Algebra

Goethe–Universität Frankfurt — Wintersemester 2014/2015
für Bachelor und L3

JAKOB STIX

ZUSAMMENFASSUNG. — Die Vorlesung Algebra behandelt die Theorie der Körpererweiterungen, also Galoistheorie und ihre Anwendungen.

Dieses Skript wird fortlaufend aktualisiert. Es muß davon ausgegangen werden, daß es noch einige Zeit dauern wird, bis eine stabile Version entstanden ist und die gröbsten Fehler korrigiert sind. Sie lesen das Skript **auf eigene Gefahr!**

Bitte teilen Sie mir Korrekturvorschläge per Email oder persönlich nach der Vorlesung mit.

INHALTSVERZEICHNIS

1. Einführung

Die *lineare Algebra* behandelt die theoretische Grundlage für lineare Gleichungssyteme: n Gleichungen im Grad 1 in m Unbekannten. Thema in der Vorlesung *Geometrie* ist das strukturelle Verständnis von quadratischen Formen: eine Form vom Grad 2 in m Variablen. In der *Algebra* widmen wir uns dem Fall beliebigen Grades, wenn auch nur in einer Variablen. Wen der allgemeine Fall beliebig vieler Geichungen beliebigen Grades in beliebig vielen Variablen interessiert, der sei auf die Vorlesung in *algebraischer Geometrie* vertröstet. Grundlage dafür ist aber die *Algebra* und mit ihr die Theorie der Körper.

1.1. Panorama am Beispiel der komplexen Zahlen.

Die komplexen Zahlen

$$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$$

kann man als zweidimensionalen $\mathbb{R}$-Vektorraum mit Basis $1, i$ beschreiben. Diese Vektorraumstruktur ist eine wichtige Eigenschaft, die sich verallgemeinert und oft Verwendung findet.

Ein allgemeines Element von $\mathbb{C}$ hat demnach die Form

$$z = a + bi$$

mit $a, b \in \mathbb{R}$. Damit ist Addition auf $\mathbb{C}$ erklärt, nämlich wie im $\mathbb{R}$-Vektorraum:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

An die Mulitplikation stellen wir die Forderungen

- sie soll die von $\mathbb{R}$ fortsetzen, und
- assoziativ, kommutativ, distributiv und mit 1 sein.

Es gilt also notwendigerweise

$$(a + bi)(c + di) = ac + (bc + ad)i + bdi^2.$$

Das Element $i^2 \in \mathbb{C}$ läßt sich eindeutig in Koordinaten bezüglich der Basis $1, i$ ausdrücken: es gibt $a_0, a_1 \in \mathbb{R}$ mit

$$i^2 = -a_1 i - a_0$$

oder eben:

$$i^2 + a_1 i + a_0 = 0.$$

Hier hat man die Wahl! Wenn man die festgelegt hat, dann ist die Multiplikation auf $\mathbb{C}$ fixiert. Wir wählen

$$i^2 = -1,$$

also

$$(a + bi)(c + di) = ac - bd + (bc + ad)i.$$

1.1.1. *Eigenschaften der Multiplikation.*

Wie sehen wir am besten, daß diese Multiplikation die geforderten Eigenschaften hat, also kommutativ (sieht man sofort!), assoziativ und distributiv ist?

Variante A: durch stupides Nachrechnen. Das ist mühsam, und man lernt und sieht nichts.

Variante B: durch eine Einbettung in einen Ring. Die Abbildung

$$\begin{aligned} \rho : \ \mathbb{C} &\to \mathrm{M}_2(\mathbb{R}) \\ a + bi &\mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{aligned}$$

ist mit Addition (klar) verträglich und auch mit der Multiplikation: sei $z = a+bi$ und $w = c+di$, dann gilt

$$\rho(zw) = \rho(ac - bd + (bc + ad)i) = \begin{pmatrix} ac - bd & -(bc + ad) \\ bc + ad & ac - bd \end{pmatrix}$$
$$= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \rho(z)\rho(w).$$

Damit gibt es automatisch eine Eins, denn die Einheitsmatrix ist im Bild: $\rho(1)$. In $\mathrm{M}_2(\mathbb{R})$ ist die Multiplikation assoziativ und distributiv, damit also auch in $\mathbb{C}$, denn:

Wichtiges Prinzip: da ρ injektiv ist, kann man Identitäten (Gesetze) nach Anwenden von ρ testen.

Variante C: durch konzeptionelle Überlegungen. Wir nutzen die universellen Eigenschaften des Polynomrings, den wir in Kapitel 2 in Erinnerung rufen.

Zuerst konstruieren wir $\mathbb{C}$ neu. Die alte Konstruktion fügt fein, minimalistisch ein Element i hinzu und fragt zwangsläufig nach einer Gleichung für i^2. Die neue Konstruktion ist dagegen grob, maximal: wir nehmen zunächst mit dem Polynomring

$$\mathbb{R}[T]$$

eine Variable hinzu, also ein Element, das keinen algebraischen Zwängen (Gleichungen) unterliegt, und gehen dann zur größten Quotientenstruktur über, die ein Ring ist, und in der die Variable die gewünschte Gleichung löst:

$$\mathbb{R}[T]/(T^2 + 1)$$

Das Polynom T^2+1 hat keine Nullstelle in $\mathbb{R}$ und damit auch keinen Linearfaktor. Somit ist T^2+1 irreduzibel. Weil der Polynomring ist ein Hauptidealring ist, folgt daraus, daß $\mathbb{R}[T]/(T^2+1)$ ein Körper ist. Höhere Potenzen T^n mit $n \geq 2$ können durch kleinere ersetzt werden:

$$T^n = -T^{n-2} + T^{n-2}(1 + T^2) \equiv -T^{n-2} \mod (T^2 + 1).$$

Bei Grad ≤ 1 geht das nicht mehr. Also bilden die Restklassen

$$1 = 1 \mod (T^2 + 1), \quad t = T \mod (T^2 + 1)$$

eine $\mathbb{R}$-Basis des $\mathbb{R}$-Vektorraums $\mathbb{R}[T]/(T^2 + 1)$.

Wir identifizieren nun das neue mit dem zuerst eingeführten $\mathbb{C}$:

$$f : \mathbb{R}[T]/(T^2 + 1) \xrightarrow{\sim} \mathbb{C}$$
$$t \mapsto f(t) = i$$

und ansonsten $\mathbb{R}$-linear, also für $a, b \in \mathbb{R}$ gilt

$$a + bt \mapsto a + bi.$$

Man rechnet sofort nach, daß die auf $\mathbb{R}[T]/(T^2+1)$ per Faktorringkonstruktion (also im Endeffekt wegen der Idealeigenschaft von (T^2+1)) vorhandene Multiplikation nach Identifikation mit $\mathbb{C}$ in die von uns ad hoc aufgrund von $i^2 = -1$ eingeführte Multiplikation übergeht. Das zeigt sofort, daß $\mathbb{C}$ isomorph zu $\mathbb{R}[T]/(T^2 + 1)$ und damit ein Körper ist.

1.1.2. *Gleichungen versus Zahlen.* Hier kann man eine Dualität zwischen Polynomen wie T^2+1 und Zahlen, die durch eine Relation definiert sind — wie hier i definiert durch $i^2 = -1$ — erkennen. Ob man eine neue Zahl i zu $\mathbb{R}$ hinzufügt und die definierende Relation ausnutzt, um Addition und Multiplikation zu definieren, oder ob man formal eine Variable T hinzunimmt, und verfügt, daß eine Gleichung gelten soll: $T^2 + 1 = 0$, kommt auf das gleiche raus.

Wir ziehen daraus die Lehre, daß Zahlen in Erweiterungen durch die von ihnen erfüllten Gleichungen beschrieben werden. Umgekehrt lassen sich zu vorgegebenen Gleichungen Rechenbereicheserweiterungen definieren, in denen diese Gleichugen gelöst werden.

Im Nachhinein kann man die Identifikation

$$\mathbb{R}[T]/(T^2+1) \xrightarrow{f} \mathbb{C}$$

schrittweise bekommen. Es gibt mit der Inklusion einen Ringhomomorphismus $\mathbb{R} \to \mathbb{C}$, alles ist kommutativ und damit gibt es zu $i \in \mathbb{C}$ die Auswertungsabbildung

$$F : \mathbb{R}[T] \to \mathbb{C}$$

welche T in i auswertet. Da T^2+1 dabei auf $i^2+1=0$ abgebildet wird, ist $T^2+1 \in \ker(F)$, somit gilt die Inklusion der Ideale

$$(T^2+1) \subseteq \ker(F).$$

Die universelle Eigenschaft des Quotienten gegeben durch die Faktorringabbildung $\mathbb{R}[T] \to \mathbb{R}[T]/(T^2+1)$ führt zur eindeutigen $\mathbb{R}$-linearen Abbildung

$$f : \mathbb{R}[T]/(T^2+1) \to \mathbb{C}$$

mit

$$f(t) = i.$$

Das ist das f von oben. Hat man erst mal die Abbildung (fast ohne etwas nachrechnen zu müssen[1]), so zeigt man die Eigenschaft 'Isomorphie' auf unterschiedliche Weise. Zum Beispiel ist $\mathbb{R}[T]/(T^2+1)$ von $\mathbb{R}$-Dimension 2, genau wie $\mathbb{C}$. Außerdem ist die Abbildung sicher surjektiv, da mit $1, i$ eine $\mathbb{R}$-Basis im Bild ist. Eine surjektive lineare Abbildung endlich-dimensionaler Vektorräume ist schon ein Isomorphismus (von Vektorräumen; aber das reicht für Isomorphie von Ringen).

1.1.3. *Körper, nicht nur Ring.* Bisher haben wir unterschiedliche Konstruktionen und Methoden gesehen, wie man vermeidet, unnötig viel zu rechnen, um Rechengesetze nachzuweisen. Wieso ist nun $\mathbb{C}$ ein Körper? Die etwas aufwändigere Variante C warf die Körpereigenschaft nebenbei ab. Die direkten Überlegungen erlauben es jedoch den Wert von Automorphismen zu betonen und sind daher auch interessant.

Wir wissen nun, daß $\mathbb{C}$ ein Ring ist, der $\mathbb{R} \subseteq \mathbb{C}$ als Unterring hat. Um ein Körper zu sein, fehlt es noch nachzuweisen, daß jedes Element $z \in \mathbb{C}$, $z \neq 0$ invertierbar ist. Dazu verwenden wir die **komplexe Konjugation**

$$\begin{aligned} \bar{\ } : \ \mathbb{C} &\to \mathbb{C} \\ z = a+bi &\mapsto \bar{z} = a - bi \end{aligned}$$

Dies ist ein Körperautomorphismus von $\mathbb{C}$, der $\mathbb{R}$ elementweise fest läßt. Genauer besteht die Automorphismengruppe[2] von $\mathbb{C}$ als Erweiterung von $\mathbb{R}$

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\sigma : \mathbb{C} \xrightarrow{\sim} \mathbb{C} \ ; \ \sigma|_{\mathbb{R}} = \mathrm{id}\} = \{\mathrm{id}, \bar{\ }\}$$

nur aus der Identität und der komplexen Konjugation.

Warum ist $z \mapsto \bar{z}$ ein Ringhomomorphismus?

- Weil man es der Multiplikation sofort ansieht.
- Weil die der Transposition in $\mathrm{M}_2(\mathbb{R})$ entspricht. Diese Begründung muß man durchdenken, denn — Vorsicht! — transponieren dreht die Reihenfolge der Produkte um (ein Antihomomorphismus). Aber $\mathbb{C}$ lebt als Bild von ρ in einem kommutativen Teilbereich von $\mathrm{M}_2(\mathbb{R})$, der von der Transposition in sich überführt wird, und daher darf man zurücktauschen.
- Das folgt aus der universellen Eigenschaft von $\mathbb{R}[T]/(T^2+1)$, weil $-i$ auch eine Lösung von $T^2+1=0$ ist. Dazu später mehr, wenn die Symmetrien der Körper zu den Symmetrien der Lösungsmengen der definierenden Gleichungen in Bezug gebracht werden.

[1] Daß $\mathbb{C}$ ein Ring ist, muß man leider schon wissen.

[2] Als Menge der Strukturerhaltenden Symmetrien automatisch eine Gruppe; und unsere erste Galoisgruppe!

Und warum handelt es sich bei der komplexen Konjugation um einen Isomorphismus?

- Das sieht man in der Basis $1, i$.
- Die Transposition ist involutiv.
- oder:

Proposition 1. *Sei K ein Körper, A ein Ring und $f : K \to A$ ein Ringhomomorphismus (mit Eins!). Dann ist f injektiv.*

Beweis. Sei $0 \neq a \in K$ im Kern von f. Dann gilt für jedes $x \in K$:

$$f(x) = f(xa^{-1}a) = f(xa^{-1})f(a) = f(xa^{-1}) \cdot 0 = 0.$$

Somit ist $f \equiv 0$ identisch die Nullabbildung und auch $f(1) = 0$, was für Ringe mit Eins nicht sein darf. □

Genauer zeigt der Beweis, daß ohne die Eins zu berücksichtigen entweder $\ker(f) = (0)$ oder $\ker(f) = K$ gilt. Da Ideale dasselbe sind wie Kerne von Ringhomomorphsimen, ergibt sich sofort:

Korollar 2. *Ein Körper K hat nur die zwei trivialen Ideale (0) und $(1) = K$.*

Proposition 3.

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\sigma : \mathbb{C} \xrightarrow{\sim} \mathbb{C} \ ; \ \sigma|_{\mathbb{R}} = \mathrm{id}\} = \{\mathrm{id}, \bar{\ }\}$$

Beweis. Daß es mindestens die zwei Automorphismen gibt, haben wir durch Konstruktion gesehen. Fehlt noch, daß dies alle sind.

Ein solches σ ist eindeutig durch seinen Wert bei i festgelegt:

$$\sigma(a + bi) = a + b\sigma(i).$$

aber wegen

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

muß $\sigma(i)$ auch eine Lösung von $T^2 + 1$ sein. Davon gibt es in einem Körper höchstens 2 und das sind i (entsprechend der Identität) und $-i$ entsprechend der komplexen Konjugation. □

Wir haben immer noch einzusehen, daß jedes $0 \neq z = a + bi \in \mathbb{C}$ invertierbar ist. Die Norm, eine multiplikative Symmetrisierung,

$$N(z) = z\bar{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 \in \mathbb{R}$$

ist eine reelle Zahl. genauer gilt $N(z) > 0$ genau dann, wenn $z \neq 0$. Damit finden wir das Inverse als

$$z^{-1} = N(z)^{-1} \cdot \bar{z} \in \mathbb{C}$$

sofern $z \neq 0$.

1.1.4. *Zwischenkörper und Galoistheorie.* Ein Körper K mit

$$\mathbb{R} \subseteq K \subseteq \mathbb{C}$$

muß notwendigerweise $\mathbb{R}$ oder $\mathbb{C}$ sein. Zum einen wird K durch die Multiplikation mit Skalaren aus $\mathbb{R}$ ein $\mathbb{R}$-Untervektorraum sein, hat also

$$1 = \dim_{\mathbb{R}} \mathbb{R} \leq \dim_{\mathbb{R}} K \leq \dim_{\mathbb{R}} \mathbb{C} = 2$$

und damit keinen echten Platz zwischen $\mathbb{R}$ und $\mathbb{C}$.

Galoistheorie hat noch eine andere Begründung parat, die im konkreten Fall $\mathbb{C}/\mathbb{R}$ mit Kanonen auf Spatzen schießt, aber hier als Vorgriff schon einmal angegeben werden soll. Die Körperautomorphismen von $\mathbb{C}$, welche auf K die Identität sind, bilden offensichtlich eine Untergruppe

$$\mathrm{Aut}_K(\mathbb{C}) \subseteq \mathrm{Aut}_{\mathbb{R}}(\mathbb{C}).$$

Nach dem Hauptsatz der Galoistheorie stehen die Untergruppen von $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ über diese Konstruktion in Bijektion mit den Zwischenkörpern. Den Zwischenkörper zur Untergruppe $H \subseteq \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ bekommt man zurück als den Körper der Invarianten

$$\mathbb{C}^H = \{z \in \mathbb{C} \ ; \ h(z) = z \text{ für alle } h \in H\},$$

was tatsächlich offensichtlich ein Zwischenkörper ist. Da die Gruppe $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ nur aus 2 Elementen besteht ist die Liste der Untergruppen kurz.

- $\{\mathrm{id}\}$ gehört zu $\mathbb{C}$,
- $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ gehört zu $\mathbb{R} = \mathbb{C}^{\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})}$. In der Tat sind die komplexen Zahlen z mit $z = \bar{z}$ genau die reellen Zahlen.

1.2. **Jenseits von $\mathbb{C}$.** Auf der Suche nach weiteren Erweiterungen von $\mathbb{C}$ mit mehr imaginären Zahlen fand Hamilton den Schiefkörper $\mathbb{H}$ der Hamiltonschen Quaternionen. Das ist ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit Basis $1, i, j, k$ und Relationen

$$i^2 = j^2 = k^2 = -1,$$
$$ij + ji = ik + ki = jk + kj = 0.$$

Doch dies hat einen Preis: $\mathbb{H}$ ist nicht mehr kommutativ. Die Quaternionen sind sehr nützlich und Quelle schöner Mathematik, aber in dieser Vorlesung geht es um Körper, also kommutative Körper.

Vielleicht können wir ja weitermachen wie beim Übergang von $\mathbb{R}$ nach $\mathbb{C}$?

Satz 4. *Jede quadratische Gleichung über $\mathbb{C}$ hat bereits eine Nullstelle in $\mathbb{C}$.*

Beweis. Nach quadratischer Ergänzung geht es nur noch darum, eine Quadratwurzel ziehen zu können. Aber jedes $z \in \mathbb{C}$ ist ein Quadrat und hat somit eine Quadratwurzel in $\mathbb{C}$. Dies sieht man am besten in Polarkoordinaten. Es gilt

$$e^{i\varphi} = \cos\varphi + i \sin\varphi$$

und daher gibt es zu jedem $z \in \mathbb{C}$ ein $r \geq 0$ und $\varphi \in [0, 2\pi)$ mit

$$z = re^{i\varphi}.$$

Wir nehmen dann

$$w = \sqrt{r}e^{i\varphi/2}$$

und sehen sofort $z = w^2$. ☐

Damit kommen wir durch Lösungen quadratischer Gleichungen nicht über $\mathbb{C}$ hinaus. Satz 4 wird uns später zusammen mit etwas endlicher Gruppentheorie einen algebraischen Beweis des Fundamentalsatzes der Algebra bescheren, der auf Galoistheorie beruht.

Will man jenseits von $\mathbb{C}$ noch interessante Multiplikationen auf $\mathbb{R}$-Vektorräumen finden, so muß man also auf weitere Axiome verzichten. Die Fragen nach den Dimensionen, in denen nullteilerfreien Multiplikationen auf $\mathbb{R}^n$ definiert werden können, wurde von Adams mit topologischen[3] und K-theoretischen Methoden schließlich gelöst: solche Multiplikationen existieren genau für

$$n = 1, 2, 4, 8$$

entsprechend $\mathbb{R}$, den komplexen Zahlen $\mathbb{C}$, den Hamilton Quaternionen $\mathbb{H}$ und den Cayley Octonionen $\mathbb{O}$.

[3]Es gibt einen Bezug zu Vektorfeldern auf Sphären: S^{n-1} muß parallelisierbar sein, das heißt das Tangentialbündel wird durch $n-1$ Vektorfelder, die punktweise eine Basis bilden erzeugt. Auf der S^2 geht das nicht, da man bekanntlich einen Igel nicht kämmen kann, es somit nicht mal ein Vektorfeld ohne Nullstelle auf S^2 gibt.

Teil 1. Theorie der Körper und Körpererweiterungen

2. Faktorringe des Polynomrings

2.1. Erinnerung zum Polynomring. Sei K ein Körper. Der **Polynomring** über K ist

$$K[T] = \{f = \sum_{i=0}^{n} a_i T^i \ ; \text{ für ein } n \in \mathbb{N}_0 \text{ und } a_i \in K \text{ für } 0 \leq i \leq n\}$$

mit der gewöhnlichen Addition von Polynomen

$$(a_0 + a_1 T + \ldots + a_n T^n) + (b_0 + b_1 T + \ldots + b_m T^m) := (a_0 + b_0) + (a_1 + b_1)T + \ldots$$

und Multiplikation definiert durch

$$\begin{aligned}&(a_0 + a_1 T + \ldots + a_n T^n) \cdot (b_0 + b_1 T + \ldots + b_m T^m)\\ &:= (a_0 b_0) + (a_1 b_0 + a_0 b_1)T + \ldots + (\sum_{i+j=d, i,j \geq 0} a_i b_j) T^d + \ldots.\end{aligned}$$

Der Polynomring ist ein kommutativer Ring mit 1 (das konstante Polynom 1).

Den **Grad** von $0 \neq f = \sum_{i=0}^{n} a_i T^i$ definiert man als

$$\deg(f) = \max\{i \ ; \ a_i \neq 0\}.$$

Die Gradfunktion erfüllt, falls $f, g, f + g \neq 0$:

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$

und, falls $f, g \neq 0$:

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

Hieraus schließt man insbesondere, daß für $f, g \neq 0$ dann auch $fg \neq 0$ gilt: der Polynomring ist ein **Integritätsring**, ein Ring ohne Nullteiler.

Die Einheiten u von $K[T]$, also die Teiler von 1 mit $\deg(1) = 0$ haben $\deg(u) = 0$, sind also genau die konstanten Polynome ungleich 0:

$$K^\times = (K[T])^\times.$$

Die Gradfunktion macht den Polynomring über K zu einem **euklidischen Ring**. Für alle $f \in K[T]$ und $0 \neq q \in K[T]$ gibt es $d, r \in K[T]$ mit

$$f = dq + r$$

und $r = 0$ oder

$$\deg(r) < \deg(q).$$

Dies folgt aus dem Algorithmus zur Polynomdivision und läßt sich auch so berechnen.

Jeder euklidische Ring ist ein **Hauptidealring**, das heißt jedes Ideal von $K[T]$ wird von einem Element erzeugt. Genauer liefert der Beweis, daß jedes Ideal $\neq (0)$ erzeugt wird von einem Element kleinsten Grades im Ideal. Dieser Erzeuger wird eindeutig, wenn man ihn als normiert fordert, d.h., der Koeffizient vor der höchsten auftretenden Potenz T^d ist 1.

2.2. Faktorringe als Vektorraum. Der Polynomring $K[T]$ ist offensichtlich ein K-Vektorraum mit Basis

$$1, T, T^2, \ldots.$$

Jeder Faktorring ist insbesondere ein Faktorvektorraum und erbt die K-Vektorraumstruktur von $K[T]$.

Wir fixieren nun $f = \sum_{i=0}^{d} a_i T^i$ vom Grad $\deg(f) = d > 0$.

Lemma 5. *Der Faktorring*

$$K[T]/(f)$$

hat eine K-Basis gegeben durch die Restklassen von $1, T, \ldots, T^{d-1}$.

Beweis. Die Abbildung

$$K^d \to K[T]/(f)$$
$$(a_0, \ldots, a_{d-1}) \mapsto a_0 + a_1 T + \ldots + a_{d-1} T^{d-1} + (f)$$

ist offenbar K-linear. Sei $0 \neq (a_0, \ldots, a_{d-1})$ im Kern. Dann gibt es ein $h \in K[T]$ mit

$$g = \sum_{i=0}^{d-1} a_i T^i = hf$$

Aber f kann g aus Gradgründen nicht teilen:

$$d - 1 \geq \deg(g) = \deg(fh) = \deg(f) + \deg(h) \geq d$$

Widerspruch: die Abbildung muß injektiv sein.

Jede Restklasse von $K[T]/(f)$ hat wegen Polynomdivision mit Rest, also der euklidischen Eigenschaft der Gradfunktion, einen Vertreter vom Grad $\leq d - 1$, oder eben 0. Das zeigt die Surjektivität. □

2.3. **Faktorringe als Ringe.** Wir erinnern an die Kernzerlegung, also im Wesentlichen den Chinesischen Restsatz für Polynome. Sei $0 \neq f \in K[T]$ und $A = K[T]/(f)$. Seien $p_1, \ldots, p_s$ paarweise verschiedene normierte irreduzible Polynome in $K[T]$ (also nichtassoziierte Primelemente) und sei

$$f = \prod_{i=1}^{s} p_i^{n_i}$$

die Zerlegung von f in irreduzible Faktoren in $K[T]$. Dann gilt

$$A \simeq \prod_{i=1}^{s} K[T]/(p_i^{n_i})$$

als Ringe. Der Isomorphismus ist das Produkt der natürlichen Projektionen, welches $T + (f)$ in der i-ten Komponente auf $T + (p_i^{n_i})$ abbildet, quasi die Identität auf Vertretern ist.

Satz 6. *K Körper und $f \in K[T]$, $f \neq 0$. Dann ist f irreduzibel, genau dann, wenn $A = K[T]/(f)$ ein Körper ist.*

Beweis. Sei f nicht irreduzibel und die Zerlegung $f = gh$ mit g, h nicht Einheit ein Zeuge dafür. Es gilt also $\deg(g), \deg(h) \geq 1$. Somit gilt

$$0 < \deg(g), \deg(h) < \deg(g) + \deg(h) = \deg(f)$$

und g, h repräsentieren beide von 0 verschiedene Elemente in A. Aber $gh = f \equiv 0$. Damit sind g, h Nullteiler, und A ist kein Integritätsring und schon gar nicht ein Körper.

Sei f nun irreduzibel, und $0 \neq a \in A$. Wir wählen $g \in K[T]$ als Vertreter von a. Sei $d = (f, g)$ der größte gemeinsame Teiler von f und g in $K[T]$ (hiefür braucht man die Hauptidealeigenschaft!). Da f irreduzibel ist, hat f bis auf Einheiten nur die Teiler 1 und f (ist also ein Primelement, hierfür braucht man wieder die Hauptidealeigenschaft). Also ist $d = 1$ oder $d = f$.

Wenn $d = f$, so teilt $f \mid g$ und $a = 0$ im Widerspruch zur Annahme. Also gilt $d = 1$ und es gibt (zum Beispiel nach dem euklidischen Algorithmus) Polynome $x, y \in K[T]$ mit

$$xf + yg = 1.$$

Sei b das Bild von y in A. Dann gilt $ab = 1$ in A. Also ist jedes von 0 verschiedene Element invertierbar und A ein Körper. □

3. Körpererweiterungen als Vektorräume

Definition 7. Eine **Körpererweiterung** besteht aus einem Paar von Körpern K und L, und einem injektiven Homomorphismus $K \hookrightarrow L$ von Körpern. Meist wird K mit seinem Bild in L identifiziert. Als Notation verwenden wir

$$L/K,$$

was kein Quotient ist! Das / liest man als `über`.

In einer Körpererweiterung L/K ist L ein **Oberkörper** von K und umgekehrt K ein **Unterkörper** von L. Ein Körper M mit $K \subseteq M \subseteq L$ heißt Zwischenkörper.

Beispiele werden wir mannigfach in der Vorlesung sehen. Wenn im Kontext klar ist, daß man es mit Körpern zu tun hat, sagen wir auch schlicht **Erweiterung** zu einer Körpererweiterung. Offensichtlich ist mit M/L und L/K auch M/K in natürlicher Weise eine Körpererweiterung, indem man die Inklusionen komponiert:

$$K \hookrightarrow L \hookrightarrow M.$$

Eine sukzessive Erweiterung

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$$

nennt man einen **Körperturm**. Dieser kann aus endlich vielen oder unendlich vielen Körpern bestehen.

Beispiel 8. Sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom. Dann ist $L = K[T]/(f)$ in natürlicher Weise eine Körpererweiterung von K, siehe Satz 6.

3.1. Der Körpergrad.

Sei L/K eine Körpererweiterung. Dann ist L ein K-Vektorraum mit der Addition von L und Skalarmultiplikation von K durch Einschränkung der Multiplikation von L. Die Teilmenge $K \subseteq L$ ist ein 1-dimensionaler K-Unterrraum.

Definition 9. Der **Grad** oder **Körpergrad** einer Körpererweiterung L/K ist definiert als

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

die Dimension von L als K-Vektorraum.

Satz 10 (Gradsatz)**.** *Seien M/K und L/M Körpererweiterungen. Dann ist $[L : K]$ endlich genau dann, wenn $[L : M]$ und $[M : K]$ endlich sind, und es gilt dann*

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

Beweis. Wir haben die Inklusionen $K \subseteq M \subseteq L$ und fassen so M als K-Vektorraum und L mal als M-Vektorraum und mal als K-Vektorraum auf.

Sei $(b_i)_{i \in I}$ eine K-Basis von M und sei $(x_j)_{j \in J}$ eine M-Basis von L. Der Beweis des Gradsatzes ist erbracht, wenn wir zeigen können, daß

$$(x_j b_i)_{(i,j) \in I \times J}$$

eine K-Basis von L ist. Das zeigen wir jetzt.

Sei $y \in L$. Dann gibt es eine endliche Teilmenge $J_0 \subseteq J$ und $\mu_j \in M$ für $j \in J_0$ mit

$$y = \sum_{j \in J_0} \mu_j x_j.$$

Die $\mu_j \in M$ schreiben wir analog mit $\lambda_{i,j} \in K$ zu einer endlichen Menge $I_0 \subseteq I$ als

$$\mu_j = \sum_{i \in I_0} \lambda_{i,j} b_i$$

und erhalten

$$y = \sum_{i,j \in I_0 \times J_0} \lambda_{i,j} b_i x_j.$$

Wir haben also ein Erzeugendensystem.

Zeigen wir nun die lineare Unabhängigkeit. Wenn es eine lineare Relation unter den $b_i x_j$ gibt, dann auch eine, bei der nur Indizes $i \in I_0$ und $j \in J_0$ für gewisse endliche Teilmengen $I_0 \subseteq I$ und $J_0 \subseteq J$ auftreten. Sei etwa

$$0 = \sum_{i,j \in I_0 \times J_0} \lambda_{i,j} b_i x_j = \sum_{j \in J_0} \big(\sum_{i \in I_0} \lambda_{i,j} b_i \big) x_j.$$

Weil $(x_j)_{j \in J}$ eine M-Basis von L ist und $\sum_{i \in I_0} \lambda_{i,j} b_i \in M$, folgt für alle $j \in J_0$

$$0 = \sum_{i \in I_0} \lambda_{i,j} b_i.$$

Da $(b_i)_{i \in I}$ eine K-Basis von M ist, folgt $\lambda_{i,j} = 0$ für alle i, j. □

Beispiel 11. (1) $[\mathbb{C} : \mathbb{R}] = 2$

(2) Wenn $[L : K] = p$ eine Primzahl ist, dann gibt es keine echten Zwischenkörper, also solche verschieden von L und K. Nach dem Gradsatz gilt für ein solches M

$$[L : M][M : K] = p$$

also ist ein Faktor 1 und damit $L = M$ oder $M = K$.

(3) Sei $f \in K[T]$ irreduzibel. Dann ist $K[T]/(f)$ nach Satz 6 eine Körpererweiterung von K vom Grad

$$[K[T]/(f) : K] = \deg(f)$$

nach Lemma 5.

(4) $[\mathbb{R} : \mathbb{Q}] = \infty$, sogar überabzählbar! Eine $\mathbb{Q}$-Basis von $\mathbb{R}$ kann nicht konstruktiv angegeben werden. Da wir aber das Auswahlaxiom annehmen, gibt es eine solche $\mathbb{Q}$-Basis, halt nur nicht explizit.

3.2. **Elemente und Gleichungen.**

Definition 12. (1) Ein **algebraisches** Element einer Körpererweiterung L/K ist ein Element $\alpha \in L$ so daß es ein Polynom $f \in K[T]$ gibt mit $f \neq 0$ und $f(\alpha) = 0$. Man sagt genauer, daß α **algebraisch über** K ist.

(2) Ein Element, das nicht algebraisch ist, heißt **transzendent**.

Beispiel 13. (1) In jeder Körpererweiterung L/K sind die Elemente von K algebraisch über K, denn $a \in K$ ist Nullstelle von $T - a \in K[T]$.

(2) Wir betrachten den Unterkörper $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \subseteq \mathbb{C}$ als Erweiterung von $\mathbb{Q}$ bestehend aus allen Ausdrücken (das kann man jetzt nachrechnen, oder es folgt aus dem weiteren Aufbau der Theorie sofort)

$$a + b\sqrt{2} + c\sqrt[3]{3} + d\sqrt[3]{9} + e\sqrt{2}\sqrt[3]{3} + f\sqrt{2}\sqrt[3]{9}$$

mit $a, b, c, d, e, f \in \mathbb{Q}$. Es ist klar, daß $\sqrt{2}$ und $\sqrt[3]{3}$ algebraisch über $\mathbb{Q}$ sind. Aber

$$\alpha = \sqrt{2} + \sqrt[3]{3}?$$

Wir rechnen

$$3 = (\alpha - \sqrt{2})^3 = \alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} = (\alpha^3 + 6\alpha) - (3\alpha^2 + 2)\sqrt{2}$$

so daß Umordnen und Quadrieren die Gleichung sechsten Grades

$$2(3\alpha^2 + 2)^2 = (\alpha^3 + 6\alpha - 3)^2$$

ergibt. Somit ist α eine Nullstelle von

$$f(T) = (T^3 + 6T - 3)^2 - 2(2 + 3T^2)^2.$$

Das muß und wird transparenter gehen!

(3) Um ein Beispiel eines transzendenten Elements anzugeben, muß man entweder etwas glauben, oder man muß etwas mehr ausholen: die reellen Zahlen e (Hermite 1873) und π (Lindemann 1882) sind transzendent über $\mathbb{Q}$.

Bemerkung 14. (1) Algebraisch zu sein, ist kein absoluter Begriff, sondern hat nur relativ zum Grundkörper der Erweiterung Bedeutung. Die Zahl e ist über $\mathbb{R}$ algebraisch, aber nicht über $\mathbb{Q}$.

(2) Daß es in $\mathbb{R}$ transzendente Zahlen geben muß, folgt aus einem Abzählargument. Da $\mathbb{Q}$ abzählbar ist und in jedem Polynom aus $\mathbb{Q}[T]$ nur endlich viele Koeffizienten aus $\mathbb{Q}$ auftreten, kann man auch $\mathbb{Q}[T]$ abzählen. Jedes Polynom hat dann höchstens so viele Nullstellen wie der Grad angibt, also lassen sich auch die über $\mathbb{Q}$ algebraischen Zahlen abzählen. Da es überabzählbar viele reelle Zahlen gibt, müssen sogar fast alle reellen Zahlen transzendent über $\mathbb{Q}$ sein.

Definition 15. Sei L/K eine Körpererweiterung und sei $\alpha \in L$ ein über K algebraisches Element. Die Menge der Polynome $f \in K[T]$ mit $f(\alpha) = 0$ bildet ein Ideal, den Kern der Auswertung

$$\begin{aligned} K[T] &\to L \\ f(T) &\mapsto f(\alpha). \end{aligned}$$

Im algebraischen Fall ist der Kern $\neq (0)$. Der eindeutige normierte Erzeuger des Kerns wird **Minimalpolynom** von α über K genannt und hier mit

$$P_{\alpha/K} \in K[T]$$

bezeichnet.

Bemerkung 16. (1) Es gilt $P_{\alpha/K}(\alpha) = 0$ und jedes $f \in K[T]$ mit Nullstelle α ist ein Vielfaches von $P_{\alpha/K}$.

(2) Der Begriff des Minimalpolynom hängt entscheidend daran, daß der Polynomring über einem Körper ein Hauptidealring ist.

Proposition 17. *Das Minimalpolynom eines algebraischen Elements ist irreduzibel.*

Beweis. Sei L/K eine Körpererweiterung und $\alpha \in L$ ein über K algebraisches Element. Angenommen, das Minimalpolynom wäre nicht irreduzibel, dann gäbe es nichtkonstante $g, h \in K[T]$ mit

$$P_{\alpha/K} = gh.$$

Nicht konstant bedeutet $\deg(g), \deg(h) > 0$. Dann gilt in L

$$0 = P_{\alpha/K}(\alpha) = g(\alpha)h(\alpha),$$

so daß mindestens einer der Faktoren selbst 0 ist. ObdA gelte $g(\alpha) = 0$. Aufgrund der Definition des Minimalpolynoms gilt dann

$$P_{\alpha/K} \mid g$$

somit

$$\deg(g) < \deg(g) + \deg(h) = \deg(P_{\alpha/K}) \leq \deg(g),$$

ein Widerspruch. □

Notation 18. Sei L/K eine Körpererweiterung und $A \subseteq L$ eine Teilmenge.

(1) Es bezeichne

$$K(A) = \bigcap_{K \subseteq M \subseteq L \text{ Körper}, A \subseteq M} M$$

den kleinsten Zwischenkörper, der A enthält. Wir sagen $K(A)$ wird von A über K (als Körper) erzeugt.

(2) Es bezeichne
$$K[A] = \bigcap_{K \subseteq R \subseteq L \text{ Ring}, A \subseteq R} R$$
den kleinsten Teilring von L, der K und A enthält.

Offensichtlich gilt $K[A] \subseteq K(A)$, denn Körper sind Ringe, aber da $K[A]$ nur die polynomialen Ausdrücke in den Elementen aus A mit Koeffizienten aus K enthält, nicht aber Quotienten von solchen wie $K(A)$, ist die umgekehrte Inklusion im Allgemeinen falsch.

Satz 19. *Sei L/K eine Körpererweiterung und $\alpha \in L$. Dann ist α algebraisch über K genau dann wenn $K(\alpha) = K[\alpha]$ als Unterkörper bzw. Unterring von L.*

In diesem Fall ist das Minimalpolynom $P_{\alpha/K} \in K[T]$ definiert und es gilt
$$K(\alpha) = K[\alpha] \simeq K[T]/(P_{\alpha/K}),$$
wobei α auf die Restklasse von T abgebildet wird.

Beweis. Für $\alpha = 0$ ist nichts zu zeigen. Sei daher $\alpha \neq 0$. Im Körper $K(\alpha)$ ist nun Multiplikation mit α bijektiv. Wenn $K(\alpha) = K[\alpha]$, dann ist Multiplikation mit α auch in $K[\alpha]$ bijketiv. Es gibt also $h(T) \in K[T]$ mit
$$1 = \alpha \cdot h(\alpha)$$
insbesondere ist $h \neq 0$.

Sei $f = T \cdot h - 1 \in K[T]$. Dann ist $\deg(f) = 1 + \deg(h)$ insbesondere $f \neq 0$ und $f(\alpha) = 0$. Damit ist α algebraisch über K.

Sei umgekehrt α algebraisch über K. Dann gibt es durch $T \mapsto \alpha$ einen K-linearen[4] Homomorphismus
$$M = K[T]/(P_{\alpha/K}) \to L$$
Da $P_{\alpha/K}$ irreduzibel ist, ist M ein Körper und damit die Abbildung injektiv. Darüber hinaus ist offensichtlich das Bild genau $K[\alpha]$, was damit schon ein Körper ist und also mit $K(\alpha)$ übereinstimmt. Das zeigt alle restlichen Behauptungen. □

Korollar 20. *Ist α algebraisch in L/K, dann gilt*
$$\deg(P_{\alpha/K}) = [K(\alpha) : K].$$

Beweis. Wegen $\deg(P_{\alpha/K}) = \dim_K K[T]/(P_{\alpha/K}) = \dim_K K(\alpha) = [K(\alpha) : K]$ sonnenklar. □

3.3. **Erzeugnisse und Körpertürme.**

Definition 21. (1) Eine **algebraische** Körpererweiterung ist eine Erweiterung L/K, so daß jedes Element $\alpha \in L$ algebraisch über K ist. Andernfalls ist L/K eine **transzendente** Erweiterung.
(2) Eine **endlich erzeugte** Körpererweiterung ist eine Erweiterung L/K, so daß es eine endliche Menge $A \subseteq L$ gibt mit $L = K(A)$.
(3) Eine **endliche** Körpererweiterung ist eine Erweiterung L/K mit endlichem Grad $[L : K] < \infty$. Andernfalls ist L/K eine **unendliche** Erweiterung.

Lemma 22. *Jedes Element einer endlichen Erweiterung ist algebraisch.*

Beweis. Sei L/K eine endliche Körpererweiterung und $0 \neq \alpha \in L$. Dann gibt es ein n, so daß
$$1, \alpha, \ldots, \alpha^n$$

[4] Ein K-linearer Homomorphismus ist ein Homomorphismus der zusätzlich eine lineare Abbildung der zugrundeliegenden K-Vektorräume ist.

K-linear abhängig sind. Seien $a_i \in K$ für $i = 0, 1, \ldots, n$ Koeffizienten von α^i einer linearen Relation und

$$f(T) = \sum_{i=0}^{n} a_i T^i$$

das zugehörige Polynom in $K[T]$. Dann ist $f \neq 0$ und $f(\alpha) = 0$, somit α algebraisch über K. $\square$

Genauer zeigt das Argument:

Korollar 23. *Sei L/K eine endliche Erweiterung und $\alpha \in L$. Dann erfüllt α eine algebraische Gleichung vom Grad $\leq [L : K]$, also*

$$\deg(P_{\alpha/K}) \leq [L : K].$$

Lemma 24. *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann ist α auch algebraisch über jedem Zwischenkörper M von L/K.*

Beweis. Das folgt direkt aus der Definition, denn ein $f \in K[T]$ mit $f(\alpha) = 0$ liegt auch in $M[T]$. $\square$

Korollar 25. *Seien α und β algebraische Elemente einer Erweiterung L/K. Dann sind auch*

$$\alpha + \beta, \ \alpha\beta, \ 1/\alpha \ (\text{sofern } \alpha \neq 0)$$

algebraisch über K.

Beweis. Es ist β algebraisch über $M = K(\alpha)$, siehe Lemma 24, und daher $K(\alpha, \beta) = M(\beta)$ endlich über M nach Korollar 20. Damit ist auch

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K]$$

endlich. Der Körper $K(\alpha, \beta)$ enthält die fraglichen Elemente, also sind diese algebraisch nach Lemma 22. $\square$

Proposition 26. *Seien L/K eine Körpererweiterung und M ein Zwischenkörper. Dann sind äquivalent:*

(a) L/K *endlich.*
(b) L/K *endlich erzeugt und algebraisch.*
(c) L/K *von endlich vielen algebraischen Elementen erzeugt.*
(d) M/K *und* L/M *endlich.*

Beweis. (a) $\Longrightarrow$ (b) Sei L/K endlich. Dann ist L/K endlich erzeugt, etwa durch eine endliche K-Basis von L als Vektorraum. Nach Lemma 22 ist L/K algebraisch.

(b) $\Longrightarrow$ (c) ist offensichtlich.

(c) $\Longrightarrow$ (a) Sei $L = K(\alpha_1, \ldots, \alpha_r)$ für algebraische Elemente $\alpha_i \in L$. Sei $K_i = K(\alpha_1, \ldots, \alpha_i)$ mit $K = K_0$ und $L = K_r$. Nach Lemma 24 ist α_i algebraisch über K_{i-1}, ergo K_i/K_{i-1} endlich und somit (per Induktion) nach dem Gradsatz, Satz 10,

$$[L : K] = \prod_{i=1}^{r} [K_i : K_{i-1}] < \infty$$

also L/K endlich.

(a) $\Longleftrightarrow$ (d) Dies ist Bestandteil des Gradsatzes, Satz 10. $\square$

Lemma 27. *Sei L/K eine Körpererweiterung und $A \subseteq L$ eine Teilmenge mit $L = K(A)$. Dann ist L die Vereinigung der endlich erzeugten Zwischenerweiterungen $K(B)$, wobei B über alle endlichen Teilmengen von A läuft.*

Beweis. Das folgt sofort aus der Definition. Die Vereinigung der $K(B)$ ist ein Körper, denn mit $x \in K(B)$ und $x' \in K(B')$ für endliche Teilmengen $B, B' \subseteq A$ gilt

$$x + x', \; xx', \; 1/x \in K(B \cup B')$$

($1/x$ natürlich nur, wenn $x \neq 0$). Die Vereinigung ist dann offensichtlich der kleinste Zwischenkörper, der alle endlichen Teilmengen von A enthält, also A enthält, also der Körper $K(A) = L$. □

Bemerkung 28. Lemma 27 besagt, daß in einer Erweiterung $K(A)/K$ jedes Element $x \in K(A)$ als Quotient von Polynomen in endlich vielen Elementen von A geschrieben werden kann.

Proposition 29. *Seien L/K eine Körpererweiterung und M ein Zwischenkörper. Dann sind äquivalent:*

(a) *L/K algebraisch.*
(b) *L ist als Körpererweiterung von K von über K algebraischen Elementen erzeugt.*
(c) *L ist Vereinigung von über K endlichen Körpern.*
(d) *M/K und L/M algebraisch.*

Beweis. (a) $\Longrightarrow$ (b) Das ist klar: L ist über K von der Menge L erzeugt.

(b) $\Longrightarrow$ (c) Sei $L = K(A)$ mit A bestehend aus über K algebraischen Elementen. Für eine endliche Teilmenge $B \subseteq A$ ist der Zwischenkörper $K(B)$ von algebraischen Elementen endlich erzeugt, also nach Proposition 26 auch endlich über K. Dann folgt (c) aus Lemma 27.

(c) $\Longrightarrow$ (a) Sei $L = \bigcup_{i \in I} M_i$ für Zwischenkörper M_i, die endlich über K sind. Jedes $x \in L$ liegt dann in M_i für ein geeignetes i. Nach Lemma 22 ist damit x algebraisch über K.

(a) $\Longrightarrow$ (d) ist trivial, siehe Lemma 24.

(d) $\Longrightarrow$ (a) Sei $x \in L$ beliebig. Da L/M algebraisch ist, gibt es $0 \neq f \in M[T]$ mit $f(x) = 0$. Seien $a_1, \ldots, a_d$ die Koeffizienten von f. Da M/K algebraisch ist, ist $M_0 = K(a_1, \ldots, a_d)$ über K endlich von algebraischen Elementen erzeugt, also nach Proposition 26 endlich über K. Außerdem ist x immer noch algebraisch über M_0, eben mit demselben $f \in M_0[T]$.

Als sukzessive Erweiterung der beiden endlichen Erweiterungen $M_0(x)/M_0$ und M_0/K ist $M_0(x)/K$ endlich. Damit ist $x \in M_0(x)$ nach Lemma 22 algebraisch über K. □

Korollar 30. *Sei L/K eine Körpererweiterung. Die Menge*

$$L_a := \{\alpha \in L \; ; \quad \textit{algebraisch über } K\}$$

ist ein Zwischenkörper und maximal unter allen über K algebraischen Zwischenkörpern von L/K.

Beweis. Nach Proposition 29 ist der Zwischenkörper $K(L_a)$ algebraisch über K. Also gilt

$$L_a = K(L_a),$$

und L_a ist in der Tat ein Körper. Offensichtlich ist jeder über K algebraische Zwischenkörper in L_a enthalten, somit ist L_a maximal. □

Definition 31. Der **relative algebraische Abschluß** eines Körpers K in einer Körpererweiterung L/K ist der Körper L_a aller über K algebraischen Elemente von L.

3.4. **Einfache Erweiterungen.**

Definition 32. Eine **einfache** (oder **monogene**) Körpererweiterung ist eine algebraische Körpererweiterung L/K, die von einem Element $\alpha \in L$ erzeugt werden kann. Ein solches Element $\alpha \in L$ mit $L = K(\alpha)$ heißt **primitives Element** für L/K.

Satz 33. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent.*

(a) *Es hat L/K nur endlich viele Zwischenkörper.*
(b) *L/K ist einfache Körpererweiterung.*

Beweis. Wir müssen unterscheiden zwischen endlichen K und unendlichem K.

Fall K endlich: Wir zeigen, daß in diesem Fall beide Aussagen wahr sind. Zunächst ist L als K-Vektorraum $L \simeq K^n$ mit $n = [L : K]$ und damit auch endlich. Offensichtlich gibt es dann nur endliche viele Zwischenkörper (sogar nur endlich viele Teilmengen).

Zum andern ist $L^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers und damit zyklisch, wie wir in Theorem 117 zeigen. Sei α ein Erzeuger von $L^\times$. Dann ist $L = K(\alpha)$.

Fall K unendlich: Es habe L/K nur endlich viele Zwischenkörper. Als endliche Körpererweiterung ist L/K endlich erzeugt. Es sei $\alpha_1, \ldots, \alpha_r$ ein Erzeugendensystem (als Körper) minimaler Länge. Wir führen nun $r \geq 2$ zu einem Widerspruch. Wenn wir zeigen können, daß $K(\alpha_1, \alpha_2)$ durch ein Element β erzeugt werden kann, dann ist $\beta, \alpha_3, \ldots, \alpha_r$ ein kürzeres Erzeugendensystem, also der gesuchte Widerspruch.

Da die Voraussetzung (b) auch für alle Zwischenkörper gilt, dürfen wir L durch $K(\alpha_1, \alpha_2)$ ersetzen. Anders ausgedrückt dürfen wir oBdA annehmen, daß $L = K(\alpha, \beta)$ von zwei Elementen erzeugt wird. Wir setzen für $t \in K$

$$c_t = \alpha + t\beta$$

Dann betrachte für $t \in K$ den Zwischenkörper

$$M_t = K(c_t)$$

Wenn es nur endlich viele Zwischenkörper gibt, aber $t \in K$ aus einer unendlichen Menge gewählt werden kann, dann muß es $s \neq t \in K$ geben mit $M_t = M_s$. In diesem Körper gibt es dann auch

$$\alpha = \frac{sc_t - tc_s}{s - t}$$
$$\beta = \frac{c_t - c_s}{t - s}.$$

Also $L = M_t = M_s$, somit kann man im Erzeugendensystem α, β durch $\alpha + t\beta$ ersetzen.

