungen zunächst ausschließen.

Wir wissen, dass $K[X]$ faktoriell ist. Ist $\alpha \in K$, so können wir ein Polynom $f \in K[X]$ in eindeutiger Weise schreiben als $f = (X - \alpha)^r \cdot \Pi f_i$ mit irreduziblen f_i und $f_i(\alpha) \neq$

0. Der Exponent r wird auch *Vielfachheit* von α in f genannt. Ein nicht-konstantes Polynom f, dessen Nullstellen im algebraischen Abschluss alle einfach sind, wird *separabel* genannt.

Lemma 2.32 *Sei $f \in K[X]$ nicht-konstant. Die Nullstellen von f von Vielfachheit größer 1 sind genau die Nullstellen von ggT (f, f').*

Beweis : Ist $f = (X-\alpha)^r \Pi f_i$ mit $r > 1$, so wird $f' = r(X-\alpha)^{r-1}\Pi f_i + (X-\alpha)^r \cdot (\Pi f_i)'$ von $(X-\alpha)$ geteilt und somit auch der ggT.

Ist umgekehrt α Nullstelle von ggT(f, f'), so teilt $(X-\alpha)$ das Polynom f, also $r \geq 1$ in obiger Darstellung. Außerdem ist $f'(\alpha) = 0$ und wegen $f_i(\alpha) \neq 0$ folgt $r \geq 2$. □

Lemma 2.33 *Ist f irreduzibel und nicht konstant, so ist f nicht separabel, genau dann wenn $f' = 0$.*

Beweis : Ist a eine Nullstelle von f, so ist f das Minimalpolynom von a. Ist f nicht separabel, so ist a auch Nullstelle von f' nach dem vorigen Lemma. Da f' kleineren Grad als f hat, kann nach Definition des Minimalpolynoms nur $f' = 0$ folgen. Die Umkehrung ist klar. □

Ein Beispiel für ein nicht-separables Polynom über $K = \mathbb{F}_p(t) = \text{Quot}\,(\mathbb{F}_p[t])$ ist $f = X^p - t$. Dieses Polynom ist nach dem Eisenstein-Kriterium irreduzibel und $f' = 0$. Das Beispiel ist typisch:

Satz 2.34 *Sei $f \in K[X]$ irreduzibel.*

i) Ist char $(K) = 0$, so ist f separabel.

ii) Ist char $(K) = p \neq 0$, so sei r definiert als das Maximum aller i mit $f(X) = g(X^{p^i})$ für ein $g \in K[X]$. Dann hat jede Nullstelle von f die Vielfachheit p^r und g ist separabel und irreduzibel.

Im vorangehenden Beispiel ist $g = X - t$.

Beweis : Im Fall $i)$ folgt aus $f = \sum_{i=0}^{n} a_i X^i$ und $0 = f' = \sum_{i=1}^{n} i a_i X^{i-1}$ dass $i \cdot a_i = 0$ für $i = 1, \ldots, n$ und damit der gewünschte Widerspruch, falls f nicht konstant ist.

Im Fall $ii)$ sei $f(X) = g(X^{p^r})$ mit r maximal. Wäre $g' = 0$, so wäre g ein Polynom in X^p, im Widerspruch zur Maximalität von r. Wäre $g = g_1 \cdot g_2$ reduzibel, so wäre $f = g_1(X^{p^r}) \cdot g_2(X^{p^r})$ im Widerspruch zur Irreduzibilität von f. Also ist auch g irreduzibel und somit nach dem vorigen Lemma separabel. Über einem algebraischen Abschluss $\overline{K}$ faktorisiert sich g also als

$$g = c \cdot \prod_{i=1}^{m} (X - a_i)$$

mit einer Konstante $c \in K$ und paarweise verschiedenen a_i. Also ist

$$f(X) = g(X^{p^r}) = c \cdot \prod_{i=1}^{m} (X^{p^r} - a_i) = c \cdot \prod_{i=1}^{m} (X - b_i)^{p^r}$$

und hieraus folgen alle Behauptungen. □

Definition 2.35 *Sei L/K eine algebraische Körpererweiterung. Dann heißt $\alpha \in L$* separabel *über K, falls das Minimalpolynom von α separabel ist. Die Körpererweiterung heißt separabel, falls jedes $\alpha \in L$ separabel ist.*

Wir brauchen noch ein Kriterium, zu testen, wann eine Körpererweiterung separabel ist. Für einzelne Elemente leistet dies der Satz 2.34.

Satz 2.36 *Sei $L = K(\alpha_1, \ldots, \alpha_r)/K$ eine endliche Körpererweiterung. Dann ist L/K separabel genau dann, wenn jedes α_i separabel über K ist.*

Beweis : Die Implikation " $\Rightarrow$ " ist klar. Für die umgekehrte Implikation sei $d_i = [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$. Dann ist $d = \prod_{i=1}^{r} d_i = [L : K]$. Aufgrund der Separabilität der α_i und Lemma 2.26 gibt es d_i Fortsetzungen eines gegebenen Homomorphismus $K(\alpha_1, \ldots, \alpha_{i-1}) \longrightarrow \overline{K}$ zu einem Homomorphismus $K(\alpha_1, \ldots, \alpha_i) \longrightarrow \overline{K}$. Insgesamt gibt also d Fortsetzungen einer fixierten Einbettung $i : K \longrightarrow \overline{K}$.

Andererseits ist für jede endliche Körpererweiterung E/F die Anzahl der Fortsetzungen von $F \longrightarrow \overline{K}$ nach E kleiner gleich $[E : F]$. Wir nehmen an, dass $\beta \in L$ nicht separabel ist. Dann ist die Anzahl der Fortsetzungen von $\varphi : K(\beta) \longrightarrow L$ kleiner gleich $[L : K(\beta)]$ und die Anzahl der Fortsetzungen von $i : K \longrightarrow \overline{K}$ nach $K(\beta)$ strikt kleiner als $[(K(\beta) : K]$. Insgesamt lässt sich $i : K \longrightarrow \overline{K}$ also auf weniger als

$$[K(\beta) : K] \cdot [L : K(\beta)] = [L : K] = d$$

Weisen nach L fortsetzen, im Widerspruch zur Aussage im ersten Abschnitt. □

Separabilität ist auch im folgenden Satz die Schlüsselvoraussetzung. Wir nennen eine endliche Körpererweiterung L/K *einfach*, falls es ein $x \in L$ gibt mit $L = K(x)$. In diesem Fall heißt x ein *primitives Element* von L/K.

Satz 2.37 *Sei $L = K(a, b_1, \ldots, b_r)/K$ eine endliche Körpererweiterung und $b_1, \ldots, b_r$ separabel über K. Ist K unendlich, so ist L/K einfach.*

Beweis : Per Induktion können wir offenbar $r = 1$ annehmen. Seien f und g die Minimalpolynome von a und b_1 und F ein Zerfällungskörper von fg. Seien $a = a_1, a_2, \ldots, a_n$ die Nullstellen von f und $b = b_1, \ldots, b_n$ die Nullstellen von g in F. Die b_i sind nach Voraussetzung paarweise verschieden. Daher hat die Gleichung

$$a_i + c \cdot b_j = a_1 + c \cdot b_1$$

für jedes i und jedes j nur eine Lösung in F. Da K unendlich ist, gibt es ein $c \in K$, sodass diese Gleichung für kein Paar (i, j) erfüllt ist. Wir setzen $x = a + c \cdot b$ und wollen zeigen, dass $L = K(x)$ ist.

Da $f(x - cb) = f(a) = 0$ ist b Nullstelle von $h(X) = f(x - cX) \in K(x)[X]$. Also ist b auch Nullstelle von $\text{ggT}_{K(x)[x]}(g, h)$. Für alle anderen b_i, d.h. mit $i \geq 2$ ist $h(b_i) = f(x - cb_i) = f(a + cb_1 - cb_i) \neq 0$ nach Wahl von c. Also ist

$$\text{ggT}_{K(x)[X]}(g, h) = (X - b) \in K(x)[X]$$

und damit $b \in K(x)$. Dann ist auch $c \cdot b$ und somit $a = x - cb \in K(x)$. □

Der Satz gilt auch für K endlich, allerdings mit anderem Beweis. Als Vorbereitung für den Abschnitt über endliche Körper zeigen wir:

Satz 2.38 *(Satz vom primitiven Element) Ist K ein Körper und $H \subseteq K^*$ eine endliche Untergruppe. Dann ist H zyklisch.*

Den Satz werden wir häufig für K endlich und $H = K^*$ anwenden. Der Beweis verwendet folgendes Lemma.

Lemma 2.39 *Sei G eine abelsche Gruppe und $a, b \in G$ zwei Elemente endlicher Ordnung, $m = \text{ord}(a)$ und $n = \text{ord}(b)$.*

Dann gibt es Zerlegungen $m = m_0 \cdot m'$ und $n = n_0 \cdot n'$ mit kgV$(m, n) = m_0 \cdot n_0$ und ggT$(m_0, n_0) = 1$. Das Element $a^{m'} \cdot b^{n'}$ hat die Ordnung kgV(m, n).

Beweis : Übung.

Beweis des Satzes: Sei $a \in H$ ein Element maximaler Ordnung m und $H_m \subseteq H$ die Teilmenge von Elementen, deren Ordnung m teilt. Da K^* abelsch ist, ist H_m eine Untergruppe. Alle Elemente von H_m sind Nullstellen von $X^m - 1$, also hat H_m höchstens m Elemente. Da $\langle a \rangle \subseteq H_m$ und $|\langle a \rangle| = m$ folgt $H_m = \langle a \rangle$. Falls $H \supsetneq H_m$ so gibt es $b \in H \backslash H_m$. Dann ist $\mathrm{ord}(b)$ kein Teiler von m, also $\mathrm{kgV}\big(\mathrm{ord}(b), m\big) > m$. Nach dem vorangehenden Lemma gibt es ein Element der Ordnung $\mathrm{kgV}\big(\mathrm{ord}(b), m\big)$ in H, im Widerspruch zur Maximalität von n. □

Beweis : (des Satzes vom primitiven Element, Fall K endlich) Ist K endlich und L/K endlich, so ist auch L und damit L^* endlich. Ein Erzeuger von L^* als zyklische Gruppe erzeugt auch L/K. □

2.8 Endliche Körper

Wir wissen bereits, dass ein endlicher Körper $\mathbb{F}$ als Primkörper einen Körper $\mathbb{F}_p$ für eine Primzahl p besitzt und ein endlich-dimensionaler $\mathbb{F}_p-$ Vektorraum ist. Somit hat $\mathbb{F}$ die Kardinalität $q = p^n$ für $n = [\mathbb{F} : \mathbb{F}_p] \in \mathbb{N}$. Ziel dieses Abschnitts ist es, für jedes solche q einen endlicher Körper zu konstruieren.

Lemma 2.40 *Ist $\mathbb{F}$ ein Körper mit $q = p^n$ Elementen, so ist $\mathbb{F}$ der Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$. Insbesondere ist $\mathbb{F}/\mathbb{F}_p$ normal.*

Beweis : Die Gruppe $\mathbb{F}^*$ hat die Ordnung $q - 1$, also hat jedes Element in $\mathbb{F}^*$ eine Ordnung, die $q - 1$ teilt. Folglich sind alle Elemente in $\mathbb{F}$ Nullstelle von $X^q - X$. Da der Grad dieses Polynoms gerade $|\mathbb{F}|$ ist, enthält $\mathbb{F}$ alle Nullstellen von $X^q - X$. Also ist $\mathbb{F}$ der Zerfällungskörper dieses Polynoms. □

Satz 2.41 *Sei p prim. Dann gibt es zu jedem $n \in \mathbb{N}_{>0}$ bis auf Isomorphie genau einen Körper mit $q = p^n$ Elementen.*

Beweis : Sei L ein Zerfällungskörper von $f = X^q - X$. Sobald wir gezeigt haben, dass L genau q Elemente enthält, folgt die Eindeutigkeitsaussage aus Proposition 2.29. Sind u und v zwei Nullstellen von f, so ist wegen

$$(u + v)^q = (u^q + v^q) = u + v$$

auch $u+v$ eine Nullstelle von f. Für $b \neq 0$ ist

$$(a \cdot b^{-1})^q = a^q \cdot (b^{-1})^q = a \cdot b^{-1},$$

also auch $a \cdot b^{-1}$ Nullstelle. Ist q ungerade, so ist mit a auch $(-a)$ Nullstelle und für q gerade ist $p = 2$, also $a = -a$. Insgesamt bilden die q Nullstellen von f also einen Körper, was zu zeigen war. □

Wir wissen nun, welche endlichen Körper es gibt und wollen noch bestimmen, wann sie ineinander enthalten sind.

Korollar 2.42 *Fassen wir $\mathbb{F}_{q_1}$ und $\mathbb{F}_{q_2}$ als Teilkörper eines algebraischen Abschlusses $\overline{\mathbb{F}_p}$ auf und schreiben $q_1 = p^{n_1}$ und $q_2 = p^{n_2}$, so gilt $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ genau dann, wenn $n_1 | n_2$.*

Beweis : Ist $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$, so ist $\mathbb{F}_{q_2}$ ein $\mathbb{F}_{q_1}-$Vektorraum, also $q_2 = q_1^m$ für ein $m \in \mathbb{N}$ und daher gilt $n_1 | n_2$. Gilt umgekehrt $n_1 | n_2$, so betrachten wir ein $a \in \mathbb{F}_{q_1}$. Für dieses gilt $a^{q_1} = a$ und daher (mit $n_1 \cdot m = n_2$) :

$$a^{q_2} = a^{(q_1^m)} = (a^{q_1})^{q_1^{m-1}} = a^{(q_1^{m-1})} = a,$$

wobei wir im letzten Schritt induktiv den Exponenten verkleinert haben. Also ist $a \in \mathbb{F}_{q_2}$. □

3 Galoistheorie

Die geniale Idee von Galois besteht darin, einer Körpererweiterung, also einem bisher noch ziemlich unhandlichen Objekt, eine Gruppe zuzuordnen, also ein wesentlich handlicheres Objekt. Ist die Körpererweiterung endlich, so wird auch die Gruppe endlich sein. Außerdem werden wir Zwischenkörper mit Untergruppen in Verbindung bringen und so die motivierenden Fragen z.B. der Konstruierbarkeit mit Zirkel und Lineal später mit mehr Gruppentheorie lösen können.

3.1 Galois-Erweiterungen

Definition 3.1 *Eine algebraische Körpererweiterung L/K heißt* galoissch, *falls sie normal und separabel ist. Man bezeichnet die Gruppe $\mathrm{Aut}_K(L)$ der $K-$Automorphismen von L als Galoisgruppe und schreibt auch $Gal(L/K) := \mathrm{Aut}_K(L)$.*

Fixieren wir einen algebraischen Abschluss $\overline{K}$ von K und damit auch von L. Verkettet mit der Inklusion $L \hookrightarrow \overline{K}$ ist also jedes Element der Gruppe $\mathrm{Aut}_K(L)$ auch ein Element von $\mathrm{Hom}_K(L, \overline{K})$, wie wir die Menge aller $K-$Homomorphismen von L nach $\overline{K}$ ab sofort bezeichnen. Ist L normal, so definiert jedes Element von $\mathrm{Hom}_K(L, \overline{K})$ auch ein Element von $\mathrm{Aut}_K(L)$. Also ist $\mathrm{Hom}_K(L, \overline{K})$ für galoissche Erweiterung eine andere Darstellung der Galoisgruppe.

Proposition 3.2 *Sei L/K galoissch und $K \subseteq E \subseteq L$ ein Zwischenkörper. Dann ist L/E galoissch und* $\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/K)$ *eine Untergruppe. Ist auch E/K galoissch, so liefert jedes $\sigma \in \mathrm{Gal}(L/K)$ durch Einschränken auf E ein Element $\sigma|_E \in \mathrm{Gal}(E/K)$ und $\sigma \mapsto \sigma|_E$ ist ein surjektiver Gruppenhomomorphismus.*

Beweis : Wir hatten bereits gesehen, dass die Eigenschaften normal und separabel sich auf den oberen Teil einer Zwischenkörpererweiterung vererben. Sind $\sigma, \tau \in \mathrm{Gal}(L/E)$, d.h. $\sigma|_E = \mathrm{id}$ und $\tau|_E = \mathrm{id}$, so auch $\sigma \circ \tau^{-1}|_E = \mathrm{id}$, also $\sigma \circ \tau^{-1} \in \mathrm{Gal}(L/E)$.

Ist E/K normal, und $\sigma \in \mathrm{Gal}(L/K)$, so betrachten wir $\sigma|_E : E \longrightarrow L \longrightarrow \overline{K}$. Nach Definition faktorisiert dies über einen Automorphismus von E, den wir auch mit $\sigma|_E$ bezeichnen, verkettet mit der Einbettung $E \hookrightarrow \overline{K}$. Diese Einschränkung ist offenbar mit Komposition verträglich, also ein Gruppenhomomorphismus. Indem wir den Fortsetzungssatz 2.27 auf ein gegebenes $\tau : E \longrightarrow E \hookrightarrow L$ anwenden, folgt die Surjektivität. □

Bisher wissen wir noch nicht, wie groß $\mathrm{Gal}(L/K)$ ist, und haben die Separabilitätsvoraussetzung noch nicht verwendet.

Lemma 3.3 *Ist L/K endlich und galoissch, so ist*

$$[L : K] = \#\mathrm{Gal}(L/K).$$

Beweis : Nach dem Satz vom primitiven Element ist $L = K(\alpha)$ einfach. Dieses Minimalpolynom f von α hat $d = [L : K]$ Nullstellen $\alpha = \alpha_1, \ldots, \alpha_d$ in $\overline{K}$ aufgrund der Separabilität und diese liegen alle in L aufgrund der Normalität. Zu jedem α_j gibt es nach Lemma 2.26 genau einen Homomorphismus $\varphi : L \longrightarrow L$ mit $\varphi(\alpha) = \alpha_j$. Dies sind genau die n gesuchten Automorphismen. □

Beispiel 3.4 Sei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ und $E = \mathbb{Q}(\sqrt[3]{2})$. Dann definiert $\tau(\zeta_3) = \zeta_3^2$ und $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ einen Automorphismus von L/K, der E fixiert. Da $[L : E] = 2$

ist $\mathrm{Gal}(L/E) = \{\mathrm{id}, \tau\}$. Ein weiteres Element σ von $\mathrm{Gal}(L/K)$ ist definiert durch $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot \zeta_3$ und $\sigma(\zeta_3) = \zeta_3$. Man prüft, dass die 6 Elemente

$$\{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

paarweise verschieden sind.

Wir haben bereits Zwischenkörpern Untergruppen zugeordnet. Um umgekehrt einer Untergruppe $H \leq \mathrm{Gal}(L/K)$ einen Fixkörper zuzuordnen, betrachten wir die Menge

$$L^H = \{a \in L : \sigma(a) = a \text{ für alle } \sigma \in H\},$$

genannt den *Fixkörper* von H.

Satz 3.5 *Sei L ein Körper und $G \leq \mathrm{Aut}(L)$ eine Untergruppe mit Fixkörper $K = L^G$. Ist G endlich, so ist L/K galoissch,*

$$\#G = [L : K] \text{ und } G = \mathrm{Gal}(L/K).$$

Ist G nicht endlich, aber L/K algebraisch, so ist L/K galoissch und $\mathrm{Gal}(L/K) \geq G$.

Beweis : Sei G endlich oder L/K algebraisch. Wir wollen zeigen, dass L/K separabel ist und betrachten $a \in L$. Wir betrachten eine bezüglich Inklusion maximale Menge $E \subseteq G$, sodass die $\sigma(a)$ für $\sigma \in E$ paarweise verschieden sind. Da alle $\sigma(a)$ Nullstellen des Minimalpolynoms von a sind, ist auch im zweiten Fall E endlich. Ist $\tau \in G$ beliebig, so ist für $\sigma \in E$ auch $\tau \circ \sigma \in E$, denn sonst könnte man dieses Element zu E hinzufügen, im Widerspruch zur Maximalität von E. Also ist

$$\tau\circ : E \longrightarrow E, \sigma \mapsto \tau \circ \sigma$$

eine Bijektion. Dies bedeutet, dass

$$f_a = \prod_{\sigma \in E} \big(X - \sigma(a)\big)$$

unter τ invariant ist, da nur die Faktoren permutiert werden. Da τ beliebig war, ist $f \in K[X]$. Damit ist L/K separabel. Ist $\mathcal{F} = (f_a)_{a \in L^*}$ die Menge aller Polynome, die durch obiges Verfahren aus $a \in L^*$ gewonnen werden, so ist L offenbar Zerfällungskörper von $\mathcal{F} \subseteq K[X]$. Also ist L/K normal und damit galoissch. Ist G endlich, so folgt aus obigem Argument, dass für alle $a \in L$ gilt $[K(a) : K] \leq \#G =: n$. Wäre $[L : K] > n$, potenziell unendlich, so schreiben wir $L = K(\alpha_i, i \in I)$. Dann gibt es

eine endliche Teilmenge $J \subseteq I$, sodass $[K(\alpha_i, i \in J) : K] > n$. Nach dem Satz vom primitiven Element ist diese Körpererweiterung von einem $a \in L$ erzeugt, im Widerspruch zu $[K(a) : k] \leq n$. Da andererseits $G \subseteq \mathrm{Aut}_K(L)$ und $\#\mathrm{Aut}_K(L) \leq [L : K]$ folgt Gleichheit überall, wie behauptet.

Ist G unendlich, so ist $\infty = \#G \leq \mathrm{Aut}_K(L) = [L : K]$, was noch zu zeigen war. $\square$

Satz 3.6 *(Hauptsatz der Galois-Theorie): Sei L/K endlich und galoissch mit $G = \mathrm{Gal}(L/K)$. Dann sind die Zuordnungen*

$$\begin{array}{ccc} \{\text{Untergruppen von G}\} & \overset{\phi}{\underset{\psi}{\rightleftarrows}} & \{\text{Zwischenkörper von } L/K\} \\ H & \mapsto & L^H \\ \mathrm{Gal}(L/E) & \leftarrow & E \end{array}$$

zueinander inverse Bijektionen.

Die Untergruppe $H \leq G$ ist ein Normalteiler genau dann, wenn L^H/K galoissch ist. In diesem Fall ist H der Kern von $\sigma \mapsto \sigma|_{L^H}$, also $G/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$.

Beispiel 3.7 Wir bleiben bei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Dann ist $G = \mathrm{Gal}(L/K) \cong S_3$ via $\tau \mapsto (12)$ und $\sigma \mapsto (123)$. Diese Gruppe enthält $H_3 = \{(123), (132), \mathrm{id}\}$ als Untergruppe vom Index zwei, notwendigerweise ein Normalteiler. Der Fixkörper $L^{H_3} = \mathbb{Q}(\zeta_3)$ hat Grad $[L^H : K] = 2$. Die weiteren nichttrivialen Untergruppen sind $\{(12), \mathrm{id}\}, \{(13), \mathrm{id}\}$ und $\{(23), \mathrm{id}\}$, allesamt keine Normalteiler. Die zugehörigen Fixkörper sind $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3^2)$ und $\mathbb{Q}(\sqrt[3]{2} \cdot \zeta_3)$. Diese sind folglich über $\mathbb{Q}$ nicht normal, was wir bereits zuvor direkt aus der Definition eingesehen haben.

