Algebra II

Wintersemester 2003/04

Christoph Schweigert
Universität Hamburg
Fachbereich Mathematik
Schwerpunkt Algebra und Zahlentheorie

(Stand: 22.10.2007)

Inhaltsverzeichnis

Literatur:

Literatur, die ich bei der Vorbereitung häufig herangezogen habe:

- Falko Lorenz, Einführung in die Algebra, Teil I. Spektrum Akademischer Verlag, 1996.
- Wolfgang Soergel, Skript zur Vorlesung Algebra, erhältlich unter `http://home.mathematik.uni-freiburg.de/soergel/Skripten/Algebra.ps`
- Eine gute Zusammenstellung bietet das Buch Algebra von Serge Lang, Springer, Graduate Texts in Mathematics, das auch als Referenzwerk zu empfehlen ist.

Die aktuelle Version dieses Skriptes finden Sie unter
`http://www.math.uni-hamburg.de/home/schweigert/ws03/askript.ps`
als postscript-Datei und unter
`http://www.math.uni-hamburg.de/home/schweigert/ws03/askript.pdf`
als pdf-Datei. Bitte schicken Sie Korrekturen und Bemerkungen an `schweigert@math.uni-hamburg.de`!

Bei Frau D. Glasenapp möchte ich mich für Ihre große Hilfe bei der Erstellung dieses Skriptes und bei den Hamburger Studenten, besonders bei Frau Mareike Beutler und Frau Birgit Kergel und den Herren Chr. Curilla, Tobias Iffland, Kristian Kouros, J. Kröske, Ph. Sprüssel und Tyll Wibben, für zahlreiche Hinweise bedanken. Der Satz n.n.n aus der Vorlesung Algebra I vom Sommersemester 2003 wird in diesem Skript in der Form I.n.n.n zitiert.

1 Vertiefung der Galoistheorie

1.1 Erinnerung und Ergänzungen

Wir erinnern zunächst an Begriffe aus der Vorlesung Algebra I.

Definition 1.1.1.

(i) Eine Körpererweiterung L/K heißt galoisch, wenn sie normal und separabel ist.

(ii) Eine Körpererweiterung L/K heißt normal, wenn sie algebraisch ist und wenn jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle hat, in $L[X]$ schon vollständig in Linearfaktoren zufällt.

(iii) Eine Körpererweiterung L/K heißt separabel, wenn sie algebraisch ist und für jedes $\alpha \in L$ das Minimalpolynom $\min_K(\alpha)$ separabel ist, d.h. in seinem Zerfällungskörper grad $\min_K(\alpha)$ verschiedene Nullstellen hat.

Wir hatten schon gesehen, dass eine endliche Körpererweiterung L/K dann und nur dann normal ist, wenn L Zerfällungskörper eines Polynoms $f \in K[X]$ ist. Diesen Satz werden wir bald verallgemeinern auf nicht notwendigerweise endliche Körpererweiterungen.

Wir haben auch eine Situation kennengelernt, in der jede algebraische Erweiterung eines Körpers K separabel ist, nämlich den Fall, wenn der Körper K perfekt ist. Ein Körper von Charakteristik Null ist stets perfekt. Im Falle endlicher Charakterstik, char $K = p$, ist ein Körper genau dann perfekt, wenn der Frobenius–Automorphismus

$$\begin{array}{rcl} K & \to & K \\ x & \mapsto & x^p \end{array}$$

surjektiv ist. Daher sind insbesondere endliche Körper perfekt.

Seien E_1 und E_2 zwei Erweiterungskörper eines Körpers K. Wir führen als abkürzende Schreibweise ein

$$f: \ E_1/K \to E_2/K$$

für einen Körperhomomorphismus von E_1 nach E_2, der auf dem Unterkörper K als die Identität wirkt. Da ein von Null verschiedener Körperhomomorphismus stets injektiv ist, sind solche Körperhomomorphismen injektiv.

In folgenden Untersuchungen wird der Begriff des algebraischen Abschlusses eines Körpers eine große Rolle spielen. Um seine Existenz zu zeigen, brauchen wir den folgenden

Satz 1.1.2.
Sei $(E_i)_{i\in I}$ ein System von Erweiterungskörpern eines Körpers K. Dann gibt es einen Erweiterungskörper E von K und Körperhomomorphismen

$$\tau_i : \ E_i/K \to E/K \ ,$$

so dass E aus K durch Adjunktion der Bilder $\cup_{i\in I}\, \tau_i(E_i)$ entsteht.

Der Beweis dieses Satzes beruht auf dem Begriff des Tensorprodukts von Algebren mit Eins, der von unabhängigen Interesse ist. Der Begriff sollte verglichen werden mit dem Begriff des Tensorprodukts von Vektorräumen, den wir im Anhang wiederholen.

Wir fangen mit folgender Vorbetrachtung an.

- Sei K ein Körper und $M \neq \emptyset$ eine nicht-leere Menge. Die Menge von Abbildungen nach K:

  $$K^{(M)} := \{f : M \to K \mid f(m) = 0 \quad \text{für fast alle} \quad m \in M\}$$

  ist durch Addition und skalarer Multiplikation von Bildern in natürlicher Weise ein K-Vektorraum. Es gibt sogar eine ausgezeichnete Basis $\{e_m, m \in M\}$, nämlich die Funktionen

  $$e_m(m') = \delta_{m,m'} \qquad , m' \in M$$

  Identifiziert man e_m mit m, so hat also jedes $f \in K^{(M)}$ eine eindeutige Darstellung $f = \sum c_m \ m$ mit $c_m \in K$ und $c_m = 0$ für fast alle m. Ist die Menge M endlich, so ist offensichtlich $K^{(M)} \cong K^{|M|}$.

- Jetzt setzen wir mehr Struktur auf M als die einer Menge voraus: sei M ein Monoid mit Multiplikation,

  $$M \times M \to M \, ,$$

  und mit Eins, dann wird $K^{(M)}$ durch distributive Fortsetzung des Monoidprodukts zu einer assoziativen unitalen K-Algebra:

  $$ff' = \Big(\sum_m c_m m\Big)\Big(\sum_{m'} d_{m'} m'\Big) = \sum_{m,m'} c_m d_{m'} (m \cdot m') \, .$$

- Sei uns nun eine Familie $(A_i)_{i\in I}$ von K-Algebren mit Eins vorgegeben. Wir betrachten die Monoidstruktur auf der Menge

  $$M := \{\alpha = (a_i)_{i\in I} \, , \, a_i \in A_i \, , \, a_i = 1_{A_i} \quad \text{für fast alle} \quad i\} \, ,$$

die durch komponentenweise Multiplikation erklärt ist:

$$(a_i)(b_i) := (a_i b_i)\,.$$

Die oben geschilderte Konstruktion führt uns auf die K-Algebra

$$K^{(M)} = \Big\{ \sum_{\alpha\in M} c_\alpha \alpha | c_\alpha \in K, \quad \text{fast alle} \quad c_\alpha = 0 \Big\}\,.$$

Diese Algebra ist sehr groß. Sei nun $U \subseteq K^{(M)}$ der K-Teilraum von $K^{(M)}$, der über K von den folgenden Vektoren erzeugt wird:

- $(a_i) + (b_i) - (s_i)$ falls für *ein* j $\quad a_j + b_j = s_j$; und sonst $\quad a_i = b_i = s_i$
- $(a_i) - c(b_i)$ falls für ein j gilt $\quad a_j = cb_j$; und sonst $\quad a_i = b_i$

U ist ein Ideal in der K-Algebra $K^{(M)}$, somit ist $K^{(M)}/U$ eine K-Algebra. Die Algebra mit Eins

$$\bigotimes_{i\in I} A_i := K^{(M)}/U$$

heißt das Tensorprodukt der K-Algebren A_i. Die Abbildung

$$\begin{array}{ccc} \times_{i\in I} A_i & \to & \bigotimes_{i\in I} A_i \\ (a_i) & \mapsto & (a_i) \bmod U \end{array}$$

ist multilinear, d.h. sie ist linear an jeder Stelle $i \in I$. Wir setzen

$$\otimes_{i\in I} a_i = (a_i) \bmod U \quad \text{für} \quad (a_i) \in M\,.$$

Jedes Element aus $\bigotimes A_i$ kann in der Form

$$\sum_\alpha c_\alpha (\bigotimes_i \alpha_i) \quad \text{mit} \quad c_\alpha \in K \tag{1}$$

geschrieben werden. Man beachte, dass man hierbei nicht auf die Summation über mehrere Elemente der Form $\bigotimes_i \alpha_i$ verzichten kann. Außerdem ist die Darstellung in der Form (1) nicht eindeutig, zum Beispiel wegen Relationen der Form

$$c(a_1 \bigotimes a_2) - 1(ca_1) \bigotimes a_2 = 0$$

Die Nützlichkeit des Tensorprodukts ergibt sich aus der folgenden universellen Eigenschaft. Für jeden Wert des Index $j \in I$ hat man nun einen K-Algebren Homomorphismus

$$\begin{aligned} \sigma_j \quad &: \quad A_j \to \bigotimes_{i\in I} A_i \\ a_j \quad &\mapsto \quad 1 \times 1 \otimes \cdots \otimes a_j \otimes 1 \cdots \otimes 1 \end{aligned}$$

Das Tensorprodukt besitzt die folgende universelle Eigenschaft, über die man es auch charakterisieren kann: Sei A eine beliebige K–Algebra und seien

$$\varphi_j : A_j \to A \qquad j \in I$$

K–Algebrenhomomorphismen mit

$$\varphi_i(a)\varphi_j(b) = \varphi_j(b)\varphi_i(a) \quad \text{für} \quad i \neq j\,.$$

Dann gibt es genau einen K–Algebrenhomomorphismus

$$\varphi : \bigotimes_i A_i \to A\,,$$

so dass das folgende Diagramm

$$\begin{array}{ccccc} \bigotimes\limits_i & & A_i & \xrightarrow{\varphi} & A \\ & & \nwarrow & & \nearrow \\ & & \sigma_j & A_j & \varphi_j \end{array}$$

für alle $j \in I$ kommutiert. Den Beweis überlassen wir dem Leser als Übung.

Wir haben nun die Hilfsmittel, um Satz 1.1.2 zu beweisen:

Beweis.

Betrachte jeden Erweiterungskörper E_i als K-Algebra. Die gerade geschilderte Konstruktion liefert uns das Tensorprodukt von Algebren

$$A = \bigotimes_{i\in I} E_i$$

mit Injektionen von Algebren

$$\begin{aligned} \sigma_i : \quad & E_i \hookrightarrow A \\ & \alpha_i \mapsto 1 \otimes 1 \otimes \ldots \otimes \alpha_i \otimes 1 \cdots \otimes 1 \ . \end{aligned}$$

Nun ist zwar sicher A ist eine K–Algebra mit Eins $1_A = 1_{E_1} \otimes 1_{E_2} \cdots \otimes 1_{E_m} \neq 0$, aber im allgemeinen kein Körper. Nach dem Zornschen Lemma gibt es aber ein maximales Ideal $\mathfrak{m}$ in A. Dann ist $E = A/\mathfrak{m}$ ein

Körper und gleichzeitig eine K–Algebra, also enthält E insbesondere K als Unterkörper. Die Abbildungen

$$\tau_i : E_i \twoheadrightarrow A/\mathfrak{m} = E$$

die als Verkettung der Injektion σ_i mit der kanonischen Projektion auf den Quotienten $A/\mathfrak{m}$ definiert sind, sind K–Algebrenhomomorphismen und es ist

$$E = K\Big(\bigcup_i \tau_i E_i\Big)\,. \qquad \square$$

Definition 1.1.3.
Ein Körper C heißt algebraisch abgeschlossen, wenn jedes Polynom $f(X) \in C[X]$ vom Grade ≥ 1 eine Nullstelle in C besitzt.

Beispiel 1.1.4.
Der Körper der komplexen Zahlen ist algebraisch abgeschlossen. Der Körper der reellen Zahlen oder der Körper der rationalen Zahlen sind algebraisch nicht abgeschlossen.

Lemma 1.1.5.
Die folgenden Aussagen über einen Körper sind äquivalent:

(i) C ist algebraisch abgeschlossen.

(ii) Jedes irreduzible Polynom in $C[X]$ ist linear, d.h. von Grade 1.

(iii) Jedes Polynom in $C[X]$ vom Grade ≥ 1 zerfällt über C vollständig in Linearfaktoren.

(iv) Ist E/C eine *algebraische* Körpererweiterung, so ist $E = C$.

Beweis.

(i)⇒(ii) Sei $f \in C[X]$ irreduzibel. Nach (i) gibt es ein $\alpha \in C$, so dass $f(\alpha) = 0$, damit gilt $f = \gamma(X - \alpha)$ mit $\gamma \in C^\times$.

(ii)⇒(iii) Der Ring $C[X]$ ist euklidisch, also insbesondere faktoriell. Jedes Polynom hat also eine Primfaktorzerlegung, in der nach (ii) alle auftretenden Polynome linear sind.

(iii)⇒(iv) Sei E/C algebraisch. Für jedes $\alpha \in E$ ist $\min_C(\alpha)$ nach (iii) linear, also $\alpha \in C$.

(iv)⇒(i) Sei $f \in C[X]$ von Grad ≥ 1, E ein Zerfällungskörper von f. E/C ist algebraisch, also impliziert (iv), dass $E = C$ gilt. $\square$

Satz 1.1.6. *(Steinitz)*
Sei K ein beliebiger Körper. Dann gilt

(i) Es existiert ein Erweiterungskörper C von K mit folgenden Eigenschaften:

(a) C ist algebraisch abgeschlossen.

(b) C/K ist algebraisch.

Einen solchen Körper nennt man einen algebraischen Abschluss von K oder eine algebraisch abgeschlossene Hülle von K.

(ii) Sind C_1 und C_2 zwei algebraische Abschließungen von K, so ist C_1/K isomorph zu C_2/K.

Beweis.

Wir müssen einen Körper konstruieren, der alle algebraischen Erweiterungen von K enthält. Dazu müssen wir eine beliebige Zahl algebraischer Elemente adjungieren können. Ein Körper, der durch die Adjunktion von n algebraischen Elementen entsteht, ist aber als Quotient des Polynomrings über K in n Variablen darstellbar.

Um die Zahl der Variablen beliebig zu lassen, betrachten wir zunächst den Polynomring $K[X_1, X_2, \dots] = K[X_n, n \in \mathbb{N}]$ in abzählbar vielen Variablen. Sei I die Menge all seiner Teilmengen

$$M \subseteq K[X_n, n \in \mathbb{N}]\,,$$

zu denen es ein $m \in \mathbb{N}$ gibt, mit der Eigenschaft, dass M ein maximales Ideal im Polynomring $K[X_1, \dots, X_m]$ in m Variablen ist. Sei $E_M := K[X_1, \dots, X_m]/M$ der zugehörige Restklassenkörper, den wir als Erweiterungskörper von K auffassen. Nach Satz 1.1.2 finden wir einen Erweiterungskörper E/K und für alle $M \in I$ Injektionen

$$\sigma_M : E_M \to E\,,$$

so dass E durch Adjunktion der Bilder entsteht.

Wir wollen jetzt zunächst das folgende Zwischenresultat beweisen:
Für jede endliche Körpererweiterung L/K existiert ein Körperhomomorphismus $L/K \to E/K$.

Denn sei $L = K(\alpha_1, \dots, \alpha_m)$ mit α_i algebraisch über K. Betrachte den Homomorphismus von K-Algebren

$$\begin{array}{rccc} \varphi: & K[X_1, \dots, X_m] & \to & L \\ & X_i & \mapsto & \alpha_i \end{array}$$

Sein Kern $M = \ker \varphi$ ist ein maximales Ideal von $K[X_1, \ldots, X_m]$. Daher induziert φ einen Isomorphismus

$$\widetilde{\varphi} \ : \ E_M \to L \, .$$

Der gesuchte Homomorphismus ist dann $\sigma_M \circ \tilde{\varphi}^{-1}$. Dies beweist das Zwischenresultat.

Der Körper E, den wir eben konstruiert haben, ist noch etwas zu gross. Wir betrachten daher jetzt den algebraische Abschluss C von K in E,

$$C = \{\alpha \in E \mid \alpha \text{ algebraisch über } K\} \, .$$

C/K ist sicher algebraisch. Wir müssen noch zeigen, dass C algebraisch abgeschlossen ist.

Andernfalls gäbe es eine echte algebraische Erweiterung F/C. Sei $\alpha \in F \setminus C$. Dann ist α algebraisch über C, und C wiederum algebraisch über K. Also ist α ist algebraisch über K und wir betrachten das Minimalpolynom $f = \min_K(\alpha)$.

f habe in C die n verschiedenen Nullstellen $\beta_1, \ldots, \beta_n$. Dann hat der Zwischenkörper $L = K(\alpha, \beta_1, \ldots, \beta_n) \subseteq F$ die Eigenschaft, dass L/K endlich ist. Nach dem Zwischenresultat gibt es einen Körperhomomorphismus

$$\varphi : K(\alpha, \beta_1, \ldots, \beta_n) \to E \, ,$$

dessen Bild aber, da alle Nullstellen $\alpha, \beta_1, \ldots, \beta_n$ algebraisch über K sind, schon in C liegt. Da φ als Körperhomomorphismus injektiv ist, finden wir in C also $n + 1$ verschiedenen Nullstellen.

$$\varphi(\alpha), \varphi(\beta_1), \ldots \varphi(\beta_n) \, .$$

Dies ist ein Widerspruch zur Annahme, dass f in C genau n verschiedene Nullstellen hat. Damit hat aber C keine echte algebraische Erweiterung und ist somit nach Lemma 1.1.5 algebraisch abgeschlossen. □

Für die Eindeutigkeitsaussage (ii) in Satz 1.1.6 benötigen wir das folgende Lemma, das wir gleich etwas allgemeiner formulieren und beweisen werden:

Lemma 1.1.7.
Sei $\sigma : K \to K'$ ein Isomorphismus von Körpern und L/K eine algebraische Körpererweiterung. Ist C' ein algebraischer Abschluss von K', so lässt sich σ zu einem Homomorphismus

$$\tau : L \to C'$$

fortsetzen.

Beweis.

Wir behandeln zunächst den Fall, dass $K = K'$ und $\sigma = \mathrm{id}_K$ gilt. Satz 1.1.2, angewandt auf $E_1 = L$ und $E_2 = C'$ liefert einen Erweiterungskörper E von K mit Injektionen

$$\sigma_i : E_i \to E\,,$$

so dass gilt

$$E = \sigma_2 C'(\sigma_1 L)\,.$$

Nun ist aber $\sigma_2 C'$ auch wieder algebraisch abgeschlossen und die Körpererweiterung $E/\sigma_2 C'$ algebraisch. Also gilt $E = \sigma_2 C'$, und

$$\sigma_2 : C' \to E$$

ist ein Isomorphismus. Der Körperhomomorphismus

$$(\sigma_2)^{-1} \circ \sigma_1 \;:\; L \to C'$$

ist dann eine gewünschte Fortsetzung.

Im allgemeinen Fall $K \neq K'$ konstruieren wir zunächst eine Erweiterung L' und einen Homomorphismus ρ, so dass das folgende Diagramm vertauscht

$$\begin{array}{ccc} L & \stackrel{\rightarrow}{\rho} & L' \\ \uparrow & & \uparrow \\ K & \stackrel{\rightarrow}{\sigma} & K' \end{array}\,.$$

Hierzu nehmen wir als Menge $L' := (L \setminus K) \cup K'$ und definieren ein Produkt durch $lk' = l\sigma^{-1}(k')$ und $l_1 l_2 := \sigma^{-1}(l_1 l_2)$. Den Körperisomorphismus ρ definieren wir dann durch die Identität auf $L \setminus K$ und durch σ auf K. Wir haben schon gesehen, dass dann ein Körperhomomorphismus

$$\tau' : L' \to C'$$

existiert, und $\tau = \tau' \circ \rho : L \to C$ ist eine gewünschte Fortsetzung des Isomorphismus σ.

Wir können nun den Beweis von Satz 1.1.6 (ii) vervollständigen:

Beweis.

Seien C_1/K und C_2/K zwei algebraische Abschließungen. Nach Lemma 1.1.7 existiert ein Körperhomomorphismus $\tau : C_1/K \to C_2/K$. Da die

Körpererweiterung C_2/K algebraisch ist, ist erst recht die Körpererweiterung $C_2/\tau C_1$ algebraisch. Nun ist τC_1 algebraisch abgeschlossen, hat also keine echten algebraischen Erweiterungen, also gilt $C_2 = \tau C_1$. τ ist der gewünschte Isomorphismus zwischen den beiden algebraischen Abschließungen. □

Man beachte, dass dieser Körperhomomorphismus nicht kanonisch ist! Es ist also nicht ganz gerechtfertigt, von *dem* algebraischen Abschluss zu sprechen.

Definition 1.1.8.
Sei K ein Körper und C ein algebraischer Abschluss von K. Zwei Elemente $\alpha, \beta \in C$ heißen konjugiert über K, falls es einen Automorphismus σ von C/K gibt, so dass gilt

$$\sigma(\alpha) = \beta\,.$$

Die zu $\alpha \in C$ über K konjugierten Elemente von C heißen K–konjugierte von α.

Bemerkung 1.1.9.
Folgende Aussagen sind äquivalent:

(i) *β ist über K konjugiert zu $\alpha \in C$.*

(ii) *β ist Nullstelle von $\min_K(\alpha)$.*

(iii) *Es gibt einen K–Isomorphismus*

$$\tau : K(\alpha) \to K(\beta)$$

mit $\tau(\alpha) = \beta$.

(iv) $\min_K(\alpha) = \min_K(\beta)$. *Inbesondere besitzt jedes $\alpha \in C$ höchstens*

$$[K(\alpha) : K] = \textit{grad}\, \min_K(\alpha)$$

verschiedene K–Konjugierte in C.

Beweis.
(i)⇒(ii) Da α und β konjugiert sein sollen, gibt es einen Automorphismus $\sigma : C/K \to C/K$ mit der Eigenschaft, dass

$$\sigma(\alpha) = \beta,\,.$$

Für das Minimalpolynom $f = \min_K(\alpha)$ gilt dann

$$f(\beta) = f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0\,.$$

(ii)⇒(iv) Sei $f := \min_K(\alpha)$ das Minimalpolynom und sei $f(\beta) = 0$. Wegen der letzten Gleichheit teilt das Minimalpolynom $\min_K(\beta)$ das Polynom f. Da f irreduzibel und normiert ist, folgt $f = \min_K(\beta)$.

(iv)⇒(iii) folgt aus Satz I.4.1.4, angewandt auf $M = K(\beta)$.

(iii)⇒(i) Mit Hilfe von Lemma 1.1.7 zeigt man, dass τ zu einem Automorphismus von C/K fortgesetzt werden kann. □

Wir können jetzt die Separabilität eines Elements mit Hilfe seiner Konjugierten in einem algebraischen Abschluss ausdrücken.

Bemerkung 1.1.10.
Mit obigen Bezeichnungen sind für $\alpha \in C$ und $f = \min_K(\alpha)$ das Minimalpolynom von α vom Grad $n = \operatorname{grad} f$ folgende Aussagen äquivalent:

(i) α hat über K genau n verschiedene Konjugierte in C.

(ii) Es gibt genau n verschiedene Homomorphismen

$$K(\alpha)/K \to C/K\,.$$

(iii) f hat genau n verschiedene Nullstellen in C, d.h. f ist separabel und somit ist α separabel.

Beweis.
Da der Homomorphismus $\tau = K(\alpha)/K \to C/K$ durch die Angabe von $\tau(\alpha)$ festgelegt ist, folgt Bemerkung 1.1.10 aus Bemerkung 1.1.9. □

Den folgenden Satz über Separabilität werden wir in dieser Vorlesung nicht beweisen:

Satz 1.1.11.
Sei E/K eine algebraische Körpererweiterung und F ein Zwischenkörper. Die Körpererweiterung E/K ist genau dann separabel, wenn die beiden Körpererweiterungen E/F und F/K separabel sind.

Wir wollen auch noch den folgenden einfachen Sachverhalt festhalten:

Satz 1.1.12.
Jeder Endomorphismus einer algebraischen *Körpererweiterung ist ein Automorphismus.*

Beweis.

Sei $\sigma : E/K \to E/K$ ein Homomorphismus von Körpererweiterungen. Als solcher ist σ sicher injektiv, es bleibt $\sigma E = E$ zu zeigen. Sei also $\alpha \in E$ und $f = \min_K(\alpha)$. Dann bewirkt σ eine Permutation der endlichen Menge der Nullstellen von f. Permutationen sind aber surjektiv. □

Schließlich wollen wir auch noch Eigenschaften normaler Körpererweiterungen mit Hilfe des algebraischen Abschlusses untersuchen.

Satz 1.1.13.
Sei E/K eine algebraische Körpererweiterung und C ein algebraischer Abschluss von E (und somit auch von K). Dann sind äquivalent:

(i) *E/K ist normal*

(ii) *Für jeden Homomorphismus*

$$\sigma : E/K \to C/K$$

gilt $\sigma E = E$. Das heißt, dass σ einen Automorphismus von E vermittelt.

(iii) *Jeder Automorphismus von C/K vermittelt durch Restriktion einen Automorphismus von E/K.*

(iv) *E ist Zerfällungskörper von Polynomen, d.h. es gibt eine Menge $M \subset K[X]$ von nicht–konstanten Polynomen mit Nullstellenmenge N in C, so dass*

$$E = K(N)$$

Beweis.

(i)⇒(iv) Betrachte die Menge M aller Minimalpolynome von Elementen in E, also $M = \{\min_K(\alpha) \mid \alpha \in E\} \subseteq K[X]$ und dann die Menge N aller Nullstellen in C aller Polynome in M, $N = \{\beta \in C \mid \exists f \in M$ mit $f(\beta) = 0\}$. Offenbar gilt $E \subseteq N$. Da E/K normal ist, folgt aber auch die umgekehrte Inklusion $N \subseteq E$. Damit haben wir die Gleichheit $E = N$, und somit erst recht $E = K(N)$.

(iv)⇒(iii) Sei $\sigma : C/K \to C/K$ ein Automorphismus. Dann gilt $\sigma(N) \subseteq N$, also

$$\sigma(E) = \sigma(K(N)) \subseteq K(N) = E \ .$$

Nach Satz 1.1.12 ist dann $\sigma E = E$, also $\sigma_{|E}$ ein Automorphismus von E.

(iii)⇒(ii) Jeder vorgegebene Homomorphismus

$$\sigma : E/K \to C/K$$

läßt sich nach Lemma 1.1.7 zu einem Homomorphismus

$$\widetilde{\sigma} : C/K \to C/K$$

fortsetzen, der wegen Satz 1.1.12 sogar ein Automorphismus ist. Eingeschränkt auf E ist er nach (iii) ein Automorphismus von E, d.h. $\sigma E = E$.

(ii)⇒(i) Sei f irreduzibel und gelte $f(\alpha) = 0$ für ein $\alpha \in E$. Zu zeigen ist, dass dann alle Nullstellen von f in E liegen. Sei also $f(\beta) = 0$ für ein $\beta \in C$.

Es gibt einen K–Isomorphismus

$$\begin{array}{rccc} \sigma : & K(\alpha) & \to & K(\beta) \\ & \alpha & \mapsto & \beta \end{array}$$

Nach Lemma 1.1.7 kann dieser ausgedehnt werden zu einem Homomorphismus $\tau : E \to C$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} E & \overrightarrow{\tau} & C \\ \uparrow & & \uparrow \\ K(\alpha) & \overrightarrow{\sigma} & K(\beta) \end{array}$$

Aus der Annahme, dass (ii) gilt, folgt $\tau E = E$, insbesondere folgt daraus $E \ni \tau\alpha = \sigma\alpha = \beta$. □

Wir geben schließlich noch die folgende Charakterisierung der normalen Hülle an:

Satz 1.1.14.
Sei E/K eine algebraische Körpererweiterung und C ein algebraischer Abschluss von E (und damit auch von K). Dann ist das Kompositum aller zu E über K konjugierter Zwischenkörper gleich der normalen Hülle E' von E/K, also

$$E' = K\Big(\bigcup_{\sigma \in \mathrm{Hom}_K(E,C)} \sigma(E)\Big)\,.$$

Beweis.

Wegen Satz 1.1.13 (ii) ist das Kompositum sicher normal, enthält also die normale Hülle E', die ja der Schnitt aller normalen Erweiterungen ist. Um die umgekehrte Inklusion zu zeigen, betrachte für $\alpha \in E$ und $\sigma \in \mathrm{Hom}_K(E, C)$ das Element $\sigma(\alpha)$. Es ist eine Nullstelle des Minimalpolynoms $\min_K(\alpha)$. Dieses Polynom hat eine Nullstelle in E', nämlich α. Da E' normal sein soll, liegt auch die weitere Nullstelle $\sigma(\alpha)$ in E'. □

1.2 Galoische Körpererweiterungen

Sei E ein Körper und G eine Gruppe von Automorphismen von E, $G \subseteq \mathrm{Aut}\,(E)$.

Definition 1.2.1.
Die Menge $E^G = \{\alpha \in E \,|\, \sigma\alpha = \alpha$ für alle $\sigma \in G\}$ heißt Fixkörper von G und ist ein Körper:

$$\alpha, \beta \in E^G \;\Rightarrow\; \alpha\beta, \alpha + \beta, \alpha^{-1} \in E^G\,.$$

Satz 1.2.2.
Sei E ein Körper und $G \subseteq \mathrm{Aut}\,(E)$ und $K = E^G$. (Man beachte, dass hier G nicht als endlich vorausgesetzt wird.) Für $\alpha \in E$ betrachten wir den Orbit unter der Wirkung von G:

$$G\alpha := \{\sigma\alpha | \sigma \in G\}$$

(i) Besteht die Bahn $G\alpha$ aus endlich vielen Elementen von E, so ist α algebraisch über K.

(ii) Sei wie in (i) die Bahn $G\alpha$ endlich. Schreibt man dann die Bahn in der Form

$$G\alpha = \{\alpha = \alpha_1, \alpha_2, \ldots \alpha_n\}$$

mit lauter paarweise verschiedenen Elementen $\alpha_i \in E$, so ist das separable und normierte Polynom

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i) \tag{2}$$

das Minimalpolynom von α über K.

Beweis.

Zum Beweis betrachten wir den von $\tau \in G$ auf dem Polynomring $E[X]$ induzierten Isomorphismus

$$\begin{array}{rcl} \tau: \ E[X] & \to & E[X] \\ g = \sum_i b_i X^i & \mapsto & g^\tau = \sum_i \tau(b_i) X^i \end{array}$$

durch Wirkung auf den Koeffizienten des Polynoms. Offenbar bewirkt jedes τ eine Permutation der Nullstellen α_i Polynoms f, das in (2) definiert wurde. Außerdem ist τ als Körperautomorphismus injektiv. Da die Bahn $G\alpha$ nach Voraussetzung endlich ist, ist die Wirkung von τ auf $G\alpha$ surjektiv. Also gilt für das Polynom aus (2) die Beziehung $f^\tau = f$. Damit gilt für alle seine Koeffizienten

$$f = \sum_i \gamma_i X^i$$

und für alle $\tau \in G$ die Gleichung $\tau(\gamma_i) = \gamma_i$ Also haben wir $\gamma_i \in K = E^G$. Somit liegt $f \in K[X]$ und α ist als Nullstelle von f algebraisch über K.

Wir müssen noch zeigen, dass f gleich dem Minimalpolynom $g := \min_K(\alpha)$ ist. Aus $f(\alpha) = 0$ folgt, dass g das Polynom f teilt. Außerdem folgt aus $g(\alpha) = 0$ auch $g(\sigma\alpha) = 0$ für alle Automorphismen $\sigma \in G$. Alle Elemente von $G\alpha$ sind also auch Nullstellen des Minimalpolynoms g, also gilt grad $g \geq$ grad f. Da beide Polynome normiert sind, folgt $f = g$. □

Definition 1.2.3.
Sei E/K eine algebraische Körpererweiterung.

(i) Die Gruppe $G(E/K) = Hom_K(E, E) \subseteq Aut(E)$ heißt die Galoisgruppe von E/K.

(ii) Die Erweiterung E/K heißt galoisch, wenn

$$K = E^{G(E/K)}.$$

Bemerkung 1.2.4.

(i) Für eine beliebige algebraische Erweiterung E/K ist offensichtlich stets

$$K \subseteq E^{G(E/K)}.$$

(ii) Sei G eine Untergruppe der Automorphismengruppe $Aut(E)$ und $K = E^G$ der zugehörige Fixkörper. Dann gilt: Ist E/K algebraisch, so ist E/K galoisch. Denn aus der Inklusion $G \subseteq G(E/K)$ folgt sofort auch

$$E^{G(E/K)} \subseteq E^G = K\,,$$

womit mit (i) zusammen gezeigt ist, dass $K = E^{G(E/K)}$ gilt.

Satz 1.2.5.
Für eine algebraische Erweiterung E/K sind die folgenden Aussagen äquivalent:

(i) E/K ist galoisch.

(ii) E/K ist separabel und normal.

Beweis.

(i)⇒(ii) Sei $\alpha \in E$ ein Element in E und $f = \min_K(\alpha)$ sein Minimalpolynom. Nun ist für $G := G(E/K)$ die Bahn $G\alpha = \{\sigma\alpha | \sigma \in G\}$ als Untermenge der Nullstellenmenge von f endlich. Aus Satz 1.2.2 folgt, dass $f = \prod_{\alpha_i \in G\alpha}(X - \alpha_i)$ gilt. Das Minimalpolynom jedes Elements ist also separabel und alle Nullstellen $\alpha_i \in E$. Also zerfällt das Minimalpolynom und die Körpererweiterung ist normal und separabel.

(ii)⇒(i) Zu zeigen ist, dass für jedes $\alpha \in E\backslash K$ es ein $\tau \in G(E/K)$ gibt, das α nicht festlässt, $\tau(\alpha) \neq \alpha$. Da die Körpererweiterung $K(\alpha)/K$ separabel sein soll und die Körpererweiterung $E/K(\alpha)$ normal sein soll, folgt aus Satz I.4.2.10, dass es

$$[K(\alpha) : K] \; > 1$$

Ausdehnungen des Körperhomomorphismus $K \hookrightarrow E$ zu einem Körperhomomorphismus $K(\alpha) \to E$ gibt. Da ein solcher Körperhomomorphismus schon durch seinen Wert auf α festliegt, gibt es insbesondere einen Homomorphismus $\sigma : K(\alpha) \to E$, für den $\sigma(\alpha) \neq \alpha$ gilt.

Sei C ein algebraischer Abschluss von E, und damit auch von $\sigma(K(\alpha)) \subseteq E$. Mit Lemma 1.1.7 finden wir einen Automorphismus τ, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} C & \overrightarrow{\tau} & C \\ \uparrow & & \uparrow \\ K(\alpha) & \overrightarrow{\sigma} & \sigma(K(\alpha)) \end{array}$$

Insbesondere gilt $\tau(\alpha) \neq \alpha$ und $\tau\big|_K = \mathrm{id}_K$. Da die Körpererweiterung E/K normal sein sollte, ist aber $\tau(E) \subseteq E$. Also haben wir ein $\tau \in G(E/K)$ mit den gewünschten Eigenschaften konstruiert. □

Bemerkung 1.2.6.
Sei $f \in K[X]$ ein separables *Polynom mit Zerfällungskörper E/K. Dann ist E/K eine endliche galoische Erweiterung. Denn Zerfällungskörper sind nach I.4.1.9 (oder 1.1.13) immer normal. Seien $\alpha_1 \dots \alpha_s$ die Nullstellen von f in E, also $E = K(\alpha_1, \dots, \alpha_s)$, so ist jedes α_i separabel über K, also ist E über K nach I.4.2.10 auch separabel.*

Bemerkung 1.2.7.
Sei E/K eine galoische Erweiterung. Wir bezeichnen mit $\mathcal{Z}(E/K)$ die Menge (eigentlich den Verband) aller Zwischenkörper F von E/K, also $K \subseteq F \subseteq E$, und mit $\mathcal{U}(E/K)$ die Menge aller Untergruppen der Galoisgruppe von $G(E/K)$.

Betrachte die Abbildung

$$\begin{array}{ccc} \mathcal{Z}(E/K) & \to & \mathcal{U}(E/K) \\ F & \mapsto & G(E/F) \end{array} \tag{3}$$

Wir wollen zeigen, dass für jeden Zwischenkörper die Körpererweiterung E/F galoisch ist. Nach Satz 1.2.5 ist E/K normal und separabel. Nach Satz 1.1.11 folgt aus der Separabilität von E/K insbesondere auch die der Körpererweiterung E/F. Da E/K normal ist, ist nach Satz 1.1.13 der Körper E der Zerfällungskörper einer Menge von Polynomen in $K[X]$. Dann ist aber E erst recht der Zerfällungskörper einer Menge von Polynomen in $F[X]$, und somit ist auch E/F normal. Wiederum aus Satz 1.2.5 folgt, dass E/F galoisch ist. Achtung, die Körpererweiterung F/K muss dagegen nicht normal sein, wie wir in den Übungen in Beispielen sehen werden.