Jetzt müssen wir noch umgekehrt zeigen, daß ein $L = K(\alpha)$ mit α algebraisch nur endlich viele Zwischenkörper hat. Wir definieren dazu die folgende Abbildung

$$\{M \ ; \ K \subseteq M \subseteq L \text{ Zwischenkörper}\} \to \mathcal{T} := \{\text{normierte Teiler von } P_{\alpha/K}(T) \text{ in } L[T]\}$$
$$M \mapsto P_{\alpha/M}(T)$$

Die Abbildung ist wohldefiniert, denn sogar in $M[T]$ gilt schon

$$P_{\alpha/M}(T) \mid P_{\alpha/K}(T)$$

aufgrund der definierenden Eigenschaft des Minimalpolynoms und $P_{\alpha/K}(\alpha) = 0$.

Sei M ein Zwischenkörper und M_0 der über K von den Koeffizienten von $P_{\alpha/M}(T)$ erzeugte Zwischenkörper. Dann ist

$$K \subseteq M_0 \subseteq M \subseteq L$$

und analog zur Überlegung der Wohldefiniertheit

$$P_{\alpha/M}(T) \mid P_{\alpha/M_0}(T).$$

Andererseits ist per Konstruktion bereits $P_{\alpha/M}(T) \in M_0[T]$, so daß

$$P_{\alpha/M}(T) = P_{\alpha/M_0}(T).$$

Damit gilt

$$[L : M] = \deg(P_{\alpha/M}) = \deg(P_{\alpha/M_0}) = [L : M_0]$$

und folglich

$$[M : M_0] = [L : M_0]/[L : M] = 1$$

also

$$M = M_0.$$

Wir sehen also, daß die Koeffizienten des Minimalpolynoms über M den Zwischenkörper M erzeugen. Die Abbildung in $\mathcal{T}$ ist somit injektiv. Da $\mathcal{T}$ endlich ist (in einem Haupidealring hat jedes Element bis auf Assoziiertheit nur endlich viele Teiler) folgt die Behauptung. □

3.5. **Konstruktionen mit Zirkel und Lineal.** Um die Kraft des bereits über Körpererweiterungen Gelernten zu demonstrieren, wenden wir uns der geometrischen Fragestellung zu, welche Punkte der Ebene durch Zirkel und Lineal zu konstruieren sind. Nach der reinen alt-griechischen Lehre sind dies die einzigen gültigen Konstruktionsmethoden.

Wir stellen zunächst die Spielregeln auf. Wir betrachten die Punkte der **Ebene** E gegeben als

$$\mathbb{R}^2 \simeq \mathbb{C}.$$

Eine **Gerade** ist eine Punktmenge in E, welche für fest gegebene $a, b, c \in \mathbb{R}$ mit a, b nicht beide 0 die Form

$$L = L_{a,b;c} = \{(x, y); ax + by = c\}$$

hat. Durch je zwei verschiedene Punkte $P, Q \in E$ gibt es genau eine Gerade, die P, Q enthält.

Ein **Kreis** (oder **Kreislinie**) vom Radius $0 \leq r \in \mathbb{R}$ und Mittelpunkt $P = (x_0, y_0)$ in E ist die Menge

$$C = C_r(P) = \{(x, y) \ ; \ (x - x_0)^2 + (y - y_0)^2 = r^2\}.$$

Definition 34 (Konstruktionen mit Zirkel und Lineal)**.** Sei $M \subseteq E$ eine Punktmenge in der Ebene gegeben.

(1) Eine **konstruierbare Gerade** ist eine Gerade durch zwei verschiedene Punkte aus M.
(2) Ein(e) **konstruierbare(r) Kreis(linie)** ist eine Kreislinie mit Mittelpunkt aus M und Radius dem euklidischen Abstand zweier Punkte aus M.

Dann können mit Zirkel und Lineal die folgenden Punkte in einem Schritt konstruiert werden: Ein Schnittpunkt

(1) zweier konstruierbarer Geraden,
(2) einer konstruierbaren Geraden mit einer konstruierbaren Kreislinie,
(3) zweier konstruierbarer Kreislinien.

Die **mit Zirkel und Lineal aus** M **konstruierbaren Punkte** sind alle Punkte der Ebene P für die es eine Folge von Punkten $P_1, \ldots, P_n = P$ gibt, so daß P_{i+1} in einem Schritt aus $M \cup \{P_1, \ldots, P_i\}$ konstruiert werden kann. Die Menge aller ausgehend von M konstruierbaren Punkte der Ebene bezeichnen wir mit

$$\mathrm{ZL}(M).$$

Wir erinnern an die folgenden Konstruktionen mit Zirkel und Lineal:

- Die **Mittelsenkrechte** zu zwei Punkten P, Q: Das ist die Gerade durch die Schnittpunkte zweier Kreise $C_r(P)$ und $C_r(Q)$ mit r größer als der halbe Abstand von P und Q: etwa $r =$ Abstand von P und Q.

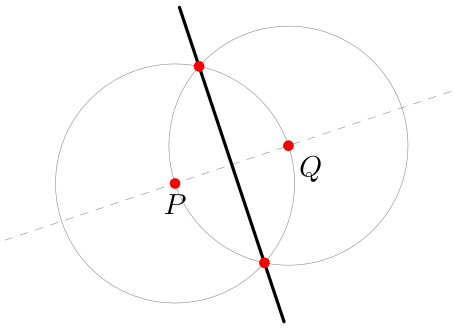

ABBILDUNG 1. Mittelsenkrechte zu P und Q.

- Die **(orthogonale) Projektion** von einem Punkt P auf eine Gerade L: das ist der Schnitt S von L mit der Mittelsenkrechten durch $\{Q_1, Q_2\} = L \cap C_r(P)$ mit r größer als der Abstand von P zu L.

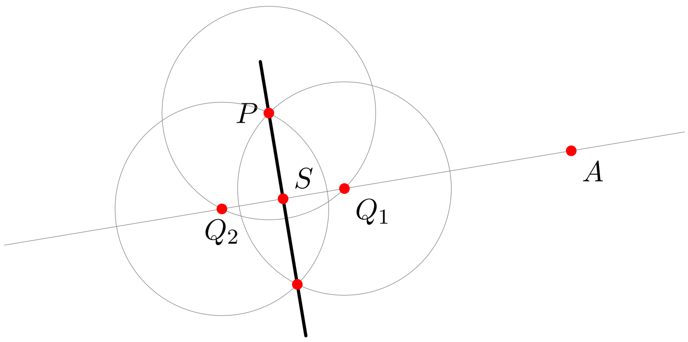

ABBILDUNG 2. Projektion von P auf die Gerade L durch Q_1 und A ist S.

- Die Parallele durch einen Punkt P zu einer Geraden L gegeben durch die Punkte A und B: hierzu bestimmt man den (richtigen) Schnittpunkt Q der Kreise um P mit Radius dem Abstand AB und um B mit Radius dem Abstand AP. Die gesuchte Parallele ist die Gerade durch P und Q (und $ABPQ$ beschreibt ein Parallelogramm).

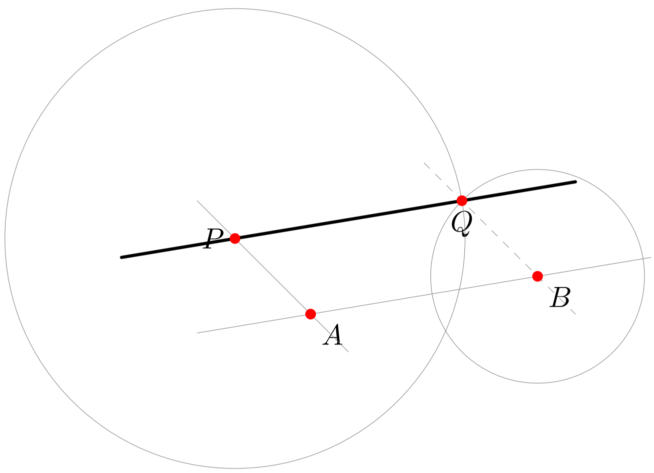

ABBILDUNG 3. Parallele durch P zur Gerade L durch A und B.

Zunächst bestehe $M = \{P\}$ aus genau einen Punkt P. Dann ist

$$\mathrm{ZL}(\{P\}) = \{P\},$$

denn aus einem Punkt kann man weder eine Gerade noch einen Kreis mit positivem Radius machen.

Translationen und Rotationen der Ebene führen Konstruktionen mit Zirkel und Lineal in ebensolche über. Wenn wir mindestens 2 Punkte $P \neq Q$ in M haben, dann können wir nach Translation und Rotation oBdA annehmen, daß $P = 0$ und $Q = 1$ als Punkte von $\mathbb{C}$ sind. Wir nehmen deshalb von jetzt ab an, daß oBdA $0, 1 \in M$.

Proposition 35. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$. Dann sind die reelle und die imaginäre Koordinatenachse konstruierbare Geraden in $\mathbb{C}$. Insbesondere kann die Teilmenge*

$$\mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$$

von $\mathbb{C}$ konstruiert werden.

Beweis. Wir tragen auf der Geraden durch 0 und 1 den Abstand dieser zwei Punkte, also 1, mit dem Zirkel in beide Richtungen fortlaufend ab und konstruieren so $\mathbb{Z} \subseteq \mathbb{C}$. Sodann konstruieren wir die Mittelsenkrechte zu 1 und -1 als Gerade durch die Schnittpunkte

$$\{\sqrt{3}i, -\sqrt{3}i\} = C_2(-1) \cap C_2(1)$$

der beiden Kreise $C_2(-1)$ und $C_2(1)$. Diese Mittelsenkrechte schneiden wir mit dem Kreis um 0 vom Radius 1 und erhalten $\pm i$.

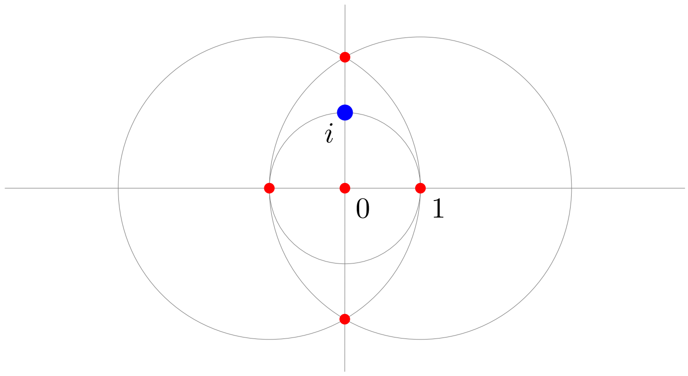

ABBILDUNG 4. Konstruktion von $i \in \mathbb{C}$.

Durch fortlaufendes Abtragen des Abstands 1 mit dem Zirkel auf der Geraden durch $-i, i$ konstruieren wir $\mathbb{Z}i \subseteq \mathbb{C}$.

Den Punkt $n+mi$ mit $n, m \in \mathbb{Z}$ erhalten wir nun als Schnitt der Parallelen zu den konstruierten Koordinatenachsen durch die Punkte n und mi. □

Bemerkung 36. Ohne den Begriff der Orientierung kann man nicht zwischen i und $-i$ unterscheiden!

Wir betrachten nun auch die rellen konstruierbaren Zahlen

$$\mathrm{ZL}^+(M) = \mathrm{ZL}(M) \cap \mathbb{R}.$$

Proposition 37. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$.*

(1) Ein $z = x + iy \in \mathbb{C}$ ist genau dann aus M konstruierbar, wenn Realteil x und Imaginärteil y als Punkte von $\mathbb{R} \subseteq \mathbb{C}$ konstruierbar sind.

(2) Es gilt

$$\mathrm{ZL}(M) = \mathrm{ZL}^+(M) + \mathrm{ZL}^+(M)i.$$

Beweis. (2) folgt sofort aus (1). Sei nun $z = x + iy \in \mathbb{C}$ konstruiert. Durch Projektion auf die Koordinatenachsen erhalten wir x, iy. Durch Drehen (Kreis um 0 durch iy geschnitten mit der reellen Achse) von der imaginären Achse zur reellen Achse erhalten wir aus iy auch y.

Seien nun umgekehrt $x, y \in \mathbb{R}$ konstruiert. Dann kann man durch Drehen und Schnitt mit der imaginären Achse aus y auch iy konstruieren. Sodann konstruiert man parallele Geraden durch x und iy parallel zur imaginären bzw. reellen Achse. Im Schnittpunkt befindet sich der damit konstruierte Punkt $z = x + iy$. □

Satz 38. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$. Dann ist $\mathrm{ZL}(M)$ ein Unterkörper von $\mathbb{C}$.*

Beweis. Man gebe Konstruktion an, wie man reelle Zahlen addieren, multiplizieren und (wenn $\neq 0$ auch) invertieren kann.

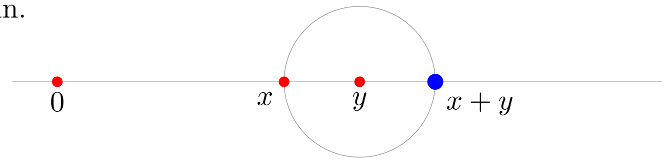

Abbildung 5. Addition von $x, y \in \mathbb{R}$ mit Zirkel und Lineal.

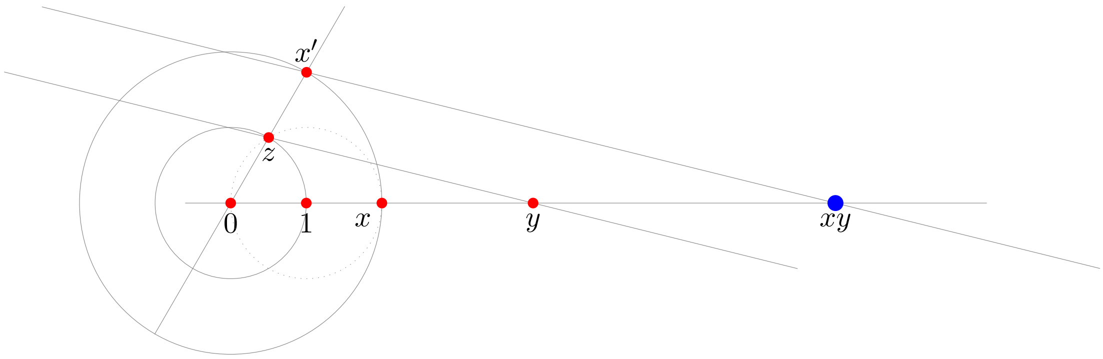

Abbildung 6. Multiplikation von $x, y \in \mathbb{R}$ mit Zirkel und Lineal.

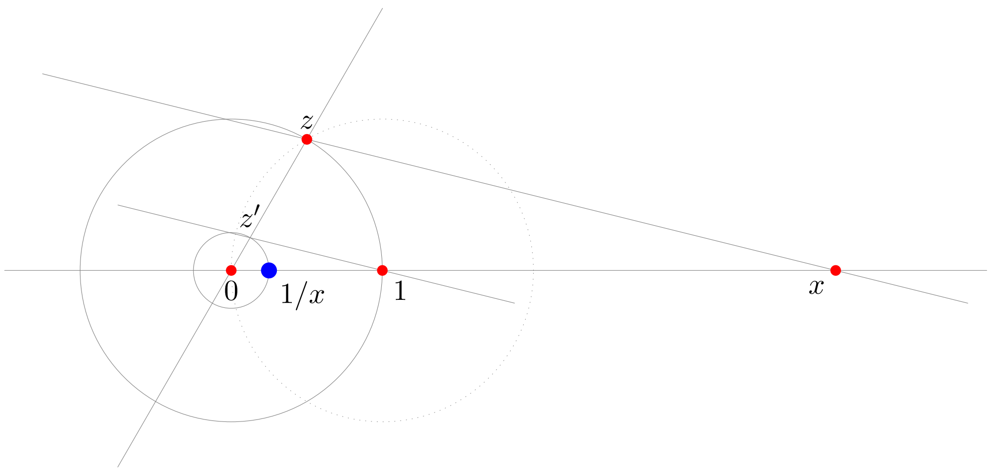

Abbildung 7. Inverses von $x \in \mathbb{R}$ mit Zirkel und Lineal.

Aus Proposition 37 und den Formeln für Summe, Produkt und Inverses komplexer Zahlen $z = x + iy$ und $w = a + ib$ ausgedrückt über Real- und Imaginärteil

$$\begin{aligned} z + w &= (x + a) + i(y + b), \\ zw &= (xa - yb) + i(xb + ya), \\ z^{-1} &= \frac{x - iy}{x^2 + y^2}, \end{aligned}$$

folgt dann sofort der Satz. □

Satz 39. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$. Dann ist $\mathrm{ZL}(M)$ abgeschlossen unter Quadratwurzelziehen.*

Beweis. Sei $z = re^{i\varphi}$ konstruiert. Wir zeigen, daß dann auch $\sqrt{r}$ und $\pm e^{i\varphi/2}$ konstruiert werden können. Damit sind die Quadratwurzeln $\sqrt{z}$ als

$$\pm\sqrt{r}e^{i\varphi/2}$$

auch konstruierbar wegen Satz 38.

Die Zahl $\pm e^{i\varphi/2}$ ergibt sich aus der bekannten Konstruktion der Winkelhalbierenden und anschließendem Schnitt mit dem Kreis von Radius 1 um 0.

Für $\sqrt{r}$ tragen wir auf der reellen Achse mit dem Zirkel die Punkte -1 und r ab. Wir finden die Mitte $P = (r - 1)/2$ als Schnitt der Mittelsenkrechten, und konstruieren den Kreis um P mit Radius $(r + 1)/2$, also durch -1 und r.

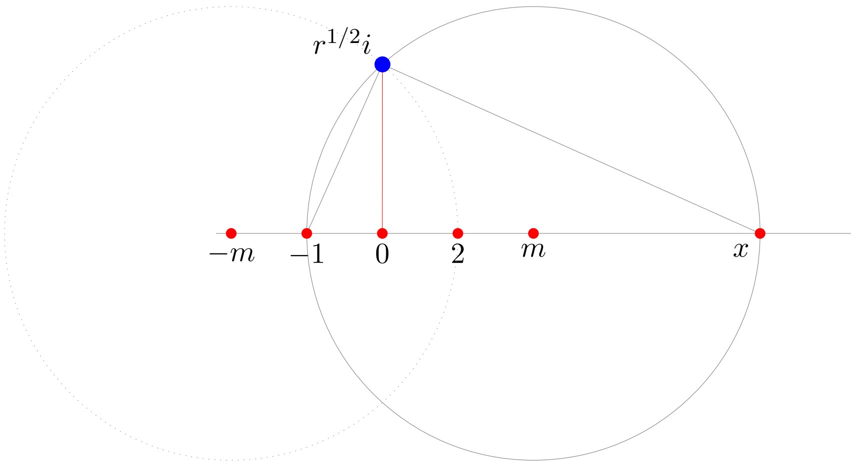

Abbildung 8. $\sqrt{r}$ mittels Höhensatz.

Dieser Kreis schneidet die imaginäre Achse nach dem Höhensatz der Dreiecksgeometrie in rechtwinkligen Dreiecken (Satz des Thales!) in den Punkten $\pm\sqrt{r}i$. Der Abstand von 0 beträgt somit $\sqrt{r}$. □

Definition 40. (1) Eine **quadratische Körpererweiterung** ist eine Erweiterung L/K vom Grad $[L : K] = 2$.

(2) Ein **quadratisch abgeschlossener** Körper ist eine Körper K, der keine quadratischen Körpererweiterungen hat.

Beispiel 41. Jede quadratische Erweiterung L/K ist einfach $L = K(\alpha)$, und zwar mit jedem $\alpha \in L$, $\alpha \notin K$. Eine quadratische Körpererweiterung liefert damit ein irreduzibles quadratisches Polynom als Minimalpolynom eines Erzeugers. Aus Satz 4 folgt, daß $\mathbb{C}$ quadratisch abgeschlossen ist. Dies ist ein erster Schritt zum Fundamentalsatz der Algebra.

Das folgende Lemma überlassen wir als Übungsaufgabe.

Lemma 42. *Sei K ein Körper mit $2 \in K^\times$. Sei L/K eine quadratische Erweiterung. Dann gibt es ein $a \in K$ und $\alpha = \sqrt{a} \in L$, d.h. $\alpha^2 = a$, mit $L = K(\alpha)$.*

Satz 43. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$. Dann ist $\mathrm{ZL}(M)$ der kleinste Oberkörper von $\mathbb{Q}(M)$ in $\mathbb{C}$, der quadratisch abgeschlossen ist.*

Beweis. Wir zeigen zunächst, daß $\mathrm{ZL}(M)$ quadratisch abgeschlossen ist. Gemäß Lemma 42 reicht es zu zeigen, daß mit $z \in \mathrm{ZL}(M)$ auch $\sqrt{z} \in \mathrm{ZL}(M)$ folgt. Das ist Satz 39.

Jetzt überlegen wir uns, daß der kleinste quadratisch abgeschlossene Oberkörper L von $K_0 = \mathbb{Q}(M)$ in $\mathbb{C}$ existiert und wie folgt zu finden ist. Wir nehmen an, daß K_n für $n \in \mathbb{N}_0$ bereits definiert ist. Wir setzen

$$A_n = \{z \in \mathbb{C} \ ; \ [K_n(z) : K_n] = 2\}$$

und definieren in $\mathbb{C}$

$$K_{n+1} = K_n(A_n).$$

Dann ist $L = \bigcup_n K_n$. Offensichtlich ist L ein Körper und in jedem quadratisch abgeschlossenen Zwischenkörper von $\mathbb{C}/\mathbb{Q}(M)$ enthalten. Nehmen wir an, daß $M = L(\alpha)$ ist eine weitere quadratische Zwischenerweiterung. Das Minimalpolynom von α hat Koeffizienten in K_n für n groß genug. Damit ist $\alpha \in A_n \subseteq K_{n+1}$, im Widerspruch zu $[L(\alpha) : L] = 2$.

Damit ist L quadratisch abgeschlossen und minimal mit dieser Eigenschaft unter den Zwischenkörpern von $\mathbb{C}/\mathbb{Q}(M)$.

Da $\mathrm{ZL}(M)$ quadratisch abgeschlossen ist, folgt $L \subseteq \mathrm{ZL}(M)$. Andererseits ensteht $\mathrm{ZL}(M)$ aus $\mathbb{Q}(M)$ durch iteriertes Hinzufügen von konstruierbaren Punkten. Wir zeigen gleich, daß dies jeweils Erweiterungen vom Grad 1 oder 2 sind. Damit gilt auch $\mathrm{ZL}(M) \subseteq L$ und der Satz ist bewiesen.

Es reicht die Erweiterung $\mathbb{Q}(M)(P)/\mathbb{Q}(M)$ für einen in einem Schritt konstruierbaren Punkt P zu studieren. Die weiteren Schritte sind ensprechend mit neuem eventuell größeren M.

Die reellen Koordinaten des Schnittpunkts zweier Geraden, welche aus M konstruiert werden, sind Lösungen linearer Gleichungen mit Koeffizienten aus $\mathbb{Q}(M)$. Damit ist dieser Punkt bereits in $\mathbb{Q}(M)$.

Die reellen Koordinaten des Schnittpunkts einer Geraden und einer Kreislinie, welche aus M konstruiert werden, sind Lösungen einer linearen Gleichung und einer quadratischen Gleichung mit Koeffizienten aus M. Man löst die lineare Gleichung nach einer reellen Koordinate auf und substituiert diese in die quadratische Gleichung. Damit sind die Koordinaten in einer höchstens quadratischen Erweiterung von $\mathbb{Q}(M)$ enthalten.

Jetzt betrachten wir die Koordinaten der Schnittpunkte zweier Kreislinien, welche aus M konstruiert werden. Die Gleichungen sind der Form

$$(X - x_0)^2 + (Y - y_0)^2 = r^2.$$

Entscheidend ist nun, daß der rein quadratische Teil $X^2 + Y^2$ für beide Gleichungen gleich ist. Die Differenz der beiden Gleichungen ist somit linear und beschreibt eine Gerade, die aus $\mathbb{Q}(M)$ konstruiert werden kann. Damit können wir nun genauso vorgehen, wie im Fall des Schnitts einer Gerade mit einem Kreis. □

Korollar 44. *Sei M eine Teilmenge der Ebene mit $0, 1 \in M$. Ein $z \in \mathbb{C}$ ist konstruierbar aus M genau dann, wenn es einen Körperturm $L = K_n \supseteq K_{n-1} \supseteq \ldots \supseteq K_1 \supseteq K_0 = \mathbb{Q}(M)$ gibt mit $z \in L$ und $[K_i : K_{i-1}] = 2$ für alle i.*

Beweis. Das folgt sofort aus der Konstruktion von $L = \mathrm{ZL}(M)$ im Beweis von Satz 43. □

Korollar 45. *Ist $z \in \mathbb{C}$ aus $\{0, 1\}$ konstruierbar, dann ist α algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ ist eine 2-er Potenz.*

Beweis. In der Notation von Korollar 44 ist $\mathbb{Q}(\alpha) \subseteq L$, also α algebraisch, und nach dem Gradsatz ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ ein Teiler von $[L : \mathbb{Q}] = 2^n$. □

Wir sind nun in der Lage im Wesentlichen als Anwendung des Gradsatzes einige klassische Fragen der Konstruierbarkeit mit Zirkel und Lineal zu beantworten.

Beispiel 46. Die **Quadratur des Kreises** ist unmöglich. Die Aufgabe verlangt, zu einem Kreis ein flächengleiches Quadrat zu konstruieren. Gegeben ist am Anfang ein Kreis mit Mittelpunkt P und einem Punkt auf der Kreislinie Q. Nach Translation und Rotation dürfen wir annehmen, daß der Mittelpunkt 0 und der Radius 1 sind, mit dem weitern Punkt gegeben durch 1. Die Kantenlänge eines zum Kreis flächengleichen Quadrats ist

$$\sqrt{\pi}$$

und diese reelle Zahl wäre mit dem Quadrat konstruierbar (man trage die Kantenlänge des Quadrats mit dem Zirkel auf der rellen Achse ab). Die Transzandenz von π impliziert die Transzendenz von $\sqrt{\pi}$ und damit die Unmöglichkeit der Quadratur des Kreises nach Korollar 45.

Beispiel 47. Das **Delisches Problem** der Würfelverdopplung ist nicht konstruierbar. Hier müssen wir eigentlich eine 3-dimensionale Version der Theorie der mit Zirkel und Lineal konstruierbaren Punkte aufstellen. Wir verstehen, wie allgemein üblich, die Aufgabe, die Zahl

$$\sqrt[3]{2}$$

aus $\{0, 1\}$ heraus zu konstruieren. Das Polynom $T^3 - 2$ ist irreduzibel in $\mathbb{Q}[T]$, denn die einzige reelle Nullstelle ist nicht rational. Damit gilt

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

Korollar 45 verbietet nun, daß $\sqrt[3]{2}$ konstruierbar ist.

Beispiel 48. Das **regelmäßige n-Eck**. Hat man ein regelmäßiges n-Eck konstruiert, dann hat man auch den Mittelpunkt U des Umkreises. Seien P_0 und P_1 aufeinanderfolgende Ecken im mathematisch positiven Drehsinnn. Dann gilt

$$\zeta_n := e^{2\pi/n} = \frac{P_1 - U}{P_0 - U}.$$

Dieses Element erfüllt $(\zeta_n)^n = 1$ und ist somit algebraisch über $\mathbb{Q}$. Es folgt sofort:

Satz 49. *Die folgenden Aussagen sind äquivalent.*

(a) *Das regelmäßige n-Eck ist konstruierbar.*
(b) *ζ_n ist aus $\{0, 1\}$ konstruierbar.*
(c) *Der Körper $\mathbb{Q}(\zeta_n)$ ist in einem Körperturm aus quadratischen Körpererweiterungen enthalten.*

Wir werden die Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ später genau studieren und dann ein Kriterium angeben können, für welche n das regelmäßige n-Eck konstruierbar ist.

Beispiel 50. Die **Dreiteilung eines allgemeinen Winkels**. Unter einem Winkel verstehen wir ein geordnetes Geradenpaar L_1, L_2 durch einen Punkt P und je einem Punkt $Q_i \in L_i$ für $i = 1, 2$ verschieden von P. Dazu gehört eine komplexe Zahl

$$w = \frac{Q_2 - P}{Q_1 - P}$$

so daß nach Translation mit P nach 0 die Gerade L_1 durch Multiplikation mit w in die Gerade L_2 übergeht. Winkeldreiteilung fragt nach einer Gerade L durch P mit einem Punkt $Q \in L$, so daß der komplexe Faktor

$$z = \frac{Q - P}{Q_1 - P}$$

der die Gerade L_1 auf L abbildet die folgende Eigenschaft hat:

$$z^3 \cdot L_1 = L_2.$$

Manche Winkel sind in diesem Sinne dreiteilbar: zum Beispiel 45° entsprechend

$$w = (1+i)/\sqrt{2}.$$

Dazu konstruiert man in der bekannten Weise ein regelmäßiges gleichseitiges Dreieck und damit den Winkel 60°. Die Differenz der beiden Winkel ist 15° und damit ein Drittel von 45°.

Algemeiner ist der Winkel zur komplexen Zahl $w = z^3$ dreiteilbar, wenn z bereits konstruierbar ist. Dies ist zwar eine tautologische Aussage, liefert aber mit $w = (a+bi)^3$ und $a, b \in \mathbb{Z}$ jede Menge dreiteilbare Winkel.

Jetzt diskutieren wir, daß im Allgemeinen die Winkeldreiteilung nicht möglich ist. Wir nehmen dazu an, daß $P = 0$, $Q_1 = 1$ und der Punkt Q_2 auf dem Kreis um 0 mit Radius 1 liegt. Damit ist w eine komplexe Zahl vom Betrag 1, wir suchen $z \in \mathbb{C}$ mit $z^3 = w$, und fragen danach, ob die Erweiterung

$$\mathbb{Q}(z)/\mathbb{Q}(w)$$

in einem Körperturm mit quadratischen Schritten enthalten ist. Aus $z^3 = w$ folgt, daß der Körpergrad $[\mathbb{Q}(z) : \mathbb{Q}(w)]$ nur die Werte 1, 2 oder 3 annehmen kann. Ein Widerspruch erhalten wir für den Wert 3.

Wir zeigen nun die Unmöglichkeit der Winkeldreiteilung im allgemeinen Fall, indem wir ein Gegenbeispiel angeben. Dazu wählen wir den Winkel 60°. Hier ist

$$w = (1 + i\sqrt{3})/2$$

selbst konstruierbar und vom Grad 2 über $\mathbb{Q}$. Angenommen, $\beta = 20°$,

$$z = \cos(\beta) + i\sin(\beta)$$

wäre konstruierbar, dann wäre $\xi = \cos(\beta)$ konstruierbar über $\mathbb{Q}$. Die Formeln für Winkelverdreifachung folgt aus den trigonometrischen Additionstheoremen:

$$\begin{aligned}\frac{1}{2} &= \cos(3\beta) = \cos(\beta)\cos(2\beta) - \sin(\beta)\sin(2\beta)\\ &= \cos(\beta)\big(\cos^2(\beta) - \sin^2(\beta)\big) - \sin(\beta)\big(2\sin(\beta)\cos(\beta)\big)\\ &= \xi\big(\cos^2(\beta) - 3\sin^2(\beta)\big) = \xi(4\xi^2 - 3).\end{aligned}$$

Damit erfüllt ξ die Gleichung

$$8\xi^3 - 6\xi - 1 = 0.$$

Lemma 51. *Das Polynom* $8T^3 - 6T - 1$ *ist irreduzibel in* $\mathbb{Q}[T]$.

Beweis. Andernfalls gäbe es eine Nullstelle $a/b \in \mathbb{Q}$ mit $a, b \in \mathbb{Z}$ und teilerfremd. Dann gilt

$$0 = b^3 f(a/b) = 8a^3 - 6ab^2 - b^3.$$

Aus $b^3 = 8a^3 - 6ab^2$ folgt $2 \mid b$. Aus $b^2(b + 6a) = 8a^3$ folgt $b^2 \mid 8$, und damit $b = \pm 2$. Außerdem folgt aus $a(8a^2 - 6b^2) = b^3$, daß $a \mid 1$. Wir müssen also nur die rationalen Zahlen $a/b = 1/2$ und $-1/2$ als Nullstellen testen. In beiden Fällen ist das negativ. □

Wir schließen

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

also keine 2-er Potenz und damit ist ξ nicht mit Zirkel und Lineal konstruierbar. Die Winkeldreiteilung von 60^o ist ohne weitere Hilfsmittel nicht möglich.

Übungsaufgaben zu §3

Übungsaufgabe 3.1. Es seien M_1 und M_2 Zwischenkörper einer Körpererweiterung L/K. Dann sind äquivalent:

(a) $M_1 = M_2$,

(b) $M_1 \subseteq M_2$ und $[M_2 : M_1] = 1$.

Übungsaufgabe 3.2. Sei $\sqrt[3]{5}$ die eindeutige reelle dritte Wurzel von 5, und sei $\zeta_3 = e^{2\pi i/3}$. Zeigen sie, daß der reelle Körper $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ zum komplexen Körper $\mathbb{Q}(\zeta_3 \cdot \sqrt[3]{5}) \subseteq \mathbb{C}$ isomorph ist.

Übungsaufgabe 3.3. Seien K_1 und K_2 zwei Körpererweiterungen von $\mathbb{Q}$. Zeigen Sie, daß $K_1 \simeq K_2$ als Körper genau dann wenn $K_1 \simeq K_2$ als Körpererweiterung von $\mathbb{Q}$.

Übungsaufgabe 3.4. Bestimmen Sie $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$.

Übungsaufgabe 3.5. Zeigen Sie, daß $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ nur endlich viele Zwischenkörper enthält.

Übungsaufgabe 3.6. Sei L/K eine quadratische Erweiterung eines Körpers K mit $2 \in K^\times$. Zeigen Sie, daß L aus K durch Adjunktion einer Quadratwurzel entsteht: es gibt ein $\alpha \in L$ mit $\alpha^2 \in K$ und $L = K(\alpha)$.

Welche Aussage liefert die Verallgemeinerung des Arguments für eine Erweiterung $K(\alpha)/K$ vom Grad n? Welche Voraussetzung braucht man hier?

Übungsaufgabe 3.7. Sei L/K eine endliche Erweiterung. Zeigen Sie, daß jeder Unterring $R \subseteq L$, der K enthält schon ein Körper ist.

4. Körpereinbettungen

4.1. **Grundsätzliches zum Auswerten von Polynomen.** Für jeden Ringhomomorphismus $\varphi : R \to S$ gibt es den zugehörigen Homomorphismus von Poynomringen

$$\Phi : R[T] \to S[T]$$

der auf Konstanten φ und $\Phi(T) = T$ abbildet, kurz: φ wird auf die Koeffizienten angewandt. Als Notation könnte man für $f = a_0 + a_1 T + \ldots$

$$\Phi(f) := {}^{\varphi}f := \varphi(a_0) + \varphi(a_1)T + \ldots$$

verwenden, aber oft unterdrücken wir diese Präzision zugunsten der besseren Lesbarkeit.

Bemerkung 52. Unter der Auswertung eines Polynoms $f = a_0 + a_1 T + a_2 T^2 + \ldots \in R[T]$ in einem Element $x \in S$ für einen Ringhomomorphsimus $\varphi : R \to S$ verstehen wir

$$f(x) = {}^{\varphi}f(x) = \varphi(a_0) + \varphi(a_1)x + \varphi(a_2)x^2 + \ldots \in S.$$

Die Notation $f(x)$ enthält nicht den Bezug zu $\varphi : R \to S$, ohne den die Auswertung aber keinen Sinn ergibt. Trotzdem wird $f(x)$ in der Regel ohne weitere Erklärung verstanden, weil φ implizit klar ist, etwa bei einem Unterring $R \subseteq S$ oder einem Unterkörper $K \subseteq L$.

4.2. **Adjunktion von Nullstellen.** In Kapitel 3.2 haben wir unter $K(\alpha)$ den von $\alpha \in L$ erzeugten Zwischenkörper von L/K verstanden. Nun adjungieren wir α als Nullstelle eines irreduziblen Polynoms (das wird sein Minimalpolynom sein) formal zu K hinzu. *Formal* bedeutet hierbei, daß es in der Konstruktion keinen a priori gegebenen alles enthaltenen Körper gibt.

Lemma 53. *Sei $f \in K[T]$ ein nicht-konstantes Polynom. Dann gibt es eine Körpererweiterung L/K in dem f eine Nullstelle hat.*

Beweis. Indem wir uns auf einen irreduziblen Faktor von f beschränken, dürfen wir annehmen, daß f selbst irreduzibel ist. Dann betrachten wir den Faktorring $L = K[T]/(f)$, in dem qua Definition das Bild $t = T + (f)$ von T unter der kanonischen Projektion eine Nullstelle von f ist: es gilt

$$f(t) = f(T) + (f) = 0.$$

Jetzt müssen wir noch einsehen, daß L eine Körpererweiterung von K ist. Der Ring L ist ein Körper nach Satz 6. Aus L wird eine Erweiterung von K durch die Einbettung $K \to K[T]$ auf die konstanten Polynome gefolgt von der Projektion $K[T] \twoheadrightarrow L$. Dies ist wegen Proposition 1 eine Einbettung, da $K \to K[T]/(f)$ nicht die Nullabbildung ist. $\square$

Bemerkung 54. Der Beweis zeigt genauer, daß man eine Nullstelle von f in einer Körpererweiterung L/K mit $[L:K] \leq \deg(f)$ finden kann.

Definition 55. Sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom. Eine Körpererweiterung L/K entsteht durch **Adjunktion einer Nullstelle** α von K, wenn gilt:
(i) $\alpha \in L$ mit $f(\alpha) = 0$,
(ii) $L = K(\alpha)$.

Wir haben in Proposition 17 gesehen, daß Minimalpolynome irreduzibel sind. Nun sehen wir, daß jedes irreduzible Polynom in geeigneter Weise ein Minimalpolynom ist.

Satz 56. *Sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom.*
(1) Es gibt eine Körpererweiterung L/K, die durch Adjunktion einer Nullstelle von f entsteht. Das Minimalpolynom dieser Nullstelle ist f (sofern f normiert ist).
(2) Je zwei solche Körper sind K-isomorph, sogar eindeutig, wenn man verlangt, daß die gewählten Nullstellen aufeinander abgebildet werden.

Beweis. (1) Sei L/K eine Erweiterung, in der f eine Nullstelle $\alpha \in L$ hat. So eine Erweiterung gibt es nach Lemma 53. Der Zwischenkörper $K(\alpha)$ entsteht durch Adjunktion der Nullstelle α.

Sei nun f normiert. Da $f(\alpha) = 0$, folgt
$$P_{\alpha/K} \mid f.$$
Weil zudem beide Polynome irreduzibel in $K[T]$ sind, folgt Gleichheit $f = P_{\alpha/K}$.

(2) Seien $K(\alpha)$ und $K(\beta)$ Körpererweiterungen von K, die durch Adjunktion einer Nullstelle von f entstehen. Dann sind α und β algebraisch und nach Satz 19 beide K-isomorph zu
$$K[T]/(f).$$
Daraus ergibt sich eine K-Isomorphie durch Komposition
$$K(\alpha) \simeq K[T]/(f) \simeq K(\beta),$$
die darüberhinaus eindeutig festgelegt ist, wenn man $\alpha \leftrightarrow T + (f) \leftrightarrow \beta$ fordert. □

4.3. Algebren über einem Körper.

Definition 57. Sei K ein Körper. Ein Ring A, der K als Unterring enthält wird **K-Algebra** genannt. Eine K-Algebra ist auch ein Vektorraum über K. Ein **K-Homomorphismus** (oder **K-Algebrahomomorphismus**)
$$f : A \to B$$
zwischen K-Algebren A, B ist ein Ringhomomorphismus, der auch K-linear bezüglich dieser K-Vektorraumstruktur ist. Die Menge aller solchen K-linearen Ringhomomorphismen wird mit $\mathrm{Hom}_K(A, B)$ oder genauer
$$\mathrm{Hom}_{K\text{-alg}}(A, B)$$
bezeichnet (wenn man den Unterschied zum K-Vektorraum der K-linearen Vektorraumhomomorphismen betonen möchte).

Ein bijektiver K-Homomorphismus ist ein **K-Isomorphismus** und bei Existenz eines K-Isomorphismus $f : A \to B$ heißen die K-Algebren A und B dann **K-isomorph**.

Beispiel 58. (1) Jede Körpererweiterung L/K macht aus L eine K-Algebra.
(2) Der Polynomring $K[T]$ ist eine K-Algebra.
(3) Der Ring $K[\varepsilon]$, der als K-Vektorraum die Basis $1, \varepsilon$ hat und dessen Multiplikation durch $\varepsilon^2 = 0$ erklärt ist, ist eine K-Algebra, genannt die **dualen Zahlen über** K. Dies ist nichts anderes als
$$K[\varepsilon] \simeq K[T]/(T^2)$$
mit einem K-Isomorphsimus $\varepsilon \leftrightarrow T + (T^2)$.

Bemerkung 59. Wenn man es noch allgemeiener möchte, dann kann man in Definition 57 den Körper K durch einen Ring R ersetzen und darauf verzichten, daß der Ringhomomorphismus $R \to A$ injektiv ist. Dann enthält man den Begriff der R-Algebra.

4.4. **Nullstellen und Einbettungen.** Wir wollen sehen, wie Nullstellen eines Polynoms Körpereinbettungen kontrollieren.

Proposition 60. *Sei K ein Körper, $f \in K[T]$ ein Polynom und A eine K-Algebra. Dann gibt es eine natürlich Bijektion zwischen K-Homomorphismen und Nullstellen:*

$$\begin{aligned} \mathrm{Hom}_K(K[T]/(f), A) &= \{\alpha \in A \ ; \ f(\alpha) = 0\} \\ (\sigma : K[T]/(f) \to A) &\mapsto \sigma(T). \end{aligned}$$

Natürlich bedeutet, daß für jeden K-Algebrahomomorphismus $\varphi : A \to B$ das folgende Diagramm von Mengen kommutiert.

$$\begin{tikzcd} \mathrm{Hom}_K(K[T]/(f), A) \arrow[r, equal] \arrow[d, "\sigma \mapsto \varphi\circ\sigma"'] & \{\alpha \in A \ ; \ f(\alpha) = 0\} \arrow[d, "\alpha \mapsto \varphi(\alpha)"] \\ \mathrm{Hom}_K(K[T]/(f), B) \arrow[r, equal] & \{\beta \in B \ ; \ f(\beta) = 0\}. \end{tikzcd}$$

Beweis. Ein K-Algebrahomomorphismus $\sigma : K[T]/(f) \to A$, wird eindeutig durch den Wert auf T (genauer der durch T repräsentierten Restklasse) festgelegt. Es sind genau die Werte möglich, für die $\sigma(f) = 0$ gilt. Aber

$$\sigma(f) = f(\sigma(T))$$

also kommen für die Bilder von T genau die Nullstellen von f in A in Frage.

Die Kommutativität des Diagramms folgt sofort aus den Definitionen der Abbidlungen. Ein Algebrahomomorphismus $\varphi : A \to B$ bildet Nullstellen von f in A auf Nullstellen in B ab:

$$0 = \varphi(f(\alpha)) = f(\varphi(\alpha)).$$

Daher ist die rechte vertikale Abbildung wohldefiniert. □

Korollar 61. *Sei $K(\alpha)$ eine Körpererweiterung von K, die durch Adjunktion der Nullstelle α des irreduziblen Polynoms f entsteht. Dann ist für jede Körpererweiterung L/K natürlich*

$$\mathrm{Hom}_K(K(\alpha), L) = \{\beta \in L \ ; \ f(\beta) = 0\}$$

durch

$$\big(\sigma : K(\alpha) \to L\big) \mapsto \sigma(\alpha).$$

Beweis. Dies folgt wegen $K(\alpha) \simeq K[T]/(f)$ sofort aus Proposition 60. Die Identifikationen von K-Homomorphismen mit Nullstellen hat die behauptete Form, da der isomorphismus $K(\alpha) \simeq K[T]/(f)$ das Element α auf (die Restklasse von) T schickt. □

Wir bekommen nun den wichtigen Satz über die Fortsetzbarkeit von Einbettungen.

Satz 62 (Fortsetzung von Einbettungen). *Sei L/K eine endliche Körpererweiterung und L_0 ein Zwischenkörper. Sei Ω_0/K eine weitere Erweiterung und*

$$\sigma_0 : L_0 \to \Omega_0$$

eine K-Einbettung. Dann gibt es eine endliche Körpererweiterung Ω/Ω_0 und eine Fortsetzung

$$\sigma : L \to \Omega,$$

d.h. eine K-Einbettung mit $\sigma|_{L_0} = \sigma_0$.

$$\begin{tikzcd} & L_0 \arrow[r] \arrow[d, "\sigma_0"] & L \arrow[d, dotted, "\sigma"] \\ K \arrow[ur] \arrow[dr] & & \\ & \Omega_0 \arrow[r] & \Omega \end{tikzcd}$$

Beweis. Bis auf die technische Reduktion auf den entscheidenden Schritt haben wir das bereits bewiesen.

Die Erweiterung L/K ist endlich erzeugt, etwa $L = K(\alpha_1, \dots, \alpha_n)$. Sei

$$K_i = K(\alpha_1, \dots, \alpha_i)$$

mit $K_0 = K$ und $L = K_n$. Wir argumentieren nun nach Induktion und zeigen, daß es zu

$$\sigma_i : K_i \to \Omega_i$$

eine endliche Erweiterung Ω_{i+1}/Ω_i und eine Fortsetzung

$$\sigma_{i+1} : K_{i+1} \to \Omega_{i+1}$$

gibt. Damit haben wir das Problem zerlegt (dévissage) auf den Fall einer einfachen Erweiterung $L = K(\alpha)$.

Sei nun $f \in K[T]$ das Minimalpolynom von α über K. Sei Ω/Ω_0 eine Erweiterung wie in Lemma 53, in der f eine Nullstelle $\xi \in \Omega$ hat. Dann entspricht ξ nach Korollar 61 einer K-Einbettung $L \to \Omega$. □

Wir müssen uns einen Überblick über die Nullstellenmengen von Polynomen verschaffen. Zunächst zeigen wir, daß Nullstellen zu Linearfaktoren führen.

Lemma 63. *Sei R ein Ring, $f \in R[T]$ ein Polynom und $\alpha \in R$ ein Element. Dann sind äquivalent.*

(1) $f(\alpha) = 0$ *in* R

(2) *Es gibt ein* $g \in R[T]$ *mit* $f = (T - \alpha)g$.

Beweis. (2) $\Longrightarrow$ (1) ist trivial.

Die umgekehrte Richtung folgt aus der Polynomdivision von f durch $T - \alpha$ in $R[T]$. Man beachte, daß Polynomdivision durch $T - \alpha$ wie gewöhnlich in Polynomringen mit Körperkoeffizienten durchführbar ist, weil $T - \alpha$ ein normiertes Polynom in $R[T]$ ist, somit stets in R nur durch 1 zu teilen ist. Es gibt somit Polynome $g, r \in R[T]$ mit

$$f = g(T - \alpha) + r$$

und r ist konstantes Polynom. Daher gilt

$$r = r(\alpha) = \big(f - (T - \alpha)g\big)|_{T=\alpha} = f(\alpha) - (\alpha - \alpha)g(\alpha) = 0$$

und somit $f = (T - \alpha)g$ in $R[T]$. □

Wenn wir betonen wollen, daß wir den Wertebereich der Nullstellen variieren können, formulieren wir die Aussage wie folgt.

Korollar 64. *Sei $f \in K[T]$ ein Polynom, und A eine K-Algebra. Sei $\alpha \in A$ ein Element. Dann sind äquivalent:*

(1) $f(\alpha) = 0$ *in* A,

(2) *Es gibt ein* $g \in A[T]$ *mit* $f = (T - \alpha)g$.

Beweis. Das ist Lemma 63 für $R = A$ angewandt auf das Bild $f \in A[T]$. □

Beispiel 65. Sei $f = T^2 \in K[T]$ und $A = K[\varepsilon]$. Es ist $a + b\varepsilon \in K[\varepsilon]$ mit $a, b \in K$ eine Nullstelle von f, genau wenn

$$0 = (a + b\varepsilon)^2 = a^2 + 2ab\varepsilon,$$

also wenn $a = 0$. Hat K mehr als 2 Elemente, so gibt es in $K[\varepsilon]$ mehr als $2 = \deg(T^2)$ Nullstellen von T^2. Zur Nullstelle $b\varepsilon$ gehört die Faktorisierung

$$T^2 = (T - b\varepsilon)(T + b\varepsilon) \in K[\varepsilon][T]$$

mit Linearfaktor $T - b\varepsilon$.

Im Kontrast zu obigem Beispiel verhalten sich Nullstellenmengen von Polynomen in Integritätsringen besser.

Satz 66. *Sei R ein Integritätsring (etwa ein Körper) und $f \in R[T]$ ein Polynom. Dann hat f höchstens $\deg(f)$ viele Nullstellen in R.*

Beweis. Sei $\alpha \in R$ eine Nullstelle. Nach Lemma 63 gibt es $g \in R[T]$ mit

$$f = (T - \alpha)g.$$

Sei $\beta \neq \alpha$ eine weitere Nullstelle. Dann gilt

$$0 = f(\beta) = (\beta - \alpha)g(\beta).$$

Da $\beta - \alpha \neq 0$ und R Integritätsring ist, folgt $g(\beta) = 0$. Somit gilt

$$\{\text{Nullstellen von } f \text{ in } R\} = \{\alpha\} \cup \{\text{Nullstellen von } g \text{ in } R\}.$$

Da $\deg(g) = \deg(f) - 1$ folgt die Aussage nun per Induktion über den Grad von f. □

Korollar 67. *Sei $K(\alpha)/K$ eine einfache Körpererweiterung und L/K eine beliebige Körpererweiterung. Dann gilt*

$$0 \leq \# \mathrm{Hom}_K(K(\alpha), L) \leq [K(\alpha) : K].$$

(Es kann auch gar keine geben!)

Beweis. Es gilt

$$\# \mathrm{Hom}_K(K(\alpha), L) = \#\{\text{Nullstellen von } P_{\alpha/K} \text{ in } L\} \leq \deg(P_{\alpha/K}) = [K(\alpha) : K],$$

nach Korollar 61, Satz 66 und Korollar 20. □

4.5. **Charaktere.** Die folgende Definition liefert die nötige Begrifflichkeit für Satz 71. Da wir diesen Satz aber nur für die multiplikative Gruppe eines Körpers anwenden, darf man über dieses Maß an Allgemeinheit im ersten Anlauf getrost hinwegsehen.