Beweis : Sei E ein Zwischenkörper der Erweiterung L/K. Dann ist $H = \mathrm{Gal}(L/E)$ eine Untergruppe von $\mathrm{Gal}(L/K)$ und $L^H = \phi \circ \psi(E)$ nach Definition. Nach der vorigen Proposition ist $\mathrm{Gal}(L/L^H) = H$ und nach Definition des Fixkörpers gilt $E \subseteq L^H$. Wir wissen bereits, dass L^H/E separabel ist, da dies für L/K und daher für L/E gilt. Um die Gleichheit einzusehen, genügt es, nach Lemma 3.3 zu zeigen, dass es nur eine Fortsetzung der Einbettung $i_E : E \longrightarrow \overline{K}$ nach L^H gibt. (Dabei haben wir den algebraischen Abschluss $\overline{K}$ so gewählt, dass er L enthält.) Jede Fortsetzung von i_E nach L^H kann man auch nach L fortsetzen. Da L/E normal ist, muss die Fortsetzung ein Automorphismus von L, verkettet mit der Einbettung $L \hookrightarrow \overline{K}$ sein. Dieser Automorphismus ist, als Fortsetzung von i_E, auf E trivial, also in H. Daher ist er auch auf L^H trivial mit $i_{L^H} : L^H \longrightarrow \overline{K}$ ist gleich i_H. Damit ist gezeigt, dass $E = L^H$ ist.

Sei umgekehrt $H \leq G$ eine Untergruppe und L^H der zugehörige Fixkörper. Dann sagt die vorangehende Proposition direkt, dass $\mathrm{Gal}(L/L^H) = H$, d.h. dass $\psi \circ \Phi = \mathrm{id}$.

Ist $H = \mathrm{Gal}(L/L^H)$ mit L^H/K normal, so ist der Kern des Homomorphismus

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(L^H/K) \\ \tau & \longmapsto & \tau|_{L^H} \end{array}$$

gerade $\mathrm{Gal}(L/L^H) = H$, also ist H ein Normalteiler. Die letzte Aussage des Satzes ist dann gerade der Homomorphiesatz für Gruppen.

Ist umgekehrt $H \triangleleft G$ ein Normalteiler, so wählen wir wie oben einen algebraischen Abschluss

$$K \hookrightarrow L^H \hookrightarrow L \overset{i_L}{\hookrightarrow} \overline{K}.$$

Wir müssen nachweisen, dass L^H/K normal ist und betrachten einen Homomorphismus $\sigma : L^H \longrightarrow \overline{K}$. Diesen können wir zu $\sigma_L : L \longrightarrow \overline{K}$ fortsetzen. Da L/K normal ist, faktorisiert σ_L als Automorphismus von L verkettet mit der Einbettung $i_L : L \longrightarrow K$. Eingeschränkt auf L^H bedeutet dies, dass sich $\sigma = i_L \circ \sigma_0$ mit $\sigma_0 : L^H \hookrightarrow L$ faktorisieren lässt. Wir wollen zeigen, dass $\sigma_0(L^H) \subseteq L^H$ ist. Sei also $a \in L^H$ und $b = \sigma_0(a) \in L$. Sei $\tau \in H = \mathrm{Gal}(L/L^H)$ beliebig. Dann ist $\tau \circ \sigma_0 = \sigma \circ \tau'$ für ein $\tau' \in H$, da H Normalteiler ist. Also ist

$$\tau(b) = \tau \circ \sigma_0(a) = \sigma_0 \circ \tau'(a) = \sigma_0(a) = b$$

Damit wird b von jedem Element in H festgelassen und liegt somit in L^H. □

Als Folge hiervon erhalten wir, dass jede separable endliche Körpererweiterung nur endlich viele Zwischenkörper besitzt. Es genügt dazu, zur normalen Hülle überzugehen, welche immer noch endlich und separabel über dem Grundkörper ist. Nun können wir den Hauptsatz anwenden und die Tatsache, dass eine endliche Gruppe nur endlich viele Untergruppen hat.

Wir wollen noch erklären, was Durchschnitt von Untergruppen und Gruppenerzeugnis unter der Korrespondenz des Hauptsatzes bedeuten. Sei dazu für $E_1 \subseteq L$ und $E_2 \subseteq L$ das *Kompositum* $E_1 \cdot E_2$ definiert als der kleinste Teilkörper von L, der sowohl E_1 als auch E_2 enthält.

Korollar 3.8 *Sei L/K endlich und galoissch. Seien E_1 und E_2 Zwischenkörper und $H_i = \mathrm{Gal}(L/E_i)$ die zugehörigen Galoisgruppen. Dann gilt*

i) $E_1 \subseteq E_2 \Leftrightarrow H_1 \geq H_2$

ii) $E_1 \cdot E_2 = L^{H_1 \cap H_2}$

iii) $E_1 \cap E_2 = L^{\langle H_1, H_2 \rangle_{\text{Gruppe}}}$

Beweis : Ist $E_1 \subseteq E_2$ und $\sigma \in \text{Gal}(L/E_2)$, so ist $\sigma \in \text{Gal}(L/E_1)$. Umgekehrt ist $E_1 = L^{H_1} \subseteq L^{H_2} = E_2$. Dies zeigt $i)$ und die anderen beiden Aussagen folgen analog. □

3.2 Galois-Gruppen zu Gleichungen

Wir wollen zu einigen Gleichungen kleinen Grades die Galoisgruppe bestimmen.

Grad 2: Sei $f = X^2 + aX + b \in K[X]$. Das Polynom ist genau dann irreduzibel, wenn f keine Nullstelle in K hat. In diesem Fall ist f separabel, falls nicht $\text{char}(k) = 2$ und $a = 0$ gilt. Wenn wir eine Nullstelle α adjungieren, so ist $f/(X - \alpha)$ linear, also ist $K(\alpha)$ der Zerfällungskörper von f. Es ist $[K(\alpha) : K] = 2$, also $\text{Gal}(K(\alpha)/K) \cong \mathbb{Z}/2$.

Bevor wir den Grad erhöhen, noch eine Strukturaussage.

Satz 3.9 *Sei $f \in K[X]$ separabel und L/K der Zerfällungskörper von f. Seien $\{\alpha_1, \ldots, \alpha_n\}$ die Nullstellen von f. Dann ist*

$$\begin{array}{rccc} \varphi: & \text{Gal}(L/K) & \longmapsto & S_{\{\alpha_1,\ldots,\alpha_n\}} \cong S_n \\ & \sigma & \longmapsto & \sigma|_{\{\alpha_1,\ldots,\alpha_n\}} \end{array}$$

ein injektiver Gruppenhomomorphismus. Insbesondere ist $\#\text{Gal}(L/K) \leq n!$

Das Polynom f ist genau dann irreduzibel, wenn f transitiv auf $\{\alpha_1, \ldots, \alpha_n\}$ operiert.

Beweis : Da σ Nullstellen von f auf Nullstellen abbildet und injektiv ist, muss es auf der endlichen Menge $\{\alpha_1, \ldots, \alpha_n\}$ eine Bijektion sein. Die Bilder der Nullstellen bestimmen σ und daher ist φ injektiv. Ist f irreduzibel, so gibt es zu jedem Paar (α_i, α_j) von Nullstellen eine Fortsetzung σ von $i_K : K \longrightarrow \overline{K}$ mit $\sigma(\alpha_i) = \alpha_j$. Da L/K normal ist, haben wir den gesuchten Automorphismus von L gefunden. Ist f reduzibel mit Zerlegung $f = g \cdot h$, so bildet f die Nullstellen von g in sich und ebenso die Nullstellen von h in sich ab. Da f separabel ist, müssen diese verschieden sein und daher gibt es keinen Automorphismus von L, der eine Nullstelle von g auf eine von h abbildet. □

Grad 3: Ist $f = X^3 + c_2X^2 + c_1X + c_0 \in K[X]$, so lässt sich, falls $\text{char}(k) \neq 3$ das Polynom durch die Substitution $X \longmapsto X - \frac{c_2}{3}$ auf die Gestalt $f = x^3 + ax + b$ bringen, die wir ab sofort betrachten. Wieder ist f irreduzibel, falls f keine Nullstelle in K hat. In diesem Fall ist bei $\text{char}(K) \neq 3$ das Polynom auch separabel. Sei α eine Nullstelle von f und L der Zerfällungskörper. Nun gibt es zwei Fälle.

Ist $L = K(\alpha)$, also $\text{Gal}(L/K)$ von Ordnung 3, so ist die Gruppe zyklisch.

Ist $L \supsetneq K(\alpha)$, so ist $[L : K] = 6$ und $\text{Gal}(L/K)$ können wir als Untergruppe von S_3 auffassen. Also hat $\text{Gal}(L/K)$ kein Element der Ordnung 6 und ist daher isomorph zu S_3.

Wir suchen noch nach einem Kriterium, welcher der Fälle auftritt, indem wir nur die Koeffizienten a und b ansehen. Seien dazu $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von f und

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

Wenn man $\sigma \in \text{Gal}(L/K)$ anwendet, so werden die Nullstellen permutiert und damit die Vorzeichen der Faktoren von δ. Es gilt also $\sigma(\delta) = \pm\delta$. Ist $\sigma \in \{(12), (23), (13)\}$, so gilt $\sigma(\delta) = -\delta$ und falls $\sigma \in \{\text{id}, (123), (132)\}$ so gilt $\sigma(\delta) = +\delta$. Also ist $\frac{\sigma(\delta)}{\delta} = \text{sign}(\sigma)$ und somit

$$\#\text{Gal}(L/K) = 3 \Leftrightarrow \text{Gal}(L/K) \subseteq \text{Ker(sign)} \Leftrightarrow \delta \in K$$

Es gilt

$$f = \prod_{i=1}^{3}(x - \alpha_1) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x + \alpha_1\alpha_2\alpha_3.$$

Also ist $\alpha_1 + \alpha_2 + \alpha_3 = 0$ mit der gegebenen Normierung und man rechnet mit Geduld

$$\delta^2 = -4a^3 - 27b^2$$

nach. Einen allgemeinen Grund hierfür sehen wir im Abschnitt über Diskriminanten. Jedenfalls folgt hieraus, dass z.B. $f = x^3 - x + 1$ die Galoisgruppe S_3 besitzt.

Grad n: Der allgemeine Fall: Wir betrachten $L = k(T_1, \ldots, T_n) = \text{Quot}\big(k[T_1, \ldots, T_n]\big)$ für einen Körper k. Die Gruppe S_n operiert hierauf, indem $S_n \ni \sigma$ in einem Polynom die Variablen vertauscht und auf Brüchen dies im Zähler und Nenner tut. Dann ist $K = L^{S_n}$ ein Körper, der Körper der *symmetrischen rationalen Funktionen* in n Variablen. Die Erweiterung L/K ist nach dem Satz 3.5

galoissch. Wir wollen bestimmen, wie Elemente von K konkret aussehen. Sicher ist $k \subseteq K$ und z.B. $T_1 + T_2 + \ldots + T_n \in K$. Für den allgemeinen Fall betrachten wir

$$\begin{aligned} f &= \prod_{i=1}^{n}(X - T_i) \\ &= \sum_{j=0}^{n}(-1)^j s_j(T_1, \ldots, T_n) \cdot X^{n-j} \in k[T_1, \ldots, T_n][X]. \end{aligned}$$

Dabei ist $s_0 = 1, s_1 = T_1 + T_2 + \ldots T_n, s_2 = T_1T_2 + T_1T_3 + \ldots + T_{n-1}T_n$ und schließlich $s_n = T_1 \cdot \ldots \cdot T_n$. Diese Polynome werden *elementar-symmetrische Polynome* genannt. Offenbar ist $k(s_1, \ldots, s_n) = \text{Quot}(k[s_1, \ldots, s_n]) \subseteq K$. Da $[L : K] = n!$ ist f irrezuzibel in $K[X]$. Da L offenbar Zerfällungskörper von f ist, folgt

$$[L : k(S_1, \ldots, S_n)] \leq n!$$

und somit $K = k(S_1, \ldots, S_n)$.

Wir wollen nun diesen Konstruktionsvorgang umkehren und $S_1, \ldots, S_n$ als Variablen betrachten sowie das Polynom

$$p = X^n + S_1X^{n-1} + \ldots + S_{n-1}X + S_n \in k(S_1, \ldots, S_n)[X]$$

und dessen Zerfällungskörper. Wir nennen p das *allgemeine Polynom* $n-$ten Grades über k. Wir wollen zeigen, dass wir S_i mit s_i identifizieren dürfen und führen dazu folgenden Begriff ein.

Definition 3.10 *Sei $E \hookrightarrow F$ eine Inklusion von Ringen und $M = \{s_1, \ldots, s_n\} \subseteq F$ eine Teilmenge. Diese heißt* algebraisch unabhängig *über E, falls der Ringhomomorphismus*

$$E[X_1, \ldots, X_n] \longrightarrow F, X_i \longmapsto s_i$$

injektiv ist. Andernfalls heißen $s_1, \ldots, s_n$ algebraisch abhängig.

Algebraische Unabhängigkeit bedeutet also die Nichtexistenz einer polynomialen Beziehung zwischen den gegebenen Elementen. Jedes algebraische Element einer Körpererweiterung ist also algebraisch abhängig.

Lemma 3.11 *Die elementar-symmetrischen Polynome $s_1, \ldots, s_n \in L^{S_n}$ sind algebraisch unabhängig über k.*

Beweis : Wir nehmen Variablen $S_1, \ldots, S_n$ und betrachten

$$\widetilde{f} = \sum_{j=0}^{n}(-1)^j S_j \cdot X^{n-j} \in k(S_1, \ldots, S_n)[X],$$

wobei $S_0 = 1$ per Definition gesetzt wurde. Sei $\widetilde{L}$ der Zerfällungskörper dieses Polynoms und $t_1, \ldots, t_n$ die Nullstellen von $\widetilde{f}$ in $\widetilde{L}$. Dann gilt

$$\widetilde{L} = k(S_1, \ldots, S_n)(t_1, \ldots, t_n) = k(t_1, \ldots, t_n),$$

da $S_1 = t_1 + \ldots + t_n$ und allgemein sich die S_i als elementarsymmetrischen Ausdruck in den t_i schreiben lassen. Wir betrachten den Ringhomomorphismus

$$ev : k[T_1, \ldots, T_n] \longrightarrow k[t_1, \ldots, t_n]; T_i \longmapsto t_i.$$

Dieser bildet $s_i \in k[T_1, \ldots, T_n]$ auf $S_i \in k[t_1, \ldots, t_n]$ ab. Die S_i Variablen sind also algebraisch unabhängig über k,

$$ev|_{k[S_1,\ldots,S_n]} : k[s_1, \ldots, s_n] \longrightarrow k[S_1, \ldots, S_n]$$

ist injektiv und offenbar ein Isomorphismus. Also ist $\{s_1, \ldots, s_n\}$ algebraisch unabhängig. □

Satz 3.12 *Das allgemeine Polynom $n-$ten Grades ist irreduzibel, separabel und hat S_n als Galoisgruppe.*

Beweis : Da die elementarsymmetrischen Funktionen $\{s_1, \ldots, s_n\}$ algebraisch unabhängig über k sind, ist

$$k(S_1, \ldots, S_n) \longmapsto k(s_1, \ldots, s_n) = K; S_j \longmapsto (-1)^j \cdot s_j$$

ein Isomorphismus. Das Bild von $p(X)$ unter diesem Isomorphismus ist $\widetilde{f}(X)$ aus dem vorigen Lemma. Mit den Notationen von dort ist $\widetilde{L}$ der Zerfällungskörper von $\widetilde{f}(X)$ und L der Zerfällungskörper von $f(X)$, welches aus $\widetilde{f}(X)$ via $ev|^{-1}_{k[s_1,\ldots,s_n]}$ hervorgeht. Also sind $p(X), \widetilde{f}(X)$ und $f(X)$ alle gleichermaßen separabel und irreduzibel und ihre Zerfällungskörper haben Grad $n!$ und Galoisgruppe S_n. □

3.3 Einheitswurzeln

Wenn wir Wurzeln ziehen, also Nullstellen von $X^p - a$ adjungieren wollen, so treten im Zerfällungskörper stets Einheitswurzel-Erweiterungen auf. Dies haben wir bereits im Beispiel $x^3 - 2$ mehrfach gesehen und wir untersuchen diese nun systematisch.

Lemma 3.13 *Falls $p \nmid n$, so ist $f = X^n - 1$ über einem Körper der Charakteristik p separabel. Falls $p \mid n$, etwa $p \cdot \widetilde{n} = n$, so sind die Nullstellen von f diejenigen von $\widetilde{f} = (X^{\widetilde{n}} - 1)$.*

Wenn wir also Einheitswurzeln adjungieren wollen, können wir immer annehmen, dass $\mathrm{char}(K) \nmid n$ gilt, andere Exponenten bringen keine neuen Einheitswurzeln dazu.

Beweis : Es ist $f' = n \cdot x^{n-1} \neq 0$, falls $p \nmid n$. Falls $\mathrm{char}(K) = p \mid n$, so ist

$$(X^{\widetilde{n}} - 1)^p = (X^n - 1),$$

was die Behauptung zeigt. □

Satz 3.14 *Es gelte $\mathrm{char}(K) \nmid n$. Dann ist die Gruppe U_n der $n-$ten Einheitswurzeln zyklisch der Ordnung n.*

Beweis : Offenbar ist die Ordnung mindestens n, die Gruppe ist nach Satz 2.38 zyklisch und die Ordnung jedes Elements teilt n. Also hat U_n genau n Elemente. □

Die Erzeuger von U_n werden *primitive $n-$te Einheitswurzeln* genannt. Abstrakt ist also $(U_n, \cdot)$ zu $(\mathbb{Z}/n\mathbb{Z}, +)$ isomorph. Es ist $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein Ring und wir können die Einheiten in diesem Ring betrachten, die wir wie üblich mit $(\mathbb{Z}/n\mathbb{Z})^*$ bezeichnen. Die Eulersche $\varphi-$Funktion ist definiert als

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*.$$

Es gilt

Lemma 3.15 *Die Eulersche $\varphi-$Funktion ist multiplikativ für teilerfremde Argumente, d.h. aus $ggT(m,n) = 1$ folgt $\varphi(m \cdot n) = \varphi(m)\varphi(n)$. Weiter ist $\varphi(p^k) = p^{k-1} \cdot (p-1)$ und*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \text{ mit } ggT(a,n) = 1\}.$$

Beweis : Die letzte Aussage folgt direkt aus dem erweiterten Euklidischen Algorithmus. Mit dieser Charakterisierung sieht man sofort, dass

$$\#\Big((\mathbb{Z}/p^k\mathbb{Z}) \backslash (\mathbb{Z}/p^k\mathbb{Z})^*\Big) = p^{k-1}$$

und damit die zweite Behauptung. Die erste ist Folge des Chinesischen Restsatzes. Dieser besagt, dass für ggT$(m,n) = 1$ die Abbildung

$$\mathbb{Z}/(mn)\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, a \longmapsto (a \mod m, a \mod n)$$

einen Isomorphismus von Ringen ist. □

Dies steht mit der Struktur der Einheitswurzeln wie folgt in Zusammenhang.

Proposition 3.16 *Die Gruppe U_n enthält genau $\varphi(n)$ primitive $n-$te Einheitswurzeln. Ist ζ eine solche, so ist $\{\zeta^k, k \in (\mathbb{Z}/n\mathbb{Z})^*\}$ die Menge aller primitiven $n-$ten Einheitswurzeln.*

Beweis : Ist $k \in (\mathbb{Z}/n\mathbb{Z})^*$ und $l \cdot k = 1$, so ist $(\zeta^k)^l = \zeta$, also ζ^k eine primitive $n-$te Einheitswurzel. Umgekehrt gilt: Ist ζ^k primitiv, so ist $\langle \zeta^k \rangle = U_n$, also gibt es ein l mit $(\zeta^k)^l = \zeta$. Folglich ist $k \cdot l = 1$ und $k \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Wir betrachten nun den Zerfällungskörper L von $X^n - 1$. Ist $K = \mathbb{Q}$, so wird L auch der $n-$te *Kreisteilungskörper* genannt. Wir können wie oben gesagt $\mathrm{char}(K) \nmid n$ annehmen, sodass L/K galoissch ist. Die Struktur der Galoisgruppe klärt der folgende Satz.

Satz 3.17 *Die Erweiterung L/K ist abelsch und $[L : K] \mid \varphi(n)$. Genauer definiert*

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}(U_n); \tau \longmapsto \tau|_{U_n}$$

einen injektiven Homomorphismus. Die Abbildung

$$\psi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(U_n), \quad a \longmapsto (\zeta \longmapsto \zeta^a)$$

ist ein Isomorphismus von Gruppen.

Beweis : Die erste Aussage folgt offenbar aus den zwei folgenden. Offenbar bildet $\tau \in \mathrm{Gal}(L/K)$ eine Nullstelle von $X^n - 1$ wieder auf eine solche ab und τ ist durch die Bilder der Nullstellen bestimmt. Also ist φ eine injektive Abbildung in die symmetrische Gruppe der Nullstellen. Zudem ist $\tau(\zeta_i \cdot \zeta_j) = \tau(\zeta_i)\tau(\zeta_j)$, sodass τ ein Homomorphismus von U_n ist, wegen Bijektivität also ein Automorphismus.

Identifiziern wir U_n mit $\mathbb{Z}/n\mathbb{Z}$, so besagt die letzte Aussage, dass

$$\widetilde{\psi} : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad a \longmapsto (x \longmapsto a \cdot x)$$

ein Isomorphismus ist. Unabhängigkeit von der Wahl des Vertreters in der Klasse von a ist offensichtlich. Das Bild $\widetilde{\psi}(a)$ von $a \in (\mathbb{Z}/n\mathbb{Z})^*$ ist ein Automorphismus, denn das Bild von $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ ist die gesuchte Umkehrabbildung. Ist $\widetilde{\psi}(a) = \mathrm{id}$, also $a \cdot 1 \equiv 1 \mod n$, so ist a das neutrale Element in $(\mathbb{Z}/n\mathbb{Z})^*$ und $\widetilde{\psi}$ daher injektiv. Bildet ein Automorphismus $\rho \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ das Element 1 auf a ab, und das Inverse zu ρ bildet 1 auf b ab, so gilt $a \cdot b = 1$ und daher $a \in (\mathbb{Z}/n\mathbb{Z})^*$, woraus die Surjektivität folgt. □

Satz 3.18 *Ist $K = \mathbb{Q}$, so ist die Abbildung*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathrm{Aut}(U_n)$$

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

Beweis : Sei f das Minimalpolynom von ζ_n. Wir zeigen, dass jede primitive $n-$te Einheitswurzel Nullstelle von f ist. Dann ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geq \varphi(n)$ und die umgekehrte Ungleichung folgt bereits aus dem vorigen Satz. Offenbar ist f ein Teiler von $X^n - 1$. Nach dem Gauß-Lemma bleiben die irreduziblen Faktoren in einer Zerlegung von $X^n - 1$ über $\mathbb{Z}[X]$ irreduzibel über $\mathbb{Q}[X]$. Da f und $X^n - 1$ normiert sind, muss f einer davon sein, also gilt $f \in \mathbb{Z}[X]$ und es gibt $h \in \mathbb{Z}[X]$, so dass $f \cdot h = X^n - 1$.

Es genügt zu zeigen, dass für alle $p \nmid n$ prim die Potenz ζ_n^p wieder eine Nullstelle von f ist, denn jedes m mit $\mathrm{ggT}(m, n) = 1$ lässt sich als Produkt solcher Primzahlen schreiben. Wäre die Behauptung falsch, so wäre ζ_n^p eine Nullstelle von $h(X)$, also ζ_n selbst eine Nullstelle von $h(X^p)$. Da f irreduzibel ist, folgt $f | h(X^p)$. Wir reduzieren nun die Koeffizienten modulo p, d.h. betrachten den Homomorphismus

$$\psi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]$$

Im Bild gilt $\psi\big(h(X^p)\big) = \psi\big(h(X)\big)^p = \psi(f) \cdot \overline{g}$ für ein Polynom $\overline{g} \in \mathbb{Z}/p\mathbb{Z}[x]$. Das aber bedeutet, dass

$$X^n - 1 = \psi(X^n - 1) = \psi(f) \cdot \psi(h) = \psi(f) \cdot \psi(f) \cdot \overline{g}$$

eine mehrfache Nullstelle hat. Da $p \nmid n$ ist dies ein Widerspruch zu den Separabilitätsaussagen am Anfang des Abschnitts. □

Das Minimalpolynom Φ_n einer primitiven $n-$ten Einheitswurzel über $\mathbb{Q}$ wird $n-$tes Kreisteilungspolynom genannt. Nach dem vorigen Satz ist

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - \zeta_n^{(i)}), \tag{2}$$

wobei $\{\zeta_n^{(1)}, \ldots, \zeta_n^{(\varphi(n))}\}$ eine Liste der primitiven $n-$ten Einheitswurzeln ist. Ist p prim, so hat

$$\Phi_p = (X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \ldots + X + 1$$

den Grad $\varphi(p) = p - 1$. Allgemein berechnet man Kreisteilungspolynome zum Beispiel wie folgt.