Ferner ist

$$G(E/F) = Hom_F(E, E) \subseteq Hom_K(E, E) = G(E/K)\,,$$

also geht die Abbildung (3) wirklich in die Untergruppen der Galoisgruppe $G(E/F)$. Sie ist auch injektiv: seien F_1 und F_2 zwei Zwischenkörper deren Galoisgruppen die gleichen Untergruppen von $G(E/K)$ sind, $G(E/F_1) = G(E/F_2)$. Dann gilt:

$$F_1 = E^{G(E/F_1)} = E^{G(E/F_2)} = F_2\,.$$

Diese Beziehung von Zwischenkörpern und Untergruppen der Galoisgruppe wollen wir nun systematisch ausbauen.

Satz 1.2.8.
Sei E/K eine galoische Körpererweiterung, F ein Zwischenkörper, $F \in \mathcal{Z}(E/K)$ und $\sigma \in G(E/K)$. Dann gilt

$$G(E/\sigma F) = \sigma G(E/F)\sigma^{-1} \equiv \{\sigma\tau\sigma^{-1} \mid \tau \in G(E/F)\}$$

und die folgenden Aussagen sind äquivalent:

(i) F/K *ist galoisch.*

(ii) $\sigma F = F$ *für alle* $\sigma \in G(E/K)$.

(iii) $\sigma G(E/F)\sigma^{-1} = G(E/F)$ *für alle* $\sigma \in G(E/K)$, *d.h.* $G(E/F)$ *ist ein Normalteiler der Galoisgruppe* $G(E/K)$.

Beweis.

Die erste Beziehung folgt durch reines Nachrechnen: für $\tau \in G(E/K)$ gilt

$$\begin{aligned} \tau \in G(E/\sigma F) &\iff \tau\sigma\alpha = \sigma\alpha \qquad \forall\, \alpha \in F \\ &\iff \sigma^{-1}\tau\sigma\alpha = \alpha \qquad \forall\, \alpha \in F \end{aligned}$$

Daraus folgt aber $\sigma^{-1}\tau\sigma \in G(E/F)$, was äquivalent zu $\tau \in \sigma G(E/F)\sigma^{-1}$ ist.

(ii) $\iff$ (iii) Da die Abbildung in Bemerkung 1.2.7 injektiv ist, gilt $\sigma F = F$ genau dann, wenn $G(E/\sigma F) = G(E/F)$. Nach der gerade bewiesenen Gleichheit ist die äquivalent zu $\sigma G(E/F)\sigma^{-1} = G(E/F)$.

(i) $\iff$ (ii) Nach Satz 1.1.11 folgt aus der Separabilität von E/K auch die Separabilität von F/K. Es dreht sich also darum zu zeigen, dass die Körpererweiterung F/K normal ist.

Sei C ein algebraischer Abschluss von E (und damit auch von K und F). Nach Satz 1.1.13 ist F/K normal genau dann, wenn für alle Körperhomomorphismen $\sigma : F/K \to C/K$ gilt $\sigma(F) = F$.

Andererseits gilt

$$\mathrm{Hom}_K(E, C) = \mathrm{Hom}_K(E, E) = G(E/K)\,;$$

die erste Gleichheit folgt, da E/K galoisch sein soll, also insbesondere normal ist aus Satz 1.1.13, die zweite Gleichheit aus Satz 1.1.12. Somit ist (ii) äquivalent zur Aussage, dass $\sigma F = F$ für alle $\sigma \in \mathrm{Hom}_K(E, C)$.

Außerdem ist wegen Lemma 1.1.7 die Restriktionsabbildung

$$\begin{array}{ccc} \mathrm{Hom}_K(E, C) & \to & \mathrm{Hom}_K(F, C) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

surjektiv. Somit folgt aus der Normalität von F/K, dass

$$\sigma F = F \quad \text{für alle} \quad \sigma \in \mathrm{Hom}_K(F, C)\,.$$

Umgekehrt folgt hieraus, dass F/K normal ist. □

Satz 1.2.9.
Sei E/K galoisch und F ein Zwischenkörper, $F \in \mathcal{Z}(E/K)$. Dann gilt: Ist F/K galoisch, so induziert die natürliche Projektion durch Einschränkung

$$\begin{array}{rccc} pr: & G(E/K) & \to & G(F/K) \\ & \sigma & \mapsto & \sigma_F \end{array}$$

einen Gruppenisomorphismus

$$G(E/K)/G(E/F) \cong G(F/K)$$

Beweis.
Wir zeigen zunächst, dass die Projektion surjektiv ist: sei C ein algebraischer Abschluss von E. Dehne $\sigma^{(1)} \in \mathrm{Hom}_K(F, C) = G(F/K)$ mit Hilfe von Lemma 1.1.7 aus zu einem Element $\sigma^{(2)} \in \mathrm{Hom}_K(C, C)$. Betrachte nun dessen Einschränkung auf E und erhalte ein Element $\sigma^{(3)} = \sigma^{(2)}_{|_E} \in \mathrm{Hom}_K(E, E) = G(E/K)$. Da Einschränkungen kommutieren, ist klar, dass $\sigma^{(3)}$ eingeschränkt auf F gleich $\sigma^{(1)}$ ist. Also ist pr surjektiv.

Nun können wir den Kern von pr berechnen,

$$\ker(pr) = \{\sigma \in G(E/K) \,|\, \sigma|_F = \mathrm{id}\} = G(E/F)$$

und den Homomorphiesatz für Gruppen anwenden, woraus die Behauptung folgt. □

Satz 1.2.10.
Sei E' die normale Hülle einer algebraischen Erweiterung E/K. Ist E/K separabel, so ist auch E'/K separabel und somit galoisch.

Beweis.
Sei C ein algebraischer Abschluss von E. Dann ist die normale Hülle gleich $E' = K(N)$ mit

$$N = \{\beta \in C | \beta \text{ ist Nullstelle eines } \min_K(\alpha),\ \alpha \in E\}\,.$$

Ist E/K separabel, dann ist jedes $\alpha \in E$ separabel über K, also auch alle $\beta \in N$. Nach I.4.2.10 ist der Körper E' separabel über K, da er von separablen Elementen erzeugt wird. □

Wir erinnern an die folgende Beziehung zwischen dem Körpergrad und der Ordnung der Galoisgruppe, die in I.4.3.6 bewiesen wurde: ist L/K eine endliche galoische Erweiterung, so ist

$$|Gal(L/K)| = [L : K] \tag{4}$$

Wir brauchen sie im Beweis des folgenden Satzes, den wir eigentlich schon im Kapitel über Separabilität hätten bringen können:

Satz 1.2.11 (Satz vom primitiven Element)**.**
Ist E/K eine endliche separable *Erweiterung, so ist E/K einfach: es gibt ein primitives Element $\alpha \in E$, so dass $E = K(\alpha)$.*

Beweis.

Wir führen den Beweis nur für Körper K mit unendlich vielen Elementen. Den Fall endlicher Körper behandeln wir später separat. Wegen Satz I.2.3.18 ist zu zeigen, dass es nur endlich viele Zwischenkörper gibt, $\mathcal{Z}(E/K)$ ist endlich. Sei E' die normale Hülle von E über K. Es reicht offensichtlich aus, zu zeigen, dass $\mathcal{Z}(E'/K)$ endlich ist.

Nun ist nach Satz 1.2.10 die Körpererweiterung E'/K ist galoisch und endlich. Wegen (4) ist dann aber die Galoisgruppe $G(E'/K)$ endlich. Damit hat sie aber auch nur endlich viele Untergruppen, $\mathcal{U}(G(E'/K))$ ist endlich. Da nach Bemerkung 1.2.7 die Abbildung

$$\mathcal{Z}(E'/K) \to \mathcal{U}(G(E'/K))$$

injektiv ist, ist auch $\mathcal{Z}(E'/K)$ endlich. □

Satz 1.2.12.
Sei E ein Körper, $G \subseteq$ Aut (E) eine endliche Gruppe und K der Fixkörper, $K = E^G$. Dann ist die Körpererweiterung E/K endlich und galoisch mit Galoisgruppe

$$G = G(E/K)\,.$$

Beweis.

Die Körpererweiterung E/K ist algebraisch nach Satz 1.2.2 und galoisch nach Bemerkung 1.2.4 (ii). Ferner folgt aus Satz 1.2.2:

$$[K(\alpha) : K] = \text{grad } \min_K \alpha \leq |G|$$

für alle $\alpha \in E$. Sei $\alpha \in E$ mit maximalem Körpergrad $[K(\alpha) : K]$, und sei $\beta \in E$ beliebig. Wegen des Satzes vom primitiven Element 1.2.11 gibt es ein Element $\gamma \in E$, so dass

$$K(\alpha, \beta) = K(\gamma)\,.$$

Andererseits gilt auch $[K(\gamma) : K] \leq [K(\alpha) : K]$, da α den Körpergrad maximieren soll. Also gilt $K(\alpha) = K(\gamma)$, d.h. $\beta \in K(\alpha)$ für alle $\beta \in E$. Daher haben wir $E = K(\alpha)$, d.h. α ist ein primitives Element. Also ist die Körpererweiterung E/K endlich mit Körpergrad

$$[E : K] \leq |G|\,.$$

Da $G \subseteq G(E/K)$ und $[E : K] = |G(E/K)|$ gilt, da E/K galoisch ist, folgen insgesamt die Inklusionen

$$|G| \leq |G(E/K)| = [E : K] \leq |G|\,.$$

Es folgt somit die Gleichheit $G = G(E/K)$. □

Theorem 1.2.13 (Hauptsatz der Galoistheorie für endliche galoische Erweiterungen)**.**
Sei E/K eine endliche galoische Körpererweiterung. Dann ist die Abbildung von Zwischenkörpern auf Untergruppen der Galoisgruppe

$$\begin{array}{rcl} \mathcal{Z}(E/K) & \to & \mathcal{U}(G(E/K)) \\ F & \mapsto & G(E/F) \end{array}$$

eine Bijektion. Für jeden Zwischenkörper F gilt

$$[E : F] = |G(E/F)|$$

und für je zwei Zwischenkörper F_1 und $F_2 \in \mathcal{Z}(E/K)$ gilt

$$F_1 \subseteq F_2 \iff G(E/F_2) \subseteq G(E/F_1)$$

Die Umkehrabbildung ist

$$\begin{array}{rcl} \mathcal{U}(E/K) & \to & \mathcal{Z}(E/K) \\ U & \mapsto & E^U\,. \end{array}$$

Wir erinnern auch noch an Satz 1.2.8:
$F \in \mathcal{Z}(E/K)$ ist genau dann galoisch über K, wenn die Galoisgruppe $G(E/F)$ eine normale Untergruppe von $G(E/K)$ ist. Dann gilt

$$G(F/K) \cong G(E/K)/G(E/F)\,.$$

Beweis.

Da die Injektivität der Abbildung schon gezeigt wurde, bleibt die Surjektivität zu zeigen. Dazu geben wir die Umkehrabbildung an. Wir bemerken erstens: sei $F \in \mathcal{Z}(E/K)$. Dann ist nach Satz 1.2.7 die Körpererweiterung E/F galoisch, also gilt

$$E^{G(E/F)} = F\,.$$

Zum zweiten überlegen wir uns folgendes: da die Körpererweiterung E/K endlich ist, ist $G(E/K)$ endlich und somit jede Untergruppe $U \leq G(E/K)$ endlich. Nach Satz 1.2.12 gilt für jede solche Untergruppe

$$U = G(E/E^U)$$

Aus den beiden Bemerkungen folgt die Bijektivität:

$$\begin{array}{ccccccc} \mathcal{Z}(E/K) & \to & \mathcal{U}(E/K) & \to & \mathcal{Z}(E/K) & \to & \mathcal{U}(E/K) \\ F & \mapsto & G(E/F) & \mapsto & E^{G(E/F)} = F & & \\ & & U & \mapsto & E^U & \mapsto & G(E/E^U) = U \end{array}$$

Ferner gilt:

$$G(E/F_2) \leq G(E/F_1) \iff F_1 = E^{G(E/F_1)} \subseteq F_2 = E^{G(E/F_2)}\,.$$

Zusammen mit den vorstehenden Sätzen ist damit der Hauptsatz für endliche Erweiterungen unendlicher Körper vollständig gezeigt. □

Beispiel 1.2.14.
Sei E Zerfällungskörper des Polynoms $f(X) = X^4 - 2$ über $\mathbb{Q}$. Dann ist

$$E = \mathbb{Q}\Big(\sqrt[4]{2}, \mathrm{i}\Big)\,,$$

denn sei $a := \sqrt[4]{2}$, dann sind $a, \mathrm{i}a, -a, -\mathrm{i}a$ die vier Nullstellen von f. Das Polynom f ist normiert und nach Eisenstein irreduzibel, also Minimalpolynom von a. Daher gilt:

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 4 = 8\,.$$

Aus der Gradformel folgt für $E = \mathbb{Q}(a, \mathrm{i})$

$$[\mathbb{Q}(a, \mathrm{i}) : \mathbb{Q}(\mathrm{i})] = 4\,,$$

also ist f auch das Minimalpolynom von a über $\mathbb{Q}(\mathrm{i})$.

Sei $\sigma \in G(E/\mathbb{Q})$ die Fortsetzung von $id_{\mathbb{Q}(i)}$ auf E durch

$$\sigma(\mathrm{i}) = \mathrm{i} \qquad \sigma(a) = \mathrm{i}a\,.$$

Offensichtlich gilt $\sigma^4 = \mathrm{id}$. Sei ferner $\tau \in G(E/\mathbb{Q})$ die Fortsetzung von $id_{\mathbb{Q}(a)}$ auf E durch

$$\tau(a) = a \qquad\qquad \tau(\mathrm{i}) = -\mathrm{i}\,.$$

Es ist klar, dass $\tau \notin \{1, \sigma, \sigma^2, \sigma^3\}$.

Da $|G(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8$, haben wir die vollständige Galoisgruppe gefunden:

$$G(E/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

Da außerdem gilt

$$\begin{array}{rclcl} \tau\sigma a & = & \tau(\mathrm{i}a) & = & -\mathrm{i}a \\ \tau\sigma\mathrm{i} & = & \tau\mathrm{i} & = & -\mathrm{i} \end{array} \qquad \begin{array}{rclcl} \sigma^3\tau(a) & = & \sigma^3(a) & = & -\mathrm{i}a \\ \sigma^3\tau(\mathrm{i}) & = & \sigma^3(-\mathrm{i}) & = & -\mathrm{i} \end{array}\,,$$

finden wir die folgende Relation:

$$\tau\sigma = \sigma^3\tau = \sigma^{-1}\tau\,.$$

Die Galoisgruppe $G(E/\mathbb{Q})$ ist also isomorph zur Diedergruppe D_4.

Wir zählen die Untergruppen von D_4 auf:

$$\begin{aligned} U_0 = \{1\} \qquad & U_1 = \{1, \sigma^2\}\ U_2 = \{1, \tau\} \\ & U_3 = \{1, \sigma\tau\}\ U_4 = \{1, \sigma^2\tau\}\ U_5 = \{1, \sigma^3\tau\} \\ & U_6 = \langle\sigma\rangle \\ & U_7 = \{1, \sigma^2, \tau, \sigma^2\tau\} \\ & U_8 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \\ & U_9 = D_4\,. \end{aligned}$$

Die Untergruppe U_0 ist die triviale Gruppe, die Untergruppen U_1 bis U_5 sind zyklisch der Ordnung zwei, U_6 ist zyklisch der Ordnung vier, und U_7 und U_8 sind isomorph zur Kleinschen Vierergruppe. Die Inklusionsbeziehungen von Untergruppen sind nun offensichtlich. Sie entsprechen im Unterkörperverband

$$U_i \leq U_j \iff F_i \supseteq F_j\,.$$

Wir wollen noch erklären, wie man die Zwischenkörper bestimmt: Sei für eine Untergruppe $U \leq G(E/K)$ die Spur über U definiert durch

$$\mathrm{Sp}_U(x) = \sum_{g \in U} gx \quad \textit{für } x \in E\,.$$

Die Spur ist linear nimmt ihre Werte in E^U an, denn es gilt für alle $h \in U$

$$h(\mathrm{Sp}_U(x)) = \sum_{g \in U} hgx = \mathrm{Sp}_U(x)\,.$$

Die Abbildung

$$\mathrm{Sp}_U : E \to E^U$$

ist in Charakteristik 0 surjektiv, denn sei $y \in E^U$, so ist

$$\mathrm{Sp}\left(\frac{1}{|U|}y\right) = y\,.$$

Wir können also die Unterkörper durch das Ausrechnen von Spuren bestimmen. Wir zeigen dies am Beispiel der Untergruppe $U_5 = \{1, \sigma^3\tau\}$:

$$\begin{aligned}
\mathrm{Sp}_{U_5}(1) &= 2 \\
\mathrm{Sp}_{U_5}(\mathrm{i}) &= \mathrm{i} + \sigma^3\tau(\mathrm{i}) = \mathrm{i} - \mathrm{i} = 0 \\
\mathrm{Sp}_{U_5}(a) &= a + \sigma^3\tau(a) = a - \mathrm{i}a = \sqrt[4]{2}(1 - \mathrm{i}) \\
\mathrm{Sp}_{U_5}(\mathrm{i}a) &= \mathrm{i}a + \sigma^3\tau(\mathrm{i})\sigma^3\tau(a) = \mathrm{i}a + (-\mathrm{i})(-\mathrm{i}a) \\
&= -a(1 - \mathrm{i})
\end{aligned}$$

Ähnlich rechnet man weiter für die anderen Elemente der K-Basis $\{1, \mathrm{i}, a, a\mathrm{i}, a^2, a^2\mathrm{i}, a^3, a^3\mathrm{i}\}$. Damit folgt $F_5 = \mathbb{Q}\left(\sqrt[4]{2}(1 - \mathrm{i})\right)$.

Aus dem Satz vom primitiven Element 1.2.11 folgt sofort

Satz 1.2.15.

(i) Ist E/K endliche, galoische Erweiterung, so ist E Zerfällungskörper eines separablen irreduziblen Polynoms $f \in K[X]$.

(ii) Umgekehrt gilt: der Zerfällungskörper eines separablen Polynoms $f \in K[X]$ ist eine endliche galoische Erweiterung von K, siehe Bemerkung 1.2.6.

Definition 1.2.16.

Sei $f \in K[X]$ ein separables Polynom. (Es würde ausreichen, zu fordern, dass alle Primteiler von f separabel sind.) Sei E der Zerfällungskörper von f über K. Die Galoisgruppe des Polynoms f über K ist per Definition

$$G(f, K) := G(E/K)\,.$$

Beispiel 1.2.17.
Wir wollen $G(X^3-2,\mathbb{Q})$ ausrechnen. Seien $\alpha_1,\alpha_2,\alpha_3$ die Nullstellen von X^3-2 in $\mathbb{C}$. Dann ist

$$E=\mathbb{Q}\left(\sqrt[3]{2},\zeta_3\right)$$

der Zerfällungskörper von f über $\mathbb{Q}$. Wir erhalten eine Injektion

$$\begin{aligned} G(E/\mathbb{Q}) &\hookrightarrow S_3 \\ \sigma &\mapsto \sigma(\alpha_1,\alpha_2,\alpha_3)=(\sigma\alpha_1,\sigma\alpha_2,\sigma\alpha_3) \end{aligned}$$

da σ durch seine Wirkung auf den Nullstellen α_1,α_2 und α_3 eindeutig bestimmt ist. Ferner gilt $|S_3|=3!=6$ und

$$|G(E/\mathbb{Q})|=[E:\mathbb{Q}]=[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}][E:\mathbb{Q}\left(\sqrt[3]{2}\right)]=3\cdot 2=6$$

Also ist die Injektion auch surjektiv und die Galoisgruppe ist $G(X^3-2,\mathbb{Q})\cong S_3$.

Bemerkung 1.2.18.
Ist $f\in K[X]$ ein separables Polynom vom Grade n, so hat man allgemein eine Injektion

$$G(f,K)\hookrightarrow S_n$$

d.h. die Galoisgruppe $G(f,K)$ ist isomorph zu einer Untergruppe der Permutationsgruppe S_n. Es folgt $G(f,K)\leq (\text{grad } f)!$.

Die Injektion muss nicht surjektiv sein: in Beispiel 1.2.14 war für das Polynom $f=X^4-2$ die Galoisgruppe $G(f/\mathbb{Q})\cong D_4$; aber es gilt $|D_4|=8$, während $|S_4|=24$.

Satz 1.2.19.
Sei $f\in K[X]$ separabel *über K mit Galoisgruppe $G=G(f,K)$. Sei N die Menge der Nullstellen von f in einem Zerfällungskörper E über K. Dann ist äquivalent*

(i) f ist irreduzibel.

(ii) G operiert transitiv auf N, d.h. zu je zwei $\alpha,\beta\in N$ gibt es $\sigma\in G$ mit $\sigma(\alpha)=\beta$.

Beweis.
(i)⇒(ii) Seien $\alpha,\beta\in N$ und f irreduzibel. Nach Satz 1.1.9 ist β konjugiert zu α, d.h. ist C ein algebraischer Abschluss von E, so gibt es $\tau\in \mathrm{Hom}_K(C,C)$ mit

$$\tau(\alpha)=\beta\,.$$

Da E/K normal ist, ist nach Satz 1.2.12 $\tau|_E$ in der Galoisgruppe $G(E/K)=G$.

(ii)⇒(i) Sei $\alpha \in N$ und $g = \min_K(\alpha)$. Dann teilt g das Polynom f. Wegen der Transitivität der Wirkung gibt es zu $\beta \in N$ ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Es folgt

$$g(\beta) = g(\sigma\alpha) = \sigma g(\alpha) = 0\,,$$

also ist jede Nullstelle von f auch Nullstelle von g. Da f als separabel vorausgesetzt war, folgt auch $f|g$. Also sind die beiden Polynome f und g assoziiert. g ist als Minimalpolynom irreduzibel, also ist auch f irreduzibel. □

1.3 Endliche Körper und Einheitswurzeln

1.3.1 Endliche Körper

Wir wollen jetzt endliche Körper untersuchen. Sei K im folgenden ein endlicher Körper und $k \subseteq K$ sein Primkörper. Dann ist $k \cong \mathbb{F}_p$ für eine Primzahl p, wobei p die Charakteristik von K ist, $\operatorname{char} K = p$. Da K ein k-Vektorraum ist, gilt notwendigerweise $|K| = p^d$ mit $d = [K : k]$ und $|K^\times| = p^d - 1$.

Satz 1.3.1.
Für jede Primzahl p und jede Zahl $d \in \mathbb{N}^\times$ existiert ein endlicher Körper K mit p^d Elementen, den wir mit $\mathbb{F}_{p^d}$ bezeichnen. Dieser ist eindeutig bestimmt als Teilkörper eines algebraischen Abschlusses $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$: er ist Zerfällungskörper des separablen Polynoms

$$f(X) = X^{p^d} - X$$

über $\mathbb{F}_p$ und besteht aus den Nullstellen dieses Polynoms.

Jeder endliche Körper K ist isomorph zu genau einem Körper $\mathbb{F}_{p^d}$. Insbesondere ist jeder endliche Körper eine galoische Erweiterung seines Primkörpers, $K/\mathbb{F}_p$ ist galoisch.

Beweis.

Sei E der Zerfällungskörper des Polynoms $f(X)$ über $\mathbb{F}_p$ in $\overline{\mathbb{F}}_p$. Wir behaupten, dass

$$E = \{\alpha \in \overline{\mathbb{F}}_p \mid f(\alpha) = 0\}$$

Dazu reicht es aus, nachzurechnen, dass $\{\alpha \in \overline{\mathbb{F}_p} \,|\, f(\alpha) = 0\}$ ein Körper ist und somit gleich E sein muss.

Seien $\alpha, \beta \in E$, $f(\alpha) = f(\beta) = 0$. In der Tat gilt:

- $(\alpha + \beta)^{p^d} - (\alpha + \beta) = \alpha^{p^d} - \alpha + \beta^{p^d} - \beta = 0$

- $(\alpha\beta)^{p^d} - \alpha\beta = \alpha^{p^d}\beta^{p^d} - \alpha\beta = \alpha\beta - \alpha\beta = 0$
- Ferner sind $0, 1$ Nullstellen von f.
- Ist $\beta \neq 0$ und $f(\beta) = 0$, so

$$(\beta^{-1})^{p^d} - \beta^{-1} = (\beta^{p^d})^{-1} - \beta^{-1} = \beta^{-1} - \beta^{-1} = 0$$

- $(-\beta)^{p^d}(-\beta) = (-)^{p^d}\beta + \beta = \begin{cases} -\beta + \beta &= 0 \quad \text{für} \quad p \neq 2 \\ \beta + \beta &= 0 \quad \text{für} \quad p = 2 \end{cases}$

Wegen $f'(X) = p^d X^{p^d-1} - 1 = -1 \neq 0$ ist das Polynom f nach I. 4.2.7 separabel. Alle Nullstellen sind also verschieden und wir sehen

$$|E| = \text{ grad } f = p^d\,.$$

Sei umgekehrt K ein endlicher Körper mit p^d Elementen. Dann sind alle $\alpha \in K^\times$ Elemente der endlichen multiplikativen Gruppe $K^\times$ mit $p^d - 1$ Elementen. Nach dem kleinen Fermatschen Satz I. 1.6.3 gilt daher $\alpha^{p^d-1} = 1$ für $\alpha \neq 0$, also $\alpha^{p^d} = \alpha$ für alle α. Also lässt K sich einbetten in die Menge

$$E = \{\alpha \in \overline{\mathbb{F}_p} \,|\, \alpha^{p^d} = \alpha\}$$

und somit $K \cong E$, da die Mächtigkeiten beider Mengen gleich sind. □

Korollar 1.3.2.
Sei q eine Primpotenz, $q = p^d$ mit $d \geq 1$. In einem algebraischen Abschluss $\overline{\mathbb{F}_p}$ existiert genau ein Erweiterungskörper von $\mathbb{F}_q$ von grad n für $n \geq 1$.

Beweis.
Der Zerfällungskörper von $X^{q^n} - X$ über $\mathbb{F}_p$ ist $\mathbb{F}_{p^{d\cdot n}}$ und hat den Grad dn über $\mathbb{F}_p$. Damit gilt

$$[\mathbb{F}_{p^{dn}} : \mathbb{F}_{p^d}] = \frac{[\mathbb{F}_{p^{dn}} : \mathbb{F}_p]}{[\mathbb{F}_{p^d} : \mathbb{F}_p]} = \frac{dn}{d} = n\,.$$

Umgekehrt hat jeder Erweiterungskörper von $\mathbb{F}_q$ vom Grad n genau q^n Elemente und ist somit nach Satz 1.3.1 isomorph zu $\mathbb{F}_{q^n}$.

Satz 1.3.3.

(i) Sei K ein beliebiger Körper und G eine endliche *Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist G zyklisch.*

(ii) Insbesondere ist die multiplikative Gruppe $K^\times$ eines endlichen Körpers K zyklisch, da sie endlich ist. Ein erzeugendes Element von $K^\times$ heißt Primitivwurzel.

Bevor wir den Satz beweisen, folgende

Bemerkung 1.3.4.
Sei ζ eine Primitivwurzel eines endlichen Körpers K und k der Primkörper von K. Dann gilt offensichtlich $K = k(\zeta)$. Somit ist K/k eine einfache Körpererweiterung.

Ist K'/K endliche und daher notwendigerweise separable Erweiterung des endlichen Körpers K, so ist

$$K' = k(\zeta') = K(\zeta')$$

mit ζ' einer Primitivwurzel von K'. Also ist auch die Körpererweiterung K'/K einfach und der Satz 1.2.11 vom primitiven Element vollständig gezeigt, ebenso wie Satz I.2.3.18.

Der Beweis von Satz 1.3.3 stützt sich auf das folgende Lemma:

Lemma 1.3.5.
Sei G eine endliche Gruppe der Ordnung n. Gilt für alle Teiler d von n

$$|\{x \in G | x^d = 1\}| \leq d\,, \tag{5}$$

so ist G zyklisch.

Beweis. von Satz 1.3.3.

Sei d ein Teiler der Gruppenordnung $|G|$. Dann gilt sicher

$$|\{\alpha \in K^\times | \alpha^d = 1\}| \leq d\,,$$

da das Polynom $X^d - 1$ höchstens d Nullstellen in K besitzen kann. Erst recht gilt für eine Untergruppe $G \leq K^\times$

$$|\{\alpha \in G | \alpha^d = 1\}| \leq d\,.$$

Nach Lemma 1.3.5 ist somit G zyklisch. Aussage (ii) in Satz 1.3.3 folgt aus Teil (i) mit $G = K^\times$.

Beweis. von Lemma 1.3.5.

Für einen Teiler d der Gruppenordnung $|G|$ sei $\psi_G(d)$ die Zahl der Elemente von G der Ordnung d. Offenbar gilt, da jedes Element eine Ordnung hat

$$\sum_{d|n} \psi_G(d) = |G|\,. \tag{6}$$

Wir behaupten, dass außerdem gilt

$$\psi_G(d) \leq \varphi(d) \tag{7}$$

mit der Eulerschen φ-Funktion. Für $\psi_G(d) = 0$ ist dies klar, da stets $\varphi(d) \geq 1$.

Sei also $\psi_G(d) \geq 1$ und a ein Element von G der Ordnung d. Betrachte die von a zyklisch erzeugte Untergruppe $H = \langle a \rangle$. Für alle d Elemente aus H gilt $x^d = 1$. Wegen der Annahme (5) liegt jedes Element der Ordnung d schon in der zyklischen Untergruppe H. Daher erhalten wir

$$\psi_G(d) = \psi_H(d) = \varphi(d)\,.$$

Insbesondere gilt für die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$

$$\psi_{\mathbb{Z}/n\mathbb{Z}}(d) = \varphi(d)\,,$$

da in $\mathbb{Z}/n\mathbb{Z}$ ein Element der Ordnung d existiert. Die Anwendung von (6) und (7) liefert nun die Ungleichungen

$$n = \sum_{d||G|} \psi_G(d) \leq \sum_{d||G|} \varphi(d) = \sum_{d||G|} \psi_{\mathbb{Z}/n\mathbb{Z}}(d) = |\mathbb{Z}/n\mathbb{Z}| = n\,.$$

Somit gilt die Gleichheit $\psi_G(d) = \varphi(d)$ für alle Teiler d von n. Insbesondere ist $\psi_G(|G|) = \varphi(|G|) \geq 1$, also besitzt G ein Element der Ordnung $|G|$, das $|G|$ zyklisch erzeugt. □

Bemerkung 1.3.6.
Für die Eulersche φ-Funktion gilt

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\{k \in \mathbb{N} | 1 \leq k \leq n, (k,n) = 1\}|$$

$$= \#\ \textit{Erzeugende Elemente von}\ \mathbb{Z}/n\,,$$

was wir in den Übungen sehen werden. Die φ-Funktion ist nach I.1.6.15 für teilerfremde ganze Zahlen m, n multiplikativ,

$$\varphi(mn) = \varphi(m)\varphi(n)\,.$$

Ferner gilt $\varphi(p^m) = p^{m-1}(p-1)$ für p prim.

Beweis.

Wir beweisen die letzte Aussage durch Induktion nach m. Für $m = 1$ gilt

$$|(\mathbb{Z}/p)^\times| = |\mathbb{F}_p^\times| = p - 1\,.$$

Für den Induktionsschritt betrachte wir die kanonische Surjektion

$$\begin{array}{rcl} \mathbb{Z}/p^{m+1} & \twoheadrightarrow & \mathbb{Z}/p^m \\ x \bmod p^{m+1} & \mapsto & x \bmod p^m \end{array}$$

Sie induziert einen Gruppenhomomorphismus

$$\lambda : \qquad (\mathbb{Z}/p^{m+1})^\times \to (\mathbb{Z}/p^m)^\times$$

der auch surjektiv ist. Denn aus $x \bmod p^m \in (\mathbb{Z}/p^m)^\times$ folgt, dass $(x, p^m) = 1$, und da p prim ist, folgt daraus auch, dass $(x, p^{m+1}) = 1$ gilt. Also ist $x \bmod p^{m+1} \in (\mathbb{Z}/p^{m+1})^\times$ Der Kern der Abbildung λ ist

$$\begin{array}{rcl} \ker(\lambda) & = & \{x \bmod p^{m+1} | x \equiv 1 \bmod p^m\} \\ & = & \{x = 1 + p^m y \bmod p^{m+1} | y \in \mathbb{N}\}\,. \end{array}$$

Er hat offensichtlich genau p Elemente. Aus dem Homomorphiesatz für Gruppen folgt

$$|(\mathbb{Z}/p^{m+1})^\times| = p\ |(\mathbb{Z}/p^m)^\times|\,.$$

□

Nachdem wir so einen guten Überblick über die Klassifikation der endlichen Körper und ihre Einheitengruppen bekommen haben, wenden wir uns nun ihren Galoisgruppen zu.

Satz 1.3.7.
Sei $q = p^d$ eine Primzahlpotenz. Die Gruppe der Automorphismen des endlichen Körpers $\mathbb{F}_q$ mit q Elementen ist zyklisch von der Ordnung d und wird erzeugt vom Frobeniusautomorphismus

$$\begin{array}{rccl} \sigma_p : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & \alpha & \mapsto & \alpha^p \end{array}$$

Beweis.

- Wegen

  $$\sigma_p^d(x) = x^{p^d} = x = \mathrm{id}\ (x) \quad \text{für alle} \quad x \in \mathbb{F}_q\,,$$

  teilt die Ordnung n von σ_p die Zahl d. Andererseits folgt aus $\sigma_p^k = 1$ die Gleichung $x^{p^k} = x$ für alle $x \in \mathbb{F}_q$, also

  $$x^{p^n} - x = 0$$

  für alle $x \in \mathbb{F}_q$. Daraus folgt die Abschätzung $|\mathbb{F}_q| = p^d \leq p^n$, also ist d kleiner gleich der Ordnung n von σ_p. Insgesamt folgt ord $\sigma_p = d$.

- Sei nun $\varphi \in \mathrm{Aut}\,(\mathbb{F}_q)$ ein beliebiger Automorphismus. Da

$$\varphi_{|\mathbb{F}_p} = \mathrm{id}$$

auf dem Primkörper $\mathbb{F}_p$, folgt $\varphi \in G(\mathbb{F}_q/\mathbb{F}_p)$. Aus der Galoistheorie folgt

$$|G(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = d$$

Damit erzeugt σ_p die Automorphismengruppe von $\mathbb{F}_q$ zyklisch. □

Korollar 1.3.8.
Seien $n, m \geq 1$ ganze Zahlen. Dann gilt

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n|m$$

Ist dies der Fall, so ist die Körpererweiterung $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ galoisch und die Galoisgruppe $G(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$ ist zyklisch erzeugt durch die Abbildung

$$\begin{array}{rccc} \sigma_{p^n}: & \mathbb{F}_{p^m} & \to & \mathbb{F}_{p^m} \\ & x & \mapsto & x^{p^n} \end{array}$$

Beweis.

Sei $d := [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$, dann gilt nach Satz 1.3.2 $nd = m$. Die umgekehrte Richtung ist nach Satz 1.3.2 klar.

Nach Satz 1.3.1 ist die Körpererweiterung $\mathbb{F}_{p^m}/\mathbb{F}_p$ separabel und normal; daher gilt dies auch für die Körpererweiterung $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$. Nach Satz 1.3.7 ist $G(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$ Untergruppe der zyklischen Gruppe $\langle\sigma_p\rangle$, also zyklisch und von der Ordnung $\frac{m}{n}$. Damit wird sie durch den Automorphismus $(\sigma_p)^n$ erzeugt.

1.3.2 Einheitswurzeln

Wir wenden uns nun dem zweiten Thema dieses Kapitels zu, den Einheitswurzeln.

Definition 1.3.9.
Sei K ein Körper. Dann bezeichnet $W(K) \subset K^\times$ die Gruppe aller Elemente endlicher Ordnung in $K^\times$ und

$$W_n(K) = \{\zeta \in K \,|\, \zeta^n = 1\}$$

die Gruppe aller Elemente aus $K^\times$, deren Ordnung n teilt. Die Elemente aus $W_n(K)$ heißen n-te Einheitswurzeln von K. Ein Element $\zeta \in W_n(K)$ heißt primitive Einheitwurzel, falls $\mathrm{ord}\,\zeta = n$.

Bemerkung 1.3.10.

(i) $W_n(K)$ *ist eine endliche zyklische Gruppe, deren Ordnung* n *teilt.*

(ii) Ist $p = char\ (K) > 1$*, so gilt*

$$W_{np}(K) = W_n(K)\,.$$

In einem Körper der Charakteristik p *kann es also keine primitiven* n*-ten Einheitswurzeln geben, wenn* n *durch die Charakteristik des Körpers geteilt wird.*

Beweis.