Definition 68. Eine **Halbgruppe** ist eine Menge P mit einer Verknüpfung

$$P \times P \to P,$$

die assoziativ ist.

Beispiel 69. (1) $\mathbb{N} = \{1, 2, 3, \ldots\}$ ist mit Addition eine Halbgruppe.
(2) $\mathbb{N}$ ist mit der Multiplikation eine Halbgruppe.
(3) $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ auch. Hat sogar ein neutrales Element.
(4) Jede Gruppe ist eine Halbgruppe.
(5) Sei R ein Ring. Dann ist R mit der Multiplikation eine Halbgruppe.

Definition 70. Ein **Charakter** einer Halbgruppe P mit Werten in einem Körper K ist eine Abbildung

$$\sigma : P \to K^\times$$

mit $\sigma(pq) = \sigma(p)\sigma(q)$ für alle $p, q \in P$.

Wir erinnern daran, daß für eine beliebige Menge X und einen Körper K die Menge der Abbildungen

$$\mathrm{Maps}(X, K) = \{f \ ; \ f : X \to K \text{ Abbildung}\}$$

durch punktweise Addition und Skalarmultiplikation zu einem K-Vektorraum wird.

Satz 71 (Dedekind, Lineare Unabhängigkeit der Charaktere)**.** *Sei P eine Halbgruppe und K ein Körper. Dann sind die Charaktere von P mit Werten in K, aufgefaßt als Elemente von*

$$\mathrm{Maps}(P, K),$$

K-linear unabhängig.

Beweis. Wir argumentieren durch Widerspruch. Für $i = 1, \ldots r$ sei $\lambda_i \in K$ und $\sigma_i : P \to K^\times$ paarweise verschiedene Charaktere, so daß

$$\sum_{i=1}^{r} \lambda_i \sigma_i = 0$$

eine nicht-triviale K-lineare Relation minimaler Länge r ist. Dann ist sicher $r \geq 2$. Wir wählen $x \in P$ mit $\sigma_1(x) \neq \sigma_2(x)$ und finden für alle $p \in P$

$$0 = \sum_{i=1}^{r} \lambda_i \sigma_i(xp) = \sum_{i=1}^{r} \lambda_i \sigma_i(x) \cdot \sigma_i(p)$$

also die beiden K-linearen Relationen

$$0 = \sum_{i=1}^{r} \lambda_i \sigma_i(x) \cdot \sigma_i$$

und

$$0 = \sigma_1(x) \cdot \sum_{i=1}^{r} \lambda_i \sigma_i = \sum_{i=1}^{r} \lambda_i \sigma_1(x) \cdot \sigma_i$$

In der Differenz fällt der Summand zu $i = 1$ weg, der zu $i = 2$ bleibt bestehen:

$$0 = \sum_{i=2}^{r} \lambda_i (\sigma_i(x) - \sigma_1(x)) \sigma_i,$$

die neue Relation ist also kürzer, aber nicht ganz verschwunden: Widerspruch. □

Korollar 72. *Seien L/K und Ω/K Körpererweiterungen. Dann gilt*

$$\# \operatorname{Hom}_K(L, \Omega) \leq [L : K].$$

Beweis. Sei $\operatorname{Hom}_{K-\mathrm{lin}}(L, \Omega)$ die Menge der K-linearen Abbildungen der K-Vektorräume L und Ω. Punktweise Addition und Skalarmultiplikation definiert auf $\operatorname{Hom}_{K-\mathrm{lin}}(L, \Omega)$ die Struktur eines Ω-Vektorraums, ein Ω-Untervektorraum von $\mathrm{Maps}(L, \Omega)$. Es gilt

$$\operatorname{Hom}_{K-\mathrm{lin}}(L, \Omega) \simeq \operatorname{Hom}_{K-\mathrm{lin}}(K^{[L:K]}, \Omega) \simeq \operatorname{Hom}_{K-\mathrm{lin}}(K, \Omega)^{[L:K]} \simeq \Omega^{[L:K]}$$

Aus Satz 71 angewandt auf $P = L^\times$ folgt sofort, daß die Menge $\operatorname{Hom}_K(L, \Omega)$ eine Ω-linear unabhängige Teilmenge von $\operatorname{Hom}_{K-\mathrm{lin}}(L, \Omega)$ ist. Damit gilt

$$\# \operatorname{Hom}_K(L, \Omega) \leq \dim_\Omega \operatorname{Hom}_{K-\mathrm{lin}}(L, \Omega) = [L : K].$$

□

4.6. Normale Erweiterungen.

Definition 73. Ein **Zerfällungskörper eines Polynoms** $f \in K[T]$ über einem Körper K ist eine endliche Erweiterung L/K,

(i) in der f vollständig in Linearfaktoren zerfällt, und
(ii) $L = K(\alpha_1, \ldots, \alpha_n)$ für die Nullstellen α_i von f in L.

Satz 74. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(a) Für jede Körpererweiterung Ω/L, die entsprechend als K-Erweiterung aufgefaßt wird, gilt

$$\mathrm{Hom}_K(L, L) = \mathrm{Hom}_K(L, \Omega),$$

d.h. jede K-Einbettung von L in Ω hat Bild schon in L.

(b) Jedes irreduzible Polynom $f \in K[T]$, das in L eine Nullstelle hat, zerfällt in $L[T]$ vollständig in Linearfaktoren.

(c) L ist der Zerfällungskörper eines Polynoms aus $K[T]$.

Beweis. (a) $\Longrightarrow$ (b): Sei $f \in K[T]$ irreduzibel mit einer Nullstelle $\alpha \in L$. Sei g ein irreduzibler Faktor von f in $L[T]$. Wir müssen zeigen, daß $\deg(g) = 1$. Sei $L(\beta)$ eine Erweiterung von L, die durch Adjunktion von einer Nullstelle β von g entsteht. Da $f(\beta) = 0$ definiert $\alpha \mapsto \beta$ eine K-Einbettung

$$\sigma_0 : K(\alpha) \to L(\beta).$$

Nach Satz 62 gibt es $L(\beta) \subseteq \Omega$ und eine Fortsetzung von σ_0

$$\sigma : L \to \Omega.$$

Aus (a) folgt, daß $\sigma(L) \subseteq L$ ist. Also gilt erst recht

$$\beta = \sigma_0(\alpha) = \sigma(\alpha) \in L.$$

Daher ist $L(\beta) = L$ und

$$\deg(g) = [L(\beta) : L] = 1.$$

(b) $\Longrightarrow$ (c): Da L/K endlich ist, gibt es $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$. Sei f das Produkt der Minimalpolynome $P_{x_i/K}$ für $i = 1, \ldots, n$. Dann zerfällt f in L wegen (b) angewandt auf die irreduziblen Faktoren $P_{x_i/K}$ in Linearfaktoren und die Nullstellen von f in L erzeugen L über K. Also ist L Zerfällungskörper von f über K.

(c) $\Longrightarrow$ (a): Sei L der Zerfällungskörper von $f \in K[T]$, und sei Ω/L eine Erweiterung. Jede Nullstelle von f in Ω entspricht einem Linearfaktor von f. Da f bereits in $L[T]$ vollständig in Linearfaktoren zerfällt, befinden sich alle Nullstellen von f in L.

Jetzt folgt (a) sofort aus Proposition 60: Jedes K-lineare $\sigma : L \to \Omega$ wird die Nullstellen von f in L auf Nullstellen von $f \in \Omega$ abbilden. Diese liegen alle in L. Da L von den Nullstellen von f über K erzeugt wird, gilt demnach $\sigma(L) \subseteq L$. □

Definition 75. Eine **(endliche) normale** Körpererweiterung ist eine endliche Körpererweiterung L/K, welche die äquivalenten Bedingungen aus Satz 74 erfüllt.

Satz 76. *Sei L/K eine normale Körpererweiterung und M eine Zwischenerweiterung. Dann ist die Restriktion auf M eine surjektive Abbildung*

$$\mathrm{Hom}_K(L, L) \to \mathrm{Hom}_K(M, L).$$

Mit andern Worten ist jede K-Einbettung $M \to L$ zu einer K-Einbettung $L \to L$ fortsetzbar.

Beweis. Sei $\sigma_0 : M \to L$ eine K-Einbettung. Nach Satz 62 gibt es eine Erweiterung Ω/L und eine Fortsetzung

$$\sigma : L \to \Omega.$$

Da L/K normal ist, faktorisiert σ als die gesuchte Fortsetzung $\sigma : L \to L$. □

Sei L/K eine Körpererweiterung und $G = \mathrm{Aut}_K(L)$ die Gruppe der K-linearen Automorphismen von L. Für jedes $f \in K[T]$ operiert offensichtlich G auf der Menge der Nullstellen

$$\mathrm{NS}_f(L) = \{\alpha \in L \ ; \ f(\alpha) = 0\},$$

zum Beispiel als Konsequenz von Proposition 60.

Korollar 77. *Sei L/K eine endliche normale Erweiterung. Dann operiert $\mathrm{Aut}_K(L)$ für jedes irreduzible $f \in K[T]$ transitiv auf der Menge der Nullstellen $\mathrm{NS}_f(L)$.*

Beweis. Seien $\alpha, \beta \in \mathrm{NS}_f(L)$ Nullstellen. Dann gibt es nach Satz 56 einen K-Isomorphismus

$$\sigma_0 : K(\alpha) \xrightarrow{\sim} K(\beta),$$

mit $\sigma_0(\alpha) = \beta$. Nach Satz 76 gibt es eine Fortsetzung $\sigma : L \to L$ der Komposition

$$K(\alpha) \simeq K(\beta) \subseteq L.$$

Da L/K endlich ist, und jeder nichttriviale Homomorphismus von einem Körper injektiv ist, muß σ ein K-Automorphismus von L sein. Dieser operiert von α nach β, so daß es α und β im selben Orbit liegen. Es gibt also nur einen Orbit auf $\mathrm{NS}_f(L)$. $\square$

Proposition 78. *Jede quadratische Erweiterung ist normal.*

Beweis. Eine quadratische Erweiterung L/K wird von einem $\alpha \in L \setminus K$ mit quadratischem

$$P_{\alpha/K} = T^2 - a_1 T + a_0$$

erzeugt. Die andere Nullstelle von $P_{\alpha/K}$ ist $a_1 - \alpha$ und damit auch in L. Dies zeigt, daß L der Zerfällungskörper von $P_{\alpha/K}$ ist. $\square$

Proposition 79. *Sei L/K eine normale Körpererweiterung und M ein Zwischenkörper. Dann ist auch L/M normal.*

Beweis. Sei Ω/L eine Erweiterung. Dann ist jede M-Einbettung $L \to \Omega$ auch eine K-Einbettung, und hat, weil L/K normal ist, sein Bild in L. $\square$

Beispiel 80. In einem Körperturm L/M und M/K gilt im Allgemeinen **nicht**:

(i) L/K normal $\Longrightarrow M/K$ normal.

(ii) L/M normal und M/K normal $\Longrightarrow L/K$ normal.

Explizite Beispiele erhält man wie folgt.

(i) Sei $K = \mathbb{Q}$ und mit $\zeta_3 = e^{2\pi/3}$ sei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Dann ist $L/\mathbb{Q}$ der Zerfällungskörper von

$$T^3 - 2,$$

denn die Nullstellen $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$ liegen in L und erzeugen L. Damit ist $L/\mathbb{Q}$ normal. Wir betrachten nun den reellen Zwischenkörper $M = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Die Erweiterung $M/\mathbb{Q}$ ist nicht normal, denn das irreduzible Polynom $T^3 - 2$ hat nicht-reelle Nullstellen, die damit auch nicht in M liegen können.

Variante: es gibt den Homomorphismus $\sigma : M \to L$ mit $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$. Damit gilt $\sigma(M) \not\subseteq M$ und M/K kann nicht normal sein.

(ii) Sei $\alpha \in \mathbb{R}$ mit $\alpha^4 = 5$. Dann ist $L = \mathbb{Q}(\alpha)$ eine höchstens quadratische Erweiterung von $M = \mathbb{Q}(\alpha^2)$, was selbst wegen $(\alpha^2)^2 = 5$ eine höchstens quadratische Erweiterung von $K = \mathbb{Q}$ ist. Nach Proposition 78 sind L/M und M/K normal. Man kann nun zeigen, daß $T^4 - 5$ in $\mathbb{Q}[T]$ irreduzibel ist. Insbesondere gilt $[L; \mathbb{Q}] = 4$ und nach dem Gradsatz in Verbindung mit den Abschätzungen $[L : M] = [M : K] = 2$.

In $\mathbb{C}$ hat $T^4 - 5$ die Nullstellen

$$\alpha, i\alpha, -\alpha, -i\alpha.$$

Davon sind einige nicht reell, also nicht in $L \subseteq \mathbb{R}$ enthalten. Damit kann $L/\mathbb{Q}$ nicht normal sein.

Wir kennen nun viele gute Eigenschaften von normalen Körpererweiterungen und wollen nun sicherstellen, daß es solche Erweiterungen zu genüge gibt.

Satz 81 (Existenz und Eindeutigkeit des Zerfällungskörpers)**.** *Jedes Polynom $f \in K[T]$ hat einen endlichen Zerfällungskörper. Je zwei Zerfällungskörper sind (nicht-kanonisch) isomorph.*

Beweis. Wir zeigen per Induktion nach dem Grad von f, daß es eine Erweiterung L/K gibt, so daß in $L[T]$ das Polynom f vollständig in Linearfaktoren zerfällt. Genauer ist die zu induzierende Aussage:

(Z_d) Für jeden Körper K und jedes Polynom $f \in K[T]$ vom Grad $\deg(f) \leq d$ gibt es eine Körpererweiterung L/K, so daß in $L[T]$ das Polynom f vollständig in Linearfaktoren zerfällt.

Daß wir nur den Grad aber nicht den Körper K fixieren, erlaubt die nötige Freiheit für den Induktionsschluß.

Wenn f konstant ist, dann ist $L = K$. Sei die Behauptung (Z_{d-1}) bereits bewiesen und sei $f \in K[T]$ ein Polynom vom Grad $\deg(f) = d$. Dann gibt es nach Satz 56 eine Erweiterung $L_1 = K(\alpha_1)/K$, die durch Adjunktion einer Nullstelle eines irreduziblen Faktors von f entsteht. In $L_1[T]$ spaltet der Linearfaktor $(T - \alpha_1)$ ab: es gibt $f_1 \in L_1[T]$ mit

$$f = (T - \alpha)f_1.$$

Da $\deg(f_1) = \deg(f) - 1 = d - 1 < d$, gibt es per Induktionsannahme eine Körpererweiterung L/L_1, so daß in $L[T]$ das Polynom f_1 vollständig in Linearfaktoren zerfällt. Dasselbe tut dann auch f.

Sei nun ohne Einschränkung f normiert und seien $\alpha_1, \ldots, \alpha_d \in L$ die Nullstellen von f mit Multiplizität, also

$$f = \prod_{i=1}^{d}(T - \alpha_i).$$

Dann ist der Zwischenkörper $K(\alpha_1, \ldots, \alpha_d) \subseteq L$ ein Erweiterung von K, die ein Zerfällungskörper von f ist: die Zerlegung in Linearfaktoren von f existiert bereits mit Koeffizienten aus $K(\alpha_1, \ldots, \alpha_d)$.

Nun beweisen wir die Eindeutigkeit. Seien L und L' zwei Zerfällungskörper von $f \in K[T]$. Nach dem Fortsetzungssatz gibt es eine endliche Erweiterung M'/L', so daß sich die Einbettung $K \to L'$ sich zu einer Einbettung $\sigma : L \to M'$ fortsetzt. Da f Koeffizienten aus K hat und $\sigma|_K = \mathrm{id}_K$, muß σ Nullstellen von f in L auf Nullstellen von f in M' abbilden:

$$\sigma(\mathrm{NS}_f(L)) \subseteq \mathrm{NS}_f(M').$$

Diese Nullstellen liegen alle in L'. Weil $\mathrm{NS}_f(L)$ den Körper L als Erweiterung von K erzeugt, schließen wir, daß

$$\sigma(L) \subseteq L'.$$

Analog schließen wir auf eine K-Einbettung $\tau : L' \to L$. Da K-Einbettungen injektive lineare Abbildungen von K-Vektorräumen sind, folgt

$$[L : K] \leq [L' : K] \leq [L : K]$$

und σ und τ sind Isomorphismen. (Aber nicht notwendigerweise zueinander Invers!). □

Korollar 82. *Ein Polynom vom Grad d hat einen Zerfällungskörper, dessen Grad $\leq d!$ ist.*

Beweis. Das folgt aus dem Beweis von Satz 81. Man muß nur in der Induktion zur Existenz die Behauptung über den Grad des Zerfällungskörpers mitbehaupten und beweisen. Für den Induktionsschritt benutzt man Bemerkung 54. In der Notation des obigen Beweises ist $[L_1 : K] \leq d$ und per Induktion $[L : L_1] \leq (d-1)!$, weshalb

$$[K(\alpha_1, \ldots, \alpha_d) : K] \leq [L : K] = [L : L_1] \cdot [L_1 : K] \leq (d-1)! \cdot d = d!$$

nach dem Gradsatz. □

Satz 83. *Für jede endliche Körpererweiterung L/K gibt es einen Oberkörper $\tilde{L}/K$ der endlich und normal über K ist.*

Beweis. Sei $L = K(\alpha_1, \ldots, \alpha_r)$ und sei $f \in K[T]$ das Produkt der Minimalpolynome der α_i über K. Nach Satz 81 gibt es einen Zerfällungskörper $\tilde{L}/L$ von f als Polynom in $L[T]$. Da f schon Koeffizienten aus K hat und ein Teil der Nullstellen die Erweiterung L/K erzeugt, ist aber $\tilde{L}/K$ auch ein Zerfällungskörper von $f \in K[T]$. Als Zerfällungskörper ist $\tilde{L}/K$ nach Satz 74 normal. $\square$

4.7. **Das Kompositum.** Sei L/K eine Körpererweiterung und M_1, M_2 seien Zwischenkörper. Dann ist $M_1 \cap M_2$ auch ein Zwischenkörper. Anders sieht es mit der Vereinigung aus: $M_1 \cup M_2$ ist nur dann ein Zwischenkörper, wenn einer der beiden den anderen enthält. Selbst wenn man die K-Vektorraumsumme nimmt, bekommt man keinen Teilkörper.

Beispiel 84. In $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ nehmen wir $M_1 = \mathbb{Q}(\sqrt{2})$ und $M_2 = \mathbb{Q}(\sqrt{3})$. Das Element $\sqrt{2} + \sqrt{3}$ ist nicht in $M_1 \cup M_2$ enthalten. Die Vereinigung als Mengen ist auch nicht einmal ein $\mathbb{Q}$-Vektorraum.

Die Vektorraumsumme $M = M_1 + M_2$ hat $(1, \sqrt{2}, \sqrt{3})$ als Basis. Wäre M ein Körper, so von Grad 3 über $\mathbb{Q}$ im Widerspruch zum Gradsatz $3 = [M : \mathbb{Q}] \mid [L : \mathbb{Q}] = 4$.

Definition 85. Das **Kompositum** zweier Zwischenkörper M_1, M_2 einer Körpererweiterung L/K ist der Zwischenkörper

$$M_1 M_2 = K(M_1 \cup M_2),$$

der kleinste Zwischenkörper, der beide enthält.

Wir erhalten das Körperturmdiagramm

$$\begin{tikzcd}[arrows=-]
 & L \arrow[d] & \\
 & M_1 M_2 \arrow[dl] \arrow[dr] & \\
M_1 \arrow[dr] & & M_2 \arrow[dl] \\
 & M_1 \cap M_2 \arrow[d] & \\
 & K &
\end{tikzcd}$$

Bemerkung 86. Ohne den gemeinsamen Oberkörper L kann man das Kompositum nicht wohldefinieren. So sind $M_1 = \mathbb{Q}(\sqrt[3]{2})$ und $M_2 = \mathbb{Q}(\zeta_3 \cdot \sqrt[3]{2})$ Unterkörper von $\mathbb{C}$, die als solche zum Kompositum

$$M_1 M_2 = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$$

führen. Andererseits sind $M_1 \simeq M_2$ als Erweiterungen von $\mathbb{Q}$. Wenn man M_2 mittels dieses Isomorphismus als Unterkörper von M_1 ansieht, wird das Kompositum plötzlich nur noch M_1.

Proposition 87. *Sei L/K eine Erweiterung und seien M_1/K und M_2/K normale Zwischenerweiterungen. Dann sind $M_1 M_2$ und $M_1 \cap M_2$ normale Erweiterungen von K.*

Beweis. Als normale Erweiterungen von K sind die M_i/K Zerfällungskörper von Polynomen $f_i \in K[T]$ für $i = 1, 2$. Dann ist $M = M_1 M_2$ der Zerfällungskörper von $f = f_1 f_2$. Damit ist M/K normal.

Sei $f \in K[T]$ ein irreduzibles Polynom, das in $M_1 \cap M_2$ eine Nullstelle hat. Dann zerfällt f in $M_i[T]$ für beide $i = 1, 2$ vollständig in Linearfaktoren. Da die Faktorisierung eindeutig ist, haben die normierten Linearfaktoren Koeffizienten in $M_1 \cap M_2$. Somit zerfällt f schon in $(M_1 \cap M_2)[T]$ vollständig in Linearfaktoren und $M_1 \cap M_2$ ist normal über K. □

Übungsaufgaben zu §4

Übungsaufgabe 4.1. Es seien L_1/K und L_2/K zwei Körpererweiterungen. Zeigen Sie, daß ein Körperhomomorphismus $f : K_1 \to K_2$ genau dann K-linear ist (also eine lineare Abbildung der zugrundeliegenden K-Vektorräume), wenn $f(a) = a$ für alle $a \in K$ gilt. Dabei idenitifizieren wir K sowohl mit seinem Bild in L_1 als auch mit seinem Bild in L_2.

Übungsaufgabe 4.2. Sei K ein Körper und $G \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Zeigen Sie, daß G eine zyklische Gruppe ist.

Anleitung: Beweis durch Widerspruch. Sei G ein kleinstes Gegenbeispiel. Dann ist G von zwei Elementen erzeugt, etwa $x, y \in G$. Sei N (bzw. M) die Ordnung von x (bzw. y). Mit Hilfe des chinesischen Restsatz kann man auf die Situation reduzieren, in der N und M Potenzen einer Primzahl p sind. Sei dann $M \mid N$. Dann ist y eine Lösung der Gleichung

$$T^N = 1$$

welche schon die N Lösungen $1, x, \ldots, x^{N-1}$ hat. Da K ein Körper ist, muß y in dieser Liste enthalten sein.

Man begründe die einzelnen Schritte.

Übungsaufgabe 4.3. Zwei quadratische Erweiterungen $K(\sqrt{a}) \simeq K(\sqrt{b})$ sind isomorph als Erweiterungen von K, genau dann wenn $a/b \in K^2$ ein Quadrat in K ist.

Übungsaufgabe 4.4. Zeigen Sie, daß jeder Ring auf eindeutige Weise eine $\mathbb{Z}$-Algebra ist.

Übungsaufgabe 4.5. Man zeige, daß $T^4 - 5$ irreduzibel in $\mathbb{Q}[T]$ ist.

Übungsaufgabe 4.6. Sei $M = M_1M_2$ das Kompositum der Zwischenkörper M_1, M_2 in einer Erweiterung L/K. Zeigen Sie:

(1) M/K ist endlich genau dann wenn M_1/K und M_2/K endlich sind.
(2) Wenn M/K endlich ist, dann gilt

$$[M : K] \leq [M_1K] \cdot [M_2 : K]$$

Geben Sie ein Beispiel an, wo $[M : K]$ kein Teiler von $[M_1 : K] \cdot [M_2 : K]$ ist.

Übungsaufgabe 4.7. Sei L/K eine Körpererweiterung und seien E, F Zwischenkörper, die endlich über K sind. Zeigen Sie die folgende Beschreibung des Kompositums EF

$$EF = \left\{ \sum_{i=1}^{n} a_i x_i \ ; \ n \in \mathbb{N}, a_i \in E, x_i \in F, i = 1, \ldots, n \right\}.$$

5. Algebraisch abgeschlossene Körper

Definition 88. Ein **algebraisch abgeschlossener Körper** ist ein Körper, der keine algebraischen Erweiterungen vom Grad $\neq 1$ hat.

Proposition 89. *Sei K ein Körper. Dann sind äquivalent.*

(a) *K ist algebraisch abgeschlossen.*
(b) *Jedes irreduzible Polynom von $K[T]$ hat Grad 1.*
(c) *Jedes Polynom in $K[T]$ zerfällt in $K[T]$ in ein Produkt aus Linearfaktoren (und eine Einheit).*
(d) *Jedes Polynom positiven Grades in $K[T]$ hat in K eine Nullstelle.*
(e) *Jedes irreduzible Polynom in $K[T]$ hat in K eine Nullstelle.*

Beweis. (a) $\Longrightarrow$ (b): Sei $f \in K[T]$ irreduzibel. Dann gibt es eine Körpererweiterung L/K vom Grad $\deg(f)$. Da K algebraisch abgeschlossen ist, gilt $\deg(f) = [L : K] = 1$.

(b) $\Longrightarrow$ (c): Jedes Polynom zerfällt in ein Produkt irreduzibler Faktoren.

(c) $\Longrightarrow$ (d): Die Nullstellen von f sind die Nullstellen seiner Linearfaktoren.

(d) $\Longrightarrow$ (e): Das ist trivial.

(e) $\Longrightarrow$ (a): Wenn es eine nichttriviale algebraische Erweiterung L/K gibt, dann ist das Minimalpolynom $P_{\alpha/K}$ eines $\alpha \in L \setminus K$ ein irreduzibles Polynom in $K[T]$. Nach Voraussetzung (e) gibt es eine Nullstelle $\beta \in K$ von $P_{\alpha/K}$, und damit in $K[T]$ den Linearfaktor $(T - \beta)$. Damit kann $P_{\alpha/K}$ nur irreduzibel sein, wenn $P_{\alpha/K} = T - \beta$ gilt. Daraus folgt $\alpha = \beta \in K$, ein Widerspruch zur Wahl von α. □

Proposition 90. *Sei Ω/K eine Körpererweiterung und Ω ein algebraisch abgeschlossener Körper. Dann ist der relative algebraische Abschluß Ω_a von K in Ω ein algebraisch abgeschlossener Körper, der algebraisch über K ist.*

Beweis. Nach Konstruktion ist Ω_a/K algebraisch. Es ist also nur zu zeigen, daß Ω_a algebraisch abgeschlossen ist. Dies zeigen wir durch Wiederspruch.

Wenn Ω_a nicht algebraisch abgeschlossen ist, dann gibt es nach Proposition 89 ein irreduzibles Polynom $f \in \Omega_a[T]$ vom Grad > 1. Da Ω algebraisch abgeschlossen ist, hat f in Ω eine Nullstelle, sagen wir $\alpha \in \Omega$. Dann ist

$$\Omega_a(\alpha) \subseteq \Omega$$

eine algebraische Erweiterung von Ω_a vom Grad $\deg(f) > 1$, also nichttrivial. Aber α bzw. $\Omega_a(\alpha)$ ist algebraisch über Ω_a und daher auch algebraisch über K nach Proposition 29. Nach Definition des relativen algebraischen Abschluß ist dann $\alpha \in \Omega_a$ im Widerspruch zu $\Omega_a \neq \Omega_a(\alpha)$. □

Definition 91. Ein **algebraischer Abschluß** eines Körpers K ist eine Erweiterung Ω/K, die

(i) algebraisch über K, und in der
(ii) Ω algebraisch abgeschlossen ist.

Beispiel 92. Nach dem noch zu beweisenden Fundamentalsatz der Algebra ist $\mathbb{C}$ algebraisch abgeschlossen. Der relative algebraische Abschluß

$$\overline{\mathbb{Q}}$$

von $\mathbb{Q}$ in $\mathbb{C}$ ist demnach ein algebraischer Abschluß von $\mathbb{Q}$.

5.1. **Maximale Ideale.** Als Anwendung des Lemma von Zorn beweisen wir die existenz maximaler Ideale. Für die Begriffe zu Ordnungsrelationen auf Mengen verweisen wir auf Anhang A.

Definition 93. Ein **maximales Ideal** ist ein Ideal $\mathfrak{m}$ in einem Ring R, so daß $\mathfrak{m} \neq R$ und für jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ gilt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Ein maximales Ideal im Ring R ist somit ein maximales Element unter den echten Idealen ($\neq R$) bezüglich der durch die Inklusion gegebenen partiellen Ordnung.

Satz 94. *Sei R ein Ring und $\mathfrak{a}$ ein Ideal in R. Dann gibt es ein maximales Ideal $\mathfrak{m} \subseteq R$, das $\mathfrak{a}$ enthält.*

Beweis. Die Menge

$$\mathscr{M} = \{\mathfrak{b} \subseteq R \; ; \; \mathfrak{b} \text{ ist Ideal in } R, \mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{b} \neq R\}$$

ist bezüglich Inklusion induktiv geordnet. In der Tat, wenn $\mathfrak{b}_i$ mit $i \in I$ eine total geordnete Teilmenge von echten Idealen ist, dann ist

$$\mathfrak{b} = \bigcup_{i \in I} \mathfrak{b}_i$$

eine obere Schranke wie wir nun beweisen. Es ist $\mathfrak{b}$ ein Ideal, denn für $x, y \in \mathfrak{b}$ gibt es i, j mit $x \in \mathfrak{b}_i$ und $y \in \mathfrak{b}_j$. Weil die Ideale $(\mathfrak{b}_i)_{i \in I}$ total geordnet sind, gilt oBdA $\mathfrak{b}_i \subseteq \mathfrak{b}_j$ und damit

$x + y \in \mathfrak{b}_j \subseteq \mathfrak{b}$. Die Abgeschlossenheit unter Multiplikation mit Elementen von R ist trivial, ebenso $\mathfrak{a} \subseteq \mathfrak{b}$ und $\mathfrak{b}_i \subseteq \mathfrak{b}$ für alle $i \in I$. Um obere Schranke zu sein, muß $\mathfrak{b} \in \mathscr{M}$ sein. Dazu fehlt noch, daß $\mathfrak{b}$ von R verschieden ist. Das gilt, weil ansonsten $1 \in \mathfrak{b}$, also $1 \in \mathfrak{b}_i$ für i groß genug, und dann $\mathfrak{b}_i = R$ nicht echt für solche i.

Wegen $\mathfrak{a} \in \mathscr{M}$ ist $\mathscr{M}$ nicht leer. Nach dem Lemma von Zorn, siehe Anhang A.3, hat $\mathscr{M}$ ein maximales Element, und das ist genau das gesuchte maximale Ideal. □

Lemma 95. *Ein Ideal $\mathfrak{a} \subseteq R$ in einem Ring R ist maximal genau dann, wenn $R/\mathfrak{a}$ ein Körper ist.*

Beweis. Der Quotient $k = R/\mathfrak{a}$ ist ein Körper, wenn k nur die Ideale (0) und $(1) = k$ hat. Es bezeichne

$$\pi : R \to k = R/\mathfrak{a}$$

die Quotientenabbildung. Die Abbildung

$$\pi^{-1} : \{\bar{\mathfrak{b}} \lhd R/\mathfrak{a}\ ;\ \text{Ideal}\} \to \{\mathfrak{b} \lhd R\ ;\ \text{Ideal mit } \mathfrak{a} \subseteq \mathfrak{b}\}$$
$$\bar{\mathfrak{b}} \mapsto \pi^{-1}(\bar{\mathfrak{b}})$$

ist bijektiv und erhält die Inklusionsrelation. Daher ist k ein Körper, wenn es zwischen $\mathfrak{a}$ und R keine echten dazwischenliegenden Ideale mehr gibt, also genau dann, wenn $\mathfrak{a}$ maximales Ideal von R ist. □

5.2. Der algebraische Abschluß.

Theorem 96 (Steinitz 1910)**.** *Jeder Körper besitzt einen algebraischen Abschluß.*

Beweis. Wir folgen Emil Artin in der Konstruktion eines algebraischen Abschlusses von K. Sei dazu X_f eine formale Variable für jedes irreduzible normierte Polynom in $K[T]$. Wir setzen

$$R = K[X_f\ ;\ \text{irreduzible normierte } f \in K[T]].$$

und betrachten das Ideal von R

$$\mathfrak{a} = (f(X_f);\ \text{alle normierten irreduziblen } f \in K[T]).$$

Wir zeigen durch Widerspruch, daß $\mathfrak{a} \neq R$, also $\mathfrak{a}$ ein echtes Ideal ist. Im Fall $\mathfrak{a} = R$ gilt nämlich $1 \in \mathfrak{a}$ und es gibt eine endliche Relation

$$1 = \sum_{i=1}^{r} g_i f_i(X_{f_i})$$

mit $g_i \in R$ und $f_i \in K[T]$ irreduzibel und normiert. Wir betrachten nun einen Zerfällungskörper L/K von

$$f = \prod_{i=1}^{r} f_i.$$

In L gibt es eine Wurzel α_i für jedes f_i, also $f_i(\alpha_i) = 0$. Wir werten in L aus mit $X_{f_i} \mapsto \alpha_i$ und alle anderen $X_h \mapsto 0$ (spielt keine Rolle). Damit ist dann

$$1 = \sum_{i=1}^{r} (g_i f_i(X_f))(\alpha_1, \ldots, \alpha_r, 0 \ldots) = 0,$$

ein Widerspruch. Sei $\mathfrak{m} \subseteq R$ ein maximales Ideal, das $\mathfrak{a}$ enthält.

Die Einbettung der Elemente von K als konstanten Polynome in R induziert eine Körpererweiterung

$$K \to E_1 := R/\mathfrak{m}.$$

Dabei ist E_1 als Erweiterung von K durch die Bilder α_f der X_f erzeugt. Da per Konstruktion

$$f(\alpha_f) = 0$$

ist E_1/K algebraisch und jedes normierte irreduzible Polynom aus $K[T]$ hat in E_1 eine Nullstelle.

Wir iterieren nun die Konstruktion. So erhalten wir einen Körperturm

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_i \subseteq \ldots$$

so daß für alle i in E_{i+1} alle irreduziblen Polynome aus $E_i[T]$ eine Nullstelle haben. Wir setzen

$$\Omega = \bigcup_i E_i.$$

Dann ist Ω ein Körper, Ω/K ist algebraisch und auch algebraisch abgeschlossen. Sei nämlich $f \in \Omega[T]$ ein irreduzibles Polynom. Dann gibt es ein i, so daß die endlich vielen Koeffizienten von f schon in E_i liegen. Damit hat f in $E_{i+1} \subseteq \Omega$ bereits eine Nullstelle. Damit ist Ω algebraisch abgeschlossen nach Proposition 89(e). □

Satz 97 (Steinitz)**.**

(1) *Sei Ω/K eine Erweiterung mit einem algebraisch abgeschlossener Körper Ω. Dann läßt sich jede algebraische Erweiterung L/K über K in Ω einbetten.*

(2) *Sind Ω_1 und Ω_2 algebraische Abschlüsse von K, dann gibt es einen K-Isomorphismus $\Omega_1 \simeq \Omega_2$.*

Beweis. (1) Sei L/K algebraisch und Ω/K eine Erweiterung mit Ω algebraisch abgeschlossen. Wir betrachten die Menge

$$\mathscr{M} = \{(M, \sigma)\ ;\ K \subseteq M \subseteq L \text{ Zwischenkörper}, \sigma : M \to \Omega\ K\text{-linear}\}$$

mit der partiellen Ordnung gegeben durch *Fortsetzung*:

$$(M, \sigma) \preceq (M', \sigma') :\iff M \subseteq M' \text{ und } \sigma'|_M = \sigma.$$

Die Menge $\mathscr{M}$ ist nicht leer, denn es gibt

$$(K, K \hookrightarrow \Omega) \in \mathscr{M}.$$

Und $\mathscr{M}$ ist induktiv geordnet, denn für eine Totalgeordnete Teilmenge $(M_i, \sigma_i)_{i\in I}$ wird auf dem Zwischenkörper

$$M = \bigcup_{i\in I} M_i \subseteq L$$

durch

$$x \mapsto \sigma_i(x) \text{ für jedes } i \text{ mit } x \in M_i$$

eine K-Einbettung

$$\sigma : M \to \Omega$$

definiert. Die Abbildung σ ist wohldefiniert, weil die verschiedenen σ_i einander fortsetzen. Offensichtlich ist

$$(M, \sigma) \in \mathscr{M}$$

eine obere Schranke für $(M_i, \sigma_i)_{i\in I}$.

Nach dem Lemma von Zorn, siehe Anhang A.3, gibt es in $\mathscr{M}$ ein maximales Element

$$(L_0, \sigma_0).$$

Wir müssen zeigen, daß $L_0 = L$ ist. Andernfalls gibt es $\alpha \in L \backslash L_0$. Sei P_{α/L_0} das Minimalpolynom von α über L_0. Mittels σ_0 fassen wir P_{α/L_0} als Polynom

$$^{\sigma_0}P_{\alpha/L_0} \in \Omega[T]$$

auf. Weiter fassen wir Ω mittels $\sigma_0 : L_0 \hookrightarrow \Omega$ als Erweiterung von L_0 auf. Weil Ω algebraisch abgeschlossen ist, gibt es demnach eine L_0-Einbettung

$$\sigma : L_0(\alpha) \to \Omega,$$

da diese nach Proposition 60 den Nullstellen von ${}^{\sigma_0}P_{\alpha/L_0}$ in Ω entsprechen. Damit haben wir in $(L_0(\alpha), \sigma)$ ein Element in $\mathscr{M}$ gefunden, das größer

$$(L_0, \sigma_0) \preceq (L_0(\alpha), \sigma)$$

und wegen $\alpha \notin L_0$ sogar echt größer ist. Dies ist ein Widerspruch zur Maximalität von (L_0, σ_0). Es muß demnach bereits $L_0 = L$ sein. Damit ist die gesuchte Fortsetzung gefunden.

(2) Nach (1) gibt es eine K-Einbettung

$$\sigma : \Omega_1 \hookrightarrow \Omega_2.$$

Wir fassen damit Ω_2 als Erweiterung von Ω_1 auf. Da Ω_2/K algebraisch ist, ist auch Ω_2/Ω_1 algebraisch. Da Ω_1 algebraisch abgeschlossen ist, folgt $\Omega_2 = \Omega_1$, oder übersetzt, die K-Einbettung σ ist ein Isomorphismus. □

Bemerkung 98. (1) Der K-Isomorphismus zwischen zwei algebraischen Abschlüssen von K ist nicht eindeutig, sofern K nicht selbst algebraisch abgeschlossen ist. Daher ziemt es sich nicht von *dem* algebraischen Abschluß von K zu sprechen.

(2) Als Konsequenz von Satz 97 kann man sich beim Studium algebraischer Körpererweiterungen von K auf die Zwischenkörper einer Erweiterung Ω/K mit Ω algebraisch abgeschlossen beschränken.

Übungsaufgaben zu §5

Übungsaufgabe 5.1. Sei K ein abzählbarer Körper. Zeigen Sie, daß ein algebraischer Abschluß von K auch abzählbar ist.

Übungsaufgabe 5.2. Zeigen Sie, daß ein endlicher Körper nicht algebraisch abgeschlossen sein kann.

6. Verschiedenes zu Körpern

6.1. **Charakteristik.** Jeder Ring R erlaubt einen einzigen Ringhomomorphismus

$$\mathbb{Z} \to R,$$

denn ein solcher ist schon als Homomorphismus abelscher Gruppen durch das Bild von $1 \in \mathbb{Z}$ festgelegt. Als Ringhomomorphismus muß das Bild der 1 wieder $1 \in R$ sein. Man überlegt sich sofort, daß der so festgelegte Gruppenhomomorphismus mit der Multiplikation verträglich ist.

Definition 99. Die **Charakteristik** eines Rings R ist diejenige nichtnegative natürliche Zahl n mit

$$n\mathbb{Z} = \ker(\mathbb{Z} \to R).$$

Lemma 100. *Die Charakteristik eines Integritätsrings (etwa eines Körpers) ist eine Primzahl oder* 0.

Beweis. Angenommen die Charakteristik des Integritätsrings R wäre $n = ab$ mit $a, b \geq 2$. Dann wäre in R

$$a \cdot b = n = 0$$

und somit einer der Faktoren schon 0, sagen wir a. Dann ist $a \in \ker(\mathbb{Z} \to R) = n\mathbb{Z}$ im Widerspruch zu $0 < a < n$. □

Beispiel 101. Wir geben für jede mögliche Charakteristik Beispiele von Körpern.

(1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben Charakteristik 0.
(2) Sei p eine Primzahl. Der Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ hat Charakteristik p.
(3) Sei L/K eine Körpererweiterung. Der Homomorphismus $\mathbb{Z} \to L$ ist die Komposition von $\mathbb{Z} \to K$ gefolgt von der Einbettung $K \hookrightarrow L$. Somit haben K und L stets die gleiche Charakteristik.

6.2. **Primkörper.** Sei K ein Körper der Charakteristik $p > 0$. Dann faktorisiert

$$\mathbb{Z} \to K$$

eindeutig zu einer Einbettung

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \hookrightarrow K.$$

Jeder Unterkörper $K_0 \subseteq K$ enthält das Bild von $\mathbb{F}_p$. Dieses Bild, das wir oft mit $\mathbb{F}_p$ identifizieren, ist somit der kleinste in K enthaltene Unterkörper (der somit existiert).

Sei K ein Körper der Charakteristik 0. Dann ist $\mathbb{Z} \hookrightarrow K$ injektiv und insbesondere jedes $0 \neq n \in \mathbb{Z}$ in K eindeutig invertierbar. Der Homomorphismus $\mathbb{Z} \to K$ setzt sich damit eindeutig zu einer Körpereinbettung

$$\mathbb{Q} \hookrightarrow K$$

fort. Jeder Unterkörper $K_0 \subseteq K$ enthält das Bild von $\mathbb{Q}$, das wir oft mit $\mathbb{Q}$ identifizieren. Somit ist $\mathbb{Q}$ der kleinste in K enthaltene Unterkörper .

Definition 102. Der **Primkörper** $\mathbb{K}$ eines Körpers K ist der kleinste in K enthaltene Unterkörper. Somit

$$\mathbb{K} = \begin{cases} \mathbb{F}_p & \text{falls Charakteristik von } K = p > 0 \\ \mathbb{Q} & \text{falls Charakteristik von } K = 0. \end{cases}$$

6.3. **Frobenius.** Eine Besonderheit von Charakteristik $p > 0$ ist der Frobenius–Morphismus. Wir betrachten im Folgenden nur kommutative Ringe.

Proposition 103. *Sei p eine Primzahl und R ein Ring der Charakteristik p. Dann definiert*

$$\begin{aligned} \mathrm{Frob} : R &\to R \\ x &\mapsto x^p \end{aligned}$$

*einen Ringendomorphismus, den **Frobenius–Morphismus** oder kurz **Frobenius** von R.*

Beweis. Offensichtlich gilt $\mathrm{Frob}(1) = 1$ und für alle $x, y \in R$ auch $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$. Die Binomische Formel gilt auch in R, also haben wir

$$\mathrm{Frob}(x + y) = (x + y)^p = \sum_{n=0}^{p} \binom{p}{n} x^{p-n} y^n,$$

und wir müssen zeigen, daß dies gleich

$$\mathrm{Frob}(x) + \mathrm{Frob}(y) = x^p + y^p$$

ist. Es bleibt zu zeigen, daß für $0 < n < p$ der Binomialkoeffizient

$$\binom{p}{n} = \frac{p!}{(p-n)!n!}$$

durch p teilbar ist. Das ist aber aus der angegebenen Formel offensichtlich.

Alternativ kann man auf der Menge $\{1, \ldots, p\}$ die zyklische Gruppe der Ordnung p operieren lassen, die von einem p-Zykel erzeugt wird. Auf der Menge der n-elementigen Teilmengen

$$\mathscr{M}_n = \{A \subseteq \{1, \ldots, p\} \ ; \ \#A = n\}$$

wird eine Operation ohne Fixpunkte induziert. Alle Orbits sind dort also der Länge p. Damit hat $\mathscr{M}_n$ eine durch p teilbare Mächtigkeit, und diese ist bekanntlich $\binom{p}{n}$. $\square$

6.4. Der Fixkörper. Der Fixkörper ist eine fundamentale Konstruktion.

Proposition 104. *Sei K ein Körper und $\sigma_i : K \to K$ für $i \in I$ eine Menge von Endomorphismen. Dann ist*

$$K_0 = \{x \in K \ ; \ \sigma_i(x) = x \text{ für alle } i \in I\}$$

ein Unterkörper von K, genannt der (gemeinsame) ***Fixkörper*** *in K von σ_i, $i \in I$.*

Beweis. Es gilt offensichtlich $0, 1 \in K_0$ und zu beliebigen $x, y \in K_0$ und $i \in I$ gilt

$$\sigma_i(x - y) = \sigma_i(x) - \sigma_i(y) = x - y$$
$$\sigma_i(xy) = \sigma_i(x)\sigma_i(y) = xy$$
$$\sigma_i(1/x) = 1/\sigma_i(x) = 1/x$$

letzteres, sofern $x \neq 0$. Damit ist alles gezeigt. □

Korollar 105. *Sei K ein Körper und $G \subseteq \mathrm{Aut}(K)$ eine Untergruppe von Automorphismen. Dann ist*

$$K^G := \{x \in K \ ; \ \sigma(x) = x \text{ für alle } \sigma \in G\}$$

ein Unterkörper von K, genannt der ***Fixkörper*** *der Operation von G auf K.*

Beweis. Spezialfall von Proposition 104 mit der Menge G von Endomorphismen. □

7. Endliche Körper

7.1. Existenz und Eindeutigkeit. Sei K ein endlicher Körper. Die Abbildung $\mathbb{Z} \to K$ kann nicht injektiv sein. Demnach hat K postive Charakteristik $p > 0$ für eine Primzahl p. Des weiteren enthält K eindeutig als Primkörper den endlichen Körper $\mathbb{F}_p$ und ist als endliche Körpererweiterung von $\mathbb{F}_p$ zu betrachten.

Proposition 106. *Sei K ein endlicher Körper der Charaktersitik $p > 0$. Dann hat K genau p^r Elemente für ein $r \in \mathbb{N}$.*

Beweis. Sei $[K : \mathbb{F}_p] = r$. Dann ist K ein $\mathbb{F}_p$-Vektorraum der Dimension r und hat deshalb p^r Elemente. □

Es gibt insbesondere keinen Körper mit 6 Elementen. Wir werden nun umgekehrt zeigen, daß es zu jeder Primpotenz $q = p^r$ bis auf Isomorphie genau einen Körper mit q Elementen gibt.

Dazu fixieren wir von nun an eine Primzahl p.

Wir betonen in unserer Untersuchung der endlichen Körper die Rolle des Frobenius und beginnen daher mit dem folgenen Satz.

Satz 107. *Sei K ein Körper mit $q = p^r$ Elementen. Dann ist*

$$\mathrm{Aut}_{\mathbb{F}_p}(K) = \langle \mathrm{Frob} \rangle \simeq \mathbb{Z}/r\mathbb{Z}$$

eine zyklische Gruppe von Ordnung r erzeugt von $\mathrm{Frob} : K \to K$.

Beweis. Der Frobenius von K ist als Körperendomoprhimus injektiv und damit als Endomorphismus einer endlichen Struktur auch bijektiv. Somit gilt $\mathrm{Frob} \in \mathrm{Aut}_{\mathbb{F}_p}(K)$.

Nach Korollar 72 gilt

$$\# \mathrm{Aut}_{\mathbb{F}_p}(K) \leq \# \mathrm{Hom}_{\mathbb{F}_p}(K, K) \leq [K : \mathbb{F}_p] = r$$

also hat Frob höchstens die Ordnung r. Wir sind fertig, wenn wir zeigen können, daß Frob genau die Ordnung r hat.

Angenomen Frob habe die Ordnung $s < r$. Dann gilt für alle $x \in K$

$$x^{p^s} = x$$

und damit hat

$$K = \mathrm{NS}_{T^{p^s} - T}(K)$$

höchstens p^s Elemente, ein Widerspruch. $\square$

Korollar 108. *Es gilt* $\mathrm{Aut}(\mathbb{F}_p) = 1$.

Beweis. Das ist der Fall $r = 1$ oder aber auch direkt klar, denn 1 erzeugt $\mathbb{F}_p$ additiv. $\square$

Definition 109. Sei $q = p^r$ eine Potenz von p. Wir definieren den **q-Frobenius** als

$$\mathrm{Frob}_q = \mathrm{Frob}^r : x \mapsto x^q$$

die r-te Potenz des Frobenius (definiert für jeden Ring der Charakteristik p).

Notation 110. Wir wählen nun einen algebraischen Abschluß $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Der Körper

$$\mathbb{F}_q$$

für $q = p^r$ ist definiert als der Fixkörper von Frob_q als Endomorphismus von $\overline{\mathbb{F}}_p$.

Satz 111 (Galois, Existenz endlicher Körper)**.** *Sei $q = p^r$ eine Potenz von p. Der Körper $\mathbb{F}_q$ hat q Elemente und ist ein Zerfällungskörper von $T^q - T$ in $\overline{\mathbb{F}}_p$.*

Beweis. Per Definition gilt

$$\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p \ ; \ x^q = x\} = \mathrm{NS}_{\overline{\mathbb{F}}_p}(T^q - T),$$

demnach hat $\mathbb{F}_q$ höchstens q Elemente und ist ein Zerfällungskörper von $T^q - T$.