Proposition 3.19 *Es gilt* $X^n - 1 = \prod_{d|n, d>0} \Phi_d$.

Beweis : Sei P_d die Menge der primitiven $d-$ten Einheitswurzeln. Jede $n-$te Einheitswurzel ist in einem der P_d für ein $d|n$, genauer ist $d(\zeta) = \min\{a > 0 : \zeta^a = 1\}$. Also ist $U_n = \bigcup_{d|n, d>0} P_d$ und diese Vereinigung ist disjunkt. Die Behauptung folgt nun aus der Darstellung (2) des Kreisteilungspolynoms. □

Will man Φ_n berechnen und kennt man bereits Φ_d für $d < n$, so kann man Φ_n durch abdividieren der anderen Faktoren aus der Proposition (nicht besonders effizient) berechnen, z.B.

$$\Phi_{104} = X^{48} - X^{44} + X^{40} - X^{36} + X^{32} - X^{28} + X^{24} - X^{20} + X^{16} - X^{12} + X^8 - X^4 + 1.$$

Dabei stellt man fest, dass alle $\Phi_n, n \leq 104$ nur Koeffizienten in $\{-1, 0, +1\}$ haben. Ab Φ_{105} ändert sich das, denn einer der Koeffizienten von Φ_{105} ist -2. Das liegt daran, dass $105 = 3 \cdot 5 \cdot 7$ Produkt dreier verschiedener Primfaktoren ungleich zwei ist. Sei $A(n)$ das Maximum der Beträge der Koeffizienten von Φ_n. Diese Funktion $A(n)$ ist vollkommen elementar definiert, n hat viele Publikationen der elementaren Zahlentheorie hervorgerufen und dennoch ist einiges unbekannt. Zum Beispiel hatte 1968 Schwester Marion Beiter einiges über $A(n)$ im Fall von $n = p \cdot q \cdot r$ Produkt dreier Primzahlen $(p < q < r)$ herausgefunden und vermutet, dass $A(p \cdot q \cdot r) \leq \frac{p+1}{2}$. Die Schranke $A(p \cdot q \cdot r) \leq \frac{3p}{4}$ ist in der Tat bewiesen, aber in [GM] wurde gezeigt, dass es eine Folge (p_j, q_j, r_j) gibt mit $\limsup A(p_j q_j r_j)/p_j \geq 2/3$. Also ist die ursprüngliche Vermutung falsch, aber der optimale Wert des $\limsup$, welcher irgendwo in $[2/3, 3/4]$ liegen muss, ist bislang unbekannt.

3.4 Norm und Spur

Ist L/K eine endliche Körpererweiterung und $\alpha \in L$, so will man oft charakteristische Größen von α schnell bestimmen. Natürlich besitzt α ein Minimalpolynom f_α und (wenn wir wie immer f_α normiert voraussetzen) so sind alle Koeffizienten von f_α solche charakteristischen Größen, aber manche davon sind bequemer zu bestimmen als andere.

Zum Vergleich sei $\varphi : V \to V$ ein Endomorphismus eines endlichdimensionalen $K-$Vektorraums V. Dann wird φ sein charakteristisches Polynom $\chi = \chi_\varphi$ zugeordnet und zwei Koeffizienten werden in der linearen Algebra besonders studiert. Ist

$\chi = \sum_{i=0}^{n} c_i X^{n-i}$, so ist

$$\mathrm{Spur}(\varphi) = -c_1 \text{ und } \mathrm{Det}(\varphi) = (-1)^n c_n.$$

Natürlich stimmt dieser Begriff mit der Spur und Determinante einer Matrix überein, wenn man eine beliebige Darstellungsmatrix verwendet.

Wir spezialisieren auf $V = L$ und $\varphi = \varphi_\alpha$ die (Links-)Multiplikation mit $\alpha \in L$.

Definition 3.20 *Die* Spur *von $\alpha \in L$ ist definiert als*

$$\mathrm{Spur}_K^L(\alpha) = \mathrm{Spur}(\chi_{\varphi_\alpha})$$

und die Norm durch

$$\mathrm{Norm}_K^L(\alpha) = \mathrm{Det}\big(\chi_{\varphi_\alpha}\big).$$

Aus den bekannten Rechenregeln $\mathrm{Spur}(a\varphi + b\zeta) = a\,\mathrm{Spur}(\varphi) + b\,\mathrm{Spur}(\zeta)$ und $\mathrm{Det}(\varphi \circ \zeta) = \mathrm{Det}(\varphi) \cdot \mathrm{Det}(\zeta)$ für beliebige Endomorphismen von V und $a, b \in K$ folgt sofort für $\alpha, \beta \in L$ und $a, b \in K$

$$\mathrm{Spur}_K^L(a\alpha + b\beta) = a\,\mathrm{Spur}_K^L(\alpha) + b\,\mathrm{Spur}_K^L(\beta), \quad \mathrm{Norm}_K^L(\alpha\beta) = \mathrm{Norm}_K^L(\alpha) \cdot \mathrm{Norm}_K^L(\beta).$$

Proposition 3.21 *Ist $L = K(\alpha)$, so sind Spur und Norm Koeffizienten des Minimalpolynoms, genauer gesagt ist $f_\alpha = \sum_{i=0}^{n} c_i X^{n-i}$ das Minimalpolynom von α, so ist*

$$\mathrm{Spur}_K^L(\alpha) = -c_1 \quad \textit{und} \quad \mathrm{Norm}_K^L(\alpha) = (-1)^n c_n.$$

Beweis : Es ist nun zu zeigen, dass für $L = K(\alpha)$ das Minimalpolynom f_α und χ_{φ_α} übereinstimmen. Da $f_\alpha(\alpha) = 0$ ist auch für jedes $x \in L$

$$\begin{aligned} f_\alpha(\varphi_\alpha)(x) &= \left(\sum_{i=0}^{n} c_i \varphi_\alpha^{n-i}\right)(x) = \sum_{i=0}^{n} c_i(\alpha^{n-i} \cdot x) \\ &= \left(\sum_{i=0}^{n} c_i \alpha^{n-i}\right) \cdot x = 0. \end{aligned}$$

Das Minimalpolynom von φ_α teilt also f_α und aus der gleichen Rechnung folgt die umgekehrte Teilbarkeit. Das Minimalpolynom von f_α und das von φ_α stimmen also überein.

Aus Gradgründen ist hier das Minimalpolynom von φ_α gleich dem charakteristischen Polynom und daraus folgt die Behauptung. □

Im anderen Extrem gilt, ist $\alpha \in K$, so ist die Darstellungsmatrix eine Diagonalmatrix mit α auf der Diagonale und daher

$$\mathrm{Spur}_K^L(\alpha) = [L:K] \cdot \alpha \quad \text{und} \quad \mathrm{Norm}_K^L(\alpha) = \alpha^{[L:K]}.$$

Proposition 3.22 *Norm und Spur sind transitiv, d.h. sind $K \leq F \leq L$ endliche Körpererweiterungen, so gilt für alle $\alpha \in L$*

$$\mathrm{Spur}_K^L(\alpha) = \mathrm{Spur}_K^F\big(\mathrm{Spur}_F^L(\alpha)\big) \textit{ und } \mathrm{Norm}_K^L(\alpha) = \mathrm{Norm}_K^F\big(\mathrm{Norm}_F^L(\alpha)\big).$$

Beweis : Sei $m = [F : K]$ und $n = [L : F]$. Sei $x_1, \ldots, x_m$ eine $K-$Basis von F und $y_1, \ldots, y_n$ eine $F-$Basis von L. Dann ist $\{x_i y_j\}$ eine K-Basis von L und wir suchen die Darstellungsmatrix $M_K \in K^{mn \times mn}$ von φ_α in dieser Basis. Sei zunächst $M_F = (\alpha_{\mu\nu})_{\mu\nu} \in F^{n\times n}$ die Darstellungsmatrix von φ_α als F-linearer Endomorphismus von L. Sei $(a_{ij}^{\mu\nu})_{ij} \in K^{m\times m}$ die Darstellungsmatrix der Multiplikation mit $\alpha_{\mu\nu}$. Wir betrachten die Abbildung („Blockdarstellung“)

$$B : \begin{array}{ccc} F^{n\times n} & \longmapsto & K^{mn\times mn} \\ (\alpha_{\mu\nu})_{\mu\nu} & \longmapsto & \left(a_{\overline{ij}}^{\lceil \frac{i}{m} \rceil, \lceil \frac{j}{n} \rceil}\right)_{ij} \end{array},$$

wobei Querstriche Restklassen modulo m, aber im Vertretersystem $1, \ldots, m$ bedeuten.

Dann ist

$$\begin{aligned} \varphi_\alpha(x_i y_j) &= x_i \sum_{\nu=1}^{n} \alpha_{j\nu} y_\nu = \sum_{\nu=1}^{n} (\alpha_{j\nu} x_i) y_\nu \\ &= \sum_{\nu=1}^{n} \sum_{\mu=1}^{m} (a_{i\mu}^{j\nu} \cdot x_\mu) y_\nu \\ &= \sum_{\nu=1}^{n} \sum_{\mu=1}^{m} B(M_F)_{(j-1)\cdot m+i,\ (\nu-1)m+\mu} \cdot x_\mu y_\nu, \end{aligned}$$

also ist $B(M_F)$ in der Tat die Darstellungsmatrix M_K. Wir behaupten, dass für alle $M \in F^{n\times n}$

$$\mathrm{Spur}(B(M)) = \mathrm{Spur}_K^F(\mathrm{Spur}(M)) \text{ und } \mathrm{Det}(B(M)) = \mathrm{Norm}_K^F(\mathrm{Det}(M))$$

gilt. Daraus folgt direkt

$$\mathrm{Spur}_K^L(\alpha) = \mathrm{Spur}(B(M_F)) = \mathrm{Spur}_K^F(\mathrm{Spur}(M_F) = \mathrm{Spur}_K^F(\mathrm{Spur}_F^L(\alpha))$$

die gewünschte Behauptung für die Spur und analog für die Norm.

Die behauptete Aussage für die Spur folgt direkt aus

$$\mathrm{Spur}_K^F(\mathrm{Spur}(M)) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ii}^{jj} = \sum_{k=1}^{m\cdot n} B(M)_{k,k}.$$

Für die Determinantenaussage zeigen wir, dass B ein Ringhomomorphismus ist. Bis auf die Multiplikativität ist das offensichtlich. Für $M = (\alpha_{\mu\nu})$ und $N = (\beta_{\mu\nu})$, welche als Darstellungsmatrizen $(a_{ij}^{\mu\nu})_{i,j=1,\ldots,n}$ und $(b_{ij}^{\mu\nu})_{i,j=1,\ldots,n}$ haben, rechnen wir nach, dass

$$\begin{aligned}\left(\sum_{\lambda=1}^{n}\alpha_{\mu\lambda}\beta_{\lambda\nu}\right) x_i &= \sum_{\lambda=1}^{n}\beta_{\lambda\nu}\sum_{j=1}^{m} a_{ij}^{\mu\lambda}x_j = \sum_{\lambda=1}^{n}\sum_{j=1}^{m} a_{ij}^{\mu\lambda}\beta_{\lambda\nu}x_j \\ &= \sum_{\lambda=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{m} a_{ij}^{\mu\lambda}b_{jk}^{\lambda\nu}x_k.\end{aligned}$$

Die Matrixeinträge von

$$B(MN) = B\left(\left(\sum_{\lambda=1}^{n}\alpha_{\mu\lambda}\beta_{\lambda\nu}\right)_{\mu\nu}\right)$$

sind also von der Bauart

$$\sum_{\lambda=1}^{n}\sum_{j=1}^{m} a_{ij}^{\mu\lambda}b_{jk}^{\lambda\nu}, \qquad i,k \in \{1,\ldots,m\};\ \mu,\nu \in \{1,\ldots,n\}.$$

Dies sind auch genau die Einträge von $B(M)\cdot B(N)$, was wir zeigen wollten. Die Determinantenaussage ist für obere und untere Dreiecksmatrizen offensichtlich und nach dem Gauß-Algorithmus lässt sich jede Matrix als Produkt solcher Matrizen schreiben. (Zeilen-/Spaltenvertauschung benötigt man nicht gesondert, wie man anhand von

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

einsieht.) Ist also $M = \prod_{i=1}^{k} D_i$ mit D_i Dreiecksmatrizen, so ist schließlich

$$\begin{aligned}\mathrm{Det}\left(B(M)\right) &= \mathrm{Det}\left(B\left(\prod_{i=1}^{k} D_i\right)\right) = \prod_{i=1}^{k}\mathrm{Det}\left(B(D_i)\right) \\ &= \prod_{i=1}^{k}\mathrm{Norm}_K^F\left(\mathrm{Det}(D_i)\right) = \mathrm{Norm}_K^F\left(\mathrm{Det}\left(\prod_{i=1}^{k} D_i\right)\right) \\ &= \mathrm{Norm}_K^F\left(\mathrm{Det}(M)\right).\end{aligned}$$

□

Satz 3.23 *Ist L/K separabel und endlich vom Grad $[L : K] = r$ und $\tau_i \colon L \hookrightarrow \overline{K}$ für $i = 1, \ldots, r$ die Fortsetzung der Einbettung $K \hookrightarrow \overline{K}$ in einem algebraischen Abschluß, so ist für alle $\alpha \in L$*

$$\mathrm{Spur}_K^L(\alpha) = \sum_{i=1}^{r} \tau_i(\alpha) \quad \textit{und} \quad \mathrm{Norm}_K^L(\alpha) = \prod_{i=1}^{r} \tau_i(\alpha).$$

Ist L/K galoissch, so können wir τ_i als Automorphismen von L auffassen und die Summe bzw. das Produkt beinhaltet nur Elemente in L.

Beweis : Den Spezialfall $\alpha \in K$ haben wir bereits behandelt. Wir betrachten nun den Spezialfall $L = K(\alpha)$. Dann hat das Minimalpolynom die Faktorisierung

$$\sum_{i=0}^{n} c_i X^{n-i} = f_\alpha = \prod_{i=1}^{r} \Big(X - \tau_i(\alpha) \Big).$$

Also ist

$$\mathrm{Spur}_K^L(\alpha) = -c_1 = \sum_{i=1}^{r} \tau_i(\alpha)$$

und

$$\mathrm{Norm}_K^L(\alpha) = (-1)^n c_n = \prod_{i=1}^{r} \tau_i(\alpha).$$

Den allgemeinen Fall setzen wir aus diesen Spezialfällen und der Transitivität zusammen. Wir betrachten dazu $K \subset K(\alpha) \subset L$. Es seien $r_1 = \Big[K(\alpha) : K\Big]$ und $r_2 = [L : K(\alpha)]$. Weiter seien $\tau_1, \ldots, \tau_r$ die (paarweise verschiedenen) Fortsetzungen der Inklusion $K \to \overline{K}$ nach L, $\eta_1 \ldots, \eta_{r_1}$ seien die (paarweise verschiedenen) Fortsetzungen der Inklusion $K \to \overline{K}$ nach $K(\alpha)$ und für jedes $i = 1, \ldots, r_1$ seien η_{ij}, $j = 1, \ldots, r_2$ die (paarweise verschiedenen) Fortsetzungen von $\eta_i : K(\alpha) \to \overline{K}$ nach L. Die Einbettungen

$$\Big\{ \eta_{ij} : L \longrightarrow \overline{K},\ i = 1, \ldots, r_1 \text{ und } j = 1, \ldots, r_2 \Big\}$$

sind paarweise verschieden und damit bis auf Umnummerierung gleich $\tau_1, \ldots, \tau_r$. Denn angenommen $\eta_{ij} = \eta_{kl}$. Dann gilt nach Einschränkung auf $K(\alpha)$, dass $\eta_i = \eta_{ij}|_{K(\alpha)} = \eta_{kl}|_{K(\alpha)} = \eta_k$, also $i = k$ und damit auch $j = l$. Also ist

$$\begin{aligned} \mathrm{Spur}_K^L(\alpha) = \mathrm{Spur}_K^{K(\alpha)}(\mathrm{Spur}_{K(\alpha)}^L(\alpha)) &= [L : K(\alpha)] \cdot \sum_{i=1}^{r_1} \eta_i(\alpha) \\ &= \sum_{i=1}^{r_1} \sum_{j=1}^{r_2} \eta_{ij}(\alpha) = \sum_{i=1}^{r} \tau_i(\tau) \end{aligned}$$

und

$$\begin{aligned}\mathrm{Norm}_K^L(\alpha) = \mathrm{Norm}_K^{K(\alpha)}(\mathrm{Norm}_{K(\alpha)}^L(\alpha)) &= \prod_{i=1}^{r_1} \eta_i(\alpha)^{[L:K(\alpha)]} \\ &= \prod_{i=1}^{r_1}\prod_{j=1}^{r_2} \eta_{ij}(\alpha) = \prod_{i=1}^{r} \tau_i(\alpha)\end{aligned}$$

□

3.5 Zyklische Erweiterungen

Angenommen K enthält bereits die n-ten Einheitswurzeln. Wir wollen die Erweiterungen von K charakterisieren, die als Zerfällungskörper von $X^n - c$ auftreten. Dies leistet der folgende Satz, dessen Beweis einige Hilfsmittel erfordert. In diesem Abschnitt ist stets $\mathrm{char}(K)$ kein Teiler von n.

Satz 3.24 *Ist $U_n \subset K$ und $L = K(a)$, wobei a Nullstelle von $X^n - c$ ist, dann ist L/K zyklisch. Weiter ist $d = [L : K]$ ein Teiler von n, es ist $a^d \in K$ und $f_a = X^d - a^d \in K[X]$ ist das Minimalpolynom.*
Ist umgekehrt $U_n \subset K$ und L/K zyklisch von Ordnung n, so gibt es ein $a \in L$ mit $L = K(a)$ und $f_a = X^n - a^n \in K[X]$ ist das Minimalpolynom von a.

Als ersten Schritt beweisen wir einen Satz, der als lineare Unabhängigkeit von Charakteren bezeichnet wird. Ein K-wertiger *Charakter* einer Gruppe G ist ein Homomorphismus

$$\chi\colon G \longrightarrow K^*.$$

Das Produkt zweier Charaktere χ_1 und χ_2 ist definiert durch

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$$

und mit dieser Verknüpfung wird die Menge der Charaktere eine Gruppe.

Die Menge $Abb(G, K)$ der Abbildungen von G nach K bildet via

$$(f_1 + f_2)(g) = f_1(g) + f_2(g) \text{ und } (\lambda \cdot f_1)(g) = \lambda \cdot f_1(g)$$

einen K-Vektorraum. Dieser enthält per Definition alle Charaktere von G.

Satz 3.25 *Verschiedene K-wertige Charaktere $\chi_1, \ldots, \chi_n$ von G sind linear unabhängig in $Abb(G, K)$.*

Beweis : Angenommen die Behauptung ist falsch und wir wählen ein Gegenbeispiel mit n minimal. Offenbar ist $n \geqslant 2$. Sei

$$\sum_{i=1}^{n} a_i \cdot \chi_i = 0$$

die lineare Relation. Alle a_i sind von Null verschieden aufgrund der Minimalität. Es gilt also $\sum_{i=1}^{n} a_i \cdot \chi_i(g \cdot h) = 0$ für alle $g, h \in G$. Wir wählen g so, dass $\chi_1(g) \neq \chi_2(g)$ ist. Es ist

$$\sum_{i=1}^{n} a_i \chi_i(g) \cdot \chi_i = 0,$$

da wir oben bereits gesehen haben, dass die Beziehung für alle $h \in G$ gilt. Aus den beiden Relationen können wir die neue Relation

$$\sum_{i=2}^{n} a_i \Big(\chi_i(g) - \chi_1(g)\Big)\chi_i = 0$$

zusammenbauen. Da $a_2\Big(\chi_1(g) - \chi_2(g)\Big) \neq 0$, ist diese Relation nicht trivial, im Widerspruch zur Minimalität. □

Damit können wir folgende Charakterisierung zyklischer Erweiterungen beweisen. Was hier ein Hilfssatz ist, kann als der Anfang der Galoiskohomologie gesehen werden.

Proposition 3.26 (Hilberts Satz 90) *Sei L/K zyklisch und $\langle\tau\rangle = Gal\,(L/K)$. Dann ist $\mathrm{Norm}_K^L(b) = 1$ genau dann, wenn es ein $a \in L^*$ gibt mit $b = a \cdot \tau(a)^{-1}$.*

Beweis : Wenn es solch ein a gibt, so folgt offenbar

$$\mathrm{Norm}_K^L(b) = \frac{\mathrm{Norm}_K^L(a)}{\mathrm{Norm}_K^L\big(\tau(a)\big)} = 1$$

nach Satz 3.23. Für die Umkehrung sei solch ein b gegeben und wir setzen $n = [L : K]$. Wir betrachten die Elemente $\tau^i \in \mathrm{Gal}(L/K)$ als Charaktere der Gruppe L^*. Aufgrund deren linearer Unabhängigkeit ist

$$f = \tau^0 + b \cdot \tau^1 + b \cdot \tau(b) \cdot \tau^2 + \ldots + b \cdot \tau(b)\tau^2(b) \cdots \tau^{n-2}(b) \cdot \tau^{n-1}$$

nicht die Nullabbildung $L^* \longrightarrow L$. Also gibt es ein $c \in L$, sodass $a = f(c) \neq 0$ ist. Dann ist

$$b \cdot \tau(a) = b \cdot \tau^1(c) + b \cdot \tau(b) \cdot \tau^2(c) + \ldots + \underbrace{b \cdot \tau(b)\tau^2(b) \cdots \tau^{n-1}(b)}_{=\mathrm{Norm}_K^L(b)=1} \underbrace{\tau^n(c)}_{=\tau^0(c)} = a,$$

also $b = a \cdot \tau(a)^{-1}$. □

Beweis von Proposition 3.24 : Wir beginnen mit der Umkehrung. Da eine primitive n-te Einheitswurzel ζ in K enthalten ist und L/K als zyklisch vorausgesetzt ist, gilt

$$\mathrm{Norm}_K^L(\zeta^{-1}) = \prod_{i=0}^{n-1} \sigma^i(\zeta^{-1}) = \zeta^{-n} = 1.$$

Nach Hilberts Satz 90 gibt es also ein $a \in L$ mit $\sigma(a) = \zeta \cdot a$. Insbesondere sind die Galois- Bilder $\sigma^i(a) = \zeta^i a$ für $i = 0, \ldots, n-1$ paarweise verschieden und damit $L = K(a)$, denn $[K(a) : K] \geq n$. Weiter ist $\sigma(a^n) = \zeta^n a^n = a^n$, also $a^n \in K$. Also ist a Nullstelle des Polynoms $X^n - a^n \in K[X]$, welches aus Gradgründen das Minimalpolynom von a ist.

Für die andere Richtung können wir $c \neq 0$ annehmen. Die Nullstellen $\zeta^i a$ für $i = 0, \ldots, n-1$ sind paarweise verschieden und damit alle Nullstellen von $X^n - c$. Also ist L Zerfällungskörper dieses Polynoms und aufgrund der Charakteristikvoraussetzung ist L/K separabel und somit galoissch. Ist $\sigma \in \mathrm{Gal}(L/K)$, so ist auch $\sigma(a)$ eine Nullstelle von $X^n - c$, also $\sigma(a) = \zeta_\sigma a$ für ein $\zeta_\sigma \in U_n$.