(i) Die Gruppe $W_n(K)$ ist endlich, da alle ihre Elemente Nullstellen des Polynoms $X^n - 1$ sind. Als endliche Untergruppe von der Einheitengruppe $K^\times$ ist $W_n(K)$ nach Satz 1.3.3 zyklisch. Sei ζ ein Erzeuger von $W_n(K)$; seine Ordnung ord $(\zeta) = |W_n(K)|$ teilt dann n.

(ii) Ist $p = \text{char } K > 1$, so folgt aus

$$\zeta^{np} = (\zeta^n)^p = 1$$

schon $\zeta^n = 1$, denn der Frobeniusautomorphismus σ_p ist als Körperautomorphismus injektiv. Also gilt die Inklusion $W_{np}(K) \subseteq W_n(K)$, die andere Inklusion ist ohnehin trivial.

Bemerkung 1.3.11.

(i) Die Gruppe der komplexen Einheitswurzeln $W_n(\mathbb{C}) = \{e^{2\pi ik/n} \mid k = 0, 1, \ldots n-1\}$ *hat* n *Elemente.*

(ii) Sei C *ein algebraisch abgeschlossener Körper und* $n \in \mathbb{N}$*. Ist char* $K = p > 0$*, so sei* $(n, p) = 1$*. Dann gilt*

$$|W_n(C)| = n\,.$$

Da die Gruppe $W_n(C)$ *zyklisch ist, gibt es insbesondere eine primitive* n*-te Einheitswurzel in* C*.*

Beweis.

(ii) Das Polynom $f(X) = X^n - 1$ ist in $C[X]$ separabel, da die Ableitung $f'(X) = nX^{n-1}$ ungleich Null ist. Also hat es keine mehrfachen Nullstellen.

Satz 1.3.12. *und* **Definition**
Sei K ein Körper, $n \in \mathbb{N}$. Der Zerfällungskörper E des Polynoms $X^n - 1$ über K heißt Körper der n-ten Einheitswurzeln über K. Es gilt:

(i) $E = K(\zeta)$, wobei ζ eine primitive m-te Einheitswurzel ist mit

$$\begin{array}{rcll} m & = & \frac{n}{p^{wp(n)}} & , \ falls \ \ p = char\,(K) > 0 \\ m & = & n & , \ falls \ \ char\,(K) = 0 \end{array}$$

(ii) E/K ist galoisch und es gibt eine Injektion

$$G(E/K) \hookrightarrow (\mathbb{Z}/m)^\times$$

Insbesondere ist die Galoisgruppe $G(E/K)$ abelsch.

Beweis.

Die Behauptung in (i) ist nach Bemerkung 1.3.10 offensichtlich. Wegen Bemerkung 1.3.10 (ii) können wir annehmen, dass $(n, p) = 1$ gilt, mit $p = \text{char } K > 0$. Daraus folgt, dass das Polynom $X^n - 1$ separabel über K ist und die Körpererweiterung E/K daher galoisch ist.

Sei $\zeta_n \in E$ primitive n-te Einheitswurzel, ord $(\zeta_n) = n$. Für jedes Element $\sigma \in G(E/K)$ hat $\sigma(\zeta_n)$ ebenfalls die Ordnung n, also gilt $\sigma\zeta_n = \zeta_n^k$ mit $(k, n) = 1$, denn nur dann ist ζ_n^k wieder primitiv. Um k zu normieren, schreiben wir vor, dass $1 \leq k \leq n$ gilt. Damit ist k eindeutig durch σ bestimmt.

Sei $\zeta \in W_n(E)$, so ist $\zeta = \zeta_n^j$ für ein geeignetes $j \in \mathbb{Z}$. Es gilt dann

$$\sigma(\zeta) = \sigma(\zeta_n^j) = \sigma(\zeta_n)^j = (\zeta_n^k)^j = \zeta^k$$

Daher bekommen wir eine Injektion

$$\begin{array}{rcl} G(E/K) & \hookrightarrow & (\mathbb{Z}/n)^\times \\ \sigma & \mapsto & k \text{ mit } \sigma\zeta = \zeta^k\,. \end{array}$$

Die ist sogar ein Gruppenhomomorphismus. Er ist injektiv, denn wegen $E = K(\zeta_n)$ ist σ schon durch die Angabe des Bildes $\sigma(\zeta_n)$ festgelegt. □

Man beachte, dass im Falle $K = \mathbb{R}$ oder $K = \mathbb{C}$ und $n > 2$

$$\mathbb{R}(\zeta_n) = \mathbb{C} = \mathbb{C}(\zeta_n)$$

ist, also für die Galoisgruppe gilt $|G(K(\zeta_n)/K)| = 2$ oder 1. Die obige Abbildung ist in diesem Fall also sicher nicht surjektiv. Anders verhält sich dies für die rationalen Zahlen:

Satz 1.3.13 (Gauß)**.**
Sei $E = \mathbb{Q}(\zeta_n)$ mit ζ_n einer primitiven n-ten Einheitswurzel. Dann ist die Injektion in Satz 1.3.12 (ii) eine Isomorphie,

$$G(E/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times .$$

Insbesondere gilt

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

Beweis.

Zu zeigen ist, dass es zu jedem $k \in \mathbb{Z}$, das koprim zu n ist, $(k, n) = 1$, ein $\sigma \in G(E/\mathbb{Q})$ gibt, so dass $\sigma\zeta = \zeta^k$ gilt.

- Sei $f = \min_{\mathbb{Q}}(\zeta)$ das Minimalpolynom. Es reicht aus, zu zeigen, dass ζ^k Nullstelle von f ist. Denn f ist als Minimalpoynom irreduzibel, und in char $\mathbb{Q} = 0$ sicher separabel, so dass nach Satz 1.2.19 die Galoisgruppe transitiv auf den Nullstellen von f operiert.
- Wir reduzieren nun die Behauptung auf den Fall, dass $k = p$ eine Primzahl ist, die n nicht teilt.

  Denn ist $k = p_1^{r_1} \dots p_s^{r_s}$ ein Produkt solcher Primzahlen, so finden wir zunächst Automorphismen σ_i von $E/\mathbb{Q}$, so dass

  $$\sigma_i(\zeta) = \zeta^{p_i} ,$$

  für die dann natürlich auch

  $$\sigma_i^{r_i}(\zeta) = \zeta^{p_i^{r_i}}$$

  gilt. Wir rechnen dann nach, dass

  $$\sigma_1^{r_1} \dots \sigma_s^{r_s}(\zeta) = \zeta^{p_1^{s_1} \dots p_s^{r_s}} = \zeta^k$$

  gilt, also haben wir den gewünschten Automorphismus gefunden.
- Da ζ Nullstelle von f und von $X^n - 1 \in \mathbb{Q}[X]$ ist, finden wir in $\mathbb{Q}[X]$ eine Zerlegung

  $$f(X)g(X) = X^n - 1$$

  mit normierten Polynomen $f, g \in \mathbb{Q}[X]$. Nach dem Lemma von Gauß (I.3.3.10) sind diese Polynome sogar in $\mathbb{Z}[X]$.

- Sei also p eine Primzahl, die n nicht teilt. Widerspruchsbeweis: Angenommen, es würde $f(\zeta^p) \neq 0$ gelten. Dann gilt $g(\zeta^p) = 0$, also ist ζ Nullstelle des Polynoms $g(X^p) \in \mathbb{Z}[X]$. Dieses wird daher vom Minimalpolynom f von ζ geteilt und wir finden $h \in \mathbb{Q}[X]$, so dass gilt
$$f(X)h(X) = g(X^p)\,. \tag{8}$$
Wiederum nach dem Lemma von Gauß liegt das Polynom $h \in \mathbb{Z}[X]$.
Die Idee ist nun, modulo der Primzahl p zurechnen und die folgende Surjektion von Polynomringen auszunutzen:
$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X]\,.$$
Dies können wir deshalb, weil alle Polynome ganzzahlige Koeffizienten haben. Da für
$$\bar{g} = \sum_i \alpha_i X^i \in \mathbb{F}_p[X]$$
gilt
$$(\bar{g}(X))^p = \sum_i \alpha_i^p X^{i_p} = \sum_i \alpha_i X^{i_p} = \bar{g}(X^p)\,.$$
Aus Gleichung (8) folgt daher
$$\bar{f}(X)\bar{h}(X) = \overline{g(X^p)} = (\bar{g}(X))^p\,.$$
Aus ihr folgt, dass die Polynome $\bar{f}$ und $\bar{g}$ eine gemeinsame Nullstelle im algebraischen Abschluss $\overline{\mathbb{F}}_p$ des Körpers $\mathbb{F}_p$ haben.
Dann hat aber das Polynom
$$\bar{f}\bar{g} = X^n - 1 \in \mathbb{F}_p[X]$$
eine doppelte Nullstelle. Aber das Polynom $X^n - 1$ ist auch im Polynomring $\mathbb{F}_p[X]$ separabel: seine Ableitung $nX^{n-1} \neq 0$, da $(n, p) = 1$, so dass die Annahme $f(\zeta^p) \neq 0$ zum Widerspruch geführt ist. □

Sei C eine algebraisch abgeschlossene Erweiterung von $\mathbb{Q}$, etwa $\mathbb{C}$ oder der algebraische Abschluß $\overline{\mathbb{Q}}$. Setze $W_n = W_n(C)$. Dann gilt die Zerlegung
$$X^n - 1 = \prod_{\zeta \in W_n} (X - \zeta)\,. \tag{9}$$
Es liegt nahe, die Linearfaktoren zu Wurzeln gleicher Ordnung zusammenzufassen. Dies motiviert die folgende

Definition 1.3.14.
Das Polynom

$$F_n(X) := \prod_{\text{ord } \zeta = n} (X - \zeta)$$

heißt n-tes Kreisteilungspolynom.

Lemma 1.3.15.
Es gilt:

(i) F_n *ist normiert.*

(ii) *grad* $F_n = \varphi(n)$

(iii) $X^n - 1 = \prod_{d|n} F_d(X)$

(iv) $F_n(X) \in \mathbb{Z}[X]$.

Beweis.

(i), (ii) sind offensichtlich.

(iii) Sei $\zeta \in W_n$, dann teilt $d = \text{ord } \zeta$ sicher n. Dann benutze die Zerlegung (9).

(iv) Sei ζ_n eine primitive n-te Einheitswurzel und $\sigma \in G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Es gilt

$$F_n^\sigma(X) = \prod_{\text{ord } \zeta = n} (X - \sigma(\zeta)) = F_n(X)\,.$$

Da die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ galoisch ist, heißt dies, dass alle Koeffizienten von F_n im Fixkörper $\mathbb{Q}$ liegen, $F_n^\sigma \in \mathbb{Q}[X]$. Da außerdem $F_n(X)$ das Polynom $X^n - 1$ teilt, gibt es ein Polynom $g \in \mathbb{Q}[X]$ mit $F_n(X)g(X) = X^n - 1$. Nach dem Lemma von Gauß folgt $F_n(X) \in \mathbb{Z}[X]$.

Satz 1.3.16.
Das Kreisteilungspolynom $F_n(X)$ *ist irreduzibel im Polynomring* $\mathbb{Q}[X]$ *über den rationalen Zahlen.*

Beweis.

Sei ζ_n eine primitive n-te Einheitswurzel. Das Minimalpolynom $\min_{\mathbb{Q}}(\zeta_n)$ teilt dann das Kreisteilungspolynom F_n. Nach Satz 1.3.13 gilt aber

$$\text{grad } \min_{\mathbb{Q}}(\zeta) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \text{grad } F_n(X)\,.$$

Also gilt $\min_{\mathbb{Q}}(\zeta) = F_n$, da auch das Kreisteilungspolynom F_n normiert ist. F_n ist dann als Minimalpolynom irreduzibel.

Beispiel 1.3.17.
Sei p eine Primzahl. Dann ist, wie schon in I.3.3.15. gesehen,

$$F_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}\,.$$

Allgemeiner gilt für Primzahlpotenzen

$$F_{p^m}(X) = \frac{X^{p^m} - 1}{X^p - 1} = 1 + X^{p^{m-1}} + X^{2p^{m-1}} + \ldots + X^{(p-1)p^{m-1}}\,,$$

denn $F_{p^m}(X)$ teilt $1 + X^{p^{m-1}} + \cdots + X^{(p-1)p^{m-1}}$: jede Einheitswurzel der Ordnung p^m ist Nullstelle des Zählers, aber nicht des Nenners. Außerdem stimmen die Grade der Polynome überein:

$$\mathit{grad}\ F_{p^m} = \varphi(p^m) = p^{m-1}(p-1)\,.$$

1.4 Kreisteilungskörper, quadratisches Reziprozitätsgesetz

1.4.1 n-Teilung des Kreises

Wir wollen noch einmal auf das Problem der Konstruierbarkeit mit Zirkel und Lineal zurückkommen.

Satz 1.4.1.
Sei $M \subseteq \mathbb{C}$ eine Untermenge, die $0, 1$ enthält und K der unter komplexer Konjugation abgeschlossene Körper $K = \mathbb{Q}(M \cup \overline{M})$. Dann sind für eine komplexe Zahl $z \in \mathbb{C}$ äquivalent:

(i) z ist aus M konstruierbar, $z \in \mathcal{A}M$.

(ii) z ist algebraisch über K. Ist E die normale Hülle der Körpererweiterung $K(z)/K$, so ist $[E : K] = 2^m$ für ein $m \geq 0$.

Beweis.

(i)⇒(ii) Nach Satz I.2.1.6 gibt es einen Erweiterungskörper K_m von K, der z enthält und aus K durch sukzessive Adjunktion von Quadratwurzeln hervorgeht. Das heißt, dass K_m sich in der Form $K_m = K(\omega_1, \omega_2, \ldots, \omega_m)$ schreiben lässt, wobei $\omega_i^2 \in K(\omega_1, \ldots, \omega_{i-1}) =: K_{i-1}$ liegt, aber $\omega_i \notin K(\omega_i, \ldots, \omega_{i-1})$ liegt. Sei E_m die normale Hülle von K_m. Dann ist die Körpererweiterung E_m/K galoisch: normal ist sie ohnehin, und separabel ist sie, da wir in Charakteristik Null arbeiten.

Zu zeigen ist, dass $[E_m : K]$ Zweierpotenz ist. Wir führen den Beweis durch Induktion nach m. Für den Induktionsanfang $m = 1$ betrachten wir die quadratische Erweiterung $K_1 = K(\omega_1)$. Quadratische Erweiterungen sind stets normal. Also gilt $E_1 = K_1$ und $[E_1 : K] = 2$.
Für den Induktionsschritt nehmen wir an, dass $[E_{m-1} : K]$ eine Zweierpotenz ist. E_m ist als normale Hülle Körpers $K_m = K_{m-1}(\omega_m)$ von der Form

$$E_m = K_{m-1}(\alpha_1, \ldots, \alpha_s)\,,$$

wobei wir setzen $\alpha_1 = \omega_m$ und mit $\alpha_2, \ldots \alpha_s$ die verschiedenen Konjugierten von ω_m über K_{m-1} in einem algebraischen Abschluß C bezeichnen.
Nun ist aber α_i^2 über K konjugiert zu ω_i^2, was in E_{m-1} liegt. Da E_{m-1} über K normal ist, folgt auch $\alpha_i^2 \in E_{m-1}$. Der Körper $E_m = E_{m-1}(\alpha_1, \ldots, \alpha_s)$ entsteht also durch Adjunktion von Quadratwurzeln. Also ist der Körpergrad

$$[E_m : E_{m-1}]$$

eine Zweierpotenz. Zusammen mit der Induktionsannahme ist dann auch

$$[E_m : K] = [E_m : E_{m-1}][E_{m-1} : K]$$

eine Zweierpotenz. Damit ist auch $[K(z) : K]$ eine Zweierpotenz.

(ii) $\Rightarrow$(i) Sei z algebraisch über dem Körper K, sei E die normale Hülle von $K(z)/K$ und sei der Körpergrad $[E : K]$ eine Zweierpotenz. Dann ist die Körpererweiterung E/K ist galoisch und die Galoisgruppe $G(E/K)$ ist eine 2-Gruppe. Nach I.1.11.1 gibt es eine Kette von Untergruppen

$$G(E/K) = H_0 > H_1 > \ldots > H_n = \{1\}\,,$$

so dass H_i ein Normalteiler von $G(E/K)$ ist und $[H_{i-1} : H_i] = 2$ ist. Nach dem Hauptsatz der Galoistheorie gibt es eine Kette von Zwischenkörpern

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = E\,,$$

mit Körpergraden

$$[K_i : K_{i-1}] = [H_{i-1} : H_i] = 2$$

Nach Satz I.2.1.6 ist daher z aus M konstruierbar, $z \in \mathcal{A}M$. $\square$

Wir können jetzt die Konstruierbarkeit des regelmäßigen n-Ecks untersuchen. In anderen Worten: für welche natürliche Zahlen n ist $\zeta := \mathrm{e}^{2\pi \mathrm{i}/n} \in \mathcal{A}\mathbb{Q}$?

Da die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoisch ist, ist nach Satz 1.4.1 $\zeta \in \mathcal{A}\mathbb{Q}$ genau dann, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Zweierpotenz ist. Nach Satz 1.3.13 muss dann $\varphi(n)$ eine Zweierpotenz sein. Sei $n = 2^e p_1^{e_1} \dots p_s^{e_s}$ die Primzahlzerlegung von n, wobei die p_i ungerade Primzahlen sind. Dann ist

$$\varphi(n) = 2^{e-1}(p_1 - 1)p_1^{e_1-1} \dots (p_s - 1)p_s^{e_s-1}\,.$$

Daher ist $\varphi(n)$ genau dann Zweierpotenz, wenn n von der Form $n = 2^e p_1 \dots p_s$ ist und für alle p_i die Zahl $p_i - 1$ eine Zweierpotenz ist. Wir haben damit:

Satz 1.4.2 (Gauß)**.**
Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form

$$n = 2^e p_1 \dots p_s$$

ist, mit $e \geq 0$, p_i paarweise verschiedene Primzahlen der Gestalt

$$p_i = 1 + 2^{2^{k_i}} \quad k_i \geq 0\,.$$

Der Beweis dieses Satzes wird vervollständigt durch das folgende

Lemma 1.4.3.
Für $m \in \mathbb{N}$ ist $1 + 2^m$ höchstens dann eine Primzahl, wenn m von der Form $m = 2^k$ für ein $k \geq 0$ ist.

Beweis.

Sei m ein Produkt, $m = m_1 m_2$ mit $m_2 > 1$ einer ungeraden Zahl. Dann ist die Zahl $p := 1 + 2^m$ keine Primzahl, da gilt

$$p = 1 - (-2^{m_1})^{m_2} = (1 + 2^{m_1})(1 - 2^{m_1} + 2^{2m_1} - \dots + 2^{m_1(m_2-1)})\,,$$

also p das Produkt zweier natürlicher Zahlen größer als Eins ist.

Bemerkung 1.4.4.
Für $k \in \mathbb{N} \cup \{0\}$ heißt die Zahl

$$F_k = 2^{2^k} + 1$$

k-te Fermatzahl. Die Zahlen

$$F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad F_4 = 65537$$

sind alle Primzahlen. Fermat selbst hat behauptet, alle Fermatzahlen F_k seien prim, aber die Fermatzahlen

$$F_k \quad \textit{mit} \quad 5 \leq k \leq 16$$

sind keine Primzahlen. Es ist zur Zeit keine weitere Fermat-Primzahl F_k mit $k > 4$ bekannt.

1.4.2 Das quadratische Reziprozitätsgesetz

Als Motivation schildern wir die folgende Fragestellung: sei $p \neq 2$ eine Primzahl und $E = \mathbb{Q}(\zeta_p)$ der p-te Kreisteilungskörper. Da die Galoisgruppe

$$G(E/\mathbb{Q}) = (\mathbb{Z}/p)^\times$$

zyklisch von der Ordnung $p-1$ ist, gibt es genau eine Untergruppe vom Index 2 und somit wegen der Galois-Korrespondenz genau eine quadratische Erweiterung F der rationalen Zahlen $\mathbb{Q}$, die in diesem Kreisteilungskörper enthalten ist, $F \subseteq \mathbb{Q}(\zeta_p)$. Mit anderen Worten: es gibt genau eine quadratfreie Zahl $d \neq 1$ mit

$$\sqrt{d} \in \mathbb{Q}(\zeta_p)\,.$$

Welche Zahl ist das?

Dazu betrachte den Körper $\mathbb{F}_{p^r}$ mit p^r Elementen. Seine Einheitengruppe $\mathbb{F}_{p^r}^\times$ ist nach Satz 1.3.3 (ii) zyklisch von der Ordnung $p^r - 1$, also hat die Untergruppe $\mathbb{F}_{p^r}^{\times 2}$ der Elemente von $\mathbb{F}_{p^r}^\times$, die sich als Quadrat schreiben lassen, Index zwei:

$$[\mathbb{F}_{p^r}^\times : \mathbb{F}_{p^r}^{\times 2}] = 2 \quad \text{für} \quad p^r \neq 2\,. \tag{10}$$

Definition 1.4.5.
Sei $\nu \in \mathbb{Z}$, $\nu \neq 0$. Dann setze

$$\left(\frac{\nu}{p}\right) := \begin{cases} +1 & \textit{falls} \quad \nu = x^2 \bmod p \quad \textit{für ein} \quad x \in \mathbb{Z} \\ -1 & \textit{falls} \quad \nu \neq x^2 \bmod p \quad \textit{für alle} \quad x \in \mathbb{Z} \end{cases}$$

In Worten: $\left(\frac{\nu}{p}\right) = 1$ genau dann, wenn $\nu \bmod p$ ein Quadrat in $\mathbb{F}_p^\times$ ist. $\left(\frac{\nu}{p}\right)$ heißt das Legendre-Symbol und hängt nur von der Restklasse von ν modulo p ab.

Für $p \neq 2$ zeigt (10), dass die Faktorgruppe $\mathbb{F}_{p^r}^\times / \mathbb{F}_{p^r}^{\times 2}$ isomorph zu $\mathbb{Z}_2$ ist. Daraus folgt sofort

$$\left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right) = \left(\frac{\nu\mu}{p}\right),$$

d.h.

$$\left(\frac{\cdot}{p}\right) : \left(\mathbb{Z}/p\right)^\times \to \{\pm 1\}$$

ist ein Gruppenhomomorphismus, der für $p \neq 2$ surjektiv ist.

Lemma 1.4.6.
Nach Satz 1.3.13 ist die Abbildung

$$G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p)^\times\,,$$

die $\sigma \in G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ das Elemente $a \in (\mathbb{Z}/p)^\times$ zuordnet, für das $\sigma(\zeta_p) = (\zeta_p)^a$ gilt, ein Isomorphismus von Gruppen. Daher ist auch

$$\begin{array}{rccc} \chi & : & G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \to & \{\pm 1\} \\ & & \sigma & \mapsto & \left(\frac{a}{p}\right) \end{array}$$

ein Gruppenhomomorphismus.

Sei $p \neq 2$ und setze $\ker \chi =: H$. Dann ist der eindeutig bestimmte quadratische Teilkörper von $\mathbb{Q}(\zeta_p)$ gleich dem Fixkörper E^H.

Das folgende Lemma fasst elementare Eigenschaften des Legendre-Symbols zusammen:

Lemma 1.4.7 (Eulersches Kriterium)**.**
Sei $p \neq 2$ eine Primzahl. Dann gilt:

(i) $\left(\frac{\nu}{p}\right) = 1 \iff \nu^{\frac{p-1}{2}} = 1 \bmod p$

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(iii) $\left(\frac{1}{p}\right) = 1$

Beweis.

Aussage (iii) folgt wegen $1^2 = 1$ aus der Multiplikativität des Legendre-Symbols. (ii) folgt als Spezialfall unmittelbar aus (i). Zum Beweis von (i) bemerken wir, dass $\left(\frac{\nu}{p}\right) = 1$ genau dann gilt, wenn $\nu \in H$ liegt. Die Untergruppe H der zyklischen Gruppe $(\mathbb{Z}/p)^\times$ von $p-1$ Elementen enthält aber genau die Elemente, deren Ordnung $\frac{p-1}{2}$ teilt. □

Satz 1.4.8.

(i) Sei $\zeta = \zeta_p$ eine primitive p-te Einheitswurzel. Betrachte

$$S := \sum_{\nu \in G(\mathbb{Q}(\zeta)/\mathbb{Q})} \chi(\sigma)\sigma(\zeta) = \sum_{\nu \in (\mathbb{Z}/p)^\times} \left(\frac{\nu}{p}\right)\zeta^\nu \in \mathbb{Q}(\zeta_p)\,.$$

Dann gilt

$$S^2 = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p =: p^* \quad \text{für} \quad p \neq 2\,.$$

(ii) Für $p \neq 2$ ist $\mathbb{Q}(\sqrt{p^*})$ der eindeutig bestimmte quadratische Erweiterungskörper von $\mathbb{Q}$ in $\mathbb{Q}(\zeta_p)$.

Beweis.

(ii) folgt unmittelbar aus (i): da $S \in \mathbb{Q}(\zeta_p)$ liegt und $S^2 = p^*$ gilt, ist $\pm\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$. Andererseits liegt $\sqrt{p^*} \notin \mathbb{Q}$, also ist $\mathbb{Q}(\sqrt{p^*})$ der gesuchte Körper.

(i) folgt aus der folgenden Rechnung:

$$S^2 = \sum_{\nu,\mu} \Big(\frac{\nu}{p}\Big)\ \Big(\frac{\mu}{p}\Big)\zeta^{\nu+\mu} = \sum_{\nu,\mu} \Big(\frac{\nu\mu}{p}\Big)\zeta^{\nu+\mu}$$

Ersetze nun die Summationsvariable ν durch $\mu\nu$. Läuft ν über die multiplikative Gruppe $(\mathbb{Z}/p)^\times$, so auch $\nu\mu$:

$$S^2 = \sum_{\nu,\mu} \Big(\frac{\nu\mu^2}{p}\Big)\zeta^{\nu\mu+\mu} = \sum_{\nu,\mu} \Big(\frac{\nu}{p}\Big)\zeta^{\mu(\nu+1)}\,.$$

Wir spalten nun diese Summe auf, um die Identität

$$1 + \zeta + \zeta^2 + \ldots \zeta^{p-1} = 0$$

benutzen zu können:

$$\begin{aligned} S^2 &= \sum_{\mu} \Big(\frac{-1}{p}\Big)\zeta^0 + \sum_{\nu\neq -1} \Big(\frac{\nu}{p}\Big) \sum_{\mu} \zeta^{\mu(\nu+1)} \\ &= \Big(\frac{-1}{p}\Big)(p-1) + \sum_{\nu\neq -1} \Big(\frac{\nu}{p}\Big)(-1) \\ &= \Big(\frac{-1}{p}\Big)p - \sum_{\nu\in(\mathbb{Z}/p)^\times} \Big(\frac{\nu}{p}\Big) \\ &= \Big(\frac{-1}{p}\Big)p\ , \end{aligned}$$

da das Legendre-Symbol genauso oft den Wert $+1$ wie -1 annimmt. □

Bemerkung 1.4.9.
Für $p \neq 2$ gilt

$$\sigma\Big(\sqrt{p^*}\Big) = \chi(\sigma)\sqrt{p^*}$$

für alle $\sigma \in G(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Beweis.

Sei $\sigma = \sigma_a$ mit a koprim zu p, so gilt:

$$\begin{aligned}\sigma(S) &= \sigma_a(S) = \sum_\nu \Big(\frac{\nu}{p}\Big)\zeta^{a\nu} = \sum_\nu \Big(\frac{\nu a^{-1}}{p}\Big)\zeta^{\nu} \\ &= \Big(\frac{a}{p}\Big)\sum_\nu \Big(\frac{\nu}{p}\Big)\zeta^{\nu} = \chi(\sigma)S\,. \qquad \square\end{aligned}$$

Theorem 1.4.10 (quadratisches Reziprozitätsgesetz von Gauß)**.**

(i) Seien p, q zwei verschiedene Primzahlen ungleich zwei, $p, q \neq 2$ und $p \neq q$. Dann gilt

$$\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)$$

In Worten:
Gilt $p = 1 \bmod 4$ oder $q = 1 \bmod 4$, so ist q ein quadratischer Rest modulo p genau dann, wenn p ein quadratischer Rest modulo q ist.
Gilt $p = q = 3 \bmod 4$, so ist q quadratischer Rest modulo p genau dann, wenn p nicht *quadratischer Rest q ist.*

(ii) Für $p \neq 2$ gelten die folgenden Ergänzungssätze :

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{für } \ p = 1 \bmod 4 \\ -1 & \text{für } \ p = 3 \bmod 4 \end{cases}$$

$$\Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p = 1, -1 \bmod 8 \\ -1 & p = 3, -3 \bmod 8 \end{cases}$$

Beispiel: Ist 29 ein Quadrat modulo 43? Wir rechnen

$$\begin{aligned}\Big(\frac{29}{43}\Big) &= \Big(\frac{43}{29}\Big) = \Big(\frac{14}{29}\Big) = \Big(\frac{2}{29}\Big)\Big(\frac{7}{29}\Big) = -\Big(\frac{7}{29}\Big) \\ &= -\Big(\frac{29}{7}\Big) = -\Big(\frac{1}{7}\Big) = -1\,,\end{aligned}$$

also ist 29 kein Quadrat modulo 43.

Beweis.

(i) Wir rechnen im Ring $R = \mathbb{Z}[\zeta]$ mit $\zeta = \zeta_p$. Ein allgemeines Element dieses Ring R ist von der Form

$$\alpha = \sum_{\sigma \in G(\mathbb{Q}(\zeta)/\mathbb{Q})} a_\sigma \sigma(\zeta) \quad \text{mit} \quad a_\sigma \in \mathbb{Z}\,.$$

Wir rechnen nun modulo dem Hauptideal qR:

$$\begin{aligned}\sigma_q(\alpha) &= \sum a_\sigma \sigma(\zeta)^q = \sum a_\sigma^q \sigma(\zeta)^q \bmod qR \\ &= \Big(\sum a_\sigma \sigma(\zeta)\Big)^q \bmod qR\end{aligned}$$

Also gilt $\sigma_q(\alpha) = \alpha^q \bmod qR$. Setzen wir speziell $\alpha = \sqrt{p^*}$, so liefert Bemerkung 1.4.9

$$\sigma_q\Big(\sqrt{p^*}\Big) = \Big(\frac{q}{p}\Big)\sqrt{p^*} = \Big(\sqrt{p^*}\Big)^q \bmod qR\,.$$

Diese Gleichung multiplizieren wir mit $\sqrt{p^*}$ und erhalten

$$\Big(\frac{q}{p}\Big)p^* = (p^*)^{\frac{q+1}{2}} \bmod qR\,.$$

Nach unseren Voraussetzungen gilt $(p^*, q) = 1$, also ist $p^* \bmod q$ invertierbar in $\mathbb{Z}/q \subseteq R/q$. Es folgt

$$\Big(\frac{q}{p}\Big) = (p^*)^{\frac{q-1}{2}} \bmod qR\,,$$

also $\Big(\frac{q}{p}\Big) - (p^*)^{\frac{q-1}{2}} \in qR \cap \mathbb{Z}$, da q ungerade sein sollte.
Ein Koeffizientenvergleich bezüglich der $\mathbb{Q}$-Basis $(1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$ von $\mathbb{Q}(\zeta)/\mathbb{Q}$ zeigt, dass $q\mathbb{Z}[\zeta] \cap \mathbb{Z} = q\mathbb{Z}$ gilt. Daher folgt

$$\Big(\frac{q}{p}\Big) = (p^*)^{\frac{q-1}{2}} \bmod q\mathbb{Z} = \Big(\frac{p^*}{q}\Big) \bmod q\mathbb{Z}\ ,$$

wobei in der letzten Gleichung Lemma 1.4.7 (i) verwendet wurde. Wir finden

$$\Big(\frac{q}{p}\Big) = \Big(\frac{p^*}{q}\Big) = \Big(\frac{-1}{q}\Big)^{\frac{p-1}{2}}\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)\,,$$

wobei in der letzten Gleichheit noch einmal $q \neq 2$ benutzt wurde.

(ii) Um die Gleichung $\Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}}$ zu zeigen, betrachten wir den Körper $\mathbb{Q}(\zeta)$ mit $\zeta = \zeta_8 = \mathrm{e}^{2\pi\mathrm{i}/8}$ und rechnen im Ring $\mathbb{Q}(\zeta_8)$. Wegen

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2 + \mathrm{i} - \mathrm{i} = 2$$

ist

$$y = \zeta + \zeta^{-1} = \sqrt{2}$$

Ferner gilt

$$y^p = \zeta^p + \zeta^{-p} \bmod p\,.$$

Ist $p = \pm 1 \bmod 8$, so gilt

$$y^p = \zeta + \zeta^{-1} = y \bmod p\,,$$

also ist $y^{p-1} = 1 \bmod p$, d.h. $2^{\frac{p-1}{2}} = 1 \bmod p$. Nach Eulers Kriterium 1.4.7 (i) folgt $\left(\frac{2}{p}\right) = 1$ Ist $p = \pm 5 \bmod 8$, so gilt

$$y^p = -\zeta - \zeta^{-1} = -y \bmod p\,,$$

d.h. es ist $2^{\frac{p-1}{2}} = -1 \bmod p$. Wiederum mit 1.4.7 (i) folgt $\left(\frac{2}{p}\right) = -1$. □

1.5 Fortsetzung der Galoistheorie

Satz 1.5.1 (Translationssatz)**.**
Sei E/K eine endliche galoische Körpererweiterung und K'/K eine beliebige Körpererweiterung. Wegen Satz 1.1.2 können wir ohne Einschränkung annehmen, dass E und K' Teilkörper eines Körpers C sind. Sei $EK' = K'(E)$ das Kompositum von E und K' in C, vgl. I.2.2.13. Dann gilt

(i) Die Körpererweiterung EK'/K' ist galoisch.

(ii) Die Restriktionsabbildung

$$\begin{array}{rcl} G(EK'/K') & \to & G(E/K) \\ \sigma & \mapsto & \sigma_{|E} \end{array}$$

liefert einen Isomorphismus von Gruppen,

$$G(EK'/K') \xrightarrow{\sim} G(E/E \cap K')\,,$$

d.h. die Galoisgruppe $G(EK'/K')$ kann mit einer Untergruppe der Galoisgruppe $G(E/K)$ identifiziert werden.

Beweis.
Die Körpererweiterung EK'/K' ist nach I.2.2.14 algebraisch und nach I.4.2.10 separabel. Da die Körpererweiterung E/K normal ist, ist E Zerfällungskörper einer Menge M von Polynomen in $K[X]$. Damit ist aber auch EK' Zerfällungskörper einer Menge M' von Polynomen in $K'[X]$. Also ist auch die Körpererweiterung EK'/K' normal.

Damit ist die Körpererweiterung EK'/K' galoisch und die Abbildung aus (ii) ein wohldefinierter Gruppenhomomorphismus. Dieser Homomorphismus ist injektiv: aus $\sigma_{|_E} = 1$ folgt, dass σ die Identität ist, da σ als Element von $G(EK'/K')$ ohnehin auf K' als die Identität wirkt. Sei H das Bild der Abbildung in $G(E/K)$. Dann ist $K' \cap E \subseteq E^H$, da ein Element $\sigma \in G(EK'/K')$ alle Elemente von K' festlässt.

Sei umgekehrt $\alpha \in E^H$. Dann wird α von allen Elementen $\sigma \in G(EK'/K')$ festgelassen. Nach dem Hauptsatz der Galoistheorie folgt $\alpha \in K'$. Daher gilt auch die umgekehrte Inklusion $E^H \subseteq E \cap K'$. Wiederum nach dem Hauptsatz folgt

$$H = G(E/E^H) = G(E/K' \cap E)\,.$$

□

Bemerkung 1.5.2.
In der Situation von Satz 1.5.1 teilt der Körpergrad $[EK' : K']$ den Körpergrad $[E : K]$. Denn dieser ist gleich der Ordnung der Galoisgruppe, $[EK' : K'] = |G(EK'/K')|$, und die Ordnung einer Untergruppe teilt nach dem Satz von Lagrange die Ordnung $|G(E/K)| = [E : K]$. Achtung:
Ist die Körpererweiterung E/K nicht galoisch, so gilt diese Aussage im allgemeinen nicht. Als Gegenbeispiel betrachten wir:

$$K = \mathbb{Q} \quad E = \mathbb{Q}\Big(\sqrt[3]{2}\Big) \quad K' = \mathbb{Q}\Big(\sqrt[3]{2} \cdot \zeta_3\Big)\,.$$

Dann ist das Kompositum gleich

$$EK' = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)\,,$$

und es gilt $[E : K] = 3 = [K' : K]$. Ferner ist $[EK' : E] = 2$. Daher gilt

$$[EK' : K'] = \frac{[EK' : K]}{[K' : K]} = \frac{6}{3} = 2\,,$$

was nicht $[E : K] = 3$ teilt.

Satz 1.5.3.
Seien E_1/K und E_2/K zwei endliche galoische Erweiterungen, ohne Einschränkung seien wieder E_1 und E_2 Teilkörper eines Körpers C. Dann gilt

(i) Die Körpererweiterung E_1E_2/K ist galoisch.