Angenommen, $\mathbb{F}_q$ habe weniger als q Elemente, sagen wir p^s mit $s < r$. Dann ist nach Satz 107

$$\mathrm{id} = \mathrm{Frob}_q = (\mathrm{Frob})^r \in \mathrm{Aut}(\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) \simeq \mathbb{Z}/s\mathbb{Z}$$

und damit $s \mid r$. Dann ist $m = (p^r - 1)/(p^s - 1) \in \mathbb{N}$ wegen

$$p^r - 1 = ((p^s - 1) + 1)^{r/s} - 1 \equiv 0 \mod (p^s - 1).$$

Nun hat $T^q - T$ wegen

$$\frac{T^q - T}{T^{p^s} - T} = \frac{T^{m(p^s-1)} - 1}{T^{p^s-1} - 1} = T^{(m-1)(p^s-1)} + \ldots + T^{p^s-1} + 1 = f \in \mathbb{F}_p[T]$$

den nichttrivialen Faktor f. Per Definition hat f alle seine Nullstellen in $\mathbb{F}_q$. Diese sind verschieden von 0. Außerdem gilt wegen $\mathrm{Frob}^s = \mathrm{id}$ auch $x^{p^s} = x$ für alle $x \in \mathbb{F}_q$, oder eben $x^{p^s-1} = 1$ falls $x \neq 0$. Somit gilt für alle $x \in \mathbb{F}_q^\times$

$$f(x) = (x^{p^s-1})^{m-1} + \ldots (x^{p^s-1}) + 1 = m.$$

Aber $p \nmid m$ so daß f keine Nullstelle in $\mathbb{F}_q$ hat, ein Widerspruch. $\square$

Bemerkung 112. Daß $T^q - T$ in paarweise verschiedene Linearfaktoren zerfällt, folgt später viel einfacher aus der Theorie separabler Polynome und der algebraischen Differentiation, siehe Beispiel 143.

Satz 113 (Eindeutigkeit endlicher Körper)**.** *Sei $q = p^r$.*

(1) $\overline{\mathbb{F}}_p$ *hat genau einen Unterkörper mit q Elementen, den Zerfällungskörper $\mathbb{F}_q$ des Polynoms $T^q - T \in \mathbb{F}_p[T]$.*

(2) *Je zwei Körper mit q Elementen sind isomorph.*

Beweis. (1) Sei $K \subseteq \overline{\mathbb{F}}_p$ ein Unterkörper mit q Elementen. Nach Satz 107 gilt $\mathrm{Frob}_q|_K = \mathrm{id}_K$. Damit ist

$$K \subseteq \mathrm{NS}_{T^q - T}(\overline{\mathbb{F}}_p) = \mathbb{F}_q$$

und wegen der gleichen endlichen Mächtigkeit sogar $K = \mathbb{F}_q$.

(2) Sei K ein Körper mit q Elementen. Dann ist K eine algebraische Erweiterung von $\mathbb{F}_p$ und hat daher nach dem Steinitzschen Fortsetzungssatz, Satz 97, eine Einbettung $\sigma : K \hookrightarrow \overline{\mathbb{F}}_p$. Das Bild $\sigma(K)$ ist als Unterkörper mit q Elementen nach (1) gleich $\mathbb{F}_q$. Daher ist σ ein Isomorphismus $K \simeq \mathbb{F}_q$. Damit sind auch je zwei Körper mit q Elementen isomorph. $\square$

Korollar 114. *Jeder endliche Körper hat für jedes $m \geq 1$ bis auf Isomorphie genau eine Erweiterung vom Grad m.*

Beweis. Die Existenz folgt aus Satz 113. Als endlichen Körper darf man $\mathbb{F}_q$ nehmen und als Erweiterung

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^m}.$$

Jede andere endliche Erweiterung von $\mathbb{F}_q$ läßt sich nach Satz 97 $\mathbb{F}_q$-linear in $\overline{\mathbb{F}}_p$ einbetten. Dann muß es aber wieder wegen Satz 113 schon die angegebene sein. □

7.2. **Galoistheorie für endliche Körper.** Der explizite und durch eine algebraische Formel gegebene Frobeniusautomorphismus macht Galoistheorie endlicher Körper explizit und direkt beweisbar.

Bemerkung 115. Eine kurze exakte Sequenz von Gruppen (oder Objekten mit einem Begriff von Kern und Bild) ist ein Diagramm

$$1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1$$

von Gruppen, so daß an jeder Stelle Kern und Bild der beiden dort beginnenden bzw. dort endenden Homomorphismus übereinstimmen, also

(i) ι injektiv,
(ii) $\mathrm{im}(\iota) = \ker(\pi)$ und
(iii) π surjektiv ist.

Theorem 116 (Galoistheorie für endliche Körper)**.** *Sei L/K eine Erweiterung endlicher Körper mit $q = \#K = p^r$ und $\#L = q^m$ Elementen.*

(1) *Die K-Automorphismengruppe von L*

$$\mathrm{Aut}_K(L) = \langle \mathrm{Frob}_q \rangle \simeq \mathbb{Z}/m\mathbb{Z}$$

ist zyklisch von Ordnung $m = [L : K]$, erzeugt vom q-Frobenius.

(2) *Es gibt für jeden Teiler $d \mid [L : K]$ genau einen Zwischenkörper M_d mit $[M : K] = d$.*

(3) *Die Zuordnung*

$$\{\textit{Zwischenkörper von } L/K\} \to \{\textit{Untergruppen von } \mathrm{Aut}_K(L)\}$$
$$M \mapsto \mathrm{Aut}_M(L)$$

ist eine Bijektion. Die Umkehrabbildung wird gegeben durch

$$U \mapsto L^U$$

für eine Untergruppe $U \subseteq \mathrm{Aut}_K(L)$. Dabei gilt für Zwischenkörper M, M_0, M_1:

(a) *Die Bijektion ist inklusionsumkehrend: aus $M_0 \subseteq M_1$ folgt*

$$\mathrm{Aut}_{M_1}(L) \subseteq \mathrm{Aut}_{M_0}(L),$$

und für Untergruppen $U_0 \subseteq U_1 \subseteq \mathrm{Aut}_K(L)$ gilt

$$L^{U_1} \subseteq L^{U_0}.$$

(b) $[M : K] = (\mathrm{Aut}_K(L) : \mathrm{Aut}_M(L))$

(c) *Die Sequenz*

$$1 \to \mathrm{Aut}_M(L) \xrightarrow{\iota} \mathrm{Aut}_K(L) \xrightarrow{\mathrm{res}_M} \mathrm{Aut}_K(M) \to 1$$

ist exakt, wobei ι die Inklusion und res_M die Restriktion $\mathrm{res}_M(\sigma) = \sigma|_M$ ist.

(4) *Ein Zwischenkörper M von L/K ist normal genau dann, wenn $\mathrm{Aut}_M(L)$ ein Normalteiler in $\mathrm{Aut}_K(L)$ ist, wegen abelschen Gruppen also immer.*

Beweis. Nach Korollar 114 dürfen wir $K = \mathbb{F}_q$ und $L = \mathbb{F}_{q^m}$ in $\overline{\mathbb{F}}_p$ annehmen.

(1) Wir kennen $\mathrm{Aut}_{\mathbb{F}_p}(L) = \langle \mathrm{Frob} \rangle \simeq \mathbb{Z}/rm\mathbb{Z}$ nach Satz 107. Davon ist $\mathrm{Aut}_K(L)$ diejenige Untergruppe, welche die Idenitität auf K induziert. Der Frobenius auf K hat Ordnung r, also tun dies genau die Potenzen von Frob_q, also die Elemente der Untergruppe $r\mathbb{Z}/rm\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}$.

(2) folgt aus Korollar 114 und dem Gradsatz.

(3) Nach (2) sind die Zwischenkörper gerade von der Form $M_d = \mathbb{F}_{q^d}$. Die zugehörige Gruppe ist

$$\mathrm{Aut}_{M_d}(L) = \{\mathrm{Frob}_q^i \ ; \ \mathrm{Frob}_q^i|_{M_d} = \mathrm{id}\} = \langle \mathrm{Frob}_{q^d} \rangle.$$

Unter dem Isomorphismus $\mathrm{Aut}_K(L) \simeq \mathbb{Z}/m\mathbb{Z}$ wird daraus die Untergruppe $d\mathbb{Z}/m\mathbb{Z}$.

Die Behauptung über die Umkehrabbildung folgt sofort aus der Definition der $\mathbb{F}_{q^d}$ als Fixkörper von Frob_{q^d}.

Die Aussage (a) folgt sofort aus der expliziten Beschreibung, ebenso die exakte Sequenz, die isomorph ist zu

$$0 \to d\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \to 0.$$

(4) Eine Erweiterung endlicher Körper ist normal, weil jeder endliche Körper als Zerfällungskörper eines Polynoms aus $\mathbb{F}_p[T]$ über $\mathbb{F}_p$ normal ist. □

7.3. **Asymptotisches Zählen irreduzibler normierter Polynome.** In diesem Abschnitt sind wir daran interessiert, die normierten irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad d zu zählen.

Theorem 117. *Sei K ein Körper. Eine endliche Untergruppe $G \subseteq K^\times$ ist zyklisch.*

Beweis. Die Gleichung $T^d = 1$ hat für jedes $d \geq 1$ in K höchstens d viele Lösungen. Die Gruppe G enthält deshalb höchstens d Elemente $g \in G$ mit einer Ordnung $\mathrm{ord}(g) \mid d$. Damit folgt das Theorem aus dem folgenden Satz. □

Satz 118. *Sei G eine endliche Gruppe und für jedes $d \geq 1$ gelte*

$$\#\{g \in G \ ; \ \mathrm{ord}(g) \mid d\} \leq d.$$

Dann ist G zyklisch.

Beweis. Sei N die Gruppenordnung von G. Die Ordnung jedes Elements in G teilt N als Korollar zum Satz von Lagrange. Sei

$$\pi_G(d) := \#\{g \in G \ ; \ \mathrm{ord}(g) = d\}.$$

Wir müssen zeigen, daß $\pi_G(N) \neq 0$.

Je zwei Elemente x, y in G der gleichen Ordnung d erzeugen die gleiche Untergruppe. Denn $\langle x \rangle$ und $\langle y \rangle$ bestehen sämtlich aus Elementen, deren Ordnung ein Teiler von d ist. Davon gibt es nur d nach Voraussetzung also gilt

$$\langle x \rangle = \{g \in G \ ; \ \mathrm{ord}(g) \mid d\} = \langle y \rangle \simeq \mathbb{Z}/d\mathbb{Z}.$$

Damit gibt es in G entweder kein Element der Ordnung d oder genauso viele Elemente der Ordnung d wie in $\mathbb{Z}/d\mathbb{Z}$, also

$$\pi_G(d) \leq \varphi(d) = \pi_{\mathbb{Z}/d\mathbb{Z}}(d) = \pi_{\mathbb{Z}/N\mathbb{Z}}(d)$$

wobei $\varphi(n)$ die Eulersche φ-Funktion ist. Ein Vergleich mit $\mathbb{Z}/N\mathbb{Z}$ zeigt

$$\pi_G(N) = N - \sum_{d|N, d\neq N} \pi_G(d) \geq N - \sum_{d|N, d\neq N} \pi_{\mathbb{Z}/N\mathbb{Z}}(d) = \pi_{\mathbb{Z}/N\mathbb{Z}}(N) \neq 0$$

was verschieden von 0 ist, denn $\mathbb{Z}/N\mathbb{Z}$ enthält Elemente der Ordnung N. □

Korollar 119. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Beweis. Das folgt sofort aus Theorem 117. □

Korollar 120. *Jede Erweiterung endlicher Körper ist einfach.*

Beweis. Sei L/K eine Erweiterung endlicher Körper und α ein Erzeuger von $L^\times$. Dann gilt $L = K(\alpha)$. $\square$

Korollar 121. *Für jedes $d \geq 1$ gibt es in $\mathbb{F}_q[T]$ ein irreduzibles Polynom vom Grad d.*

Beweis. Sei α ein primitives Element für die Erweiterung $\mathbb{F}_{q^d}/\mathbb{F}_q$. Dann ist $P_{\alpha/\mathbb{F}_q}$ irreduzibel vom Grad $[\mathbb{F}_{q^d} : \mathbb{F}_q] = d$. $\square$

Jetzt wollen wir es genauer wissen. Wir setzen

$$\psi_q(n) = \#\{f \in \mathbb{F}_q[T] \ ; \ f \text{ normiert und irreduzibel}, \ \deg(f) = n\}.$$

Wir brauchen noch die Möbius-Funktion

$$\mu(n) = \begin{cases} (-1)^r & n = p_1 \cdot \ldots \cdot p_r \text{ paarweise verschiedene Primzahlen } p_i \\ 0 & \text{sonst.} \end{cases}$$

und Möbius Inversion:

Lemma 122. *Sei $f : \mathbb{N} \to R$ eine Funktion mit Werten in einem Ring R. Wenn*

$$F(n) = \sum_{d|n} f(d),$$

dann gilt die Möbius-Inversionsformel

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Beweis. Wir rechnen

$$\begin{aligned} \sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \mu(d) \left(\sum_{e|\frac{n}{d}} f(e) \right) = \sum_{ed|n} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \left(\sum_{d|\frac{n}{e}} \mu(d) \right) = \sum_{e|n} f(e) \left(\prod_{\ell|\frac{n}{e}, \text{ prim}} (1 + (-1)) \right) = f(n). \end{aligned}$$

Hier bilden wir im letzten Schritt das Produkt über die Primteiler ℓ von n/e, und dieses Produkt ist 0 außer für $n/e = 1$. Die entsprechende Gleichheit sieht man durch einfaches Ausmultiplizieren des Produkts der Faktoren $(1 + (-1))$. $\square$

Satz 123 (Primzahlsatz für Polynome)**.** *Es gilt*

$$\psi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

und

$$|\psi_q(n) - \frac{q^n}{n}| \leq \frac{2}{n} \cdot q^{n/2}.$$

Beweis. Wir betrachten die Abbildung

$$\begin{aligned} \Phi : \mathbb{F}_{q^n} &\to \{f \in \mathbb{F}_q[T] \ ; \ \text{ irreduzibel, normiert}, \ \deg(f) \mid n\} \\ \alpha &\mapsto P_{\alpha/\mathbb{F}_q}. \end{aligned}$$

Die Abbildung ist surjektiv, denn Adjunktion einer Nullstelle α eines irreduziblen Polynoms f vom Grad $\deg(f) = d \mid n$ erzeugt $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ und für dieses α ist f das Minimalpolynom. Hieraus sehen wir weiter, daß jedes solche f ein Teiler von $T^{q^n} - T$ ist, denn jedes $\alpha \in \mathbb{F}_{q^n}$ ist Nullstelle von $T^{q^n} - T$.

Die Fasern $\Phi^{-1}(f)$ sind gerade die Nullstellen des Polynoms f. Da jedes solche f ein Teiler von $T^{q^n} - T$ ist und dieses Polynom q^n verschiedene Wurzeln, nämlich die Elemente von $\mathbb{F}_{q^n}$ hat, folgt

$$T^{q^n} - T = \prod_{\alpha \in \mathbb{F}_{q^n}} (T - \alpha) = \prod_{f \in \mathbb{F}_q[T],\ \text{normiert, irred. } \deg(f) | n} f.$$

Wir vergleichen den Grad auf beiden Seiten und erhalten

$$q^n = \sum_{d|n} \sum_{\deg(f)=d} d = \sum_{d|n} d\psi_q(d),$$

wobei wir hier über irreduzible normierte $f \in \mathbb{F}_q[T]$ summieren. Möbius–Inversion, Lemma 122, zeigt die exakte Formel für $\psi_q(n)$.

Sei ℓ der kleinste Primteiler von n und $m = n/\ell \leq n/2$. Der Summand für $d = 1$ ist q^n/n. Für die restliche Summe benutzen wir die Dreiecksungleichung und schätzen $|\mu(d)|$ durch 1 ab:

$$|\psi_q(n) - \frac{q^n}{n}| \leq \frac{1}{n} \sum_{e|n, e<n} q^e \leq \frac{1}{n} \sum_{e=1}^{m} q^e = \frac{q^{m+1} - q}{n(q-1)} \leq \frac{q/(q-1)}{n} q^m \leq \frac{2}{n} q^{n/2}.$$

Dies zeigt die Abschätzung (denn für $n = 1$ ist nichts zu zeigen). □

Bemerkung 124. Die Abschätzung von Satz 123 bedeutet, daß asymptotisch für $q^n \to \infty$ der Anteil der normierten Polynome vom Grad n, welche irreduzibel sind, gegen $1/n$ strebt. Der Fehlerterm ist dabei mit $2/(n\sqrt{q^n})$ recht gut. Man schreibt

$$\psi_q(n) = \frac{q^n}{n} + \mathcal{O}(\frac{2}{n} q^{n/2}).$$

Übungsaufgaben zu §7

Übungsaufgabe 7.1. Finden Sie Normalformen für quadratische Körpererweiterungen in Charakteristik 2.

Übungsaufgabe 7.2 (Artin-Schreier Erweiterungen in Charakteristik p). Sei K ein Körper der Charakteristik $p > 0$. Zeigen Sie:

(1) Die Abbildung $\wp(x) = x^p - x$

$$\wp = \mathrm{Frob} - \mathrm{id} : K \to K$$

ist ein Gruppenhomomorphismus der additiven Gruppe.

(2) $\wp(x) = \wp(x+1)$

(3) Wenn $a \notin \wp(K)$, dann ist $T^p - T - a \in K[T]$ irreduzibel.

(4) Sei weiter $a \notin \wp(K)$ und $K(\alpha)/K$ die Adjunktion einer Nullstelle α von $T^p - T - a$. Dann ist $K(\alpha)$ der Zerfällungskörper von $T^p - T - a$.

(5) Bestimmen Sie $G = \mathrm{Aut}_K(K(\alpha))$ und bestimmen Sie den Fixkörper von $K(\alpha)$ unter G.

Übungsaufgabe 7.3. Sei K ein Körper der Charakteristik $p > 0$. Zeigen Sie, daß der Primkörper $\mathbb{F}_p$ von K der Fixkörper

$$\{x \in K \ ; \ \mathrm{Frob}(x) = x\}$$

des Frobenius ist.

Übungsaufgabe 7.4. Beweisen Sie Theorem 116.

Übungsaufgabe 7.5. Zeigen Sie, daß $T^q - T + 1$ in $\mathbb{F}_q[T]$ keine Nullstelle hat. Folgern Sie daraus, daß ein algebraisch abgeschlossener Körper nicht endlich sein kann.

Übungsaufgabe 7.6. Schreiben Sie alle irreduziblen normierten Polynome vom Grad ≤ 4 in $\mathbb{F}_p[T]$ für $p \leq 3$ auf.

Übungsaufgabe 7.7. Wann ist $\mathbb{F}_q$ ein Unterkörper von $\mathbb{F}_{q'}$?

Übungsaufgabe 7.8. Die Zeta-Funktion des Polynomrings.

(a) Für ein Ideal $(0) \neq \mathfrak{a} \subseteq \mathbb{F}_q[X]$ definieren wir $N(\mathfrak{a}) := \dim_{\mathbb{F}_q} \mathbb{F}_q[X]/\mathfrak{a}$.
Zeigen Sie, daß $N(\mathfrak{a}) \in \mathbb{N}$ ist und bestimmen Sie $N(\mathfrak{a})$ für $\mathfrak{a} = (f)$. Zeigen Sie weiter, daß $N(-)$ multiplikative ist: für alle $0 \neq f, g \in \mathbb{F}_q[X]$ gilt $N((fg)) = N((f))N((g))$.

(b) Wir rechnen im Potenzreihenring $\mathbb{Q}[[T]]$. Dort hat $1 - aT^r$, $a \in \mathbb{Q}, r > 0$ ein Inverses bezüglich der Multiplikation. Welches? Wir schreiben dafür $\frac{1}{1-aT^r}$.

(c) Wir definieren die Zeta-Funktion

$$\mathrm{Z}_{\mathbb{F}_q[X]}(T) := \sum_{(0)\neq\mathfrak{a}\subseteq\mathbb{F}_q[X]} T^{N(\mathfrak{a})} \in \mathbb{Q}[[T]],$$

wobei über alle von (0) verschiedenen Ideale $\mathfrak{a}$, auch $\mathbb{F}_q[X]$, summiert wird.
Zeigen Sie, daß $\mathrm{Z}_{\mathbb{F}_q[X]}(T)$ ein Element von $\mathbb{Q}[[T]]$ definiert und daß $\mathrm{Z}_{\mathbb{F}_q[X]}(T) = \frac{1}{1-qT}$ gilt.

(d) Wir übersetzen nun die eindeutige Primfaktorzerlegung von $\mathbb{F}_p[X]$ in eine Produktzerlegung von $\mathrm{Z}_{\mathbb{F}_p[X]}(T)$. Zeigen Sie, daß in $\mathbb{Q}[[T]]$ das Eulerprodukt gilt:

$$\mathrm{Z}_{\mathbb{F}_p[X]}(T) = \prod_{f\in\mathbb{F}_q[X] \text{ irreduzibel, normiert}} \frac{1}{1 - T^{N((f))}}.$$

Es ist zu begründen, warum das Produkt eine Potenzreihe in $\mathbb{Q}[[T]]$ darstellt.

(e) Es sei N_d die Anzahl der normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_q[X]$. Zeigen Sie für alle $n \in \mathbb{N}$ die Gleichung

$$q^n = \sum_{d|n} d \cdot N_d,$$

indem Sie formal die Operation $T\frac{d}{dT}\log(-)$ auf beiden Seiten der Identität aus (c) & (d) anwenden.
Dabei ist $\log(-)$ nur für Potenzreihen mit konstantem Term 1 als

$$\log(1-z) = -\sum_{n=1}^{\infty} \frac{1}{n} z^n$$

definiert. Dies ist wegen der gleichen Gründe sinnvoll, die in (d) das unendliche Produkt als wohldefiniert nachweisen. Differenziert werden die formalen Potenzreihen gliedweise.
Tipp: Für diesen formalen Logarithmus gilt ebenso $\log(ab) = \log(a) + \log(b)$, auch für ∞-viele Faktoren.

(f) Berechnen Sie die Anzahl der irreduziblen normierten Polynome vom Grad d in $\mathbb{F}_q[X]$ für $d = 12$ und $q = 2, 3, 4$.

8. Der rationale Funktionenkörper

Die folgende Konstruktion wird unseren Vorrat an interessanten Beispielen erhöhen.

8.1. **Lokalisieren.** Beim Übergang zu Faktorringen werden Relationen erzwungen. Beim Übergang zum Quotientenkörper forcieren wir Einheiten. Dies ist ein Beispiel für den Prozess des Lokalisierens.

Definition 125. Eine multiplikativ abgeschlossene Teilmenge eines Rings R ist eine Teilmenge $S \subseteq R$, mit

(i) $1 \in S$,
(ii) wenn $s, t \in S$, dann auch $st \in S$.

Beispiel 126. (1) $K[T] \setminus \{0\}$ in $K[T]$.

(2) $\mathbb{Z} \setminus \{0\}$ in $\mathbb{Z}$.
(3) $R \setminus \{0\}$ in R für einen Integritätsring R.
(4) $R^\times$ in R für jeden Ring.
(5) $\{1, p, p^2, \ldots\} \subseteq \mathbb{Z}$.
(6) $\{1, f, f^2, \ldots\} \subseteq R$ für jeden Ring R und jedes Element $f \in R$.

Wir formulieren nun abstrakt den Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$.

Satz 127 (Lokalisieren)**.** *Sei R ein Ring und sei $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann gibt es einen Ring, bezeichnet mit $S^{-1}R$, und einen Ringhomomorphismus*

$$i : R \to S^{-1}R,$$

so daß die folgenden Eigenschaften gelten:
(i) Für jedes $s \in S$ ist $i(s)$ eine Einheit von $S^{-1}R$.
(ii) Jeder Ringhomomorphismus $f : R \to A$ so daß für alle $s \in S$ das Bild $f(s)$ in A Einheit ist, faktorisiert eindeutig über $S^{-1}R$. Das heißt, es gibt einen eindeutigen Ringhomomorphismus $F : S^{-1}R \to A$, so daß das Diagramm

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[dr, "f"'] & S^{-1}R \arrow[d, dotted, "F"] \\ & A \end{tikzcd}$$

kommutiert.

Der Ring $S^{-1}R$ ist zusammen mit der Lokalisierungsabbildung $i : R \to S^{-1}R$ und den Forderungen (i) und (ii) eindeutig bis auf eindeutigen Isomorphismus.

Beweis. Die Eindeutigkeitsaussage beweist sich rein formal aus den geforderten Eigenschaften von selbst. Angenommen, es gibt zwei Lokalisierungen $(S^{-1}R)_1$ und $(S^{-1}R)_2$, dann erzwingt (ii) die Existenz von Ringhomomorphismen

$$\varphi : (S^{-1}R)_1 \to (S^{-1}R)_2 \quad \text{und} \quad \psi : (S^{-1}R)_2 \to (S^{-1}R)_1.$$

Man sieht sofort, daß $\varphi \circ \psi$ und $\psi \circ \varphi$ ein Faktorisierungsproblem wie in (ii) lösen, das auch die Identität löst. Da es nur eine eindeutige Lösung haben darf, sind φ und ψ zueinander inverse Isomorphismen.

Darüberhinaus sind die Isomorphismen φ und ψ eindeutig, wenn man fordert, daß sie mit den Lokalisierungsabbildungen kompatibel sind.

Der Gehalt des Satzes steckt also in der Konstruktion eines solchen Rings $S^{-1}R$ zusammen mit dem Lokalisierungshomomorphsimus $R \to S^{-1}R$. Die Idee zur Konstruktion ist *Bruchrechnen.* Wir definieren dazu auf der Menge

$$R \times S$$

eine Relation

$$(a, s) \sim (b, t) \iff \text{es gibt } u \in S \text{ mit } u(at - bs) = 0.$$

Man rechnet leicht nach, daß es sich um eine Äquivalenzrelation handelt: symmetrisch und reflexiv ist klar (mit $u = 1$). Transitiv sieht man wie folgt. Sei $(a, s) \sim (b, t)$, bezeugt durch $u \in S$ und $u(at - bs) = 0$, und sei $(b, t) \sim (c, r)$, bezeugt durch $v \in S$ und $v(br - ct) = 0$, dann ist $(a, s) \sim (c, r)$, weil $uvt \in S$ und

$$uvt(ar - cs) = vr(uat) - us(vct) = vr(ubs) - us(vbr) = 0.$$

Wir schreiben suggestiv

$$\frac{a}{s}$$

für die Äquivalenzklasse mit Vertreter (a, s). Die Definition der Relation liest sich dann

$$\frac{a}{s} = \frac{uat}{ust} = \frac{ubs}{ust} = \frac{b}{t}$$

als bekannte Gleichung durch Erweitern und Kürzen von Brüchen. Die Menge aller Äquivalenzklassen bezeichnen wir mit $S^{-1}R$.

Addition und Multiplikation auf $S^{-1}R$ definiert man wie für Brüche:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{at+bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st}. \end{aligned}$$

Es ist eine Übungsaufgabe, zu zeigen, daß dies aus $S^{-1}R$ einen Ring mit $1 = \frac{1}{1}$ macht. Die Abbildung $i : R \to S^{-1}R$

$$i(a) = \frac{a}{1}$$

ist offensichtlich ein Ringhomomorphsimus.

Sei $s \in S$. Wegen

$$i(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1$$

schickt i die Elemente von S auf Einheiten von $S^{-1}R$.

Sei $f : R \to A$ ein Ringhomomorphimus wie in (ii). Dann definieren wir $F : S^{-1}R \to A$ durch

$$F(\frac{a}{s}) := f(a)f(s)^{-1}.$$

Dies ist eine wohldefineirte Abbildung, denn aus $a/s = b/t$ folgt mit $u \in S$ und $u(at - bs)$

$$f(a)f(s)^{-1} = f(uat)f(ust)^{-1} = f(ubs)f(ust)^{-1} = f(b)f(t)^{-1}.$$

Außerdem ist F ein Ringhomomorphismus: die Eins wird bewahrt

$$F(1) = F(1/1) = f(1)f(1)^{-1} = 1,$$

F ist additiv

$$\begin{aligned} F(a/s + b/t) &= F((at+bs)/st) = f(at+bs)f(st)^{-1} \\ &= f(at)f(st)^{-1} + f(bs)f(st)^{-1} = F(a/s) + F(b/t), \end{aligned}$$

und multiplikativ

$$\begin{aligned} F(a/s \cdot b/t) &= F(ab/st) = f(ab)f(st)^{-1} \\ &= f(a)f(s)^{-1} \cdot f(b)f(t)^{-1} = F(a/s) \cdot F(b/t), \end{aligned}$$

Die in (ii) geforderte Faktorisierungseigenschaft gilt, da für alle $a \in R$

$$F(a/1) = f(a)f(1)^{-1} = f(a).$$

Die Definition von F ist zudem die einzig mögliche, da

$$F(\frac{a}{s}) = F(\frac{a}{1} \cdot \frac{1}{s}) = F(i(a)i(s)^{-1}) = F(i(a)) \cdot F(i(s))^{-1} = f(a)f(s)^{-1}.$$

Die verbleibenden Details der Beweise, insbesondere das Assoziativgesetz und das Distributivgesetz in $S^{-1}R$, bleiben der geneigten Leserschaft zur Übung überlassen. $\square$

Bemerkung 128. (1) Der Faktor u in der Definition der Äquivalenzrelation auf den Paaren (a, s) aus dem Beweis von Satz 127 wird benötigt, falls es im Ring R Nullteiler gibt. Für Integritätsringe R kann man stets $u = 1$ verwenden.

(2) Es ist erlaubt, daß das multiplikative System $S \subseteq R$ die 0 anthält. Dann allerdings ist $S^{-1}R = 0$ der Nullring.

Die Umkehrung gilt auch: wenn $S^{-1}R = 0$, dann ist $1/1 = 0/1$. Also gibt es $u \in S$ mit

$$u = u(1 \cdot 1 - 0 \cdot 1) = 0.$$

Proposition 129. *Die Lokalisierungsabbildung $i : R \to S^{-1}R$ ist injektiv genau dann, wenn in S keine Nullteiler enthalten sind.*

Beweis. Sei $a \in R$ mit $i(a) = 0$. Dann ist $a/1 = 0/1$ und es gibt $u \in S$ mit $0 = u(a \cdot 1 - 0 \cdot 1) = ua$. Dies zeigt die Aussage, denn dieselbe Argumentation funktioniert auch rückwärts. □

8.2. **Der Quotientenkörper.** Aus dem Kriterium von Proposition 129 folgt sofort, daß die Abbildung in die Lokalisierung eines Integritätsrings stets injektiv ist.

Proposition 130. *Sei R ein Integritätsring und $S = R \setminus \{0\}$. Dann ist S multiplikativ abgeschlossen und*

$$\mathrm{Quot}(R) = S^{-1}R$$

*ein Körper, genannt der **Quotientenkörper** von R.*

Beweis. Sei $a/s \in K$. Dann ist $a/s \neq 0$ äquivalent zu $a \neq 0$ (Übung!). Solche Elemente sind invertierbar mit Inversem s/a. □

Bemerkung 131. Sei K ein Körper und $R \subseteq K$ ein Unterring. Dann ist R Integritätsring. Sei $S = R \setminus \{0\}$. Da $S \subseteq K$ nur aus Einheiten besteht, gibt es nach der universellen Eigenschaft des Lokalisierens eine Fortsetzung der Inklusion $R \subseteq K$ zu einem Ringhomomorphismus

$$\mathrm{Quot}(R) \to K.$$

Da $\mathrm{Quot}(R)$ ein Körper ist, muß diese Abbildung injektiv sein. Es folgt, daß jeder Körper K, der den Integritätsring $R \subseteq K$ enthält, auch den Quotientenkörper enthält. Der Quotientenkörper von R ist also in diesem Sinne der kleinste Körper der R enthält.

Diese Bemerkung haben wir schon benutzt, als wir in Charakteristik 0 den Körper $\mathbb{Q}$ als Primkörper erkannt haben.

Definition 132. Der **Rationale Funktionenkörper** über einem Körper K ist der Quotientenkörper, bezeichnet mit $K(X)$, des Polynomrings $K[X]$. Die Elemente von $K(X)$ sind gebrochenrationale Funktionen

$$f(X) = \frac{g(X)}{h(X)}$$

mit $g(X), h(X) \in K[X]$ und $h(X) \neq 0$.

Analog zu Satz 19, der von algebraischen Elementen erzeugte Teilerweiterungen beschreibt, können wir nun von transzendenten Elementen erzeugte Erweiterungen beschreiben.

Satz 133. *Sei K ein Körper.*

(1) Das Element X in $K(X)$ ist transzendent über K.

(2) Für jede Körpererweiterung L/K und ein transzendentes Element $\tau \in L$ gibt es genau eine K-Einbettung

$$K(X) \hookrightarrow L,$$

die X auf τ abbildet, somit $K(\tau) \simeq K(X)$.

Beweis. (1) Sei $f \in K[T]$ ein Polynom. Dann ist die Auswertung von f in X nichts anderes als $f(X)$, mit der Variablen T ersetzt durch X. Da die Abildung $K[X] \to K(X)$ injektiv ist, erfüllt X keine algebraische Relation über K. Die Variable X ist also transzendent über K.

(2) Sei $\tau \in L$ transzendent über K. Dann gibt es einen eindeutigen Ringhomomorphismus

$$K[X] \to L$$

mit $X \mapsto \tau$, also $f(X) \mapsto f(\tau)$. Dieser ist injektiv, da τ transzendent ist: $f(\tau) = 0$ impliziert $f = 0$. Damit wird $K[X] \setminus \{0\}$ auf invertierbare Elemente von L abgebildet und somit existiert die eindeutige Fortsetzung

$$K(X) \to L$$

wie verlangt. Das Bild ist genau $K(\tau)$. □

Beispiel 134. Sei K ein Körper. Die Erweiterung $K(X)/K$ hat unendlich viele Zwischenkörper

$$K(X) \supsetneq K(X^2) \supsetneq K(X^4) \ldots \supsetneq K.$$

Angenommen X^n ist algebraisch über K. Dann gibt es ein $f \in K[T]$, $f \neq 0$ mit $f(X^n) = 0$. Dann ist X eine Nullstelle des Polynoms $f(T^n)$ vom Grad $n \cdot \deg(f)$, also eines nicht-triviales Polynoms. Da X transzendent ist, erhalten wir einen Widerspruch. Somit sind die $X^n \in K(X)$ transzendent über K, und nach Satz 133 ist $K(X^n) \simeq K(X)$ für alle $n \geq 1$.

Es muß noch gezeigt werden, daß die Zwischenkörper verschieden sind. Dazu sei

$$X^n \in K(X^d)$$

es gibt also $f, g \in K[T]$ mit $g \neq 0$ und

$$X^n g(X^d) = f(X^d).$$

Durch Koeffzientenvergleich ergibt sich $d \mid n$.

Korollar 135. *Eine Körpererweiterung L/K mit nur endlich vielen Zwischenkörpern ist endlich algebraisch und von einem Element erzeugt.*

Beweis. Es muß L von endlich vielen Elementen erzeugt sein, da sonst

$$K \subseteq K(x_1) \subseteq K(x_1, x_2) \subseteq K(x_1, x_2, x_3) \subseteq \ldots$$

undendlich viele Zwischenkörper beschreibt.

Angenommen L/K wäre nicht algebraisch. Dann gibt es $\tau \in L$, das transzendent über K ist. der Zwischenkörper $K(\tau)$ ist isomorph zu $K(X)$. Damit gibt es nach Beispiel 134 in $K(\tau)/K$ und damit in L/K unendlich viele Zwischenkörper, Widerspruch.

Nun haben wir L/K als von endlich vielen algebraischen Elementen erzeugt erkannt. Damit ist L/K endlich nach Proposition 26. Das Korollar folgt nun aus Satz 33. □

9. Separable Erweiterungen

Einige formale Begriffe der Analysis funktionieren auch in der Algebra.

9.1. Algebraische Differentiation und mehrfache Nullstellen.

Definition 136. Eine **Derivation** auf einem Ring R ist eine Gruppenhomomorphismus

$$\partial : R \to R,$$

der zugrundeliegenden additiven Gruppe $(R, +)$ des Rings R: für alle $f, g \in R$

$$\partial(f + g) = \partial(f) + \partial(g),$$

welche die Leibniz–Regel erfüllt: für alle $f, g \in R$ gilt

$$\partial(fg) = f\partial(g) + g\partial(f).$$

Beispiel 137. (1) Sei $U \subseteq \mathbb{R}$ eine offene Teilmenge und $R = \mathrm{C}^\infty(U)$ der Ring der unendlich oft stetig differenzierbaren reellwertigen Funktionen auf U. Dann ist die Differentiation der Analysis

$$\partial(f) = \frac{df}{dx}(x)$$

eine Derivation von $\mathrm{C}^\infty(U)$.

(2) Sei $R = K[T]$ der Polynomring über einem Körper K. Dann definiert für $f = a_nT^n + \ldots + a_1T + a_0$

$$f' := na_nT^{n-1} + \ldots + a_1$$

eine Derivation $f \mapsto f'$ auf $K[T]$. Dies ist die **algebraische (oder formale) Differentiation**.

Diese Derivation ist K-linear, wie man in der Basis der Potenzen T^i sofort sieht. Die Leibniz–Regel ist linear in beiden Argumenten. Es reicht deshalb, die Regel für Basiselemente zu verifizieren.

$$\begin{aligned}(T^n \cdot T^m)' = (T^{n+m})' = (n+m)T^{n+m-1} &= T^m \cdot nT^{n-1} + T^n \cdot mT^{m-1}\\ &= T^m \cdot (T^n)' + T^n \cdot (T^m)'.\end{aligned}$$

Für $K = \mathbb{R}$ und der Interpretation reeller Polynome als Polynomfunktionen ist algebraische Differentiation nichts anderes als Differentiation im Sinne der Analysis.

Beispiel 138. Sei K ein Körper der Charakteristik $p > 0$. Dann gilt

$$(T^p)' = pT^{p-1} = 0,$$

obwohl T^p kein konstantes Polynom ist.

Proposition 139. *Sei K ein Körper und $f \in K[T]$. Dann sind äquivalent:*

(a) $f' = 0$

(b) Es ist f konstant, oder K hat Charakteristik $p > 0$ und es gibt ein $g \in K[T]$ mit $f = g(T^p)$.

Beweis. Dies folgt offensichtlich aus der Definition. □

Proposition 140. *Sei $f \in K[T]$ ein Polynom. Die mehrfachen Nullstellen (in einer Erweiterung von K) sind genau die Nullstellen von* $\mathrm{ggT}(f, f')$.

Beweis. Der $\mathrm{ggT}(f, g)$ für $f, g \in K[T]$ kann über den euklidischen Algorithmus berechnet werden. Dieser ändert sich nicht, wenn man f, g als Polynome in $L[T]$ für eine Erweiterung L/K auffaßt. Wir dürfen daher oBdA annehmen, daß f in Linearfaktoren zerfällt.

Wichtiges Prinzip: Übergang zu einem Erweiterungskörper (Skalarerweiterung), der die Situation vereinfacht aber Wesentliches beibehält.

Es habe nun f eine mehrfache Nullstelle. Dann gibt es $\alpha \in K$ und $g \in K[T]$ mit

$$f = (T - \alpha)^2 g$$

und nach Leibniz

$$f' = 2(T - \alpha)g + (T - \alpha)^2 g' = (T - \alpha)(2g + (T - \alpha)g').$$

Damit ist $T - \alpha$ auch ein Teiler von f'.

Sei umgekehrt α eine Nullstelle von f und f'. Dann gibt es $g \in K[T]$ mit $f = (T - \alpha)g$ und nach Leibniz

$$0 = f'(\alpha) = (g + (T - \alpha)g')(\alpha) = g(\alpha).$$

Daher ist α eine mehrfache Nullstelle von f. □

9.2. **Separable Polynome.**

Definition 141. Ein **separables** Polynom ist ein Polynom ohne mehrfache Nullstellen in jeder Körpererweiterung. Andernfalls nennt man das Polynom **inseparabel**.

Proposition 142. *Für $f \in K[T]$ sind äquivalent:*

(a) f ist separabel.

(b) $\mathrm{ggT}(f, f') = 1$, *also f und f' sind teilerfremd.*

(c) f hat im algebraischen Abschluß von K genau $\deg(f)$ *viele Nullstellen.*

Beweis. (a) $\iff$ (c) ist trivial und (a) $\iff$ (b) folgt sofort aus Proposition 140. □

Beispiel 143. Wir betrachten $f = T^{q^n} - T \in \mathbb{F}_q[T]$. Dann ist $f' = -1$ und somit teilerfremd zu f. Dies zeigt erneut (und schneller), daß $T^{q^n} - T$ im algebraischen Abschluß q^n verschiedene Nullstellen hat.

Korollar 144. *Ein irreduzibles Polynom $f \in K[T]$ ist inseparabel genau dann, wenn $f' = 0$.*

Beweis. Es gibt eine mehrfache Nullstelle, genau dann, wenn $\mathrm{ggT}(f, f') \neq 1$ keine Einheit ist. Da f irreduzibel ist, muß dann
$$\mathrm{ggT}(f, f') = f$$
sein, und $f \mid f'$. Aber f ist kein Teiler von f' wegen $\deg(f') < \deg(f)$, außer wenn $f' = 0$ ist. □

Satz 145. *Sei K ein Körper. Dann sind äquivalent.*

(a) *K hat Charakteristik 0 oder K hat Charakteristik p und $K = K^p$, d.h.* $\mathrm{Frob} : K \to K$ *ist ein Automorphismus.*

(b) *Jedes irreduzible Polynom in $K[T]$ ist separabel.*

Beweis. Wir machen eine Fallunterscheidung nach der Charakteristik von K. In Charakteristik 0 ist $f' \neq 0$ für alle irreduziblen Polyniome f. Nach Korollar 144 sind somit alle irreduziblen Polynome separabel.

Sei nun K von Charakteristik $p > 0$. Angenommen $a \in K \setminus K^p$ ist keine p-te Potenz in K. Sei $L = K(\alpha)$ eine Erweiterung, die durch Adjunktion einer Wurzel α von $T^p - a$ entsteht. In $L[T]$ gilt
$$T^p - a = T^p - \alpha^p = (T - \alpha)^p.$$
Daher ist kein irreduzibler Faktor von $T^p - a$ separabel, denn keiner ist von Grad 1, da $a \notin K^p$.

Angenommen, es gilt $K = K^p$. Wir müssen zeigen, daß jedes irreduzible Polynom f separabel ist. Wir zeigen dies durch Widerspruch. Wenn f nicht separabel ist, dann ist nach Korollar 144 schon $f' = 0$. Nach Proposition 139 gibt es somit $g = \sum_{i=0}^d a_i T^i$ mit $f = g(T^p)$. Nach Voraussetzung gibt es $b_i \in K$ mit $b_i^p = a_i$. Wir setzen $h = \sum_{i=0}^d b_i T^i$ und finden
$$f = g(T^p) = \sum_{i=0}^d a_i T^{pi} = \sum_{i=0}^d b_i^p T^{pi} = \left(\sum_{i=0}^d b_i T^i\right)^p = h^p.$$
Damit ist f selbst eine p-te Potenz und sicher nicht irreduzibel, Widerspruch. □

Bemerkung 146. Wenn K ein Körper der Charakteristik $p > 0$ ist, dann ist die Menge der p-ten Potenzen K^p ein Unterkörper von K, der sogar als Körper isomorph zu K ist. Der Isomorphismus wird durch den Frobenius gegeben.

Definition 147. Einen Körper, der die äquivalenten Bedingung aus Satz 145 erfüllt, nennt man **perfekt** (oder **vollkommen**).

Korollar 148. *Endliche Körper sind perfekt.*

Beweis. Der Frobenius ist für endliche Körper ein Automorphismus, siehe Satz 107. □

Beispiel 149. Das Hauptbeispiel für nicht perfekte Körper ist der Körper $K(T)$ der rationalen Funktionen. Das Bild des Frobenius ist
$$\mathrm{Frob}(K(X)) = K^p(X^p).$$
Dies ist in $K(X^p)$ enthalten, wovon $K(X)$ eine Erweiterung vom Grad p ist. Ein Beispiel für ein inseparables Polynom in $K(X)[T]$ ist
$$T^p - X = 0,$$
denn X ist keine p-te Potenz in $K(X)$.

9.3. **Separable Elemente und Erweiterungen.**

Definition 150. Ein **separables** Element einer Körpererweiterung L/K ist ein algebraisches Element $\alpha \in L$, so daß $P_{\alpha/K}$ separabel ist. Wenn $P_{\alpha/K}$ inseparabel ist, heißt α **inseparabel**.

Proposition 151. *Sei K ein perfekter Körper. Dann ist jedes algebraische Element über K auch separabel.*

Beweis. Minimalpolynome sind irreduzibel. Per Definition gibt es in $K[T]$ gar keine inseparablen irreduziblen Polynome. □

Bemerkung 152. Separabel zu sein, ist ein relativer Begriff in Bezug auf den Grundkörper. Sei K ein Körper der Charakteristik $p > 0$ und $a \in K \setminus K^p$. Sei $L = K(\alpha)$ die Adjunktion der Nullstelle α von $T^p - a$. Dann ist α inseparabel über K aber separabel über L.

Definition 153. Sei L/K eine endliche Erweiterung und Ω/K eine algebraisch abgeschlossene Erweiterung. Der **Separabilitätsgrad** von L/K ist

$$[L : K]_s = \#\operatorname{Hom}_K(L, \Omega).$$

Proposition 154. *Der Separabilitätsgrad einer endlichen Erweiterung L/K ist unabhängig von der Wahl eines algebraischen Abschlusses von K.*

Beweis. Jede K-Einbettung $\sigma : L \to \Omega$ nimmt Werte in über K algebraischen Elementen an. Damit faktorisiert σ über den relativen algebraischen Abschluß Ω_a. Wir dürfen also in der Definition des Separabilitätsgrads annehmen, daß Ω ein algebraischer Abschluß von K ist. Sei Ω' ein weitere solcher. Dann gibt es nach Satz 97 einen K-Isomorphismus $\psi : \Omega \simeq \Omega'$. Die Abbildung

$$\psi\circ : \operatorname{Hom}_K(L, \Omega) \to \operatorname{Hom}_K(L, \Omega')$$

der Komposition mit ψ ist offensichtlich bijketiv. □

Definition 155. Eine **endliche separable Erweiterung** ist eine endliche Körpererweiterung L/K mit

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

Bemerkung 156. In Korollar 72 haben wir bewiesen, daß stets

$$[L : K]_s \leq [L : K].$$

Proposition 157. *Sei L/K eine Erweiterung, $\alpha \in L$ algebraisch über K und Ω eine algebraisch abgeschlossene Erweiterung von K. Dann sind äquivalent:*

(a) *Das Element α ist separabel über K.*
(b) *Das Polynom $P_{\alpha/K}$ ist separabel.*
(c) $\deg(P_{\alpha/K}) = \#\operatorname{NS}_{P_{\alpha/K}}(\Omega)$.
(d) *Die Erweiterung $K(\alpha)/K$ ist separabel.*

Beweis. (a) $\iff$ (b) gilt per Definition und (b) $\iff$ (c) folgt aus Proposition 142.

Es gilt $[K(\alpha) : K] = \deg(P_{\alpha/K})$, und

$$[K(\alpha) : K]_s = \#\operatorname{Hom}_K(K(\alpha), \Omega) = \#\operatorname{NS}_{P_{\alpha/K}}(\Omega)$$

Damit sind äquivalent:

$$[K(\alpha) : K] = [K(\alpha) : K]_s$$

und

$$\deg(P_{\alpha/K}) = \#\operatorname{NS}_{P_{\alpha/K}}(\Omega),$$

und dies zeigt (c) $\iff$ (d). □

Somit verstehen wir separable Erweiterungen, die von einem Element erzeugt sind.

Satz 158. *Sei $L/M/K$ ein Körperturm. Dann ist der Separabilitätsgrad multiplikativ:*

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

Insbesondere ist L/K seprabel genau dann, wenn L/M und M/K separabel sind.

Beweis. Sei Ω eine algebraisch abgeschlossene Erweiterung von K. Wir betrachten die Restriktionsabbildung

$$\begin{aligned} r : \mathrm{Hom}_K(L,\Omega) &\to \mathrm{Hom}_K(M,\Omega) \\ \sigma &\mapsto \sigma|_M \end{aligned}$$

Die Abbildung r ist surjektiv nach dem Fortsetzungssatz von Steinitz, Satz 97. Die Faser $r^{-1}(\sigma)$ sind von der Form

$$\mathrm{Hom}_M(L,\Omega)$$

wobei Ω als Erweiterung von M vermöge $\sigma : M \to \Omega$ aufzufassen ist. Nach Proposition 154 enthalten alle Fasern genau $[L:M]_s$ Elemente, und weil es davon $[M:K]_s$ viele gibt folgt die Teleskopformel.

Der Zusatz folgt, indem man mit dem Gradsatz vergleicht

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

in welchem nach Bemerkung 156 die entsprechenden Terme höchstens größer sind. Es gilt Gleichheit

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

auf der linken Seite genau dann, wenn Gleichheit

$$[L:M] = [L:M]_s \text{ und } [M:K] = [M:K]_s$$

auf der rechten Seite gilt. □

Satz 159. *Für eine endliche L/K Körpererweiterung sind äquivalent:*

(a) *L/K ist separabel.*
(b) *L ist von endlich vielen über K separablen Elementen erzeugt: $L = K(\alpha_1, \ldots, \alpha_n)$ mit α_i separabel über K für $1 \leq i \leq n$.*
(c) *Jedes Element von L ist separabel über K.*

Beweis. (a) $\Longrightarrow$ (c): Wenn L/K separabel ist, dann ist für jedes $\alpha \in L$ nach Satz 158 die Erweiterung $K(\alpha)/K$ separabel und daher α separabel über K nach Proposition 157.

(c) $\Longrightarrow$ (b): Die endliche Erweiterung L/K ist endlich erzeugt, und nach Voraussetzung damit durch endlich viele separable Elemente erzeugt.