Diese Zuordnung $\mathrm{Gal}(L/K) \longrightarrow U_n$, $\sigma \mapsto \zeta_\sigma$ ist ein Homomorphismus, denn für σ, $\tau \in \mathrm{Gal}(L/K)$ gilt

$$\zeta_{\sigma\tau} \cdot a = (\sigma\tau)(a) = \sigma(\zeta_\tau \cdot a) = \zeta_\tau \cdot \sigma(a) = \zeta_\tau \cdot \zeta_\sigma \cdot a.$$

Außerdem ist diese Zuordnung injektiv, denn aus $\sigma(a) = a$ folgt wegen $L = K(a)$, dass $\sigma = \mathrm{id}$ gilt. Da U_n zyklisch ist, muss auch $\mathrm{Gal}(L/K)$ zyklisch sein. Sei nun $\sigma \in \mathrm{Gal}(L/K)$ ein Erzeuger dieser Gruppe, welche eine Ordnung d mit $d \mid n = \#U_n$ hat. Dann ist ζ_σ eine primitive d-te Einheitswurzel. Wie am Ende der anderen Implikation ist wieder

$$\sigma(a^d) = \zeta_\sigma^d \cdot a^d = a^d,$$

also $a^d \in K$ und aus Gradgründen $X^d - a^d \in K[X]$ das Minimalpolynom von a über K. □

3.6 Auflösbarkeit I: Körpererweiterungen

Die bekannte Lösungsformel für quadratische Gleichungen und die weniger bekannten Versionen für kubische Gleichungen und Gleichungen vom Grad 4 enthalten nur Wurzeln und Körperoperationen des Grundkörpers. Im folgenden Begriff gestatten wir aus technischen Gründen auch die Hinzunahme von Einheitswurzeln. Wenn wir damit keine Gleichungen 5. oder höheren Grades auflösen können, dann sicher auch nicht ohne Verwendung von Einheitswurzeln.

Wir schränken uns in diesem Abschnitt auf Charakteristik 0 ein. Für eine entsprechende Theorie in $\mathrm{char}(K) = p > 0$ müssten wir noch zyklische Erweiterungen vom Grad p, sogenannte Artin-Schreier-Erweiterungen diskutieren.

Definition 3.27 *Eine Körpererweiterung L/K mit $\mathrm{char}(K) = 0$ heißt* durch Radikale auflösbar*, falls L in einem Körper E enthalten ist, der eine Kette von Erweiterungen*

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

besitzt, sodass E_{j+1} aus E_j durch Adjunktion

(1) einer Einheitswurzel oder

(2) einer Nullstelle eines Polynoms $X^n - a \in E_j[X]$

hervorgeht.

Angenommen die Erweiterung E/K ist galoissch. Wir können den Körperturm der Auflösbarkeit durch Radikale so sortieren, dass $E_{j+1} = E_j(\alpha_{j+1})$ mit α_j eine Einheitswurzel für $j \in \{1, \ldots, r\}$ und vom Typ (2) für $j \in \{r+1, \ldots, m\}$ ist. Dann ist also E_{j+1}/E_j galoissch für jedes j. Diesen Sachverhalt werden wir bald in der Sprache der Gruppentheorie formulieren. Zuvor halten wir noch zwei Bemerkungen über Auflösbarkeit durch Radikale fest, deren gruppentheoretisches Analogon wir nach einem längeren Ausflug in die Gruppentheorie formulieren.

Lemma 3.28 *Ist L/K durch Radikale auflösbar und F/K algebraisch sowie FL das Kompositum in einem fixierten algebraischen Abschluss $\overline{F}$ von F, so ist auch FL über F durch Radikale auflösbar.*

Beweis : Klar, man betrachte E als Teilkörper von $\overline{F}$. Dann ist die Kette $F \subseteq FE_1 \subseteq \ldots \subseteq FE_m$ von der gewünschten Gestalt. □

Lemma 3.29 *Ist $M \supseteq L \supseteq K$ eine Kette von Körpererweiterungen, dann ist M/K durch Radikale auflösbar genau dann, wenn M/L und L/K dies sind.*

Beweis : Die direkte Implikation ist klar, denn eine durch Radikale auflösbare Erweiterung von M/K ist auch eine von L/K und das Kompositum von einer Radikalauflösung von M/K mit L liefert eine Radikalauflösung von M/L.
Umgekehrt sei L_1 eine Erweiterung von L, sodass L_1/K eine Kette von Radikalerweiterungen besitzt. Sei E eine Erweiterung von M, sodass E/L eine Kette von Radikalerweiterungen besitzt. Dann besitzt auch das Kompositum EL_1 in einem algebraischen Abschluss von K über L_1 eine Kette von Radikalerweiterungen. Zusammen mit der Kette von L_1/K sichert das die Auflösbarkeit von M/K. □

4 Mehr Gruppentheorie

In diesem Abschitt wollen wir die Struktur endlicher Gruppen näher untersuchen, motiviert durch die Untersuchung endlicher Galoiserweiterungen. Die Struktur dieser Gruppen ist außerordentlich kompliziert. Die Bausteine, sogenannte einfache Gruppen, sind inzwischen (seit 1981) klassifiziert, aber der Beweis umfasst ca. 10.000 Seiten Veröffentlichungen in Fachzeitschriften. Die Schwierigkeit liegt darin, dass wir hier auf nicht-abelsche Gruppen fokussiert sind. Die Klassifikation abelscher Gruppen werden wir in einem späteren Kapitel vollständig verstehen.

Wir setzen in diesem Abschnitt grundlegende Definitionen wie Gruppenoperationen sowie Zykelschreibweise von Permutationsgruppen voraus. Diese können z.B. in [GA] nachgelesen werden.

4.1 Die Sylowsätze

Ist H eine Untergruppe von G, so teilt die Ordnung von H die Ordnung von G. Die umgekehrte Frage, für welche Teiler der Ordnung von G es Untergruppen der entsprechenden Ordnung gibt, und wenn ja wie viele, ist viel schwerer zu beantworten. Ist der Teiler eine Primzahlpotenz, so geben die Sylowsätze darauf eine befriedigende Antwort.

Definition 4.1 *Sei G eine endliche Gruppe und p eine Primzahl. Ist* $\mathrm{ord}(G)$ *eine p-Potenz, so wird G eine* p-Gruppe *genannt. Eine Untergruppe $H \leqslant G$ heißt* p-Sylow-Gruppe, *falls H eine p-Gruppe ist und p den Index $[G : H]$ nicht teilt.*

Die p-Sylowgruppen in G sind also die p-Untergruppen maximaler Ordnung in G. Wir untersuchen zunächst die Struktur von p-Gruppen. Erinnern wir uns daran, dass das *Zentrum* von G definiert ist als

$$Z(G) = \{\sigma \in G \colon \tau\sigma = \sigma\tau \text{ für alle } \tau \in G\}.$$

Proposition 4.2 *Sei G eine p-Gruppe der Ordnung p^k mit $k \geqslant 1$. Dann teilt p die Ordnung von $Z(G)$, also $Z(G) \neq \{1\}$.*

Beweis : Wir betrachten die Operation von G auf G selbst durch Konjugation, $(g, h) \longmapsto ghg^{-1}$. Die Bahnbilanz besagt für ein Vertretersystem $x_1, \ldots, x_n$ der Bahnen, dass

$$\mathrm{ord}(G) = \sum_{i=1}^{n} [G : \mathrm{Stab}_G(x_i)].$$

Ist $x \in Z(G)$, so ist seine Bahn einelementig und $G = \mathrm{Stab}_G(x)$. Also können wir annehmen, dass $\{x_1, \ldots, x_k\} = Z(G)$. Dann besagt die Bahnbilanz

$$\mathrm{ord}(G) = \mathrm{ord}(Z(G)) + \sum_{i=k+1}^{n} [G : \mathrm{Stab}_G(x_i)].$$

Da für $i > k$ der Stabilisator von x_i strikt kleiner als G ist, sind $\mathrm{ord}(G)$ und $[G : \mathrm{Stab}_G(x_i)]$ durch p teilbar, also auch $\mathrm{ord}(Z(G))$. □

Korollar 4.3 *Ist G eine p-Gruppe der Ordnung p^k, dann gibt es eine Kette von Untergruppen*

$$G = G_k \supseteq G_{k-1} \supseteq \ldots G_1 \supseteq G_0 = \{1\},$$

wobei $\mathrm{ord}(G_j) = p^j$ *und G_j in G_{j+1} ein Normalteiler ist.*

Dieser Satz beantwortet also für p-Gruppen vollständig die Existenz von Gruppen für alle Teiler von p^k und die Kette ist Modell dessen, was wir unten als auflösbar definieren werden.

Beweis : Der Fall $k = 0$ oder $k = 1$ ist trivial und wir argumentieren per Induktion. Sei $a \in Z(G)\backslash\{1\}$ und $\mathrm{ord}(a) = p^r$. Dann hat $b = a^{p^{r-1}}$ die Ordnung p und $\langle b\rangle \subseteq Z(G)$

ist ein Normalteiler in G. Also ist $G/\langle b\rangle$ eine Gruppe der Ordnung p^{k-1}, auf die wir die Induktionsvoraussetzung anwenden. Sei

$$G/\langle b\rangle = \overline{G}_{k-1} \supseteq \overline{G}_{k-2} \supseteq \ldots \supseteq \overline{G}_1 \supseteq \overline{G}_0 = \{1\}$$

die zugehörige Kette und $\pi\colon G \longrightarrow G/\langle b\rangle$ die Quotientabbildung. Dann hat $\pi^{-1}(\overline{G}_k)$ die Ordnung p^{k+1}. Wir setzen also $G_j = \pi^{-1}(\overline{G}_{j-1})$ für $j \geqslant 1$ und $G_0 = \{1\}$. Dann ist G_j der Kern des Homomorphismus.

$$pr_j \circ \pi|_{G_{j+1}} : G_{j+1} \longrightarrow \overline{G}_j \longrightarrow \overline{G}_j/\overline{G}_{j-1},$$

also ein Normalteiler in G_{j+1}. □

Korollar 4.4 *Ist* $\mathrm{ord}(G) = p$ *oder* $\mathrm{ord}(G) = p^2$*, so ist* G *abelsch.*

Beweis : Der erste Fall folgt direkt aus der Proposition. Ist im zweiten Fall $Z(G) = G$, so ist die Folge klar. Im anderen Fall ist $G/Z(G)$ von Ordnung p, also zyklisch und die Aussage folgt aus dem nächsten Lemma. □

Lemma 4.5 *Ist* $G/Z(G)$ *zyklisch, so ist* G *abelsch.*

Beweis : Wähle $a \in G$ so, dass $\langle\overline{a}\rangle = G/Z(G)$. Sind g, h beliebig und $\overline{g} = \overline{a}^m$ und $\overline{h} = \overline{a}^n$ ihre Restklassen, d.h. es gibt $g_1, h_1 \in Z(G)$ mit $g = a^m g_1$ und $h = a^n h_1$. Dann gilt

$$gh = a^m g_1 a^n h_1 = a^{m+n} g_1 h_1, \quad hg = a^n h_1 a^m g_1 = a^{n+m} h_1 g_1 = a^{m+n} g_1 h_1,$$

also $gh = hg$ wie behauptet. □

Satz 4.6 (Sylow) *Sei* G *eine endliche Gruppe und* p *prim.*

i) Jede p*-Untergruppe* H *ist in einer* p*-Sylowgruppe* S *enthalten.*

ii) Ist S *eine* p*-Sylowgruppe und* S_2 *zu* S *konjugiert, so ist auch* S_2 *eine* p*-Sylowgruppe.*

iii) Umgekehrt sind je zwei p*-Sylowgruppen zueinander konjugiert.*

iv) Die Anzahl s *der* p*-Sylowgruppen genügt den zwei Bedingungen.*

$$s \mid \mathrm{ord}(G) \quad \textit{und} \quad s \equiv 1 \mod p.$$

Wir beginnen den Beweis mit einem Lemma, das letztlich die Kongruenz in iv) liefert.

Lemma 4.7 *Ist* $\mathrm{ord}(G) = n = p^k \cdot m$*, aber nicht notwendig* $ggT(p, m) = 1$*, dann gilt für die Anzahl* s *der* p*-Untergruppen* $H \leq G$ *mit* $\mathrm{ord}H = p^k$ *die Kongruenz*

$$s \equiv \binom{n-1}{p^k-1} \equiv \frac{1}{m}\binom{n}{p^k} \mod p.$$

Beweis : Sei $X \subseteq P(G)$ die Menge aller p^k-elementigen Teilmengen. Die Menge X hat $\binom{n}{p^k}$ Elemente. G operiert auf X durch Linksmultiplikation:

$$G \times X \longrightarrow X, \quad (g, U) \longmapsto \{g \cdot u, u \in U\} =: gU.$$

Sei $G(U)$ für $U \in X$ die G-Bahn von U und $G_U = \{g \in G : gU = U\}$ der Stabilisator von U. Jedes U ist eine Teilmenge von G und daher operiert G_U auf U durch Linksmultiplikation. Die Untergruppe $G_U \leqslant G$ operiert auch durch Linksmultiplikation auf ganz G. Die Bahnen haben alle die Mächtigkeit $\mathrm{ord}(G_U)$ und entsprechen den Rechtsnebenklassen $G_U \setminus G$. Also ist auch U eine disjunkte Vereinigung solcher Rechtsnebenklassen. Daher teilt die Ordnung von G_U die Mächtigkeit von U, also

$$\#G_U = p^{k'} \quad \text{für ein} \quad k' \leqslant k.$$

Wir wählen nun ein Vertretersystem $(U_i)_{i\in I}$ der Bahnen der G-Operation auf X. Die Bahnbilanz besagt dann

$$\binom{n}{p^k} = \#X = \sum_{i\in I}[G : G_{U_i}].$$

Sei $\#G_{U_i} = p^{k_i}$, also $[G : G_{U_i}] = m \cdot p^{k-k_i}$. Mit der Indexmenge $I_0 \subseteq I$ indizieren wir Bahnen mit dem größtmöglichen Stabilisator. Für alle anderen ist $[G : G_U]$ durch mp teilbar, also

$$m \cdot \#I_0 = \sum_{i\in I_0}[G : G_{Ui}] \equiv \binom{n}{p^k} \mod mp.$$

Wir müssen also nur noch zeigen, dass die Anzahl s der Untergruppen mit Mächtigkeit p^k mit $\#I_0$ übereinstimmt. Eine solche Untergruppe $H \leqslant G$ ist ein Element von X und wir betrachten seine G-Bahn $G(H)$. Da H eine Untergruppe ist, besteht diese Bahn aus m Elementen, den Nebenklassen g_iH mit geeigneten $g_i \in G$ und der Stabilisator G_H von H ist gerade H selbst. Also gibt H eine Bahn in I_0. Sind H und H'

zwei verschiedene Untergruppen der Mächtigkeit p^k, so sind die Bahnen verschieden, denn anderfalls wäre $gH = H'$ für ein $g \in G$ und wegen $1 \in H'$ folgt $g^{-1} \in H$, also $gg^{-1}H = H'$ und damit $H = H'$. Ist umgekehrt $U_i \in X$ mit $\#G_{U_i} = p^k$, so ist U_i Vereinigung von Rechtsnebenklassen von G_{U_i} hier aber genauer eine Rechtsnebenklasse von G_{U_i}, also etwa $U_i = G_{U_i} \cdot u_i$. Dann ist

$$G(U_i) = G(u_i^{-1} G_{U_i} u_i)$$

und $H = u_i^{-1} G_U u_i$ ist eine p-Untergruppe mit p^k-Elementen. Damit ist die Bijektion und das Lemma bewiesen.

Nun ist

$$\begin{aligned} \binom{m \cdot p^k}{p^k} &= \frac{mp^k \cdot (mp^k - 1) \cdot \ldots \cdot \big(mp^k - (p^k - 1)\big)}{p^k \cdot (p^k - 1) \cdot \ldots \cdot 1} \\ &= \prod_{j=0}^{p^k - 1} \frac{mp^k - j}{p^k - j}. \end{aligned}$$

Ist $\nu_p(j) = s$, so ist auch $\nu_p(p^k - j) = s$ für $j = 1, \ldots, p^k - 1$ und $\nu_p(mp^k - j) = s$, sodass insgesamt jeder der Faktoren im Produkt p-Bewertung 0 hat. Also hat auch das Produkt p-Bewertung 0 und ist modulo p betrachtet kongruent 1. Damit haben wir die Kongruenz in Satz 4.6 iv) bewiesen. □

Lemma 4.8 *Sei G eine endliche Gruppe, $H \leqslant G$ eine p-Untergruppe und $S \leqslant G$ eine p-Sylowgruppe. Dann existiert ein $g \in G$ mit $H \leqslant gSg^{-1}$.*

Beweis : Wir betrachten die Operation von H auf den Linksnebenklassen G/S durch Linksmultiplikation, d.h. $(h, gS) \longmapsto hgS$. Die Ordnung jeder Bahn ist ein Teiler von $\mathrm{ord}(H)$, also eine p-Potenz. Da $p \nmid \mathrm{ord}(G/S)$, muss mindestens eine der Bahnen die Ordnung $p^0 = 1$ haben. Für diese Bahn gilt also $hgS = gS$ für alle $h \in H$ und wegen $1 \in S$ folgt für dieses g, dass $h \in gSg^{-1}$ für alle $h \in H$, was zu zeigen war. □

Da mit S auch gSg^{-1} eine p-Sylowgruppe ist (die offensichtliche Aussage ii) von Satz 4.6), ist H in einer p-Sylowgruppe enthalten und wir haben Satz 4.6 i) bewiesen. Offenbar beweist das Lemma auch Satz 4.6 iii). Für die fehlende Aussage in iv) erinnern wir an die Definition des *Normalisators* von S (in G)

$$N_S = \{g \in G \colon gSg^{-1} = S\}.$$

Der Normalisator enthält offenbar stets S.

Lemma 4.9 *Ist G eine endliche Gruppe und S eine p-Sylowgruppe in G, so ist die Anzahl der p-Sylowgruppen gleich dem Index $[G : N_S]$.*

Beweis : Sei X die Menge der p-Sylowgruppen, auf denen G durch Konjugation operiert. Wir haben bereits oben gezeigt, dass es nur eine Bahn gibt. Per Definition ist der Stabilisator eines $S \in X$ gerade der Normalisator. Also besagt die Bahnbilanz $\#X = [G : N_S]$, was zu zeigen war. □

Da $N_S \geqslant S$ folgt Satz 4.6 iv) aus

$$s = [G : N_S] \mid [G : S] = m.$$

Wir halten noch eine wichtige Folge aus Satz 4.6 zusammen mit Proposition $(\ldots)$ fest.

Korollar 4.10 *Ist G eine endliche Gruppe und p prim, ein Teiler von* $\mathrm{ord}(G)$*, so gibt es ein Element der Ordnung p in G.*

4.2 Auflösbarkeit

Zu zwei Elementen $g, h \in G$ definieren wir den Kommutator

$$[g, h] = ghg^{-1}h^{-1}.$$

Diese Definition verallgemeinert man auf Untergruppen, indem man

$$[H_1, H_2] = \langle [h_1, h_2] : h_1 \in H_1, h_2 \in H_2 \rangle$$

als die von Kommutatoren erzeugte Untergruppe definiert. (Im allgemeinen ist das Produkt von Kommutatoren nicht selbst Kommutator zweier Elemente.) Die Gruppe G ist genau dann abelsch, wenn $[G, G] = 1$ ist. Folgendes Lemma erklärt, warum Kommutatoren im Zusammenhang mit Ketten von Untergruppen und abelschen (oder zyklischen) Faktorgruppen relevant sind.

Lemma 4.11 *Es gilt $[a, b]^{-1} = [b, a]$ und $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$ und $[G, G] \lhd G$. Genauer ist $[G, G]$ der kleinste Normalteiler, sodass die Faktorgruppe abelsch ist.*

Beweis : Die Formeln ergeben sich direkt durch Nachrechnen und zeigen auch, dass $[G,G]$ ein Normalteiler ist. In der Faktorgruppe $G/[G,G]$ gilt für alle $g,h \in G$

$$\overline{g}\overline{h}\overline{g}^{-1}\overline{h}^{-1} = \overline{[g,h]} = \overline{1},$$

also ist die Faktorgruppe abelsch. Ist $N \lhd G$ Normalteiler und G/N abelsch, so gilt für alle $g,h \in G$

$$\overline{g}\overline{h}\overline{g}^{-1}\overline{h}^{-1} = \overline{1} \quad \text{in} \quad G/N,$$

also ist $ghg^{-1}h^{-1} \in N$ und somit enthält N die Kommutatorgruppe $[G,G]$. □

Definition 4.12 *Sei G eine Gruppe. Eine Kette von Untergruppen*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{1\},$$

sodass G_{i+1} in G_i Normalteiler ist, wird als Normalreihe *von G bezeichnet. Die Gruppe G heißt* auflösbar, *falls G eine Normalreihe besitzt, sodass G_i/G_{i+1} abelsch ist.*

Lemma 4.13 *Eine endliche Gruppe G ist auflösbar, genau dann wenn G eine Normalreihe besitzt, sodass G_i/G_{i+1} zyklisch ist.*

Beweis : Zunächst zeigen wir, dass jede abelsche Gruppe eine Normalreihe besitzt, deren sukzessive Quotienten zyklisch sind. Dazu genügt es zu zeigen, dass es eine Kette von Untergruppen gibt, sodass G_i/G_{i+1} Primzahlordnung besitzt, denn die Eigenschaft Normalteiler ist in einer abelschen Gruppe automatisch erfüllt. Wir zeigen dies durch Indikation nach Anzahl der verschiedenen Primteiler. Gibt es nur einen Primteiler, ist also $\text{ord}(G) = p^k$, so liefert Korollar 4.3 die gewünschte Kette. Im Allgemeinen sei S eine p-Sylowgruppe und $\pi\colon G \longrightarrow G/S$ die Quotientabbildung. Nach Induktionsvoraussetzung besitzt G/S eine Kette von Untergruppen $\overline{G}_j, j = 0,\ldots,n$, sodass $\overline{G}_j/\overline{G}_{j+1}$ zyklisch ist. Die Kette

$$G = \pi^{-1}(\overline{G}_0) \supseteq \pi^{-1}(\overline{G}_1) \supseteq \ldots \supseteq \pi^{-1}(\overline{G}_n) = S$$

fortgesetzt mit einer Kette von Untergruppen von S mit zyklischen Quotienten leistet das Verlangte.
Den allgemeinen Fall erledigen wir mit dem gleichen Prinzip. Sei $\pi_i\colon G \longrightarrow G_i/G_{i+1}$ die Quotientabbildung und $G_i/G_{i+1} = \overline{G}_{i,0} \supseteq \overline{G}_{i,1} \supseteq \ldots \supseteq \overline{G}_{i,n(i)-1} \supseteq \{e\}$ die Kette mit zyklischen Quotienten nach dem ersten Fall. Sei $G_{i,j} = \pi^{-1}(\overline{G_{i,j}})$. Diese Gruppen bilden die gewünschte Kette von G, da $G_{i,j}/G_{i,j+1} \cong \overline{G_{i,j}}/\overline{G_{i,j+1}}$ zyklisch ist. □

Wir charakterisieren Auflösbarkeit durch den iterierten Kommutator definiert durch

$$D^0G = G, \quad D^{i+1}G = [D^iG, D^iG].$$

Diese bilden die Kette

$$G = D^0G \supseteq D^1G \supseteq D^2G \supseteq \ldots \supseteq D^nG \supseteq D^{n+1}G \supseteq \ldots$$

und $D^iG/D^{i+1}G$ ist stets abelsch.