(ii) Der Homomorphismus

$$\begin{array}{rcl} G(E_1E_2/K) & \to & G(E_1/K) \times G(E_2/K) \\ \sigma & \mapsto & (\sigma|_{E_1}, \sigma|_{E_2}) \end{array}$$

ist injektiv. Ist $E_1 \cap E_2 = K$, so ist diese Abbildung sogar ein Isomorphismus.

Beweis. (i) Nach Satz 1.5.1 (i) ist die Körpererweiterung E_1E_2/E_2 galoisch; E_2/K galoisch wurde vorausgesetzt. E_1E_2/K ist separabel nach I.4.2.10. Sei $\sigma : E_1E_2 \to C$ ein K-Homomorphismus in einen algebraischen Abschluss C. Da E_i/K normal ist, gilt nach Satz 1.1.13 $\sigma(E_i) \subseteq E_i$. Für das Kompositum

$$E_1E_2 = \Big\{ \sum_{\text{endlich}} a_ib_i \quad | a_i \in E_1 \text{ und } b_i \in E_2 \Big\}$$

folgt somit $\sigma(E_1E_2) \subseteq E_1E_2$. Also ist auch die Körpererweiterung E_1E_2/K normal und somit galoisch.

(ii) Sei $\sigma \in G(E_1E_2/K)$, so dass $\sigma|_{E_i} = \mathrm{id}$. Dann ist auch $\sigma = \mathrm{id}_{E_1E_2}$, also ist der angegebene Gruppenhomomorphismus injektiv. Gilt nun überdies $E_1 \cap E_2 = K$, so liefert Satz 1.5.1 die folgenden Isomorphismen:

$$\begin{array}{rcl} G(E_1E_2/E_2) & \xrightarrow{\sim} & G(E_1/K) \\ G(E_1E_2/E_1) & \xrightarrow{\sim} & G(E_2/K)\,. \end{array}$$

Für $\sigma_i \in G(E_i/K)$ gibt es somit

$$\rho_1 \in G(E_1E_2/E_2) \quad \rho_2 \in G(E_1E_2/E_1)$$

mit die Eigenschaft, dass $(\rho_i)_{|E_i} = \sigma_i$. Setze $\tau := \rho_1\rho_2 \in G(E_1E_2/K)$. Man rechnet nach:

$$\tau_{|_{E_1}} = (\rho_1)_{|E_1}(\rho_2)_{|E_1} = \sigma_1 \mathrm{id}_{E_1} = \sigma_1\,,$$

und entsprechend auch $\tau_{|E_2} = \sigma_2$. Also ist der angegebene Gruppenhomomorphismus auch surjektiv. □.

Definition 1.5.4.

(i) Sei K ein Körper und M ein Monoid. Ein <u>Charakter</u> von M mit Werten in K ist ein Homomorphismus von Monoiden

$$\chi : M \to K^\times\,.$$

Ein Charakter heißt <u>trivial</u>, wenn $\chi(m) = 1$ für alle $m \in M$ gilt.

(ii) Die Funktionen $f : M \to K$ bilden einen K-Vektorraum. Entsprechend heißen Funktionen

$$f_i : M \to K, \quad i = 1, \ldots, n$$

<u>linear unabhängig über K</u>, falls aus

$$a_1 f_1 + \cdots + a_n f_n = 0 \quad \textit{mit} \quad a_i \in K$$

folgt, dass $a_1 = a_2 = \cdots = a_n = 0$ gilt.

Satz 1.5.5 (Artin)**.**
Seien $\chi_1, \ldots \chi_n$ paarweise verschiedene Charaktere eines Monoids M mit Werten in einem Körper K. Dann sind diese Charaktere als Funktionen auf M linear unabhängig.

Beweis.

Induktion nach n. Induktionsanfang $n = 1$: wegen $\chi(M) \subseteq K^\times$ ist ein einzelner Charakter linear unabhängig.

Sei $n > 1$ und

$$a_1\chi_1 + \cdots + a_m\chi_m = 0 \tag{11}$$

eine Relation minimaler Länge m, in der alle Koeffizienten $a_m \neq 0$ sind. Es gilt also $2 \leq m \leq n$.

Da $\chi_1 \neq \chi_2$ sein soll, gibt es wenigstens ein $z \in M$, für das $\chi_1(z) \neq \chi_2(z)$ gilt. Es gilt für alle $x \in M$

$$\begin{aligned} 0 &= a_1\chi_1(zx) + \cdots + a_m\chi_m(zx) \\ &= a_1\chi_1(z)\chi_1(x) + \cdots + a_m\chi_m(z)\chi_m(x). \end{aligned}$$

Damit erhalten wir eine weitere verschwindende Linearkombination der Charaktere,

$$\sum_i a_i\chi_i(z)\,\chi_i = 0\,.$$

Wir teilen diese Gleichung durch $\chi_1(z)$ und subtrahieren sie von (11) und erhalten die verschwindende Linearkombination

$$a_2\Bigg(\underbrace{\frac{\chi_2(z)}{\chi_1(z)} - 1}_{\neq 0}\Bigg)\chi_2 + \cdots + a_m\left(\frac{\chi_m(z)}{\chi_1(z)} - 1\right)\chi_m = 0\,.$$

Sie ist nicht trivial und hat eine kürzere Länge als die Relation (11), im Widerspruch zur angenommenen Minimalität der Relation (11). □

Wir wollen uns jetzt noch eine besonders schöne K-Basis einer endlichen Galoiserweiterung E/K verschaffen.

Satz 1.5.6 (Existenz einer Normalbasis)**.**
Sei E/K endliche galoische Erweiterung mit Galoisgruppe G. Dann existiert ein Element $\alpha \in E$, so das

$$\{\sigma(\alpha)\}_{\sigma\in G}$$

eine K-Basis von E ist. Eine solche Basis heißt Normalbasis von E/K. Das Element $\alpha \in E$ ist ein primitives Element der Körpererweiterung E/K, d.h. es gilt $E = K(\alpha)$.

Beispiel 1.5.7. *Sei p eine Primzahl, ζ_p eine primitive p-te Einheitswurzel über $\mathbb{Q}$ und $E = \mathbb{Q}(\zeta_p)$. Dann ist*

$$\{\sigma^i(\zeta_p) = (\zeta_p)^i \quad i = 1, 2, \ldots, p-1\}$$

eine Normalbasis von $E/\mathbb{Q}$.

Beweis.

- Es reicht aus, zu zeigen, dass es ein Element $\alpha \in E$ gibt, so dass das folgende Element von E nicht verschwindet:

  $$\det(\tau^{-1}\sigma\alpha)_{\tau,\sigma\in G} \neq 0\,.$$

  Denn aus einer Relation $\sum_{\sigma\in G} a_\sigma\sigma(\alpha) = 0$ mit Koeffizienten $\alpha_\sigma \in K$ folgt für alle $\tau \in G$

  $$\sum_{\sigma\in G} a_\sigma\tau^{-1}\sigma(\alpha) = 0\,.$$

  Also ist der Spaltenvektor (a_σ) der Koeffizienten im Kern der Matrix

  $$(\tau^{-1}\sigma\alpha)_{\tau,\sigma\in G}$$

  mit nicht–verschwindender Determinante. Also ist $a_\sigma = 0$ für alle $\sigma \in G$. Daher ist die Familie $(\sigma\alpha)_{\sigma\in G}$ linear unabhängig und wegen $[E : K] = |G|$ eine K-Basis von E.

- Solch ein Element wollen wir ausgehend vom Satz vom primitiven Element finden. Nach diesem Satz gibt es ein $\beta \in E$, so dass $K(\beta) = E$. Sei $f(X) = \min_K(\beta)$ das Minimalpolynom von β, das separabel ist und über E in paarweise verschiedene Linearfaktoren zerfällt:

  $$f(X) = \prod_{\sigma\in G}(X - \sigma\beta) \quad \in E[X]\,.$$

Für jedes Element $\sigma \in G$ der Galoisgruppe betrachte das Polynom

$$g^\sigma(X) := \frac{f(X)}{X - \sigma\beta} \quad \in E[X]\,.$$

Es gilt $g^\sigma(\beta) = 0$ für $\sigma \neq e$, aber $g^e(\beta) \neq 0$.
Betrachte die quadratische Matrix von Polynomen in $E[X]$:

$$\left(g^{\tau^{-1}\sigma}(X)\right)_{\tau,\sigma\in G} = \left(\frac{f(X)}{X - \tau^{-1}\sigma\beta}\right)_{\tau,\sigma\in G}.$$

Ihre Determinante, die natürlich auch im Polynomring $E[X]$ liegt,

$$d(X) := \det(g^{\tau^{-1}\sigma}(X))_{\tau,\sigma} \in E[X]$$

verschwindet nicht: durch Einsetzen des primitiven Elements $\beta \in E$ erhält man nämlich eine Diagonalmatrix, also gilt für die Determinante

$$d(\beta) = \det(g^{\tau^{-1}\sigma}(\beta)) = g(\beta)^n \neq 0\,.$$

Wir betrachten jetzt den Fall endlicher und unendlicher Körper getrennt. Sei zunächst K unendlich. Das Polynom $d \in E[X]$ hat nur endlich viele Nullstellen in K, also gibt es ein Element $\gamma \in K$ mit $d(\gamma) \neq 0$. Das heißt aber, es giltj

$$\det(g^{\tau^{-1}\sigma}(\gamma)) = \det\left(\tau^{-1}\sigma\frac{f(\gamma)}{\gamma - \beta}\right) \neq 0\,,$$

und das Element $\alpha := \frac{f(\gamma)}{\gamma-\beta} \in E$ hat die gewünschten Eigenschaften.

Wir betrachten nun noch den Fall, wenn der Körper K endlich ist. Nach Satz 1.3.8 ist die Galoisgruppe $G(E/K)$ zyklisch erzeugt von dem Automorphismus $\sigma : X \mapsto X^q$ mit $q = |K|$. Wir behaupten nun, dass das Minimalpolynom des K-linearen Endomorphismus $\sigma : E \to E$ das Polynom $X^n - 1$ ist mit $n = [E : K]$.

Sicher ist σ Nullstelle von $X^n - 1$, da $\sigma^n = 1$ gilt. Ferner sind $\{1, \sigma, \ldots, \sigma^{n-1}\}$ verschiedene Charaktere des Monoids $E^\times$ mit Werten in E, nach Satz 1.5.5 sind diese Charaktere linear unabhängig. Daher kann σ nicht Nullstelle eines echten Teilers von $X^n - 1$ sein. Damit ist aber die Dimension des K-Vektorraums

E gleich dem Grad des Minimalpolynoms von σ, also stimmen Minimalpolynom und charakteristisches Polynom von σ überein.

Aus der linearen Algebra sollte folgender Sachverhalt bekannt sein (vgl. etwa Falko Lorenz, Lineare Algebra II, p. 166, Kapitel IX, §5, F16)

Satz 1.5.8.
Sei V ein endlich-dimensionaler K-Vektorraum und $f \in \mathrm{End}(V)$. Der Vektorraum V heißt zyklisch bezüglich f, wenn es einen Vektor $w \in V$ gibt, so dass $\{f^k w \ , \ k = 0, 1, 2, \ldots\}$ ein Erzeugendensystem von V ist. Es gilt: Genau dann ist V zyklisch bezüglich f, wenn das Minimalpolynom von f mit dem charakteristischen Polynom übereinstimmt.

Es gibt also für den Endomorphismus σ einen zyklischen Vektor $\alpha \in E$; das heißt aber, $\{\alpha, \sigma\alpha, \ldots, \sigma^{n-1}\alpha\}$ ist eine K-Basis von E.

- Schließlich überlegen wir uns noch, dass das eben gefundene Element $\alpha \in E$ auch primitiv ist. Offenbar ist $K(\alpha) \subseteq E$. Außerdem gilt $[K(\alpha) : K] = \mathrm{grad}\, \min_K(\alpha) = |G| = [E : K]$. □

1.6 Unendliche Galoiserweiterungen

Sei K ein Körper und C ein algebraischer Abschluss von K. Sei $C_s \subseteq C$ der separable Abschluss von C/K, d.h. der größte Teilkörper von C, der nur über K separable Elemente enthält. Die Körpererweiterung C_s/K ist galoisch: denn die normale Hülle C_s' von C_s ist nach Satz 1.2.10 auch separabel über K und daher gleich C_s. Eine beliebige Galoiserweiterung von K kann als Teilkörper von C_s aufgefasst werden. Nur können wir die bisher entwickelten Techniken nicht direkt auf diese Erweiterung anwenden, denn C_s/K ist i.a. keine endliche Erweiterung.

Beispiel 1.6.1.
Sei p eine Primzahl, $K = \mathbb{F}_p$. Da K perfekt ist, gilt $C = C_s$. Wir bezeichnen diesen Körper mit $\mathbb{F}_{p^\infty}$. Mit $\varphi \in G(\mathbb{F}_{p^\infty}/\mathbb{F}_p)$ bezeichnen wir den Frobeniusautomorphismus

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{p^\infty} & \to & \mathbb{F}_{p^\infty} \\ & x & \mapsto & x^p \end{array}$$

Sei $H = \langle\varphi\rangle$ die vom Frobeniusautomorphismus zyklisch erzeugte Untergruppe der Galoisgruppe $G(\mathbb{F}_{p^\infty}/\mathbb{F}_p)$. Der zugehörige Fixkörper ist

$$\mathbb{F}_{p^\infty}^H = \mathbb{F}_p\,.$$

Würde der Hauptsatz der Galoistheorie so stimmen, wie er für endliche Erweiterungen formuliert wurde, so würde daraus für die Galoisgruppe folgen

$$H = G(\mathbb{F}_{p^\infty}/\mathbb{F}_p)\,.$$

Dies gilt aber nicht: für eine von p verschiedene Primzahl q betrachten wir den Unterkörper

$$\mathbb{F} := \bigcup_m \mathbb{F}_{p^{q^m}} \subseteq \mathbb{F}_{p^\infty}\,.$$

Für jedes Element $x \in \mathbb{F}$ gilt $x^{p^{q^m}} = x$ für ein geeignetes m. Daher ist der Körpergrad $[\mathbb{F}_p(x) : \mathbb{F}_p]$ eine q-Potenz. Daher muss $\mathbb{F}$ strikt kleiner als $\mathbb{F}_{p^\infty}$ sein. Nach den Fortsetzungssätzen gibt es daher ein von der Identität verschiedenes $\tau \in G(\mathbb{F}_{p^\infty}/\mathbb{F})$.

Gälte aber andererseits $H = \langle\varphi\rangle = G(\mathbb{F}_{p^\infty}/\mathbb{F})$, so gäbe es ein n, so dass $\varphi^n = \tau$. Daraus würden dann aber die Inklusionen

$$\mathbb{F} \subseteq \mathbb{F}_{p^\infty}^{\langle\tau\rangle} = \mathbb{F}_{p^\infty}^{\langle\varphi^n\rangle} = \mathbb{F}_{p^n}$$

folgen, aus denen wir schließen, dass der Körpergrad $[\mathbb{F} : \mathbb{F}_p]$ den Körpergrad $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ teilen müsste. Aber der Körpergrad $[\mathbb{F} : \mathbb{F}_p]$ ist unendlich. Widerspruch, also kann τ nicht in H liegen, und H nicht die ganze Galoisgruppe sein.

Sei nun E/K eine beliebige Galoiserweiterung mit Galoisgruppe $G = G(E/K)$ und F ein galoischer Zwischenkörper von E/K. Wir haben die Restriktionsabbildungen (vgl. 1.2.9)

$$\begin{array}{ccc} G & \to & G(F/K) \\ \sigma & \mapsto & \sigma^F := \sigma_{|F} \end{array}$$

Wir betrachten sie alle gleichzeitig, genauer betrachten wir

$$\begin{array}{rccc} h: & G & \to & \prod\limits_{L\subseteq E} G(L/K) \\ & \sigma & \mapsto & (\sigma^L)_L\,. \end{array}$$

wobei $L \subseteq E$ über alle endlichen galoischen Erweiterungen von K laufen soll. Wir bemerken, dass man den Körper E durch solche Körpererweiterungen ausschöpfen kann:

$$E = \bigcup_{\substack{L/K \text{ endl.,galoisch} \\ L\subseteq E}} L\,.$$

Aus $\sigma \in G$ mit $\sigma^L = 1$ für alle L, also $\sigma_{|L} = \mathrm{id}_{|L}$ für alle solchen Zwischenkörper L, folgt $\sigma = \mathrm{id}_E$. Die Abbildung h ist daher injektiv,

Allerdings ist die Abbildung h nicht surjektiv, wir wollen ihr Bild untersuchen. Für endliche galoische Erweiterungen L, L' von K in E und $L \subseteq L'$ betrachten wir die Restriktionen

$$\begin{array}{rccc} f_{L/L'}: & G(L'/K) & \twoheadrightarrow & G(L/K) \\ & \tau & \to & \tau^L\,. \end{array}$$

In der Situation $L \subseteq L' \subseteq L''$ gilt dann

$$f_{L/L''} = f_{L/L'} \circ f_{L'/L''}\,.$$

Das Bild von h liegt also in der folgenden Untergruppe

$$\{(\sigma_L)_L \in \prod_{L/K} G(L/K) \mid f_{L/L'}(\sigma_{L'}) = \sigma_L \;\forall\; L \subset L'\}\,.$$

Wir formalisieren nun diese Situation.

Definition 1.6.2.

(i) Sei I eine partiell geordnete Menge. I heißt gerichtet, falls es zu je zwei Elementen $i, i' \in I$ ein Element $j \in I$ gibt mit

$$i \leq j \quad \textit{und} \quad i' \leq j\,.$$

(ii) Sei $(G_i)_{i\in I}$ eine Familie von (Gruppen, Ringen, Körpern, topologischen Räumen, ganz allgemein Objekten einer Kategorie), die durch eine gerichtete Menge I indiziert ist. Sei

$$f_{ij} : G_j \to G_i$$

eine Familie von Abbildungen (Gruppen-, Ring-, Körperhomomorphismen, stetige Abbildungen, ganz allgemein von Morphismen einer Kategorie) für $i \leq j$.

Dann heißt (G_i, f_{ij}) ein projektives System, falls

$$f_{ik} = f_{ij} f_{jk} \quad \textit{für} \quad i \leq j \leq k$$

gilt, d.h. wenn das Diagramm

$$\begin{array}{ccccc} & & G_k & & \\ & \swarrow^{f_{jk}} & & \searrow^{f_{ik}} & \\ G_j & & \xrightarrow[f_{ij}]{} & & G_i \end{array}$$

für alle $i \leq j \leq k$ kommutativ ist.

(iii) *Der projektive Limes eines projektiven Systems* (G_i, f_{ij}) *ist eine Menge* $(\dots,$ *allgemein ein Objekt einer Kategorie)*

$$G := \varprojlim_{\substack{i\in I \\ f_{ij}}} G_i \,,$$

zusammen mit Abbildungen $(\dots)$

$$f_i \,:\, G \to G_i \,,$$

so dass alle Diagramme der Form

$$\begin{array}{ccccc} & & G & & \\ & f_j \swarrow & & \searrow f_i & \\ G_j & & \to & & G_i \\ & & f_{ij} & & \end{array} \qquad i \le j$$

kommutieren und die folgende universellen Eigenschaft gilt: Ist H *eine Menge* $(\dots)$ *und seien*

$$g_i \,:\, H \to G_i$$

Abbildungen, so dass alle Diagramme der Form

$$\begin{array}{ccccc} & & H & & \\ & g_j \swarrow & & \searrow g_i & \\ & G_j & \to & G & \\ & & f_{ij} & & \end{array}$$

kommutieren, so existiert eine eindeutig *bestimmte Abbildung* $g : H \to G$, *so dass* $f_j \circ g = g_j$ *für alle* $j \in I$ *gilt.*

(iv) *Analog definiert man ein* induktives *(direktes) System und einen induktiven Limes* $G = \varinjlim G_i$, *indem man alle Pfeile in allen Diagrammen umdreht.*

Bemerkung 1.6.3.

(i) *Projektive und induktive Limites sind bis auf kanonische Isomorphie eindeutig, wenn sie existieren. Der Beweis benutzt, wie üblich, die universelle Eigenschaft.*

(ii) *Der projektive Limes eines projektiven Systems* (G_i, f_{ij}) *von Gruppen existiert und lässt sich als Untergruppe des Produkts realisieren:*

$$G = \varprojlim_{f_{ij}} G_i = \left\{ (\sigma_i)_{i\in I} \in \prod_{i\in I} G_i \,|\, f_{ij}(\sigma_j) = \sigma_i \quad \text{für} \quad i \le j \right\} .$$

(iii) Der induktive Limes eines induktiven Systems von Körpern (E_i, g_{ij}) existiert. Er ist isomorph zum Kompositum der Körper E_i. Man beachte, dass alle g_{ij} als Körperhomomorphismen injektiv sind.

Satz 1.6.4.
Sei E/K galoisch mit Galoisgruppe $G = G(E/K)$. Die Abbildung

$$\begin{array}{rccc} h: & G & \to & \prod_{L/K} \quad G(L/K) \\ & \sigma & \mapsto & \sigma^L := \sigma|_L \quad , \end{array}$$

wobei $L \subseteq E$ endlich und galoisch über K sein soll, vermittelt einen Isomorphismus auf den projektiven Limes

$$G(E/K) \xrightarrow{\sim} \varprojlim G(L/K)\,.$$

Beweis.

Sei $I := \{L \subseteq E | L/K$ endlich, galoisch $\}$. Dies ist eine bezüglich der Inklusion "$\subseteq$" gerichtete geordnete Menge, denn mit L_1 und L_2 liegt auch das Kompositum L_1L_2 in I. Sei

$$\widetilde{G} = \varprojlim_I G(L/K)$$

der projektive Limes der Galoisgruppen. Die Restriktion auf L

$$\begin{array}{rccc} g_L: & G & \to & G(L/K) \\ & \sigma & \mapsto & \sigma^L \end{array}$$

erfüllt für $L \subseteq L'$

$$g_L = f_{L/L'} \circ g_{L'}\,.$$

Also gibt es nach der universellen Eigenschaft des projektiven Limes einen Gruppenhomomorphismus

$$h : G(E/K) \hookrightarrow \varprojlim G(L/K) \subseteq \prod_{L \in I} G(L/K)\,.$$

Dieser ist nach den Bemerkungen vor Definition 1.6.2 injektiv, seine Surjektivität bleibt zu zeigen. Sei also

$$(\sigma_L)_{L \in I} \in \varprojlim G(L/K)$$

vorgeben. Wir müssen ein $\sigma \in G(E/K)$ finden, so dass $\sigma_{|L} = \sigma_L$ für alle $L \in I$ gilt. Sei

$$\sigma : E = \bigcup_{L \in L} L \to E$$

definiert für $x \in L_0$ durch $\sigma(x) := \sigma_{L_0}(x)$. Dies ist wohldefiniert, denn seien $L_1, L_2 \in I$ und $L_3 = L_1 \cap L_2$, so gilt

$$(\sigma_{L_1})_{|L_3} = (\sigma_{L_2})_{|L_3}\,.$$

Betrachte das Kompositum $L = L_1 L_2$, hier gilt

$$(\sigma_L)_{|L_i} = f_{L_i/L}(\sigma_L) = \sigma_{L_i} \qquad i = 1, 2\,.$$

Daher gilt

$$(\sigma_{L_1})_{|L_1 \cap L_2} = (\sigma_L|_{L_1})_{|L_1 \cap L_2} = \sigma_L|_{L_1 \cap L_2} = (\sigma_L|_{L_2})_{|L_1 \cap L_2} = (\sigma_{L_2})_{|L_1 \cap L_2} \qquad \square$$

Definition 1.6.5. *Eine topologische Gruppe G ist eine Gruppe, die mit der Struktur eines topologischen Raumes versehen ist, so dass die Abbildung*

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & xy^{-1} \end{array}$$

stetig ist.

Bemerkung 1.6.6.
Ist $(G_i)_{i \in I}$ eine Familie topologischer Gruppen, so ist auch ihr Produkt $\prod_{i \in I} G_i$ in natürlicher Weise eine topologische Gruppe: die Produkttopologie ist die gröbste Topologie, für die alle Projektionen

$$\prod_j G_j \twoheadrightarrow G_j$$

stetig sind.

Ist (G_i, f_{ij}) ein projektives System topologischer Gruppen – was insbesondere heißt, dass alle f_{ij} stetige *Gruppenhomomorphismen sind — und sind alle G_i hausdorffsch, dann ist der projektive Limes*

$$\varprojlim G_i$$

eine abgeschlossene Untergruppe von $\prod_{i \in I} G_i$. (Beweis kommt in den Übungen). Damit ist der projektive Limes eines gerichteten Systems topologischer Gruppen wieder in natürlicher Weise eine topologische Gruppe.

Definition 1.6.7.
Sei E/K eine beliebige galoische Erweiterung. Dann ist die Galoisgruppe $G(E/K)$ in natürlicher Weise mit einer Topologie versehen: Seien $L/K, L \subseteq$

E endliche galoische Teilkörper von E/K und seien die endlichen Galoisgruppen $G(L/K)$ mit der diskreten Topologie versehen. Das heißt, alle Untermengen von $G(L/K)$ werden als offene (und somit auch als abgeschlossene) Mengen deklariert. Durch die Produkttopologie wird das Produkt dieser Galoisgruppen zu einer topologischen Gruppe. Der projektive Limes

$$\lim_{\leftarrow} G(L/K)$$

als Untergruppe erhält somit die Struktur einer topologischen Gruppe. Mit Hilfe des Isomorphismus aus Satz 1.6.4 erhält die Galoisgruppe $G(E/K)$ eine Topologie, die Krulltopologie.

Wir beschreiben diese Topologie nun genauer:

Satz 1.6.8.

(i) Sei E/K eine galoische Erweiterung. Dann ist die mit der Krulltopologie versehene Galoisgruppe $G(E/K)$ kompakt.

(ii) Die Familie der Untergruppen $(G(E/L))$ wobei $L \subseteq E$ eine über K endliche galoische Erweiterung ist, stellt ein System offener Basisumgebungen der $1 \in G$ dar. Das heißt: $G(E/L)$ ist offen und jede Umgebung der $1 \in G$ enthält eine Menge der Form $G(E/L)$. Da die Translationen stetig sind, bilden dann auch die Mengen $\sigma G(E/L)$ eine Umgebungsbasis eines beliebigen Elements $\sigma \in G$.

Beweis.

(i) Da die Gruppe $G(L/K)$ endlich ist, ist diese Gruppe in der diskreten Topologie kompakt. Nach dem Satz von Tychonoff ist das Produkt $\prod_L G(L/K)$ kompakt. Der projektive Limes $\lim_{\leftarrow} G(L/K)$ ist dann als abgeschlossene Untergruppe der kompakten Gruppe $\prod G(L/K)$ kompakt.

(ii) Betrachte wieder das gerichtete System $I = \{L \,|\, L/K \text{ endlich, galoisch, } L \subseteq E\}$. Sei $S \subseteq I$ eine endliche Teilmenge. Wir setzen

$$U_S := \prod_{L \in S} \{1\} \times \prod_{L \notin S} G(L/K) \subseteq \prod_{L \in I} G(L/K)$$

für die entsprechende Untermenge im Produkt der Gruppen. Aus der Definition der Produkttopologie folgt sofort, dass

$$\{U_S | S \subseteq I \text{ endlich}\}$$

ein System offener Basisumgebungen der $1 \in \prod_{L \in I} G(L/K)$ ist. Der Schnitt mit $\lim\limits_{\leftarrow} G(L/K)$ ist dann eine Basis von $1 \in \lim\limits_{\leftarrow} G(L/K)$.
Sei $S \subseteq I$ endlich und L_S das Kompositum aller L_i für $i \in S$. Dann ist de Zwischenkörper $L_S \in I$ und es gilt

$$U_S \cap \lim_{\leftarrow} G(L/K) = U_{\{L_S\}} \cap \lim_{\leftarrow} G(L/K)\,.$$

Dies folgt aus der Definition des projektiven Limes: seine Elemente sind von der Form $(x_i)_{i \in I}$. Auf der linken Seite gilt $x_{L_i} = 1$ für alle $i \in S$, auf der rechten Seite gilt $x_{L_s} = 1$, was wegen der Eigenschaft $f_{L/L'}(x_{L'}) = x_L$ des projektiven Limes äquivalent ist. Da das Urbild unter dem Isomorphismus h von $U_{L_S} \cap \lim\limits_{\leftarrow} G(L/K)$ genau $G(E/L_S)$ ist, folgt die Aussage.

Lemma 1.6.9.
Jede offene Untergruppe einer topologischen Gruppe ist abgeschlossen.

Beweis.
Sei $H \subseteq G$ eine offene Untergruppe und $\mathcal{P}$ ein Repräsentantensystem der Nebenklassen von G/H. Da die Translation mit $g \in G$

$$\begin{array}{ccc} H & \xrightarrow{\sim} & gH \\ h & \mapsto & gh \end{array}$$

ein topologischer Isomorphismus ist, ist die Untermenge gH von G offen für alle $g \in G$. Also ist

$$G \backslash H = \dot{\bigcup}_{\substack{g \in \mathcal{P} \\ g \neq e}} gH$$

als disjunkte Vereinigung offener Mengen offen, also ihr Komplement H abgeschlossen. □

Theorem 1.6.10 (Hauptsatz der Galoistheorie für beliebige Galoiserweiterungen)**.**
Sei E/K eine galoische Körpererweiterung. Dann ist die Abbildung

$$\mathcal{Z}(E/K) \longrightarrow \mathcal{U}(E/K)$$

von der Menge aller Zwischenkörper auf die Menge aller abgeschlossenen *Untergruppen der Galoisgruppe $G(E/K)$*

$$\begin{array}{ccc} F & \mapsto & G(E/F) \end{array}$$

eine Bijektion. Die abgeschlossenen Untergruppen $G(E/F)$ von $G(E/K)$ sind genau dann auch offen, falls die Körpererweiterung F/K endlichen Grad hat.

Beweis. Wir führen den Beweis in 5 Schritten.

1. Schritt: Sei F/K endlich, $F \subseteq E$, dann ist die Galoisgruppe $G(E/F)$ offen, also nach Lemma 1.6.9 auch abgeschlossen.

Beweis des ersten Schritts:
Sei L die normale Hülle von der Körpererweiterung F/K in E. Dann ist die Erweiterung L/K endlich und galoisch. Nach Satz 1.6.8 ist $G(E/L) \subseteq G(E/K)$ eine offene Untergruppe. Nun ist $G(E/L) \subseteq G(E/F)$, also ist

$$G(E/F) = \dot{\bigcup_g} gG(E/L)$$

als disjunkte Vereinigung von offenen Nebenklassen offen.

2. Schritt: Sei F/K ein beliebiger Zwischenkörper, dann ist die Galoisgruppe $G(E/F)$ abgeschlossen in $G(E/K)$.

Beweis des zweiten Schritts:
Sei $\sigma \in G(E/K) \setminus G(E/F)$. Wir wollen eine offene Umgebung von σ konstruieren, die $G(E/F)$ nicht trifft.

Da σ auf F nicht die Identität sein soll, gibt es sicher einen Unterkörper $F_0 \subseteq F$, der endlich über K ist, auf dem σ nicht die Identität ist, also $\sigma \notin G(E/F_0)$. Daraus folgt

$$\sigma G(E/F_0) \cap G(E/F) = \emptyset\,,$$

denn gäbe es ein $\tau \in G(E/F)$ von der Form $\tau = \sigma\rho$ mit $\rho \in G(E/F_0)$, dann wäre $\sigma = \tau\rho^{-1} \in G(E/F_0)$, Widerspruch. Nach Schritt 1 ist die Untergruppe $G(E/F_0)$ offen, also ist auch $\sigma G(E/F_0)$ eine offene Umgebung von σ, die aber $G(E/F)$ nicht trifft. Also ist $G(E/F)$ abgeschlossen.

3. Schritt: Nach Satz 1.2.7 ist die Abbildung injektiv, denn dort wurde im Beweis Endlichkeit nicht benutzt.

4. Schritt: Sei $H \subseteq G(E/K)$ eine offene Untergruppe und $F = E^H$ der Fixkörper. Dann ist die Körpererweiterung F/K endlich.

Beweis des vierten Schritts:
Nach Satz 1.6.8 (ii) gibt es eine endliche galoische Erweiterung L/K mit

$L \subseteq E$, so dass $G(E/L) \subseteq H$ gilt. Damit gilt aber auch die Inklusion $F = E^H \subseteq E^{G(E/L)} = L$, also ist auch die Körpererweiterung F/K endlich.

5. Schritt: Sei $H \subseteq G(E/K)$ eine abgeschlossene Untergruppe. Dann ist $H = G(E/E^H)$.

Beweis des fünften Schritts:
Sei H eine nicht notwendigerweise abgeschlossene Untergruppe von $G(E/K)$. Sei $\overline{H}$ die abgeschlossene Hülle,

$$\overline{H} := \bigcap A$$

wobei A alle abgeschlossenen Untergruppen von $G(E/K)$ durchläuft, die H enthalten. Ist H abgeschlossen, so gilt natürlich $\overline{H} = H$. Die abgeschlossene Hülle $\overline{H}$ ist offenbar eine abgeschlossene Untergruppe von $G(E/K)$, und es gilt $H \leq G(E/E^H)$. Nach Schritt 2 ist $G(E/E^H)$ abgeschlossen, woraus die Inklusion

$$\overline{H} \leq G(E/E^H)$$

folgt. Wir behaupten, dass für eine beliebige Untergruppe

$$\overline{H} = G(E/E^H) \tag{12}$$

gilt, woraus insbesondere für abgeschlossene Untergruppen die Behauptung folgt.

Dazu sei $\sigma \in G(E/E^H)$. Um $\sigma \in \overline{H}$ zu zeigen, müssen wir für jede Basisumgebung von σ der Form $\sigma G(E/L)$ zeigen, dass

$$\sigma G(E/L) \cap H \neq \emptyset\,,$$

wobei L die endlichen galoischen Zwischenkörper von E/K durchläuft. Betrachte dazu die Surjektion

$$\begin{array}{ccc} G(E/E^H) & \twoheadrightarrow & G(LE^H/E^H) \\ \cup| & & \cup| \\ H & \twoheadrightarrow & H_0 \end{array}$$

Dann gilt

$$E^H \subseteq (LE^H)^{H_0} \subseteq E^H\,,$$

also ist

$$E^H = (LE^H)^{H_0}\,.$$

Aus dem Hauptsatz der Galoistheorie für endliche Erweiterungen folgt die Gleichheit

$$H_0 = G(LE^H/E^H)\,.$$

Das heißt aber: zu jedem $\sigma \in G(E/F)$ gibt es ein $\tau \in H$, mit

$$\sigma_{|LE^H} = \tau_{|LE^H}\,.$$

Da aber $\rho = \sigma^{-1}\tau \in G(E/L)$ gilt, haben $\tau \in \sigma G(E/L) \cap H$, womit der Durchschnitt nicht leer ist. □

Wir wollen noch einen Kommentar zur Gleichung (12) machen, die für beliebige Untergruppen H der Galoisgruppe gilt. Sie sagt aus, dass die Krulltopologie genau die Eigenschaft hat, dass die Vervollständigung bezüglich dieser Topologie die Galoiskorrespondenz zu einer Korrespondenz macht. Insofern enthält diese Topologie eine Menge *algebraischer* Information!

Bemerkung 1.6.11.
Man kann die folgenden Tatsachen zeigen, deren Beweis wir nicht bringen:

(i) Ist F ein Zwischenkörper einer galoischen Erweiterung E/K und ist F/K ebenfalls galoisch, so ist die natürliche Surjektion

$$G(E/K) \twoheadrightarrow G(F/K)$$

stetig und offen und vermittelt eine Isomorphie topologischer Gruppen

$$G(E/K)/G(E/F) \xrightarrow{\sim} G(F/K)\,,$$

wobei der Quotient $G(E/K)/G(E/F)$ mit der Quotiententopologie versehen sein soll, d.h. der feinsten Topologie, für die die Restklassenabbildung stetig ist.

(ii) Ist F ein Zwischenkörper von E/K, so induziert die Krulltopologie von $G(E/K)$ auf der Untergruppe $G(E/F)$ ebenfalls die Krulltopologie.

(iii) Ist $H \leq G(E/K)$ eine offene Untergruppe, so ist der Index $[G(E/K) : H]$ endlich und es gilt $[G(E/K) : H] = [E^H : K]$.

1.7 Norm und Spur

Ziel des restlichen Teils dieses Kapitels ist die Untersuchung der Auflösbarkeit polynomialer Gleichungen durch Wurzeln. Um erst einmal Wurzeln zu untersuchen, brauchen wir einige Hilfsmittel aus der linearen Algebra.