(b) $\Longrightarrow$ (a): Dies zeigen wir nach Induktion über die Anzahl der Erzeuger. Wir nehmen also an, daß $M = K(\alpha_1, \ldots, \alpha_{n-1})$ über K separabel ist, und $\alpha_n \in L$ über K separables Element ist. Es gilt in $M[T]$

$$P_{\alpha_n/M} \mid P_{\alpha_n/K}.$$

Somit hat das Minimalpolynom von α_n über M auch keine mehrfachen Nullstellen und α_n ist separabel über M. Damit sind L/M und M/K separabel und nach Satz 158 auch L/K. □

Korollar 160. *Sei L/K eine Körpererweiterung und M, E Zwischenkörper, die über K endlich sind. Sei $F = ME$ das Kompositum in L.*

(1) *Wenn M/K separabel ist, dann auch F/E.*
(2) *Wenn M/K normal ist, dann auch F/E.*

$$\begin{tikzcd}[arrows=dash]
 & L \\
 & F = ME \arrow[u] \arrow[dl] \arrow[dr, "\text{normal, sep.}"] & \\
M \arrow[dr, "\text{normal, sep.}"'] & & E \arrow[dl] \\
 & K &
\end{tikzcd}$$

Beweis. (1) Wir schreiben nach Satz 159 $M = K(\alpha_1, \dots, \alpha_n)$. Dann ist $F = E(\alpha_1, \dots, \alpha_n)$ und die α_i sind wie im Beweis von Satz 159 weiter separabel über E. Daher ist auch F/E separabel.

(2) Sei $F \subseteq \Omega$ eine Erweiterung und $\sigma : F \to \Omega$ eine E-Einbettung. Dann ist die Einschränkung $\sigma|_M : M \to \Omega$ eine K-Einbettung, die wegen M/K normal Bild in M hat. Damit gilt

$$\sigma(F) = \sigma(ME) = \sigma(M)E = ME = F$$

und F/E ist auch normal. □

9.4. Primitive Elemente.

Theorem 161 (Satz vom primitiven Element)**.** *Sei L/K eine endliche separable Körpererweiterung. Dann ist L/K einfach, d.h., $L = K(\alpha)$ für ein geignetes Elment $\alpha \in L$.*

Beweis. Wir suchen ein α, mit $\deg(P_{\alpha/K}) = [L : K]$. Denn dann gilt

$$[K(\alpha) : K] = \deg(P_{\alpha/K}) = [L : K]$$

und nach dem Gradsatz

$$[L : K(\alpha)] = 1$$

somit $L = K(\alpha)$.

Sei $K \hookrightarrow \Omega$ eine algebraisch abgeschlossene Erweiterung. Da L/K separabel ist, gilt

$$n = [L : K] = [L : K]_s = \# \operatorname{Hom}_K(L, \Omega).$$

Seien $\sigma_1, \dots, \sigma_n$ die Elemente von $\operatorname{Hom}_K(L, \Omega)$. Dann sind $\sigma_i(\alpha)$ gerade die Nullstellen von $P_{\alpha/K}$ in Ω. Daher

$$n = [L : K] \geq [K(\alpha) : K] = \deg(P_{\alpha/K}) \geq \#\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}.$$

Wir haben zu zeigen, daß für geeignetes α die $\sigma_i(\alpha)$ paarweise verschieden sind.

Zurück zum Anfang. Der Fall K endlich wurde bereits in Korollar 120 behandelt. Sei daher nun K als unendlich angenommen. Per Induktion reicht der Fall $L = K(a, b)$. Dann gilt für alle $i \neq j$

$$(\sigma_i(a), \sigma_i(b)) \neq (\sigma_j(a), \sigma_j(b)) \in \Omega^2$$

denn sonst wäre $\sigma_i = \sigma_j$. Sei nun

$$f(T) = \prod_{i<j} \big((\sigma_i(a) + \sigma_i(b)T) - (\sigma_j(a) + \sigma_j(b)T) \big)$$

Keiner der Faktoren verschwindet identisch. Daher ist $f(T) \in \Omega[T]$ von 0 verschieden, insbesondere hat f auch in K höchstens endlich viele Nullstellen. Damit gibt es $t \in K$ und $f(t) \neq 0$. Für dieses t setzen wir $c = a + bt$ und finden für $i < j$

$$\sigma_i(c) = \sigma_i(a) + \sigma_i(b)t \neq \sigma_j(a) + \sigma_j(b)t = \sigma_j(c).$$

da sonst der Faktor $i < j$ in $f(T)$ bei t eine Nullstelle hätte. Dieses c ist das gesuchte Element. □

Korollar 162. *Eine endliche separable Körpererweiterung hat nur endlich viele Zwischenkörper.*

Beweis. Das folgt sofort aus Theorem 161 zusammen mit Satz 33. □

9.5. **Inseparable Elemente und Erweiterungen.**

Definition 163. Ein rein inseparables Element ist ein algebraisches Element α einer Körpererweiterung L/K in Charakteristik $p > 0$, so daß für hinreichend großes $n \in \mathbb{N}$ gilt $\alpha^{p^n} \in K$.

Proposition 164. *Wenn $\alpha \in L/K$ ein rein inseparables Element ist, dann gibt es $a \in K$ und $n \in \mathbb{N}_0$, so daß*

$$P_{\alpha/K} = T^{p^n} - a.$$

Beweis. Nach Definition gibt es $m \in \mathbb{N}$ und $b \in K$, so daß $\alpha^{p^m} = b$. Damit ist

$$P_{\alpha/K} \mid T^{p^m} - b = (T - \alpha)^{p^m}$$

ein Polynom mit nur einer einzigen Nullstelle. Es gibt also $N \in \mathbb{N}$ mit

$$P_{\alpha/K} = (T - \alpha)^N.$$

Der konstante Koeffizient α^N ist auch in K. Sei $p^n = \mathrm{ggT}(N, p^m)$. Dann gibt es $r, s \in \mathbb{Z}$ mit

$$p^n = rp^m + sN$$

und somit

$$a = \alpha^{p^n} = (\alpha^{p^m})^r \cdot (\alpha^N)^s \in K.$$

Wir schließen, daß

$$P_{\alpha/K} \mid T^{p^n} - a$$

und weil $p^n \leq N = \deg(P_{\alpha/K})$ muß sogar, wie behauptet, Gleichheit gelten. □

Bemerkung 165. Rein inseparabel zu sein, ist ein relativer Begriff in Bezug auf den Grundkörper. Sei K ein Körper der Charakteristik $p > 0$ und L/K eine nichttriviale separable Erweiterung. Dann ist jedes $\alpha \in L/K$ rein inseparabel über L (trivial) aber nicht rein inseparabel über K. Sonst wäre das Minimalpolynom nach Proposition 164 von der Form $f = T^{p^n} - a$ mit $f' = 0$, also inseparabel, im Widerspruch zu L/K separabel.

Definition 166. Eine endliche **rein inseparable** Körpererweiterung ist eine endliche Erweiterung L/K, so daß es keine nicht-triviale separable Teilerweiterung gibt, d.h., es gibt kein $K \subseteq M_0 \subseteq M_1 \subseteq L$ mit M_1/M_0 separabel und $[M_1 : M_0] > 1$.

Beispiel 167. Sei $L = \mathbb{F}_p(X)$ und $K = \mathbb{F}_p(X^p) \subseteq L$. Dann ist L/K rein inseparabel: da der Grad $[L : K] = p$ eine Primzahl ist, kann es keine anderen Zwischenerweiterungen geben als L/K selbst. Das Element $X \in L$ hat das inseparable Minimalpolynom

$$T^p - X^p = (T - X)^p.$$

Außerdem ist X rein inseparabel über K, denn X^p liegt schon in K.

Satz 168. *Sei L/K eine endliche Erweiterung. Dann sind äquivalent.*

(a) L/K *ist rein inseparabel.*
(b) $[L : K]_s = 1$.
(c) $L^{p^n} \subseteq K$ *für hinreichend großes* $n \in \mathbb{N}$.
(d) L *is von endlich vielen über* K *rein inseparablen Elementen erzeugt.*

(e) *Alle $\alpha \in L$ sind über K rein inseparabel.*

Beweis. (e) $\implies$ (d) $\implies$ (c) ist trivial.

Wenn (c) gilt, dann kann man jede Einbettung $\tau : K \to \Omega$ in einen algebraisch abgeschlossenen Körper Ω nur auf eine eindeutige Weise fortsetzen: es gibt eine Fortsetzung nach Steinitz Satz 97. Und diese ist eindeutig, da $\mathrm{Frob} : \Omega \to \Omega$ injektiv ist und deshalb für zwei K-Einbettungen $\sigma_1, \sigma_2 : L \to \Omega$ gilt

$$\sigma_1 = \sigma_2 \iff \mathrm{Frob}^n \circ \sigma_1 = \mathrm{Frob}^n \circ \sigma_2 \iff \sigma_1|_{L^{p^n}} = \sigma_2|_{L^{p^n}},$$

und das gilt, weil auf L^{p^n} beide Einbettungen mit τ übereinstimmen. Damit ist $[L : K]_s = 1$ und (b) gilt.

(b) $\implies$ (a): Aus der Version des Gradsatzes für den Separabilitätsgrad folgt für jedes $K \subseteq M_0 \subseteq M_1 \subseteq L$, daß $[M_1 : M_0]_s$ ein Teiler von $[L : K]_s = 1$ ist.

(a) $\implies$ (e): Dies beweisen wir durch Widerspruch. Sei $\alpha \in L$ nicht rein inseparabel über K. Wir schreiben

$$P_{\alpha/K} = f(T^{p^n})$$

für $f \in K[T]$ und n maximal möglich. Dann ist f nicht linear, sonst wäre

$$\alpha^{p^n} = f(\alpha^{p^n}) - f(0) = P_{\alpha/K}(\alpha) - f(0) = -f(0) \in K.$$

Aber f muß irreduzibel sein, denn eine Zerlegung von $f = gh$ würde auch eine Zerlegung

$$P_{\alpha/K} = f(T^{p^n}) = g(T^{p^n})h(T^{p^n})$$

nach sich ziehen. Damit ist

$$f = P_{\alpha^{p^n}/K}$$

und, wegen $f' \neq 0$ per Konstruktion, ein separables irreduzibles Polynom. Damit haben wir in L/K eine nicht-triviale ($\deg(f) > 1$) separable Teilerweiterung $K(\alpha^{p^n})/K$ gefunden. Das ist der gesuchte Widerspruch. $\square$

Korollar 169. *Sei $L/M/K$ ein Körperturm endlicher Erweiterungen. Dann ist L/K rein inseparabel genau dann, wenn L/M und M/K rein inseparabel sind.*

Beweis. Wir verwenden Satz 168 (c) (oder (b)), und damit ist alles klar. $\square$

Korollar 170. *Sei L/K eine endliche Körpererweiterung. Dann ist $\alpha \in L$ separabel und rein inseparabel über K genau dann wenn $\alpha \in K$.*

Beweis. Das Element α ist rein inseparabel und separabel genau dann, wenn $K(\alpha)/K$ rein inseparabel und separabel ist, also

$$[K(\alpha) : K] = [K(\alpha) : K]_s = 1.$$

Das bedeutet $\alpha \in K$. $\square$

Korollar 171. *Sei L/K eine endliche rein inseparable Erweiterung von Körpern der Charakteristik $p > 0$. Dann gibt es einen Körperturm*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

und Elemente $\alpha_i, a_i \in K_i$ mit

(i) $[K_{i+1} : K_i] = p$,
(ii) $K_{i+1} = K_i(\alpha_{i+1})$ *und* $\alpha_{i+1}^p = a_i \in K_i$.

Insbesondere ist $[L : K]$ eine p-Potenz.

Beweis. Wir beweisen dies per Induktion nach dem Grad $[L : K]$. Wenn M ein echter Zwischenkörper von L/K ist, dann ist auch M/K und L/M rein inseparabel. Wenn der Satz für M/K und für L/M gilt, dann kann man die jeweiligen Körpertürme zusammensetzen und bekommt einen Turm wie im Satz behauptet.

Wir dürfen daher annehmen, daß $L = K(\alpha)$ einfach ist. Dann ist α ein rein inseparables Element und hat nach Proposition 164 ein Minimalpolynom der Form $T^{p^n} - a$. Dann ist

$$K \subseteq K(\alpha^{p^{n-1}}) \subseteq K(\alpha^{p^{n-2}}) \subseteq \ldots \subseteq K(\alpha^p) \subseteq K(\alpha) = L$$

der gesuchte Körperturm. □

Satz 172 (Relativer separabler Abschluß)**.** *Sei L/K eine endliche Erweiterung. Dann gibt es eine eindeutige Zwischenerweiterung L_s mit den folgenden Eigenschaften.*

(i) *L_s/K ist separabel und jeder über K separable Zwischenkörper ist in L_s enthalten.*
(ii) *L/L_s ist rein inseparabel.*
(iii) $[L : K]_s = [L_s : K]$.
(iv) *$L_s = L^{p^n}K$ für hinreichend großes $n \in \mathbb{N}$.*

Beweis. Seien E, F Zwischenkörper, die über K separabel sind. Dann ist EF/F und F/K separabel, und demnach auch EF/K. Das Kompositum aller über K separabler Zwischenkörper ist demnach auch über K separabel. Dieses Kompositum ist der eindeutige maximale separable Zwischenkörper L_s.

Aus dem Beweis von Satz 168 folgt, daß ein nicht rein inseparables Element $\alpha \in L$ zu einer echten separablen Erweiterung $K(\alpha^{p^n})/K$ führt. Wir wenden dies auf L/L_s an. Da L_s in L keine nicht-trivialen separablen Teilerweiterungen mehr haben kann, diese wären auch über K separabel und so bereits in L_s enthalten, muß L/L_s rein inseparabel sein.

Es folgt nun

$$[L : K]_s = [L : L_s]_s \cdot [L_s : K]_s = 1 \cdot [L_s : K] = [L_s : K].$$

Sei $L = K(\alpha_1, \ldots, \alpha_r)$. Dann ist $M_n := L^{p^n}K = K(\alpha_1^{p^n}, \ldots, \alpha_r^{p^n})$. Das Argument am Ende des Beweises von Satz 168 zeigt, daß M_n/K für hinreichend großes n separabel ist. Außerdem ist L/M_n ersichtlich rein inseparabel. Daher gilt $M_n = L_s$ für $n \gg 0$. □

Korollar 173. *Sei K ein Körper der Charakteristik $p > 0$. Dann ist jede endliche Erweiterung L/K mit $p \nmid [L : K]$ separabel.*

Beweis. Sei L_s der relative separable Abschluß. Dann ist $[L : L_s]$ nach Korollar 171 eine Potenz von p. Als Teiler von $[L : K]$ muß dies $[L : L_s] = 1$ sein, also ist $L = L_s$ separabel über K. □

Definition 174. Der **Inseparabilitätsgrad** einer endlichen Erweiterung L/K ist

$$[L : K]_i = [L : L_s].$$

Korollar 175. *Sei L/K eine endliche Erweiterung. Es gilt*

$$[L : K] = [L : K]_s \cdot [L : K]_i$$

und $[L : K]_i$ ist eine Potenz der Charakteristik von K.

Beweis. Die Gleichung folgt sofort aus Satz 172 und dem Gradsatz. Der Rest folgt aus Korollar 171. □

Bemerkung 176. Einen Körper, der keine nicht-trivialen separablen algebraischen Erweiterungen mehr hat, nennt man **separabel algebraisch abgeschlossen**.

Die Konstruktion des relativen separablen Abschlußes funktioniert auch in unendlichen algebraischen Erweiterungen. Wenden wir dies auf einen algebraischen Abschluß $\overline{K}/K$ an, dann erhalten wir einen **separablen Abschluß**

$$K^{\mathrm{sep}}/K$$

von K. Dieser läßt sich beschreiben als

$$K^{\mathrm{sep}} = \{\alpha \in \overline{K}\ ;\ \alpha \text{ ist separabel über } K\}.$$

Ferner ist K^{sep} eine algebraische Erweiterung von K, die separabel algebraische abgeschlossen ist.

Die Steinitz'schen Sätze über den algebraischen Abschluß gelten analog in Bezug auf separable algebraische Erweiterungen.

Satz 177 (Steinitz für separable Erweiterungen)**.** *Sei K ein Körper.*

(1) K besitzt eine algebraische Erweiterung, die separabel algebraische abgeschlossen ist.
(2) Je zwei separable Abschlüsse von K sind K-isomorph.
(3) Sei K^{sep} ein separabler Abschluß von K und L/K eine separable Erweiterung. Dann gibt es eine K-Einbettung $L \to K^{\mathrm{sep}}$.

Übungsaufgaben zu §9

Übungsaufgabe 9.1. Sei K ein Körper und $K(X)$ der rationale Funktionenkörper. Zeigen Sie, daß die Quotientenregel eine Derivation auf $K(X)$ definiert:

$$\left(\frac{g}{h}\right)' := \frac{g'h - gh'}{h^2}.$$

Übungsaufgabe 9.2. Sei K eine Körper der Charakteristik $p > 0$, und sei $L = K(\alpha)$ eine endliche Erweiterung von K. Zeigen Sie, daß L/K genau dann separabel ist, wenn $L = K(\alpha^p)$ gilt.

Übungsaufgabe 9.3. Sei L/K eine endliche Erweiterung. Zeigen Sie, daß K genau dann perfekt ist, wenn L perfekt ist.

Übungsaufgabe 9.4. Sei F ein unendlicher Körper der Charakteristik $p > 0$. Sei $F(X, Y)$ der Quotientenkörper des Polynomrings $F[X, Y]$ in zwei Variablen X und Y.

(1) Zeigen Sie, daß $L = F(X, Y)$ eine rein inseparable Erweiterung des Unterkörpers $K = F(X^p, Y^p)$ ist.
(2) Bestimmen Sie den Grad $[L : K]$ und zeigen Sie, daß es unendlich viele Zwischenkörper gibt.

Übungsaufgabe 9.5. (1) Sind rein inseparable Erweiterungen normal?
(2) Sei L/K eine endliche Körpererweiterung und L_s der relative separable Abschluß von K in L.
Zeigen Sie, daß L/K normal ist genau dann, wenn L_s/K normal ist.

Teil 2. Galoistheorie

10. Irreduzibilitätskriterien

10.1. Diskrete Bewertungsringe. Das Konzept der Nullstellen- und Polordnung wird durch den Begriff der diskreten Bewertung abstrahiert.

Definition 178. Eine **diskrete Bewertung** eines Körpers K ist ein surjektiver Gruppenhomomorphsimus

$$v : K^\times \twoheadrightarrow \mathbb{Z},$$

so daß für alle $x, y \in K^\times$ mit $x + y \neq 0$ gilt

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

Diese Abschätzung nennen wir **(nichtarchimedische) Dreiecksungleichung**.

Elemente $\pi \in K^\times$ mit $v(\pi) = 1$ heißen **uniformisierende Elemente** von v.

Die folgenden Beispiele sind für uns die wichtigsten.

Beispiel 179. (1) Sei p eine Primzahl $\mathbb{Z}$. Wir definieren die p-adische Bewertung auf $\mathbb{Q}$ durch

$$v_p : \mathbb{Q}^\times \to \mathbb{Z}$$
$$v_p(p^n \frac{a}{b}) = n \text{ wenn } p \nmid ab.$$

Diese p-adische Bewertung zählt die Faktoren p in einer rationalen Zahl. Sie ist wohldefiniert und ein Homomorphismus aufgrund der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$. Die nötige Abschätzung gilt, weil die Summe mindestens durch die Primpotenz teilbar ist, durch die beide Summanden teilbar sind.

Es gilt für $n \in \mathbb{N}_{>0}$

$$n = \prod_p p^{v_p(n)}.$$

(2) Hier ist die abstrakte Variante. Sei R ein Ring mit eindeutiger Primfaktorzerlegung, also etwa ein Hauptidealring wie $\mathbb{Z}$ oder $F[T]$ für einen Körper F. Sei $\pi \in R$ ein Primelement und $K = \mathrm{Quot}(R)$. Dann gibt es für jedes $x \in K^\times$ eindeutig

$$x = \pi^n \frac{y}{z}$$

mit $n \in \mathbb{Z}$ und $y, z \in R$, wobei π kein Teiler von y und z ist. Die π-(adische) Bewertung auf K ist gegeben durch

$$v_\pi : K^\times \to \mathbb{Z}$$
$$v_\pi(\pi^n \frac{y}{z}) = n \text{ wenn } \pi \nmid yz.$$

Wie im Spezialfall $R = \mathbb{Z}$ und $\pi = p$ folgt alles sofort: wohldefiniert, Gruppenhomomorphismus, Abschätzung der Teilbarkeitsordnung.

(3) Das abstrakte Beispiel leifert konkret für $R = K[T]$ und $\pi = T$ die Bewertung

$$\mathrm{ord}_0 : K(T)^\times \to \mathbb{Z}$$

welches jeder rationalen Funktion die Nullstellenordnung in $T = 0$ zuordnet.

Lemma 180. *Sei v eine diskrete Bewertung auf dem Körper K. Dann gilt für alle $x \in K^\times$:*

(1) $v(-x) = v(x)$, *insbesondere* $v(-1) = 0$.

(2) $v(1/x) = -v(x)$.

Beweis. Es gilt $2v(-1) = v((-1)^2) = v(1) = 0$ in $\mathbb{Z}$, also $v(-1) = 0$. Der Rest ist noch trivialer. □

Proposition 181 (Nicht-archimedische Dreiecksungleichung)**.** *Sei v eine diskrete Bewertung auf dem Körper K. Dann gilt für $x, y, x+y \in K^\times$, wenn*

$$v(x) \neq v(y),$$

genauer

$$v(x+y) = \min\{v(x), v(y)\}.$$

Beweis. Wir zeigen, daß für $a, b, c \in K^\times$ mit $a + b + c = 0$ das Minimum von

$$\{v(a), v(b), v(c)\}$$

mindestens doppelt angenommen wird. Daraus folgt mit $a = x$, $b = y$ und $c = -(x+y)$ die Behauptung.

Angenommen, das Minimum wird nur einmal angenommen. Dann gilt oBdA

$$v(a) < v(b), v(c)$$

und dann ist

$$v(a) = v(-a) = v(b+c) \geq \min\{v(b), v(c)\} > v(a)$$

ein Widerspruch. □

Bemerkung 182. Sei v eine diskrete Bewertung auf dem Körper K. Für eine relle Zahl $\rho > 1$ wird durch

$$|x|_v := \rho^{-v(x)}$$

auf K eine Norm definiert, wenn man auch noch $|0|_v = 0$ setzt. Die nicht-archimedische Dreiecksungleichung wird zur Dreiecksungleichung

$$|x+y|_v \leq \max\{|x|_v, |y|_v\} \leq |x|_v + |y|_v$$

für $|\ |_v$. Wie üblich definiert

$$d_v(x, y) = |x - y|_v$$

dann eine Metrik auf K, die v-adische Metrik.

Im Beispiel der p-adischen diskreten Bewertung v_p auf $\mathbb{Q}$ bekommt man eine Norm, in der eine Zahl dann klein ist, wenn sie oft durch p teilbar ist.

Proposition 183. *Sei v eine diskrete Bewertung auf dem Körper K. Dann gilt:*

(1) *Die Menge*

$$R = \{x \in K^\times \ ;\ v(x) \geq 0\} \cup \{0\}$$

ist ein Unterring von K mit $K = \mathrm{Quot}(R)$, genannt der ***Bewertungsring*** *von v.*

(2) *Die Einheitengruppe von R ist*

$$R^\times = \{x \in K^\times \ ;\ v(x) = 0\}.$$

(3) *Der Ring R ist ein Hauptidealring mit einem bis auf Einheiten eindeutigen Primelement. Die Primelemente sind genau die uniformisierenden von v.*

(4) *Der Ring R hat ein eindeutiges maximales Ideal*

$$\mathfrak{m} = \{x \in K^\times \ ;\ v(x) > 0\} \cup \{0\},$$

und dieses wird von π erzeugt, wenn π uniformisierendes Element ist.

(5) *Der Faktorring $k = R/\mathfrak{m}$ ist ein Körper, genannt der* ***Restklassenkörper*** *von v.*

Beweis. (1) Nach der Dreiecksungleichung gilt mit $x, y \in R$ auch $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$, also $x + y \in R$ (wenn $x + y = 0$, so ist das trivial). Da $x, y \in R$ auch $xy \in R$ impliziert, und wegen $1^2 = 1$ notwendig $v(1) = 0$, ist R in der Tat ein Unterring.

Ein $x \in R$ ist eine Einheit, genau dann, wenn es ein $y \in R$ gibt mit $xy = 1$. Da

$$v(y) = v(1) - v(x) = -v(x)$$

geht das genau dann, wenn $v(x) = 0$ ist. Dann hat $y = 1/x \in K$ auch Bewertung 0 und ist in R. Dies zeigt (2).

Sei π eine Uniformisierende, also $v(\pi) = 1$. Dann setzen wir für $x \in K^\times$

$$y = x/\pi^{v(x)}$$

finden $v(y) = v(x) - v(x) \cdot v(\pi) = 0$. Demnach ist $y \in R^\times$ und

$$x = \pi^n y.$$

Es folgt, daß K der Quotientenkörper von R ist. Damit ist nun (1) gezeigt.

(3) Sei $I \subseteq R$ ein Ideal. Wir setzen

$$n = v(I) = \min\{m \ ; \ \text{ es gibt } x \in I \text{ mit } v(x) = m\}.$$

Das Minimum existiert, denn es handelt sich um das Minimum einer Teimenge von $\mathbb{N}$. Außerdem wird das Minimum angenommen. Sei $x \in I$ ein solches Element mit $v(x) = n$. Dann ist für jedes $y \in I$ mit $z = y/x$

$$v(z) = v(y) - v(x) \geq 0,$$

also $z \in R$ und

$$y = xz \in (x).$$

Wir schließen $I = (x)$ und R ist Hauptidealring.

Sei π eine Uniformisierende von v. Jede Nichteinheit $x \in R$ hat $v(x) > 0$ und wird daher durch π geteilt. Damit ist π das einzige mögliche Primelement (bis auf Einheit). In der Tat ist π irreduzibel, da $x, y \in R$ mit $xy = \pi$ erzwingt

$$1 = v(\pi) = v(x) + v(y),$$

und $v(x), v(y)$ sind 0 und 1 in einer Reihenfolge. Nach (2) ist somit ein Faktor eine Einheit.

(4) Man sieht sofort wie in (3), daß

$$\mathfrak{m} = (\pi).$$

Da $R \setminus \mathfrak{m} = R^\times$ nur aus Einheiten besteht und ein echtes Ideal keine Einheiten enthalten darf, ist jedes Ideal in $\mathfrak{m}$ enthalten. Damit ist $\mathfrak{m}$ das eindeutige maximale Ideal von R.

(5) Der Faktorring $k = R/\mathfrak{m}$ ist ein Körper, weil $\mathfrak{m}$ maximal ist. $\square$

Beispiel 184. (1) Der Potenzreihenring $K[[T]]$ über einem Körper K ist ein Hauptidealring mit genau einem Primelement T (bis auf Multiplikation mit einer Einheit. Die T-Bewertung auf $K((T)) := \mathrm{Quot}(K[[T]])$ wird gegeben durch

$$\begin{aligned} v : K((T))^\times &\to \mathbb{Z} \\ v(\sum_{i \geq 0} a_i T^i) &\mapsto \min\{i \ ; \ a_i \neq 0\} \end{aligned}$$

Der zugehörige Bewertungsring ist $K[[T]]$, das maximale Ideal besteht aus den Potenzreihen mit konstantem Element 0 und der Restklassen Körper ist als Quotient

$$\begin{aligned} K[[T]] &\to K \\ f &\mapsto f(0), \end{aligned}$$

die einzige Auswertung von T in K, die sinnvoll ist.

Insbesondere folgt aus diesen Überlegungen, daß

$$K((T)) = \{f = \sum_{i \geq n} a_i T^i \ ; \ n \in \mathbb{Z}, a_i \in K\} = \bigcup_{n \geq 0} T^{-n} K[[T]]$$

gilt. Der Quotientenkörper des formalen Potenzreihenrings ist somit der formale Laurentreihenring (mit endlicher Polordnung).

(2) Wir betrachten die p-adische Bewertung. Der Bewertungsring $\mathbb{Z}_{(p)}$ besteht aus allen rationalen Zahlen, deren (reduzierter) Nenner nicht durch p teilbar ist. Der Restklassenkörper ist gegeben durch

$$\mathbb{Z} \to \mathbb{F}_p$$

was sich aufgrund der universellen Eigenschaft der Lokalisierung (am multiplikativen System aller nicht durch p teilbaren natürlichen Zahlen) auf den Bewertungsring $\mathbb{Z}_{(p)}$ ausdehnt. Da das maxmiale Ideal eindeutig ist, muß dies die Quotientenabbildung zum Restklassenkörper sein.

Eine diskrete Bewertung führt zu einer Bewertung auf dem rationalen Funktionenkörper. Sei v eine Bewertung auf dem Körper K. Für ein $0 \neq f = \sum_{i=0}^{N} a_i X^i \in K[X]$ setzen wir

$$v(f) = \min\{v(a_i)\ ;\ a_i \neq 0\}.$$

Lemma 185 (Gauß-Lemma)**.** *Für alle $f, g \in K[X]$ verschieden von 0 gilt*

$$v(fg) = v(f) + v(g).$$

Beweis. Sei $f = \sum_{i=0}^{n} b_i X^i$ und $g = \sum_{i=0}^{m} c_i X^i$, und $fg = \sum_{i=0}^{n+m} a_i X^i$. Es gilt

$$\begin{aligned} v(a_l) = v(\sum_{i+j=l} b_i c_j) &\geq \min\{v(b_i c_j)\ ;\ i+j=l \text{ und } b_i c_j \neq 0\} \\ &= \min\{v(b_i) + v(c_j)\ ;\ i+j=l \text{ und } b_i c_j \neq 0\} \\ &\geq \min\{v(b_i)\ ;\ b_i \neq 0\} + \min\{v(c_j)\ ;\ c_j \neq 0\} = v(f) + v(g). \end{aligned}$$

Also gilt auch, in dem wir das Minimum für $0 \leq l \leq n+m$ über die linke Seite dieser Ungleichungen nehmen,

$$v(fg) \geq v(f) + v(g).$$

Es bleibt zu zeigen, daß in dieser Ungleichung Gleichheit besteht. Wir setzen

$$r = \min\{i\ ;\ v(b_i) = v(f)\}$$

und

$$s = \min\{i\ ;\ v(c_i) = v(g)\}$$

Dann berechnen wir den Koeffizienten von X^{r+s} in f als

$$a_{r+s} = \sum_{i+j=r+s} b_i c_j = b_r c_s + \sum_{i+j=r+s, i\neq r} b_i c_j$$

Für $i + j = r + s$ aber $i < r$ oder $j < s$ (das sind alle außer $(i,j) = (r,s)$) folgt

$$v(b_i c_j) = v(b_i) + v(c_j) > v(f) + v(g)$$

denn ein Index ist kleiner als r bzw. s und so gewinnen wir 1. Weil $v(b_r c_s) = v(f) + v(g)$ folgt mit der nichtarchimedischen Dreiecksungleichung aus Proposition 181 per Induktion

$$v(a_{r+s}) = v(b_r c_s) = v(f) + v(g).$$

Dies beweist die Behauptung. □

Definition 186. Die **Gauß-Bewertung** zu einer diskreten Bewertung v auf dem Körper K ist die diskrete Bewertung

$$v : K(X)^\times \to \mathbb{Z}$$

welche auf $f = g/h$ mit Polynomen $g, h \in K[X]$ durch

$$v(f) = v(g) - v(h)$$

definiert wird.

Beweis. Wir haben zu zeigen, daß v wohldefiniert und eine Bewertung ist. Wenn

$$\frac{g}{h} = f = \frac{a}{b}$$

dann gilt $gb = ha$ und nach Lemma 185

$$v(g) + v(b) = v(h) + v(a).$$

Dann ist aber

$$v(g) - v(h) = v(a) - v(b)$$

und $v(f)$ ist wohldefiniert.

Weiter ist v ein surjektiver Gruppenhomomorphismus $K(X)^\times \to \mathbb{Z}$, denn

$$v(\frac{g}{h} \cdot \frac{a}{b}) = v(\frac{ga}{hb}) = v(ga) - v(hb) = v(g) - v(h) + v(a) - v(b) = v(\frac{g}{h}) + v(\frac{a}{b}).$$

Die Dreiecksungleichung folgt offensichtlich für Polynome direkt aus der Definition und der Dreicksungleichung für v auf K. Im allgemeinen Fall führt man die Dreiecksungleichung durch Multipliktion mit dem Produkt der Nenner auf den Polynomfall zurück. □

10.2. **Das Eisensteinkriterium.** Um mehr Beispiele konstruieren zu können, benötigen wir ein Kriterium, mit dem sich ein Polynom als irreduzibel erkennen läßt. Das Eisensteinkriterium ist eines davon.

Satz 187. *Sei R der Bewertungsring einer diskreten Bewertung v auf dem Körper K. Sei $f \in R[T]$ ein Polynom, das sich in $R[T]$ nicht als Produkt nichtkonstanter Polynome schreiben läßt. Dann ist f auch in $K[T]$ irreduzibel.*

Beweis. Sei in $K[T]$ eine Zerlegung

$$f = \sum_{i=0}^{N} a_i T^i = gh$$

mit $g, h \in K[T]$. Dann gilt nach dem Gauß-Lemma, Lemma 185

$$0 \leq v(f) = v(g) + v(h).$$

Sei π eine Uniformisierende für die Bewertung v. Die Polynome

$$G = \pi^{-v(g)} g \quad \text{ und } \quad H = \pi^{-v(h)} h$$

sind per Definition der Gauß-Bewertung aus $R[T]$. Es gilt aber auch die Zerlegung in $R[T]$

$$f = \pi^{v(f)} GH.$$

Da f in $R[T]$ irreduzibel ist, muß G oder H konstant sein. Damit ist auch g oder h konstant und f irreduzibel in $K[T]$. □

Satz 188 (Eisensteinkriterium)**.** *Sei R der Bewertungsring einer diskreten Bewertung v auf dem Körper K. Sei $f = \sum_{i=0}^{n} a_i T^i \in K[T]$ ein Polynom mit*

$$v(a_i) = \begin{cases} 0 & i = n, \\ > 0 & 0 < i < n \text{ sofern } a_i \neq 0, \\ 1 & i = 0. \end{cases}$$

Dann ist f irreduzibel.

Beweis. Nach Voraussetzung ist $f \in R[T]$. Nach Satz 187 reicht es aus zu zeigen, daß f in $R[T]$ irreduzibel ist. Nehmen wir an, daß

$$f = gh$$

mit $g, h \in R[T]$. Die Quotientenabbildung $R \to k$ (bezeichnet mit $a \mapsto \bar{a}$) auf den Restklassenkörper k der Bewertung v führt auf Koeffizienten angewandt zu einem Ringhomomorphismus von Polynomeringen

$$R[T] \twoheadrightarrow k[T],$$

den wir mit $F \mapsto \bar{F}$ bezeichnen. Es gilt nach Voraussetzung

$$\bar{f} = \bar{a}_n T^n = \bar{g}\bar{h}.$$

Da in $k[T]$ eindeutige Primfaktorzerlegung besteht, folgt mit $d = \deg(g)$ und $e = \deg(h)$ und gewissen $\bar{a}, \bar{b} \in k^\times$

$$\bar{g} = \bar{a}T^d \quad \text{und} \quad \bar{h} = \bar{b}T^e.$$

Man beachte, daß in der offensichtlichen Abschätzung $\deg(\bar{g}) \leq \deg(g)$ (bzw. $\deg(\bar{h}) \leq \deg(h)$) Gleichheit gelten muß (der Grad kann nicht kleiner werden), da

$$\deg(\bar{g}) + \deg(\bar{h}) = \deg(\bar{f}) = \deg(f) = \deg(g) + \deg(h).$$

Insbesondere folgt, daß die konstanten Terme $g(0)$, $h(0)$ positive Bewertung haben. Damit gilt

$$v(a_0) = v(g(0)h(0)) = v(g(0)) + v(h(0)) \geq 2$$

im Widerspruch zur Annahme. □

Beispiel 189. (1) Das Polynom aus $\mathbb{Q}[T]$

$$T^{10} + 9T^7 + 3T^2 + 18T + 3$$

ist irreduzibel. Das Eisensteinkriterium funktioniert für die Primzahl 3, genauer in unserem Aufbau für die p-adische Bewertung zu $p = 3$.

(2) Sei F ein Körper und $K = F((X))$. Dann ist für alle $n > 0$

$$T^n - X$$

irreduzibel in $K[T]$. Hier funktioniert das Eisensteinkriterium für die Bewertung auf dem Potenzreihenring, die durch die Nullstellenordnung gegeben ist.

Korollar 190. *Sei $f \in \mathbb{Z}[T]$ ein Polynom $f = \sum_{i=0}^n a_i T^i$. Sei p eine Primzahl, so daß $p \nmid a_n$, $p \mid a_i$ für alle $i < N$ aber $p^2 \nmid a_0$. Dann ist f irreduzibel in $\mathbb{Q}[T]$.*

Beweis. Das folgt aus dem Eisensteinkriterium für die p-adische Bewertung von $\mathbb{Q}$. □

Es gibt noch die folgende Trickkiste zu beachten.

Bemerkung 191. (1) Skalierungstrick:

Zu einem Polynom $f = \sum_{i=0}^d a_i T^i \in K[T]$ vom Grad $d = \deg(f)$ und $0 \neq \lambda \in K$ kann man das Polynom

$$F = \lambda^d f(\lambda^{-1}T) = \sum_{i=0}^d \lambda^{d-i} a_i T^i$$

betrachten. Dann gilt offensichtlich in $K[T]$

$$f \text{ irreduzibel} \iff F \text{ irreduzibel}.$$

Der Koeffizient von T^i in F ist $\lambda^{d-i}a_i$. Wenn K eine diskrete Bewertung trägt mit Bewertungsring R, dann kann durch geschickte Wahl von λ erzwungen werden, daß $F \in R[T]$. Jetzt kann man das Eisensteinkriterium anzuwenden versuchen.

(2) Inversionstrick: Zu einem Polynom $f = \sum_{i=0}^d a_i T^i \in K[T]$ vom Grad $d = \deg(f)$ kann man das Polynom

$$F = T^d f(1/T) = \sum_{i=0}^d a_{d-i} T^i$$

betrachten. Dann gilt offensichtlich in $K[T]$
$$f \text{ irreduzibel } \iff F \text{ irreduzibel.}$$
Hier spiegeln sich die Koeffizienten am mittleren Grad.

(3) Translationstrick: Zu einem Polynom $f \in K[T]$ und $a \in K$ kann man das Polynom
$$F = f(T+a) \in K[T]$$
betrachten. Dann gilt offensichtlich in $K[T]$
$$f \text{ irreduzibel } \iff F \text{ irreduzibel.}$$

Beispiel 192. Als Standardbespiel für den Spiegelungstrick hat sich das Kreisteilungspolynom zur Primzahl p erwiesen. Das ist das Polynom
$$\Phi_p(T) = \frac{T^p - 1}{T-1} = T^{p-1} + T^{p-2} + \ldots + T^2 + T + 1 \in \mathbb{Z}[T],$$
nur daß in dieser Form das Eisensteinkriterium nicht anwendbar ist. Für die Translation um 1 gilt allerdings
$$\Phi_p(T+1) = \frac{(T+1)^p - 1}{T+1-1} \equiv \frac{T^p + 1^p - 1}{T} = T^{p-1} \mod p$$
und der Konstante Koeffizient ist
$$\Phi_p(T+1)|_{T=0} = \Phi_p(1) = p \notin p^2\mathbb{Z}.$$
Damit zeigt das Eisensteinkriterium für die p-adische Bewertung, daß $\Phi_p(T+1)$ und damit auch $\Phi_p(T)$ irreduzibel ist.

Bemerkung 193. Nicht jedes irreduzible Polynom kann durch das Eisensteinkriterium als irreduzibel erkannt werden, selbst nicht nach Translation oder anderen Tricks. Als Beispiel sei
$$f = T^4 - 8T^2 + 36$$
welches das Minimalpolynom des Erzeugers
$$\alpha = \sqrt{-1} + \sqrt{5}$$
für die Erweiterung $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$ von $\mathbb{Q}$ vom Grad 4 ist. Der Beweis, daß man mit Eisenstein nichts ausrichten kann, benötigt algebraische Zahlentheorie[5].

10.3. **Irreduzibilität eines homomorphen Bildes.** Wir beweisen nun eine genauere Version[6] von Satz 187, in der R ein beliebiger Hauptidealring ist.

Definition 194. Sei R ein Hauptidealring mit Quotientenkörper K und $0 \neq f \in K[T]$ ein Polynom. Wir definieren den **Inhalt** von f als
$$c(f) = \prod_{\pi} \pi^{v_\pi(f)} \in K^\times.$$
Das Produkt erstreckt sich über Vertreter π aller Primelemente von R bis auf Multiplikation mit einer Einheit von R. Dabei ist $v_\pi(-)$ die π-Bewertung, hier $v_\pi(f)$ also die kleinste π-Potenz, die in allen Koeffizienten aufgeht. Der Inhalt $c(f)$ hängt also implizit von der Wahl der Primelemente π ab. Die Wahl beinflußt $c(f)$ nur durch Multiplikation mit einer Einheit.

Bemerkung 195. Wenn $f \in R[T]$ ein Polynom ist, dann sieht man sofort
$$c(f) = \text{ggT der Koeffizienten von } f$$
und ist als solches wohldefiniert als Ideal von R.

[5] Das Eisensteinkriterium führt zu total verzweigten Erweiterungen. Die gegebene Erweiterung hat $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ als Galoisgruppe und kann somit nur bei $p = 2$ total verzweigt sein. Dort sorgt die bei 2 unverzweigte Zwischenerweiterung $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ dafür, daß die Verzweigung nicht total ist.

[6] Die natürliche Voraussetzung, mit dem gleichen Beweis, verlangt, daß R ein faktorieller Ring ist, das ist ein Ring mit eindeutiger Primfaktorzerlegung.

Lemma 196. *Sei R ein Hauptidealring mit Quotientenkörper K und $0 \neq f, g \in K[T]$ Polynome. Dann gilt*

$$c(fg) = c(f)c(g),$$

der Inhalt ist also multiplikativ.

Beweis. In beiden Seiten vergleich man die Anzahl der Faktoren π für jede Sorte Primelement π. Da kommt $v_\pi(fg) = v_\pi(f) + v_\pi(g)$ im Wesentlichen nach dem Gauß-Lemma, Lemma 185, heraus. □

Satz 197. *Sei R ein Hauptidealring mit Quotientenkörper K. Sei $f \in R[T]$ ein Polynom, das sich in $R[T]$ nicht als Produkt nichtkonstanter Polynome schreiben läßt. Dann ist f auch in $K[T]$ irreduzibel.*

Beweis. Sei $f = gh$ mit $g, h \in K[T]$. Dann setzen wir

$$G = c(g)^{-1}g \quad \text{und} \quad H = c(h)^{-1}h$$

und finden $G, H \in R[T]$ per Definition des Inhalts. Nach Lemma 196 gilt dann die Zerlegung

$$f = c(f)GH$$

mit Faktoren aus $R[T]$. Somit muß einer der Faktoren G, H konstant sein, und f ist irreduzibel. □

Lemma 198. *Sei $\varphi : A \to B$ ein Homomorphismus von Integritätsringen und sei $f \in A[T]$, so daß $\varphi(f) \in B[T]$ den gleichen Grad wie f hat.*

Sei in jeder Faktorisierung von $\varphi(f)$ in $B[T]$ ein Faktor konstant. Dann gilt dies auch für $A[T]$.

Beweis. Aus $f = gh$ mit $gh \in A[T]$ folgt $\varphi(f) = \varphi(g)\varphi(h)$ in $B[T]$ und einer der Faktoren $\varphi(g)$ oder $\varphi(h)$ muß konstant sein. Weil

$$\begin{aligned} \deg(f) &= \deg(\varphi(f)) = \deg(\varphi(g)) + \deg(\varphi(h)) \\ &\leq \deg(g) + \deg(h) = \deg(f) = \deg(\varphi(g)) + \deg(\varphi(h)) \end{aligned}$$

geht der Grad von g und h durch φ nicht runter. Also ist auch g oder h konstant. □

Korollar 199. *Sei R ein Hauptidealring mit Quotientenkörper K, und sei $\varphi : R \to A$ ein Homomorphismus zu einem Integritätsring A. Sei $0 \neq f \in R[T]$ ein Polynom, so daß*

(i) $\deg(f) = \deg(\varphi(f))$, *und*

(ii) in jeder Faktorisierung von $\varphi(f)$ in $A[T]$ ist eine Faktor konstant.

Dann ist f irreduzibel in $K[T]$.

Beweis. Nach Lemma 198 hat auch jede Faktorisierung von f in $R[T]$ einen konstanten Faktor. Nach Satz 197 ist damit f in $K[T]$ irreduzibel. □

Beispiel 200. Wir betrachten $R = \mathbb{Z}$ mit $K = \mathbb{Q}$ und $\varphi : \mathbb{Z} \to \mathbb{F}_p$ die Projektion. Das Polynom

$$f = T^p - T - 1 \in \mathbb{Z}[T]$$

reduziert sich modulo p, also durch Abbilden mit φ, zum Polynom $\bar{f} = T^p - T - 1 \in \mathbb{F}_p[T]$. Dieses ist irreduzibel. Denn sei α eine Nullstelle in einer endlichen Erweiterung $\mathbb{F}_p(\alpha)$, dann gilt

$$\mathrm{Frob}(\alpha) = \alpha^p = \alpha + 1.$$

Somit gilt

$$\mathrm{Frob}^r(\alpha) = \alpha + r$$

und Frob hat auf $\mathbb{F}_p(\alpha)$ die Ordnung p. Dies ist, wie wir bereits wissen gleich $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, und daher ist $\bar{f} \in \mathbb{F}_p[T]$ irreduzibel. Nach Korollar 199 ist dann auch f irreduzibel in $\mathbb{Q}[T]$.

Bemerkung 201. Das Eisensteinkriterium und das Kriterium mittels eines homomorphen Bildes haben ähnliche Struktur. In beiden Fällen benutzt man einen Homomorphsimus $\varphi : R \to k$ auf einem geeigneten Teilring $R \subseteq K$. Zunächst muß von Beginn an $f \in R[T]$ Koeffizienten im Teilring R haben und man betrachtet $\bar{f} = \varphi(f)$. Dann aber schließen beide Kriterien aus diametral entgegengesetzten Voraussetzungen auf irreduzibilität von f :

- Beim Kriterium in Korollar 199 muß $\bar{f}$ selbst irreduzibel sein.
- Beim Eisensteinkriterium aus Satz 188 muß $\bar{f}$ vollständig in identische Linearfaktoren zerlegt sein.

Die beiden Kriterien ergänzen sich somit.

Übungsaufgaben zu §10

Übungsaufgabe 10.1. Zeigen Sie, daß die Abbildung

$$v : K(X)^\times \to \mathbb{Z}$$
$$v(\frac{f}{g}) \mapsto \deg(g) - \deg(f)$$

eine diskrete Bewertung auf $K(X)$ definiert. Diese Bewertung wird die Gradbewertung genannt.

Beschreiben Sie die Bewertung, welche aus der Gradbewertung durch Vorschalten des K-Automorphismus von $K(X)$, der durch $X \mapsto X^{-1}$ festgelegt wird, entsteht.

Finden Sie einen Hauptidealring in K, so daß die Gradbewertung eine zu einem Primelement gehörige diskrete Bewertung ist.

Übungsaufgabe 10.2. Sei R der Bewertungsring einer diskreten Bewertung v auf dem Körper K. Zeigen Sie, daß die Sequenz von abelschen Gruppen

$$0 \to R^\times \xrightarrow{i} K^\times \xrightarrow{v} \mathbb{Z} \to 0$$

mit der Inklusion i und der Bewertung v exakt ist.

Überlegen Sie sich, wie sie die Bewertung v definieren können, wenn sie nur den diskrete Bewertungsring als Unterring $R \subseteq K$ gegeben haben.

Übungsaufgabe 10.3. Sei R der Bewertungsring einer diskreten Bewertung v auf dem Körper K. Zeigen Sie, daß für jedes $x \in K^\times$ gilt:

$$x \in R \quad \text{oder} \quad 1/x \in R.$$

Übungsaufgabe 10.4. (a) Zeigen Sie, daß die folgenden Polynome in $\mathbb{Q}[X]$ irreduzibel sind:
(1) $3X^5 + 14X^3 - 21X^2 + 49X - 7$,
(2) $X^{12} + 27X + 1002$,
(3) $X^4 + 1$.

(b) Sei $p \in \mathbb{Z}$ eine Primzahl $f = \sum_{i=0}^{2n+1} a_i X^i \in \mathbb{Z}[X]$ ein Polynom vom Grad $2n+1$. Angenommen p teilt nicht a_{2n+1} aber $p|a_i$ für alle $i \leq 2n$ und sogar $p^2|a_i$ für alle $i \leq n$ wobei p^3 wiederum nicht a_0 teilt. Man zeige, daß ein solches f irreduzibel in $\mathbb{Q}[X]$ ist.

11. Galoiserweiterungen

11.1. **Galoissch.** Unter den endlichen Körpererweiterung spielen die galoisschen Körpererweiterungen eine besondere Rolle.

Theorem 202. *Sei L/K eine Körpererweiterung. Dann sind äquivalent:*
(a) Es gibt eine endliche Gruppe $G \subseteq \mathrm{Aut}_K(L)$ mit $K = L^G$.
(b) $\# \mathrm{Aut}_K(L) = [L : K]$ und dies ist endlich.
(c) $[L : K]$ ist endlich und L/K ist separabel und normal.
(d) $L = K(\alpha)$ für ein algebraisches Element $\alpha \in L$ mit separablem Minimalpolynom $P_{\alpha/K}$, das in L vollständig in Linearfaktoren zerfällt.

Beweis. (a) $\implies$ (d): Zu $\alpha \in L$ betrachten wir die Menge der G-konjugierten Elemente

$$M = \{g(\alpha)\ ;\ g \in G\}.$$

Dies ist eine transitive G-Menge. Für jedes $g \in G$ ist die Einschränkung von $g : L \to L$ auf M eine Permutation von M. Wir betrachten nun

$$f = \prod_{\beta \in M} (T - \beta).$$

Für jedes $g \in G$ gilt nun

$${}^g f = \prod_{\beta \in M} {}^g(T - \beta) = \prod_{\beta \in M} (T - g(\beta)) = \prod_{\beta \in M} (T - \beta) = f.$$

Damit hat f Koeffizienten im Fixkörper $L^G = K$, also $f \in K[T]$.