Proposition 4.14 *Die Gruppe G ist genau dann auflösbar, wenn es ein n gibt, sodass $D^nG = \{1\}$.*

Beweis : Wenn es so ein n gibt, dann ist G offenbar auflösbar. Ist umgekehrt G auflösbar und $\{G_i, i = 1, \ldots, n\}$ eine Normalreihe, so zeigen wir induktiv $D^iG \subseteq G_i$. Dies ist für $i = 0$ per Definition richtig. Da G_i/G_{i+1} abelsch ist, folgt $[G_i, G_i] \subseteq G_{i+1}$, also per Induktion

$$D^{i+1}G = [D^iG, D^iG] \subseteq [G_i, G_i] \subseteq G_{i+1}.$$

Die Behauptung folgt nun aus $D^nG \subseteq G_n = \{1\}$. □

Wir haben in Korollar 4.3 gesehen, dass endliche Gruppen von Primzahlordnung auflösbar sind. Andererseits wurde in [GA] gezeigt, dass A_5 einfach ist, d.h. keinen Normalteiler außer $\{1\}$ und der ganzen Gruppe besitzt. Da A_5 nicht abelsch ist, ist A_5 nicht auflösbar. Wir verallgemeinern diese Aussage auf alle A_n und S_n unter Verwendung des Kommutatorkriteriums.

Als Vorbereitung benötigen wir folgendes Lemma.

Lemma 4.15 *Für $n \geqslant 3$ besteht A_n aus allen Elementen von S_n, die sich als Produkt von 3-Zykeln schreiben lassen.*

Beweis : Da ein 3-Zykel eine gerade Permutation ist, bleibt nur eine Inklusion zu zeigen. Dazu genügt es offenbar jedes Produkt von zwei Transpositionen als Produkt von 3-Zykeln zu schreiben. Seien $a, b, c, d \in \{1, \ldots, n\}$ paarweise verschieden. Dann ist

$$(ab)(cd) = (acb) \circ (acd)$$

und

$$(ab)(bc) = (abc),$$

womit alle Fälle abgedeckt sind. □

Proposition 4.16 *Es gilt $[S_n, S_n] = A_n$ für alle $n \geqslant 2$. Für $n \geqslant 5$ ist $[A_n, A_n] = A_n$. Für $n = 4$ ist $[A_4, A_4] \cong (\mathbb{Z}/2\mathbb{Z})^2$ die Kleinsche Vierergruppe V_4 bestehend aus allen Doppeltranspositionen und der Identität. Die Gruppen A_2 und A_3 sind zyklisch.*

Beweis : Da $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ zyklisch ist, folgt wie im vorigen Beweis $[S_n, S_n] \subseteq A_n$. Zum Nachweis der umgekehrten Inklusion genügt es nach dem vorigen Lemma, jeden 3-Zykel als Kommutator zu schreiben. Dies leistet

$$(abc) = (ac)(bc)(ac)^{-1}(bc)^{-1}.$$

Für $n = 4$ ist $[A_4, A_4] \subseteq V_4$, da $V_4 \lhd A_4$ (Konjugation bildet Doppeltranspositionen auf Doppeltranspositionen ab) ist und $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ abelsch. Die Identität

$$(ab)(cd) = (abc)(acd)(abc)^{-1}(acd)^{-1}$$

liefert die umgekehrte Inklusion.
Für $n \geqslant 5$ ist genug Platz, sodass wir zu einem gegebenen 3-Zykel (abc) zwei Elemente d, e finden, sodass die Elemente a, b, c, d, e paarweise verschieden sind. Dann gilt

$$(abc) = (abd)(ace)(abd)^{-1}(ace)^{-1}$$

und da die A_n von 3-Zykeln erzeugt ist, folgt $A_n \subseteq [A_n, A_n]$ und damit $A_n = [A_n, A_n]$. □

Wir führen noch eine Konstruktion von Gruppen ein, die Beispiele von auflösbaren Gruppen liefert, die weder abelsch noch von Primzahlordnung sind.

Seien dazu zwei Gruppen H und N sowie ein Homomorphismus $\Psi\colon H \longrightarrow \mathrm{Aut}(N)$ gegeben. Dann wird die Menge $G = N \times H$ zusammen mit der Verknüpfung

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\Psi(h_1)(n_2), h_1h_2)$$

zu einer Gruppe. (Merkregel: Will man h_1 nach rechts an n_2 vorbeiziehen, so muss man n_2 um $\Psi(h_1)$ abändern.) Wir prüfen die Assoziativität:

$$\begin{aligned}
\Big((n_1, h_1) \cdot (n_2, h_2)\Big) \cdot (n_3, h_3) &= \Big(n_1\Psi(h_1)(n_2), h_1h_2\Big) \cdot (n_3, h_3) \\
&= \Big(n_1\Psi(h_1)(n_2)\Psi(h_1h_2)(n_3), h_1h_2h_3\Big) \\
(n_1, h_1) \cdot \Big((n_2, h_2) \cdot (n_3, h_3)\Big) &= (n_1, h_1) \cdot \Big(n_2\Psi(h_2)(n_3), h_2h_3\Big) \\
&= \Big(n_1\Psi(h_1)\big(n_2\Psi(h_2)(n_3)\big), h_1h_2h_3\Big) \\
&= \Big(n_1\Psi(h_1)(n_2)\Psi(h_1h_2)(n_3), h_1h_2h_3\Big).
\end{aligned}$$

Neutrales Element ist offenbar $(1,1)$ und das Inverse zu (n,h) ist $\Big(\big(\Psi(h^{-1})(n)\big)^{-1}, h^{-1}\Big)$. Die Gruppe bezeichnet man als *semidirektes Produkt* von N und H in Zeichen $N \rtimes H = G$. Via der Abbildungen $n \longmapsto (n,1)$ und $h \longmapsto (1,h)$ kann man N und H als Untergruppen von G auffassen. Offenbar ist $N \cap H = \{(1,1)\}$ nur das neutrale Element in G. Außerdem ist N sogar ein Normalteiler, denn

$$\begin{aligned}(n_2,h_2)\cdot(n_1,1)\cdot(n_2,h_2)^{-1} &= \Big(n_2\Psi(h_2)(n_1),h_2\Big)\Big(\Psi(h_2^{-1})(n_2)^{-1},h_2^{-1}\Big)\\ &= \Big(n_2\Psi(h_2)(n_1)n_2^{-1},1\Big) \in N.\end{aligned}$$

Ist umgekehrt G eine Gruppe, die einen Normalteiler N und eine weitere Untergruppe H mit $N \cap H = \{1\}$ und $G = N \cdot H$ enthält, so ist für jedes h die Abbildung $n \longmapsto hnh^{-1} \in N$ ein Automorphismus von N und die damit erhaltene Abbildung $\Psi\colon H \longrightarrow \mathrm{Aut}(N)$ ist wegen

$$\Psi(gh)(n) = ghnh^{-1}g^{-1} = \Psi(g)\Big(\Psi(h)(n)\Big)$$

ein Homomorphismus. Wir betrachten die Abbildung

$$\varphi\colon N \times H \longrightarrow G, \quad (n,h) \longmapsto n\cdot h$$

und behaupten, dass die Abbildung φ ein Homomorphismus ist, falls $N \times H$ mit der Verknüpfung eines semidirekten Produkts bezüglich obigem Ψ versehen wird. Wegen $N \cap H = \{1\}$ und $G = N \cdot H$ ist φ dann sogar ein Isomorphismus. Wir müssen also noch nachrechnen:

$$\varphi(n_1,h_1)\cdot\varphi(n_2,h_2) = n_1h_1n_2h_2$$

und

$$\begin{aligned}\varphi\Big((n_1,h_1)\cdot(n_2,h_2)\Big) &= \varphi\Big(n_1\Psi(h_1)(n_2),h_1h_2\Big)\\ &= \varphi(n_1h_1n_2h_1^{-1},h_1h_2) = n_1h_1n_2h_2.\end{aligned}$$

Insgesamt haben wir gezeigt:

Satz 4.17 *Ist G eine Gruppe, die einen Normalteiler N und eine weitere Untergruppe H mit $N \cap H = \{1\}$ und $G = N \cdot H$ enthält, so ist G zu einem semidirekten Produkt $N \rtimes H$ isomorph.*

Ein Beispiel für ein semidirektes Produkt ist die Abbildung Ψ, die alles auf die Identität in $\mathrm{Aut}(N)$ schickt. Damit erhalten wir gerade das bekannte direkte Produkt. Ein interessanteres Beispiel ist $N = \mathbb{Z}/p\mathbb{Z}$ und $H = \mathrm{Aut}(N)$. Dann ist N und $G/N = H$ abelsch und $\mathrm{ord}(G) = p\cdot(p-1)$ und wir haben ein Beispiel für eine auflösbare, nichtabelsche Gruppe.

5 Zurück zur Körpertheorie

5.1 Auflösbarkeit II

Im ersten Abschnitt über Auflösbarkeit haben wir den Begriff von Auflösbarkeit beschrieben, der uns eigentlich interessiert, die Auflösbarkeit durch Radikale. Wir definieren hier einen zweiten Auflösbarkeitsbegriff, den wir praktisch aufgrund der Methoden des vorigen Abschnitts testen können. Auch in diesem Abschnitt ist zur Vereinfachung die Charakteristik aller Körper gleich Null.

Definition 5.1 *Eine endliche Körpererweiterung L/K heißt* auflösbar*, falls es einen Oberkörper $E \supseteq L$ gibt, sodass E/K galoissch ist und* $\mathrm{Gal}(E/K)$ *auflösbar ist.*

Ist L/K bereits galoissch, so ist L/K auflösbar genau dann, wenn $\mathrm{Gal}(L/K)$ auflösbar ist. Ist nämlich $E \supseteq L$ der Oberkörper aus der Definition von auflösbar, so ist die Einschränkung $\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(L/K)$ nach Proposition 3.2 wohldefiniert und surjektiv. Als Quotient einer auflösbaren Gruppe ist $\mathrm{Gal}(L/K)$ auch wieder auflösbar.

Dieser Auflösbarkeitsbegriff hat dieselben formalen Eigenschaften wie Auflösbarkeit durch Radikale.

Lemma 5.2 *Sei F eine algebraische Körpererweiterung von K und seien F und L in einen algebraischen Abschluss $\overline{K}$ von K eingebettet. Ist L/K auflösbar, so ist auch FL/F auflösbar.*

Beweis : Mit E/K ist auch FE/F wieder galoissch. Ist $\tau \in \mathrm{Gal}(FE/F)$, so fixiert τ erst recht den Körper K. Die Einschränkung auf E definiert also einen Homomorphismus

$$\mathrm{Gal}(FE/F) \longrightarrow \mathrm{Gal}(E/K).$$

Dieser ist injektiv, denn ist $\tau \in \mathrm{Aut}(FE)$ eingeschränkt auf E und F die Identität, so ist $\tau = \mathrm{id}$. Wir verwenden nun, dass eine Untergruppe einer auflösbaren Gruppe wieder auflösbar ist. □

Lemma 5.3 *Ist $K \subseteq L \subseteq M$ eine Kette von Körpererweiterungen, so ist M/K genau dann auflösbar, wenn L/K und M/L auflösbar sind.*

Beweis : Ist M/K auflösbar, also E/K eine zugehörige galoissche Erweiterung mit $\mathrm{Gal}(E/K)$ auflösbar, so ist $E \supseteq L$ und daher L/K auflösbar. Weiter ist $\mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/K)$ als Untergruppe einer auflösbaren Gruppe wieder auflösbar. Dies zeigt eine Implikation.

Für die Umkehrung zeigen wir zunächst, dass wir L zu L' und M zu M' vergrößern können, sodass L'/K und M'/L' galoissch mit auflösbarer Galoisgruppe sind. Die Existenz von L' folgt aus der Definition der Auflösbarkeit und für M' nehmen wir das Kompositum $E \cdot L'$, wobei E der Oberkörper aus der Definition der Auflösbarkeit von M/L ist. Wir lassen ab sofort die Striche weg und nehmen an, dass die Kette $K \subseteq L \subseteq M$ selbst die gewünschten Eigenschaften besitzt.
M/K ist separabel, da beide Teilschritte dies sind, aber M/K ist nicht notwendigerweise galoissch. Sei also $\widetilde{M}/K$ die normale Hülle von M/K. Diese konstruiert man, indem man einen algebraischen Abschluss $\overline{K}$ von K fixiert und dann $\widetilde{M}$ als das Kompositum aller $\tau(M)$ für $\tau \in \mathrm{Hom}_K\big(M, \overline{K}\big)$ definiert. Es genügt nun zu zeigen, dass $\mathrm{Gal}(\widetilde{M}/K)$ auflösbar ist. Da L/K galoissch ist, kann man $\tau \in \mathrm{Gal}(\widetilde{M}/K)$ auf L einschränken und erhält somit eine Surjektion

$$\mathrm{Gal}(\widetilde{M}/K) \longrightarrow \mathrm{Gal}(L/K).$$

Da nach Voraussetzung $\mathrm{Gal}(L/K)$ auflösbar ist, genügt es die Auflösbarkeit des Kerns $\mathrm{Gal}(\widetilde{M}/L)$ nachzuweisen. Da M/L galoissch ist, gilt dies auch für $\tau(M)/L$ für jedes $\tau \in \mathrm{Hom}_K\big(M, \overline{K}\big)$. Das Produkt der Restriktionsabbildungen definiert einen Homomorphismus

$$\mathrm{Gal}(\widetilde{M}/L) \longrightarrow \prod_{\tau \in \mathrm{Hom}_K\left(M, \overline{K}\right)} \mathrm{Gal}\Big(\tau(M)/L\Big), \sigma \longmapsto (\sigma_{|\tau(M)})_\tau$$

der nach Definition des Kompositums injektiv ist. Jeder Faktor auf der rechten Seite ist zu $\mathrm{Gal}(M/L)$ isomorph. Also steht auf der rechten Seite ein Produkt auflösbarer Gruppen und $\mathrm{Gal}(\widetilde{M}/L)$ ist als Untergruppe hiervon auflösbar. □

Satz 5.4 *Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.*

Beweis : Sei L/K auflösbar. Wir können annehmen, dass L/K galoissch mit auflösbarer Galoisgruppe ist, denn wenn wir Radikalauflösbarkeit für eine Körpererweiterung gezeigt haben, folgt dies per Definition auch für den ursprünglichen Körper. Wir vergrößern den Körperturm noch weiter. Sei m das Produkt aller Primzahlen,

welche $[L : K]$ teilen und F/K der Zerfällungskörper von $X^m - 1$. Per Definition ist F/K durch Radikale auflösbar und es genügt zu zeigen, dass das Kompositum FL in einem algebraischen Abschluss $\widetilde{K}$ durch Radikale auflösbar ist. Dazu genügt es nach Lemma 3.29 die Auflösbarkeit von FL/F durch Radikale zu zeigen. Die Auflösbarkeit dieser Galois-Erweiterung folgt direkt aus der von L/K. Sei also

$$\mathrm{Gal}(FL/F) = G_0 \supset G_1 \supset \ldots \supset G_{n-1} \supset G_n = \{1\}$$

die nach Lemma 4.13 existierende Normalreihe mit Faktoren, die zyklisch von Primzahlordnung sind. Nach dem Hauptsatz der Galoistheorie gehört dazu eine Kette von Körpererweiterungen

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_{n-1} \subset F_n = FL,$$

wobei $\mathrm{Gal}(F_{i+1}/F_i)$ zyklisch von Primzahlordnung p_i ist. Da $\mathrm{Gal}(FL/F)$ isomorph zu einer Untergruppe von $\mathrm{Gal}(L/K)$ ist, muss p_i den Grad $[L : K]$ teilen. Also enthält F_i eine primitive p_i-te Einheitswurzel. Nach Satz 3.24 ist also $F_{i+1} = F_i[\sqrt[p_i]{a_i}]$ für ein Element $a_i \in F_i$. Dies zeigt die Auflösbarkeit von FL/F durch Radikale.

Umgekehrt sei nun L/K durch Radikale auflösbar und

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_{n-1} \subseteq K_n$$

mit $K_n \supset L$ der zugehörige Körperturm. Wieder genügt es die Auflösbarkeit von K_n/K zu zeigen, d.h. wir können $L = K_n$ ohne Einschränkung annehmen. Nach Lemma 5.3, verallgemeinert induktiv auf n Schritte, genügt es zu zeigen, dass K_{i+1}/K_i auflösbar ist. Entsteht K_{i+1} aus K_i durch Adjunktion einer Einheitswurzel, so folgt dies aus Satz 3.17. Enthält K_i bereits eine n-te Einheitswurzel und ist $K_{i+1} = K_i[\sqrt[n]{a_i}]$, so folgt dies aus Satz 3.24. Sind die n-ten Einheitswurzeln nicht bereits in K_i enthalten, so sei F/K_i der Zerfällungskörper von $X^n - 1$. Mit den eben genannten Argumenten sind F/K_i und FK_{i+1}/F auflösbar, also nach Lemma 5.3 auch FK_{i+1}/K_i und damit K_{i+1}/K_i auflösbar. □

Korollar 5.5 *Sei L/K vom Grad ≤ 4. Dann ist L/K auflösbar und somit durch Radikale auflösbar.*

Beweis : Nach dem Satz vom primitiven Element können wir $L = K(\alpha)$ mit $\alpha \in L$ schreiben. Sei F/K der Zerfällungskörper des Minimalpolynoms f_α. Dann läßt sich $\mathrm{Gal}(F/K)$ in die Permutationsgruppe der Nullstellen von f_α injektiv abbilden, also $\mathrm{Gal}(F/K) \leqslant S_4$. Da S_4 auflösbar ist, folgt die Behauptung. □

Korollar 5.6 *Die allgemeine Gleichung n-ten Grades für $n \geqslant 5$ ist nicht auflösbar.*

Beweis : Folgt direkt aus Satz 3.12 und Proposition 4.16. □

Das letzte Korollar ist noch etwas unbefriedigend. Wir wollen noch konkret Gleichungen hinschreiben, die nicht auflösbar sind.

Lemma 5.7 *Sei p prim und $G \leqslant S_p$ eine transitive Untergruppe, d.h. die Operation von G auf $\{1, \dots p\}$ hat nur eine Bahn. Dann enthält G eine Untergruppe H der Ordnung p. Ist G auflösbar, so gibt es genau ein solches H, insbesondere $H \lhd G$.*

Beweis : Da G/G_1 bijektiv zur G-Bahn von 1, also zu $\{1, \dots p\}$ ist, muss p die Ordnung von G teilen. Da $p^2 \nmid p!$ folgt $p^2 \nmid \text{ord}(G)$. Also hat jede p-Sylowgruppe in G die Ordnung p. Daraus folgt auch die Existenz von H. Sei nun G auflösbar, $G = G_0 \supset G_1 \supset \dots \supset G_n = \{1\}$ die zugehörige Normalreihe mit zyklischen Quotienten von Primzahlordnung. Wir zeigen zuerst induktiv, dass für alle $i < n$ die Gruppe G_i immer noch transitiv auf $\{1, \dots, p\}$ operiert. Der Fall $i = 0$ ist der Induktionsanfang nach Voraussetzung. Für beliebiges i ist G_i in G_{i-1} ein Normalteiler. Für $g \in G_{i-1}$ und $x \in \{1, \dots, p\}$ ist $g(G_i x) = G_i(gx)$. Also haben wir eine wohldefinierte Operation von G_{i-1} auf den G_i-Bahnen, welche nach Induktionsvoraussetzung transitiv ist. Also haben alle G_i-Bahnen gleiche Ordnung. Da $i < n$, also $G_i \supsetneq \{1\}$ ist die Ordnung sicher nicht 1. Da nach Bahnbilanz $p = (\#\text{ Bahnen}) \cdot (\#\text{ Bahn von } 1)$ gilt und p prim ist, muss die Anzahl der Bahnen gleich 1 sein, wie behauptet.

Da $\text{ord}(G) = \prod_{i=0}^{n-1} \text{ord}(G_i/G_{i+1})$ und $(G_{n-1}/G_n) = p$ folgt wegen $p^2 \nmid \text{ord}(G)$, dass $p \neq \text{ord}(G_i/G_{i+1})$ für $i = 0, \dots, n-2$. Daraus folgt $H \subseteq G_i$ für alle $i = 0, \dots, n-1$, denn H liegt im Kern der Verkettung $H \longrightarrow G_i \longrightarrow G_i/G_{i+1}$. Daraus folgt $H = G_{n-1}$ und hiermit die Eindeutigkeit und die Eigenschaft Normalteiler. □

Lemma 5.8 *Sei wieder p prim, $G \leq S_p$ transitiv und auflösbar. Hat $\sigma \in G$ zwei Fixpunkte, so ist $\sigma = id \in S_p$.*

Beweis : Sei $H \lhd G$ der Normalteiler der Ordnung p aus dem vorigen Lemma. Dann ist H von einem p-Zykel erzeugt, denn nur diese Permutationen in S_p haben die Ordnung p. Sei also (nach Umnummerieren der Elemente) $H = \langle \pi \rangle$ und $\pi = (1\ 2 \dots p)$. Durch Umnummerieren können wir zudem annehmen, dass einer der

Fixpunkte von σ gleich 1 ist. Sei $1 < i \leq p$ ein weiterer Fixpunkt von σ. Da H Normalteiler ist, muss

$$\sigma \circ \pi \circ \sigma^{-1} = \big(\sigma(1)\, \sigma(2) \ldots \sigma(p)\big) = \pi^r \in H$$

für ein $r \in \mathbb{N}$ sein. Es ist $\pi^r = (\overline{1}\ \overline{1+r}\ \overline{1+2r} \ldots \overline{1+pr})$, wobei der Querstrich den Vertreter in $\{1, \ldots, p\}$ der Restklasse modulo p bezeichnet. Wegen $\sigma(1) = 1$ ist also $\sigma(k) = \overline{1 + (k-1) \cdot r}$. Aus $\sigma(i) = i$ folgt $\overline{(i-1)} = \overline{(i-1) \cdot r}$ und damit $r = 1$. Dies bedeutet $\sigma = \mathrm{id}$, wie behauptet. □

Proposition 5.9 *Sei $f \in K(x)$ irreduzibel, separabel und vom Grad p. Sei L/K der Zerfällungskörper von f und* Gal(L/K) *auflösbar. Sind α und β zwei verschiedene Nullstellen von f, so ist $L = K(\alpha, \beta)$.*

Beweis : Wir können Gal(L/K) als Untergruppe von S_p, der Permutationsgruppe der Nullstellen von f auffassen. Da f irreduzibel ist, gibt es zu je zwei Nullstellen α_i und α_j ein $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(\alpha_i) = \alpha_j$. Nach vorigem Lemma ist $\mathrm{Gal}(L/K(\alpha, \beta)) = \{\mathrm{id}\}$ und nach dem Hauptsatz der Galois-Theorie also $L = K(\alpha, \beta)$. □

Korollar 5.10 *Sei $f = X^p - 4x + 2 \in \mathbb{Q}[X]$ für $p \geqslant 5$ prim und $L/\mathbb{Q}$ der Zerfällungskörper von f. Dann ist $L/\mathbb{Q}$ nicht auflösbar.*

Beweis : Nach dem Eisenstein-Kriterium ist f irreduzibel. Es gilt $f(x) \longrightarrow \pm\infty$ für $x \longrightarrow \pm\infty$. Da $f'' = 0$ genau dann, wenn $x = 0$, hat der Graph von $\mathbb{R} \ni x \longmapsto f(x)$ höchstens einen Wendepunkt, wegen $f(1) < 0$ und $f(-1) > 0$ sogar genau einen. Also hat f genau drei reelle Nullstellen. Wäre $L/\mathbb{Q}$ auflösbar, so könnte man den Zerfällungskörper nach der vorigen Proposition durch Adjunktion von zwei dieser Nullstellen erhalten, im Widerspruch zu Tatsache, dass f auch $p-3$ komplexe Nullstellen hat. □

5.2 Nochmal Zirkel und Lineal

Wir betrachten nochmal den Körper $F_{\sqrt{\ }}$ aus Satz 1.1, der Körper aller Punkte, die man durch Konstruktionen mit Zirkel und Lineal erhält. Die Struktur dieses Körpers wird durch folgende Charakterisierung besser handhabbar.