Sei K ein Körper und E/K eine endliche Körpererweiterung. Betrachte E als endlich-dimensionalen K-Vektorraum. Jedes $\alpha \in E$ gibt durch Multiplikation einen K-linearen Endomorphismus

$$\begin{array}{rccc} \alpha_{E/K}: & E & \to & E \\ & x & \mapsto & \alpha x\,. \end{array}$$

Definition 1.7.1.
Das charakteristische Polynom $P(\alpha_{E/K})$ bzw. die Spur $\mathrm{Sp}(\alpha_{E/K})$ bzw. die Determinante $\det(\alpha_{E/K})$ heißen charakteristisches Polynom, Spur und Norm von α:

$$\begin{array}{rcl} P_{E/K}(\alpha) & := & P(\alpha_{E/K}) \in K[X] \\ \mathrm{Sp}_{E/K}(\alpha) & := & \mathrm{tr}(\alpha_{E/K}) \in K \\ N_{E/K}(\alpha) & := & \det(\alpha_{E/K}) \in K\,. \end{array}$$

Bemerkung 1.7.2.
Aus Standardresultaten aus der linearen Algebra schließen wir sofort:

(i) Die Spur $\mathrm{Sp}_{E/K} : E \to K$ ist eine K-Linearform auf E. Die Abbildung

$$\begin{array}{rcl} E \times E & \to & K \\ (\alpha, \beta) & \mapsto & \mathrm{Sp}_{E/K}(\alpha\beta) \end{array}$$

ist eine symmetrische K-Bilinearform auf E.

(ii) Die Norm $N_{E/K} : E^\times \to K^\times$ ist ein Gruppenhomomorphismus auf den Einheitengruppen.

(iii) Ist $P_{E/K}(\alpha) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ das charakteristische Polynom, so gilt

$$\begin{array}{rcl} \mathrm{Sp}_{E/K}(\alpha) & = & -a_{n-1} \\ N_{E/K}(\alpha) & = & (-1)^n a_0\,. \end{array}$$

Lemma 1.7.3.

(i) Sei F ein Zwischenkörper von E/K und $m := [E : F]$. Dann gilt für $\alpha \in F$:

$$\begin{aligned} P_{E/K}(\alpha) &= P_{F/K}(\alpha)^m \\ \mathrm{Sp}_{E/K}(\alpha) &= m\ \mathrm{Sp}_{F/K}(\alpha) \\ N_{E/K}(\alpha) &= N_{F/K}(\alpha)^m \end{aligned}$$

(ii) Sei E/K eine endliche Erweiterung, $\alpha \in E$ und $f = \min_K(\alpha) = X^n + \ldots + a_0$ das Minimalpolynom. Setze $m := [E : K(\alpha)]$. Dann gilt

$$\begin{aligned} P_{K(\alpha)/K}(\alpha) &= f \\ P_{E/K}(\alpha) &= f^m \\ \mathrm{Sp}_{E/K}(\alpha) &= -ma_{n-1} \\ N_{E/K}(\alpha) &= (-1)^{mn} a_0^m \end{aligned}$$

Dies erlaubt es, Norm und Spur eines Elements $\alpha \in E$ aus seinem Minimalpolynom abzulesen.

Beweis.

(i) folgt daraus, dass $E \cong F^m$ als K-Vektorraum.

(ii) Da das Minimalpolynom f das charakteristische Polynom $P_{K(\alpha)/K}(\alpha)$ teilt, und

$$\text{grad } f = [K(\alpha) : K] = \text{grad } P_{K(\alpha)/K}(\alpha)$$

folgt $f = P_{K(\alpha)/K}$ und aus (i) die weiteren Behauptungen. □

Satz 1.7.4.
Sei E/K eine endliche und separable Körpererweiterung, C ein algebraischer Abschluss von E und setze $G = Hom_K(E, C)$. Dann gilt für $\alpha \in E$

(i) $\mathrm{Sp}_{E/K}(\alpha) = \sum_{\sigma \in G} \sigma\alpha$,

(ii) $N_{E/K}(\alpha) = \prod_{\sigma \in G} \sigma\alpha$.

Beweis.
Wir setzen $F = K(\alpha)$ und $n = [F : K]$. Da E/K separabel ist, können wir nach I.4.2.10 (iii) schreiben

$$\mathrm{Hom}_K(K(\alpha), C) = \{\rho_1, \ldots, \rho_n\}$$

und es gilt

$$\min_K(\alpha) = \prod_i (X - \rho_i\alpha)\,.$$

Nach Lemma 1.7.3 folgt

$$\begin{aligned} \mathrm{Sp}_{K(\alpha)/K}(\alpha) &= -a_{n-1} = \sum_{i=1}^{n} \rho_i\alpha \\ N_{K(\alpha)/K}(\alpha) &= (-1)^N a_0 = \prod_{i=1}^{n} \rho_i\alpha \ . \end{aligned}$$

Zu jedem Homomorphismus ρ_i gibt es nach I.4.2.10 $m = [E : F]$ Fortsetzungen zu einem Morphismus $\sigma \in G = \mathrm{Hom}_K(E, C)$. Also folgt

$$\sum_{\sigma\in G} \sigma\alpha = m \sum_{i=1}^{n} \rho_i\alpha = \mathrm{Sp}_{E/K}(\alpha)\,,$$

wobei die letzte Gleichung aus Lemma 1.7.3 (i) folgt.

Ebenso rechnet man für die Norm

$$\prod_{\sigma\in G} \sigma\alpha = \left(\prod_{i=1}^{n} \rho_i\alpha\right)^m = (N_{K(\alpha)/K}(\alpha))^m = N_{E/K}(\alpha)\,. \qquad \square$$

Bemerkung 1.7.5.
Es gilt der folgende Schachtelungssatz: sei E/K eine endliche Körpererweiterung, F ein Zwischenkörper. Dann gilt

$$\begin{aligned} \mathrm{Sp}_{E/K} &= \mathrm{Sp}_{F/K} \circ \mathrm{Sp}_{E/F} \\ N_{E/K} &= N_{F/K} \circ N_{E/F} \end{aligned}$$

Beweis: ausgelassen.

Satz 1.7.6.
Sei E/K eine endliche separable *Körpererweiterung. Dann ist die Spur $\mathrm{Sp}_{E/K} : E \to K$ surjektiv und die symmetrische Bilinearform*

$$\begin{aligned} E \times E &\to K \\ (\alpha, \beta) &\mapsto \mathrm{Sp}(\alpha\beta) \end{aligned}$$

ist nicht ausgeartet, d.h. aus $\mathrm{Sp}(\alpha\beta) = 0$ für alle $\alpha \in E$ folgt $\beta = 0$.

Beweis.

Da $\mathrm{Sp}_{E/K}$ eine K-Linearform ist, reicht es zu zeigen, dass $\mathrm{Sp}_{E/K} \neq 0$. Aber würde

$$\sum_{\sigma} \sigma\alpha = 0$$

für alle $\alpha \in E$, gälten, so stünde dies im Widerspruch zur linearen Unabhängigkeit der Charaktere $\sigma \in \mathrm{Hom}_K(E, C)$, die aus Satz 1.5.5 folgt.

Ist $\beta \neq 0$ und wäre $\mathrm{Sp}_{E/K}(\alpha\beta) = 0$ für alle $\alpha \in E$, so gälte $\mathrm{Sp}_{E/K}(\gamma) = 0$ für alle $\gamma \in E$, Widerspruch. □

Satz 1.7.7 (Satz 90 von Hilbert)**.**
Sei E/K endlich galoisch mit zyklischer Galoisgruppe $G = G(E/K)$, also $G = \langle\sigma\rangle$. Dann ist für $\gamma \in E^\times$ äquivalent

(i) $N_{E/K}(\gamma) = 1$

(ii) Es gibt ein $\alpha \in E^\times$ mit $\gamma = \frac{\alpha}{\sigma\alpha}$.

Beweis.

(ii) ⇒ (i) Aus der Multiplikativität der Norm folgt $N_{E/K}\left(\frac{\alpha}{\sigma\alpha}\right) = \frac{N_{E/K}(\alpha)}{N_{E/K}(\sigma\alpha)} = 1$.

(i) ⇒ (ii) Sei $n = |G|$. Wegen der linearen Unabhängigkeit der Charaktere $1, \sigma, \ldots \sigma^{n-1}$ ist für jedes $\gamma \in E^\times$ die K-lineare Selbstabbildung von E

$$\mathrm{id} \; + \gamma\sigma + \gamma\sigma(\gamma)\sigma^2 + \ldots + \gamma\sigma(\gamma)\sigma^2(\gamma)\ldots\sigma^{n-2}(\gamma)\sigma^{n-1}$$

nicht identisch Null. Es gibt also ein $\Theta \in E^\times$, so dass

$$\alpha := \Theta + \gamma\sigma(\Theta) + \gamma\sigma(\gamma)\sigma^2(\Theta) + \ldots + \gamma\sigma(\gamma)\ldots\sigma^{n-2}(\gamma)\sigma^{n-1}(\Theta) \neq 0\,.$$

Wenden wir darauf die Abbildung $\gamma\sigma$ an, so folgt

$$\begin{aligned} \gamma\sigma(\alpha) &= \gamma\sigma(\Theta) + \gamma\sigma(\gamma)\sigma^2(\Theta) + \ldots + \gamma\sigma(\gamma)\ldots\sigma^{n-1}(\gamma)\sigma^n(\Theta) \\ &= \alpha - \Theta + N_{E/K}(\gamma)\cdot\Theta\,, \end{aligned}$$

wobei wir die Definition von α und die Gleichung $\sigma^n = 1$ ausgenutzt haben. Aus der Bedingung $N_{E/K}(\gamma) = 1$ folgt die gewünschte Gleichung $\gamma\sigma(\alpha) = \alpha$. □

Korollar 1.7.8. *Sei K ein* endlicher *Körper und E/K eine endliche Körpererweiterung. Dann ist die Normabbildung*

$$N_{E/K} : E^\times \to K^\times$$

surjektiv.

Beweis.

E/K ist galoisch mit zyklischer Galoisgruppe $G = G(E/K) = \langle\sigma\rangle$. Betrachte den Gruppenhomomorphismus

$$\begin{array}{rcl} \delta : E^\times & \to & E^\times \\ \alpha & \mapsto & \frac{\alpha}{\sigma\alpha} \end{array}$$

und die Normabbildung

$$N_{E/K} : E^\times \to K^\times$$

Es ist $\ker\delta = \{\alpha \in E^\times | \sigma\alpha = \alpha\} = K^\times$, wobei die letzte Gleichheit aus dem Hauptsatz der Galoistheorie folgt. Nach Satz 1.7.7 gilt andererseits $\ker N_{E/K} = \operatorname{im}\delta$. Wir kombinieren alle Gleichungen und erhalten

$$|E^\times| = |\operatorname{im}\ \delta|\ |\ker\delta| \ = \ |\operatorname{im}\ N|\ |\ker N|$$

mithin

$$|\operatorname{im}\ N| = |\ker\delta| = |K^\times|\ . \qquad \square$$

Es gibt auch eine additive Version des Satzes 90 von Hilbert:

Bemerkung 1.7.9.

(i) Sei E/K eine endliche galoische Körpererweiterung mit zyklischer Galoisgruppe, $G = G(E/K) = \langle\sigma\rangle$. Dann ist für $\gamma \in E$ äquivalent

(i) $\operatorname{Sp}_{E/K}(\gamma) = 0$

(ii) Es gibt ein $\alpha \in E$ mit $\gamma = \sigma\alpha - \alpha$.

(ii) Für allgemeinere Galoisgruppen G gilt immer noch:

$$Ker\ \operatorname{Sp}_{E/K} = \Big\{ \sum_{\substack{\tau\in G \\ \text{endlich.}}} \tau\alpha - \alpha \Big\}$$

Beweis: ausgelassen, benutzt Normalbasen.

1.8 Reine Gleichungen, Wurzeln

Definition 1.8.1.
Sei K ein Körper. Dann heißt das Polynom

$$f(X) = X^n - \gamma \quad \in K[X]$$

für $\gamma \neq 0$ ein reines Polynom über K. Seine Nullstellen in einem Zerfällungskörper von f über K heißen n-te Wurzeln von γ. Da $f'(X) = nX^{n-1}$ gilt, ist f genau dann separabel, wenn die Charakteristik von K die Zahl n nicht teilt.

Satz 1.8.2.
Sei K ein Körper, der eine primitive n-te Einheitswurzel enthält. (Das heißt insbesondere, dass die Charakteristik von K die Zahl n nicht teilen kann.) Sei $\gamma \in K^\times$. Dann ist die Galoisgruppe G des reinen Polynoms $X^n - \gamma$ zyklisch und $|G|$ teilt n. Ist α eine n-te Wurzel von γ, so ist

$$|G| = \min\{d \in \mathbb{N} | \alpha^d \in K\} =: d_0$$

und $X^{d_0} - \alpha^{d_0}$ ist das Minimalpolynom von α über K. $K(\alpha)$ ist der Zerfällungskörper E von $X^n - \gamma$ über K.

Beweis.

- Sei α eine feste Nullstelle von $X^n - \gamma$. Dann erhält man alle Nullstellen von $X^n - \gamma$ in der Form $\alpha\zeta$, wenn ζ alle n-ten Einheitswurzeln durchläuft. Also gilt $E = K(\alpha)$.
- Sei $\sigma \in G$. Dann ist auch $\sigma\alpha$ eine Nullstelle von $X^n - \gamma$, also gilt $\sigma(\alpha) = \alpha\zeta$ mit $\zeta = \zeta(\sigma)$ einer n-ten Einheitswurzel. Wir bekommen so eine Injektion in die Gruppe $W_n(K)$ der n-ten Einheitswurzeln:
$$\begin{array}{ccc} G & \to & W_n(K) \\ \sigma & \mapsto & \frac{\sigma(\alpha)}{\alpha} =: \zeta(\sigma)\,, \end{array}$$
denn $\zeta(\sigma) = 1$ impliziert $\sigma(\alpha) = \alpha$, also auch $\sigma = \mathrm{id}$. Dies ist ein Gruppenhomomorphismus, denn es gilt
$$\rho\sigma(\alpha) = \rho(\zeta(\sigma)\alpha) = \zeta(\sigma)\zeta(\rho)\alpha = \zeta(\rho\sigma)\alpha\,.$$
G ist also Untergruppe der zyklischen Gruppe $W_n(K)$ der Ordnung n und daher zyklisch. Die Ordnung $|G|$ teilt n.

- Sei also $G = \langle\sigma\rangle$, $\mathrm{ord}(\sigma) = d_0$. Dann ist $\zeta(\sigma)$ eine primitive d_0-te Einheitswurzel. Denn sei $\zeta(\sigma)$ primitive $\tilde{d}$-te Einheitswurzel. Dann gilt
$$\sigma(\alpha^{\tilde{d}}) = \sigma(\alpha)^{\tilde{d}} = \zeta(\sigma)^{\tilde{d}}\alpha^{\tilde{d}} = \alpha^{\tilde{d}}\,,$$
also liegt $\alpha^{\tilde{d}} \in K$. Liegt umgekehrt $\alpha^d \in K$, so folgt
$$\alpha^d = \sigma(\alpha^d) = \zeta(\sigma)^d\alpha^d\,,$$
also gilt $\zeta(\sigma)^d = 1$, mithin teilt $\tilde{d}$ die Zahl d. Es folgt $d = \tilde{d} = d_0$.
- Schließlich gilt $\min_K(\alpha) = X^{d_0} - \alpha^{d_0}$, denn α ist Nullstelle dieses Polynoms und
$$\mathrm{grad}\,\min_K(\alpha) = [K(\alpha) : K] = [E : K] = |G| = d_0 \qquad \square$$

Wir zeigen auch eine Umkehrung dieses Satzes:

Satz 1.8.3.
Sei E/K eine endliche galoische Körpererweiterung mit zyklischer Galoisgruppe. Man sagt dann kurz, E/K sei zyklisch. Sei $n = |G(E/K)|$ und enthalte K eine primitive n-te Einheitswurzel. Dann entsteht E aus K durch Adjunktion einer n-ten Wurzel eines Elements aus K, d.h. $E = K(\alpha)$ mit α Nullstelle von $X^n - \gamma \in K[X]$.

Beweis.

- Sei σ ein Erzeuger von $G(E/K)$. Nach Voraussetzung enthält K eine primitive n-te Einheitswurzel ζ. Wegen $N_{E/K}(\zeta) = 1$, gibt es nach nach dem Satz 90 von Hilbert 90 (1.7.7) ein Element $\alpha \in E$ mit
$$\frac{\sigma\alpha}{\alpha} = \zeta\,.$$
Nun gilt
$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n\,,$$
also ist $\gamma := \alpha^n \in K$. Damit ist α Nullstelle des Polyoms $X^n - \gamma \in K[X]$.
- Außerdem hat α genau n Konjugierte, die wegen der Zyklizität der Galoisgruppe von der Form $\sigma^i(\alpha) = \zeta^i\alpha$ sind. Sie liegen alle im Körper $K(\alpha)$. Also ist die Körpererweiterung $K(\alpha)/K$ galoisch und $X^n - \gamma$ das Minimalpolynom von α. Daher gilt
$$[K(\alpha) : K] = n = |G| = [E : K]\,,$$
woraus $E = K(\alpha)$ folgt.

Die folgenden Bemerkungen werden wir nicht beweisen:

Bemerkungen 1.8.4.

(i) Über einem beliebigen Körper K kann man die Irreduzibilität des Polynoms $f = X^n - \gamma$ mit $\gamma \in K^\times$ untersuchen. Man kann zeigen, dass f genau dann irreduzibel ist, wenn

(a) für jeden Primteiler q von n das Element γ keine q-te Potenz in $K^\times$ ist, $\gamma \notin K^{\times q}$

(b) sollte 4 die Zahl n teilen, das Element γ auch nicht von der Form $\gamma = -4\lambda^4$ mit $\lambda \in K$ ist.

(ii) In Satz 1.8.2 und Satz 1.8.3 musste angenommen werden, dass der Körper K eine primitive Einheitswurzel enthält. Ist $p = \operatorname{char} K > 0$ und teilt p die Gruppenordnung n, so ist dies nicht erfüllbar. Zumindest für den Fall $n = p$ kann man dann den folgenden Satz heranziehen (Artin-Schreier), bei dem man die reinen Polynome durch andere Polynome ersetzt:

Sei E/K eine zyklische Erweiterung eines Körpers K der Charakteristik p vom Grad p. So entsteht E aus K durch Adjunktion einer Nullstelle eines Polynoms der Gestalt

$$X^p - X - \gamma \in K[X]\,.$$

Sei umgekehrt $f(X) = X^p - X - \gamma \in K[X]$ und E Zerfällungskörper von f über K. Dann gilt $E = K$ oder f ist irreduzibel über K und E/K ist zyklisch vom Grad p.

(iii) In der Kummertheorie wird die in diesem Kapitel skizzierte Theorie auf die gleichzeitige Adjunktion mehrerer Wurzeln erweitert. Wir skizzieren die Kernaussage dieser Theorie ohne Beweis.

Wir fixieren eine natürliche Zahln n. Der Körper K enthalte wieder eine primitive n-te Einheitswurzel. Sei

$$\mathcal{U}_n = \{A \subseteq K^\times \quad \textit{Untergruppe} \quad | K^{\times n} \subseteq A\}$$

und C ein algebraischer Abschluss von K. Sei ferner

$$\begin{aligned} \mathcal{Z}_n(K) \;=\; & \{E \subset C, E/K \quad \textit{galoisch,} \quad G(E/K) \\ & \textit{abelsch, alle Elemente von } E \textit{ haben einen Grad,} \\ & \textit{der } n \textit{ teilt}\} \end{aligned}$$

Dann gilt:

(a) *Die Abbildung* $A \mapsto E_A := K\Big(\sqrt[n]{A}\Big)$ *ist eine Bijektion von* $\mathcal{U}_n$ *auf* $\mathcal{Z}_n(K)$.

(b) *Die Körpererweiterung* E_A/K *ist endlich, dann und nur dann, wenn die Quotientengruppe* $A/K^{\times n}$ *endlich ist.*
In diesem Fall sind die Galoisgruppe $G(E_A/K)$ *und die Quotientengruppe* $A/K^{\times n}$ *isomorph, aber nicht natürlich isomorph. Eine natürliche Isomorphie besteht zwischen* $G(E_A/K)$ *und der Charaktergruppe von* $A/K^{\times n}$.

1.9 Auflösbare Körpererweiterungen

Motivation 1.9.1.
Sei K *ein Körper, dessen Charakteristik ungleich zwei ist. Wie schon in der Schule betrachten wir das normierte Polynom*

$$f(X) = X^2 + pX + q \in K[X] \tag{13}$$

mit Koeffizienten p *und* q. *In einem Zerfällungskörper* E *von* f *über* K *lassen sich die Nullstellen von* f *darstellen als*

$$-\frac{p}{2} \pm \sqrt{d}, \quad d = \frac{p^2}{4} - q \quad \sqrt{d} \in E\,. \tag{14}$$

Im 16. Jahrhundert fand man ähnliche Ausdrücke für die Nullstellen eines kubischen Polynoms

$$f(X) = X^3 + aX^2 + bX + c$$

durch geeignete Wurzeln (Cardano). Für $\operatorname{char} K \neq 3$ *macht man zunächst die Substitution*

$$g(X) := f\Big(X - \frac{a}{3}\Big)$$

und erhält ein Polynom der Form

$$g(X) = X^3 + pX + q \in K[X]\,.$$

Dieses Polynom g *hat für* $\operatorname{char} K \neq 2, 3$ *die Nullstellen*

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} \quad + \quad \sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 - \Big(\frac{p}{3}\Big)^3}}$$

(mit geeigneter Interpretation der Wurzeln).

Ebenso konnten Polynome vierten Grades behandelt werden. 1826 zeigte Abel, dass für die Nullstellen beliebiger Polynome von Grad ≥ 5 *keine solchen Auflösungsformeln durch Wurzeln existieren. Dies führte zu den Untersuchungen von Galois.*

Definition 1.9.2.

(i) Sei F/K eine Körpererweiterung. Man sagt, F entstehe aus K durch sukzessive Adjunktion von Radikalen der Exponenten $n_1, \dots n_r$, wenn es eine Kette

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = F$$

von Zwischenkörpern K_i von F/K gibt, so dass K_i aus K_{i-1} durch Adjunktion einer n_i-ten Wurzel (auch ein Radikal vom Exponenten n_i genannt) entsteht. F/K heißt dann Radikalerweiterung.

(ii) Eine Körpererweiterung E/K heißt durch Radikale (der sukzessiven Exponenten n_i) auflösbar, wenn es eine Radikalerweiterung F/K (der sukzessiven Exponenten n_i) gibt mit $E \subseteq F$.

(iii) Ein Polynom $f \in K[X]$ heißt durch Radikale auflösbar, wenn es eine Körpererweiterung E/K gibt, die durch Radikale auflösbar ist, und f über E in Linearfaktoren zerfällt.

Bemerkungen 1.9.3.

(i) Jede Radikalerweiterung entsteht offenbar auch durch sukzessive Adjunktion von Radikalen von Primzahlexponenten.

(ii) Seien F_1, F_2 Zwischenkörper einer Erweiterung C/K und F_1F_2 das Kompositum in C. Ist F_1/K Radikalerweiterung, so auch F_1F_2/F_2. Sind F_1, F_2 beide Radikalerweiterungen über K, so ist auch F_1F_2/K Radikalerweiterung. Entsprechendes gilt für Erweiterungen, die durch Radikale auflösbar sind.

(iii) Ist F/K Radikalerweiterung (bzw. durch Radikale auflösbar), so gilt dies auch für die normale Hülle F' von F/K. Denn F' ist nach Satz 1.1.14 das Kompositum aller zu F über K konjugierten Körper. Deshalb kann man (ii) anwenden.

(iv) Sei $f \in K[X]$ irreduzibel, E/K eine durch Radikale auflösbare Erweiterung, in der f eine Nullstelle besitzt. Dann ist wegen (iii) das Polynom f durch Radikale auflösbar.

(v) Sei F/K eine galoische Radikalerweiterung, $G = G(F/K)$. Sei

$$K = K_0 \subsetneqq \cdots \subsetneqq K_r = F$$

eine Körperkette, von der wir nach (i) voraussetzen, dass

$$K_i = K_{i-1}(\alpha_i)$$

mit $(\alpha_i)^{p_i} \in K_i$ und p_i prim. Da F/K separabel ist, ist K_i/K_{i-1} separabel, also sind alle Primzahlen p_i von der Charakteristik von K verschieden. Wir setzen $n := p_1 \dots p_r$; dann existiert im algebraischen Abschluss von K eine primitive n-te Einheitswurzel ζ.

Wir nehmen nun zusätzlich an, dass diese Einheitswurzel in K liegt, $\zeta \in K$. Nach Satz 1.8.2 ist dann K_i/K_{i-1} zyklisch vom Grad p_i. Der Hauptsatz der Galoistheorie garantiert nun die Existenz einer Kette von Untergruppen der Galoisgruppe

$$G = H_0 > H_1 > \ldots > H_r = \{1\}\,,$$

so dass $H_i = G(F/K_i)$ ein Normalteiler von $G(F/K_{i-1})$ ist und so dass für den Quotienten gilt

$$H_{i-1}/H_i = G(K_i/K_{i-1}) \cong \mathbb{Z}_{p_i}\,.$$

Also ist die Galoisgruppe G auflösbar, vgl. I.1.12 für den Begriff einer auflösbaren Gruppe.

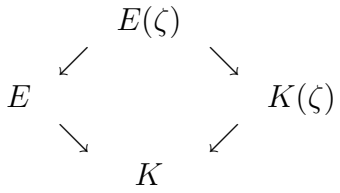
Wir wollen uns nun von der Annahme freimachen, dass K eine primitive n-te Einheitswurzel enthält.

Satz 1.9.4.
Ist E/K eine durch Radikale auflösbare Erweiterung und E' die normale Hülle von E/K, so ist die Galoisgruppe $G(E'/K)$ eine auflösbare Gruppe.

Beweis.

- Nach Bemerkung 1.9.3 (iii) ist auch die normale Hülle E' durch Radikale auflösbar. Also können wir schon ohne Einschränkung der Allgemeinheit annehmen, dass E normal ist.
- Nach Definition gibt es eine Radikalerweiterung F/K mit $E \subseteq F$. Wiederum nach Bemerkung 1.9.3 (iii) dürfen wir auch F auch als normal annehmen. Da die Restriktionsabbildung $\mathrm{Hom}_K(F,F) \twoheadrightarrow \mathrm{Hom}_K(E,E)$ surjektiv ist, reicht es zu zeigen, dass die Galoisgruppe $G(F/K)$ auflösbar ist. Die Galoisgruppe $G(E/K)$ ist dann als Quotient einer auflösbaren Gruppe auch auflösbar.
- Wir können uns also auf den Fall zurückziehen, wenn E/K eine normale Radikalerweiterung ist. Nach Bemerkung 1.9.3 (i) entsteht E aus K durch sukzessive Adjunktion von Radikalen der Primzahlexponenten $p_1, \ldots, p_r$.

- Sei n das Produkt aller derjenigen p_i, die von der Charakteristik von K verschieden sind, $n := \prod p_i$, und sei ζ eine primitive n-te Einheitswurzel in einem algebraischen Abschluss C von K.
  Betrachte das Diagramm von Körpererweiterungen:



  Offenbar ist die Körpererweiterung $E(\zeta)/K$ normal, da sie durch Adjunktion von ζ aus der normalen Körpererweiterung E/K hervorgegangen ist. Wir wissen schon, dass die Galoisgruppe $G(K(\zeta)/K)$ abelsch, also auflösbar ist. Es reicht daher aus, die Auflösbarkeit der Gruppe $G(E(\zeta)/K(\zeta))$ zu zeigen. Denn wir haben eine exakte Sequenz

$$0 \to G(E(\zeta)/K(\zeta)) \to G(E(\zeta)/K) \to G(K(\zeta)/K) \to 0\,,$$

  aus der folgt, dass $G(E(\zeta)/K)$ als Erweiterung von auflösbaren Gruppen auslösbar ist. Damit ist aber auch $G(E/K)$ als Quotient der auflösbaren Gruppe $G(E(\zeta)/K)$ auflösbar.
  Es kann also zusätzlich angenommen werden, dass die Einheitswurzel ζ in K liegt. Ist E/K galoisch, sind wir nach Bemerkung 1.9.3 (v) fertig.

- Im allgemeinen Fall führen wir den Beweis durch Induktion nach der Zahl r der Exponenten. Für $r = 0$ ist nichts zu beweisen. Sei also $r > 0$, $K_1 \neq K$. Ist $p_1 \neq \text{char } K$, so ist

$$G(K_1/K) \cong \mathbb{Z}_{p_1}\,.$$

  Ist $p_1 = \text{char } K$, so zeigt man mit Methoden, die wir nicht in dieser Vorlesung entwickelt haben, dass die Galoisgruppe trivial ist, $G(K_1/K) = 1$. In jedem Fall folgt, dass K_1/K normal ist und die Gruppe $G(K_1/K)$ auflösbar ist. Nach Induktionsannahme ist $G(E/K_1)$ auflösbar. Wegen der exakten Sequenz

$$0 \to G(E/K_1) \to G(E/K) \to G(K_1/K) \to 0$$

  ist auch $G(E/K)$ auflösbar. □

Wir zeigen auch noch eine Umkehrung dieses Satzes:

Satz 1.9.5.
Sei die Körpererweiterung E/K endlich und E' die normale Hülle von E/K. Ist die Galoisgruppe $G(E'/K)$ auflösbar von einer Ordnung prim zu char K, so ist E/K durch Radikale auflösbar.

Beweis.

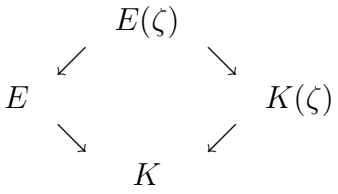
- Wie im Beweis von Satz 1.9.4 können wir wieder annehmen, dass E normal ist, $E = E'$. Sei E_s die separable Hülle von K in E. Man kann zeigen (ohne Beweis):

  — Die Körpererweiterung E/E_s ist stets durch Radikale auflösbar.

  — Für die Galoisgruppen gilt $G(E/K) = G(E_s/K)$ und E_s/K ist normal.

  Also dürfen wir zusätzlich annehmen, dass E/K galoisch ist.

- Sei also $n = |G(E/K)| = [E : K]$. Nach Voraussetzung teilt char (K) die Zahl n nicht. Also gibt es im algebraischen Abschluss von K eine primitive n-te Einheitswurzel ζ. Wir betrachten wieder das Diagramm

  Es reicht aus zu zeigen, dass $E(\zeta)/K(\zeta)$ durch Radikale auflösbar ist: denn dann ist auch $E(\zeta)/K$ durch Radikale auflösbar, weil $K(\zeta)/K$ ohnehin eine Radikalerweiterung ist. Mit $E(\zeta)/K$ ist aber erst recht E/K durch Radikale auflösbar.

  Wir stellen nun fest, dass nach dem Translationssatz 1.5.1 (ii) die Galoisgruppe $G(E(\zeta)/K(\zeta))$ eine Untergruppe der Galoisgruppe $G(E/K)$ und somit auflösbar ist.

- Wir können uns also auf die folgende Situation zurückziehen:
  Sei E/K galoisch mit auflösbarer Galoisgruppe $G(E/K)$ und sei $\zeta \in K$ eine primitive $[E : K]$-te Einheitswurzel.

  Wir finden eine Kette von Untergruppen der Galoisgruppe

  $$G(E/K) = G = H_0 \geq H_1 \geq \cdots \geq H_r = \{1\},$$

  mit H_i normal in H_{i-1} und Quotienten H_{i-1}/H_i zyklisch von Primzahlordnung. Sei

  $$K = K_0 \leq K_1 \leq \cdots \leq E$$

die entsprechende Kette von Zwischenkörpern. Die Körpererweiterungen K_i/K_{i-1} sind galoisch und zyklisch von Primzahlordnung p_i.

Da p_i die Ordnung n teilt, enthält K_{i-1} eine primitive p_i-te Einheitswurzel. Nach Satz 1.8.3 entsteht dann aber K_i durch Adjunktion einer p_i-ten Wurzel. Also ist E über K durch Radikale auflösbar.

□

Satz 1.9.6.
Sei $f \in K[X]$. Dann gilt, wenn E der Zerfällungskörper von f über K ist:

(i) Wenn f durch Radikale auflösbar ist, folgt, dass die Galoisgruppe $G(E/K)$ auflösbar ist.

(ii) Ist die Galoisgruppe $G(E/K)$ auflösbar und teilt char (K) nicht die Ordnung von $G(E/K)$, so ist das Polynom f durch Radikale auflösbar.

Beweis.
Da ein Polynom f genau dann durch Radikale auflösbar ist, wenn sein Zerfällungskörper E durch Radikale auflösbar ist, folgt dies aus Satz 1.9.4 und aus Satz 1.9.5. □

Diese Sätze geben eine befriedigende Antwort auf die Frage, für welche Polynome $f \in K[X]$ die Nullstellen durch sukzessives Wurzelziehen ausgedrückt werden können. Aber in der einleitenden Motivation (1.9.1) trat eine weitergehende Frage auf: gibt es Auflösungsformeln für *alle* Polynome eines gegebenen Grades, d.h. können wir in Gleichung (13) p und q als Variablen betrachten und Formeln wie in Gleichung (14) finden?

Auch eine weitere Frage wollen wir untersuchen:
Welche endlichen Gruppen können als Galoisgruppen von galoischen Erweiterungen auftreten?
Wir werden zeigen, dass die symmetrische Gruppe S_n mit beliebigen n als Galoisgruppe einer geeigneten(!) galoischen Erweiterung auftritt. Nach dem Satz von Cayley (I.1.7.1) ist jede Gruppe isomorph zu einer Gruppe von Permutationen und tritt somit als Galoisgruppe auf. Unbekannt ist die Antwort auf die oben gestellte Frage, wenn der Grundkörper fest vorgegeben ist: man spricht vom "Umkehrproblem der Galoistheorie". Das folgende tiefliegende Resultat verdanken wir Safarevič: Jede endliche auflösbare Gruppe ist Galoisgruppe einer Erweiterung von $\mathbb{Q}$.

Unser Leitgedanke ist nun, wie in (13) die Koeffizienten des zu untersuchenden Polynoms variabel zu lassen. Wir brauchen daher einen Körper mit diesen Variablen.

Sei k ein Körper, $k(X_1, \ldots, X_n)$ der Körper der rationalen Funktionen in n Variablen $X_1 \ldots, X_n$ über k.

$$k(X_1, \ldots, X_n) = \text{Quot}\,(k[X_1, \ldots, X_n]) = \left\{ \frac{g_1}{g_2} \;\middle|\; g_1, g_2 \in k[X_1, \ldots, X_n], g_2 \neq 0 \right\}.$$

Definition 1.9.7.
Die Polynome $s_i = s_i(X_1, \ldots, X_n) \in k[X_1, \ldots X_n]$

$$\begin{aligned} s_1 &= X_1 + \ldots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_{n-1}X_n \\ s_3 &= X_1X_2X_3 + \ldots \\ s_n &= X_1X_2X_3 \ldots X_n \end{aligned}$$

heißen i-te elementarsymmetrische Funktion in den Variablen $X_1, \ldots, X_n$. *Es gilt im Polynomring* $k(X_1, \ldots X_n)[X]$ *über dem Körper* $k(X_1, \ldots X_n)$

$$f(X) = \prod_{i=1}^{n}(X - X_i) = X^n - s_1X^{n-1} + s_2X^{n-2} - \ldots (-1)^n s_n\,. \qquad (15)$$

Satz 1.9.8.
Die Permutationsgruppe S_n *kommt als Galoisgruppe einer Körpererweiterung vor.*

Beweis.

- Die symmetrische Gruppe S_n operiert in natürlicher Weise auf dem Polynomring $k[X_1, \ldots, X_n]$ in n Variablen und somit auf rationalen Quotientenkörper $k(X_1, \ldots, X_n)$ in n Variablen: für eine Permutation $\sigma \in S_n$ setze $\sigma h(X_1, \ldots, X_n) := h(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Dann ist
$$\begin{array}{ccc} k[X_1, \ldots, X_n] & \to & k[X_1, \ldots, X_n] \\ h & \mapsto & \sigma h \end{array}$$
ist ein Isomorphismus von k-Algebren, der sich eindeutig auf den Quotientenkörper $k(X_1, \ldots, X_n)$ fortsetzen lässt.
- Wir setzen $F := k(X_1, \ldots, X_n)$ und fassen die Permutationsgruppe S_n als Untergruppe der Galoisgruppe $G(F/K)$ auf. Nun operiert S_n durch Operation auf den Koeffizienten auf dem Polynomring $F[X]$. Wir finden für $\sigma \in S_n$ und f wie in (15)
$$\sigma f = \prod_{i=1}^{n}(X - X_{\sigma i}) = \prod_{i=1}^{n}(X - X_i) = f\,.$$

Also liegen die Koeffizienten von f im Fixkörper

$$F^{S_n} = k(X_1, \ldots, X_n)^{S_n} .$$

Nun bemerken wir, dass wir f auch als Polynom mit Koeffizienten im Körper $k(s_1, \ldots, s_n)$ auffassen dürfen und der rationale Funktionenkörper $k(X_1, \ldots, X_n)$ der Zerfällungskörper des separablen Polynoms f über $k(s_1, \ldots, s_n)$ ist. Also ist die Körpererweiterung $k(X_1, \ldots, X_n)/k(s_1, \ldots, s_n)$ galoisch.