Wegen $\alpha \in M$ ist $f(\alpha) = 0$, und es gilt

$$P_{\alpha/K} \mid f.$$

Da f separabel ist und über L vollständig in Linearfaktoren zerfällt, gilt dasselbe auch für $P_{\alpha/K}$. Da dies für alle $\alpha \in L$ gilt, ist L/K eine algebraische Erweiterung, in der jedes Element separabel ist und alle Minimalpolynome $P_{\alpha/K}$ über L vollständig in Linearfaktoren zerfallen. Außerdem gilt für alle $\alpha \in L$

$$[K(\alpha) : K] = \deg(P_{\alpha/K}) \leq \#M \leq \#G.$$

Damit haben wir fast (c) gezeigt. Es fehlt $[L : K]$ endlich. Dazu brauchen wir den Satz vom primitiven Element, mit dem wir auch (d) zeigen. Angenommen L/K wäre nicht endlich erzeugt (und damit endlich), dann gibt es durch sukzessives Adjungieren von Erzeugern einen Körperturm

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots$$

von Zwischenkörpern, so daß $[L_i : K]$ endlich ist und mit $i \to \infty$ gegen unendlich strebt. Da L_i/K auch separabel ist, gibt es nach dem Satz vom primitiven Element, Theorem 161, Elemente $\alpha_i \in L_i$ mit $L_i = K(\alpha_i)$. Dann ist aber für alle i

$$\#G \geq [L_i : K]$$

beschränkt, ein Widerspruch. Wir wenden Theorem 161 nochmals, diesmal auf L/K, an und finden $L = K(\alpha)$ für ein geeignetes α. Damit ist (d) bewiesen.

(d) $\implies$ (c): In diesem Fall ist L der Zerfällungskörper eines separablen Polynoms, also L/K endlich, separabel und normal.

(c) $\implies$ (b): Sei $L \subseteq \Omega$ eine algebraisch abgeschlossene Erweiterung. Wir betrachten Ω als Erweiterung von K via $K \subseteq L \subseteq \Omega$. Da L/K normal ist, faktorisiert jeder K-Homomorphismus $L \to \Omega$ über $L \subseteq \Omega$:

$$\mathrm{Hom}_K(L, L) = \mathrm{Hom}_K(L, \Omega).$$

Und da jeder Körperhomomorphimus injektiv ist und L ein endlicher K-Vektorraum, so ist jeder K-Homomorphismus $L \to L$ schon ein Automorphismus:

$$\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L).$$

Damit gilt

$$\#\,\mathrm{Aut}_K(L) = \#\,\mathrm{Hom}_K(L, L) = \#\,\mathrm{Hom}_K(L, \Omega) = [L : K]_s$$

und dies ist gleich $[L : K]$, denn L/K ist separabel.

(b) $\implies$ (a): Nach Voraussetzung ist $G := \mathrm{Aut}_K(L)$ endlich, Wir erhalten einen Zwischenkörper von L/K durch:

$$M = L^G.$$

Offensichtlich ist $G \subseteq \mathrm{Aut}_M(L)$, so daß nach Korollar 72

$$[L : K] = \#\,\mathrm{Aut}_K(L) = \#G \leq \#\,\mathrm{Aut}_M(L) = \#\,\mathrm{Hom}_M(L, L) \leq [L : M].$$

Wir schließen

$$1 \leq [M : K] = \frac{[L : K]}{[L : M]} \leq 1,$$

also $[M : K] = 1$. Somit gilt $K = M = L^G$. □

Definition 203. (1) Eine endliche **galoissche** Körpererweiterung ist eine Körpererweiterung L/K, welche die äquivalenten Eigenschaften von Theorem 202 erfüllen. Man nennt eine galoissche Erweiterung auch einfach **Galoiserweiterung**.
(2) Die **Galoisgruppe** einer Galoiserweiterung L/K ist die Gruppe

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L).$$

Beispiel 204. (1) $\mathbb{C}/\mathbb{R}$ ist galoissch, den $\mathbb{R}$ ist der Fixkörper der komplexen Konjugation, welche eine Gruppe der Ordnung 2 erzeugt.
(2) Jede Erweiterung endlicher Körper ist normal und separabel, also galoissch.
(3) Sei K ein Körper von Charakteristik $\neq 2$, und sei L/K eine quadratische Erweiterung. Dann ist L/K galoissch, denn L/K ist normal nach Proposition 78 und separabel nach Korollar 173, da die Charakteristik kein Teiler von $2 = [L : K]$ ist. In der Tat ist $L = K(\sqrt{a})$ für ein $a \in K$ und $\mathrm{Gal}(L/K)$ die Gruppe von Ordnung 2, welche von der Involution definiert durch

$$\sqrt{a} \mapsto -\sqrt{a}$$

erzeugt wird.
(4) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht galoissch, da sie nicht normal ist.

Beispiel 205. Das folgende Beispiel enstammt einem Brief von J.-P. Serre als Antwort auf eine Frage von Abhyankar[7], war aber schon vorher bekannt[8].

Der 1-dimensionale projektive Raum $\mathbb{P}^1(\mathbb{F}_q)$ über dem Körper $\mathbb{F}_q$ ist die Menge der Geraden durch 0 im $\mathbb{F}_q$-Vektorraum $\mathbb{F}_q^2$. Dieser wird beschrieben durch

$$\mathbb{P}^1(\mathbb{F}_q) = (\mathbb{F}_q^2 \setminus \{0\})/\mathbb{F}_q^\times.$$

Die Restklasse der Gerade durch (u, v) wird mit $[u : v]$ bezeichnet. Die **projektiv lineare Gruppe** in Dimension 2 mit $\mathbb{F}_q$-Koeffizienten ist

$$\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\}$$

Dies ist eine endliche Gruppe der Ordnung

$$\#\,\mathrm{PGL}_2(\mathbb{F}_q) = \frac{\#\,\mathrm{GL}_2(\mathbb{F}_q)}{q-1} = (q-1)q(q+1),$$

die auf $\mathbb{P}^1(\mathbb{F}_q)$ wie folgt wirkt. Zu $[u : v] \in \mathbb{P}^1(\mathbb{F}_q)$ und $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ setzen wir

$$M.[u : v] = [au + bv : cu + dv].$$

Dies hängt nur vom Bild von M in $\mathrm{PGL}_2(\mathbb{F}_q)$ ab und definiert eine Operation, weil hier nur der Effekt die tautologische Operation

$$\mathrm{GL}_2(\mathbb{F}_q) \times \mathbb{F}_q^2 \to \mathbb{F}_q^2$$

durch Matrixmultiplikation (für später unten unorthodox als

$$M.(u, v) = (au + bv, cu + dv).$$

notiert) auf den Geraden durch 0 beschrieben wird.

[7] Appendix in: Abhyankar, Shreeram S., *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), no. 1, 68–133.

[8] Rivoire, Paul, *Fonctions rationnelles sur un corps fini*, Ann. Inst. Fourier, Grenoble **6** (1955–1956), 121–124.

Jetzt betrachten wir die Koordinate
$$T = \frac{u}{v}$$
als Variable, welche mit Werten in $\mathbb{F}_q \cup \{\infty\}$ die Punkte des $\mathbb{P}^1(\mathbb{F}_q)$ parametrisiert. Die Operation führt dann zu
$$M.T = \frac{au+bv}{cu+dv} = \frac{aT+b}{cT+d}.$$
Diesen gebrochen linearen Ausdruck nennt man eine **Möbiustransformation**. Es gilt $M.T = T$ genau dann, wenn $M = 1 \in \mathrm{PGL}_2(\mathbb{F}_q)$. Damit ist klar, daß wir eine endliche Untergruppe von Automorphismen
$$\begin{aligned} \mathrm{PGL}_2(\mathbb{F}_q) &\hookrightarrow \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(T)) \\ M &\mapsto (T \mapsto M.T) \end{aligned}$$
gefunden haben.

Wir setzen nun $L = \mathbb{F}_q(T)$ und K für den Fixkörper zur Gruppe $\mathrm{PGL}_2(\mathbb{F}_q)$ von Automorphismen. Damit ist L/K eine galoissche Erweiterung mit Galoisgruppe
$$\mathrm{Gal}(L/K) = \mathrm{PGL}_2(\mathbb{F}_q).$$

Nun wollen wir den Körper K konkret bestimmen, und L als Erweiterung von K beschreiben. Dazu betrachten wir (nach Dickson) die Polynome
$$A(u,v) = vu^q - uv^q = v^{q+1}(T^q - T)$$
und
$$\begin{aligned} B(u,v) &= \frac{vu^{q^2} - uv^{q^2}}{A(u,v)} = \frac{v^{q^2+1}(T^{q^2} - T)}{v^{q+1}(T^q - T)} = v^{q^2-q}\frac{(T^{q^2} - T^q) + (T^q - T)}{T^q - T} \\ &= v^{q^2-q} \cdot \big((T^q - T)^{q-1} + 1\big). \end{aligned}$$

Es gilt für $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$,
$$\begin{aligned} A(M.(u,v)) &= (cu+dv)(au+bv)^q - (au+bv)(cu+dv)^q \\ &= (cu+dv)(au^q+bv^q) - (au+bv)(cu^q+dv^q) = \det(M) \cdot A(u,v) \end{aligned}$$
und (verwende im Zähler die Rechnung für $A(u,v)$ und q^2 statt q)
$$B(M.(u,v)) = \frac{\det(M) \cdot (vu^{q^2} - uv^{q^2})}{\det(M) \cdot A(u,v)} = B(u,v).$$
Wir setzen
$$X = \frac{B(u,v)^{q+1}}{A(u,v)^{q^2-q}} = \frac{((T^q - T)^{q-1} + 1)^{q+1}}{(T^q - T)^{q^2-q}},$$
und finden, weil $\det(M) \in \mathbb{F}_q^\times$ und daher $\det(M)^q = \det(M)$,
$$M.X = \frac{B(M.(u,v))^{q+1}}{A(M.(u,v))^{q^2-q}} = \frac{B(u,v)^{q+1}}{\det(M)^{q^2-q} \cdot A(u,v)^{q^2-q}} = X.$$

Das Element X gehört somit zum Fixkörper K. Die Definition von X zeigt
$$\begin{aligned} 0 &= ((T^q - T)^{q-1} + 1)^{q+1} - X(T^q - T)^{q^2-q} \\ &= T^{(q-1)q(q+1)} + \ldots - XT^{(q-1)q^2} + \ldots + 1, \end{aligned}$$
so daß T Nullstelle eines Polynoms vom Grad $(q-1)q(q+1)$ über dem Unterkörper $\mathbb{F}_q(X) \subseteq K$ ist. Da T transzendent über $\mathbb{F}_q$ ist, muß auch X transzendent über $\mathbb{F}_q$ sein, Satz 133 zeigt, daß $\mathbb{F}_q(X)$ ein rationaler Funktionenkörper ist. Des weiteren haben wir den Körperturm
$$L = \mathbb{F}_q(T) \supseteq K = \mathbb{F}_q(T)^{\mathrm{PGL}_2(\mathbb{F}_q)} \supseteq \mathbb{F}_q(X),$$

und nach Theorem 202

$$(q-1)q(q+1) \geq [L:\mathbb{F}_q(X)] \geq [L:K] = \#\operatorname{Aut}_K(L) \geq \#\operatorname{PGL}_2(\mathbb{F}_q) = (q-1)q(q+1).$$

Es gilt hier somit Gleichheit und als Konsequenz des Gradsatzes

$$K = \mathbb{F}_q(X).$$

Damit ist

$$f(T) = ((T^q - T)^{q-1} + 1)^{q+1} - X(T^q - T)^{q^2-q} \in \mathbb{F}_q(X)[T]$$

irreduzibel, $L = \mathbb{F}_q(T)$ entsteht als Adjunktion der Nullstelle T zu $\mathbb{F}_q(X)$, und die Erweiterung $\mathbb{F}_q(T)/\mathbb{F}_q(X)$ ist galoissch mit Galoisgruppe

$$\operatorname{Gal}(\mathbb{F}_q(T)/\mathbb{F}_q(X)) = \operatorname{PGL}_2(\mathbb{F}_q).$$

Später, wenn wir den Hauptsatz der Galoistheorie beweisen haben, betrachten wir dieses Bespiel erneut.

11.2. **Die galoissche Hülle.**

Definition 206. (1) Eine **normale Hülle** einer endlichen Körpererweiterung L/K ist eine Erweiterung $\tilde{L}/L$, die
   - (i) normal über K ist, und
   - (ii) für jede Erweiterung M/L, die normal über K ist, eine L-Einbettung $\tilde{L} \to M$ erlaubt.

   Somit ist eine normale Hülle von L ein gewissem Sinne eine kleinste Erweiterung, die über K normal ist und L enthält.

(2) Eine **galoissche Hülle** einer endlichen separablen Körpererweiterung L/K ist eine Erweiterung $\tilde{L}/L$, die
   - (i) galoissch über K ist, und
   - (ii) für jede Erweiterung M/L, die galoissch über K ist, eine L-Einbettung $\tilde{L} \to M$ erlaubt.

   Somit ist eine galoissche Hülle von L ein gewissem Sinne eine kleinste Erweiterung, die über K galoissch ist und L enthält.

Proposition 207. *Jede endliche Erweiterung L/K besitzt eine normale Hülle. Diese ist eindeutig bis auf uneindeutigen L-Isomorphsimus.*

Beweis. Die Eindeutigkeit ist einfach: sind $\tilde{L}_i/L$ für $i = 1, 2$ normale Hüllen, dann gibt es zwei L-Einbettungen $\tilde{L}_1 \to \tilde{L}_2$ und umgekehrt $\tilde{L}_2 \to \tilde{L}_1$. Damit kann man wie im Beweis von Satz 81 die Grade $[\tilde{L}_i : K]$ wechselseitig gegeneinander abschätzen und zeigt so, daß diese Einbettungen Isomorphismen sind.

Sei $\tilde{L}/L$ die im Beweis von Satz 83 konsturierte normale Erweiterung: der Zerfällungskörper des Produkts $f = \prod_i P_{\alpha_i/K}$ der Minimalpolynome von Erzeugern $\alpha_1, \ldots, \alpha_s$ von L/K. Sei M/L eine weitere über K normale Erweiterung. Wir betten $\tilde{L}$ und M in einen algebraischen Abschluß $\overline{L}$ von L ein. Da $P_{\alpha_i/K}$ in M eine Nullstelle hat und M normal ist, sind alle Nullstellen von $P_{\alpha_i/K}$ und damit von f schon in M enthalten. Diese Nullstellen erzeugen aber $\tilde{L}$, woraus $\tilde{L} \subseteq M$ folgt. Dies ist die gesuchte L-Einbettung. Die Wahl der Einbettung wurde getroffen, als die L-Einbettungen nach $\overline{L}$ gewählt wurden. ∎

Korollar 208. *Sei L/K eine endliche separable Erweiterung.*

(1) Die normale Hülle $\tilde{L}/K$ ist eine Galoiserweiterung.
(2) Die galoissche Hülle existiert und ist eindeutig.
(3) Die normale Hülle ist eine Galoishülle.

Beweis. (1) Dies folgt sofort aus der Konstruktion in 207, denn als Zerfällungskörper der separablen Polynome $P_{\alpha_i/K}$ ist $\tilde{L}/K$ auch separabel. Die Erweiterung $\tilde{L}/K$ ist somit separabel und normal, daher galoissch.

(2) und (3) folgen dann aus den entsprechenden Eigenschaften der normalen Hülle. □

Beispiel 209. Die galoissche Hülle von $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$.

11.3. **Der Normalbasensatz.** In Anlehnung an die komplexe Konjugation definiert man konjugierte Elemente.

Definition 210. Sei L/K eine Galoiserweiterung. Die zu einem Element $\alpha \in L$ (über K) konjugierten Elemente sind die Elemente der Bahn von α

$$\{\sigma(\alpha)\ ;\ \sigma \in \mathrm{Gal}(L/K)\}$$

unter der tautologischen Galoiswirkung von $\mathrm{Gal}(L/K)$ auf L.

Galoissche Erweiterungen haben spezielle Basen.

Definition 211. Sei L/K eine endliche galoissche Körpererweiterung vom Grad n und $\sigma_1, \ldots, \sigma_n$ die Elemente der Galoisgruppe $\mathrm{Gal}(L/K)$. Eine K-Basis von L der Form

$$\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$$

für ein $\alpha \in L$ nennt man eine **Normalbasis** von L/K. Ein solches α nennt man ein **freies Element** (für die Erweiterung L/K).

Beispiel 212. Sei $L = K(\sqrt{a})$ eine quadratische Erweiterung eines Körpers K der Charakteristik $\neq 2$. Dann erzeugt $\sqrt{a}$ keine Normalbasis, denn die konjugierten sind

$$\sqrt{a}, -\sqrt{a}$$

somit keine Basis. Eine Normalbasis erzeugt hingegen $1 + \sqrt{a}$:

$$1 + \sqrt{a}, 1 - \sqrt{a}.$$

Theorem 213 (Normalbasensatz)**.** *Jede endliche Galoiserweiterung hat eine Normalbasis.*

Beweis. Da der Beweis unterschiedliche Methoden verlangt, je nachdem ob K endlich oder unendlich ist, trennen wir die Aussagen auf. Satz 214 behandelt unendliche Körper, während Satz 217 den Fall endlicher Körper erledigt, denn Galoiserweiterungen endlicher Körper haben stets zyklische Galoisgruppe, siehe Theorem 116. □

Satz 214. *Sei K ein unendlicher Körper. Jede Galoiserweiterung von K hat eine Normalbasis.*

Beweis. Sei L/K eine endliche galoissche Körpererweiterung vom Grad n und $\sigma_1, \ldots, \sigma_n$ die Elemente der Galoisgruppe $\mathrm{Gal}(L/K)$. Sei $\alpha_1, \ldots, \alpha_n$ eine K-Basis von L. Wir suchen $x = (x_1, \ldots, x_n) \in K^n$ so daß von $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$ die Konjugierten

$$\sigma_1(\alpha), \ldots, \sigma_n(\alpha) \tag{11.1}$$

eine Normalbasis bilden. Wir betrachten die Matrix

$$S(x) = (\sigma_i^{-1}\sigma_j(\alpha))_{1 \leq i,j \leq n} \in \mathrm{M}_n(L).$$

Wenn es $0 \neq a = (a_1, \ldots, a_n) \in K^n$ gibt, so daß

$$a_1\sigma_1(\alpha) + \ldots + a_n\sigma_n(\alpha) = 0,$$

also gerade (11.1) keine Normalbasis ist, dann folgt

$$S(x)a = 0,$$

denn auch die anderen Zeilen

$$a_1\sigma_i^{-1}\sigma_1(\alpha) + \ldots + a_n\sigma_i^{-1}\sigma_n(\alpha) = \sigma_i^{-1}\big(a_1\sigma_1(\alpha) + \ldots + a_n\sigma_n(\alpha)\big) = \sigma_i^{-1}(0) = 0$$

sind 0. Wir schließen, daß (11.1) eine Normalbasis ist, wenn
$$\det(S(x)) \neq 0.$$

Nun ersetzen wir die Elemente $x_i \in K$ durch Variablen X_i. Es entsteht eine Matrix
$$S(X_1, \ldots, X_n) = (\sum_k X_k \sigma_i^{-1}\sigma_j(\alpha_k)) \in \mathrm{M}_n(L[X_1, \ldots, X_n])$$
mit Einträgen im Polynomring, so daß die Auswertung in $x \in K^n$ (nur für K!)
$$S(x_1, \ldots, x_n) = S(x) \in \mathrm{M}_n(L)$$
die alte Matrix reproduziert. Die Determinante
$$D(X_1, \ldots, X_n) = \det(S(X_1, \ldots, X_n)) \in L[X_1, \ldots, X_n]$$
ist ein (homogenes) Polynom (vom Grad n) in den Variablen $X_1, \ldots, X_n$. Wenn wir ein $x \in K^n$ finden, so daß $D(x) \neq 0$, dann sind wir fertig, denn Determinante vertauscht mit Auswerten von Polynomen.

Als erstes müssen wir zeigen, daß $D(X_1, \ldots, X_n)$ nicht das Nullpolynom ist. Dazu behaupten wir, daß es ein $y = (y_1, \ldots, y_n) \in L^n$ gibt mit
$$S(y) = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$
und demnach $D(y) = 1 \neq 0$ (es macht gar nichts, daß wir hier Werte in L einsetzen). Nach Definition von $S(X_1, \ldots, X_n)$ ist dies äquivalent zu
$$\sum_{k=1}^n y_k \sigma_i^{-1}\sigma_j(\alpha_k) = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$
was wiederum äquivalent ist zu
$$\sum_{k=1}^n y_k \sigma_i(\alpha_k) = \begin{cases} 1 & \sigma_i = \mathrm{id}_L \\ 0 & \text{sonst.} \end{cases}$$
Dies folgt nun, wenn die Abbildung $L^n \to L^n$ gegeben durch die Matrix
$$M = (\sigma_i(\alpha_k))_{1 \leq i,k \leq n} \in \mathrm{M}_n(L)$$
invertierbar ist. Eine L-Linearkombination mit Koeffizienten λ_i der Zeilen von M liefert die Werte auf der Basis $\alpha_1, \ldots, \alpha_n$ der Abbildung
$$\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n : L \to L$$
Aus der L-linearen Unabhängigkeit der Charaktere $\sigma_i : L \to L$ folgt, daß die Zeilen von M linear unabhängig sind, ergo $\det(M) \neq 0$ und das gesuchte $y \in L^n$ ist garantiert. Folglich ist $D(X_1, \ldots, X_n)$ nicht das Nullpolynom.

Weil K unendlich ist, kann aber dann $D(X_1, \ldots, X_n)$ nach Satz 216 nicht auf ganz K^n verschwinden, und wir finden $x \in K^n$ mit $D(x) \neq 0$. Damit ist der Satz bewiesen. $\square$

Definition 215. Eine **Polynomfunktion** $K^n \to K$ ist die zu einem Polynom $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ definierte Auswertungsabbildung
$$f : K^n \to K$$
$$x = (x_1, \ldots, x_n) \mapsto f(x) = f(x_1, \ldots, x_n).$$
Die Menge aller Polynomfuntkionen bezeichnen wir mit $\mathcal{O}(K^n)$. Dies ist eine K-Algebra bezüglich punktweiser Additon, Multiplikation und Skalarmultiplikation.

Die Ringstruktur im Polynomring ist gerade so gemacht, daß die Zuordnung

$$K[X_1, \ldots, X_n] \to \mathcal{O}(K^n)$$
$$f \mapsto f = (x \mapsto f(x))$$

ein K-Algebrahomomorphismus ist.

Satz 216. *Sei K ein unendlicher Körper. Dann ist die Abbildung*

$$K[X_1, \ldots, X_n] \to \mathcal{O}(K^n)$$

injektiv. Es gilt genauer: wenn $M \subseteq K$ eine unendliche Teilmenge ist und $f \in K[X_1, \ldots, X_n]$ mit

$$f(m_1, \ldots, m_n) = 0$$

für alle $m_1, \ldots, m_n \in M$, dann ist schon $f = 0$.

Beweis. Wir beweisen dies per Induktion nach n. Für den Induktionsanfang im Fall $n = 0$ ist nichts zu tun. Das Polynom f ist hier konstant und nach Auswertung 0, also identisch 0.

Wir schreiben nun f als Polynom in der Variablen X_n als

$$f = a_d(X_1, \ldots, X_{n-1})X_n^d + \ldots + a_1(X_1, \ldots, X_{n-1})X_n + a_0(X_1, \ldots, X_{n-1}).$$

Sodann fixieren wir $m_1, \ldots, m_{n-1}$ und erhalten für jede solche Wahl ein Polynom

$$f_{m_1,\ldots,m_{n-1}}(X_n) = a_d(m_1, \ldots, m_{n-1})X_n^d + \ldots + a_1(m_1, \ldots, m_{n-1})X_n + a_0(m_1, \ldots, m_{n-1}) \in K[X_n]$$

mit Nullstellen in allen $X_n = m \in M$. Da ein Polynom nur endlich viele Nullstellen haben kann, muß $f(m_1, \ldots, m_{n-1}, X_n) = 0$ sein, was bedeutet, daß für $i = 0, \ldots, d$ die Polynome

$$a_i(X_1, \ldots, X_{n-1}) \in K[X_1, \ldots, X_{n-1}]$$

auf M^{n-1} verschwinden. Per Induktion folgt daher $a_i = 0$ für alle i und so $f = 0$. $\square$

Satz 217. *Sei L/K ein Galoiserweiterung mit einer zyklischen Galoisgruppe* $\mathrm{Gal}(L/K)$*. Dann hat L/K eine Normalbasis.*

Beweis. Sei σ ein Erzeuger der Galoisgruppe und $n = [L : K]$. Wir analysieren σ als K-linearen Endomorphismus des K-Vektorraums L. Zum einen ist $\sigma^n = \mathrm{id}_L$. Zum andern sind $\mathrm{id}_L, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ linear unabhängig. Daher ist

$$T^n - 1$$

das Minimalpolynom von σ. (Das ist das Minimalpolynom als K-Vektorraumendomorphismus und damit nicht notwendigerweise irreduzibel.)

Sei $T^n - 1 = \prod_{i=1}^s p_i(T)^{e_i}$ die Zerlegung von $T^n - 1$ in $K[T]$ in irreduzible Faktoren. Wir betrachten nun die Kernzerlegung von σ auf L. Zu jedem Primfaktor p_i gibt es einen direkten σ-stabilen Summanden V_i, mit

$$L = \bigoplus_{i=1}^s V_i$$

und auf

$$V_i = \ker\big(p_i(\sigma)^{m_i} : L \to L\big)$$

hat σ das Minimalpolynom $p_i^{e_i}$. Dann muß es in V_i einen Vektor $v_i \in V_i$ geben mit

$$p_i(\sigma)^{e_i}(v_i) = 0$$

aber nicht für eine kleinere Potenz (sonst wäre das Minimalpolynom von σ ein echter Teiler von $T^n - 1$). Sei

$$\alpha = v_1 + \ldots + v_s$$

die Summe aller dieser Vektoren. Dann impliziert $f(\sigma)(\alpha) = 0$ schon $f(\sigma)(v_i) = 0$ für alle $1 \leq i \leq s$ und daher $T^n - 1 \mid f$. Es folgt, daß die K-lineare Abbildung

$$\begin{aligned} K[T]/(T^n - 1) &\to L \\ f &\mapsto f(\sigma)(\alpha) \end{aligned}$$

injektiv, und wegen Dimensionsvergleich auch Bijektiv ist. Folglich ist das Bild der Basis

$$1, T, T^2, \ldots, T^{n-1}$$

nämlich

$$\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)$$

eine K-Basis von L. Das ist die gesuchte Normalbasis. □

Bemerkung 218. Im Jahre 1986 haben H. W. Lenstra und R. Schoof[9] gezeigt, daß für eine Erweiterung $\mathbb{F}_{q^m}/\mathbb{F}_q$ endlicher Körper ein Element $\alpha \in \mathbb{F}_{q^m}$ existiert, so daß zum einen

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$$

eine $\mathbb{F}_q$-Basis ist, also eine Normalbasis von $\mathbb{F}_{q^m}/\mathbb{F}_q$, und gleichzeitig α die multiplikative Gruppe $\mathbb{F}_{q^m}^\times$ erzeugt, also ein primitives Element für $\mathbb{F}_{q^m}$ ist.

Übungsaufgaben zu §11

Übungsaufgabe 11.1. Sei $\mathbb{F} = \mathbb{F}_p^{\mathrm{alg}}$ der algebraische Abschluß von $\mathbb{F}_p$. Wir betrachten die Untergruppe $\Gamma = \langle \mathrm{Frob}_p \rangle$ in $\mathrm{Aut}(\mathbb{F})$.

(1) Zeigen Sie, daß $\Gamma \simeq \mathbb{Z}$.
(2) Bestimmen Sie $\mathbb{F}_0 = \mathbb{F}^\Gamma$. Ist $\mathbb{F}/\mathbb{F}_0$ galoissch?
(3) Bestimmen Sie $\mathrm{Aut}(\mathbb{F})$.

Übungsaufgabe 11.2. Man beweise oder widerlege die Aussage:

Im Beweis von Theorem 96 ist E_1 schon algebraisch abgeschlossen.

Übungsaufgabe 11.3. Sei L/K eine endliche normal Erweiterung. Zeigen Sie, daß es eine Zwischenerweiterung L_i gibt, so daß L_i/K rein inseparabel und L/L_i separabel ist. Zeigen Sie weiter, daß L_i eindeutig ist mit dieser Eigenschaft und L/L_i galoissch ist

Übungsaufgabe 11.4. Zeigen Sie, daß $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ galoissch ist und bestimmen Sie eine Normalbasis. Erzeugt $\zeta_3 + \sqrt[3]{2}$ eine Normalbasis?

12. Der Hauptsatz der Galoistheorie

12.1. Galoistheorie von Erweiterungen. Wir beweisen nun den zentralen Satz der Vorlesung.

Theorem 219 (Hauptsatz der Galoistheorie)**.** *Sei L/K eine Galoiserweiterung.*

(1) *K ist der Fixkörper von $\mathrm{Gal}(L/K)$ und $[L : K] = \# \mathrm{Gal}(L/K)$.*
(2) *Wenn $K \subseteq M \subseteq L$ ein Zwischenkörper ist, so ist L/M ebenfalls eine Galoiserweiterung, und*

$$\begin{aligned} \{\textit{Zwischenkörper } K \subseteq M \subseteq L\} &\leftrightarrow \{\textit{Untergruppen } H \leq \mathrm{Gal}(L/K)\} \\ M &\mapsto \mathrm{Gal}(L/M) \\ L^H &\leftarrow\!\shortmid H \end{aligned}$$

sind zueinander inverse Bijektionen, genannt ***Galoiskorrespondenz****.*

[9] Lenstra, H.W., jr; Schoof, R.J. (1987). Primitive normal bases for finite fields. Mathematics of Computation **48** (1987), 217–231.

Die Galoiskorrespondenz ist inklusionsumkehrend und idenitifiziert Körpergrad mit Index. Für Zwischenkörper E, F und Untergruppen U, V gilt

(a) $E \subseteq F \iff \mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/E)$ *und dann gilt*

$$[F : E] = \big(\mathrm{Gal}(L/E) : \mathrm{Gal}(L/F)\big).$$

(b) $U \subseteq V \iff L^V \subseteq L^U$ *und dann gilt*

$$(V : U) = [L^U : L^V].$$

(3) *Sei M ein Zwischenkörper und $\sigma \in \mathrm{Gal}(L/K)$. Dann gilt*

$$\mathrm{Gal}(L/\sigma(M)) = \sigma\,\mathrm{Gal}(L/M)\sigma^{-1}$$

und die folgende Aussagen sind äquivalent:

(a) *M ist eine Galoiserweiterung von K.*

(b) *M ist invariant unter $\mathrm{Gal}(L/K)$.*

(c) *$\mathrm{Gal}(L/M)$ ist ein Normalteiler in $\mathrm{Gal}(L/K)$.*

Wenn diese Bedingungen erfüllt sind, so ist

$$\begin{aligned}\mathrm{Gal}(L/K) &\to \mathrm{Gal}(M/K)\\ \sigma &\mapsto \sigma|_M\end{aligned}$$

surjektiver Gruppenhomomorphismus mit Kern $\mathrm{Gal}(L/M)$, also kanonisch

$$\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M).$$

(4) *Seien E und F Zwischenkörper von L/K und U und V Untergruppen von $\mathrm{Gal}(L/K)$. Dann gilt:*

(a)

$$\begin{aligned}\mathrm{Gal}(L/EF) &= \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F),\\ L^{U\cap V} &= L^U L^V.\end{aligned}$$

(b) *Es bezeichne $\langle - \rangle$ das Erzeugnis in $\mathrm{Gal}(L/K)$:*

$$\begin{aligned}\mathrm{Gal}(L/E \cap F) &= \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/F)\rangle,\\ L^{\langle U,V\rangle} &= L^U \cap L^V.\end{aligned}$$

Beweis. (1) Wenn $U \subseteq V$ Untergruppen von $\mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$ sind, dann gilt offensichtlich

$$L^V \subseteq L^U.$$

Nach Theorem 202 (a) gibt es eine endliche Untergruppe $G \subseteq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$, so daß gilt

$$K = L^G \supseteq L^{\mathrm{Gal}(L/K)} \supseteq K.$$

Dies zeigt, daß K der Fixkörper von $\mathrm{Gal}(L/K)$ ist. Die Behauptung $[L : K] = \mathrm{Gal}(L/K)$ wurde in Theorem 202 (b) bereits bewiesen.

(2) Nach Theorem 202 (c) ist galoissch dasselbe wie normal und separabel. Wenn L/K normal und separabel ist, dann gilt dasselbe für L/M für jeden Zwischenkörper M.

Die angegebenen Abbildungen $M \mapsto \mathrm{Gal}(L/M)$ und $H \mapsto L^H$ sind wohldefiniert. Außerdem zeigt (1) angewandt auf L/M, daß

$$L^{\mathrm{Gal}(L/M)} = M.$$

Wenn wir noch

$$\mathrm{Gal}(L/L^H) = H$$

zeigen, dann sind die Abbildungen zueinander invers und damit bijektiv.

Es gilt sicher $H \subseteq \mathrm{Gal}(L/L^H)$. Damit reicht es aus, beide Seiten zu zählen. Die Erweiterung L/L^H ist auch galoissch, nach (1) vom Grad

$$\#\,\mathrm{Gal}(L/L^H) = [L : L^H],$$

und nach Theorem 202 (d) von einem Element erzeugt. Sei $L = L^H(\alpha)$. Wie im Beweis von Theorem 202 gesehen, ist

$$f = \prod_{\sigma \in H} (T - \sigma(\alpha)) \in L^H[T]$$

ein Polynom vom Grad $\#H$ mit Nullstelle α. Damit haben wir

$$\#\operatorname{Gal}(L/L^H) = [L : L^H] = \deg(P_{\alpha/L^H}) \leq \#H.$$

Dies zeigt $H = \operatorname{Gal}(L/L^H)$.

In den Aussage (a) und (b) sind

$$E \subseteq F \Longrightarrow \operatorname{Gal}(L/F) \subseteq \operatorname{Gal}(L/E)$$

und

$$U \subseteq V \Longrightarrow L^V \subseteq L^U$$

klar per Definition. Die umgekehrten Implikationen folgen dann sofort aus den offensichtlichen Richtungen und der Bijektion der Galoiskorrespondenz:

$$\operatorname{Gal}(L/F) \subseteq \operatorname{Gal}(L/E) \implies E = L^{\operatorname{Gal}(L/E)} \subseteq L^{\operatorname{Gal}(L/F)} = F$$

und

$$L^U \subseteq L^V \implies V = \operatorname{Gal}(L/L^V) \subseteq \operatorname{Gal}(L/L^U) = U.$$

Die Aussagen über Grade und Index entsprechen sich ebenso unter Galoiskorrespondenz, es reicht daher, eine der beiden Gleichungen zu zeigen. Wir nutzen (1) für $M = E$ und $M = F$ sowie Gradsatz und Satz von Lagrange und finden

$$[F : E] = \frac{[L : E]}{[L : F]} = \frac{\#\operatorname{Gal}(L/E)}{\#\operatorname{Gal}(L/F)} = (\operatorname{Gal}(L/E) : \operatorname{Gal}(L/F)).$$

(3) Sei $g \in \operatorname{Gal}(L/M)$ und $x \in \sigma(M)$, etwa $x = \sigma(y)$ mit $y \in M$. Dann gilt

$$\sigma g \sigma^{-1}(x) = \sigma g(y) = \sigma(y) = x.$$

Daher gilt wird $\sigma(M)$ von $\sigma g \sigma^{-1}$ elementweise fixiert und

$$\sigma \operatorname{Gal}(L/M)\sigma^{-1} \subseteq \operatorname{Gal}(L/\sigma(M)).$$

Beide Seiten sind Untergruppen der Ordnung

$$\#\sigma \operatorname{Gal}(L/M)\sigma^{-1} = \#\operatorname{Gal}(L/M) = [L : M] = [L : \sigma(M)] = \#\operatorname{Gal}(L/\sigma(M)),$$

also die gleiche Untergruppe.

Wir zeigen nun die Äquivelenz von (a)–(c).

(a) $\Longrightarrow$ (b): Wenn M/K galoissch ist, dann ist M/K normal und für jedes $\sigma \in \operatorname{Gal}(L/K)$ hat

$$\sigma|_M : M \to L$$

Bild in M, genauer $\sigma(M) = M$. Dies zeigt (b).

(b) $\Longrightarrow$ (c): Wenn für alle $\sigma \in \operatorname{Gal}(L/K)$ gilt $\sigma(M) = M$, dann ist

$$\sigma \operatorname{Gal}(L/M)\sigma^{-1} = \operatorname{Gal}(L/\sigma(M)) = \operatorname{Gal}(L/M),$$

somit $\operatorname{Gal}(L/M)$ ein Normalteiler in $\operatorname{Gal}(L/K)$.

(c) $\Longrightarrow$ (a): Als Zwischenerweiterung von L/K ist M/K immer separabel. Wir müssen zeigen, daß M/K auch normal ist. Dazu müssen wir zeigen, daß für jede Erweiterung $M \subseteq \Omega$ und eine K-Einbettung $\tau : M \to \Omega$ das Bild schon in M ist. OBdA ist Ω sogar eine Erweiterung von L. Nach dem Fortsetzungssatz (nachdem wir eventuell Ω durch eine Erweiterung ersetzen) dürfen wir annehmen, daß τ die Einschränkung einer K-Einbettung $\sigma : L \to \Omega$ ist. Da L/K normal ist, gilt $\sigma(L) = L$. Somit hat $\tau = \sigma|_M$ schon einmal Bild in L. Nun ist jedes $x \in \sigma(M)$, etwa $x = \sigma(y)$ mit $y \in M$, invariant unter jedem $g \in \operatorname{Gal}(L/M)$:

$$g(x) = g(\sigma(y)) = \sigma\big(\sigma^{-1} g \sigma(y)\big) = \sigma(y) = x,$$

denn $\sigma^{-1}g\sigma$ ist nach Voraussetzung in $\mathrm{Gal}(L/M)$. Damit haben wir gezeigt, daß

$$\tau(M) = \sigma(M) \subseteq L^{\mathrm{Gal}(L/M)} = M,$$

und damit ist M/K normal. Das zeigt (a).

Sei nun M/K eine normale Zwischenerweiterung. Dann ist die Restriktionsabbildung

$$\sigma \mapsto r(\sigma) = \sigma|_M$$

surjektiv und eine Abbildung

$$\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L) \xrightarrow{r} \mathrm{Hom}_K(M, L) = \mathrm{Hom}_K(M, M) = \mathrm{Gal}(M/K).$$

Der Kern von r ist per Definition $\mathrm{Gal}(L/M)$. Der Rest folgt aus dem Homomorphiesatz.

(4) (a) Die Gruppe $\mathrm{Gal}(L/EF)$ besteht aus allen $\sigma \in \mathrm{Gal}(L/K)$, die alle Elemente von EF fixieren. Das passiert genau dann, wenn alle Elemente von E und alle Elemente von F fixiert werden, also wenn σ sowohl in $\mathrm{Gal}(L/E)$ als auch in $\mathrm{Gal}(L/F)$ enthalten ist. Dies zeigt die erste Behauptung, und die zweite folgt sofort durch Anwendung der Galoiskorrespondenz.

Mit (b) verfahren wir andersherum, denn diesmal folgt $L^{\langle U,V\rangle} = L^U \cap L^V$ sofort aus der Definition des Fixkörpers und der offensichtlichen Erkenntnis, daß es, um invariant unter einer Gruppe von Automorphismen zu sein, genügt, wenn das Element invariant unter Erzeugern der Gruppe ist. Galoiskorrespondenz zeigt diesmal die erste Behauptung aus der zweiten. □

Bemerkung 220. Theorem 116 folgt nun als Spezialfall von Theorem 219.

Bemerkung 221. Nach Theorem 219 können Aussagen über separable Körpererweiterungen L_i/K und Polynome $f_i \in K[T]$ in der Regel in Fragen über Gruppen überführt werden. Dazu muß man nur eine gemeinsame Galoissche Hülle $\tilde{L}/K$ für den Körper oder die Zerfällungskörper bilden und mittels Galoiskorrespondenz in Aussagen über Untergruppen von $\mathrm{Gal}(\tilde{L}/K)$ übersetzen.

Diese Maschine der Galoistheorie ist keine Garantie, daß man ein Problem so lösen kann, aber oft wird das Problem übersichtlicher. Ich sehe das so: ein Körper hat zwei Verknüpfungen, eine Gruppe nur noch eine. Das muß leichter sein (auch wenn man sich einhandelt, daß die eine Verknüpfung der Gruppe in der Regel nicht mehr abelsch ist).

Damit sollte klar sein, daß von nun an die Vorlesung graduell in Richtung Algebra (endlicher) Gruppen driftet. Wenn man von der Übersetzung in gruppentheoretische Fragen etwas gewinnen möchte, so muß man mehr über (endliche) Gruppen wissen.

Beispiel 222. Wir nehmen das Beispiel 205 wieder auf. Dies war die Erweiterung $\mathbb{F}_q(T)/\mathbb{F}_q(X)$ gegeben mit

$$\mathrm{Gal}(\mathbb{F}_q(T)/\mathbb{F}_q(X)) = \mathrm{PGL}_2(\mathbb{F}_q)$$

gegeben durch die Operation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .T = \frac{aT+b}{cT+d}.$$

Die Gruppe $G = \mathrm{PGL}_2(\mathbb{F}_q)$ hat die folgende Borelsche Untergruppe

$$\begin{aligned} B = \mathrm{Aff}^1(\mathbb{F}_q) &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\} \\ &\simeq \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ ; \ a, d \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\} / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\} \subseteq \mathrm{PGL}_2(\mathbb{F}_q) \end{aligned}$$

der affin linearen Transformationen. Diese Matrizen wirken durch

$$T \mapsto aT + b,$$

eben durch affin lineare Transformationen. Wir bestimmen nun den zu B unter der Galoiskorrespondenz gehörenden Zwischenkörper. Wegen

$$\#B = (q-1)q$$

hat der Fixkörper den Grad
$$[\mathbb{F}_q(T) : \mathbb{F}_q(T)^B] = (q-1)q.$$
Wir erinnern, daß der Fixkörper $\mathbb{F}_q(T)^G$ der rationele Funktionenkörper in X definert durch
$$X = \frac{((T^q - T)^{q-1} + 1)^{q+1}}{(T^q - T)^{q^2-q}}$$
ist. Setzen wir
$$Y = (T^q - T)^{q-1} + 1$$
so gilt
$$X = \frac{Y^{q+1}}{(Y-1)^q} = \frac{Y^{q+1}}{Y^q - 1}$$
Damit haben wir Inklusionen von rationalen Funktionenkörpern
$$K = \mathbb{F}_q(X) \subseteq \mathbb{F}_q(Y) \subseteq \mathbb{F}_q(T).$$
Wegen
$$Y^{q+1} - XY^q + X = 0$$
ist der Grad $[\mathbb{F}_q(Y) : \mathbb{F}_q(X)]$ höchstens $q+1$. Das Polynom in $K[S]$
$$S^{q+1} - XS^q + X$$
ist nach dem Eisensteinkriterium irreduzibel, und zwar bezüglich der Bewertung gegeben durch die Nullstellenordnung in $X = 0$, also bezüglich dem Primelement X im Polynomring $\mathbb{F}_q[X]$. Damit ist $\mathbb{F}_q[Y]$ ein Kandidat für $\mathbb{F}_q(T)^B$, es hat den richtigen Grad, und so fehlt nur noch zu zeigen, daß Y invariant unter B ist:
$$\begin{aligned}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.Y &= \big((aT+b)^q - (aT+b)\big)^{q-1} + 1 \\ &= \big((aT^q+b) - (aT+b)\big)^{q-1} + 1 = \big(a(T^q - T)\big)^{q-1} + 1 = Y\end{aligned}$$
denn $a \in \mathbb{F}_q^\times$ erfüllt $a^{q-1} = 1$ nach kleinem Fermat (oder Invarianz unter q-Frobenius). Somit gilt
$$\mathbb{F}_q(T)^B = \mathbb{F}_q(Y).$$

Es fällt auf, daß die Unterkörper von $\mathbb{F}_q(T)$, welche über $\mathbb{F}_q$ transzendent sind, sämtlich wieder rationale Funktionenkörper sind. Das ist kein Zufall, sondern Lüroth's Theorem[10].

Bemerkung 223. Welche endliche Gruppen als Galoisgruppe einer Galoiserweiterung L/K bei festem K vorkommen können, ist oft schwer zu entscheiden.

- Wenn $K = \mathbb{F}_q$ ein endlicher Körper ist, dann kommen genau alle zyklischen Gruppen vor, siehe Theorem 116.
- Dasselbe gilt für $K = \mathbb{C}((T))$, oder $K = \Omega((T))$, wenn Ω ein algebraisch abgeschlossener Körper der Charakteristik 0 ist. Das ist uns aber im Moment noch zu schwer.
- Wenn $K = F(T)$ und $F = \Omega((T))$ mit Ω algebraisch abgeschlossen, dann hat David Harbater bewiesen, daß jede endliche Gruppe als Galoisgruppe einer geeigneten Erweiterung vorkommt.
- Das **inverse Galoisproblem** fragt nach den Galoisgruppen, die für endliche galoissche Erweiterungen von $\mathbb{Q}$ auftreten können. Man vermutet, daß jede endliche Gruppe das tut und hat auch schon viele endliche Gruppen realisiert, zum Beispiel alle Gruppen von ungerader Primpotenzordnung (unabhängig von Scholz und Reichardt), und allgemeiner für alle auflösbaren Gruppen (Shafarevich). Darüberhinaus sind viele einfache und lineare Gruppen realisiert worden (Matzat, et. al.).

[10] Jacob Lüroth, 1844–1910, deutscher Mathematiker.

12.2. **Galoistheorie eines Polynoms.** Die Galoisgruppe eines Polynoms ist mehr als eine Gruppe: eine Permutationsgruppe.

Definition 224. Die **symmetrische Gruppe** auf einer Menge M ist die Gruppe

$$S_M = \{\varphi : M \to M \ ; \ \varphi \text{ bijektiv}\}$$

mit der Komposition als Verknüpfung.

Beispiel 225. Für $M = \{1, \ldots, n\}$ ist das nichts anderes als die symmetrische Gruppe S_n.

Definition 226. (1) Eine **Permutationsgruppe** ist eine Gruppe G zusammen mit einer Menge M und einem injektiven Gruppenhomomrphismus

$$G \to S_M,$$

also einer treuen Operation von G auf M. Die Zahl $\#M$ heißt der **Grad** von G.

(2) Eine Permutationsgruppe $G \hookrightarrow S_M$ heißt **transitive**, wenn die Operation von G auf M transitiv ist, also nur einen Orbit hat.

(3) Sei $n \in \mathbb{N}$. Eine Permutationsgruppe $G \hookrightarrow S_M$ heißt n**-transitive**, wenn die Operation von G auf M gilt: zu je zwei n-Tupeln paarweise verschiedener Elemente $x_1, \ldots, x_n$ und $y_1, \ldots, y_n$ aus M gibt es ein $g \in G$ mit

$$g(x_i) = y_i$$

für alle $i = 1, \ldots, n$.

(4) Sei $n \in \mathbb{N}$. Eine Permutationsgruppe $G \hookrightarrow S_M$ heißt **scharf** n**-transitive**, wenn die Operation von G auf M gilt: zu je zwei n-Tupeln paarweise verschiedener Elemente $x_1, \ldots, x_n$ und $y_1, \ldots, y_n$ aus M gibt es **genau** ein $g \in G$ mit

$$g(x_i) = y_i$$

für alle $i = 1, \ldots, n$.

Jedes mathematische Objekt hat seinen zugehörigen Begriff von (strukturerhaltender) Abbildung.

Definition 227. Ein **Homomorphismus von Permutationsgruppen** von $G \to S_M$ nach $H \to S_N$ besteht aus einem Gruppenhomomorphismus

$$f : G \to H$$

und einer Abbildung von Mengen

$$\Phi : M \to N$$

so daß für alle $g \in G$ und alle $m \in M$ gilt

$$\Phi(g.m) = f(g).\Phi(m).$$

Ein Isomorphismus von Permutationsgruppen ist ein Homomorphsimus mit Inversem, also in obiger Notation, wenn $f : G \to H$ ein Gruppenisomorphsimus und Φ bijektiv sind.

Beispiel 228. (1) Sei q eine Primzahlpotenz. Die Gruppe $\mathrm{PGL}_2(\mathbb{F}_q)$ ist vermöge ihrer Operation auf $\mathbb{P}^1(\mathbb{F}_q)$ eine Permutationsgruppe auf einer Menge von $\#\mathbb{P}^1(\mathbb{F}_q) = q + 1$ Elementen, und zwar eine scharf 3-fach transitive. Daraus kann man wieder auf die Ordnung von $\mathrm{PGL}_2(\mathbb{F}_q)$ schließen: $(q - 1)q(q + 1)$.

(2) Jede Gruppe kann als Permutationsgruppe angesehen werden. Dazu läßt man G auf $M = G$ durch Translation von links operieren:

$$\begin{aligned} G \times M &\to M \\ (g, h) &\mapsto gh \end{aligned}$$

Damit ist $G \hookrightarrow S_G$ eine Permutationsgruppe, und zwar eine scharf 1-transitiven Permutationsgruppe. Wenn $\#G = n$ endlich ist und man eine Liste $G = \{g_1, \ldots, g_n\}$ der Elemente von G, die zu einer Bijektion $G \leftrightarrow \{1, \ldots, n\}$ führt, festgelegt hat, dann entsteht dadurch

$$G \hookrightarrow S_G \simeq S_n$$

und man hat den Satz von Cayley bewiesen:

Satz 229 (Cayley). *Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.*

(3) Eine gegebene Gruppe G kann in der Regel auf viele Arten als transitive Permutationsgruppe auftreten. Sei etwa $G = S_n$ mit $n \geq 3$. Dann ist $S_n \hookrightarrow S_{n!}$ nach der Konstruktion über die Translationsoperation. Andererseits operiert S_n natürlich auf $\{1, \ldots, n\}$, was zur Identität $\mathrm{id} : S_n \to S_n$ führt. Diese Permutationsgruppe ist die einzige scharf n-transitive auf einer Menge mit n Elementen.