Proposition 5.11 *Für $z \in \mathbb{C}$ sind äquivalent*

1) $z \in F_{\sqrt{\ }}$

2) Es gibt eine Kette von Körpererweiterungen

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subseteq \ldots L_n \subseteq \mathbb{C}$$

mit $z \in L_n$ und $[L_{i+1} : L_i] = 2$ für $i = 0, \ldots, n-1$.

In 2) können wir zudem annehmen, dass $L_n/\mathbb{Q}$ galoissch ist.

Beweis : Für die Implikation $1) \Rightarrow 2)$ betrachten wir nochmals den Beweis von Satz 1.1. In jedem Konstruktionsschritt entsteht der neue Punkt aus einem Schnitt zweier Geraden- und/oder Kreisgleichung. Der Lösungspunkt liegt also in einer quadratischen Erweiterung des Körpers, erzeugt von den bisher konstruierten Punkten. Da jede Konstruktion endlich viele Schritte hat, folgt die Aussage 2). Umgekehrt entsteht jede quadratische Erweiterung durch Adjunktion einer Quadratwurzel nach Satz 3.24. Im einleitenden Abschnitt haben wir gezeigt, dass sich jede Quadratwurzel von konstruierten Punkten wieder mit Zirkel und Lineal konstruieren lässt. Damit folgt 1).

Für den Zusatz betrachten wir die Homomorphismen $\sigma_j : L_n \longrightarrow \overline{\mathbb{Q}}, j \in J$ in einen fixierten algebraischen Abschluss. Das Kompositum der $\sigma_j(L_n), j \in J$ ist die normale Hülle von $L_n/\mathbb{Q}$. Da

$$\mathbb{Q} \subseteq \sigma_j(L_1) \subseteq \sigma_j(L_2) \subseteq \ldots \subseteq \sigma_j(L_n)$$

ebenfalls eine Kette mit $[\sigma_j(L_{i+1}) : \sigma_j(L_i)] = 2$ ist, erhält man auch das Kompositum durch eine Kette von Körpererweiterungen vom Grad zwei. □

Korollar 5.12 *Ist $z \in F_{\sqrt{\ }}$, so ist z algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(z) : \mathbb{Q}]$ ist eine Zweierpotenz. Insbesondere ist z.B. $\sqrt[3]{2} \notin F_{\sqrt{\ }}$.*

Korollar 5.13 *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, falls $\varphi(n)$ eine Zweierpotenz ist.*

Also ist z.B. das regelmäßige 7-Eck nicht konstruierbar, das regelmäßige 17-Eck hingegen schon. Die erste Konstruktion davon (siehe das Deckblatt) geht auf Gauß zurück.

Beweis : Ist das regelmäßige n-Eck konstruierbar, so ist $\zeta_n \in F_{\sqrt{}}$, also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ eine Zweierpotenz. Ist umgekehrt $\varphi(n)$ eine Zweierpotenz, so gibt es nach Korollar 4.3 und dem Hauptsatz der Galois-Theorie eine Kette von Zwischenkörpern mit Erweiterungsgrad 2 und damit ist $\zeta_n \in F_{\sqrt{}}$ nach Proposition 5.11. □

Man kann die Werte n mit $\varphi(n)$ Zweierpotenz noch genauer beschreiben. Für $\ell \in \mathbb{N}$ wird $F_\ell = 2^{2^\ell} + 1$ die ℓ-te Fermatsche Zahl genannt. Unter den Fermatschen Zahlen sind $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ und $F_4 = 65537$ die einzigen {bekannten} Primzahlen. Die Existenz weiterer Fermatscher Primzahlen ist eine offene Frage. Wir überlassen folgenden Satz als Übungsaufgabe.

Proposition 5.14 *Für $n \geq 2$ ist $\varphi(n)$ genau dann eine Zweierpotenz, falls es Fermatsche Primzahlen $p_1, \ldots, p_r$ und $m \in \mathbb{N}$ gibt mit $n = 2^m p_1 \cdot \ldots \cdot p_r$.*

6 Moduln

Als Motivation für Algebra wurde eingangs das Lösen diophantischer Gleichungen angegeben. Bereits das Lösen linearer diophantischer Gleichungssysteme geht über den Rahmen der linearen Algebra hinaus. Dort wird, z.B. beim Gauß-Algorithmus an geeigneter Stelle dividiert, was nicht gestattet ist, wenn wir bei ganzzahligen Koeffizienten verbleiben wollen.
Wir müssen also Strukturen untersuchen, bei denen der Skalar-Körper nur noch ein Ring ist. Diese werden Moduln genannt. Man beachte, dass ein $\mathbb{Z}$-Modul nach untenstehender Definition nichts anderes ist als eine abelsche Gruppe. Struktursätze für (endliche) $\mathbb{Z}$-Moduln sind also Aussagen über (endliche) abelsche Gruppen. Wir werden viel präzisere Aussagen machen können als die Sylowsätze für (allgemeine, nicht notwendig abelsche) Gruppen.

Sei R ein Ring, wie immer kommutativ und mit Einselement. Ein *R-Modul* M ist eine abelsche Gruppe $(M, +)$ und eine Skalarmultiplikation

$$\cdot : R \times M \longrightarrow M,$$

die den (vom Vektorraum-Fall bekannten) Axiomen

$$\begin{aligned} a \cdot (x + y) &= a \cdot x + a \cdot y \\ (a + b) \cdot x &= a \cdot x + b \cdot x \\ a \cdot (bx) &= (a \cdot b)x; \qquad 1 \cdot x = x \end{aligned}$$

für alle $a, b \in R$ und $x, y \in M$ genügt. Wörtlich wie lineare Abbildungen definiert man *R-Modulhomomorphismen*, wie Untervektorräume definiert man *Untermoduln*, wie Faktorräume definiert man Quotientenmoduln.

Beispiel 6.1 i) Für jeden Ring R ist R ein freier (Definition siehe unten) R-Modul. Untermoduln hiervon sind gerade die Ideale von R.

ii) Sei V ein K-Vektorraum und $\varphi \in \mathrm{End_K(V)}$ ein Endomorphismus. Vermöge der Skalarmultiplikation

$$K[X] \times V \longrightarrow V, \left(\sum a_i X^i, v\right) \longmapsto \sum a_i \varphi^i(v)$$

wird V zu einem $K[X]$-Modul. Umgekehrt, falls V ein $K[X]$-Modul ist, so definiert

$$\varphi(v) = X \cdot v$$

einen Endomorphismus. Damit erhält man eine Bijektion zwischen $K[X]$-Moduln und Paaren $\big(V, \varphi \in \mathrm{End_K(V)}\big)$.

Wie im Vektorraumfall definiert man den *Schnitt* und die *Summe* (sowie eine *direkte Summe*) von R-Moduln und diese sind wiederum R-Moduln. Ebenso wie im Vektorraumfall definiert man *Erzeugendensystem* sowie *linear unabhängig*.

Ein linear unabhängiges Erzeugendensystem wird auch hier *Basis* genannt. Wenn es eine solche gibt, so heißt der Modul *frei* und es gilt wie im Vektorraumfall der Satz von der eindeutigen Darstellung als Linearkombination von Basisvektoren.

Der erste wesentliche Unterschied zum Vektorraumfall ist, dass nicht jeder R-Modul eine Basis besitzt: Für jedes Element x in dem $\mathbb{Z}$-Modul (d.h. der abelschen Gruppe) $\mathbb{Z}/p\mathbb{Z}$ gilt $p \cdot x = 0$,womit wir eine nichttriviale Linearkombination gefunden haben.

Ist R allgemeiner ein nullteilerfreier Ring und M ein R-Modul, so formulieren wir das eben gesehene Phänomen, indem wir alle Elemente $x \in M$, sodass es ein $a \in R \setminus \{0\}$ gibt mit $ax = 0$, *Torsionselemente* nennen. Die Menge aller Torsionselemente bilden einen Untermodul $M_{\text{tor}} \subseteq M$, genannt *Torsionsuntermodul*. Ist $M = M_{\text{tor}}$, so nennt man M einen *Torsionsmodul*. Beispielsweise ist im $\mathbb{Z}$-Modul $M = \mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z}$ der Torsionsuntermodul $M_{\text{tor}} = \mathbb{Z}/s\mathbb{Z}$. Das nächste Ziel ist zu zeigen, dass jeder $\mathbb{Z}$-Modul solch eine direkte Summenzerlegung besitzt.

6.1 Elementarteiler

Wir schränken uns in diesem Abschnitt auf den Fall, dass R ein Hauptidealring ist, ein. Dies beinhaltet die wichtigen Fälle $R = \mathbb{Z}$ und $R = K[X]$ und die Hauptaussagen dieses Abschnitts sind ohne diese Voraussetzung nicht richtig.

Wir benötigen den Begriff der Länge eines R-Moduls M. Eine *Kette* der Länge ℓ in M besteht aus R-Untermoduln

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M.$$

Das Supremum über die Längen aller Ketten von M wird die *Länge von* M genannt und mit $\ell_R(M)$ bezeichnet. Der Nullmodul hat die Länge Null und der $\mathbb{Z}$-Modul $\mathbb{Z}$ hat die Länge ∞, wie man an der Kette $\ldots p^{k+1} \cdot \mathbb{Z} \subsetneq p^k\mathbb{Z} \subsetneq \ldots$ leicht sieht. Dies ist insbesondere eine Kette von Idealen in $\mathbb{Z}$, die wir beginnend von einem gegebenen Ideal beliebig lang machen können.

Umgekehrt bricht eine aufsteigende Kette von Idealen in R beginnend bei $0 \subsetneq a_1 \subsetneq a_2 \subsetneq \ldots$ nach endlich vielen Schritten ab, denn $\bigcup\limits_{i \geqslant 0} a_i \subset R$ ist wieder ein Ideal erzeugt von einem Element x, da R Hauptidealring ist. Nun ist $x \in a_n$ für ein n und somit $a_{n+k} = a_n$ für alle $k \geqslant 0$. Aufgrund dieser Eigenschaft sagt man, dass Hauptidealringe *noethersch* sind. Der Längenbegriff hat folgende Eigenschaften.

Lemma 6.2 *a) Ist $M = M' \oplus M''$ eine direkte Summe von R-Moduln, so ist $\ell_R(M) = \ell_R(M') + \ell_R(M'')$.*

b) Ist $a = \varepsilon \cdot p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ die Primfaktorzerlegung von $a \in R$ mit $\varepsilon \in R^*$ und $\nu_i \in \mathbb{N}$, so ist $\ell_R(R/aR) = \sum_{i=1}^r \nu_i$.

Beweis : Zu Teil a): Sind $0 \subsetneq M_1' \subsetneq M_2' \subsetneq \ldots \subsetneq M_r' = M'$ und $0 \subsetneq M_1'' \subsetneq M_2'' \subsetneq \ldots \subsetneq M_s'' = M$ Ketten, so ist

$$0 \subsetneq M_1' \oplus 0 \subsetneq M_2' \oplus\ 0 \subsetneq \ldots \subsetneq M_r' \oplus 0 \subsetneq M_r' \oplus M_1'' \subsetneq \ldots \subsetneq M_r'' \oplus M_s'' = M$$

eine Kette der Länge $r + s$, also $\ell_R(M) \geqslant \ell_R(M') + \ell_R(M'')$. Für die umgekehrte Ungleichung betrachten wir die Projektion $\pi'' \colon M \longrightarrow M''$ mit dem Kern M'. Ist

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M$$

eine Kette von M, so bilden die $\pi''(M_i)$ eine (nicht unbedingt echt aufsteigende) Kette von M'' und die $M_i \cap (M' \oplus 0)$ eine (nicht unbedingt echt aufsteigende) Kette

von M'. Da $M_i \subsetneq M_{i+1}$ gilt $\pi''(M_i) \subsetneq \pi''(M_{i+1})$ oder $M_i \cap (M' \oplus 0) \subsetneq M_{i+1} \cap (M' \oplus 0)$. Daraus folgt die umgekehrte Ungleichung. Zur Aussage b): Nach dem chinesischen Restesatz ist

$$R/aR \cong \oplus_{i=1}^{r} R/p_i^{\nu_i} R,$$

welches ein Isomorphismus von Ringen und damit auch von $\mathbb{Z}$-Moduln ist. Nach Teil a) müssen wir also nur noch den Fall $a = p^\nu$ betrachten. In diesem Fall konstruiert man eine Kette der geforderten Länge ν wie in Korollar 4.3 und eine solche Kette kann man nicht weiter verfeinern, da die Quotienten R/pR, also Körper sind. □

Ist $x_1, \ldots, x_n$ eine Basis von M (d.h. gibt es eine solche), so ist

$$M \cong Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_n.$$

In diesem Fall wird $n = \text{Rang}(M)$ der *Rang* von M genannt. Im allgemeinen definieren wir den *Rang* von M als das Supremum über die Anzahl linear unabhängiger Elemente in M.

Der folgende Satz wird Elementarteilersatz genannt. Aus ihm werden alle wichtigen Sätze über R-Moduln (für R Hauptidealring) folgen.

Satz 6.3 *Ist F ein freier R-Modul von endlichem Rang und M ein Untermodul von F vom Rang n. Dann existieren $x_1, \ldots x_n \in F$, die Teil einer Basis von F sind, sowie $\alpha_1, \ldots, \alpha_n \in R \setminus \{0\}$, sodass*

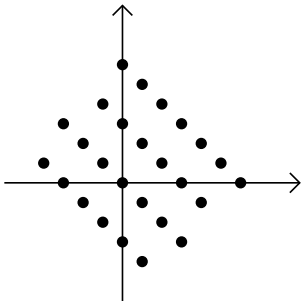
i) $\{\alpha_1 x_1, \ldots, \alpha_n x_n\}$ *eine Basis von M ist und*

ii) $\alpha_i \mid \alpha_{i+1}$ *für* $1 \leqslant i < n$.

Die Elemente $\alpha_1, \ldots, \alpha_n$ sind bis auf Einheiten in R eindeutig bestimmt und werden Elementarteiler *von M genannt.*

Die Situation des Satzes tritt in der Natur z.B. beim Studium von Gittern auf, d.h. von freien $\mathbb{Z}$-Moduln vom Rang n, die diskret in $\mathbb{R}^n$ eingebettet sind. Gesucht sind dann die Elementarteiler wie z.B. im folgenden Bild für ein Untergitter des Standardgitters $\mathbb{Z}^2 \subseteq \mathbb{R}^2$.

Zum Beweis des Satzes benötigen wir den Begriff des Inhalts $\text{cont}(x)$ für $x \in F$. Sei dazu $F^* = \text{Hom}_R(F, R)$ der Dualraum von F. Die Menge $\{\varphi(x), \varphi \in F^*\} \subseteq R$ ist ein Ideal von R, also erzeugt von einem Element $c \in R$, das bis auf Einheiten eindeutig bestimmt ist und mit $\text{cont}(x)$ bezeichnet wird.



Lemma 6.4 *Ist F frei von endlichem Rang, so gelten folgende Aussagen.*

i) Ist $\{y_1, \ldots, y_r\}$ eine Basis von F und $x = \sum_{i=1}^{r} c_i y_i$ die Basisdarstellung von $x \in F$, so ist $\mathrm{cont}(x) = \mathrm{ggT}(c_1, \ldots, c_r)$.

ii) Für alle $x \in F$ gibt es $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$.

iii) Für $x \in F$ und $\psi \in F^*$ gilt $\mathrm{cont}(x) \mid \psi(x)$.

iv) Ist $M \subseteq F$ ein Untermodul, so gibt es ein $x \in M$ mit $\mathrm{cont}(x) \mid \mathrm{cont}(y)$ *für alle $y \in M$.*

Beweis : ii) und iii) sind nach Definition klar. Zu i) sei $\varphi_1, \ldots, \varphi_r$ die zu $y_1, \ldots, y_r$ duale Basis und $\mathrm{ggT}(c_1, \ldots, c_r) = \sum_{i=1}^{r} a_i c_i$ mit $a_i \in R$. Wir setzen $\varphi = \sum a_i \varphi_i$. Dann ist $\varphi(x) = \mathrm{ggT}(c_1, \ldots, c_r)$, also $\mathrm{cont}(x) \mid \mathrm{ggT}(c_1, \ldots, c_r)$. Andererseits ist ein beliebiges $F^* \ni \psi = \sum b_i \varphi_i$ Linearkombination der φ_i. Dann wird $\psi(x) = \sum b_i c_i$ von $\mathrm{ggT}(c_1, \ldots, c_r)$ geteilt und folglich $\mathrm{ggT}(c_1, \ldots, c_r) \mid \mathrm{cont}(x)$.

Für iv) betrachten wir die Menge $\mathfrak{I}$ der Ideale der Form $\mathrm{cont}(y) \cdot R$ mit $y \in M$. Da R noethersch ist, hat jede Kette ein Supremum, also gibt es in $\mathfrak{I}$ ein maximales Element $\mathrm{cont}(x) \cdot R$.

Sei $\varphi \in F^*$ so, dass $\varphi(x) = \mathrm{cont}(x)$. Zunächst zeigen wir $\varphi(x) \mid \varphi(y)$ für alle $y \in M$. Wir schreiben

$$a\varphi(x) + b\varphi(y) = d =: \mathrm{ggT}\big(\varphi(x), \varphi(y)\big).$$

Wegen $\varphi(ax + by) = d$ und iii) folgt $\mathrm{cont}(ax + by) \mid d \mid \varphi(x) = \mathrm{cont}(x)$. Da $\mathrm{cont}(x) \cdot R$ maximal in $\mathfrak{I}$ gewählt war, folgt hieraus $\mathrm{cont}(ax + by) = \mathrm{cont}(x) = d = \varphi(x) \mid \varphi(y)$.

Wir sind fertig, sobald wir für jedes $\psi \in F^*$ und jedes $y \in M$ die Beziehung $\varphi(x) \mid \psi(y)$ gezeigt haben. Es gilt $\varphi(x) \mid \psi(x)$ und $\varphi(x) \mid \varphi(y)$. Daher gilt $\varphi(x) \mid \psi(y)$

genau dann, wenn $\varphi(x) \mid \Big(\psi(y) - \frac{\varphi(y)}{\varphi(x)}\psi(x)\Big) = \psi\left(y - \frac{\varphi(y)}{\varphi(x)} \cdot x\right)$. Wir können also ohne Einschränkung y durch $y - \frac{\varphi(y)}{\varphi(x)} \cdot x$ ersetzen, anders gesagt $\varphi(y) = 0$ annehmen. Mit dem gleichen Argument können wir ψ durch $\psi - \frac{\psi(x)}{\varphi(x)} \cdot \varphi$ ersetzen und damit $\psi(x) = 0$ annehmen. Sei nun

$$a\varphi(x) + b\psi(y) = d =: \mathrm{ggT}\big(\varphi(x), \psi(y)\big).$$

Dann ist

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y) = d,$$

also $\mathrm{cont}(ax + by) \mid d \mid \varphi(x) = \mathrm{cont}(x)$. Wieder besagt die Maximalität, dass diese Teilbarkeitsbeziehung alles Gleichheiten (bis auf Einheiten) sind und daher

$$\varphi(x) \mid d \mid \psi(y),$$

was zu zeigen war. □

Beweis von Satz 6.3 : Wir zeigen zunächst induktiv nach $n = \mathrm{Rang}(M)$ die im Satz implizit enthaltene Aussage, dass M frei ist. M ist sicher torsionsfrei, da F dies ist. Also ist für $n = 0$ nichts weiter zu zeigen. Wir wählen für den Induktionsschritt ein $x \in M$ wie in Lemma 6.4 iv) und $\varphi \in F^*$, sodass $\varphi(x) = \mathrm{cont}(x)$. Weiter gibt es ein $x_1 \in F$ mit $x = \varphi(x) \cdot x_1$, denn falls $x = \sum c_i y_i$ in einer Basis $y_1, \ldots, y_r$ von F, so leistet $\sum c_i/\varphi(x) \cdot y_i$ das Verlangte. Wir definieren $F' = \mathrm{Ker}(\varphi)$ und $M' = M \cap F'$. Wir behaupten, dass

$$F = Rx_1 \oplus F' \quad \text{und} \quad M = Rx \oplus M'$$

gilt. In der ersten Formel ist die Summe offenbar direkt und ist $y \in F$, so ist $y - \varphi(y) \cdot x_1 \in \mathrm{Ker}(\varphi)$. Die zweite Summe ist ebenso direkt, wir müssen zeigen, dass die beiden Summanden ganz M aufspannen. Unter Verwendung von Lemma 6.4 iv) ist

$$y = \frac{\varphi(y)}{\varphi(x)} \cdot x + \left(y - \frac{\varphi(y)}{\varphi(x)}x\right)$$

die gewünschte Darstellung für ein $y \in M$ beliebig. Wir können nun die Induktionsvoraussetzung auf M' anwenden und erhalten, dass M frei ist.

Wir können ebenso per Induktion nach $\mathrm{Rang}(M)$ annehmen, dass die Folgerungen des Satzes für M' bereits gelten, d.h. dass $x_2, \ldots, x_n$ Teil einer Basis von F' ist und es $\alpha_2, \ldots, \alpha_n$ gibt mit $\alpha_i \mid \alpha_{i+1}$ für $i \geqslant 2$, sodass $\alpha_2 x_2, \ldots, \alpha_n x_n$ eine Basis von M' ist. Mit x_1 wie oben und $\alpha_1 = \varphi(x)$ wir oben ist nur noch $\alpha_1 \mid \alpha_2$ zu zeigen. Sei dazu $\varphi_2 \in F^*$ mit $\varphi_2(x_2) = 1$. Dann gilt nach dem vorigen Lemma $\varphi(x) \mid \varphi_2(\alpha_2 x_2)$, also $\alpha_1 \mid \alpha_2$.

Die Eindeutigkeitsaussage folgt aus dem nächsten Lemma. □

Lemma 6.5 *Sei R ein Hauptidealring und $T \cong \bigoplus_{i=1}^{n} R_i/\alpha_i R_i$, wobei $\alpha_1, \ldots, \alpha_n \in R \setminus \{0\}$ Nichteinheiten mit $\alpha_i \mid \alpha_{i+1}$ sind. Dann sind $\alpha_1, \ldots, \alpha_n$ bis auf Einheiten in R eindeutig.*

Beweis : Der Beweis verwendet die Elemente größter Ordnung in T und daher ist es günstig, die Reihenfolge der Indizierung umzudrehen. Sei also $\widetilde{\alpha}_i = \alpha_{n-i+1}$ und folglich $\widetilde{\alpha}_{i+1} \mid \widetilde{\alpha}_i$. Wir nehmen an, dass es eine weitere Summenzerlegung

$$T \cong \bigoplus_{i=1}^{n} R/\widetilde{\alpha}_i R \cong \bigoplus_{j=1}^{m} R/\widetilde{\beta}_j R$$

ebenfalls mit $\beta_{j+1} \mid \beta_j$ gibt. Wir nehmen an, dass die Zerlegungen echt verschieden sind, sei k der kleinste Index mit $\widetilde{\alpha}_k R \neq \beta_k R$. Wir betrachten die Zerlegung des R-Moduls $\widetilde{\alpha}_k T$. Da für $\ell > k$ die $\widetilde{\alpha}_\ell$ alle Teiler von $\widetilde{\alpha}_k$ sind, erhalten wir

$$\widetilde{\alpha}_k T \cong \bigoplus_{i=1}^{k-1} \widetilde{\alpha}_k (R/\widetilde{\alpha}_i R) \cong \bigoplus_{i=1}^{k-1} \widetilde{\alpha}_k (R/\widetilde{\alpha}_i R) \oplus \widetilde{\alpha}_k \cdot (R/\widetilde{\beta}_k R) \oplus \ldots.$$

Da $\ell_R(\widetilde{\alpha}_k T) < \infty$ folgt aus dem Vergleich der Längen beider Seiten mit Hilfe von Lemma 6.2, dass $\widetilde{\alpha}_k \cdot (R/\widetilde{\beta}_k R) = 0$ ist, mit anderen Worten $\widetilde{\alpha}_k R \subset \widetilde{\beta}_k R$. Durch Vertauschen der Rollen von $\widetilde{\alpha}_k$ und $\widetilde{\beta}_k$ erhalten wir die umgekehrte Inklusion, insgesamt die Gleichheit im Widerspruch zur Wahl von k. Ist $\widetilde{\alpha}_j = \widetilde{\beta}_j$ für alle $j \leq \min\{m, n\}$, so folgt ebenfalls durch Berechnen von $\ell_R(T)$, dass $m = n$ ist. Insgesamt beweist dies das Lemma. □

Beweis von Satz 6.3, Eindeutigkeit : Nach dem bereits Bewiesenen gibt es Elementarteiler $\alpha_1 \mid \alpha_2 \mid \ldots \mid \alpha_n$ von M und wir nehmen an, dass $\beta_1 \mid \beta_2 \mid \ldots \mid \beta_m$ ebenfalls Elementarteiler (bzgl. einer anderen Basis von F) sind. Wir definieren zu M die Menge:

$$M_{\mathsf{Sat}} = \{y \in F : \exists 0 \neq a \in R : a \cdot y \in M\}.$$

Man prüft sofort, dass M_{Sat} ein Untermodul von F ist, genannt die *Saturierung* von M in F. Wir behaupten, dass

$$M_{\mathsf{Sat}}/M \cong \bigoplus_{i=1}^{n} R/\alpha_i R \cong \bigoplus_{j=1}^{m} R/\beta_j R$$

ist. Sobald wir dies gezeigt haben, folgt die Eindeutigkeitsaussage aus dem vorangegangenen Lemma.