- Es gilt
$$G(k(X_1, \ldots, X_n)/k(s_1 \ldots, s_n)) \cong S_n .$$
Denn jedes Element σ der Galoisgruppe bewirkt eine Permutation der Nullstellen von f und jede Permutation aus S_n ist umgekehrt Element der Galoisgruppe. Also kommt die Permutationsgruppe S_n als Galoisgruppe einer Körpererweiterung vor. □

Korollar 1.9.9.

(i) Eine rationale Funktion $r \in k(X_1, \ldots, X_n)$ ist genau dann symmetrisch, d.h. es gilt $\sigma r = r$ für alle $\sigma \in S_n$, wenn r eine rationale Funktion in den elementarsymmetrischen Funktionen s_i ist, $r \in k(s_1, \ldots, s_n)$.

(ii) Das Polynom $f = \prod_{i=1}^{n} X - X_i$ aus (15) ist irreduzibel über $k(s_1 \ldots, s_n)$.

Beweis.

(i) Eine rationale Funktion $r \in k(X_1, \ldots, X_n)$ ist genau dann symmetrisch, wenn $r \in k(X_1, \ldots, X_n)^{S_n} = k(s_1, \ldots, s_n)$.

(ii) Da die Permutationsgruppe S_n transitiv auf den Nullstellen des separablen Polynoms f operiert, können wir Satz 1.2.19 anwenden.

Jetzt haben wir die Hilfsmittel bereit, um Variablen in den Koeffizienten eines Polynoms in X zu behandeln.

Definition 1.9.10.
Sei k ein Körper und $K = k(u_1, \ldots, u_n)$ der rationale Funktionenkörper über k in n Variablen. Das Polynom

$$g(X) = X^n - u_1 X^{n-1} + u_2 X^{n-2} - \ldots (-1)^n u_n \in K[X]$$

heißt das allgemeine Polynom n-ten Grades über k.

Satz 1.9.11.
Das allgemeine Polynom n-ten Grades über k ist separabel. Es ist irreduzibel über dem Körper K seiner Koeffizienten. Seine Galoisgruppe heißt Galoisgruppe der allgemeinen Gleichung n-ten Grades über k und ist isomorph zur Permutationsgruppe S_n.

Beweis.

- Sei E der Zerfällungskörper des Polynoms g über K:

$$g(X) = \prod_{i=1}^{n}(X - x_i) \in E[X] \quad \text{mit} \quad x_i \in E\,.$$

Dann ist

$$E = K(x_1, \ldots, x_n) = k(x_1, \ldots, x_n)$$

da $u_i := s_i(x_1, \ldots, x_n)$ schon im Körper $k(x_1, \ldots, x_n)$ liegt.

- Wir wollen zeigen, dass der Zerfällungskörper E isomorph ist zum rationalen Funktionenkörper über k in n Variablen. Dazu betrachten wir den Polynomring $k[X_1, \ldots, X_n]$. Sei

$$\varphi : k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$$

der eindeutig bestimmte k-Algebrenhomomorphismus mit $\varphi(X_i) = x_i$. Für diesen Homomorphismus gilt

$$s_i = s_i(X_1, \ldots, X_n) \mapsto s_i(x_1, \ldots, x_n) = u_i\,.$$

Also haben wir einen k-Algebrenisomorphismus

$$k[s_1, \ldots, s_n] \xmapsto{\sim} k[u_1, \ldots, u_n]$$

mit Umkehrabbildung $u_i \mapsto s_i$, der natürlich einen Isomorphismus der Quotientenkörper induziert:

$$\tilde{\varphi} : K' := k(s_1, \ldots, s_n) \xrightarrow{\sim} K = k(u_1, \ldots, u_n)\,.$$

Wir behaupten, dass auch φ auf dem großen Polynomring $k[X_1, \ldots, X_n]$ ein Isomorphismus ist. Surjektivität ist klar, sei also $h \in k[X_1, \ldots, X_n]$ mit der Eigenschaft, dass Einsetzen der $x_i \in E$ in h Null ergibt, $h(x_1, \ldots, x_n) = 0$. Betrachte

$$N(h) := \prod_{\sigma \in S_n} \sigma h = h \prod_{\sigma \neq e} \sigma h \in k[X_1, \ldots, X_n]$$

Sicher ist $N(h)^\sigma = N(h)$ für alle $\sigma \in S_n$, also ist $N(h) \in k(s_1, \ldots, s_n)$. Da $h \in \ker \varphi$, ist auch $N(h) \in \ker \varphi$. Da aber $\tilde{\varphi}$ ein Isomorphismus ist, folgt $h = 0$. Also haben wir Injektivität gezeigt. Insbesondere sind die Nullstellen $x_i \in E$ paarweise verschieden und das Polynom g ist separabel.

- Setze nun φ zu einem eindeutigen Isomorphismus $\tilde{\varphi}$ der Quotientenkörper fort:

$$\begin{array}{ccc} k(X_1, \ldots, X_n) & \xrightarrow[\varphi]{\sim} & k(x_1, \ldots, x_n) = E \\ \uparrow & & \uparrow \\ K' = k(s_1, \ldots, s_n) & \xrightarrow[\widetilde{\varphi}]{\sim} & k(u_1, \ldots, u_n) = K \end{array}$$

Hierbei gilt $\varphi(f) = g$. Wegen Korollar 1.9.9 ist dann das Polynom g irreduzibel und wegen Satz 1.9.8 ist die Galoisgruppe

$$\text{Gal}\,(g, k(u_1, \ldots, u_n)) \cong S_n\,.$$

□

Satz 1.9.12.
Sei $r \in k(X_1, \ldots, X_n)$ eine symmetrische rationale Funktion, dann gibt es genau *eine rationale Funktion $g \in k(X_1, \ldots, X_n)$, durch die man r in den elementarsymmetrischen Funktionen ausdrücken kann, $r = g(s_1, \ldots, s_n)$.*

Beweis.
$k(s_1, \ldots s_n)$ kann als rationaler Funktionenkörper in den n Variablen $s_1, \ldots, s_n$ angesehen werden, da $\widetilde{\varphi}$ im Beweis von Satz 1.9.11 ein Isomorphismus ist. Nach Korollar 1.9.9 (i) ist r genau dann symmetrisch, wenn $r \in k(s_1, \ldots s_n)$. □

Satz 1.9.13 (Abel)**.**
Das allgemeine Polynom n-ten Grades ist für $n \geq 5$ nicht durch Radikale auflösbar.

Beweis.
Nach Satz 1.9.11 ist seine Galoisgruppe die Permutationsgruppe S_n, die nach Bemerkung I.1.12.6 (ii) für $n \geq 5$ nicht auflösbar ist. Die Behauptung folgt nun aus Satz 1.9.4. □

Satz 1.9.14.
Sei k ein Körper mit char $k \neq 2, 3$. Dann ist jedes $f \in K[X]$ vom Grad $n \leq 4$ durch Radikale auflösbar.

Beweis.
Die Galoisgruppe ist als Untergruppe der auflösbaren Gruppe S_4 auflösbar. Die Behauptung folgt dann wegen $|S_4| = 24 = 2^3 \cdot 3$ aus Satz 1.9.5. □

2 Moduln

2.1 Darstellungen endlicher Gruppen

Definition 2.1.1.
Eine Darstellung einer Gruppe G über einem Körper K ist ein Paar (V, ρ) bestehend aus einem K-Vektorraum V und einem Gruppenhomomorphismus ρ in die invertierbaren K-linearen Abbildungen von V,

$$\rho : G \to \mathrm{GL}(V) := \{\varphi \in \ End_K(V), \varphi \text{ invertierbar } \}.$$

Bemerkung 2.1.2.

(i) Gegeben eine Darstellung (V, ρ), schreiben wir oft ρ_V für ρ.

(ii) Ist (V, ρ) eine Darstellung von G über K, so ist die Abbildung

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto \rho(g)v \end{aligned}$$

eine Operation der Gruppe G auf der Menge V.

(iii) Ist $G \times V \to V$ eine Operation der Gruppe G auf einem K-Vektorraum V, so dass gilt

$$g(v + w) = gv + gw \qquad g(\lambda v) = \lambda g v$$

für $v, w \in V, g \in G$ und $\lambda \in K$, so definiert

$$\rho(g)v = gv$$

eine Darstellung $\rho : G \to GL(V)$.

Eine Darstellung ist also eine "Operation auf einem Vektorraum durch lineare Abbildungen".

(iv) Jeder Vektorraum V wird eine Darstellung seiner Isomorphismengruppe $GL(V)$ durch $\rho = \mathrm{id}_{GL(V)}$.

(v) Jeder Vektorraum V wird Darstellung einer beliebigen Gruppe G durch die triviale Operation $\rho(g) = \mathrm{id}_V$ für alle $g \in G$.

(vi) Ist L/K eine Körpererweiterung, so ist L, aufgefasst als K-Vektorraum eine Darstellung von $\mathrm{Gal}(L/K)$ über K.

(vii) Eine Darstellung (V, ρ) der Gruppe $\mathbb{Z}$ angeben heißt, einen Automorphismus $A \in GL(V)$ anzugeben, nämlich $A = \rho(1)$. Dann ist $\rho(n) = A^n$.

(viii) *Darstellungen von $\mathbb{Z}/2\mathbb{Z}$ sind äquivalent zu einem Vektorraum V mit einem Automorphismus $A : V \to V$, so dass $A^2 = \mathrm{id}_V$. Konkret heißt dies, wenn die Charakteristik des Körpers K ungleich zwei ist, dass V direkte Summe der Eigenräume von A zu den Eigenwerten ± 1 ist,*

$$V = V^+ \oplus V^- .$$

Denn es gilt die Zerlegung in Eigenvektoren

$$v = \frac{1}{2}(v + Av) + \frac{1}{2}(v - Av)$$

von A. Hat dagegen der zu Grunde liegende Körper Charakteristik 2, so gibt es nur den Eigenwert 1. Wegen $A^2 = \mathrm{id}_V$ haben die Jordan–Blöcke Größen 1 oder 2. In der Tat gilt dann:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Definition 2.1.3.

(i) *Seien V, W Darstellungen einer Gruppe G über einem festen Körper K. Ein Homomorphismus von Darstellungen ist eine K–lineare Abbildung $f : V \to W$, so dass gilt*

$$f(gv) = gf(v) \quad \text{für alle } g \in G .$$

Ein Isomorphismus ist ein bijektiver Homomorphismus. Zwei Darstellungen heißen isomorph, wenn es einen Isomorphismus gibt.

(ii) *Gegeben zwei Darstellungen einer Gruppe G über einem Körper K definieren wir die direkte Summe der Darstellungen als den Vektorraum $V \oplus W$ mit der Operation $g(v, w) = (gv, gw)$.*

Ähnlich definiert man direkte Summen unendlich vieler Darstellungen.

(iii) *Eine Teilmenge $W \subset V$ einer Darstellung V heißt Unterdarstellung genau dann, wenn W ein unter G stabiler Untervektorraum ist; das heißt, dass aus $g \in G$ und $w \in W$ folgt, dass $gw \in W$.*

(iv) *Eine Darstellung V von G heißt irreduzibel oder einfach, wenn $V \neq 0$ und wenn 0 und V die einzigen Unterdarstellungen sind.*

(v) *Eine Darstellung V von G heißt unzerlegbar, wenn V nicht der Nullraum ist und es keine zwei von Null verschiedenen Unterdarstellungen $W_1, W_2 \subset V$ gibt, so dass*

$$V = W_1 \oplus W_2 .$$

Beispiele 2.1.4.

(i) Eindimensionale Darstellungen sind irreduzibel.

(ii) Ist char $K \neq 2$ so hat $\mathbb{Z}_2$ zwei irreduzible eindimensionale Darstellungen $K_\pm$. Jede Darstellung ist vollständig reduzibel, d.h. isomorph zu genau einer Darstellung der Gestalt

$$K_+^m \oplus K_-^n \quad \text{für } m, n \in \mathbb{N}\,.$$

(iii) Ist char $K = 2$, so ist die triviale Darstellung K irreduzibel und die zwei–dimensionale Darstellung P unzerlegbar, aber nicht irreduzibel. Jede endlich–dimensionale Darstellung ist isomorph zu

$$K^n \oplus P^m \quad \text{für } n, m \in \mathbb{N}\,.$$

Ziel ist die Beschreibung der Darstellungen einer Gruppe. Es ist sinnvoll, dafür Methoden in einem etwas allgemeineren Rahmen zu entwickeln.

2.2 Moduln über Ringen

Definition 2.2.1.

*(i) Sei R ein Ring mit 1, nicht notwendig kommutativ, und M eine abelsche Gruppe. M heißt R–*Linksmodul*, falls es eine Skalarmultiplikation*

$$\begin{aligned} R \times M &\to M \\ (\alpha, x) &\mapsto \alpha x \end{aligned}$$

gibt, die folgende Eigenschaften besitzt:

(i) Distributivität: $(\alpha+\beta)x = \alpha x + \beta x$, $\alpha(x+y) = \alpha x + \alpha y$

(ii) Assoziativität: $(\alpha\beta)x = \alpha(\beta x)$

(iii) Unitalität: $1x = x$

$$x, y \in M, \quad \alpha, \beta \in R\,.$$

*(ii) Analog wird ein R–*Rechtsmodul *definiert.*

(iii) Ein R–Bimodul ist ein R–Linksmodul, der auch R–Rechtsmodul ist, und für den gilt

$$(\alpha x)\beta = \alpha(x\beta) \qquad \forall\ x \in M, \alpha, \beta \in R$$

Beispiele 2.2.2.

(i) Jeder Ring R ist auch Modul über sich selbst:

$$\begin{aligned} R \times R &\to R \\ (\alpha, \beta) &\mapsto \alpha \cdot \beta \end{aligned}$$

(ii) Jede abelsche Gruppe $(G, +)$ wird zu einem $\mathbb{Z}$–Modul durch die folgende Skalarmultiplikation:

$$\begin{aligned} \mathbb{Z} \times G &\to G \\ (n, x) &\mapsto nx = \begin{cases} \underbrace{x + \ldots + x}_{n-\text{mal}} & n > 0 \\ 0 & n = 0 \\ -|n|x & n < 0\,. \end{cases} \end{aligned}$$

(iii) Ist R ein Körper, so ist jeder R–Linksmodul ein R-Vektorraum.

(iv) Wir vereinbaren die Regel "Punkt vor Strich".

(v) Wie bei Vektorräumen zeigt man

$$0_R m = 0_M \qquad \forall\ m \in M$$

und schließt $(-1)m = -m$.

Um das Beispiel in 2.2.2 (ii) genauer zu untersuchen, überlegen wir uns zunächst folgendes: für jede gegebene abelsche Gruppe $(M, +)$ bilden die Gruppenhomomorphismen $\varphi \in \text{End}\,(M)$ einen Ring, den Endomorphismenring. Die Addition in diesem Ring ist die Addition von Abbildungungen durch Addition der Funktionswerte,

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)\,.$$

Die Multiplikation im Endomorphismenring ist die Verkettung von Abbildungen, $\varphi\psi = \varphi \circ \psi$, das Einselement ist hierbei natürlich die Identität auf M. Endomorphismenringe sind im allgemeinen nicht kommutativ.

Lemma 2.2.3.
Sei M eine abelsche Gruppe und R ein Ring

(i) Ist $\varphi : R \to \text{End}\,(M)$ ein Ringhomomorphismus, so wird durch die Vorschrift

$$rm = \varphi(r)\, m$$

M zum R–Modul.

(ii) Ist M ein R–Modul, so liefert die Abbildung

$$\begin{array}{rccl} \varphi: & R & \to & Abb\ (M,M) \\ & r & \mapsto & \varphi(r) \quad mit \quad \varphi(r)m = rm \end{array}$$

einen Ringhomomorphismus.

Beweis. Übung.

Da es für jeden (unitalen) Ring E nur einen (unitalen) Ringhomomorphismus $\mathbb{Z} \to E$ gibt, trägt jede abelsche Gruppe nur eine $\mathbb{Z}$–Modulstruktur, nämlich die aus 2.2.2 (ii).

Um den Zusammenhang zu Kapitel 2.1 herzustellen, brauchen wir die folgende

Definition 2.2.4.
Sei K ein Ring und G eine Gruppe. Der Gruppenring $K[G]$ ist als abelsche Gruppe die Menge aller Abbildungen

$$f : G \to K\,,$$

die nur für endlich viele $g \in G$ von Null verschiedene Werte annehmen. Wir schreiben die Elemente auch als formale Linearkombination

$$f = \sum f(g)g \quad mit\ f(g) \in K\,.$$

Die Multiplikation im Gruppenring ist ist die Konvolution (oder Faltung):

$$\left(\sum_{g\in G} a_g g\right) \star \left(\sum_{h\in G} b_h h\right) \quad = \quad \sum_{x\in G}\left(\sum_{gh=x} a_g b_h\right) x\,.$$

Man hat einen Ringhomomorphismus

$$\begin{array}{ccl} K & \hookrightarrow & K[G] \\ a & \mapsto & ae\ , \end{array}$$

wobei e das neutrale Element von G ist, und einen Gruppenhomomorphismus

$$\begin{array}{ccl} G & \to & K[G]^\times \\ g & \mapsto & 1g \end{array}$$

der es erlaubt, G als Basis von $K[G]$ aufzufassen. Hierbei identifiziert man das Gruppenelement $g \in G$ mit der Funktion, die überall verschwindet außer auf g, wo sie Wert eins hat. Gruppenringe sind also Ringe mit einer ausgezeichneten Basis.

Lemma 2.2.5.
Sei G eine Gruppe und K ein Körper. Man erhält eine Bijektion

$$\{ \text{ Darstellungen von } G \text{ über } K\} \overset{\sim}{\Longleftrightarrow} \{K[G] - \text{Moduln } \}$$

durch Einschränkung der Operation von $K[G]$ zu Operationen von K und G einerseits und durch offensichtliche Ausdehnung auf $K[G]$ andererseits.

Beweis. Übung.

Lemma 2.2.6 (Restriktion der Skalare)**.**
Ist $\varphi : R \to S$ ein Ringhomomorphismus, so wird jeder S–Modul (und insbesondere auch S selbst) ein R–Modul durch

$$rm = \varphi(r)m\,.$$

Dies heißt Restriktion der Skalare, selbst wenn R nicht Unterring von S ist.

Zum Beispiel sei $\mathfrak{a} \subset R$ ein Ideal von R, und $\mathrm{can} : R \to R/\mathfrak{a}$, die kanonische Surjektion, dann ist der Quotient $R/\mathfrak{a}$ in natürlicher Weise R–Modul.

Lemma 2.2.7. *Übergang zu Polynomringen*
Sei k ein Körper.

(i) Ist M ein $k[X]$–Modul, so hat M durch Restriktion die Struktur eines k–Vektorraums. Die Multiplikation mit X ist eine k–lineare Abbildung $M \to M$

(ii) Ist M ein k–Vektorraum und $A : M \to M$ eine k–lineare Abbildung, so macht die Vorschrift

$$fm := f(A)m \quad \forall\ m \in M, f \in k[X]$$

M zu einem $k[X]$–Modul.

Moduln über dem Polynomring $k[X]$ über einem Körper sind also gerade k–Vektorräume mit einem k–linearen Endomorphismus.

Definition 2.2.8.
(i) Eine Abbildung $f : M \to N$ von einem R–Modul M in einen R–Modul N heißt R–linear oder R–Modulmorphismus, wenn gilt

$$\begin{aligned} f(m+m') &= f(m) + f(m') \\ f(rm) &= rf(m) \end{aligned}$$

für $m, m' \in M$ und $r \in R$. Für die Menge der R–Homomorphismen schreiben wir auch $Hom_R(M, N)$.

(ii) Ein bijektiver Homomorphismus von Moduln heißt Isomorphismus.

Beispiel 2.2.9.
Sei M ein R–Modul. So ist die Abbildung

$$\begin{aligned} M &\to Hom_R(R, M) \\ m &\mapsto (r \mapsto rm) \end{aligned}$$

ein Isomorphismus von abelschen Gruppen. Sein Inverses ordnet einem Homomorphismus $\varphi \in Hom_R(R, M)$ sein Bild auf der Eins $\varphi(1)$ zu.

Definition 2.2.10.
Sei M ein R–Linksmodul und $U \subseteq M$ eine Untergruppe. Dann heißt U Untermodul von M, falls die Skalarmultiplikation von M auf U definiert ist, d.h.

$$m \in U, \quad r \in R \quad \Rightarrow \quad rm \in U\,.$$

Bemerkung 2.2.11.

(i) Die Untergruppen einer abelschen Gruppe sind genau die $\mathbb{Z}$–Untermoduln.

(ii) Fasst man den Ring R als Modul über sich selbst auf, so sind die R–Untermoduln von R gerade die Ideale von R. Genauer gesagt sind die R-Links-Untermoduln die Linksideale, die R-Rechts-Untermoduln die Rechtsideale und die R-Bi-Untermoduln die beidseitigen Ideale.

(iii) Bild und Kern eines Modulhomomorphismus sind Untermoduln. Ebenso ist das Urbild von Idealen ein Ideal.

(iv) Ist U ein Untermodul von M, dann wird die Faktorgruppe M/U zu einem R–Modul, dem Faktormodul oder Quotientenmodul von M nach U durch die folgende Skalarmultiplikation:

$$\begin{aligned} R \times M/U &\to M/U \\ (\alpha, x + U) &\mapsto \alpha x + U \end{aligned}$$

(v) Dies soll durch das folgende Beispiel weiter illustriert werden: Sei $\mathfrak{a}$ ein Ideal von R und M ein R–Modul, so ist

$$\mathfrak{a}M = \left\{ \sum_{endl} \alpha_i x_i \;\middle|\; \alpha_i \in \mathfrak{a}, x_i \in M \right\}$$

ein Untermodul von M. $M/\mathfrak{a}M$ ist dann ein R–Modul; und sogar ein $R/\mathfrak{a}$–Modul: die Skalarmultiplikation

$$(\alpha + \mathfrak{a})(x + \mathfrak{a}M) = \alpha x + \mathfrak{a}M$$

ist wohldefiniert. Dazu betrachten wir einen konkreten Fall: der Ring $\mathbb{Z}$ der ganzen Zahlen ist natürlich ein $\mathbb{Z}$–Modul; $n\mathbb{Z}$ ist ein Ideal für jedes $n \in \mathbb{Z}$ und die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist ein $\mathbb{Z}$–Modul und sogar ein $\mathbb{Z}/n\mathbb{Z}$–Modul.

Definition 2.2.12.

(i) Sei $A \subseteq M$ Teilmenge eines R–Moduls M. Dann bezeichnet

$$\langle A \rangle = \left\{ \sum_{endl} \alpha_i a_i \;\middle|\; \alpha_i \in R, a_i \in A \right\}$$

den von A <u>erzeugten Untermodul</u> von M. Es gilt

$$\langle A \rangle = \bigcap_{\substack{U \subset M \, Untermodul \\ A \subseteq U}} U$$

d.h. $\langle A \rangle$ ist der kleinste Untermodul von M, der A enthält.

(ii) Gilt $\langle A \rangle = M$, so heißt die Menge A <u>Erzeugendensystem</u> von M. M heißt <u>endlich erzeugt</u>, falls es ein endliches Erzeugendensystem gibt.

Satz 2.2.13. *(Homomorphiesätze für Moduln)*

(i) Seien M, N R–Moduln und $f : M \to N$ ein Modulhomomorphismus, so gibt es einen kanonischen Isomorphismus

$$\begin{array}{ccc} M/\ker f & \xrightarrow{\sim} & f(M) \\ x + \ker f & \mapsto & f(x) \end{array}$$

(ii) Sind U und V Untermoduln eines Moduls M, so gilt

$$(U + V)/V \quad \xrightarrow{\sim} \quad U/(U \cap V)$$

mit $U + V = \{u + v, u \in U \text{ und } v \in V\}$. Man bestimme hierzu den Kern der Abbildung

$$u + v \quad \mapsto \quad u + U \cap V$$

(iii) Gilt $U \subseteq V \subseteq M$ mit Untermoduln, so ist V/U Untermodul von M/U und es gilt

$$(M/U)\,/\,(V/U) \quad \xrightarrow{\sim} \quad M/V\,.$$

Definition 2.2.14.

(i) Sei U ein R-Untermodul eines R-Moduls M. Dann heißt

$$Ann\,(U) = \{\alpha \in R \mid \alpha u = 0 \quad \textit{für alle } u \in U\}$$

der Annulator von U. Dies ist ein Ideal von R. Der Annulator eines Elementes $x \in M$ ist definiert als

$$Ann(x) = \{\alpha \in R \,|\, \alpha x = 0\}\,.$$

Es gilt

$$\begin{array}{rcl} R/Ann(x) & \xrightarrow{\sim} & Rx \\ \overline{\alpha} & \mapsto & \alpha x \end{array}$$

(ii) Ein Modul M heißt treu, falls $Ann\ M = (0)$ ist.

(iii) Ein Element $x \in M$ heißt Torsionselement, falls $Ann\ (x) \neq 0$ ist. Mit $Tor\ M$ wird die Menge aller Torsionselemente bezeichnet, die aber im allgemeinen kein Untermodul ist.

(iv) Ein Modul M heißt torsionsfrei, falls $Tor\ M = (0)$ ist.

Satz 2.2.15.

Ist M Modul über einem Integritätsring R, so ist $Tor\ M$ ein Untermodul von M und $M/Tor\ M$ ist torsionsfreier R–Modul.

Beweis.

Ein integrer Ring R ist per definitionem kommutativ.

- Ist daher $x \in$ Tor(M) ein Torsionselement, $\beta \in R$, so finden wir ein von Null verschiedenes $\alpha \in$ Ann (x). Dann gilt aber $\alpha(\beta x) = (\alpha\beta)x = \beta(\alpha x) = 0$. Damit ist aber auch $\beta x \in$ Tor M.
- Seien nun zwei Torsionselemente vorgegeben, $x, y \in$ Tor M. Wir finden $\alpha, \alpha' \in R\backslash\{0\}$, so dass $\alpha x = \alpha' y = 0$. Dann ist das Produkt $\alpha\alpha' \neq 0$, da R integer sein soll, und es gilt $\alpha\alpha'(x+y) = 0+0 = 0$. Also gilt auch $x + y \in$ Tor M.

- Schließlich sei $x + \text{ Tor } M \in M/\text{Tor } M$ ein Torsionselement. Wir finden wieder $\alpha \in R\backslash\{0\}$, so dass $\alpha(x + \text{Tor } M) = 0$. Da dann aber $\alpha x \in \text{ Tor } M$ liegt, gibt es $\beta \in R \setminus \{0\}$ mit $\beta\alpha x = 0$. Da R integer sein sollte, ist auch $\beta\alpha \neq 0$, also $x \in \text{ Tor } M$. Also ist der Quotient $M/\text{Tor } M$ torsionsfrei. □

Definition 2.2.16.

(i) Gegeben sei eine Familie $(M_\lambda)_{\lambda\in\Lambda}$ von Moduln über einem Ring R. Wir bilden zwei neue R–Moduln:
das <u>Produkt</u>

$$\prod_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda\}$$

und die <u>direkte Summe</u>

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda, \text{ nur endlich viele } m_\lambda \text{ sind nicht Null}\}.$$

Ihre Modulstruktur über R erhalten diese Mengen durch die komponentenweise Addition und die komponentenweise Multiplikation mit Skalaren aus R.

Offensichtlich fallen für endliche Familien, $|\Lambda| < \infty$, die Begriffe der direkten Summe und des Produkts zusammen. Beide Begriffe können auch durch universelle Eigenschaften charakterisiert werden. Hierfür führen wir die kanonische

$$\begin{array}{ccc} \textit{Injektion} & \textit{bzw.} & \textit{Surjektion} \\ i_\lambda : M_\lambda \hookrightarrow \bigoplus_{\lambda\in\Lambda} M_\lambda & & pr_\lambda : \prod_{\lambda\in\Lambda} M_\lambda \twoheadrightarrow M_\lambda \end{array}$$

ein. Die beiden universellen Eigenschaften können nun folgendermaßen formuliert werden: ist M ein beliebiger R–Modul, so gibt es die folgenden zwei Bijektionen:

$$\begin{array}{rcl} Hom\,(\oplus M_\lambda, M) & \xrightarrow{\sim} & \prod_{\lambda\in\Lambda} Hom_R(M_\lambda, M) \\ f & \mapsto & (f \circ i_\lambda)_{\lambda\in\Lambda} \\ Hom\left(M, \prod_{\lambda\in\Lambda} M_\lambda\right) & \xrightarrow{\sim} & \prod_{\lambda\in\Lambda} Hom_R(M, M_\lambda) \\ f & \mapsto & (pr_\lambda \circ f)_{\lambda\in\Lambda} \end{array}$$

(ii) *Eine Familie* $(m_\lambda)_{\lambda\in\Lambda}$ *von Elementen eines Moduls heißt* linear unabhängig *oder* frei, *wenn aus*

$$\sum_{\lambda\in\Lambda} r_\lambda m_\lambda = 0\,,$$

mit einer Familie $(r_\lambda)_{\lambda\in\Lambda}$ *von Elementen aus* R, *in der nur endlich viele Mitglieder von Null verschiedenen sind, folgt, dass* $r_\lambda = 0$ *für alle* λ.

(iii) *Eine (nicht notwendigerweise endliche) Untermenge* $S \subset M$ *heißt* Basis *des Moduls* M, *falls* S *linear unabhängig ist und* S *ein Erzeugendensystem von* M *ist,* $\langle S\rangle = M$.

(iv) *Ein Modul heißt* frei, *wenn er eine Basis besitzt.*

Bemerkung 2.2.17.

(i) *Ist* R *ein Körper und* M *ein Vektorraum, so ist* M *frei, denn jeder Vektorraum besitzt eine Basis. Es gibt aber Moduln, die nicht frei sind: sei* $R = \mathbb{Z}$ *und* $M = \mathbb{Z}_2$. *Wegen* $2\cdot\overline{1} = \overline{0}$ *ist* $\{\overline{1}\}$ *nicht linear unabhängig und wegen* $n\overline{0} = \overline{0}$ *erzeugt* $\overline{0}$ *nicht.*

(ii) *Ein* R*–Modul* M *ist frei über* S *genau dann, wenn*

$$M \cong \bigoplus_{s\in S} Rs\,.$$

In diesem Fall bildet S *eine Basis des Moduls. Man beachte, dass dann gilt* $Rs \cong R$ *als* R*–Modul.*

Beweis.

Wegen $Rs \hookrightarrow M$ *gibt es auf Grund der universellen Eigenschaft der direkten Summe einen Morphismus*

$$\bigoplus_{s\in S} Rs \longrightarrow M$$

Dieser ist surjektiv, da $\langle S\rangle = M$ *und injektiv, da* S *linear unabhängig. Die Umkehrung ist trivial.*

(iii) *Ist* M *frei und endlich erzeugt, so gibt es ein* $n \in \mathbb{N}$ *derart, dass*

$$M \cong R^n = \underbrace{R \oplus \ldots \oplus R}_{n-mal}$$

Denn sei $M = \langle x_1, \ldots, x_n \rangle$ und S eine Basis, so ist jedes x_i eindeutig darstellbar

$$x_i = \sum_{endl.} \alpha_{ij} s_j \qquad \alpha_{ij} \in R, s_j \in S\,.$$

Es gibt also eine endliche Teilmenge von S, die natürlich immer noch frei ist, und die M erzeugt. Im Gegensatz zu Vektorraumbasen können Modulbasen verschiedene Mächtigkeiten haben.

(iv) Seien Moduln $M_1, \ldots, M_m$ und $N_1, \ldots N_n$ über einem Ring R gegeben. Dann haben wir eine natürliche Identifikation

$$Hom_R(M_1 \oplus \cdots \oplus M_m, N_1 \oplus \cdots \oplus N_n) \xrightarrow{\sim} \prod_{i,j} Hom_R(M_i, N_j)\,.$$

Schreiben wir also die Elemente der direkten Summe $M_1 \oplus \cdots \oplus M_m$ als Spaltenvektoren, wobei der Eintrag in der i-ten Zeile im Modul M_i liegt, so kann man jeden Homomorphismus zwischen den direkten Summen durch eine Matrix beschreiben, deren Einträge Homomorphismen in $Hom_R(M_i, N_j)$ sind. Die Komposition der Homomorphismen wird dann durch die Multiplikation der Matrizen beschrieben.

Satz 2.2.18.
Ist R ein kommutativer *Ring mit* 1 *und M ein freier R–Modul, dann haben je zwei Basen gleiche Mächtigkeit. Diese Mächtigkeit heißt* Rang *von M. Insbesondere gilt*

$$rang_R M = n \iff M \cong R^n\,.$$

Beweis.

Da R kommutativ ist, gibt es ein maximales Ideal $\mathfrak{m}$ in R. Der Quotient $k := R/\mathfrak{m}$ ist dann ein Körper, und nach 2.2.11 (v) ist $M/\mathfrak{m}M$ ein Vektorraum über k.

Sei S eine Basis von M, also $M \cong \bigoplus_{s\in S} Rs$. Dann folgt $\mathfrak{m}M \cong \bigoplus_{s\in S} \mathfrak{m}s$, und für den Quotienten erhalten wir

$$M/\mathfrak{m}M \cong \bigoplus_{s\in S} ks$$

Also gilt $\dim_k(M/\mathfrak{m}M) = |S|$ und die Behauptung folgt aus der Unabhängigkeit der Mächtigkeit von Vektorraumbasen. □

Satz 2.2.19.
Jeder R-Modul ist ein homomorphes Bild eines freien R–Moduls.

Beweis.

Wir definieren uns einen sehr großen freien Modul mit Basis M:

$$F := \bigoplus_{m \in M} R_m \qquad R_m \cong R \quad \text{für alle } m \in M$$

Die Abbildung

$$\begin{array}{rcl} F & \to & M \\ (\alpha_m)_{m \in M} & \mapsto & \displaystyle\sum_{m \in M} \alpha_m m \end{array}$$

ist dann ein surjektiver R–Modulhomomorphismus.

Satz 2.2.20.

Seien F, M R–Moduln und sei F frei. Sei $f : M \twoheadrightarrow F$ Epimorphismus. Dann existiert ein R–Modulmorphismus

$$g : F \to M$$

mit $f \circ g = \mathrm{id}_F$ und es gilt $M \cong \ker f \oplus g(F)$. Man sagt dann, dass g spaltet.

Beweis.

Sei S eine Basis von F. Wähle ein Urbild $m_s \in M$ von $s \in S$ und definiere

$$g : F \to M$$

durch

$$\sum \alpha_i s_i \mapsto \sum \alpha_i m_{s_i} \qquad \alpha_i \in R$$

Da F ein freier Modul ist, ist dies wohldefiniert und ein Homomorphismus von Moduln. Es gilt dann

$$f \circ g(s) = f(m_s) = s \quad \text{für alle } s \in S$$

also $f \circ g = \mathrm{id}_F$. □

Nun benutzen wir g, um für jedes $x \in M$ die folgende Zerlegung zu finden:

$$x = gf(x) + (x - gf(x))\,.$$

Offenbar liegt $gf(x) \in g(F)$, außerdem gilt

$$f(x - gf(x)) = f(x) - f(x) = 0\,.$$

Also haben wir die Darstellung von M als Summe $M = \ker f + g(F)$. Sei nun $x \in \ker f \cap g(F)$. Dann gilt $x = g(y)$ für ein $y \in F$ und $0 = f(x) = fg(y) = y$, also $y = 0$, woraus $x = 0$ folgt. □

Man könnte versucht sein, freie Moduln durch die in Satz 2.2.20 beschriebene Eigenschaft zu charakterisieren. Tatsächlich gibt es aber Moduln, die diese Eigenschaft haben ohne frei zu sein. Sie bilden die wichtige Klasse der projektiven Moduln.

Korollar 2.2.21.
Ist N ein Untermodul von M, so dass M/N frei ist, so gibt es einen Untermodul N' von M, so dass

$$M = N \oplus N' \qquad N' \cong M/N\,.$$

Beweis.
Betrachte die Surjektion $f : M \twoheadrightarrow M/N$, finde mit Satz 2.2.20 einen Modulhomomorphismus $g : M/N \to M$ und setze $N' = g(M/N)$. Dann gilt $M = N \oplus N'$ und $f(N') = fg(M/N) = M/N$. Also ist $f_{|N'}$ surjektiv. Da außerdem gilt $\ker f|_{N'} = N' \cap N = 0$, ist $f_{|N'}$ ein Isomorphismus. □

2.3 Einfache Moduln und Kompositionsreihen

Definition 2.3.1.
Ein Modul M über einem Ring heißt einfach, wenn er nicht Null ist und außer den Untermoduln M und Null keine Untermoduln hat.