Definition 230. Die **Galoisgruppe eines Polynoms**, genauer eines Polynoms $f \in K[X]$ mit ausschließlich separablen Nullstellen, ist die Galoisgruppe

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$$

eines Zerfällungskörpers L/K als Permuationsgruppe

$$\mathrm{Gal}(f) \to S_{\mathrm{NS}_f(L)}$$

mit der natürlichen Operation auf der Menge der Nullstellen f in L.

Beweis. Die Galoisgruppe eines Polynoms ist bis auf Isomorphie wohldefiniert. Zunächst ist ein Zerfällungskörper L normal über K und, da f nur ausschließlich separablen Nullstellen hat, ist L/K auch separabel. Damit ist L/K galoissch nach Theorem 202 (c).

Wenn L' ein weiterer Zerfällungskörper von f ist, dann gibt es nach Satz 81 einen K-Isomorphismus $\sigma : L \simeq L'$. Dann ist offensichtlich

$$\begin{aligned} \sigma(-)\sigma^{-1} : \mathrm{Gal}(L/K) &\to \mathrm{Gal}(L'/K) \\ \tau &\mapsto \sigma\tau\sigma^{-1} \end{aligned}$$

ein Gruppenisomorphismus. Außerdem ist

$$\sigma|_{\mathrm{NS}_f(L)} : \mathrm{NS}_f(L) \to \mathrm{NS}_f(L')$$

eine Bijektion, die mit $\sigma(-)\sigma^{-1}$ kompatibel ist: zu $\tau \in \mathrm{Gal}(L/K)$ und $\alpha \in \mathrm{NS}_f(L)$ gilt:

$$\sigma|_{\mathrm{NS}_f(L)}(\tau.\alpha) = \sigma(\tau(\alpha)) = \sigma\tau\sigma^{-1}(\sigma(\alpha)) = (\sigma(-)\sigma^{-1}).\sigma|_{\mathrm{NS}_f(L)}(\alpha).$$

Jetz müssen wir noch zeigen, daß die Operation von $\mathrm{Gal}(f)$ auf $\mathrm{NS}_f(L)$ treu ist:

$$\mathrm{Gal}(f) \hookrightarrow S_{\mathrm{NS}_f(L)}.$$

Aber wenn $\sigma \in \mathrm{Gal}(f) = \mathrm{Gal}(L/K)$ trivial auf den Nullstellen von f in L operiert, dann ist $\sigma = \mathrm{id}$, weil diese Nullstellen den Zerfällungskörper erzeugen. □

Beispiel 231. Sei $f = T^2 - a \in K[T]$ irreduzibel und K von Charakteristik $\neq 2$. Dann ist der Zerfällungskörper von f gegeben durch $L = K(\sqrt{a})$ und $\mathrm{Gal}(f)$ ist die Permatationsgruppe aller Permutationen von

$$\{\sqrt{a}, -\sqrt{a}\}$$

also zyklisch von Ordnung 2.

Beispiel 232. Wir wollen die Galoisgruppe des Polynoms $T^4 - 2 \in \mathbb{Q}[T]$ bestimmen. Nach Eisenstein mit $p = 2$ ist dies irreduzibel. Sei

$$\alpha = \sqrt[4]{2}$$

die positive reelle Nullstelle. Dann sind die alle Nullstellen in $\mathbb{C}$ gegeben durch

$$M = \{\pm\alpha, \pm i\alpha\}.$$

Damit ist die galoissche Hülle $L = \mathbb{Q}(\alpha, i)$ vom Grad höchstens 2 über $\mathbb{Q}(\alpha)$, aber sogar genau 2, denn $L \neq \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, weil i nicht reell ist. Damit ist

$$G = \mathrm{Gal}(T^4 - 2)$$

eine Gruppe der Ordnung 8, als Permutationsgruppe auf M vom Grad 4:

$$G \hookrightarrow S_M.$$

Wir ordnen die Nullstellen M als Quadrat an wie folgt:

$$\begin{tikzcd}
\alpha \arrow[r, dash] \arrow[d, dash] & i\alpha \arrow[d, dash] \\
-i\alpha \arrow[r, dash] & -\alpha
\end{tikzcd}$$

Die komplexe Konjugation definiert ein $c \in G$, die Speigelung an der Geraden durch $\pm\alpha$. Wegen

$$\alpha^2 = \sqrt{2}$$

ist $M = \mathbb{Q}(\sqrt{2}, i)$ ein Zwischenkörper. Als Komposition der beiden quadratischen Zwischenkörper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$ ist $M/\mathbb{Q}$ galoissch und zwar vom Grad 4, denn $[L : M] \leq 2$. Damit ist natürlich

$$\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$$

und es gibt $\tau \in \mathrm{Gal}(M/\mathbb{Q})$ mit

$$\tau(\sqrt{2}) = -\sqrt{2}$$
$$\tau(i) = i.$$

Sei $\sigma \in G$ eine Fortsetzung auf L von τ. Dann ist

$$\sigma(\alpha)^2 = \sigma(\alpha^2) = \tau(\sqrt{2}) = -\alpha^2,$$

und somit $\sigma(\alpha) = \pm i\alpha$. Wir nehmen an, daß

$$\sigma(\alpha) = i\alpha.$$

Die andere Wahl $-i\alpha$ führt analog zum gleichen Ergebnis. Dann muß σ die Drehung um $\pi/2$ im Urzeigersinn sein:

$$\begin{aligned}
\sigma(\alpha) &= i\alpha, \\
\sigma(i\alpha) &= \sigma(i)\sigma(\alpha) = i \cdot i\alpha = -\alpha, \\
\sigma(-\alpha) &= -\sigma(\alpha) = -i\alpha, \\
\sigma(-i\alpha) &= -\sigma(i\alpha) = \alpha.
\end{aligned}$$

Also enthät G Erzeuger der Diedergruppe D_4 der Ordnung 8 in der Darstellung als Permutationsgruppe des betrachteten Quadrats. Da $D_4 \subseteq G$, und beide Gruppen haben Ordnung 8, so gilt

$$\mathrm{Gal}(T^4 - 2) = D_4.$$

Wir machen nun in diesem Fall die Galoiskorrespondenz explizit. Dazu berechenen wir den Verband der Untergruppen von $D_4 = \langle \sigma, c \rangle$:

$$\begin{tikzcd}
 & & 1 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle \sigma c \rangle \arrow[dr, dash] & \langle \sigma^3 c \rangle \arrow[d, dash] & \langle \sigma^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle \sigma^2 c \rangle \arrow[d, dash] & \langle c \rangle \arrow[dl, dash] \\
 & \langle \sigma^2, \sigma c \rangle \arrow[dr, dash] & \langle \sigma \rangle \arrow[d, dash] & \langle \sigma^2, c \rangle \arrow[dl, dash] & \\
 & & D_4 & &
\end{tikzcd}$$

und vergleichen mit den Zwischenkörpern (Position H wird durch L^H ersetzt):

$$\begin{tikzcd}
 & & \mathbb{Q}(\alpha, i) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha + i\alpha) \arrow[dr, dash] & \mathbb{Q}(\alpha - i\alpha) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(i\alpha) \arrow[d, dash] & \mathbb{Q}(\alpha) \arrow[dl, dash] \\
 & \mathbb{Q}(i\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Bemerkung 233. Jede (endliche) Galoisgruppe ist Galoisgruppe eines Polynoms. Sei L/K endlich galoissch und α ein primitives Element: $L = K(\alpha)$. Dann ist

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(P_{\alpha/K}),$$

aber die Operation auf

$$\mathrm{NS}_{P_{\alpha/K}}(L) \simeq \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, L) = \mathrm{Gal}(L/K)$$

ist nichts anderes als die Translationsoperation von links. Dies bringt keine zusätzliche Information über $\mathrm{Gal}(L/K)$.

Besser ist es, wenn man eine Operation auf einer kleineren Menge findet. Dazu sei L/K endlich galoissch und Zerfällungskörper eines Polynoms $f \in K[T]$ vom Grad $n < [L : K]$. Dann ist

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(f),$$

und dies ist nun eine Permutationsgruppe vom Grad n, also nicht die Translationsoperation.

Beispiel 234. Das irreduzible Polynom

$$f(S) = S^{q+1} - XS^q + X \in \mathbb{F}_q(X)[S]$$

hat Galoisgruppe $\mathrm{PGL}_2(\mathbb{F}_q)$ als Permutationsgruppe vom Grad $q+1$ durch die Operation auf $\mathbb{P}^1(\mathbb{F}_q)$ mittels Möbiustransformationen. Hier ist der Grad der Permutationsgruppe $q+1$ wesentlich kleiner als die Ordnung der Gruppe $(q-1)q(q+1)$. Dies folgt aus den Erkenntnissen von Beispiel 222 wie folgt.

In der Notation von Beispiel 222 ist in der Erweiterung $\mathbb{F}_q(Y)/\mathbb{F}_q(X)$ das Minimalpolynom von Y gerade unser $f(S)$. Wir müssen nun die Galoissche Hülle von $\mathbb{F}_q(Y)/\mathbb{F}_q(X)$ bestimmen.

Da $\mathbb{F}_q(Y)$ in der galoisschen Erweiterung $\mathbb{F}_q(T)/\mathbb{F}_q(X)$ liegt, finden wir auch seine galoissche Hülle (über $\mathbb{F}_q(X)$) in $\mathbb{F}_q(T)$.

Die Suche nach der kleinsten, über $\mathbb{F}_q(X)$ galoisschen Teilerweiterung wird per Galoiskorrespondenz übersetzt in die Suche nach dem größten Normalteiler [11] N von $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q(T)/\mathbb{F}_q(X))$ gehört, der in $B = \mathrm{Gal}(\mathbb{F}_q(T)/\mathbb{F}_q(Y))$ enthalten ist. Man überlegt sich leicht, daß dies der Normalteiler

$$N = \bigcap_g gBg^{-1}$$

ist. Weil B der Stabilisator von $[1:0] \in \mathbb{P}^1(\mathbb{F}_q)$ ist, demnach gBg^{-1} der Stabilisator von $g.[1:0]$ ist, stabilisiert N ganz $\mathbb{P}^1(\mathbb{F}_q)$. Damit ist $N = 1$, denn die Wirkung ist treu. Zu $N = 1$ gehört der Körper $\mathbb{F}_q(T)$ nach Galoiskorrespondenz.

Die Galoisgruppe des Polynoms $f(S)$ ist demnach $\mathrm{Gal}(\mathbb{F}_q(T)/\mathbb{F}_q(X) = \mathrm{PGL}_2(\mathbb{F}_q)$. Den Nachweis, daß die angegebenen Strukturen als Permutationsgruppe übereinstimmen, überlassen wir zur Übung.

Proposition 235. *Sei f ein separables, nicht konstantes Polynom. Dann ist* $\mathrm{Gal}(f)$ *genau dann transitive Permutationsgruppe, wenn f irreduzibel ist.*

Beweis. Sei L ein Zerfällungskörper von f über K. Wenn f irreduzibel ist, dann operiert $\mathrm{Gal}(L/K)$ transitiv auf den Nullstellen von f nach Korollar 77.

Sei also umgekehrt die Operation transitiv, und als Ansatz für einen Widerspruchsbeweis $f = gh$ mit g irreduzibel und h nicht konstant. Da f separabel ist, sind g und h teilerfremd, haben also keine gemeinsame Nullstelle. Daher ist

$$\mathrm{NS}_f(L) = \mathrm{NS}_g(L) \amalg \mathrm{NS}_h(L)$$

eine disjunkte Vereinigung von nicht-leeren Mengen. Da jedes $\sigma \in \mathrm{Gal}(L/K)$ Nullstellenmengen in sich überführt, kann die Operation nicht transitiv sein. □

Lemma 236. *Sei p eine Primzahl, und $\sigma, \tau \in S_p$ seien*

(1) σ ein p-Zykel, und

(2) τ eine Transposition.

Dann wird die Gruppe S_p von σ und τ erzeugt.

Beweis. Weil es arithmetisch und von der Notation her einfacher ist, permutieren wir mit S_p hier $\{0, 1, \ldots, p-1\}$ als Restklassenvertreter von $\mathbb{Z}/p\mathbb{Z}$.

Nach evetueller Umnummerierung (das ist eine Konjugation in S_p) dürfen wir annehmen, daß

$$\sigma = (0, 1, 2, \ldots, p-1)$$

der Standard p-Zykel ist. Die Potenzen von σ sind nun

$$\sigma^n = (0, n, 2n, \ldots, in, \ldots, (p-1)n),$$

(mit Einträgen modulo p). Für $p \nmid n$ und weil p eine Primzahl ist, ist σ^n auch ein p-Zykel: aus

$$p \mid (in - jn) = (i - j)n$$

folgt $i \equiv j \bmod p$, somit sind die Einträge von σ^n paarweise verschieden.

Sei $\tau = (a, b)$ die Transposition. Wir ersetzen σ durch eine geeignete Potenz (die wir wieder mit σ bezeichnen), so daß auch $\sigma(a) = b$ ist. Nach eventuell erneuter Umnummerierung dürfen wir daher annehmen, daß $a = 0$ und $b = 1$, somit

$$\sigma = (0, 1, 2, \ldots, p-1)$$
$$\tau = (0, 1).$$

[11] Die Gruppe $\mathrm{PGL}_2(\mathbb{F}_q)$ hat gar keine nicht-trivialen Normalteiler, sofern $q > 4$.

Sei $G = \langle \sigma, \tau \rangle$ die von σ und τ erzeugte Untergruppe. Aus

$$\sigma^n \tau \sigma^{-n} = (\sigma^n(0), \sigma^n(1)) = (n, n+1)$$

folgt, daß für alle $0 \leq n \leq p-2$ auch $(n, n+1) \in G$. Von diesen Transpositionen weiß man, daß sie S_p erzeugen (Bubblesort-Algorithmus).

Alternativer Beweis: Sei G das Erzeugnis von σ und τ als Permuationsgruppe in S_p. Dies G ist transitiv schon allein durch den p-Zykel σ. Weil die Länge eines Blocks ein Teiler des Grades der Permutationsgruppe ist, folgt aus p Primzahl, daß G primitiv ist.

Somit ist G primitive Permutationsgruppe, die eine Transposition enthält. Aus Korollar 390 von Appendix B schließen wir $G = S_p$. □

Satz 237. *Sei $K \subseteq \mathbb{R}$ ein reeller Körper, und sei $f \in K[T]$ irreduzibel. Wenn*

(i) $\deg(f) = p$ *eine Primzahl ist, und*
(ii) f *genau 2 nicht reellen Wurzeln hat (also f zerfällt in $\mathbb{R}$ als Produkt von einem quadratischen Faktor mit sonst lauter linearen Faktoren),*

dann ist $\mathrm{Gal}(f) \simeq S_p$ *als Permutationsgruppe.*

Beweis. Seien $\alpha_1, \ldots, \alpha_p$ die Nullstellen von f in einem Zerfällungskörper L von f. Dann ist $\mathrm{Gal}(f)$ ein Permutationsgruppe in S_p. Nach Proposition 235 ist

$$\mathrm{Gal}(f) \hookrightarrow S_p$$

treu und transitiv. Daher gilt nach der Orbit–Stabilisatorformel (Bahnenformel)

$$p \mid \# \mathrm{Gal}(f).$$

Nach dem Satz von Cauchy hat $\mathrm{Gal}(f)$ daher ein Element der Ordnung p. Die einzigen Elemente in S_p der Ordnung p sind Zykeln der Länge p.

Nun nutzen wir die Information über die Nullstellen in $\mathbb{R}$. Die komplexe Konjugation $z \mapsto \bar{z}$ fixiert K und liefert durch Einschränkung daher ein Element

$$c \in \mathrm{Gal}(f).$$

Da $\mathrm{NS}_f(L) \cap \mathrm{NS}_f(\mathbb{R})$ alle bis auf zwei Nullstellen enthält, muß c eine Transpostion, die Vertauschung der verbliebenen zwei Nullstellen, sein. Nun folgt der Satz aus dem rein gruppentheoretischen Lemma 236. □

Bemerkung 238. (1) Die Anzahl der reellen Nullstellen kann man mittels Sturmschen Ketten bestimmen.
(2) Die analoge Aussage in Lemma 236 für p nicht Primzahl gilt nicht. Die Elemente

$$\sigma = (1, 2, 3, 4), \tau = (1, 3) \in S_4$$

erzeugen die Diedergruppe $D_4 \subseteq S_4$, wie man sich durch den Effekt auf die Ecken des Quadrats

$$\begin{array}{ccc} 1 & — & 2 \\ | & & | \\ 4 & — & 3 \end{array}$$

klar macht. Es ist σ eine Drehung und τ eine Spiegelung.

Beispiel 239. Das Polynom $f = T^5 - 4T + 2 \in \mathbb{Q}[T]$ ist irreduzibel nach Eisenstein zu $p = 2$. Reelle Nullstellen gibt es nach dem Zwischenwertsatz und der Liste

$$\begin{aligned} f(-2) &= -22 < 0 \\ f(0) &= 2 > 0 \\ f(1) &= -1 < 0 \\ f(2) &= 26 > 0 \end{aligned}$$

mindestens 3. Zwischen zwei Nullstellen (die einfach sein müssen, da f als irreduzibles Polynom separabel ist) muß eine Nullstelle der Ableitung $f'(T) = 4T^4 - 4$ liegen. Die Ableitung hat nur zwei reelle Nullstellen, so daß

$$\mathrm{Gal}(f) \simeq S_5,$$

weil die Voraussetzung von Satz 237 erfüllt sind.

Satz 240. *Jede endliche Gruppe G ist Galoisgruppe einer geeigneten Galoiserweiterung.*

Beweis. Wir schreiben G wie im Satz von Cayley als Untergruppe von S_n für $n = \#G$. Da Untergruppen von Galoisgruppen wieder Galoisgruppen sind, reicht es also $G = S_n$ zu betrachten. Da mit $n < m$ eine Einbettung $S_n \hookrightarrow S_m$ existiert (Permutationenn der ersten n Einträge, der Rest fixiert), genügt es, den Fall $G = S_p$ für eine Primzahl p zu zeigen (es gibt unendlich viele und damit beliebig große Primzahlen).

Nach Satz 237 haben wir nur ein irreduzibles Polynom vom Grad p zu konstruieren, das genau $p-2$ reelle Nullstellen hat. Im konkreten Fall läßt sich so ein Polynom leicht durch Ausprobieren und Sturmsche Ketten finden. Eine Beispielserie erhalten wir mit $n + 2 = p$ aus dem folgenden Lemma 241. □

Lemma 241. *Für $n \geq 1$ hat das Polynom*

$$f(T) = 2 + T^2 \prod_{a=1}^{n} (T + 4a) \in \mathbb{Z}[T]$$

$\deg(f) - 2 = n$ *reelle Nullstellen und ist irreduzibel in* $\mathbb{Q}[T]$.

Beweis. Das Eisensteinkriterium mit $p = 2$ zeigt, daß f irreduzibel in $\mathbb{Q}[T]$ ist. Das Polynom

$$g(T) = f(T) - 2 = T^2 \prod_{a=1}^{n} (T + 4a)$$

hat $\deg(f) - 1 = n + 1$ Nullstellen, die bei $T = 0$ ist doppelt. Es handelt sich bei $T = 0$ um ein lokales Minimum, wie man durch Einsetzen von Werten $t > 0$ sieht. Zwischen den einfachen Nullstellen bei $-4a - 4$ und $-4a$ gibt es ein eindeutiges lokales Minimum (stets < 0) oder Maximum (stets > 0).

Durch das Verschieben um 2 verliert das Polynom $g(T)$ die doppelte Nullstelle ersatzlos. Es bleibt zu zeigen, daß kein weiteres lokales Minimum das Vorzeichen gewechselt hat. Dann kann man aus dem Zwischenwertsatz wieder auf $\deg(f) - 2$ reelle Nullstellen schließen.

Dazu reicht es aus, für jedes $1 \leq b \leq n - 1$ ein $\xi_b \in [-4b - 4, -4b]$ zu finden mit

$$|g(\xi_b)| > 2.$$

Wir wählen die Mitte:

$$|g(-4b - 2)| = (4b + 2)^2 \prod_{a=1}^{b} (4(b - a) + 2) \cdot \prod_{a=b+1}^{n} (4(a - b) - 2) \geq 6^2 \cdot 2^n > 2,$$

denn jeder Faktor im Produkt ist ≥ 2. □

Übungsaufgaben zu §12

Übungsaufgabe 12.1. Sei L/K eine Körpererweiterung und seine E, F Zwischenkörper, die über K endlich sind. Zeigen Sie:

Wenn E/K galoisch ist, dann ist auch EF/F Galoissch und die Einschränkungsabbildung

$$\begin{aligned} r : \mathrm{Gal}(EF/F) &\to \mathrm{Gal}(E/E \cap F) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

ist ein Isomorphismus von Gruppen.

Übungsaufgabe 12.2. Bestimmen Sie die Galoisgruppe der galoisschen Hülle von $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ und von $\mathbb{Q}(\sqrt{3+\sqrt{3}})/\mathbb{Q})$.

Übungsaufgabe 12.3. Die Gruppe $\mathrm{PGL}_2(\mathbb{F}_q)$ hat die Untergruppen (D: split Cartan, N: nilpotentes Radikal der Borel B, C: non-split Cartan)

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\} \simeq \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \ ; \ a, d \in \mathbb{F}_q^\times \right\} / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\}$$

$$N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \ ; \ x \in \mathbb{F}_q \right\} \simeq \left\{ \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times, x \in \mathbb{F}_q \right\} / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\}$$

$$C = \left\{ \begin{pmatrix} a & xb \\ b & a \end{pmatrix} \ ; \ a, b \in \mathbb{F}_q \right\} / \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ ; \ a \in \mathbb{F}_q^\times \right\} \simeq \mathbb{F}_{q^2}^\times / \mathbb{F}_q^\times$$

Für C soll q keine Potenz von 2 sein, und das Element $x \in \mathbb{F}_q$ ist kein Quadrat ist. So etwas gibt es stets, und $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{x})$. Der Isomorphismus zu $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times$ ist definiert durch die Multiplikationsoperation von $\mathbb{F}_{q^2}^\times$ auf dem 2-dimensionalen $\mathbb{F}_q$-Vektorraum $\mathbb{F}_{q^2}$. Dies definiert zunächst eine Einbettung $\mathbb{F}_{q^2}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{F}_q)$, welche in $\mathrm{PGL}_2(\mathbb{F}_q)$ das Bild C hat und über $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times$ faktorisiert.

Bestimmen Sie die Fixkörper von D, N und C auf $\mathbb{F}_q(T)$ analog zu Beispiel 222.

Übungsaufgabe 12.4. Sei Ω/K eine Körpererweiterung, L/K ein endlicher galoisscher Zwischenkörper und E ein weiterer beliebiger Zwischenkörper. Wir setzen $F = EL$ in Ω für das Kompositum von E und L. Zeigen Sie

(1) F/E ist endlich galoissch und die Abbildung $\sigma \mapsto \sigma|_L$ ist ein injektiver Gruppenhomomorphismus
$$\mathrm{res}_L^F : \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K).$$
(2) Bestimmen Sie das Bild von res_L^F und beschreiben Sie den zugehörigen Fixkörper.
(3) Zeigen Sie, daß $[F : E]$ ein Teiler von $[L : K]$ ist.
(4) Finden Sie ein Gegenbeispiel zu (3), wenn L/K nicht galoissch ist.

Übungsaufgabe 12.5. Sei M/K eine Körpererweiterung und L_1, L_2 Zwischenerweiterungen, die über K endlich und galoissch sind. Sei $L = L_1L_2$ das Kompositum in M. Zeigen Sie, daß L/K galoissch und

$$\begin{aligned} \mathrm{res} : \mathrm{Gal}(L/K) &\to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\mapsto (\sigma|_{L_1}, \sigma|_{L_2}) \end{aligned}$$

ein injektiver Gruppenhomomorphismus ist. Bestimmen Sie außerdem das Bild.

Tipp: Betrachten Sie $L_{12} = L_1 \cap L_2$ und nutzen sie das **Faserprodukt** von Gruppen. Das ist für Gruppen G_1, G_2 zusammen mit Gruppenhomomorphismen $\varphi_i : G_1 \to G_{12}$ für $i = 1, 2$ die Untergruppe

$$G_1 \times_{G_{12}} G_2 := \{(a_1, a_2) \in G_1 \times G_2 \ ; \ \varphi_1(a_1) = \varphi_2(a_2)\}$$

von $G_1 \times G_2$. (Die Homomorphismen φ_1, φ_2 gehören dazu, fallen aber bei der Notation üblicherweise raus.)

Übungsaufgabe 12.6. Zeigen Sie, daß $\mathrm{PGL}_2(K)$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .[u : v] = [au + bv : cu + dv]$$

scharf 3-fach transitiv auf $\mathbb{P}^1(K)$ operiert. Folgern Sie Isomorphismen

$$\mathrm{PGL}_2(\mathbb{F}_2) \simeq S_3$$

und

$$\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4.$$

Übungsaufgabe 12.7. Zeigen Sie, daß die Quaternionengruppe Q_8 nur auf eine einzige Art als transitive Permutationsgruppe auftritt.

Übungsaufgabe 12.8 (Explizite Kummertheorie für quadratische Erweiterungen (von $\mathbb{Q}$)). Seien $a_i \in \mathbb{Q}^\times$ für $i = 1, \ldots, r$ gegeben. Wir betrachten den Körper

$$K = \mathbb{Q}(\sqrt{a_i}\ ;\ i = 1, \ldots, r)$$

der von den Quadratwurzeln der a_i erzeugt wird.

(1) Zeigen Sie, daß $K/\mathbb{Q}$ galoissch mit $[K : \mathbb{Q}]$ eine 2er-Potenz ist.

(2) Sei $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Wir definieren auf der Untergruppe $\Delta := \langle a_1, \ldots, a_r \rangle \subseteq \mathbb{Q}^\times$ eine Abbildung

$$\begin{aligned} \Delta &\to \{\pm 1\} \\ d &\mapsto \chi_\sigma(d) = \frac{\sigma(\delta)}{\delta}, \end{aligned}$$

wobei $\delta \in K^\times$ beliebig mit $\delta^2 = d$ ist. Zeigen Sie, daß χ_σ wohldefiniert und ein Gruppenhomomorphismus ist.

(3) Zeigen Sie, daß χ_σ einen Gruppenhomomorphismus

$$\Delta(\mathbb{Q}^\times)^2/(\mathbb{Q}^\times)^2 \simeq \Delta/(\Delta \cap (\mathbb{Q}^\times)^2) \to \{\pm 1\}$$

induziert. Dieser sei auch mit χ_σ bezeichnet.

(4) Zeigen Sie, daß

$$\begin{aligned} \chi : \mathrm{Gal}(K/\mathbb{Q}) &\to \mathrm{Hom}\left(\Delta(\mathbb{Q}^\times)^2/(\mathbb{Q}^\times)^2, \{\pm 1\}\right) \\ \sigma &\mapsto \chi_\sigma \end{aligned}$$

ein Gruppenisomorphismus ist.

Tipp: Sowohl $\mathrm{Gal}(K/\mathbb{Q})$ als auch $\Delta(\mathbb{Q}^\times)^2/(\mathbb{Q}^\times)^2$ sind als endlich dimensionale Vektorräume über $\mathbb{F}_2$ aufzufassen. Dann ist χ die adjungierte Abbidlung zur Paarung

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}) \times \Delta(\mathbb{Q}^\times)^2/(\mathbb{Q}^\times)^2 &\to \{\pm 1\} \\ (\sigma, d) &\mapsto \chi_\sigma(d). \end{aligned}$$

Es ist zu zeigen, daß diese Paarung nicht ausgeartet ist.

(5) Formulieren Sie eine Aussage darüber, wann die Menge der Quadratwurzeln

$$\left\{ \alpha_\varepsilon = \sqrt{\prod_{i=1}^{r} a_i{}^{\varepsilon(i)}}\ ;\ \varepsilon : \{1, \ldots, r\} \to \{0, 1\} \right\}$$

über $\mathbb{Q}$ linear unabhängig sind als Elemente des $\mathbb{Q}$-Vektorraums $\mathbb{C}$.

13. Norm und Spur

Zu einem Element $a \in L$ einer endlichen Erweiterung L/K kann man die Linksmultiplikation definieren:

$$\begin{aligned} \lambda_a : L &\to L \\ x &\mapsto \lambda_a(x) = ax. \end{aligned}$$

Dies ist eine K-lineare Abbildung und hat als solches ein charakteristisches Polynom

$$\chi_{a,L/K}(T) = \det(T - \lambda_a) \in K[T].$$

Lemma 242. *Wenn $L = K(\alpha)$, dann ist*

$$\chi_\alpha(T) = P_{\alpha/K}.$$

Beweis. Nach Cayley–Hamilton ist α eine Nullstelle von $\chi_\alpha(T)$, daher

$$P_{\alpha/K} \mid \chi_\alpha(T).$$

Da beide Polynome den Grad $[K(\alpha) : K]$ haben und normiert sind, müssen sie gleich sein. □

13.1. Formeln für Norm und Spur.

Wir studieren nun spezielle Koeffizienten von $\chi_{a,L/K}(T)$ genauer.

Definition 243. (1) Die **Spur** einer endlichen Körpererweiterung L/K ist die Abbildung

$$\begin{aligned} \mathrm{tr}_{L/K} : L &\to K \\ a &\mapsto \mathrm{tr}_{L/K}(a) = \mathrm{tr}(\lambda_a). \end{aligned}$$

(2) Die **Norm** einer endlichen Körpererweiterung L/K ist die Abbildung

$$\begin{aligned} N_{L/K} : L &\to K \\ a &\mapsto N_{L/K}(a) = \det(\lambda_a). \end{aligned}$$

Proposition 244. *Für eine endliche Erweiterung L/K vom Grad $d = [L : K]$ gilt:*

(1) Die Spur $\mathrm{tr}_{L/K}$ ist eine K-lineare Abbildung.

(2) Für alle $x \in K$ gilt

$$\mathrm{tr}_{L/K}(x) = dx.$$

(3) Die Norm $N_{L/K}$ ist multiplikativ.

(4) Insbesondere ist

$$N_{L/K} : L^\times \to K^\times$$

ein Gruppenhomomorphismus.

(5) Für alle $x \in K$ gilt

$$N_{L/K}(x) = x^d.$$

(6) Das Charakteristische Polynom hat die Form

$$\chi_a(T) = T^d - \mathrm{tr}_{L/K}(a)T^{d-1} + \ldots + (-1)^d N_{L/K}(a).$$

Beweis. Die Spur von K-linearen Abbildungen ist linear und die Determinante ist multiplikativ. Daher gilt mit $a, b \in L$ und $x, y \in K$

$$\begin{aligned} \mathrm{tr}_{L/K}(xa + yb) &= \mathrm{tr}(\lambda_{xa+yb}) = \mathrm{tr}(x\lambda_a + y\lambda_b) \\ &= x \cdot \mathrm{tr}(\lambda_a) + y \cdot \mathrm{tr}(\lambda_b) = x \cdot \mathrm{tr}_{L/K}(a) + y \cdot \mathrm{tr}_{L/K}(b), \end{aligned}$$

und

$$N_{L/K}(ab) = \det(\lambda_{ab}) = \det(\lambda_a\lambda_b) = \det(\lambda_a)\det(\lambda_b) = N_{L/K}(a)N_{L/K}(b).$$

Da für $a \neq 0$ die Abbildung λ_a bijektiv ist, nimmt die Norm auf $L^\times$ Werte in $K^\times$ an.

Die Aussage über das charakteritische Polynom sind Standard in linearer Algebra. Die Aussagen im Fall $x \in K$ sind trivial, weil dann $\lambda_x = x \cdot \mathrm{id}_L$ gilt. □

Satz 245. *Sei L/K eine endliche Erweiterung und Ω eine algebraisch abgeschlossene Erweiterung von K. Seien*

$$\sigma_1, \ldots, \sigma_r : L \to \Omega$$

die $r = [L : K]_s$ vielen K-Einbettungen von L nach Ω. Dann gilt für alle $a \in L$

(1) $\operatorname{tr}_{L/K}(a) = [L : K]_i \cdot \sum_{i=1}^r \sigma_i(a)$,

(2) $N_{L/K}(a) = (\prod_{i=1}^r \sigma_i(a))^{[L:K]_i}$.

Insbesondere sind die Elemente von Ω, welche auf der rechten Seite stehen schon in K enthalten.

Wenn L/K sogar endlich galoissch ist, dann entfallen Faktor/Exponent $[L : K]_i$ und Summe/Produkt laufen über die Elemente von $\operatorname{Gal}(L/K)$.

Beweis. Wir betrachten zunächst einen Spezialfall: $L = K(\alpha)$ und $a = \alpha$. Zur Abkürzung setzen wir $q = [L : K]_i$, das ist eine Potenz von $p = \operatorname{char}(K)$. Dann wird die maximale separable Zwischenerweiterung von

$$\alpha^q$$

erzeugt (siehe Satz 172), und dieses Element hat Minimalpolynom

$$P_{\alpha^q/K} = \prod_{i=1}^r (T - \sigma_i(\alpha^q)).$$

Das Minimalpolynom von α lautet dann

$$\chi_{\alpha,L/K} = P_{\alpha/K} = P_{\alpha^q/K}(T^q) = \prod_{i=1}^r (T^q - \sigma_i(\alpha^q)) = \left(\prod_{i=1}^r (T - \sigma_i(\alpha))\right)^q.$$

Die Behaupteten Formeln für Norm und Spur folgen per Koeffizientenvergleich.

Den allgemeinen Fall führen wir nun mittels den Aussagen von Korollar 246 auf den Spezialfall zurück. Da wir Korollar 246 aber mittels Satz 245 beweisen werden, müssen wir einen Beweis führen.

Sei $a \in L$ beliebig. Wir setzen $M = K(a)$. Wir betrachten die K-Basis $1, a, \ldots, a^{m-1}$ von M und wählen eine M-Basis $y_1, \ldots, y_n$ von L. Dann sind die Produkte $a^i y_j$ für $1 \leq i \leq m$, $1 \leq j \leq n$ eine K-Basis von L.

Die Abbildung $\lambda_a \in \operatorname{End}_K(L)$ hat in der gewählten Basis eine Matrix in Blockdiagonalgestalt, und zwar hat jeder Block die Matrix von $\lambda_a \in \operatorname{End}_K(M)$ in der gewählten Basis. Dann lesen wir ab:

$$\operatorname{tr}_{L/K}(a) = [L : M] \cdot \operatorname{tr}_{M/K}(a),$$
$$N_{L/K}(a) = \left(N_{M/K}(a)\right)^{[L:M]}.$$

Die Restriktion von L nach $M = K(a)$ liefert eine surjektive Abbildung

$$\operatorname{Hom}_K(L, \Omega) \to \operatorname{Hom}_K(M, \Omega)$$

deren Fasern alle die Mächtigkeit $[L : M]_s$ haben, denn der Separabilitätsgrad ist unabhängig von der Wahl der Einbettung $\tau : M \to \Omega$. Nun rechnen wir:

$$\begin{aligned}
\operatorname{tr}_{L/K}(a) &= [L : M] \cdot \operatorname{tr}_{M/K}(a) = [L : M] \cdot [M : K]_i \cdot \sum_{\tau : M \to \Omega} \tau(a) \\
&= [L : K]_i \cdot [L : M]_s \cdot \sum_{\tau : M \to \Omega} \tau(a) \\
&= [L : K]_i \cdot \sum_{\tau : M \to \Omega} \Big(\sum_{\sigma : L \to \Omega,\ \sigma|_M = \tau} \sigma(a) \Big) = [L : K]_i \cdot \sum_{\sigma : L \to \Omega} \sigma(a).
\end{aligned}$$

Die Formel für die Norm folgt analog durch die gleiche Rechnung in multiplikativer Form.

$$N_{L/K}(a) = \big(N_{M/K}(a)\big)^{[L:M]} = \big(\prod_{\tau:M\to\Omega} \tau(a)\big)^{[L:M]\cdot[M:K]_i}$$
$$= \left(\prod_{\tau:M\to\Omega} \tau(a)^{[L:M]_s} \right)^{[L:K]_i} = \left(\prod_{\sigma:L\to\Omega} \sigma(a) \right)^{[L:K]_i}.$$

Die Indizes σ und τ laufen dabei über sämtliche K-lineare Einbettungen nach Ω. ☐

Korollar 246 (Transitivität). *Sei $L/M/K$ ein Körperturm endlicher Erweiterungen. Dann gilt:*

(1) $\mathrm{tr}_{L/K} = \mathrm{tr}_{M/K} \circ \mathrm{tr}_{L/M}$,
(2) $N_{L/K} = N_{M/K} \circ N_{L/M}$.

Beweis. Das folgt sofort aus Satz 245, denn

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

und für Ω algebraische abgeschlossene Erweiterung von K und $a \in L$ beliebig:

$$\mathrm{tr}_{L/K}(a) = [L : K]_i \cdot \sum_{\sigma:L\to\Omega} \sigma(a) = [M : K]_i \cdot \sum_{\tau:M\to\Omega} \Big([L : M]_i \cdot \sum_{\sigma:L\to\Omega,\ \sigma|_M=\tau} \sigma(a)\Big)$$
$$= [M : K]_i \cdot \sum_{\tau:M\to\Omega} \tau(\mathrm{tr}_{L/M}(a)) = \mathrm{tr}_{M/K}(\mathrm{tr}_{L/M}(a)),$$

wobei wir im entscheidenden Schritt die L/M-Spur von a über die Einbettung $\tau : M \to \Omega$ ausrechnen (das geht auch!) und daher $\tau(\mathrm{tr}_{L/M}(a)) \in \Omega$ erhalten.

Die Rechnung für die Norm geht genauso nur multiplikativ. ☐

Korollar 247. *Sei L/K eine endliche Erweiterung und $\alpha \in L$ beliebig mit*

$$P_{\alpha,L/K} = T^d - a_1T^{d-1} + \ldots + (-1)^d a_d \in K[T].$$

Dann gilt

(1) $\mathrm{tr}_{L/K}(\alpha) = \frac{[L:K]}{d} \cdot a_1$,
(2) $N_{L/K}(\alpha) = (a_d)^{[L:K]/d}$.

Beweis. Das folgt sofort aus Korollar 246 für $M = K(\alpha)$ und Proposition 244 (6). ☐

Satz 248. *Die Norm für Erweiterungen endlicher Körper ist surjektiv.*

Beweis. Das ist eine Übungsaufgabe. ☐

13.2. Die Spurform.

Definition 249. Sei L/K eine endliche Körpererweiterung. Die **Spurform** von L/K ist die symmetrische Bilinearform auf dem K-Vektorraum L definiert durch

$$L \times L \to K$$
$$(a, b) \mapsto \mathrm{tr}_{L/K}(ab).$$

Satz 250. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(a) *L/K ist separabel.*
(b) $\mathrm{tr}_{L/K} \neq 0$.
(c) *Die Spur ist surjektiv.*
(d) *Die Spurform ist nichtausgeartet.*

Beweis. (a) $\iff$ (b): Wenn L/K separabel ist, dann ist

$$\mathrm{tr}_{L/K} = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma$$

die Summe aller Charaktere. Diese sind linear unabhängig. Demnach ist ihre Summe nicht die Nullabbildung: es gibt ein $a \in L$ mit $\mathrm{tr}_{L/K} \neq 0$.

Wenn L/K inseparabel ist, dann ist $[L:K]_i$ ein Vielfaches der Charakteristik von K, somit gilt $[L:K]_i = 0$ in K. Die Spur ist dann nach Satz 245 die Nullabbildung.

(b) $\iff$ (c): Die Spur ist eine K-Linearform. Daher ist sie surjektiv genau dann, wenn sie von 0 verschieden ist.

(b) $\iff$ (d): Sei $\mathrm{tr}_{L/K}(a) \neq 0$ für ein $a \in L$. Dann ist die Spurform nichtausgeartet, da zu jedem $0 \neq x \in L$ gilt

$$\mathrm{tr}_{L/K}(x \cdot ax^{-1}) = \mathrm{tr}_{L/K}(a) \neq 0.$$

Umgekehrt, wenn die Spurform nichtausgeartet ist, dann ist insbesondere die Spur nicht die Nullabbildung. □

Übungsaufgaben zu §13

Übungsaufgabe 13.1 (Normalbasensatz und Spur). Sei L/K galoissch, und sei $\alpha \in L$ ein Erzeuger einer Normalbasis. Zu $H \subseteq \mathrm{Gal}(L/K)$ setzen wir

$$\alpha_H = \mathrm{tr}_{L/L^H}(\alpha)$$

Zeigen Sie die folgenden Aussagen.

(1) $L^H = K(\alpha_H)$.

(2) Wenn $N \lhd \mathrm{Gal}(L/K)$ ein Normalteiler ist, dann erzeugt α_N eine Normalbasis für L^N/K.

Übungsaufgabe 13.2 (duale Basis bzgl. Spurform). Sei $L = K(\alpha)$ von einem Element α mit separablem Minimalpolynom $f \in K[X]$ erzeugt.

(1) Bestimmen Sie

$$\mathrm{tr}_{L/K}\big(\alpha^i / f'(\alpha)\big)$$

für $0 \leq i < \deg(f)$.

Tipp: Partialbruchzerlegung von $1/f(X)$, Substitution $Y = 1/X$ und Potenzreihenentwicklung in $Y = 0$.

(2) Sei $\sum_{i=0}^{\deg(f)-1} \beta_i X^i$ das Polynom $\frac{f(X)}{X-\alpha} \in L[X]$. Zeigen Sie, daß $\beta_i / f'(\alpha)$ mit $0 \leq i < \deg(f)$ die Dualbasis von $1, \alpha, \ldots, \alpha^{\deg(f)-1}$ bezüglich der Spurform ist.

Tipp: Definieren Sie die Spur eines Polynoms aus $L[X]$ und berechnen Sie

$$\mathrm{tr}_{L/K}\big(\alpha^i / f'(\alpha) \cdot \sum_j \beta_j X^j\big).$$

14. Kreisteilungskörper

14.1. **Einheitswurzeln.** In diesem Kapitel behandeln wir Torsion in der multiplikativen Gruppe eines Körpers.

Definition 251. Eine **Einheitswurzel** ist ein Element ζ eines Rings R, so daß $\zeta^n = 1$ für ein $0 < n \in \mathbb{N}$. Man spricht genauer von einer n-ten Einheitswurzel, wenn $\zeta^n = 1$ gilt.

Eine Einheitswurzel ist stets eine Einheit, denn aus $\zeta^n = 1$ folgt

$$\zeta \cdot \zeta^{n-1} = 1.$$

Einheitswurzeln sind also nichts anderes als die Elemente der Einheitengruppe $R^\times$ von endlicher Ordnung.

Wir bezeichnen die Menge der n-ten Einheitswurzeln im Körper K mit

$$\mu_n(R) = \{\alpha \in R^\times \ ; \ \alpha^n = 1\},$$

und alle Einheitswurzeln mit

$$\mu_\infty(R) = \{\alpha \in R^\times \ ; \ \alpha^n = 1 \text{ für eine } 0 < n \in \mathbb{N}\}.$$

Satz 252. *Sei R ein Integritätsring und $n \in \mathbb{N}$. Dann ist $\mu_n(R)$ eine endliche zyklische Untergruppe von $R^\times$. Die Ordnung von $\mu_n(R)$ ist ein Teiler von n.*

Beweis. Mit $\zeta, \xi \in \mu_n(R)$ ist auch $\zeta\xi, \zeta^{-1} \in \mu_n(R)$. Daher ist $\mu_n(R) \subseteq R^\times$ eine Untergruppe. Als Nullstellen des Polynoms $T^n - 1$ gibt es davon in einem Integritätsring nur eindlich viele, Satz 66.

Sei K der Quotientenkörper von R. Dann ist $\mu_n(R) \subseteq K^\times$ eine endliche Untergruppe und daher nach Theorem 117 zyklisch. Sei $N = \#\mu_n(R)$ und $\zeta \in \mu_n(R)$ ein Erzeuger. Dann gilt $\zeta^n = 1$ und ζ hat Ordnung N, also $N \mid n$. □

Beispiel 253. (1) Für $\mathbb{C}$ kennen wir die Einheitswurzeln:

$$\mu_n(\mathbb{C}) = \left\{ e^{2\pi i \frac{a}{n}} \ ; \ a = 0, \ldots, n-1 \right\},$$

denn dies sind alles n-te Einheitswurzeln, und auch schon die maximal mögliche Anzahl derselben. Ein offensichtlicher Erzeuger der Gruppe ist

$$e^{2\pi i/n}.$$

Dies sind spezielle Funktionswerte[12] einer wichtigen analytischen Funktion.

(2) Für $\mathbb{C}$ können wir sogar die Gruppe aller Einheitswurzeln beschreiben. Die Abbildung

$$\mathbb{Q}/\mathbb{Z} \to \mu_\infty(\mathbb{C})$$
$$a/n \mapsto e^{2\pi i \frac{a}{n}}$$

ist ein Gruppenisomorphismus.

(3) In einem endlichen Körper $\mathbb{F}$ sind alle Elemente $x \neq 0$ Einheitswurzeln: die multiplikative Gruppe $\mathbb{F}^\times$ ist endlich, somit hat x endliche Ordnung.

Beispielsweise gilt für $\mathbb{F} = \mathbb{F}_q$

$$\mu_{q-1}(\mathbb{F}_q) = \mathbb{F}_q^\times$$

Allerdings gibt es hier keinen offensichtlichen Erzeuger dieser zyklischen Gruppe.

(4) Sei K ein Körper der Charakteristik $p > 0$. Dann ist

$$\mu_p(K) = 1.$$

In der Tat folgt aus $\zeta^p = 1$ schon $(\zeta - 1)^p = 0$, und daher in einem Körper $\zeta = 1$.

(5) Sei K eine Körper und $\mu_n(K) = \langle \zeta \rangle \neq 1$. Der Ring $R = K \times K$ ist kein Integritätsring und Satz 252 gilt nicht: $\mu_n(R) = \mu_n(K) \times \mu_n(K)$ ist nicht zyklisch.

Lemma 254. *Sei K ein Körper der Charakteristik $p > 0$ und $n = p^e \cdot m$ mit $p \nmid m$. Dann ist*

$$\mu_n(K) = \mu_m(K).$$

Beweis. Nach dem chinesischen Restsatz gilt

$$\mu_n(K) = \mu_m(K) \times \mu_{p^e}(K).$$

In obigem Beispiel haben wir $\mu_p(K) = 1$ und damit auch $\mu_{p^e}(K) = 1$ gesehen. □

Für Körper der Charakteristik $p > 0$ soll man sich deshalb auf Einheitswurzeln mit zu p teilerfremder Ordnung beschränken.

[12]Diesem Motiv begegnet man wiederholt: Analysis und Arithmetik sind über die spezielle Werte spezieller Funktionen miteinander verwoben.

14.2. **Das Kreisteilungspolynom.**

Definition 255. Eine **primitive** n-te Einheitswurzel, ist eine Einheitswurzel ζ der Ordnung n.

Bemerkung 256. Sei R ein Integritätsring. Die primitven n-ten Einheitswurzeln sind genau die Erzeuger von $\mu_n(R)$ sofern $\mu_n(R)$ maximale Ordnung n hat. Dies ist zum Beispiel für algebraisch abgeschlossene Körper der Fall, wenn die Charakteristik kein Teiler von n ist.

Definition 257. Sei $n \in \mathbb{N}$ und $\bar{\mathbb{Q}}$ ein algebraisher Abschluß von $\mathbb{Q}$. Das n-te Kreisteilungspolynom ist

$$\Phi_n(T) = \prod_{\zeta \in \mu_n(\bar{\mathbb{Q}}) \text{ primitiv}} (T - \zeta).$$

Satz 258. *(1)* $\Phi(T)$ *ist unabhängig vom gewählten algebraischen Abschluß* $\bar{\mathbb{Q}}$.
(2) *Es gilt* $\Phi_n(T) \in \mathbb{Z}[T]$.
(3) $\Phi_n(T)$ *läßt sich rekursiv berechnen durch*

$$T^n - 1 = \prod_{d|n} \Phi_d(T) \tag{14.1}$$

(4) $\deg(\Phi_n) = \varphi(n)$, *mit* $\varphi(-)$ *der Eulerschen* φ*-Funktion*

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

Beweis. (4) Da wir in Charakteristik 0 sind, gilt

$$\mu_n(\bar{\mathbb{Q}}) \simeq \mu_n(\mathbb{C}) \simeq \mathbb{Z}/n\mathbb{Z}.$$

Es gibt daher genau

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

viele Erzeuger von $\mathbb{Z}/n\mathbb{Z}$, also primitive n-te Einheitswurzeln. Das ist der Grad von $\Phi_n(T)$.

(3) Jede n-te Einheitswurzel ist primitive d-te Einheitswurzel für genau ein d mit $d \mid n$. Daher:

$$T^n - 1 = \prod_{\zeta \in \mu_n} (T - \zeta) = \prod_{d|n} \Big(\prod_{\zeta \in \mu_n, \mathrm{ord}(\zeta) = d} (T - \zeta) \Big) = \prod_{d|n} \Phi_d(T).$$

(2) Dies zeigen wir per Induktion nach n zusammen mit der offensichtilichen Behauptung, daß $\Phi_n(T)$ normiert ist und daher Inhalt $c(\Phi_n) = 1$ hat. Nun ist nach (3)

$$\Phi_n(T) = \frac{T^n - 1}{\prod_{d|n,\ d<n} \Phi_d(T)} \in \mathbb{Q}[T]$$

mit Inhalt

$$c(\Phi_n) = \frac{c(T^n - 1)}{\prod_{d|n, d<n} c(\Phi_d)} = 1$$

insbesondere $\Phi_n \in \mathbb{Z}[T]$.