Zum Beweis der Behauptung verwenden wir die Basis $x_1, \ldots, x_n$ aus dem bereits bewiesenen Teil des Satzes. Es ist $\bigoplus_{i=1}^{n} R \cdot x_i \subseteq M_{\mathsf{Sat}}$ denn $\alpha_i(r_i \cdot x_i) = r_i(\alpha_i \cdot x_i) \in M$

für beliebiges r_i. Um zu zeigen, dass die Inklusion eine Gleichheit ist, nehmen wir $y \in M_{\mathsf{Sat}}$ beliebig her. Wir ergänzen $x_1, \ldots, x_n$ zu einer Basis $x_1, \ldots, x_t$ von F und schreiben $y = \sum_{i=1}^{t} c_i x_i$. Es ist $a \cdot y \in M$ für ein $0 \neq a \in R$ nach Definition der Saturierung. Also ist $\sum_{i=1}^{t} a c_i x_i \in M$. Daraus folgt, dass $a \cdot c_i = 0$ für $i = n+1, \ldots, t$. Da R nullteilerfrei ist, folgt $c_i = 0$, was zu zeigen war.

Insgesamt ist also

$$M = \bigoplus_{i=1}^{n} R \cdot (\alpha_i x_i) \subseteq M_{\mathsf{Sat}} = \bigoplus_{i=1}^{n} R \cdot x_i$$

und daraus folgt die obige Behauptung über den Quotientenmodul. □

Der oben genannte Beweis ist allerdings nicht konstruktiv, d.h. nicht direkt in einen programmierbaren Algorithmus umzusetzen. Das Problem ist die Anwendung von Lemma 6.4 iv) zu Beginn des Beweises. Das gewünschte Element x dort wird als maximales Element einer Kette gewonnen und wir haben bisher uns keine Gedanken gemacht (wie wir größere Ideale in dieser Kette finden können und vor allem), wann diese Kette aufhört.

In der Praxis liegt die freie Modul F oft durch Angabe einer Basis $x_1, \ldots, x_r$ und M durch Erzeuger $z_1, \ldots, z_m$ vor, wobei $z_j = \sum_{i=1}^{r} a_{ij} x_i$. Wir fassen die Koeffizienten in einer Matrix $A = (a_{ij})$ zusammen. Ziel ist es, die Elementarteiler anhand von A auszurechnen.

Sind $I \subseteq \{1, 2, \ldots, r\}$ und $J \subseteq \{1, 2, \ldots, m\}$ zwei Teilmengen mit t Elementen, so bezeichnen wir mit A_{IJ} die $t \times t$-Matrix, deren Eintrag an der Stelle (u, v) gerade $a_{i_u j_v}$ ist, wobei die Indexmengen als $I = \{i_1, \ldots, i_t\}$ mit $i_\ell < i_{\ell+1}$ und $J = \{j_1, \ldots, j_t\}$ mit $j_\ell < j_{\ell+1}$ für alle ℓ aufgezählt sind. Als *t-Minore* von A bezeichnet man die Determinante einer Matrix A_{IJ} mit I und J wie oben. Zum Beweis des folgenden Satzes ist es günstig, den Begriff des t-fachen äußeren Produkts $\Lambda^t F$ eines Moduls F zu verwenden. Wir definieren diesen hier ad hoc und nur für freie R-Moduln. Sei also $x_1, \ldots, x_r$ eine Basis von F. Dann ist $\Lambda^t F$ der freie R-Modul erzeugt von Symbolen der Form $x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}$, wobei $1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant r$. Wir definieren für jede Indexmenge $j_1, j_2, \ldots, j_t$ ein Element $x_{j_1} \wedge x_{j_2} \wedge \ldots x_{j_t} \in \Lambda^t F$, indem wir dies als Null erklären, falls zwei Indizes gleich sind und andernfalls die Permutation $\pi \in S_t$ verwenden, sodass $j_\ell = i_\pi(\ell)$ mit $i_1 < i_2 < \ldots < i_t$. Dann definieren wir

$$x_{i_{\pi(1)}} \wedge x_{i_{\pi(2)}} \wedge \ldots \wedge x_{i_{\pi(t)}} = \operatorname{sgn}(\pi) x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}.$$

Schließlich definieren wir für ein beliebiges t-Tupel $z_1, \ldots, z_t$ von Elementen in F ein Element („t-faches äußeres Produkt“) $z_1 \wedge z_2 \wedge \ldots \wedge z_t \in \Lambda^t F$ durch sogenannte multilineare Fortsetzung. Damit ist gemeint, dass falls $z_i = \sum_{i=1}^{r} a_{ij} x_j$ die Basisdarstellung von z_i ist, wir das t-fache äußere Produkt der z_i definieren als

$$\begin{aligned} z_1 \wedge \ldots \wedge z_t &= \left(\sum_{j=1}^{r} a_{1j}x_j\right) \wedge \left(\sum_{j=1}^{r} a_{2j}x_j\right) \wedge \ldots \wedge \left(\sum_{j=1}^{r} a_{tj}x_j\right) \\ &= \sum_{j_1,\ldots,j_t=1}^{r} a_{1j_1} \cdot a_{2j_2} \cdot \ldots \cdot a_{tj_t} \cdot (x_{j_1} \wedge x_{j_2} \wedge \ldots \wedge x_{j_t}) \\ &= \sum_{\substack{j_1,\ldots,j_t=1 \\ \text{alle } j_k \text{ verschieden}}}^{r} a_{1j_1} \cdot a_{2j_2} \cdot \ldots \cdot a_{tj_t} \cdot (x_{j_i} \wedge x_{j_2} \wedge \ldots \wedge x_{j_t}) \\ &= \sum_{1 \le i_1 < i_2 < \ldots < i_t \le r} \left(\sum_{\pi \in S_t} \operatorname{sgn}(\pi) a_{1i_{\pi(1)}}, a_{2i_{\pi(2)}} \ldots a_{ti_{\pi(t)}}\right) (x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_t}) \end{aligned} \tag{3}$$

(Die Rechnung zeigt auch, dass die Definition von $\Lambda^t F$ nicht von der Wahl einer Basis abhängt, denn falls $z_1, \ldots, z_t$ eine andere Basis ist, so ist die Determinante der Basiswechselmatrix eine Einheit.)
Aus dieser Rechnung folgt auch, dass aus einer Inklusion $M \subseteq F$ von R-Moduln eine Inklusion $\Lambda^t M \subseteq \Lambda^t R$ der äußeren Produkte entsteht. Ist die Basis $x_1, \ldots, x_t$ durch Ergänzen einer Basis von $x_1, \ldots, x_n$ wie im Elementarteilersatz entstanden, so bilden die $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von M und somit die Elemente

$$\alpha_{i_1} x_{i_1} \wedge \alpha_{i_2} x_{i_2} \wedge \ldots \wedge \alpha_{i_t} x_{i_t} = (\alpha_{i_1} \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_t}) x_{i_1} \wedge x_{i_2} \ldots \wedge x_{i_t} \tag{4}$$

eine Basis von $\Lambda^t M$. Diese sind (von Null verschiedene) Vielfache von Basiselementen von $\Lambda^t F$.

Satz 6.6 *Sei F ein endlich erzeugter freier R-Modul mit Basis $x_1, \ldots, x_r$. Sei $M \subseteq F$ ein Untermodul mit Erzeugern $z_1, \ldots, z_m$, wobei $z_i = \sum_{j=1}^{r} a_{ij} x_j$ und seien $\alpha_1, \ldots, \alpha_n$ die Elementarteiler von M. Sei μ_t der* ggT *aller t-Minoren der Koeffizientenmatrix $A = (a_{ij})$. Dann gilt*

$$\mu_t = \prod_{i=1}^{t} \alpha_i.$$

Beweis : Wir beginnen mit dem Fall $t = 1$. Es ist $\alpha_1 R$ das Ideal, welches von allen $\varphi(y)$ mit $(\varphi \in F^*)$ und $y \in M$ erzeugt wird. Ist $\psi_1, \ldots, \psi_r$ die Dualbasis zu $x_1, \ldots, x_r$,

so lässt sich ein beliebiges φ als Linearkombination $\varphi = \sum_{\ell=1}^{r} b_\ell \psi_\ell$ schreiben. Weiter ist $y = \sum_{i=1}^{m} c_i z_i$ und insgesamt

$$\begin{aligned}\varphi(y) &= \sum_{\ell=1}^{r} b_\ell \psi_\ell \left(\sum_{i=1}^{m} c_i \cdot z_i \right) \\ &= \sum_{\ell=1}^{r} b_\ell \psi_\ell \left(\sum_{i=1}^{m} \sum_{j=1}^{r} c_i \cdot a_{ij} x_j \right) \\ &= \sum_{i=1}^{m} \sum_{j=1}^{r} c_i a_{ij} b_j\end{aligned}$$

Also ist das Ideal $\alpha_1 R$ gerade von den a_{ij} für $i = 1, \ldots, m$ und $j = 1, \ldots, r$ erzeugt, d.h. von den 1-Minoren von A. Wir wenden diese Aussage auf die Inklusion von freien R-Moduln $\Lambda^t M \subset \Lambda^t F$ für beliebiges t an. Unter Verwendung der Basis aus Gleichung (4) sieht man, dass der erste Elementarteiler für diese Inklusion gleich $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_t$ ist, da $\alpha_i \mid \alpha_{i+1}$ und somit der ggT über alle Indextupel $\{i_1, \ldots, i_t\}$ angenommen wird. Mit dem Erzeugendensystem $z_1, \ldots, z_m$ von M wird $\Lambda^t M$ von den $z_{j_1} \wedge \ldots \wedge z_{j_t}$ aufgespannt, deren Basisdarstellung in den $x_{i_1} \wedge \ldots \wedge x_{i_t}$ wir in Gleichung (3) ausgerechnet haben, dort im Spezialfall $j_1 = 1, \ldots, j_t = t$. Dort war der Koeffizient die t-Minore $A_{\{1,\ldots,t\},\{i_1,\ldots,i_t\}}$. Für beliebiges $j_1, \ldots, j_t$ erhalten wir analog als Koeffizient eine beliebige t-Minore von A. Insgesamt besagt das erste Argument, dass der ggT aller t-Minoren gleich $\alpha_1 \cdot \ldots \cdot \alpha_t$ ist, was zu zeigen war. □

Wir wollen noch aus diesem Satz eine Algorithmus zur Bestimmung der Elementarteiler eines Untermoduls ableiten. Äquivalenterweise suchen wir zu einer Matrix A (der Koeffizientenmatrix aus dem vorigen Satz) invertierbare Matrizen S und T (die zu einem Basiswechsel in M bzw. F gehören), sodass $D = TAS$ die Einträge $D_{ii} = \alpha_i$ mit $\alpha_i \mid \alpha_{i+1}$ für $i = 1, \ldots, n$ und sonst nur Nullen als Einträge hat.

Angenommen wir haben bereits erreicht, dass der linke obere Eintrag a_{11} alle Einträge von A teilt. Dann ist insbesondere a_{i1} und a_{1j} für alle i, j durch a_{11} teilbar. Also ist die Addition des $-\frac{a_{1j}}{a_{11}}$-fachen der ersten Spalte zur j-ten Spalte eine durch ein Element in $\mathrm{GL}_2(R)$, also ein Basiswechsel in F beschrieben. Ebenso ist die Addition des $\left(-\frac{a_{i1}}{a_{11}}\right)$-fachen der ersten Zeile zur i-ten Zeile Resultat eines Basiswechsels in M. Am Ende dieser Schritte hat die Matrix in der ersten Zeile und Spalte mit Ausnahme von a_{11} nur Nullen und wir können induktiv den Algorithmus auf die Untermatrix ohne die erste Zeile und Spalte anwenden. Um die erste Annahme zu erreichen nehmen wir vereinfachend an, dass der Ring R euklidisch bzgl. der Gradfunktion δ ist. (Dies beinhaltet $R = K[x]$ und $\delta = \deg$ sowie $R = \mathbb{Z}$ und $\delta = |\cdot|$).

Sei

$$d = \min_{i,j=1\ldots n} \big\{\delta(a_{ij})\big\}.$$

Einen der Matrixeinträge mit kleinstem Grad $\neq 0$ können wir durch Zeilen- und Spaltenvertauschungen in der linken oberen Ecke annehmen. Wir zeigen, dass entweder a_{11} alle Einträge von A teilt oder wir d durch elementare Zeilen- und Spaltenumformungen (d.h. Basiswechsel in M bzw. F) verringern können.

Falls ein Eintrag der ersten Zeile, etwa a_{1j} nicht durch a_{11} teilbar ist, so schreiben wir $a_{ij} = q \cdot a_{11} + b$ mit $\delta(b) < d$ und durch $(-q)$-fache Addition der ersten Spalte auf die j-te Spalte erreichen wir, dass in der neuen Matrix $\widetilde{A}$ der Eintrag $\widetilde{a}_{1j} = b$ ist und $\delta(b) < d$ gilt. Analog gehen wir vor, wenn ein Eintrag der ersten Spalte nicht durch a_{11} teilbar ist. Da $d \in \mathbb{N}$ müssen wir dies nur endlich oft durchführen. Wie in der Anfangsbemerkung können wir nun durch Zeilen- und Spaltenoperationen erreichen, dass $a_{i1} = 0$ und $a_{1j} = 0$ für $i \geqslant 2$ und $j \geqslant 2$.
Angenommen in der „Restmatrix“ gibt es noch einen Eintrag a_{ij} mit $i \geqslant 2$ und $j \geqslant 2$, der nicht durch a_{11} teilbar ist, also $a_{ij} = qa_{11} + b$ mit $0 < \delta(b) < d$. Dann addieren wir die erste Zeile zur i-ten, sodass nun $a_{i1} = a_{11}$, aber a_{ij} unverändert ist. Schließlich addieren wir $(-q)$ mal die erste Spalte auf die j-te Spalte, sodass nun $a_{ij} = b$ gilt. Auf diese Weise haben wir d verringert und beginnen mit dem Algorithmus von neuem. Da $d \in \mathbb{N}$ müssen wir dies nur endlich oft durchführen. Danach ist a_{11} in der Tat der erste Elementarteiler und wir können uns im gesamten Algorithmus auf die Restmatrix mit $i \geqslant 2$ und $j \geqslant 2$ beschränken.

6.2 Struktursätze für Moduln über Hauptidealringen

Wir halten einige wichtige Folgerungen aus dem Elementarteilersatz fest. In diesem Abschnitt ist immer noch R ein Hauptidealring.

Korollar 6.7 *Sei M ein endlich erzeugter R-Modul und $M_{tor} \subseteq M$ der Torsionsuntermodul. Dann ist M_{tor} endlich erzeugt und es gibt einen freien R-Modul M_F, sodass $M \cong M_{tor} \oplus M_F$. Insbesondere hat jeder endlich erzeugte torsionsfreie R-Modul eine Basis.*

Beweis : Seien $z_1, \ldots, z_r$ Erzeuger von M und $F \cong R^r$ ein freier R-Modul vom Rang r mit Basis $y_1, \ldots, y_r$. Sei $\varphi\colon F \longrightarrow M$ der Homomorphismus mit $\varphi(y_i) = z_i$. (Wie bei Vektorräumen ist auch bei freien Moduln ein Homomorphismus eindeutig durch die Bilder der Basis festgelegt und die Bilder der Basis können beliebig

gewählt werden.) Wir wenden den Elementarteilersatz auf das Paar $\mathrm{Ker}(\varphi) \subseteq F$ an. Seien $x_1, \ldots, x_n$ die Elemente von $\ker(\varphi)$ aus diesem Satz, durch $x_{n+1}, \ldots, x_r$ zu einer Basis von F ergänzt und $\alpha_1, \ldots, \alpha_n$ die Elementarteiler, also

$$\mathrm{Ker}(\varphi) = \bigoplus_{i=1}^{n} R \cdot (\alpha_i x_i) \leqslant F = \bigoplus_{i=1}^{n} R \cdot x_i \oplus \bigoplus_{i=n+1}^{r} R \cdot x_i.$$

Also ist

$$M \cong F/\mathrm{Ker}(\varphi) \cong \bigoplus_{i=1}^{n} (R/\alpha_i R)\, x_i \oplus \bigoplus_{i=n+1}^{r} R \cdot x_i.$$

Der erste Summand ist offenbar ein Torsionsmodul, der zweite ist frei und wir haben die gewünschte Zerlegung gefunden. □

Wir zerlegen den Torsionsuntermodul weiter und definieren hierzu für ein Primelement p in R

$$M_p = \{x \in M : p^n x = 0 \quad \text{für ein} \quad n \in \mathbb{N}\},$$

genannt der *p-Torsionsanteil* von M.

Korollar 6.8 *Ist M ein endlich erzeugter Torsionsmodul, so ist*

$$M = \bigoplus_{p \in P} M_p,$$

wobei P die Menge der Primelemente (bis auf Assoziiertheit) von R bezeichnet. Dabei ist $M_p = 0$ für fast alle $p \in P$. Weiter gibt es für jedes p eine Folge natürlicher Zahlen $1 \leq \nu_{p,1} \leq \nu_{p,2} \leq \ldots \leq \nu_{p,r(p)}$, sodass

$$M_p \cong \bigoplus_{j=1}^{r(p)} R/p^{\nu_{p,j}} R$$

Mit dieser Eigenschaft sind die Zahlen $\nu_{p,j}$ eindeutig durch M bestimmt.

Dies ist auch der angekündigte Struktursatz über endlich erzeugte abelsche Gruppen (d.h. $\mathbb{Z}$-Moduln). Jede solche ist direkte Summe eines freien $\mathbb{Z}$-Moduls (also $\mathbb{Z}^r$) und eines Torsionsmoduls, für welche obige Zerlegung gilt. Da $\mathbb{Z}/p^\nu\mathbb{Z}$ für alle $j \leq \nu$ eine Untergruppe der Ordnung p^j enthält, folgt aus dem Korollar oben, dass eine endliche abelsche Gruppe der Ordnung n für jeden Teilnehmer m von n eine Untergruppe der Ordnung m enthält.

Beweis von Korollar 6.8 : Nach dem vorigen Korollar wissen wir bereits, dass $M = M_{\text{tor}} \cong \bigoplus_{i=1}^{n} R/\alpha_i R$ ist, wobei $\alpha_i \mid \alpha_{i+1}$ gilt. Sei $\alpha_i = \varepsilon_i \prod_{p \in P} p^{\nu_{p,i}}$ die Faktorisierung der α_i, wobei $\varepsilon_i \in R^*$. Nach dem chinesischen Restesatz gilt

$$R/\alpha_i R \cong \bigoplus_{p \in P} R/p^{\nu_{p,i}} R.$$

Durch Kombination dieser Zerlegung erhält man

$$M \cong \bigoplus_{p \in P} \bigoplus_{i=1}^{n} R/p^{\nu_{p,i}} R.$$

Dies ist offenbar bereits die gewünschte Zerlegung in p-Torsionsanteile. Um die $\nu_{p,i}$ wie gefordert zu erhalten, genügt es, diejenigen $\nu_{p,i}$ wegzulassen, die Null sind und zur Zerlegung sowieso nicht beitragen. Die Eindeutigkeitsaussage folgt leicht aus der Eindeutigkeitsaussage in Lemma 6.5. □

7 Transzendente Körpererweiterungen

7.1 Transzendenzbasen

Im Körper $\mathbb{Q}\big(x, y, \sqrt{x+y}\big)$ sind alle drei Elemente x, y und $\sqrt{x+y}$ transzendent über $\mathbb{Q}$, aber wenn wir bereits x und y adjungiert haben, wird $\sqrt{x+y}$ algebraisch über dem Zwischenkörper $\mathbb{Q}(x, y)$. Außerdem ist $\mathbb{Q}\big(x, y, \sqrt{x+y}\big) = \mathbb{Q}\big(x, \sqrt{x+y}\big)$, denn $y = \big(\sqrt{x+y}\big)^2 - x$. Die Anzahl der transzendenten Elemente, die wir benötigen, um einen Körper zu erzeugen, messen wir mit folgendem Begriff.

Definition 7.1 *Eine Teilmenge A eines Körpers L ist eine* Transzendenzbasis *der Erweiterung L/K, falls A algebraisch unabhängig über K ist und $L/K(A)$ algebraisch ist. Gibt es eine Transzendenzbasis A, sodass $L = K(A)$, so heißt L* rein transzendent *über K.*

Wie in der linearen Algebra gilt ein Austauschsatz, den wir nur im endlichen Fall beweisen, da dies für die Wohldefiniertheit des Begriffs Transzendenzgrad (siehe unten) ausreicht.

Proposition 7.2 *Ist $A = \{a_1, \ldots, a_n\} \subseteq L$ algebraisch unabhängig über $K \subseteq L$ und $t \in L$ über $K(a_1, \ldots, a_n)$ algebraisch, aber über K transzendent, so gibt es ein j, sodass $A' = \{a_1, \ldots, a_n\} \setminus \{a_j\} \cup \{t\}$ algebraisch unabhängig über K ist und a_j algebraisch über $K(A')$.*

Beweis : Da t über $K(A)$ algebraisch ist, gibt es eine Gleichung $f(a_1, \ldots, a_n, t) = 0$ mit $f \in K[x_1, \ldots, x_n, y]$, wobei für die Variablen x_i die a_i und t für y eingesetzt wurde. (Dabei haben wir bereits etwaige Polynome in den x_i im Nenner durch Durchmultiplizieren entfernt.) Nach der Transzendenzvoraussetzung an t ist f in einer der Variablen x_j nicht-konstant. Wir können dann f aber auch als algebraische Gleichung für a_j über $K(A')$ interpretieren. Ohne Einschränkung sei $j = 1$. Angenommen A' wäre algebraisch abhängig. Da $\{a_2, \ldots, a_n\} \subseteq A$ algebraisch unabhängig ist, müsste dann t algebraisch über $K(a_2, \ldots, a_n)$ sein. Dann ist aber auch a_1 algebraisch über $K(a_2, \ldots, a_n)$, im Widerspruch zur Voraussetzung. □

Wir definieren den *Transzendenzgrad* trdeg(L/K) einer Körpererweiterung L/K als die Mächtigkeit einer endlichen Transzendenzbasis, falls es eine solche gibt, und als ∞ sonst.