Lemma 2.3.2.
Sei R ein Ring, E einfacher R-Modul und M beliebiger R–Modul

(i) Jeder Homomorphismus $E \to M$ ist injektiv oder Null. Denn der Kern ist ein Untermodul von E.

(ii) Jeder Homomorphismus $M \to E$ ist surjektiv oder Null. Denn das Bild ist ein Untermodul von E.

(iii) Der Endomorphismenring $End_R(E)$ ist ein Schiefkörper, d.h. alle von Null verschiedenen Endomorphismen sind invertibel.

Definition 2.3.3.
Sei R ein Ring und M ein R–Modul. M heißt von endlicher Länge genau dann, wenn es eine endliche Kette von Untermoduln

$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0$$

gibt, so dass alle Quotientenmoduln M_i/M_{i-1} einfach sind. Eine solche Kette heißt Kompositionsreihe von M, die Moduln M_i/M_{i-1} heißen Subquotienten

der Kompositionsreihe. Die minimal mögliche Länge r einer Kompositionsreihe heißt Länge des Moduls M.

Wir sehen gleich, dass eine Version des Satzes von Jordan–Hölder für Moduln gilt. Die Subquotienten sind bis auf Reihenfolge eindeutig und heißen auch Kompositionsfaktoren des Moduls M.

Satz 2.3.4 (Jordan–Hölder)**.**

(i) Hat ein Modul M endliche Länge, so auch jeder Untermodul $N \subset M$ und jeder Quotient M/N von M und es gilt

$$\ell(M) = \ell(M/N) + \ell(N)$$

(ii) Je zwei Kompositionsreihen eines Moduls haben dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten.

Sind also

$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0$$

und

$$M = \tilde{M}_s \supset \tilde{M}_{s-1} \supset \ldots \supset \tilde{M}_0 = 0$$

zwei Kompositionsreihen eines Moduls M, so gilt $r = s$ und es gibt eine Permutation $\sigma \in S_r$ mit

$$\tilde{M}_i/\tilde{M}_{i-1} \cong M_{\sigma i}/M_{\sigma i-1} \quad \textit{für alle } i\,.$$

Beweis.

Sei M ein R–Modul mit Kompositionsreihe

$$M = M_r \supset \ldots \supset M_0 = 0$$

und $N \subset M$ ein Untermodul. Wir betrachten

$$\text{can}: \quad M \twoheadrightarrow \overline{M} = M/N$$

und setzen

$$N_i := M_i \cap N \qquad \text{und } \overline{M}_i = \text{can}\,(M_i)$$

Betrachte das kommutierende Diagramm:

$$\begin{array}{ccccc} N_{i-1} & \hookrightarrow & N_i & \twoheadrightarrow & N_i/N_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ M_{i-1} & \hookrightarrow & M_i & \twoheadrightarrow & M_i/M_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ \overline{M}_{i-1} & \hookrightarrow & \overline{M}_i & \twoheadrightarrow & \overline{M}_i/\overline{M}_{i-1} \end{array}$$

Die Zeilen sind exakt, die ersten zwei Spalten auch. Nach dem Neunerlemma I. 1.13.2 erhalten wir exakte Sequenzen

$$N_i/N_{i-1} \quad \hookrightarrow \quad M_i/M_{i-1} \twoheadrightarrow \overline{M}_i/\overline{M}_{i-1} \tag{16}$$

Ist $N \neq 0$, so gibt es i mit $N_i/N_{i-1} \neq 0$. Da M_i/M_{i-1} einfach ist, gilt $\overline{M}_i/\overline{M}_{i-1} = 0$. Also gilt für alle Quotienten

$$\ell(M/N) < \ell(M)$$

und ebenso gilt für jeden echten Untermodul

$$\ell(N) < \ell(M)\,.$$

Damit ist aber $\ell(M)$ auch gleich dem Maximum der Längen von Ketten echt absteigender Untermoduln von M. Es folgt daraus, dass alle Untermoduln und Quotienten endliche Länge haben. Ebenso folgt, dass je zwei Kompositionsreihen gleiche Länge haben.

Aus (16) folgt dann sofort

$$\ell(N) + \ell(M/N) = \ell(M)\,.$$

(ii) folgt per Induktion wie in I. 1.12.3 (Satz von Jordan–Hölder für Gruppen).

Korollar 2.3.5.
Sei R ein Ring, der einen Körper K als Teilring hat. Ist R endlich dimensional über K, so gibt es bis auf Isomorphismus höchstens $\dim_K R$ *verschiedene einfache R–Moduln.*

Beweis.

Jeder R-Modul M ist insbesondere auch K-Vektorraum, also gilt $\dim_K M \geq 1$. Daher gilt

$$\ell(M) \leq \dim_K(M)\,.$$

Sei nun M ein einfacher R-Modul, $a \in M$ und $a \neq 0$. Dann ist der von a erzeugte Untermodul $\langle a \rangle$ ungleich Null, also $\langle a \rangle = M$, da ein einfacher Modul keine nicht-trivialen Untermoduln hat. Wir haben daher eine Surjektion

$$\begin{array}{rcl} \varphi : R & \twoheadrightarrow & M \\ \lambda & \mapsto & \lambda a \end{array}$$

Nach dem Homomorphiesatz ist $M \cong R/\ker\varphi$; also ist jeder einfache R-Modul Quotient von R, tritt also in einer Kompositionsreihe und damit in allen Kompositionsreihen als Subquotient auf. Somit gibt es höchstens $\ell(R)$ verschiedene einfache R-Moduln. □

Wir wenden nun unsere Einsichten auf den Gruppenring aus Definition 2.2.4 an.

Satz 2.3.6.
Sei G eine endliche Gruppe und K ein Körper. So gibt es bis höchstens $|G|$ verschiedene Isomorphieklassen von irreduziblen Darstellungen von G über K.

Beweis. Nach Lemma 2.2.5 fassen wir Darstellungen von G als Moduln über dem Gruppenring $K[G]$ auf. Die Behauptung folgt dann direkt aus Korollar 2.3.5, da $\dim_K K[G] = |G|$. □

Satz 2.3.7 (Schursches Lemma)**.**
Sei G eine endliche Gruppe, K ein algebraisch abgeschlossener Körper und V eine irreduzible Darstellung über K. Dann besitzt V außer den Skalaren keine Endomorphismen:

$$K \xrightarrow{\sim} End_G(V)\,.$$

Beweis. Da G endlich sein soll, ist $K[G]$ endlich–dimensional über K und somit auch V als Quotient von $K[G]$. Da V nach Annahme einfach ist, gilt insbesondere $V \neq 0$. Jeder Endomorphismus $\varphi \in \mathrm{End}_G(V)$ hat also wenigstens einen Eigenwert λ. Der entsprechende Eigenraum ist als Kern von $\varphi - \lambda\,\mathrm{id}_V$ eine G-Unterdarstellung von V. Da V einfach sein soll, muss der Kern gleich V sein, $\varphi = \lambda\,\mathrm{id}_V$. □

Beispiel 2.3.8 (Gegenbeispiele)**.**

(i) Die Gruppe der vierten Einheitswurzeln in den komplexen Zahlen, $G = W_4(\mathbb{C}) \cong \mathbb{Z}_4$ operiert durch Multiplikation auf dem zwei-dimensionalen $\mathbb{R}$–Vektorraum $\mathbb{C}$. Dies gibt eine irreduzible reelle Darstellung von G auf $\mathbb{C}$, aber es gilt auch

$$K = \mathbb{R} \subsetneq End_G(V) \cong \mathbb{C}$$

Aber der Körper $\mathbb{R}$ ist nicht algebraisch abgeschlossen, so dass wir Satz 2.3.7 nicht anwenden dürfen.

(ii) Sei $K \subset L$ eine echte Körpererweiterung. Dann trägt der K-Vektorraum $V = L$ eine irreduzible Darstellung der Gruppe $G = L^\times$ über K. In diesem Beispiel ist

$$End_G V = L$$

was natürlich ungleich K ist, selbst wenn K algebraisch abgeschlossen ist. Aber für algebraisch abgeschlossenes K ist die Gruppe $G = L^\times$ sicher nicht endlich!

2.4 Reduzibilität

Satz 2.4.1 (Maschke)**.**
Sei G eine endliche Gruppe und K ein Körper, dessen Charakteristik nicht die Gruppenordnung teilt. Dann ist jede Darstellung von G über K eine direkte Summe von einfachen Unterdarstellungen.

Der Beweis ist einfach für den Fall $K = \mathbb{R}$ oder $K = \mathbb{C}$ und endlichdimensionale Darstellungen. Er beruht in diesem Fall auf dem folgenden Lemma.

Lemma 2.4.2.
Ist V endlich–dimensionale Darstellung über $\mathbb{R}$ oder $\mathbb{C}$ der endlichen Gruppe G, so gibt es auf V ein G–invariantes Skalarprodukt, (bzw. hermitesches Skalarprodukt für $K = \mathbb{C}$), d.h. es gilt $(gv, gw) = (v, w)$ für alle Elemente $g \in G$.

Beweis.
Ist $b : V \times V \to \mathbb{C}$ irgendein Skalarprodukt, so definiert

$$(v, w) = \sum_{g \in G} b(gv, gw)$$

ein G–invariantes Skalarprodukt, denn es gilt

$$(gv, gw) = \sum_{\tilde{g} \in G} b(\tilde{g}gv, \tilde{g}gw) = (v, w) \quad .$$

□

Beweis. von 2.4.1 für $K = \mathbb{R}$ oder $K = \mathbb{C}$ und Darstellungen endlicher Dimension.

Ist $W \subset V$ eine Unterdarstellung, so ist auch ihr orthogonales Komplement $W^\perp \subset V$ unter einem invarianten Skalarprodukt eine Unterdarstellung: denn aus $\langle v, w\rangle = 0$ für alle $w \in W$ folgt wegen der Invarianz auch $\langle gv, w\rangle = \langle v, g^{-1}w\rangle = 0$, für alle $g \in G$ und $w \in W$. Wir haben also die folgende orthogonale Zerlegung in Unterdarstellungen:

$$V = W \oplus W^\perp .$$

Induktiv zeigt man, dass V in eine direkte Summe einfacher Unterdarstellungen zerfällt. □

Diese Technik heißt auch "Weyls Unitaritätstrick". Der allgemeine Fall, d.h. allgemeinere Körper und auch Darstellungen unendlicher Dimension, braucht mehr Begriffe, die wir jetzt einführen.

Definition 2.4.3.

(i) Seien V, W zwei Darstellungen einer Gruppe G über einem Körper K, so wird der Raum $Hom_K(V, W)$ zu einer Darstellung durch die Vorschrift

$$(gf)(v) = g(f(g^{-1}v))$$

oder, anders gesagt, durch $gf := g \circ f \circ g^{-1}$.

(ii) Allgemeiner sei V Darstellung einer Gruppe G und W Darstellung einer Gruppe H. So gibt die Vorschrift

$$(g, h)f = \rho_W(h) \circ f \circ \rho_V(g^{-1})$$

eine Operation von $G \times H$ auf $Hom_K(V, W)$.

Der Fall (i) ergibt sich für $G = H$ und die diagonale Einbettung

$$\begin{array}{ccc} G & \hookrightarrow & G \times G \\ g & \mapsto & (g, g) \end{array}$$

Daher nennt man die Operation in (i) auch die diagonale Operation oder Operation durch Konjugation auf dem Hom–Raum, um sie zu unterscheiden von der Operation durch Nachschalten

$$g : f \mapsto \rho_W(g) \circ f$$

und der Operation durch Vorschalten

$$g : f \mapsto f \circ \rho_V(g^{-1})$$

Bemerkung 2.4.4.
Es gilt

$$Hom_K(V,W)^G = Hom_{K[G]}(V,W)$$

für jedes Paar V, W von G–Darstellungen. Denn beide Räume sind

$$\begin{aligned} Hom_K(V,W)^G &= \{f : V \to W \text{ linear}, g \circ f \circ g^{-1} = f\} \\ &= Hom_{K[G]}(V,W) \end{aligned}$$

Beweis. des Satzes von Maschke 2.4.1 für endlich–dimensionale Darstellungen.

- Ist $i : W \hookrightarrow V$ eine Unterdarstellung, so finden wir eine Abbildung von K–Vektorräumen

  $$\pi \; : \; V \to W$$

  so dass $\pi \circ i = \mathrm{id}_W$. Das Problem ist, dass dies nur eine Abbildung von Vektorräumen, aber nicht von G–Darstellungen ist. Die Idee ist nun, die Abbildung durch Mittelung über die Gruppe G so zu verbessern, dass sie mit der Wirkung von G vertauscht. Betrachte daher

  $$\psi = \frac{1}{|G|} \sum_{g \in G} g\pi = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}$$

  Diese Definition macht natürlich nur dann Sinn, wenn die Charakteristik von K die Gruppenordnung nicht teilt.

- Wir rechnen nun

  $$h \circ \psi = \frac{1}{|G|} \sum_{g \in G} hg \circ \pi \circ g^{-1} = \frac{1}{|G|} \sum_{\tilde{g} \in G} \tilde{g} \circ \pi \circ \tilde{g}^{-1} h = \psi \circ h \; ,$$

  wobei wir substituierten $\tilde{g} = hg$. Also ist $\psi \in \mathrm{Hom}_G(V,W)$. Außerdem gilt weiterhin

  $$\psi \circ i = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1} \circ i = \sum_{g \in G} \frac{1}{|G|} g \circ \pi \circ i \circ g^{-1} = \mathrm{id}_W \, ,$$

  wobei wir in der zweiten Gleichheit ausnutzten, dass i ein G–Morphismus ist.

- Also ist $\ker \psi$ eine G–Darstellung. Es gilt sogar

  $$V = \ker \psi \oplus i(W) \, .$$

  Denn

  $$v \in \ker \psi \cap i(W)$$

heißt $v = i(w)$, also $0 = \psi(w) = \psi \circ i(w) = w$, woraus wieder $v = 0$ folgt. Ferner haben wir die Zerlegung

$$v = (v - i \circ \psi(v)) + i \circ \psi(v) \ ,$$

bei der wieder der zweite Summand in $i(W)$ liegt, der erste aber wegen

$$\psi(v - i \circ \psi(v)) = \psi(v) - \psi \circ i \circ \psi(v) = 0$$

im Kern von ψ. (Die Struktur dieses Arguments sollte mit dem Beweis von Satz 2.2.20 verglichen werden.) Im Falle $\dim V < \infty$ sind wir nach einer Induktion fertig.

Definition 2.4.5.
Ein Modul heißt halbeinfach, wenn er eine direkte Summe von einfachen Untermoduln ist.

Satz 2.4.6.
Sei R ein Ring und M ein R–Modul. Dann sind äquivalent:

(i) *M ist halbeinfach*

(ii) *M ist eine (nicht–notwendig direkte) Summe von einfachen Untermoduln.*

(iii) *Jeder Untermodul U von M besitzt ein* Komplement *D, d.h. es gibt zu jedem Untermodul U einen Untermodul D mit $D \oplus U = M$.*

Beweis.

(i) $\Rightarrow$ (ii) ist klar nach Definition.

(ii) $\Rightarrow$ (iii) Sei $M = \sum_{i \in I} M_i$ Summe einfacher Untermoduln M_i. Für jede Teilmenge $J \subset I$ setzen wir

$$M_J = \sum_{i \in J} M_i \, .$$

U sei der Untermodul, für den wir ein Komplement suchen. Nun finden wir mit Hilfe des Zornschen Lemmas unter allen Teilmengen $J \subset I$ mit $M_J \cap U = 0$ eine bezüglich Inklusion maximale Teilmenge. Wir behaupten, dass

$$M_J + U = M$$

gilt. Wäre $M_J \oplus U$ echter Untermodul von M, so gäbe es wenigstens ein $M_i \not\subset M_J \oplus U$, also

$$M_i \cap (M_J + U) = 0\,,$$

da M_i einfach sein soll. Damit gilt aber auch $(M_i + M_J) \cap U = 0$, im Widerspruch zur Maximalität von J.

(iii) $\Rightarrow$ (i)

Wir zeigen zunächst, dass die Eigenschaft (iii) sich auch auf Untermoduln vererbt. Seien $U \subset N \subset M$ Untermoduln, V ein Komplement von U in M, so ist $V \cap N$ Komplement von U in N.

Mit Hilfe des Zornschen Lemmas finden wir eine maximale Familie einfacher Untermoduln, deren Summe S in M direkt ist. Gälte $S \neq M$, so finden wir wegen (iii) ein Komplement D von S, das ungleich Null ist. Ziel ist nun, in D einen einfachen Untermodul E zu finden. Denn dann können wir $S \subset M$ vergrößern zu $E \oplus S \subset M$, im Widerspruch zur Maximalität von S.

Sei $D \ni d \neq 0$, und Rd der Untermodul von D, der von d erzeugt ist. Ist Rd einfach, sind wir fertig. Sonst finde nach dem Zornschen Lemma einen maximalen Untermodul B von Rd, der das Element d nicht enthält. B hat ein Komplement E in Rd, das einfach ist, denn jeden Untermodul E' von E könnten wir zu B hinzunehmen, im Widerspruch zur Maximalität der Wahl von B. □

Beweis. des Satzes von Maschke 2.4.1 im allgemeinen Fall:
Wir haben schon im Beweis nach Bemerkung 2.4.4 gesehen, dass jeder Untermodul U von V ein Komplement besitzt, nämlich $\ker \psi$. Die Behauptung des Satzes 2.4.1 folgt jetzt aus Satz 2.4.6. □

Korollar 2.4.7.
Jeder Quotient und jeder Untermodul eines halbeinfachen Moduls ist halbeinfach.

Beweis. Für jeden Untermodul $U \subset M$ ist der Quotient M/U eine Summe einfacher Untermoduln, nach Satz 2.4.6 also halbeinfach. Wiederum nach Satz 2.4.6 finden wir ein Komplement D zu U. Damit ist auch $U \cong M/D$ selbst halbeinfach. □

2.5 Fouriertransformation für Gruppen

Sei M ein R–Modul. Dann ist $\mathrm{End}_R(M)$ ein Ring, dessen Multiplikation die Hintereinanderausführung von Endomorphismen ist. Durch

$$\begin{array}{rcl} \mathrm{End}_R(M) \times M & \to & M \\ (\varphi, m) & \mapsto & \varphi(m) \end{array}$$

wird M auch ein $\mathrm{End}_R(M)$–Modul. Jedes $x \in R$ gibt durch

$$\begin{array}{rccl} \rho_x : & M & \to & M \\ & m & \mapsto & xm \end{array}$$

ein Element von $\mathrm{End}_R(M)$, das natürlich in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ liegt. Wir haben also einen Ringhomomorphismus

$$\varphi_{\mathrm{Jac}} : R \to \mathrm{End}_{\mathrm{End}_R(M)}(M)\,.$$

Satz 2.5.1. *(Jacobsonscher Dichtesatz)*
Sei R ein Ring und M ein halbeinfacher *R–Modul. Dann ist das Bild $\varphi_{\mathrm{Jac}}(R)$ in $End_{\mathrm{End}_R(M)}(M)$ dicht im folgenden Sinne: für gegebenes $f \in End_{\mathrm{End}_R(M)}(M)$ und endlich viele gegebene Elemente $m_1, \ldots, m_r \in M$ gibt es stets ein $x \in R$ mit $f(m_i) = xm_i$ für alle i. Wir können also die Wirkung jedes Elements φ auf endlich vielen Elementen des Moduls wiedergeben durch die Multiplikation mit einem Skalar $x \in R$.*

Beweis.

Wir betrachten zunächst den Fall $r = 1$. Betrachte zum Untermodul $Rm_1 \subset M$ ein Komplement D, also

$$M = Rm_1 \oplus D$$

Die Abbildung

$$\pi : M \twoheadrightarrow Rm_1 \hookrightarrow M,$$

die als Verkettung von kanonischer Surjektion und kanonischer Injektion definiert ist, liegt in $\mathrm{End}_R(M)$; nach Annahme über f gilt daher

$$f \circ \pi = \pi \circ f\,,$$

also

$$f(m_1) = f \circ \pi(m_1) = \pi \circ f(m_1)\,.$$

Daraus folgt $f(m_1) \in Rm_1$. Es gibt also ein $x \in R$, so dass

$$f(m_1) = xm_1\,.$$

Für den allgemeinen Fall $r > 1$ betrachten wir die direkte Summe

$$(m_1, \ldots, m_r) \in M \oplus \ldots \oplus M$$

und die Abbildung

$$f \times f \times \ldots \times f\,,$$

die in der Tat mit allen Elementen von

$$\mathrm{End}_R(M \oplus \ldots \oplus M) = \mathrm{Mat}_r(\mathrm{End}_R M)$$

kommutiert und wenden den Fall $r = 1$ an. □

Korollar 2.5.2.
Ist K ein algebraisch abgeschlossener Körper und ist A ein Teilring von $Mat_n(K)$, so dass K^n einfach ist als A–Modul, so gilt

$$A = Mat_n(K)\,.$$

Beweis.
Es ist $\mathrm{End}_A(K^n) = K$. Denn sei $\varphi \in \mathrm{End}_A(K^n)$ kein Vielfaches der Identität, so hat φ einen nicht–trivialen Eigenraum, der A–Untermodul wäre. Aber K^n sollte ja einfach als A-Modul sein.

Nach dem Dichtesatz 2.5.1 ist nun A dicht in $\mathrm{End}_K(K^n)$. Da K^n von endlich vielen $m_i \in K^n$ erzeugt wird, folgt Surjektivität. □

Korollar 2.5.3.
Sei K ein algebraisch abgeschlossener Körper und V eine irreduzible endlich–dimensionale Darstellung der Gruppe G über K. So definiert die Operation von G auf V eine Surjektion

$$K[G] \twoheadrightarrow End_K(V)$$

Beweis.
Wende Korollar 2.5.2 auf das Bild von $K[G]$ in $\mathrm{End}_K(V)$ an. □

Satz 2.5.4 (Fouriertransformation)**.**
Sei K ein algebraisch abgeschlossener Körper und G eine endliche Gruppe. Seien $L_1, \ldots, L_r$ die bis auf Isomorphie verschiedenen irreduziblen Darstellungen von G

(i) Die Operation von G definiert eine Surjektion

$$F : K[G] \twoheadrightarrow (End_K L_1) \times \cdots \times (End_K L_r)\,. \tag{17}$$

(ii) Teilt die Charakteristik von K nicht die Gruppenordnung $|G|$, so ist dies sogar ein Isomorphismus.

Beweis.

(i) Der $K[G]$–Modul $L_1 \oplus \cdots \oplus L_r$, hat den Endomorphismenring

$$\mathrm{End}_{K[G]}(L_1 \oplus \cdots \oplus L_r) = K \times K \times \cdots \times K\,.$$

Die Surjektivität folgt wieder aus dem Dichtesatz 2.5.1.

(ii) Teilt die Charakterstik von K nicht die Gruppenordnung, so ist nach dem Satz von Maschke 2.4.1 der Gruppenring $K[G]$ halbeinfach, also direkte Summe einfacher Unterdarstellungen. Liegt $a \in K[G]$ im Kern der Surjektion, so ist daher auch die Linksmultiplikation mit a die Nullabbildung auf $K[G]$. Daraus folgt mit $a = \sum \lambda_g g$ auch $ae = 0$, also $\lambda_g = 0$ für alle Gruppenelemente $g \in G$, mithin $a = 0$. □

Korollar 2.5.5.
Sei K ein algebraisch abgeschlossener Körper und G eine endliche Gruppe, deren Gruppenordnung nicht durch die Charakteristik von K geteilt wird. Seien $L_1, \ldots, L_r$ Repräsentanten der Isomorphieklassen einfacher Darstellungen. Dann gilt

$$|G| = (\dim L_1)^2 + (\dim L_2)^2 + \cdots + (\dim L_r)^2$$

Korollar 2.5.6.
Unter den gleichen Voraussetzungen gilt: Es gibt bis auf Isomorphie genauso viele einfache Darstellungen von G wie Konjugationsklassen in G.

Beweis.

Das Zentrum $Z(R)$ eines Ringes ist

$$Z(R) := \{z \in R \,|\, za = az \quad \forall\ a \in R\}\,.$$

Es ist ein kommutativer Teilring von R. (Achtung: im allgemeinen ist das Zentrum des Gruppenrings *viel* größer als der Gruppenring des Zentrums der Gruppe G, der natürlich auch ein kommutativer Unterring von $K[G]$ ist.)

Nach Satz 2.5.4 ist für den Gruppenring einer endlichen Gruppe $\dim_K Z(K[G])$ gleich der Zahl inäquivalenter irreduzibler Darstellungen. Andererseits gilt für $\varphi = \sum\limits_h \varphi_h\ h \in Z(K[G])$:

$$\begin{aligned} \varphi g &= \sum_{h\in G} \varphi_h h \cdot g = \sum_{h\in G} \varphi_{hg^{-1}} h \\ g\varphi &= \sum_{h\in G} \varphi_{g^{-1}h} h\,. \end{aligned}$$

Also gilt $\varphi_{ghg^{-1}} = \varphi_h$ für alle $g, h \in G$. Aufgefasst als Funktion

$$\varphi : G \to K$$

ist φ also auf Konjugationsklassen konstant: φ ist eine Klassenfunktion. □

Bemerkung 2.5.7.
Wir wollen noch die Beziehung zur Fouriertransformation erklären. Betrachten wir dafür die abelsche Gruppe aller komplexen Zahlen vom Betrage Eins,

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}\,.$$

Man kann zeigen, dass alle irreduziblen, stetigen, endlich–dimensionalen Darstellungen eindimensional sind und die Isomorphieklassen beschrieben werden durch den Homomorphismus

$$\begin{array}{rccll} L_n: & S^1 & \to & \mathbb{C} \cong GL(1,\mathbb{C}) & \text{für } n \in \mathbb{Z}\,. \\ & z & \mapsto & z^n & \end{array}$$

Als Analogon des Gruppenrings betrachten wir stetige komplexwertige Funktionen auf S^1, $C^0(S^1)$, die wir natürlich mit den periodischen Funktionen auf $\mathbb{R}$ identifizieren dürfen. Diese Funktionen operieren auf einer stetigen endlich–dimensionalen Darstellung V durch

$$fv = \int_{S^1} f(z)\rho_V(z)(v)\,dz \quad \forall\ f \in C(S^1)\ v \in V$$

insbesondere also auf der irreduziblen Darstellung L_n durch Multiplikation mit

$$\int_{S^1} f(z)z^n \,\mathrm{d}z\ ,$$

was genau die Fourierkoeffizienten sind. Die Abbildung aus 2.5.4

$$C(S^1) \xrightarrow{\sim} \prod_{n\in\mathbb{Z}} End_{\mathbb{C}} L_n$$

ordnet einer Funktion $f \in C(S^1)$ also gerade ihre Fourierkoeffizienten zu.

2.6 Charaktere

In diesem Abschnitt sei K ein algebraisch abgeschlossener Körper und G eine endliche Gruppe, so dass char K die Gruppenordnung $|G|$ nicht teilt.

Definition 2.6.1.
Sei L einfache Darstellung von G. Nach Satz 2.5.4 gibt es genau ein Element $e_L \in K[G]$, das durch die Identität auf L operiert und durch Null auf jeder einfachen Darstellung M von G, die nicht zu L isomorph ist:

$$e_L : M \to M = \begin{cases} \mathrm{id}_M & \textit{falls} \quad M \cong L \\ 0 & \textit{falls} \quad M \textit{ einfach, } M \ncong L \end{cases}$$

Dieses Element

$$e_L = F^{-1}\Big(\mathrm{id}_{End_K L}\Big)$$

heißt Projektor zur einfachen Darstellung L.

Lemma 2.6.2.
Seien $(L_i)_{i=1\ldots r}$ die irreduziblen Darstellungen von G bis auf Isomorphismie und $e_i \in K[G]$ ihre Projektoren. So gilt

$$e_i \star e_j = \delta_{ij} e_i$$
$$1 = e_1 + \cdots + e_r$$

und die e_i bilden eine Basis des Zentrums von $K[G]$.

Beweis. folgt sofort aus Satz 2.5.4.

Definition 2.6.3.
(i) Für eine endlich–dimensionale Darstellung V von G definiert man ihren Charakter

$$\chi_V : G \to K$$

durch $\chi_V(g) = \mathrm{tr}_V g = \mathrm{tr}_V \rho(g)$.

(ii) Gegeben $f \in K[G]$, definieren wir $\hat{f} \in K[G]$ durch $\hat{f}(g) = f(g^{-1})$. Dies ist eine Involution auf den Gruppenring.

Theorem 2.6.4 (Charakter–Projektor–Formel)**.**
Zwischen dem Charakter χ_L und dem Projektor e_L zu einer einfachen Darstellung L besteht die Beziehung

$$e_L = \frac{\dim L}{|G|}\ \hat{\chi}_L$$

Beweis.
Wir geben die inverse Fouriertransformation explizit an. Betrachte die Konvolution mit $g \in G$ von links

$$\begin{aligned} \tau_g : K[G] &\to K[G] \\ \tau_g\Big(\sum_{h\in G} \lambda_h h\Big) &= \sum_{h\in G} \lambda_h\ gh\,. \end{aligned}$$

So gilt

$$tr_{K[G]}\tau_g = \begin{cases} |G| & \text{für } g = e \\ 0 & \text{sonst.} \end{cases}$$

Bezeichnet allgemeiner für $f = \sum_{h\in G} f(h)h \in K[G]$

$$\tau_f : K[G] \to K[G]$$

die Konvolution von links mit f im Ring $K[G]$, so gilt

$$\tau_f = \sum_{h\in G} f(h)\tau_h$$

und daher

$$\mathrm{tr}_{K[G]}(\tau_{g^{-1}} \circ \tau_f) = \sum_{h\in G} f(h)\mathrm{tr}_{K[G]}(\tau_{g^{-1}h}) = |G|\, f(g)\,.$$

Insgesamt herhält man

$$f(g) = \frac{1}{|G|}\mathrm{tr}_{K[G]}(\tau_{g^{-1}} \circ \tau_f) \qquad . \tag{18}$$

Die rechte Seite wertet man leicht nach Anwendung von F mit Hilfe des folgenden Lemmas aus:

Lemma 2.6.5.
Ist L endlich–dimensionaler K–Vektorraum und $A : L \to L$ eine K–lineare Abbildung, so gilt für die Spur der induzierten Abbildung

$$\begin{array}{rccc} \tau_A : & End_K L & \to & End_K L \\ & \varphi & \mapsto & A \circ \varphi \end{array}$$

die Beziehung

$$\mathrm{tr}_{End_K L}\tau_A = \dim_K L \cdot \mathrm{tr}_L A$$

Beweis. Ohne Beschränkung der Allgemeinheit sei $L = K^n$. Dann ist $\mathrm{End}_K(K^n) \cong \mathrm{Mat}_n(K)$. τ_A operiert auf jeder Spalte wie A auf K^n selbst, also ist die Matrix von τ_A blockdiagonal mit n Blöcken der Gestalt A. □

Weiter im **Beweis** von 2.6.4:
Aus Gleichung (18) folgt

$$f(g) = \frac{1}{|G|}\mathrm{tr}_{K[G]}\,(\tau_{g^{-1}}\circ\tau_f) = \frac{1}{|G|}\sum_{i=1}^{r}\mathrm{tr}_{\mathrm{End}_k L_i}\,(\tau_{\rho_i(g)}\circ\tau_{\rho_i(f)}) = \sum_{i=1}^{r}\frac{\dim L_i}{|G|}tr_{L_i}\,(g^{-1}\circ f)\,.$$

für alle $f \in K[G]$.

Speziell entspricht der Projektor e_i an der i-ten–Stelle der Funktion

$$g \mapsto \frac{\dim L_i}{|G|} tr_{L_i} g^{-1} \qquad \square$$

Bemerkungen 2.6.6.

(i) Der Charakter ist eine Klassenfunktion:

$$\chi_L(ghg^{-1}) = \chi_L(h) \qquad \forall\ g, h \in G$$

(ii) Sind V und W Darstellungen von G, so gilt für ihre direkte Summe $\chi_{V \oplus W} = \chi_V + \chi_W$.

(iii) Sind V und W G–Darstellungen, so wird das Tensorprodukt $V \otimes W$ zur G–Darstellung durch

$$g(v \otimes w) = (gv) \otimes (gw)\,.$$

Es gilt

$$\chi_{V \otimes W} = \chi_V \cdot \chi_W\,.$$

(iv) Für eine G–Darstellung V nennen wir den Dualraum $V^* = Hom(V, k)$ mit der Wirkung

$$(g\lambda)(v) = \lambda(g^{-1}v) \quad \textit{für } \lambda \in V^*, g \in G\,, v \in V$$

die kontragrediente Darstellung. Es gilt

$$\chi_{V^*} = \hat{\chi}_V\,.$$

Satz 2.6.7.

Habe K Charakteristik Null. So teilt die Dimension jeder einfachen G–Darstellung die Gruppenordnung $|G|$.

Beweis.

Sei L einfache Darstellung und L^* die kontragrediente Darstellung. Die Beziehung

$$e_{L^*} \ * \ e_{L^*} = e_{L^*}$$

für die Projektoren ist äquivalent zu

$$\chi_L * \chi_L = \frac{|G|}{\dim L}\ \chi_L \tag{19}$$

Da gilt $g^n = 1$ mit $n = |G|$ und χ_L als Spur die Summe der Eigenwerte von $\rho(g)$ ist, liegt $\chi_L(g)$ in $\mathbb{Z}[\zeta]$, mit ζ einer primitiven n-ten Einheitswurzel.

Sei $I \subset \mathbb{Z}[\zeta]$ das von den Werten der Charaktere erzeugte Ideal. Aus Gleichung (19) folgt die Inklusion

$$I \supset \frac{|G|}{\dim L}\, I\,.$$

$\mathbb{Z}[\zeta]$ ist endlich–erzeugte torsionsfreie abelsche Gruppe, also auch I, also $I \cong \mathbb{Z}^r$ für ein $r \in \mathbb{N}$. Also

$$\frac{|G|}{\dim L} \in \mathbb{Z}$$

□

Satz 2.6.8.
Betrachte auf $K[G]$ die symmetrische Bilinearform

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1})$$

Die Charaktere bilden eine Orthonormalbasis für den Raum der Klassenfunktionen bezüglich dieser Bilinearform.

Beweis.
Offenbar gilt

$$(\varphi, \psi) = \frac{1}{|G|}(\varphi * \psi)(e) \qquad \text{mit} \quad e \in G$$

dem neutralen Element. Aus der Orthogonalität der Projektoren

$$e_i * e_j = \delta_{ij} e_j$$

folgt sofort die Orthogonalität einfacher Charaktere. Wertet man die daraus mit Theorem 2.6.4 folgende Gleichung

$$\chi_L * \chi_L = \frac{|G|}{\dim L}\chi_L$$

auf dem neutralen Element e aus und beachtet

$$\chi_L(e) = \mathrm{tr}_L e = \dim L\,,$$

so folgt auch $(\chi_L, \chi_L) = 1$. Insbesondere sind die Charaktere einfacher Darstellungen linear unabhängig im Raum der Klassenfunktionen. Wegen Korollar 2.5.6 liegt eine Basis für den gesamten Raum der Klassenfunktionen vor. □

Korollar 2.6.9.
Betrachtet man auf dem komplexen Gruppenring $\mathbb{C}[G]$ das hermitesche Skalarprodukt $\langle \cdot, \cdot \rangle$, das gegeben ist durch

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)} \,,$$

so bilden die einfachen Charaktere eine Orthonormalbasis im Raum der Klassenfunktionen.

Beweis.

- Wir zeigen für jeden Charakter $\chi = \chi_V$ über $\mathbb{C}$

  $$\chi(g^{-1}) = \overline{\chi(g)} \,.$$

  Zu jedem komplexen Vektorraum $(V, +, \cdot)$ konstruieren wir dafür einen anderen komplexen Vektorraum $(\overline{V}, +, *)$: als abelsche Gruppe sind beide Vektorräume gleich, $(V, +) = (\overline{V}, +)$, aber die Skalarmultiplikation ist

  $$\lambda * v = \overline{\lambda} \cdot v \qquad \text{für alle } \lambda \in \mathbb{C}, v \in V \,.$$

  Hierbei ist $\overline{\lambda}$ die zu λ konjugierte komplexe Zahl.
- Ist V eine G–Darstellung, so auch $\overline{V}$ mit der gleichen linearen Abbildung eine G-Darstellung, aber es gilt

  $$\chi_{\overline{V}}(g) = \overline{\chi_V(g)} \,.$$

- Andererseits wissen wir, dass für die kontragrediente Darstellung gilt

  $$\chi_{V^*}(g) = \chi_V(g^{-1})$$

  Es reicht also aus, einen Isomorphismus von G-Darstellungen

  $$V^* \cong \overline{V}$$

  zu zeigen. Nach Lemma 2.4.2 gibt es ein G-invariantes (hermitesches) Skalarprodukt auf V. Wir definieren

  $$i : V^* \to \overline{V}$$

  auf $\varphi \in V^*$ durch

  $$\varphi(v) = \langle i(\varphi), v \rangle$$

  für alle $v \in V$. Da $\langle \cdot, \cdot \rangle$ nicht entartet ist, ist dies eine Bijektion. i ist sogar ein G–Morphismus, denn für alle $g \in G$, $v \in V$ und $\varphi \in V^*$ gilt:

  $$\langle i(g\varphi), v \rangle = g\varphi(v) = \varphi(g^{-1}v) = \langle i(\varphi), g^{-1}v \rangle = \langle gi(\varphi), v \rangle \,.$$

□

Definition 2.6.10.

(i) Die Quaternionen sind die reelle 4–dimensionale unitale Algebra $\mathbb{H}$ mit Generatoren $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ und Relationen

$$\begin{aligned} \mathrm{i}^2 &= \mathrm{j}^2 = \mathrm{k}^2 = -1 \\ \mathrm{ij} &= \mathrm{k}\,. \end{aligned}$$

Dies ist ein Schiefkörper.

(ii) Ein $\mathbb{H}$–Vektorraum ist per definitionem ein $\mathbb{H}$–Modul. Diese Benennung ist sinnvoll, da alle $\mathbb{H}$-Moduln frei sind.

Lemma 2.6.11. *Ein $\mathbb{H}$–Modul ist äquivalent zu einem komplexen Vektorraum V mit einer antilinearen Abbildung J, für deren Quadrat $J^2 = -\mathrm{id}_V$ gilt.*

Beweis.

Setze $J(v) = jv$. Alles weitere folgt durch Nachrechnen. Insbesondere ist jeder $\mathbb{H}$–Modul frei.

Satz 2.6.12.

Sei G eine Gruppe und V eine einfache Darstellung von G über $\mathbb{C}$ von endlicher Dimension. So sind wir in genau einem der drei Fälle:

(a) V entsteht aus einer reellen Darstellung $V_{\mathbb{R}}$ durch Erweiterung der Skalare, d.h.

$$V = V_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}$$

Man sagt dann, V sei von reellem Typ.

(b) V entsteht aus einer quaternionalen Darstellung $V_{\mathbb{H}}$ auf einem $\mathbb{H}$–Modul durch Restriktion der Skalare. Man sagt dann auch, V sei von quaternionalem Typ.

(c) V ist nicht isomorph zu $\overline{V}$. In diesem Fall sagt man auch, V sei von komplexen Typ.

Beweis.

Ist $V \cong \overline{V}$, so gilt nach dem Schurschen Lemma 2.3.7

$$\dim_{\mathbb{C}} \mathrm{Hom}_G(V, \overline{V}) = 1\,;$$

sind die Moduln V und $\overline{V}$ nicht isomorph, so gibt es keine nicht–verschwindenden G–Morphismen.

Für einen Homomorphismus $J \in \mathrm{Hom}_G(V, \overline{V})$ gilt

$$Jav = a * Jv = \overline{a}Jv \qquad \forall\ a \in \mathbb{C}, v \in V$$

d.h. J ist antilinear. Wiederum nach dem Schurschen Lemma ist

$$J^2 = \lambda\ id_V \quad \text{mit } \lambda \in \mathbb{C}^* .$$

Wegen

$$\lambda Jv = J^3 v = J(J^2 v) = J\lambda v = \overline{\lambda}Jv$$

gilt $\lambda = \overline{\lambda}$, also ist λ reell, $\lambda \in \mathbb{R}$. Ersetzen wir J durch ein skalares Vielfaches J', also $J' = zJ$ mit $z \in \mathbb{C}^*$, so ist

$$(J')^2 = zJzJ = |z|^2 J^2 = |z|^2 \lambda\ \mathrm{id}_V .$$

Wir finden also einen $\mathbb{C}$–linearen G–Isomorphismus J^2, für den entweder gilt (a) $J^2 = \mathrm{id}_V$ oder (b) $J^2 = -\mathrm{id}_V$.

Im Falle (a) betrachten wir den reellen Vektorraum der J–Fixpunkte V^J, der eine reelle G–Darstellung trägt. Die Abbildung

$$\begin{array}{rcl} V^J \otimes_{\mathbb{R}} \mathbb{C} & \to & V \\ v \otimes_{\mathbb{R}} (\lambda_1 + \mathrm{i}\lambda_2) & \mapsto & \lambda_1 v + \lambda_2 \mathrm{i} v \end{array}$$

mit $\lambda_1, \lambda_2 \in \mathbb{R}$ ist dann ein Isomorphismus von komplexen G–Darstellungen. (Auf der linken Seite operiert G nicht-trivial nur auf V^J, aber trivial auf $\mathbb{C}$.) Im Falle (b) definiert J nach Lemma 2.6.11 auf V die Struktur eines $\mathbb{H}$–Vektorraums.

2.7 Noethersche Moduln

Sei R ein Ring mit Eins.

Satz 2.7.1.
Für einen R–(Links)Modul sind folgende Bedingungen äquivalent.

(i) Jede aufsteigende Kette $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq N_{k+1} \subseteq \ldots$ von Untermoduln wird stationär, d.h. es gibt einen Index k, so dass $N_i = N_k$ für alle $i \geq k$.

(ii) Jede nicht–leere Teilmenge von Untermoduln von M besitzt bezüglich der Inklusion ein maximales Element.

(iii) Jeder Untermodul ist endlich erzeugt.

Definition 2.7.2.

(i) Ein R–Modul M, der eine der Bedingungen aus 2.7.1 erfüllt, heißt (links–)noetherscher Modul.

(ii) Ein Ring R heißt (links–)noethersch, wenn er als Modul über sich selbst noethersch ist.

Beweis. (von 2.7.1)

(i) $\Rightarrow$ (ii) Jede nicht–leere Menge X von Untermoduln ist bezüglich Inklusion induktiv geordnet: denn sei $N_1 \subseteq N_2 \subseteq \dots$ eine Kette in X, so ist $\bigcup_i N_i = N_k \in X$ nach (i) eine obere Schranke für die Familie $\{N_i\}$. Die Existenz eines maximalen Elements folgt nun aus dem Zornschen Lemma.

(ii) $\Rightarrow$ (iii) Sei $N \subseteq M$ Untermodul. Wir betrachten die Menge

$$X := \{N' | N' \subseteq N \quad \text{Untermodul von } M, N' \text{ endlich erzeugt}\}$$

Zumindest der Nullmodul liegt in X, $0 \in X$, also ist X nicht leer. Sei $N_0 \in X$ ein maximales Element. Wir behaupten, dass dann $N_0 = N$ gilt. Denn wäre $x \in N \backslash N_0$, so wäre $\langle N_0, x\rangle \in X$ und das Erzeugnis $\langle N_0, x\rangle$ wäre immer noch endlich erzeugt, im Widerspruch zur Maximalität von N_0.

(iii) $\Rightarrow$ (i) Sei $N_1 \subseteq N_2 \subseteq \dots$ eine Kette von Untermoduln. Ihre Vereinigung $N' := \bigcup_i N_i$ ist ein Untermodul und wegen (iii) endlich erzeugt:

$$N' = \langle x_1, \dots, x_r\rangle$$

Daher gibt es $k \in \mathbb{N}$ so dass $x_i \in N_k$ für alle $i = 1, \dots r$. Hieraus folgt $N' \subseteq N_k$, die Kette der Untermoduln wird also stationär. $\square$

Beispiel 2.7.3.

Wir geben ein Beispiel eines Ringes, der nicht noethersch ist:

$$\begin{aligned} R &= \{f(X) \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\} \\ &= \{f = m + Xg \mid m \in \mathbb{Z}, g \in \mathbb{Q}[X]\} \end{aligned}$$

Jede Untergruppe G von $(\mathbb{Q}, +)$ gibt ein Ideal

$$A_G = GX + X^2\mathbb{Q}[X]$$

von R. Betrachte für jedes $i \in \mathbb{N}$ die Untergruppe $G_i = \left\{\frac{m}{i}, m \in \mathbb{Z}\right\}$. Wir bekommen so eine unendliche aufsteigende Kette von Idealen

$$A_{G_2} \subset A_{G_4} \subset A_{G_8} \subset \dots .$$

in R. Beispiele für noethersche Ringe folgen unmittelbar aus Korollar 2.7.7 unten.

Satz 2.7.4.

(i) Untermoduln und epimorphe Bilder noetherscher Moduln sind noethersch.

(ii) Ist U ein Untermodul und sind U und M/U noethersch, so ist auch M noethersch.

Beweis.

(i) Sei M noethersch, U Untermodul von M. Jeder Untermodul U' von U ist auch Untermodul von M, also endlich erzeugt.

Sei M' ein epimorphes Bild von M, also $f : M \to M'$, also $M' = M/\ker f$. Sei ferner V Untermodul von M/U und $f^{-1}(V)$ das Urbild von V unter der Surjektion f. Dann ist $f^{-1}(V)$ als Untermodul von M endlich erzeugt:

$$f^{-1}(V) = \langle v_1, \dots, v_r \rangle \quad \text{mit } v_i \in M\,.$$

Hieraus folgt

$$V = \langle v_1 + U, \dots, v_r + U \rangle\,,$$

also auch V ist endlich erzeugt.

(ii) Sei $N_1 \subseteq N_2 \subseteq \dots$ eine aufsteigende Kette von Untermoduln in M. Wir erhalten durch die kanonische Surjektion $f : M \twoheadrightarrow M/U$ eine aufsteigende Kette von Untermoduln in M/U

$$(N_1 + U)/U \subseteq (N_2 + U)/U \subseteq \dots$$

und durch Schnitt mit U eine aufsteigende Kette von Untermoduln in U:

$$N_1 \cap U \subseteq N_2 \cap U \subseteq \dots$$

Da sowohl U als auch M/U noethersch sein sollen, gibt es ein $k \in \mathbb{N}$, so dass

$$N_k + U = N_{k+1} + U = \dots$$

und $N_k \cap U = N_{k+1} \cap U = \dots$

Daraus folgt aber $N_k = N_{k+1}$. Denn sei $x \in N_{k+1}$, dann folgt aus der Stationarität der Kette im Quotientenmodul, dass man x schreiben kann in der Form $x = y + u$ mit $y \in N_k$ und $u \in U$. Somit liegt $u = x - y \in U \cap N_{k+1} = U \cap N_k \subset N_k$. Daraus folgt aber $x \in N_k$. □

Korollar 2.7.5.
Endliche direkte Summen noetherscher Moduln sind noethersch.

Beweis.
Seien U, V noethersche Moduln. Dann ist $(U \oplus V)/V \cong U$ noethersch. Aus Satz 2.7.4 folgt nun, dass auch die direkte Summe $U \oplus V$ noethersch ist.

Satz 2.7.6.
Ein Modul über einem noetherschen kommutativen Ring ist noethersch genau dann, wenn er endlich erzeugt ist.

Beweis.
Jeder noethersche Modul ist als Untermodul seiner selbst endlich erzeugt. Sei umgekehrt $M = \langle a_1, \ldots, a_r \rangle$ und sei $F = R^n$. Betrachte die Surjektion

$$\begin{array}{rcl} F = R^n & \twoheadrightarrow & M \\ (\alpha_1, \alpha_2, \ldots, \alpha_r) & \mapsto & \displaystyle\sum_{i=1}^{r} \alpha_i a_i \end{array}$$

Nach Satz 2.7.5 ist die direkte Summe R^n noethersch, nach Satz 2.7.4 ist M dann als epimorphes Bild noethersch.

Korollar 2.7.7.

(i) Hauptidealringe sind noethersch.

(ii) Endlich erzeugte Moduln über Hauptidealringen sind noethersch.

(iii) Endlich erzeugte abelsche Gruppen sind noethersche $\mathbb{Z}$–Moduln.

(iv) Jede Untergruppe einer endlich–erzeugten abelschen Gruppe ist endlich erzeugt.

Beweis.

(i) Die Untermoduln eines Ringes sind seine Ideale, die im Falle eines Hauptidealrings sogar von einem Element erzeugt werden, also insbesondere endlich erzeugt sind. Nach Satz 2.7.1 sind also Hauptidealringe noethersch.

(ii) Aus Satz 2.7.6 folgt dann sofort, dass endlich erzeugte Moduln über Hauptidealringen noethersch sind.

(iii) Klar als Spezialfall von (ii).

(iv) Folgt aus Satz 2.7.1, da eine Untergruppe einer abelschen Gruppe auch ein $\mathbb{Z}$–Untermodul ist.

Satz 2.7.8 (Hilbertscher Basissatz)**.**
Sei R ein kommutativer Ring. Ist R noethersch, so ist auch der Polynomring $R[X]$ noethersch.

Beweis.

Sei $I \subset R[X]$ ein Ideal. Sei $\mathfrak{a}_i \subset R$ das Ideal, das aus den höchsten Koeffizienten, den Leitkoeffizienten, aller Polynome vom Grad i im Ideal I besteht. Die Multiplikation mit dem Monom X zeigt die folgende Inklusion von Idealen von R:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots .$$

Für diese aufsteigende Idealkette im noetherschen Ring R gibt es ein j, so dass gilt

$$\mathfrak{a}_j = \mathfrak{a}_{j+1} = \ldots .$$

Jedes $\mathfrak{a}_i$ mit $i \leq j$ ist als Ideal des noetherschen Rings R endlich erzeugt. Wähle also endlich viele Polynome aus I, deren Leitkoeffizienten $\mathfrak{a}_i$ erzeugen. Die Gesamtheit dieser Polynome erzeugt I. □

2.8 Normalform der Matrix eines Homomorphismus

Sei R ein Ring mit Eins. Wie über Körpern können wir Homomorphismen von endlich–erzeugten *freien* R–Moduln durch Matrizen mit Einträgen in R beschreiben:

$$\mathrm{Hom}_R(R^n, R^m) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \mathrm{Hom}_R(R, R) = \mathrm{Mat}_{n\times m}(R)\,.$$

Wie für Körper zeigt man, wenn R kommutativ ist:

Lemma 2.8.1.
Sei R ein kommutativer Ring. Für $A = (a_{ij}) \in Mat_n(R)$ ist die Determinante

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

multiplikativ,

$$\det A \det B = \det AB$$

Genau dann ist die quadratische Matrix A invertierbar, wenn ihre Determinante eine Einheit in R ist, $\det A \in R^\times$.

Beweis.

Der Beweis der Multiplikativität der Determinante ist der gleiche wie der in der linearen Algebra. Ist A invertierbar, so ist wegen der Multiplikativität $\det A \det A^{-1} = 1$, also die Determinante invertierbar. Umgekehrt gilt mit der adjungierten Matrix

$$A^{\#}_{ij} = (-1)^{i+j} \det A^{ji}$$

für Matrizen über jedem kommutativen Ring R die Identität

$$A^{\#} A = (\det A) I \,.$$

□

Noch ein weiterer Satz aus der linearen Algebra gilt auch für endlicherzeugte Moduln über Hauptidealringen:

Satz 2.8.2 (Elementarteilersatz)**.**
Sei R ein Hauptidealring und $f : M \to N$ ein Homomorphismus zwischen zwei freien R–Moduln von endlichem Rang m bzw. n.

(i) Es gibt eine Diagonalmatrix $D \in Mat_{n\times m}(R)$ für deren Einträge die Teilbarkeitsbeziehung

$$d_{11} \mid d_{22} \mid d_{33} \dots \mid d_{rr}$$

gilt, wobei $r = \min(n, m)$ ist, und Isomorphismen $M \cong R^m$, $N \cong R^n$, so dass das Diagramm

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \wr & & \wr \\ R^m & \xrightarrow{D} & R^n \end{array}$$

kommutiert.

(ii) Die Diagonaleinträge d_{ii} sind eindeutig bis auf Assoziiertheit im Ring R.

Beweis.

- Wir dürfen $M = R^m$ und $N = R^n$ annehmen. f wird dann durch eine Matrix $A \in \mathrm{Mat}_{n\times m}(R)$ beschrieben. Wir suchen invertible quadratische Matrizen

$$X \in \mathrm{Mat}_n(R)\,, \quad Y \in \mathrm{Mat}_m(R)\ ,$$

  so dass XAY die gewünschte Diagonalform hat.

- Für eine Matrix A bezeichne $(A) \subset R$ das von den Einträgen der Matrix erzeugte Ideal. Für jede Matrix X folgt aus der Beziehung

$$(XA)_{ij} = \sum_k X_{ik}A_{kj}$$

  sofort die Inklusionsbeziehung

$$(XA) \subseteq (A)$$

  für die Ideale. Ist X invertierbar, so bekommt man auch die umgekehrte Inklusion, also

$$(XA) = (A)\,.$$

- Wir werden ein Verfahren angeben, das im Fall $(a_{11}) \subsetneqq (A)$ invertierbare Matrizen X und Y liefert, so dass $((XAY)_{11}) \supsetneqq (a_{11})$. Induktiv finden wir dann Matrizen $\tilde{X}, \tilde{Y}$, so dass

$$((\tilde{X}A\tilde{Y})_{11}) = (A)\,,$$

  indem wir das vom Element in der linken oberen Ecke erzeugte Ideal immer weiter vergrößern. Jetzt kann man Spalten– und Zeilenoperationen ausführen, die alle Elemente der ersten Zeile und Spalte eliminieren, ohne das Element in der linken oberen Ecke zu verändern: da a_{11} nun alle Einträge teilt, kann man geeignete Vielfache der erste Zeile bzw. Spalte zu jeder anderen Zeile bzw. Spalte addieren. Induktiv räumt man danach ebenso auch die weiteren Zeilen und Spalten auf.

- Für das Verfahren unterscheiden wir drei Fälle

(a) a_{11} teilt nicht alle Elemente in der ersten Zeile, etwa teilt a_{11} nicht das Element a_{12}. Schreibe, da R Hauptidealring ist, das Ideal (a_{11}, a_{12}) als Hauptideal:

$$(a_{11}, a_{12}) = (d)\,.$$

Dies erlaubt es uns, $x, y, \lambda, \mu \in R$ zu finden, so dass gilt:

$$\begin{aligned} d &= xa_{11} + ya_{12} \\ a_{11} &= d\lambda \\ a_{12} &= d\mu\,. \end{aligned}$$

Insbesondere haben wir $1 = x\lambda + y\mu$. Wir betrachten nun das Produkt der folgenden zwei Matrizen:

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right) \qquad \left(\begin{array}{cc|c} x & -\mu & \\ & & 0 \\ y & \lambda & \\ \hline 0 & & I \end{array}\right) = \left(\begin{array}{cc|c} d & * & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right)$$

Die rechte Matrix Y auf der linken Seite hat Determinante Eins, ist also invertierbar. Da das Ideal (d) das Ideal (a_{11}) echt enthält, haben wir mit X der Identität ein Paar X, Y von Matrizen gefunden, welches das Gewünschte leistet.

(b) Völlig analog läuft das Argument, falls a_{11} nicht alle Elemente der ersten Spalte teilt.

(c) Teilt a_{11} alle Elemente der ersten Zeile und Spalte, so kann man diese durch elementare Transformationen eliminieren. Wegen $(a_{11}) \neq (A)$ kann a_{11} aber nicht alle Einträge von A teilen. Durch Addition einer geeigneten Zeile zur ersten Zeile kann man deshalb wieder die Situation in (a) herstellen und fährt wie dort fort.

- Es bleibt, die Eindeutigkeit der erhaltenen Diagonalmatrix zu zeigen. Sei $J_i(A)$ für $i \geq 1$ das von den Determinanten der $i \times i$–Untermatrizen von A erzeugte Ideal. Offenbar gilt wieder

$$J_i(XA) \subseteq J_i(A)$$

für jede Matrix X, also Gleichheit der Ideale für invertierbares X. Es folgt

$$J_i(A) = (d_{11}d_{22}\cdots d_{ii})$$

und somit die Eindeutigkeit der Diagonalelemente d_{ii} bis auf Assoziiertheit. □

2.9 Endlich erzeugte Moduln über Hauptidealringen

Satz 2.9.1.
Sei M ein freier Modul von endlichem Rang über einem Hauptidealring R. Dann ist auch jeder Untermodul U von M frei und rang$(U) \leq$ rang(M).

Beweis.

Wir führen den Beweis durch Induktion nach rang$M =: n$. Für $n = 0$ ist $M = 0$, also ist nichts zu zeigen. Sei $\{x_1, \ldots, x_n\}$ eine Basis von M. Das Ideal

$$\mathfrak{a} := \left\{ \beta \in R \,|\quad \text{es gibt} \quad \beta_2 \ldots \beta_n \in U, \text{so dass } \beta x_1 + \sum_{i=2}^{n} \beta_i x_i \in U \right\}$$

ist im Hauptidealring R von der Form $\mathfrak{a} = (\alpha_1)$. Fixiere irgendwelche $\alpha_2, \ldots, \alpha_n \in R$, so dass

$$\alpha_1 x_1 + \sum_{i=2}^{n} \alpha_i x_i =: u \in U$$

Jedes $v \in U$ besitzt eine (eindeutige) Darstellung

$$v = \rho\alpha_1 x_1 + \sum_{i=2}^{n} \rho_i x_i \qquad \rho_i, \rho \in R\,.$$

Damit liegt

$$v - \rho u \in U \cap M' =: U'\ ,$$

wobei

$$M' = \langle x_2, \ldots, x_n \rangle$$

ein freier Untermodul von M vom Rang $n-1$ ist. Nach Induktionsannahme ist U' frei vom Rang $t \leq n-1$, sei also

$$\{y_1, \ldots, y_t\}$$

eine Basis von U'.

Ist $\alpha_1 = 0$, so ist $\mathfrak{a} = 0$, u liegt in U' und es ist $U' = U$, also ist U frei vom Rang $< n$. Sei also $\alpha_1 \neq 0$. Wir behaupten, dass dann $\{u, y_1, \ldots, y_t\}$ eine Basis von U ist.

Für beliebiges $v \in U$ hatten wir eine Darstellung mit

$$v - \rho u \in U'\,,$$

also liegt ein Erzeugendensystem vor, $\langle u, y_1, \ldots, y_t \rangle = U$. Um lineare Unabhängigkeit zu sehen, betrachte

$$0 = \gamma u + \sum_{i=1}^{t} \mu_i y_i \qquad \gamma, \mu_i \in R\,.$$

Wir stellen u, y_i als Linearkombination der x_i dar und erhalten die Gleichung

$$0 = \gamma\alpha_1 x_1 + \sum_{i=2}^{n} \mu_i' x_i\,.$$

mit gewissen $\mu_i' \in R$, da $y_i \in \langle x_2, \ldots, x_n \rangle$. Aus der linearen Unabhängigkeit der Familie $\{x_i\}$ folgt $\gamma = 0$. Da die y_i nach Voraussetzung linear unabhängig sind, folgt dann auch $\mu_i = 0$. □

Lemma 2.9.2.
Sei M ein endlich erzeugter Modul über einem Hauptidealring R und seien $q_1, \ldots, q_t$ Primpotenzen zu R derart, dass gilt

$$M \cong R^s \times R/q_1R \times \cdots \times R/q_tR\,. \tag{20}$$

Dann ist $s \in \mathbb{N}_0$ wohlbestimmt, d.h. es hängt nicht von der Wahl der Zerlegung (20) ab, und die Primpotenzen q_i sind wohlbestimmt bis auf Einheiten und Reihenfolge.

Beweis.

- Sei $Q = \text{Quot}\,(R)$ der Quotientenkörper von R. Dann ist $\text{Hom}_R(M, Q)$ ein Q–Vektorraum. Nach der universellen Eigenschaft 2.2.16 (i) der direkten Summe ist

  $$\text{Hom}_R(M, Q) \cong \text{Hom}_R(R/q_1R, Q) \times \cdots \times \text{Hom}_R(R/q_tR, Q) \times \text{Hom}_R(R, Q)^s\,.$$

  Nach Satz 2.2.9 ist $\text{Hom}_R(R, Q) \cong Q$. Sei $\mathfrak{a}$ ein von Null verschiedenes Ideal von R. Dann ist

  $$\text{Hom}_R(R/\mathfrak{a}, Q) = \{f \in \text{Hom}_R(R, Q) \mid f|_{\mathfrak{a}} = 0\}$$

  Jeder Modulhomomorphismus $f : R \to Q$, der nicht verschwindet, ist injektiv, da er durch $f(1)$ festliegt. Also ist

  $$\text{Hom}_R(R/\mathfrak{a}, Q) = 0\,.$$

  Es folgt

  $$s = \dim_Q \text{Hom}_R(M, Q)\,,$$

  also hängt s nicht von der Zerlegung (20) ab.

- Wir verwenden eine ähnliche Strategie, um die Unabhängigkeit der Primzahlpotenzen zu zeigen. Dafür betrachten wir für $p \in R$ irreduzibel den Restklassenkörper R/pR.

  Für jedes $n \geq 1$ ist dann $p^{n-1}M/p^nM$ ein R/pR–Vektorraum. Definiere

  $$d_p^n(M) = \dim_{R/pR}(p^{n-1}M/p^nM)\,.$$

  Offenbar gilt

  $$d_p^n(M \oplus N) = d_p^n(M) + d_p^n(N)\,.$$

  Da R integer ist, liefert die Multiplikation mit p^{n-1} einen Isomorphismus, den wir mit einer Surjektion verketten:

  $$R \xrightarrow{\sim} p^{n-1}R \twoheadrightarrow p^{n-1}R/p^nR\,.$$

  Wir bekommen dadurch einen Isomorphismus

  $$R/pR \xrightarrow{\sim} p^{n-1}R/p^nR\,.$$

  Daraus schliessen wir für alle p, n, dass

  $$d_p^n(R) = \dim_{R/pR}(p^{n-1}R/p^nR) = 1\,.$$

  Für $m > n$ ist $p^{n-1}(R/p^mR) = 0$. Für $m \leq n$ finden wir eine Surjektion

  $$\begin{array}{rcl} R \twoheadrightarrow R/p^mR & \xrightarrow{\sim} & p^{n-1}(R/p^mR) \twoheadrightarrow \\ & & p^{n-1}(R/p^mR)/p^n(R/p^mR) \end{array}$$

  mit Kern pR. Also gilt

  $$d_p^n(R/p^mR) = \begin{cases} 0 & \text{für} \quad m > n \\ 1 & \text{für} \quad m \leq n\,. \end{cases}$$

  Ist $\tilde{p}$ ein Primelement, das nicht zu p assoziiert ist, so ist die Restklasse von p eine Einheit im Ring

  $$\tilde{R} = R/\tilde{p}^mR\,.$$

  Also ist die Multiplikation mit p^n ein Isomorphismus auf $\tilde{R}$ und

  $$p^{n-1}\tilde{R}/p^n\tilde{R} \cong \tilde{R}/\tilde{R} = 0\,.$$

Damit folgt

$$d_p^n(M) = s + |\{i \,|\, p^n \quad \text{teilt} \quad q_i\}|\,,$$

so dass die Eindeutigkeit der q_i bis auf Assoziiertheit und Reihenfolge aus der Eindeutigkeit der Dimensionen $d_p^n(M)$ folgt. □

Lemma 2.9.3.
Sei M endlich erzeugter Modul über einem Hauptidealring R. So gibt es eine aufsteigende Kette $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r \subsetneqq R$ von Idealen von R, so dass

$$M \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r\,.$$

($\mathfrak{a} = 0$ ist zugelassen.)

Beweis.
Finde zunächst eine Surjektion

$$p : R^m \twoheadrightarrow M\,.$$

Da der Ring R noethersch ist, ist das Ideal $\ker p$ endlich erzeugt. Wir finden daher eine weitere Surjektion

$$f : \; R^n \twoheadrightarrow \ker p\,.$$

Da $\ker p$ Untermodul des freien Moduls R^m ist, können wir f als Abbildung

$$f : R^n \to R^m$$

auffassen; es gilt dann

$$M \cong R^m/\ker p = R^m/\text{im } f\,.$$

Satz 2.8.2 erlaubt es uns, invertierbare Abbildungen X, Y zu finden, so dass das Diagramm

$$\begin{array}{rcl} R^n & \vec{f} & R^m \\ X \uparrow & & \downarrow Y \\ R^n & \vec{D} & R^m \end{array}$$

kommutiert und D eine Diagonalmatrix ist, deren Element die Teilbarkeitsbeziehung $d_{11}|d_{22}|\ldots|d_{rr}$ mit $r = \min(m,n)$ erfüllen. Es folgt

$$M \cong R^m/\text{Im } D \cong R/d_{11}R \times \cdots \times R/d_{rr}R \times R^{m-r}$$

Schliesslich dürfen wir Faktoren mit $d_{ii} \in R^\times$ weglassen. Hieraus folgt die Existenz der angegebenen Zerlegung. □

Theorem 2.9.4.
Sei M ein endlich erzeugter Modul über einem Hauptidealring R.

(i) So gibt es genau eine aufsteigende Kette von Idealen in R wie in 2.9.3, so dass

$$M \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_r$$

(ii) Die Zerlegung, deren Existenz in Lemma 2.9.2 postuliert wurde, existiert. Sie ist dann nach Aussage des Lemmas 2.9.2 eindeutig.

Beweis.
Die Existenzaussage in (ii) folgt aus der Existenzaussage in Lemma 2.9.3, indem wir für $\mathfrak{a}_i \neq 0$ einen Erzeuger α_i wählen, $\mathfrak{a}_i = (\alpha_i)$, und diesen als Produkt von teilerfremden Primpotenzen schreiben:

$$\alpha_i = \prod_j q_j^{(i)} \ .$$

Dann wenden wir den chinesischen Restsatz (I.3.2.16) an:

$$R/\alpha_i \cong R/q_1^{(i)} \times R/q_2^{(i)} \times \cdots \times R/q_s^{(i)} \, .$$

Die Eindeutigkeitsaussage aus Lemma 2.9.2 liefert auch die Eindeutigkeitsaussage in (i). □

Korollar 2.9.5.
Die Klassifikation endlich erzeugter abelscher Gruppen aus Algebra I.1.9 folgt als Spezialfall für $R = \mathbb{Z}$ als Klassifikation endlich erzeugter $\mathbb{Z}$–Moduln.

Korollar 2.9.6.
(i) Ein endlich erzeugter torsionsfreier Modul über einem Hauptidealring ist frei. (Umgekehrt sind natürlich freie Moduln für jeden Ring torsionsfrei.)

(ii) Jeder endlich erzeugte Modul M über einem Hauptidealring R ist direkte Summe seines Torsionsuntermoduls mit einem freien Modul,

$$M \cong Tor\,(M) \oplus R^s \, .$$

Korollar 2.9.7 (Jordansche Normalform)**.**
Sei k ein algebraisch abgeschlossener Körper, V ein endlich–dimensionaler k–Vektorraum und $A : V \to V$ Endomorphismus von V. So gibt es eine Basis von V, in der A blockdiagonal ist, wobei die Blöcke auf der Diagonale konstant sind, nur 1 auf der ersten oberen Nebendiagonale steht und sonst alle Einträge null sind.

Beweis.

Nach Lemma 2.2.7 ist V ein $k[X]$–Modul. Der Polynomring $k[X]$ ist euklidisch, also insbesondere prinzipal. Finde nach Theorem 2.9.4 einen Isomorphismus von $k[X]$–Moduln

$$V \cong k[X]/(X-\lambda_1)^{n_1} \times \cdots \times k[X]/(X-\lambda_t)^{n_t}\,.$$

In jedem Summanden der rechten Seite wähle als Basis die Restklassen der Polynome

$$1, (X-\lambda), (X-\lambda)^2, \ldots, (X-\lambda)^{n-1}\,.$$

Wegen

$$X(X-\lambda)^i = \lambda(X-\lambda)^i + (X-\lambda)^{i+1}$$

hat die Multiplikation mit X, also die Wirkung von A auf V, in der angegebenen Basis die angegebene Form. □

Ähnlich folgen Normalformen für algebraisch nicht abgeschlossene Körper, zum Beispiel für $\mathbb{R}$ (siehe etwa H.J. Kowalski, Lineare Algebra, de Gruyter, Satz 35.8).

A Das Tensorprodukt von Vektorräumen

Sei K ein Körper und $(V_i)_{i\in I}$ eine Familie von K-Vektorräumen. Ein Tensorprodukt $\bigotimes_{i\in I} V_i$ der Vektorräume ist per Definition ein K-Vektorraum zusammen mit einer multilinearen Abbildung

$$\pi \,:\, \prod_{i\in I} V_i \to \bigotimes_{i\in I} V_i$$

vom Produkt der Vektorräume in diesen Vektorraum, so dass sich für jeden K-Vektorraum Z jede multilineare Abbildung

$$\beta \,:\, \prod_{i\in I} V_i \to Z$$

eindeutig in der Form $\beta = \tilde{\beta} \circ \pi$ schreiben lässt, wobei $\tilde{\beta}$ eine lineare Abbildung

$$\tilde{\beta} \,:\, \otimes_{i\in I} V_i \to Z$$

ist.

Dies ist eine universelle Eigenschaft des Tensorprodukts. Sie garantiert, mit den üblichen Argumenten, dass das Tensorprodukt bis auf kanonische Isomorphie eindeutig ist, falls es existiert. Die Existenz zeigt die folgende Konstruktion:

Wir konstruieren zunächst einen sehr großen K-Vektorraum $\mathcal{T}$, der aus allen Abbildungen φ des Produkts $\prod V_i$ nach K besteht, die nur für endlich viele Tupel $(v_i) \in \times V_i$ ungleich Null sind. Beachte, dass diese Abbildungen φ im allgemeinen *nicht* linear sind. Eine Basis von $\mathcal{T}$ ist gegeben durch die Abbildungen $b_{(v_i)}$ def folgenden Form: $b_{(v_i)}$ verschwindet überall, außer auf dem Tupel (v_i), wo es den Wert Eins annimmt. Die Elemente dieser Basis entsprechen also genau den Elementen des Produkts $\prod V_i$. Der Vektorraum $\mathcal{T}$ kann also schon für endlich viele endlich-dimensionale Vektorräume unendlich-dimensional sein.

Wir betrachten nun den Untervektorraum $\mathcal{R}$ von $\mathcal{T}$, der von allen Linearkombinationen der folgenden beiden Formen aufgespannt wird: einerseits von allen Linearkombinationen von Vektoren der Form

$$b_{u+u',v} - b_{u,v} - b_{u',v} \ ,$$

wobei u und u' Tupel sind, die sich nur in einer einzigen Stelle $i \in I$ unterscheiden, und andererseits von allen Linearkombinationen der Form

$$b_{\lambda u,v} - \lambda b_{u,v} \ ,$$

wobei λu ein Tupel ist, dessen Einträge gleich den Einträgen des Tupels u ist, außer an einer Stelle $i \in I$, wo das λ-fache steht. Wir definieren nun das Tensorprodukt als den Quotientenvektorraum

$$\bigotimes_{i \in I} V_i := \mathcal{T}/\mathcal{R} \, .$$

Sei can die zugehörige kanonische Projektion von $\mathcal{T}$ auf den Quotienten $\mathcal{T}/\mathcal{R}$. Die Abbildung π aus der Definition des Tensorprodukts ist nun gegeben durch

$$\pi((v_i)_{i \in I}) = \mathrm{can}(b_{(v_i)}) \, .$$

Es ist üblich, die Notation

$$\otimes v_{i \in I} := \mathrm{can}(b_{(v_i)})$$

einzuführen.

Es folgt sofort aus den Eigenschaften des Unterraums $\mathcal{R}$, dass die Abbildung π multilinear ist. Da das allgemeine Element von $\mathcal{T}$ eine (natürlich endliche) Linearkombination der Form

$$\sum \lambda_\alpha b_{(v_i^\alpha)}$$

mit $\alpha \in K$ ist, ist das allgemeine Element des Tensorprodukts von der Form

$$\sum \lambda_\alpha \otimes_{i\in I} v_i^\alpha \,.$$

Wir prüfen schließlich noch die universelle Eigenschaft nach: gegeben eine multilineare Abbildung β, definieren wir zunächst eine *lineare* Abbildung

$$\beta' : \mathcal{T} \to Z$$

durch ihre Werte auf der Basis von $\mathcal{T}$: $\beta'(b_{(v_i)}) = \beta((v_i))$. Da β multilinear ist, verschwindet β' auf dem Unterraum $\mathcal{R}$ von $\mathcal{T}$ und gibt daher Anlass zu einer auf dem Quotienten wohldefinierten Abbildung $\tilde{\beta}$, für die $\beta' = \tilde{\beta} \circ \mathrm{can}$ gilt. Wir haben nun

$$\tilde{\beta}(\otimes v_i) = \tilde{\beta} \circ \mathrm{can}(b_{(v_i)}) = \beta'(b_{(v_i)}) = \beta(v_i)\,.$$

Umgekehrt legt dies $\tilde{\beta}$ auf allen Elementen der Form $\otimes v_i$ fest, und diese erzeugen, wie wir gesehen haben, das Tensorprodukt linear über K. Damit ist die lineare Abbildung $\tilde{\beta}$ eindeutig durch die multilineare Abbildung β festgelegt. In diesem Sinne erlaubt der Begriff des Tensorprodukt es, multilineare Algebra auf lineare Algebra zu reduzieren.

Index