Unser nächstes Ziel ist eine Transzendenzgradformel für eine Kette von Körpererweiterungen. Seien L_1 und L_2 zwei Körpererweiterungen von K. Dann ist L_1 *linear disjunkt* zu L_2 über K, falls jede Menge $B \subseteq L_1$, die K-linear unabhängig ist, auch (im Kompositum L_1L_2 aufgefasst) L_2-linear unabhängig ist. Dieser Begriff ist asymmetrisch definiert, aber in der Tat symmetrisch in L_1 und L_2.

Lemma 7.3 *Sei L_1 linear disjunkt zu L_2 über K und $C \subseteq L_2$ K-linear unabhängig. Dann ist $C \subseteq L_1L_2$ auch L_1 linear unabhängig. Insbesondere ist L_2 linear disjunkt zu L_1 über K.*

Beweis : Angenommen die Behauptung ist falsch und es gibt $c_1, \ldots, c_n \in C$ und $a_1, \ldots, a_n \in L_1$ mit $\sum_{i=1}^{n} a_i c_i = 0$. Nach Umsortieren können wir annehmen, dass $\{a_1, \ldots, a_m\} \subseteq L_1$ K-linear unabhängig ist und die restlichen Elemente Linearkombinationen davon, also gibt es $\mu_{jk} \in K$, sodass

$$a_j = \sum_{k=1}^{m} \mu_{jk} a_k \quad \text{für} \quad j = m+1, \ldots, n.$$

Dann gilt

$$0 = \sum_{i=1}^{m} a_i c_i + \sum_{j=m+1}^{n} \sum_{i=1}^{m} \mu_{ji} a_i c_j = \sum_{i=1}^{m} \left(c_i + \sum_{j=m+1}^{n} \mu_{ji} c_j \right) a_i.$$

Also sind alle Ausdrücke in der Klammer gleich Null, im Widerspruch zur K-linearen Unabhängigkeit von C. □

Korollar 7.4 *Sind L_1 und L_2 linear disjunkt über K und $A \subseteq L_1$ algebraisch unabhängig über K, so ist $A \subseteq L_1L_2$ algebraisch unabhängig über L_2.*

Beweis : Algebraisch unabhängig über K bedeutet, dass alle Potenzen von Elementen in A und deren Produkte linear unabhängig über K sind. Mit dieser Beobachtung folgt die Behauptung aus dem vorigen Lemma. □

Korollar 7.5 *Sind L_1 und L_2 linear disjunkt über K, so gilt*

$$\text{trdeg}(L_1L_2/K) = \text{trdeg}(L_1/K) + \text{trdeg}(L_2/K).$$

Beweis : Klar nach dem vorigen Korollar. □

Korollar 7.6 *Sei $K \subseteq L \subseteq M$ ein Körperturm. Dann gilt*

$$\text{trdeg}(L/K) + \text{trdeg}(M/L) = \text{trdeg}(M/K).$$

Beweis : Sei A eine Transzendenzbasis von M/L. Diese Menge ist auch über K algebraisch unabhängig, also ist $\text{trdeg}(M/L) = \text{trdeg}(K(A)/K)$. Außerdem ist nach Definition einer Transzendenzbasis $K(A)$ und L linear disjunkt über K. Also ist nach dem vorigen Korollar $\text{trdeg}(M/L) = \text{trdeg}\big(K(A)/K\big)$. Außerdem ist nach Definition einer Transzendenzbasis $K(A)$ und L linear disjunkt über K. Also ist nach dem vorigen Korollar

$$\text{trdeg}\big(K(A)/K\big) + \text{trdeg}(L/K) = \text{trdeg}\big(L(A)/K\big)$$

und $\text{trdeg}\big(L(A)/K\big) = \text{trdeg}(M/K)$, da $M/L(A)$ algebraisch ist. □

7.2 Ganze algebraische Zahlen

Wir definieren eine Erweiterung des Begriffs von „ganzen Zahlen“, bisher in $\mathbb{Q}$ definiert, auf endlich algebraische Erweiterungen von $\mathbb{Q}$, d.h. auf sogenannte Zahlkörper. Die Kurzfassung hier stellt das Notwendige für den nächsten Abschnitt bereit - man kann damit auch eine ganze Vorlesung „Algebraische Zahlentheorie“ füllen.

Proposition 7.7 *Sei $K/\mathbb{Q}$ algebraisch und $a \in K$. Dann sind folgende Eigenschaften von a äquivalent.*

i) Es gibt ein normiertes Polynom $f \in \mathbb{Z}[X]$ mit $f(a) = 0$.

ii) Der Ring $\mathbb{Z}[a] \subseteq K$ ist ein endlich erzeugter $\mathbb{Z}$-Modul.

iii) Es gibt einen endlich erzeugten $\mathbb{Z}$-Untermodul $A \subseteq K$ mit $a \cdot A \subseteq A$.

Falls a eine der Eigenschaften der Proposition erfüllt, so nennt man a *ganz* (über $\mathbb{Q}$).

Beweis : Für die Implikation ii) $\Rightarrow$ iii) können wir $A = \mathbb{Z}[a]$ nehmen. Für die Implikation iii) $\Rightarrow$ i) seien $v_1, \ldots, v_n$ Erzeuger von A. Dann gibt es nach Voraussetzung $b_{ij} \in \mathbb{Z}$ mit

$$a \cdot v_j = \sum_{j=1}^{n} b_{ij} v_i \quad \text{für} \quad j = 1, \ldots, n.$$

Also ist a eine Nullstelle des charakteristischen Polynoms $\mathrm{Det}(B - X \cdot I_n) \in \mathbb{Z}[X]$, wobei $B = (b_{ij})_{i,j} \in \mathbb{Z}^{n \times n})$ ist. Bis auf einen Faktor $(-1)^n$ ist das charakteristische Polynom normiert und daher folgt i).
Für die Implikation i) $\Rightarrow$ ii) beachte man, dass der Ring $\mathbb{Z}[a]$ als $\mathbb{Z}$-Modul offenbar von allen $a^k, k \in \mathbb{N}$ erzeugt wird. Nach Voraussetzung ist, falls $f = \sum_{i=0}^{m} b_i X^i \in \mathbb{Z}[X]$ mit $b_m = 1$,

$$a^m = -b_0 - b_1 a - b_2 a^2 - \ldots - b_{m-1} a^{m-1}.$$

Damit liegt a^m im von $1, a, a^2, \ldots, a^{m-1}$ erzeugten $\mathbb{Z}$-Modul und durch rekursive Anwendung dieser Beziehung kann man den Grad aller a^k reduzieren. Also ist $\mathbb{Z}[a]$ von der endlichen Menge $1, a, a^2, \ldots, a^{m-1}$ erzeugt. □

Korollar 7.8 *Die Menge der ganzen Zahlen in K bilden einen Ring $\mathcal{O}_K$. Der Schnitt von $\mathcal{O}_K$ mit $\mathbb{Q}$ ist $\mathbb{Z}$. Zu jedem $a \in K$ gibt es einen Nenner $s \in \mathbb{N}$ mit $s \cdot a \in \mathcal{O}_K$.*

Beweis : Seien $a, b \in \mathcal{O}_K$ und $A, B \subseteq K$ die nach iii) der vorigen Proposition existierenden endlich erzeugten $\mathbb{Z}$-Moduln mit $aA \subseteq A$ und $bB \subseteq B$. Der von $A \cdot B$ erzeugte Untermodul $AB \subseteq K$ ist nach dem Distributivgesetz auch endlich erzeugt. Er erfüllt

$$(a + b)AB \subseteq aAB + AbB \subseteq AB, \; abAB \subseteq AB.$$

Also sind nach der vorigen Proposition auch $a + b$ und $a \cdot b$ ganz.
Jedes $a \in \mathbb{Z} \subseteq \mathbb{Q}$ ist offenbar ganz. Ist umgekehrt $a \in \mathbb{Q} \setminus \mathbb{Z}$, so ist $\mathbb{Z}[a]$ nicht endlich erzeugt, denn sonst hätte die Menge $\{a^s, s \in \mathbb{N}\}$ einen gemeinsamen Nenner.

Für die letzte Aussage sei $f_a = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ das Minimalpolynom von a, normiert auf Inhalt 1, also

$$\sum_{i=0}^{n} b_i a^i = 0.$$

Durchmultiplizieren mit b_n^{n-1} liefert, dass das normierte Polynom

$$\sum_{i=0}^{n} b_i b_n^{n-i-1} X^i \in \mathbb{Z}[X]$$

$b_n \cdot a$ als Nullstelle hat. □

7.3 Der Satz von Lindemann-Weierstrass

Ziel des Abschnitts ist der folgende Satz, der insbesondere die Transzendenz von e und von π (wegen $e^{\pi \cdot i} = -1$) beweist.

Satz 7.9 *Seien $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ algebraisch und linear unabhängig über $\mathbb{Q}$. Dann ist die Menge*

$$\{e^{a_1}, \ldots, e^{a_n}\}$$

algebraisch unabhängig über $\mathbb{Q}$.

Der Beweis verwendet zunächst zwei Reduktionsschritte.

Lemma 7.10 *Sind $c_1, \ldots, c_m \in \overline{\mathbb{Q}}$ paarweise verschieden, so ist die Menge*

$$\{e^{c_1}, \ldots, e^{c_m}\}$$

linear unabhängig über $\mathbb{Q}$.

Beweis von Satz 7.9 mit Hilfe von Lemma 7.10 : Angenommen der Satz ist falsch und es gibt ein Polynom $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$, das von Null verschieden ist, aber $P(e^{a_1}, \ldots, e^{a_n}) = 0$ erfüllt. Dann kann man dies als $\mathbb{Q}$-lineare Abhängigkeit der einzelnen Monome lesen, welche von der Gestalt

$$e^{c_k} = (e^{a_1})^{\nu_1} \cdot \ldots \cdot (e^{a_n})^{\nu_n}$$

ist, wobei $\nu_i \in \mathbb{N}$ und $\nu_1, \ldots, \nu_n$ die Exponenten des k-ten Monoms (in einer beliebigen Sortierung) sind. Da die Menge $\{a_1, \ldots, a_n\}$ über $\mathbb{Q}$ linear unabhängig ist, sind

$$c_k = a_1\nu_1 + a_2\nu_2 + \ldots + a_n\nu_n$$

paarweise verschieden. Damit sind die Voraussetzungen des Lemmas erfüllt, welches den gewünschten Widerspruch liefert. □

Lemma 7.11 *Seien $a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ paarweise verschieden und enthalten in einem Körper L, sodass $L/\mathbb{Q}$ galoissch und endlich ist. Sei zudem $\{a_1, \ldots, a_n\}$ $\mathrm{Gal}(L/\mathbb{Q})$-irrelevant, d.h. für alle $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ und alle $j \in \{1, \ldots, n\}$ gibt es ein $k \in \{1, \ldots, n\}$, sodass $\tau(a_j) = a_k$.*
Seien $b_1, \ldots, b_n \in \mathbb{Z}$, nicht alle 0, und konstant auf den Galois-Bahnen der entsprechenden a_i, d.h. gibt es $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\tau(a_j) = a_k$, so gilt $b_j = b_k$. Dann gilt

$$b_1 e^{a_1} + b_2 e^{a_2} + \ldots + b_n e^{a_n} \neq 0.$$

Beweis von Lemma 7.10 mit Hilfe von Lemma 7.11 : Angenommen das Lemma ist falsch und es gibt eine nichttriviale $\mathbb{Q}$-Linearkombination der e^{c_i}. Nach Durchmultiplizieren mit dem Hauptnenner können wir annehmen, dass dies sogar eine $\mathbb{Z}$-Linearkombination ist. Sei L die normale Hülle von $\mathbb{Q}(c_1, \ldots, c_m)/\mathbb{Q}$. Diese ist endlich über $\mathbb{Q}$, da die $c_i \in \overline{\mathbb{Q}}$ sind. Sei $\widetilde{c_1}, \ldots, \widetilde{c_s}$ die Menge der c_i samt ihrer Konjugate unter $\mathrm{Gal}(L/\mathbb{Q})$. Indem wir die Koeffizienten von $\{\widetilde{c_1} \ldots, \widetilde{c_s}\} \setminus \{c_1, \ldots, c_m\}$ als Null setzen, erhalten wir eine $\mathbb{Z}$-Linearkombination

$$\sum_{k=1}^{s} d_k e^{\widetilde{c_k}} = 0.$$

Die Exponenten haben bereits die geforderten Eigenschaften und wir erhalten eine nichttriviale Linearkombination mit der vollen Symmetriebedingung aus Lemma 7.11, indem wir definieren

$$\sum_{j=1}^{n} b_j e^{a_j} = \prod_{\tau \in \mathrm{Gal}(L/\mathbb{Q})} \left(\sum_{k=1}^{s} d_k e^{\tau(\widetilde{c}_k)} \right).$$

Zum Beweis der Symmetrie definieren wir eine Operation $\mathrm{Gal}(L/\mathbb{Q})$ auf Ausdrücken der Form $\sum f_j e^{a_j}$ für $f_j \in \mathbb{Q}$ und $a_j \in L$ durch

$$\sigma \left(\sum f_j e^{a_j} \right) \mapsto \sum f_j e^{\sigma(a_j)}.$$

Diese Operation ist verträglich mit Summe und Produkt, d.h. sind F_1 und F_2 zwei solche Exponentialausdrücke, so gilt $\sigma(F_1 F_2) = \sigma(F_1)\sigma(F_2)$ und $\sigma(F_1 + F_2) = \sigma(F_1) + \sigma(F_2)$ für alle $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Die Invarianz der linken Seite unter allen solchen σ ist die gewünschte Symmetriebedingung. Für die rechte Seite gilt die Invarianz offenbar, denn Anwenden von σ numeriert nur die Faktoren des Produkts um.

Wir müssen nur noch zeigen, dass die so definierten b_j nicht alle Null sind und dann liefert Lemma 7.11 den gewünschten Widerspruch. Dazu sortieren wir die Exponenten nach Realteil. Genauer gesagt, definieren wir auf $\mathbb{C}$ die Ordnungsrelation

$$z_1 < z_2 \text{ falls } \mathrm{Re}(z_1) < \mathrm{Re}(z_2) \quad \text{oder} \quad \mathrm{Re}(z_1) = \mathrm{Re}(z_2) \text{ und } \mathrm{Im}(z_1) < \mathrm{Im}(z_2),$$

welche zwar nicht mit Multiplikation, wohl aber mit Addition verträglich ist. In jedem Faktor (zu $\tau \in \mathrm{Gal}(L/\mathbb{Q})$) wählen wir den bzgl. dieser Relation größten Exponenten $j(\tau)$ aus, d.h. $\tau(\widetilde{c}_{j(\tau)}) = \max\{\tau(\widetilde{c}_k), k = 1, \ldots, n, d_k \neq 0\}$. Deren Produkt trägt zu einem Summand $b_j e^{a_j}$ des Ausdrucks auf der linken Seite bei - und wegen der Maximalität trägt nur ein Summand dazu bei, d.h. $b_j = \prod_{\tau \in \mathrm{Gal}(L/\mathbb{Q})} d_{j(\tau)} \neq 0$. □

Bisher haben wir nur die Homomorphie $e^{a+b} = e^a \cdot e^b$ der Exponentialfunktion verwendet. In der Funktionentheorie zeigt man, dass eine holomorphe Funktion mit dieser Eigenschaft notwendigerweise die Exponentialfunktion ist. Wir verwenden Holomorphie nicht direkt, sondern folgende Integrationseigenschaft.

Lemma 7.12 *Sei $f[X] \in \mathbb{C}[X]$ ein Polynom vom Grad m, sei $t \in \mathbb{C}$ und*

$$I(t) = \int_0^t e^{t-u} f(u) du.$$

Dann ist

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t).$$

Die Unabhängigkeit des Integrals vom Integrationsweg folgt aus der Holomorphie von e^{t-u} und f.

Beweis : Induktiv nach m zeigt man mittels partieller Integration

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t) + \int_0^t e^{t-u} f^{(n+1)}(u) du.$$

□

Wir benötigen noch eine Integralabschätzung. Zu $f \in \mathbb{C}[X]$ sei $\overline{f} \in \mathbb{R}[X]$ das Polynom, das man erhält, indem man jeden Koeffizienten durch seinen Betrag ersetzt. Dann gilt

$$|I(t)| \leq \int_0^{|t|} \mid e^{|t|-u} f(u) \mid du \leq |t|\, e^{|t|} \overline{f}(|t|) \tag{5}$$

nach der Standardabschätzung und da $\overline{f}$ monoton wachsend ist. Wir haben jetzt alle Bausteine beisammen.

Beweis von Lemma 7.11 : Angenommen das Lemma ist falsch und es gibt eine lineare Relation

$$b_1 e^{a_1} + b_2 e^{a_2} + \ldots + b_n e^{a_n} = 0 \tag{6}$$

mit a_i und b_i wie gefordert. Sei $N \in \mathbb{N}$ ein gemeinsamer Nenner für die a_i, d.h. $Na_1, \ldots, Na_n \in \mathcal{O}_L$. Sei p eine Primzahl, die wir am Ende des Beweises so groß wählen bis wir den gewünschten Widerspruch haben.
Die zentrale Rolle spielen die Hilfsfunktionen

$$f_i(X) = N^{np} \left[(X - a_1)(X - a_2) \cdot \ldots \cdot (X - a_n)\right]^p / (X - a_i) \in \mathcal{O}_L[X],$$

ein Polynom vom Grad $np - 1$, so wie die Integralfunktionen

$$I_i(t) = \int_0^t e^{t-u} f_i(u) du$$

und deren Auswertung

$$J_i = b_1 I_i(a_1) + b_2 I_i(a_2) + \ldots + b_n I_i(a_n).$$

Nach (5) ist

$$|J_i| \leq \sum_{k=1}^{n} |a_k \cdot b_k| \, e^{|a_k|} \overline{f}_i \left(|a_k|\right).$$

Wir wollen diesen Ausdruck als Funktion von p abschätzen. Die Koeffizienten von $\overline{f}_i$ sind sicher kleiner als die Koeffizienten von

$$\widetilde{f}_i = N^{np} \left[(X + |a_1|)(X - |a_2|) \cdot \ldots \cdot (X - |a_n|)\right]^p / (X - |a_i|)$$

und somit ist $\overline{f}_i(|a_k|) \leq \widetilde{f}_i(|a_k|)$ und es gilt $\widetilde{f}_i(x) \leq N^{np}(x + \max(|a_1|, \ldots, |a_n|))^{np-1}$ für alle $x \in \mathbb{R}$. Also gibt es Konstanten C_{ik}, sodass $\left|\overline{f}_i \left(|a_k|\right)\right| = C_{ik}^p$. Wir können a_k, b_k und $e^{|a_k|}$ als Konstanten, da unabhängig von p, ansehen. Daher können wir auch die obige Linearkombination exponentiell in p abschätzen, d.h. es gibt C_i, sodass $|J_i| \leq C_i^p$ und aufmultipliziert gibt es $C \in \mathbb{R}$, sodass

$$|J_1 \cdot \ldots \cdot J_n| \leq C^p$$

als Funktion von p.
Wir beginnen nun die Abschätzung von J_i nach unten und nutzen Lemma 7.12 um

$$I_i(a_k) = e^{a_k} \sum_{j=0}^{np-1} f_i^{(j)}(0) - \sum_{j=0}^{np-1} f_i^{(j)}(a_k).$$

auszuwerten. In der Linearkombination J_i fallen die positiven Summanden aufgrund von (6) weg. Es bleibt

$$J_i = -\sum_{j=0}^{np-1} \sum_{k=1}^{n} b_k f_i^{(j)}(a_k). \tag{7}$$

Da $f_i \in \mathcal{O}_L[X]$ gilt das auch für deren Ableitungen. Die Nullstellenordnung von f_i ist p an allen Stellen $a_k, k \neq i$, und sie ist $p-1$ an der Stelle a_i. Genauer ist

$$f_i^{(p-1)}(a_i) = N^{np}(p-1)! \prod_{k=1, k\neq i}^{n} (a_i - a_k)^p \in \mathcal{O}_L.$$

Diese Zahl ist durch $(p-1)!$ teilbar, es ist also sogar $f_i^{(p-1)}(a_i)/(p-1)! \in \mathcal{O}_L$. Durch Nachbau des üblichen Beweis im Fall der ganzen Zahlen können wir zeigen, dass es unendlich viele Primzahlen p gibt, die kein Element der Menge $\{N(a_i - a_k), i, j \in \{1, \ldots, n\}\}$ teilen. Wir beschränken uns ab sofort auf solche p. Für alle i, j, k mit Ausnahme der Fälle $j = p-1$ und $k = i$ gilt stets die Teilbarkeit

$$p! \mid f_i^{(j)}(a_k)$$

in $\mathcal{O}_L$.
Schließlich wollen wir noch die Galois-Symmetrie der Ausgangsgleichung (6) ausnutzen. Diese besagt, dass (7) eine $\mathbb{Q}$-Linearkombination von Ausdrücken der Bauart

$$\sum_{\tau \in \mathrm{Gal}(L/\mathbb{Q})} f_i^{(j)}\big(\tau(a_k)\big)$$

ist. Das Polynom $g = (X - a_i) f_i(X)$ ist unabhängig von i und invariant unter der Anwendung von $\tau \in Gal(L/\mathbb{Q})$, also ist $g \in \mathbb{Q}[X]$ und somit auch $g^{(j)} \in \mathbb{Q}[X]$ für alle j. Ist $g = \sum_{i=0}^{np} b_i X^i$, so erkennt man mittels Polynomdivision, dass

$$f_i(X) = b_{np} X^{np-1} + (b_{np-1} - b_{np} \cdot a_i) X^{np-2} + \ldots,$$

also, dass es von i unabhängige Polynome $R_\nu(X) \in \mathbb{Q}[X]$ gibt, sodass der ν-te Koeffizient von f_i gleich $R_\nu(a_i)$ ist. Schreibt man die Ableitungen von f_i, in denen von g, induktiv beginnend mit

$$f_i'(X) = \frac{g'(X)}{X - a_i} - \frac{g(X)}{(X - a_i)^2}$$

so liefert das gleiche Divisionsargument, dass es $R_{\nu,j}(X) \in \mathbb{Q}[X]$ gibt, welche nicht von i abhängen, sodass der ν-te Koeffizient von $f_i^{(j)}$ gleich $R_{\nu,j}(a_i)$ ist.
Ist also $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\tau(a_i) = a_s$ und $\tau(a_j) = a_t$, so ist $\tau\big(f_i^{(j)}(a_k)\big) = f_s^{(j)}(a_t)$. Folglich ist

$$\tau\left(\sum_{\tau\in\mathrm{Gal}(L/\mathbb{Q})} f_i^{(j)}\big(\tau(a_k)\big)\right) = \sum_{\tau\in\mathrm{Gal}(L/\mathbb{Q})} f_s^{(j)}\big(\tau(a_k)\big).$$

Das wiederum bedeutet, dass $J_1 \cdot \ldots \cdot J_n \in \mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$ ist und außerdem durch $(p-1)!^n$ teilbar. Da $J_i \neq 0$ ist

$$|J_1 \cdot \ldots \cdot J_n| \geqslant (p-1)!^n$$

und da nach der Stirling-Formel $k! \sim \sqrt{2\pi k}\left(\frac{k}{e}\right)^k$ für $k \longrightarrow \infty$ gilt, ergeben die obere und untere Schranke einen Widerspruch für p groß genug. □

Literatur

[GM] Y. GALLOT, P. MOREE: *Ternary cyclotomic polynomials having a large coefficient.* J. reine angew. Math. 632 (2009), 105-125

[GA] PHILIPP HABEGGER: *Grundlagen der Algebra*, Vorlesungsskript, Goethe-Universität Frankfurt/Main, Sommersemester 2012