(1) Ein Isomorphismus von algebraischen Abschlüssen bildet primitive n-te Einheitswurzeln bijektiv auf ebensolche ab. Daher wird auch $\Phi_n(T)$ entsprechend abgebildet. Da die Koeffizienten aus $\mathbb{Z}$ sind, bleiben sie erhalten. Damit ist Φ_n unabhängig von der Wahl. □

Proposition 259. *(1)* *Für alle* $n \in \mathbb{N}$ *gilt:*

$$n = \sum_{d|n} \varphi(d)$$

(2) *Für eine Primzahl* p *und* $m \in \mathbb{N}$ *gilt*

$$\varphi(p^m) = (p-1)p^{m-1}.$$

(3) *Für teilerfremde* n *und* m *gilt*

$$\varphi(nm) = \varphi(n)\varphi(m).$$

(4) *Für $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^r p_i^{m_i}$ gilt*

$$\varphi(n) = \prod_{i=1}^r (p_i - 1)p_i^{m_i-1}.$$

Beweis. (1) folgt durch Gradvergleich aus (14.1).

(2) Erzeuger in $\mathbb{Z}/p^m\mathbb{Z}$ sind die zu p^m teilerfremden Restklassen, also diejenigen, die von nicht durch p teilbaren Elementen aus $\mathbb{Z}$ repräsentiert sind. Davon gibt es genau $p^m - p^{m-1}$ viele.

(3) folgt aus dem chinesischen Restsatz und die Einschränkung auf die Einheitengruppe

$$(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

Und (4) folgt sofort aus (2) und (3). □

14.3. **Die Kreisteilungskörper.** In einem Körper K gilt

$$\mu_n(K) = \mathrm{NS}_{T^n-1}(K).$$

Damit wird die Algebra der Einheitswurzeln durch das Polynom $T^n - 1$ beherrscht. Wir wollen nun studieren, wie sich $T^n - 1$ in irreduzible Faktoren zerlegt. Das hängt natürlich von K ab.

Den Zerfällungskörper von $T^n - 1$ über K bezeichnen wir mit

$$K(\mu_n).$$

Dieser entsteht, in dem man in einem algebraischen Abschluß $\overline{K}/K$ die Gruppe $\mu_n = \mu_n(\overline{K})$ der n-ten Einheitswurzeln in $\overline{K}$ zu K adjungiert.

Lemma 260. *Sein $n \in \mathbb{N}$ und Z eine zyklische Gruppe der Ordnung n. Dann gibt es einen kanonische Ringisomorphismus*

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(Z)$$
$$a \mapsto [a] = (x \mapsto a \cdot x).$$

und einen kanonischen Gruppenisomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(Z)$$
$$a \mapsto [a] = (x \mapsto a \cdot x).$$

Beweis. Sei $\zeta \in Z$ ein Erzeuger. Dann ist jeder Endomorphismus $\varphi : Z \to Z$ durch den Wert $\varphi(\zeta)$ eindeutig bestimmt. Da ζ erzeugt, gibt es ein $a \in \mathbb{Z}$ mit $\varphi(\zeta) = a \cdot \zeta$ in additiver Schreibweise. Damit gilt für alle $x \in \mathbb{Z}$

$$\varphi(x \cdot \zeta) = x \cdot \varphi(\zeta) = ax \cdot \zeta = a \cdot (x \cdot \zeta).$$

Somit ist jeder Endomorphismus von der Form $[a]$ für ein $a \in \mathbb{Z}$. Offensichtlich hängt dies nur von der Restklasse modulo $n\mathbb{Z}$ ab, und die Zuordnung

$$a \mapsto [a]$$

ist ein Ringhomomorphismus. Fehlt nur noch die Injektivität: wenn $[a] = 0$, dann $[a]\zeta = a \cdot \zeta = 0$. Weil ζ ein Erzeuger ist, also Ordnung n hat, bedeutet dies $n \mid a$.

Die Aussage über Automorphismen ergibt sich sofort. □

Bemerkung 261. Es ist bemerkenswert, daß die Beschreibung von $\mathrm{Aut}(Z)$ nicht von der Wahl eines Erzeugers ζ von Z abhängt.

Satz 262. *Sei K ein Körper und $n \in \mathbb{N}$ ein Vielfaches von* $\mathrm{char}(K)$. *Dann gilt*

(1) *Die Erweiterung $K(\mu_n)/K$ ist galoissch.*

(2) *Die Abbildung*

$$\chi_n : \mathrm{Gal}(K(\mu_n)/K) \to \mathrm{Aut}(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma \mapsto \sigma|_{\mu_n}$$

ist ein injektiver Gruppenhomomorphismus. Insbesondere hat $K(\mu_n)/K$ eine abelsche Galoisgruppe.

(3) *Für $K = \mathbb{Q}$ ist χ_n ein Isomorphismus.*

Bemerkung 263. Den Gruppenhomomorphismus χ_n aus Satz 262 nennt man den **zyklotomischen Charakter (modulo n)**.

Beweis. (1) Die Erweiterung $K(\mu_n)/K$ ist per Definition ein Zerfällungskörper, also normal. Die Erzeuger sind Nullstellen von $f = T^n - 1$, dessen Ableitung

$$f' = nT^{n-1}$$

nur die Nullstellen $T = 0$ hat (nach Voraussetzung ist $n \neq 0$). Damit sind f und f' teilerfremd, somit f und $K(\mu_n)/K$ separabel. Separabel und normal bedeutet galoissch.

(2) Da μ_n genau die Nullstellen des Polynoms $T^n - 1$ sind, dessen Zerfällungskörper wir betrachten, ist jedes $\sigma \in \mathrm{Gal}(K(\mu_n)/K)$ eindeutig durch seine Wirkung auf den Nullstellen bestimmt. Damit ist χ_n injektiv. Da die Gruppenverknüpfung in μ_n die Körpermultiplikation ist, wird diese von $\sigma|_{\mu_n}$ erhalten. Die Abbildung χ_n ist damit wohldefiniert, denn die Werte sind tatsächlich Gruppenautomorphismen von μ_n.

(3) Wir müssen zeigen, daß es zu jedem $a \in \mathbb{Z}$ teilerfremd zu n ein $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ gibt, so daß

$$\sigma_a|_{\mu_n} = [a]$$

die Multiplikation mit a auf $\mathbb{Z}/n\mathbb{Z}$ ist (multiplikativ in μ_n ist das die Potenzierung mit a). Da Primzahlen $p \nmid n$ die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ erzeugen, reicht es aus, σ_p für solche p zu konstruieren.

Wir fixieren nun eine Primzahl $p \nmid n$. Sei $\zeta \in \mu_n$ ein Erzeuger. Dann suchen wir ein Element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ mit

$$\sigma(\zeta) = \zeta^p. \tag{14.2}$$

Dieses Element wird in der Zahlentheorie aus naheliegenden Gründen Frobeniuselement für die Primzahl p genannt. Es überrascht daher nicht, daß wir zur Konstruktion modulo p reduzieren. Sei

$$T^n - 1 = g(T)h(T)$$

mit g irreduzibel und $g(\zeta) = 0$. Nach dem Gauß-Lemma, genauer Lemma 196, kann man g und h so skalieren, daß die Koeffizienten ganzzahlig werden:

$$g, h \in \mathbb{Z}[T].$$

Da $T^n - 1$ normiert ist, müssen dann die führenden Koeffizienten von g und h entweder 1 oder -1 sein. Wir skalieren so, daß g und h auch normiert sind. Dann ist $g = P_{\lambda/\mathbb{Q}}$ das Minimalpolynom.

Nach den Sätzen über Körpereinbettungen und Nullstellen gibt es ein σ mit (14.2) genau dann, wenn ζ^p auch eine Nullstelle von g ist. Dies beweisen wir durch Widerspruch. Da ζ^p auch eine Nullstelle von $T^n - 1$ ist, gilt ansonsten nämlich

$$h(\zeta^p) = 0.$$

Damit ist ζ eine Nullstelle von $h(T^p)$ und der ggT

$$d(T) = \mathrm{ggT}(g(T), h(T^p))$$

ist nicht konstant. Wieder nach dem Lemma 196 dürfen wir annehmen, daß $d(Y) \in \mathbb{Z}[T]$ normiert ist. Jetzt reduzieren wir koeffizientenweise modulo p, das heißt wir bilden die Polynome mittels

$$\mathbb{Z}[T] \to \mathbb{F}_p[T]$$
$$F \mapsto \bar{F}$$

ab. Dann gilt

$$\overline{h(T^p)} = \bar{h}(T)^p$$

und $\bar{d}$ ist gemeinsamer Teiler von $\bar{g}$ und $\bar{h}^p$. Da d normiert ist, bleibt $\bar{d}$ nicht konstant, somit haben $\bar{g}$ und $\bar{h}$ einen nichttrivialen gemeinsamen Teiler. Wir schließen, daß

$$T^n - 1 = \bar{g}\bar{h}$$

eine mehrfache Nullstelle hat. Da aber weiterhin die Ableitung nT^{n-1} nur die Nullstelle $T = 0$ hat, ist $T^n - 1 \in \mathbb{F}_p[T]$ weiterhin separabel, also ohne mehrfache Nullstelle, Widerspruch! □

Korollar 264. *(1) Für jedes n ist $\Phi_n(T)$ irreduzibel über $\mathbb{Q}$.*
(2) $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$.

Beweis. Eine primitive n-te Einheitswurzel ζ_n ist ein primitives Element für $\mathbb{Q}(\mu_n)/\mathbb{Q}$. Darüberhinaus gilt

$$\Phi_n(\zeta_n) = 0.$$

Also gilt

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = [\mathbb{Q}(\mu_n) : \mathbb{Q}] = \deg(P_{\zeta_n/\mathbb{Q}}) \leq \deg(\Phi_n) = \varphi(n),$$

und dies zeigt (2), sodann $\Phi_n = P_{\zeta_n/\mathbb{Q}}$ und damit (1). □

Übungsaufgaben zu §14

Übungsaufgabe 14.1. Bestimmen Sie alle Zwischenkörper zu $\mathbb{Q}(\mu_{12})/\mathbb{Q}$.

Übungsaufgabe 14.2 (Beispiele für Galoiserweiterungen mit Galoisgruppe $\mathbb{Z}/6\mathbb{Z}$). Bestimmen sie alle Kreisteilungskörper $\mathbb{Q}(\mu_n)$ vom Grad 6 über $\mathbb{Q}$. Warum gilt dann $\operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$?

Übungsaufgabe 14.3. Sei $n, m \geq 1$ teilerfremd. Zeigen Sie:

(a) $\mathbb{Q}(\mu_{nm}) = \mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m)$ und die natürlichen Projektionen definieren einen Isomorphismus

$$\operatorname{Gal}(\mathbb{Q}(\mu_{nm})/\mathbb{Q}) \xrightarrow{\sim} \operatorname{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \times \operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}).$$

(b) $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}$, wobei der Schnitt in $\mathbb{Q}(\mu_{nm})$ stattfindet.

Übungsaufgabe 14.4 (Kreisteilungskörper über einem endlichen Körper). Sei p eine Primzahl $\mathbb{F}_q$ ein endlicher Körper der Charakteristik p und $p \nmid n$. Beschreiben Sie das Bild des zyklotomischen Charakters

$$\chi_n : \operatorname{Gal}(\mathbb{F}_q(\mu_n)/\mathbb{F}_q) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

Für welche n ist das n-te Kreisteilungspolynom $\Phi_n(T)$ nach Reduktion modulo p, also in $\mathbb{F}_p[T]$ irreduzibel?

Übungsaufgabe 14.5. Sei K eine endliche Körpererweiterung von $\mathbb{Q}$. Zeigen Sie, daß K nur endlich viele Einheitswurzeln enthält.

Übungsaufgabe 14.6. Es sei ζ_n eine primitive n-te Einheitswurzel.

(1) Bestimmen sie für eine Primzahl p und für $m \in \mathbb{N}$ das Kreisteilungspolynom $\Phi_{p^m}(T)$.
(2) Berechnen Sie $\operatorname{tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$ für $n \in \mathbb{N}$.
(3) Zeigen Sie

$$N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1 - \zeta_n) = \begin{cases} p & \text{falls } n = p^m \text{ eine Primpotenz,} \\ 1 & \text{sonst.} \end{cases}$$

Übungsaufgabe 14.7 (Zyklotomisches Eulersystem).

(1) Zeigen Sie, daß es ein System $(\zeta_n)_{n\in\mathbb{N}}$ von primitiven n-ten Einheitswurzeln

$$\zeta_n \in \mathbb{Q}(\mu_n)^\times$$

gibt, so daß für alle $n, m \in \mathbb{N}$ gilt

$$(\zeta_{nm})^m = \zeta_n.$$

(2) Sei p nun eine fixierte Primzahl und $(\zeta_n)_{n\in\mathbb{N}}$ ein System wie in (1). Für $n > 1$ sei

$$c_n := (1 - \zeta_n) \in \mathbb{Q}(\mu_n)^\times.$$

Für eine Primzahl $\ell \nmid n$ sei

$$\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$$

der Automorphismus der unter dem zyklotomischen Charakter χ_n von Satz 262 auf

$$\chi_n(\sigma_\ell) = \ell \in (\mathbb{Z}/n\mathbb{Z})^\times$$

abgebildet wird. Zeigen Sie, daß für alle $m \in \mathbb{N}$ und alle Primzahlen ℓ gilt:

$$N_{\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m)}(c_{\ell m}) = \begin{cases} c_m & \text{falls } \ell \mid m, \\ c_m/\sigma_\ell^{-1}(c_m) & \text{falls } \ell \nmid m \text{ und } m > 1, \\ \ell & m = 1. \end{cases}$$

Übungsaufgabe 14.8. Zeigen Sie, daß es zu jeder endlichen abelschen Gruppe A eine galoissche Erweiterung $K/\mathbb{Q}$ gibt mit $\mathrm{Gal}(K/\mathbb{Q}) \simeq A$. Zeigen Sie genauer, daß es davon unendlich viele (notwendigerweise abzählbar!) paarweise linear disjunkte Körper $K_i/\mathbb{Q}$ gibt, d.h. für $i \neq j$ gilt

$$K_i \cap K_j = \mathbb{Q}.$$

Tipp: Verwenden Sie Aufgabe 14.3 und den folgenden Spezialfall eines Satzes von Dirichlet. Zu jedem $n \in \mathbb{N}$ gibt es unendlich viele Primzahlen $p \equiv 1 \mod n$.

Teil 3. Themen der Gruppentheorie — Anwendungen der Galoistheorie

15. Die Sylowsätze

Fundamental für die Strukturtheorie endlicher Gruppen sind die Sylow-Sätze[13]. Wir folgen den Beweisen von Wielandt[14] aus dem Jahr 1959 (Publikationsdatum), deren zentrales Hilfsmittel Gruppenoperationen sind.

Definition 265. (1) Sei p eine Primzahl. Eine **p-Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

(2) Eine **Sylow-Untergruppe (Sylowgruppe)** ist eine Untergruppe $P \subseteq G$ einer endlichen Gruppe G der Ordnung eine Primzahlpotenz

$$|P| = p^r,$$

so daß $|G| = p^r m$ mit $p \nmid m$. Wenn man die Primzahl betonen möchte, spricht man von einer **p-Sylow-Untergruppe (p-Sylowgruppe)** von G.

Bemerkung 266. (1) Es folgt sofort aus dem Satz von Lagrange, daß eine p-Sylowuntergruppe von G bezüglich Inklusion unter allen Untergruppen von G, die p-Gruppen sind, maximal ist.

(2) Des weiteren folgt aus $p \nmid |G|$, daß eine p-Sylow Untergruppe von G die triviale Gruppe 1 ist. Die Theorie der p-Sylowgruppen ist nur für Primteiler p der Gruppenordnung interessant.

Theorem 267 (Sylow–Sätze, 1872)**.** *Sei G eine endliche Gruppe der Ordnung N und p ein Primteiler von N. Sei $N = p^r m$ mit $p \nmid m$.*

(1) Es gibt eine p-Sylowgruppe in G.
(2) Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.
(3) Je zwei p-Sylowgruppen von G sind konjugiert.
(4) Sei $a_p = a_p(G)$ die Anzahl der p-Sylowgruppen von G. Dann gilt
  - *(i) $a_p \mid |G|$,*
  - *(ii) $p \mid a_p - 1$.*

Bevor wir in den Beweis einsteigen benötigen wir ein paar Lemmata. Für eine natürliche Zahl N und eine Primzahl p erinnern wir an die p-adische diskrete Bewertung $v_p(-)$. Wir bezeichnen mit $v_p(N)$ denjenigen Exponenten r mit $p^r \mid N$ und $p^{r+1} \nmid N$.

Lemma 268. *Sei $n \in \mathbb{N}$ und p eine Primzahl. Sei*

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_r p^r$$

die Darstellung von n zur Basis p, also mit $0 \leq a_i \leq p-1$ für alle $0 \leq i \leq r$. Dann gilt

$$v_p(n!) = \frac{n - \sum_{i=0}^r a_i}{p-1}.$$

Beweis. Wir benutzen die Gauß-Klammer, die für jede natürliche Zahl n auf den reellen Zahlen $n \leq x < n+1$ den Wert

$$\lfloor x \rfloor = n$$

annimmt.

Von den n Faktoren $1, 2, \ldots, n$ in $n!$ sind $\lfloor \frac{n}{p^i} \rfloor$ durch p^i teilbar. Genau durch p^i teilbar sind demnach $\lfloor \frac{n}{p^i} \rfloor - \lfloor \frac{n}{p^{i+1}} \rfloor$ der Faktoren. Summieren wir diese Anzahl gewichtet mit i über alle über

[13] Peter Ludwig Mejdell Sylow, 1832–1918, norwegischer Mathematiker.
[14] Helmut Wielandt, 1910–2001, deutscher Mathematiker.

alle $i \geq 1$, so folgt (das sind endliche Summen!)

$$\begin{aligned}
v_p(n!) &= \sum_{i\geq 1} i(\lfloor \frac{n}{p^i} \rfloor - \lfloor \frac{n}{p^{i+1}} \rfloor) = \sum_{i\geq 1}(i-(i-1))\lfloor \frac{n}{p^i} \rfloor = \sum_{i\geq 1} \lfloor \frac{n}{p^i} \rfloor \\
&= \sum_{i\geq 1} a_i + a_{i+1}p + \ldots + a_r p^{r-i} \\
&= \sum_{i=1}^{r} a_i(1+p+\ldots+p^{i-1}) \\
&= \sum_{i=1}^{r} a_i \frac{p^i-1}{p-1} = \sum_{i=0}^{r} a_i \frac{p^i-1}{p-1} \\
&= \frac{1}{p-1}(\sum_{i=0}^{r} a_i p^i - \sum_{i=0}^{r} a_i) = \frac{n - \sum_{i=0}^{r} a_i}{p-1}.
\end{aligned}$$

□

Lemma 269. *Sei $N \in \mathbb{N}$ und $r = v_p(N)$. Dann ist $\binom{N}{p^r}$ nicht durch p teilbar.*

Beweis. Sei $N = a_r p^r + a_{r+1}p^{r+1} \ldots + a_m p^m$ die Darstellung von N zur Basis p. Dann ist $a_r \geq 1$ und daher

$$N - p^r = (a_r - 1)p^r + a_{r+1}p^{r+1} \ldots + a_m p^m$$

die Darstellung von $N - p^r$ zur Basis p. Es gilt

$$\binom{N}{p^r} = \frac{N!}{(N-p^r)!p^r!}$$

und daher

$$\begin{aligned}
v_p(\binom{N}{p^r}) &= v_p(N!) - v_p(N-p^r) - v_p(p^r!) \\
&= \frac{N - \sum_{i=r}^{m} a_i}{p-1} - \frac{(N-p^r) - (\sum_{i=r}^{m} a_i) + 1}{p-1} - \frac{p^r - 1}{p-1} = 0.
\end{aligned}$$

Das war zu zeigen. □

Definition 270. Ein **Fixpunkt** für eine Gruppenoperation der Gruppe G auf der Menge X ist ein Element $x \in X$ mit

$$g.x = x$$

für alle $g \in G$. Die Menge aller Fixpunkte bezeichnen wir mit

$$\mathrm{Fix}(X;G) := \{x \in X \ ; \ \text{ für alle } g \in G \text{ gilt } g.x = g\}.$$

Satz 271 (Fixpunktsatz)**.** *Sei p eine Primzahl und P eine endliche p-Gruppe. Sei X eine Menge mit P-Operation. Dann gilt*

$$|\,\mathrm{Fix}(X;P)| \equiv |X| \mod p.$$

Beweis. Dies folgt aus der Bahnenformel. Die Fixpunkte sind gerade die Bahnen der Länge 1. Daher ist $|X| - |\,\mathrm{Fix}(X;P)|$ die Summe der Bahnenlängen über alle Bahnen der Länge > 1. Diese Längen sind echte Teiler der Gruppenordnung, also durch p teilbar. □

Beweis von Theorem 267. (1) Wir zeigen nun die Existenz einer p-Sylow-Untergruppe. Sei G eine endliche Gruppe der Ordnung N, sei p eine Primzahl und $N = p^r m$ mit $p \nmid m$. Wenn $r = 0$ ist nichts zu tun. Sei daher $r \geq 1$. Sei

$$X = \{M \ ; \ M \subseteq G \text{ und } |M| = p^r\}$$

die Menge der p^r-elementigen Teilmengen. Da Translation eine freie Operation ist, gilt für jedes $g \in G$ und $M \in X$, daß

$$|gM| = |M|.$$

Daher operiert G auf X durch (Links-)Translation:

$$\begin{aligned} G \times X &\to X \\ (g, M) &\mapsto gM. \end{aligned}$$

Sei $M \in X$ beliebig. Wir zeigen nun, daß der Stabilisator G_M höchstens p^r Elemente hat. Dazu fixieren ein $x \in M$. Ein $g \in G_M$ ist dann eindeutig durch $gx \in M$ festgelegt als $g = (gx)x^{-1}$. Daher ist

$$|G_M| \leq |M| = p^r.$$

Wir suchen also ein $M \in X$ mit maximal möglichem Stabilisator. Wir arbeiten durch Widerspruch und nehmen an, daß alle Stabilisatoren G_M weniger als p^r Elemente haben. Es gilt nach dem Bahnensatz

$$p^r \mid |G| = |G_M| \cdot |G.M|.$$

Da $|G_M| < p^r$ gilt $p^r \nmid |G_M|$ und daher $p \mid |G.M|$. Es sind also alle Bahnen von durch p teilbarer Länge. Damit gilt

$$p \mid |X| = \binom{N}{p^r}$$

im Widerspruch zu Lemma 269. Also gibt es einen Stabilisator $P = G_M$ von Ordnung p^r. Dies ist die gesuchte p-Sylow-Untergruppe.

(2) Sei P eine p-Sylowgruppe von G, die es nach (1) gibt. Sei Q eine beliebige p-Untergruppe. Wir lassen Q auf G/P durch Linkstranslation operieren. Nach Satz 271 gilt

$$|\operatorname{Fix}(G/P, Q)| \equiv |G/P| = |G|/|P| = m \mod p$$

und ist daher nicht durch p teilbar. Es muß also einen Fixpunkt geben. Wenn gP von Q fixiert wird, dann ist

$$QgP = gP$$

oder äquivalent

$$Q \subseteq gPg^{-1}$$

Mit P hat auch gPg^{-1} genau p^r Elemente und ist eine p-Sylow-Untergruppe. Damit ist Q in einer p-Sylowgruppe enthalten.

(3) Sei P eine p-Sylowgruppe von G, die es nach (1) gibt. Sei Q eine beliebige p-Sylowgruppe. Der Beweis von (2) liefert ein $g \in G$ mit

$$Q \subseteq gPg^{-1}.$$

Da $|Q| = p^r = |gPg^{-1}|$ folgt Gleichheit. Je zwei p-Sylowgruppen sind also konjugiert.

(4) Wir lassen nun G durch Konjugation auf der Menge der p-Sylowgruppen

$$\mathfrak{P} = \{P \ ; \ P \text{ ist } p\text{-Sylowgruppe von } G\}$$

operieren. Diese Operation ist wohldefiniert, denn konjugierte Untergruppen haben die gleiche Ordnung. Nach (2) ist diese Operation transitiv und der Stabilisator von $P \in \mathfrak{P}$ ist der **Normalisator** von P in G

$$N_G(P) = \{g \in G \ ; \ gPg^{-1} = P\}.$$

Aus dem Satz von Lagrange folgt nun die Behauptung (i):

$$a_p = |\mathfrak{P}| = (G : N_G(P)) \mid |G|.$$

Nun sei Q eine beliebige p-Sylow-Untergruppe. Wir lassen Q auf $\mathfrak{P}$ durch Konjugation operieren. Dann gilt nach Satz 271

$$a_p \equiv |\operatorname{Fix}(\mathfrak{P}, Q)| = |\{P \in \mathfrak{P} \ ; \ Q \subseteq N_G(P)\}| \mod p.$$

Der Stabilisator $N_G(P)$ von P enthält P als normale Untergruppe. Ein p-Sylowgruppe von G, mit $Q \subseteq N_G(P)$ ist auch p-Sylowgruppe von $N_G(P)$, denn $|N_G(P)|$ teilt $|G|$ und wird daher nicht durch mehr p-Faktoren geteilt als $|G|$. Daher sind nach (2) angewandt auf $N_G(P)$ die Gruppen P und Q durch ein $g \in N_G(P)$ konjugiert! Dann gilt

$$Q = gPg^{-1} = P.$$

Die p-Sylowgruppe Q ist also der einzige Fixpunkt, somit

$$a_p \equiv 1 \mod p,$$

und das ist Aussage (ii). □

Korollar 272. *Je zwei p-Sylowgruppen von G sind zueinander isomorph.*

Beweis: Sind S_1 und S_2 zwei p-Sylowgruppen von G, dann gibt es nach Theorem 267 (2) ein $g \in G$ so daß

$$S_2 = gS_1g^{-1}. \tag{15.1}$$

Somit definert die Abbildung

$$\begin{aligned} g(-)g^{-1} : S_1 &\to S_2 \\ h &\mapsto ghg^{-1} \end{aligned}$$

einen Isomorphismus von S_1 mit S_2. In der Tat ist $g(-)g^{-1}$ als Einschränkung eines inneren Automorphismus von G injektiv und wegen (15.1) auch surjektiv. □

Korollar 273. *Eine p-Sylowgruppe ist ein Normalteiler von G genau dann, wenn $a_p(G) = 1$.*

Beweis: Ganz allgemein ist eine Untergruppe $H \leq G$ ein Normalteiler genau dann, wenn für alle $g \in G$ gilt

$$gHg^{-1} = H,$$

also wenn die Menge der zu H konjugierten Untergruppen nur aus H selbst besteht. Für eine p-Sylowgruppe $S \leq G$ besteht diese Menge nach Theorem 267 (2) genau aus der Menge aller p-Sylowgruppen von G. Somit ist S Normalteiler genau dann, wenn $a_p(G) = 1$. □

Übungsaufgaben zu §15

Übungsaufgabe 15.1. Zeigen Sie, daß jede Gruppe der Ordnung 15 zyklisch ist.

Übungsaufgabe 15.2. Seien p, q zwei verschiedene Primzahlen. Zeigen Sie, daß jede Gruppe der Ordnung pq einen Normalteiler hat.

Übungsaufgabe 15.3. Seien $p < q$ zwei Primzahlen mit $p \nmid q - 1$. Zeigen Sie, daß jede Gruppe der Ordnung pq zyklisch ist.

16. Endliche p-Gruppen

Wenn man endliche Gruppen von Ordnung $\leq N$ bis auf Isomorphie auszählt, dann sind die p-Gruppen deutlich die meisten.

16.1. Das Zentrum.

Definition 274. Wir erinnern an das **Zentrum** einer Gruppe G. Dies ist der abelsche Normalteiler

$$Z(G) = \{g \in G \ ; \ ghg^{-1} = h \text{ für alle } h \in G\}$$

aller Elemente, die mit allen Elementen von G vertauschen.

Satz 275. *Jede nichttriviale p-Gruppe hat nichttriviales Zentrum.*

Beweis. Sei $G \neq 1$ eine p-Gruppe. Wir lassen G auf sich selbst durch Konjugation operieren:

$$g.h = ghg^{-1}.$$

Das Zentrum $Z(G)$ besteht genau aus den Fixpunkten dieser Operation. Nach Satz 271 gilt daher

$$\#Z(G) \equiv \#G \equiv 0 \mod p.$$

Da $1 \in Z(G)$ gilt somit $1 \leq \#Z(G)$, also wenigstens $p \leq \#Z(G)$. □

Satz 276. *Sei G eine p-Gruppe und $H \subseteq G$ eine Untergruppe $H \neq G$. Dann ist H eine echte Untergruppe des Normalisators $N_G(H)$.*

Beweis. Wir führen den Beweis per Induktion nach der Ordnung von G. Wenn $\#G = 1$, dann ist nichts zu beweisen. Wir nehmen also an, daß der Satz für alle p-Gruppen kleinerer Ordnung als $\#G$ gilt.

Das Zentrum $Z = Z(G)$ ist nach Satz 275 nichttrivial. Außerdem ist $Z \subseteq N_G(H)$. Wenn $Z \not\subseteq H$, dann sind wir fertig. Andernfalls betrachten wir alles in der Faktorgruppe modulo dem Zentrum:

$$\overline{H} = H/Z \subseteq \overline{G} = G/Z.$$

Es gilt für $g \in G$ und sein Bild $\bar{g} \in \overline{G}$:

$$gHg^{-1} = H \iff \bar{g}\overline{H}\bar{g}^{-1} = \overline{H},$$

denn H und gHg^{-1} enthalten Z und werden so über ihr Bild in $\overline{G}$ beschrieben. Daher ist

$$N_{\overline{G}}(\overline{H}) = N_G(H)/Z$$

und nach dem Isomorphiesatz

$$N_G(H)/H \simeq \big(N_G(H)/Z\big)/\big(H/Z\big) = N_{\overline{G}}(\overline{H})/\overline{H}.$$

Letzteres ist $\neq 1$ per Induktion, da $\overline{G}$ kleinere Ordnung als G hat. Damit gilt der Satz auch für H in G. □

16.2. Filtrierungen.

Definition 277. (1) Eine **(endliche, fallende) Filtrierung** einer Gruppe G ist ein System $\mathrm{F}^\bullet(G) = \big(\mathrm{F}^i(G)\big)$ mit $i = 0, \ldots, n$ von Untergruppen

$$G = \mathrm{F}^0(G) \supseteq \mathrm{F}^1(G) \supseteq \ldots \supseteq \mathrm{F}^{n-1}(G) \supseteq \mathrm{F}^n(G) = 1.$$

Die Zahl n heißt **Länge** der Filtrierung.

(2) Eine **Subnormalreihe** (oder subnormale Filtrierung) einer Gruppe G ist eine Filtrierung $\mathrm{F}^\bullet(G)$, so daß jedes $\mathrm{F}^{i+1}(G)$ ein Normalteiler von $\mathrm{F}^i(G)$ ist. Die Quotienten

$$\mathrm{gr}^i_{\mathrm{F}}(G) := \mathrm{F}^i(G)/\mathrm{F}^{i+1}(G)$$

nennt man die **Faktoren** der Subnormalreihe (oder **Filtrationsquotienten** der Filtrierung).

(3) Eine **Normalreihe** (oder **normale** Filtrierung) einer Gruppe G ist eine Filtrierung $\mathrm{F}^\bullet(G)$, so daß jedes $\mathrm{F}^i(G)$ ein Normalteiler von G ist.

Der Gebrauch der Bezeichnung Subnormalreihe und Normalreihe ist leider in der Literatur nicht einheitlich. Manchmal wird eine Subnormalreihe schon als Normalreihe bezeichnet. In einer Normalreihe nach obiger Definition ist der i-te Faktor $\mathrm{F}^i(G)/\mathrm{F}^{i+1}(G)$ natürlich eine Untergruppe in $G/\mathrm{F}^{i+1}(G)$.

Satz 278. *In einer p-Gruppe G gibt es zu jeder Untergruppe $H \subseteq G$ eine subnormale Filtrierung $\mathrm{F}^\bullet(G)$ mit den folgenden Eigenschaften.*

(i) $\#\,\mathrm{F}^i(G)/\mathrm{F}^{i+1}(G) = p$ *für alle i, und*

(ii) $H = \mathrm{F}^i(G)$ *für ein i.*

Beweis. Wir führen den Beweis per Induktion nach dem Paar $\big(\#G, (G:H)\big)$ in lexikographischer Ordnung, also erst über die Ordnung von G und dann als zweite Induktion über den Index $(G:H)$.

Wenn $G = N_G(H)$ und $G \neq H \neq 1$, dann ist H ein Normalteiler und H sowie G/H haben kleinere Ordnung. Per Induktion gibt es dann zu $1 \subseteq H$ und $1 \subseteq G/H$ subnormale Filtrierungen wie im Satz von G/H:

$$G/H = (G/H)^0 \supseteq (G/H)^1 \supseteq \ldots \supseteq (G/H)^{n-1} \supseteq (G/H)^n = 1,$$

und von H:

$$H = H^0 \supseteq H^1 \supseteq \ldots \supseteq H^{m-1} \supseteq H^m = 1.$$

Mit der Projektion $\mathrm{pr} : G \to G/H$ definieren wir die subnormale Filtrierung (Isomorphiesatz)

$$G = \mathrm{pr}^{-1}((G/H)^0) \supseteq \mathrm{pr}^{-1}((G/H)^1) \supseteq \ldots \supseteq \mathrm{pr}^{-1}((G/H)^n) = H = H^0 \supseteq \ldots \supseteq H^m = 1.$$

Diese ist wie im Satz gefordert.

Wenn $G \neq N_G(H)$, dann ist nach Satz 276 der Index $(G : N_G(H)) < (G : H)$, also per Induktion gibt es eine subnormale Filtrierung wie im Satz durch $N_G(H)$. Von dieser nehmen wir den Anfang bis zu $N_G(H)$ und führen diese fort mit einer subnormalen Filtration wie im Satz zu H als Untergruppe von $N_G(H)$.

Es bleibt der Fall $H = 1$ oder $H = G$. In diesem Fall ist H keine echte Einschränkung für die subnormale Zentralreihe. Wir ersetzen daher H durch $\langle g\rangle$ für ein beliebiges Element $g \in G$ der Ordnung p. Jetzt bleibt nur noch der Fall, daß dann mit diesem neuen H schon $G = H \simeq \mathbb{Z}/p\mathbb{Z}$ ist. Aber in diesem Fall ist auch nichts zu zeigen. □

Korollar 279. *Sei $G \neq 1$ eine p-Gruppe und $H \subseteq G$ eine echte Untergruppe. Dann gibt es einen Normalteiler $N \subseteq G$ mit*

(i) $H \subseteq N$, *und*
(ii) $(G : N) = p$.

Beweis. Dies folgt sofort aus Satz 278 mit $N = \mathrm{F}^1(G)$. □

16.3. **Der Fundamentalsatz der Algebra.** Wir beweisen nun endlich den Fundamentalsatz der Algebra.

Theorem 280 (Fundamentalsatz der Algebra)**.** $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Beweis. Schritt 1: Sei $f \in \mathbb{R}[T]$ ein normiertes Polynom ungeraden Grades. Dann gilt

$$\lim_{x\to\pm\infty} f(x) = \pm\infty$$

und der Zwischenwertsatz der Analysis zeigt, daß f eine Nullstelle in $\mathbb{R}$ hat. Insbesondere gibt es in $\mathbb{R}[T]$ keine irreduziblen Polynome ungeraden Grades ≥ 3.

Damit hat $\mathbb{R}$ keine nichttriviale Erweiterung ungeraden Grades. Diese wäre separabel und damit nach Theorem 161 einfach. Somit wäre das Minimalpolynom eines Erzeugers irreduzibel von ungeradem Grad ≥ 3.

Schritt 2: Sei nun $K/\mathbb{C}$ eine algebraische Erweiterung. Dann gibt es eine Galoiserweiterung $L/\mathbb{R}$, die K enthält. Sei $G = \mathrm{Gal}(L/\mathbb{R})$ die Galoisgruppe, und sei $S \subseteq G$ eine 2-Sylowgruppe in G. Der Fixkörper

$$M = L^S$$

hat per Definition von Sylowgruppe einen ungeraden Grad

$$[M : \mathbb{R}] = \frac{[L : \mathbb{R}]}{[L : M]} = \frac{\#G}{\#S}.$$

Aus Schritt 1 folgt $M = \mathbb{R}$ und $G = S$ ist eine 2-Gruppe. Damit ist $H = \mathrm{Gal}(L/\mathbb{C})$ ebenfalls eine 2-Gruppe.

Schritt 3: Als 2-Gruppe hat H nach Korollar 279 einen Normalteiler $H_1 \subseteq H$ vom Index 2, oder $H = 1$. Per Galoistheorie entspricht H_1 einer quadratischen Erweiterung $L_1/\mathbb{C}$. Daraus folgt die Existenz eines irreduziblen quadratischen Polynoms in $\mathbb{C}[T]$. Dies widerspricht Satz 4, nachdem jedes quadratische Polynom in $\mathbb{C}[T]$ bereits eine Nullstelle in $\mathbb{C}$ hat.

Wir schließen, daß $H = 1$, somit $L = \mathbb{C}$ und $K \subseteq \mathbb{C}$ sein muß. Somit ist $\mathbb{C}$ algebraisch abgeschlossen. □

16.4. **Konstruierbarkeit des regelmäßigen n-Ecks.** Wir nehmen die Diskussion der Konstruierbarkeit im Sinne der Griechen mit Zirkel und Lineal Aus Abschnitt §3.5 wieder auf.

Wenn $M \subset \mathbb{C}$ eine Punktmenge ist, dann bezeichneten wir mit

$$\mathbb{Q}(M)$$

den davon erzeugten Teilkörper von $\mathbb{C}$. Und mit

$$\mathrm{ZL}(M)$$

den Erweiterungskörper von $\mathbb{Q}(M)$ aller durch Zirkel und Lineal aus M konstruierbaren Punke (als komplexe Zahlen).

Satz 281. *Seien $A, M \subseteq \mathbb{C}$ Mengen und setze $K = \mathbb{Q}(M)$. Dann sind äquivalent:*

(a) *A ist aus M in endlich vielen Schritten mit Zirkel und Lineal konstruierbar.*

(b) *Es gibt $n \in \mathbb{N}$ und eine endliche Folge von sukzessiven quadratischen Erweiterungen*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$$

so daß $K(A) \subset K_n$.

(c) *Es gibt $n \in \mathbb{N}$ und eine endliche Folge von sukzessiven quadratischen Erweiterungen*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K(A).$$

(d) *Die Erweiterung $K(A)/K$ ist endlich und die Galoisgruppe der Galoishülle von $K(A)/K$ ist eine 2-Gruppe.*

Beweis. (a) $\iff$ (b): Dies ist genau Korollar 44.

(c) $\implies$ (b): Das ist trivial.

(b) $\implies$ (d): Sei L eine endliche Galoiserweiterung, die K_n enthält, $G = \mathrm{Gal}(L/K)$ und $\mathrm{Gal}(L/K_n) = H \subseteq G$ die Untergruppe, welche per Galoiskorrespondenz zum Zwischenkörper K_n gehört. Die Galoishülle $\tilde{K}_n$ von K_n gehört dann zum größten Normalteiler $N \subseteq G$, der in H enthalten ist. Das ist

$$N = \bigcap_{g \in G} gHg^{-1},$$

denn für alle $g \in G$ gilt $N = gNg^{-1} \subseteq gHg^{-1}$, und der Schnitt ist eine unter Konjugation (das permutiert die zu schneidenden Untergruppen) stabile Untergruppe, also ein Normalteiler.

Zum Schnitt von Untergruppen gehört per Galoiskorrespondenz das Kompositum der Fixkörper

$$\tilde{K}_n = \text{ Kompositum der } g(K_n) \text{ für alle } g \in G.$$

Mit K_n ist auch $g(K_n)$ sukzessive durch quadratische Erweiterungen aufgebaut. Das Kompositum von solchen Körpern ist ebenfalls sukzessive durch quadratische Erweiterungen erzeugt. Es reicht dies für das Kompositum zweier solcher Körper einzusehen. Sei also

$$K = K'_0 \subseteq K'_1 \subseteq K'_2 \subseteq \ldots \subseteq K'_m$$

ein weiterer. Dann ist

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n \subseteq K_nK'_1 \subseteq K_nK'_2 \subseteq \ldots \subseteq K_nK'_m$$

ein in jeder Stufe quadratischer Körperturm, denn für alle $1 \leq i \leq m-1$ gilt

$$[K_nK'_{i+1} : K_nK'_i] \leq [K'_{i+1} : K'_i] = 2.$$

Der Grad der Minimalpolynome geht im Kompositum höchstens runter und bei Grad 1 kann man auf den entsprechenden Erzeuger verzichten.

Wir schließen aus dem Gradsatz, daß die Galoishülle $\tilde{K}_n/K_n$ eine Erweiterung von 2-er Potenzordnung ist. Das gilt dann auch für die in $\tilde{K}_n$ enthaltene Galoishülle $K\tilde{(A)}$ von $K(A)$. Also ist $\mathrm{Gal}(K\tilde{(A)}/K)$ eine 2-Gruppe.

(d) $\Longrightarrow$ (c): Sei L die galoissche Hülle von $K(A)/K$. Sei $H \subseteq G = \mathrm{Gal}(L/K)$ die zu $K(A)$ per Galoiskorrepsondenz gehörende Untergruppe. Dann gibt es nach Satz 278 eine Subnormalreihe von G durch H, deren Filtrationsquotienten jeweils vom Ordnung $p = 2$ sind. Der Anfang davon

$$G \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = H$$

gehört per Galoiskorrespondenz mit $K_i = L^{H_i}$ zu einem Körperturm wie in (c). □

Bemerkung 282. Die Bedingungen von Satz 281 sind nicht dazu äquivalent, daß $[K(A) : K]$ eine 2-er Potenz ist. Als Beispiel nehmen wir eine galoissche Erweiterung L/K mit Galoisgruppe A_4 und darin die Teilerweiterung M/K, die zu $H = \langle\sigma\rangle$ mit einem 3-Zykel σ gehört. Dann ist

$$[M : K] = (A_4 : H) = 4,$$

aber es gibt keine Zwischenerweiterung vom Grad 2. Eine solche entspräche einer Untergruppe $N \subseteq A_4$ vom Index 2, also einem Normalteiler. Es ist eine Übungsaufgabe, die Normalteiler von A_4 aufzulisten. Einer vom Index 2 ist nicht dabei.

Definition 283. Eine Fermat-Primzahl ist eine Primzahl der Form $p = 2^{2^n} + 1$ mit einem $n \in \mathbb{N}$.

Bemerkung 284. (1) Da für ungerades m die Zahl $2^{mn} + 1$ durch $2^n + 1$ teilbar ist, muß der Exponent N in einer Primzahl der Form $p = 2^N + 1$ selbst eine 2-er Potenz sein. Dies erklärt den Ausdruck für eine Fermat–Primzahl.

(2) Es sind nur die folgenden Fermat–Primzahlen bekannt.

$$p = 2^{2^n} + 1 = 3, 5, 17, 257, 65537.$$

entsprechend $n = 0, 1, 2, 3, 4$.

(3) Es ist nicht bekannt, ob es unendlich viele Fermat–Primzahlen gibt.

Theorem 285 (Gauß 1796)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn jeder ungerader Primfaktor von n eine Fermatprimzahl ist und nicht quadratisch in n aufgeht.*

Beweis. Das regelmäßige n-Eck ist konstruierbar genau dann, wenn die Menge der Ecken $\mu_n(\mathbb{C})$ konstruierbar ist (nach Translation zum Mittelpunkt 0 und Streckung auf Radius 1 des Umkreises). Weil $\mathbb{Q}(\mu_n)$ galoissch über $\mathbb{Q}$ ist, gilt dies nach Satz 281 genau dann, wenn

$$\varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}] = 2^m$$

eine 2-er Potenz ist. Das ist äquivalent zu der genannten Bedingungen an die ungeraden Primfaktoren von n. □

Bemerkung 286. (1) Es sind nur die folgenden regelmäßigen p-Ecke für p Primzahl und $2 < p < 2^{2^{33}} + 1$ konstruierbar:

$$p = 3, 5, 17, 257, 65537$$

Das sind die bekannten Fermatprimzahlen. Die Konstruktion des regelmäßigen 17-Ecks geht auf den jungen Gauß zurück.

(2) Es ist nicht bekannt, ob es unendlich viele Primzahlen p gibt, so daß das regelmäßige p-Eck konstruierbar wäre.

Übungsaufgaben zu §16

Übungsaufgabe 16.1. Eine **Zentralreihe** (oder **zentrale** Filtrierung) einer Gruppe G ist eine normale Filtrierung $\mathrm{F}^\bullet(G)$, so daß für alle i der i-te Filtrationsquotient $\mathrm{F}^i(G)/\mathrm{F}^{i+1}(G)$ im Zentrum von $G/\mathrm{F}^{i+1}(G)$ liegt. Eine **nilpotente** Gruppe ist eine Gruppe mit einer endlichen Zentralreihe.

Zeigen Sie, daß eine p-Gruppe nilpotent ist.

Übungsaufgabe 16.2. (a) Sei G eine Gruppe und $G/Z(G)$ zyklisch. Zeigen Sie daß dann $G = Z(G)$ abelsch ist.
(b) Bestimmen Sie für eine Primzahl p alle Gruppen der Ordnung p^2 bis auf Isomorphie.

Übungsaufgabe 16.3. Die **Fittinguntergruppe** $\Phi(G)$ einer Gruppe G besteht aus

$$\Phi(G) = \bigcap_{M \subseteq G} M$$

wobei M durch alle maximalen echten Untergruppen $M \subseteq G$ läuft. Zeigen Sie die folgenden Ausssagen.

(1) $\Phi(G)$ ist ein Normalteiler.
(2) Eine Menge von Elementen $S \subseteq G$ erzeugt die Gruppe G genau dann, wenn das Bild von S in $\overline{G} = G/\Phi(G)$ diesen Quotienten $\overline{G}$ erzeugt.
(3) Sei G eine p-Gruppe. Zeigen Sie, daß $G/\phi(G)$ eine abelsche Gruppe vom Exponenten p ist (also natürlich als $\mathbb{F}_p$-Vektorraum verstanden werden kann).
(4) Eine Teilmenge $S \subseteq G$ einer p-Gruppe ist genau dann ein minimales Erzeugendensystem, wenn die Bilder der Elemente von S in $G/\Phi(G)$ eine $\mathbb{F}_p$-Basis bilden.

17. Auflösbarkeit bei Gruppen

17.1. **Einfache Gruppen.** Wir versuchen nun Gruppen in ihre einfachen Bestandteile zu zerlegen.

Definition 287. Eine **einfache** Gruppe ist eine Gruppe $G \neq 1$, die keine echten Normalteiler hat, also keine normalen Untergruppen $N \subseteq G$ mit N verschieden von G und 1.

Beispiel 288. Für jede Primzahl p ist die zyklische Gruppe

$$\mathbb{Z}/p\mathbb{Z}$$

der Ordnung p eine einfache Gruppe. Nach dem Satz von Lagrange gibt es nicht einmal echte Untergruppen, somit erst recht keine Normalteiler.

Proposition 289. *Eine abelsche einfache Gruppe ist zyklisch von Primzahlordnung.*

Beweis. In einer abelschen Gruppe G ist jede Untergruppe Normalteiler. Sei G einfach, abelsch, und sei $1 \neq g \in G$ ein Element. Dann ist $\langle g \rangle \subseteq G$ ein Normalteiler verschieden von 1, somit gleich G. Damit muß G zyklisch sein.

Die Gruppe $G = \mathbb{Z}$ ist nicht einfach, denn für jedes $n > 1$ ist $n\mathbb{Z}$ ein nichttrivialer Normalteiler. Daher muß G endlich zyklisch sein. Da eine endliche zyklische Gruppe für jeden Teiler d der Gruppenordnung eine Untergruppe der Ordnung d besitzt, muß eine einfache zyklische Gruppe eine Primzahl als Ordnung haben. $\square$

Bemerkung 290. Die Bezeichnung *einfach* ist irreführend, denn einfache Gruppen sind nicht einfach zu verstehen. Außerdem wird unter Gruppentheoretikern auch manchmal der Begriff *einfache Gruppe* nur für nichtabelsche einfache Gruppen verwendet, also einfache Gruppen in unserem Sinn ohne die Gruppen $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

Als nächstes betrachten wir die symmetrische Gruppe S_n. Das Signum $\mathrm{sign} : S_n \to \{\pm 1\}$ ist ein nichttrivialer Homomorphismus, dessen Kern A_n die alternierende Gruppe auf n Elementen ein Normalteiler vom Index 2 in S_n ist. Damit ist S_n für $n \geq 3$ nicht einfach[15]

Definition 291. Die **Klein'sche Vierergruppe** V_4 ist die Gruppe der Doppeltranspositionen

$$V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \subseteq A_4 \subseteq S_4.$$

Die Wirkung auf dem Quadrat mit Ecken $1, 2, 3, 4$ von V_4 zeigt, daß V_4 von zwei Spiegelungen bezüglich zueinander orthogonalen Achsen (durch die Seitenmitten) erzeugt wird. Solche Spiegelungen kommutieren und somit gilt

$$V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Dieses geometrische Bild zeigt auch ohne Nachrechnen, daß es sich bei V_4 um eine Untergruppe von S_4 handelt.

Proposition 292. *Die Gruppe V_4 ist Normalteiler in S_4. Es gibt einen surjektiven Homomorphismus $S_4 \to S_3$ mit Kern V_4, also*

$$S_4/V_4 \simeq S_3.$$

Beweis. Die Formel für die Konjugation eines Zykels in S_n

$$\sigma(a_1, a_2, \ldots, a_r)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_r)) \tag{17.1}$$

zeigt, daß die Partition von n, die ein Element $\pi \in S_n$ durch die Längen der Zykel in seiner Zykelzerlegung definiert (die Orbits von $\{1, \ldots, n\}$ unter der Wirkung von $\langle \pi \rangle$), durch Konjugation nicht verändert wird.

Die Gruppe V_4 besteht aus allen Elementen von S_4 mit zugehöriger Partition $1 + 1 + 1 + 1$ oder $2 + 2$. Diese Menge ist invariant unter Konjugation, somit V_4 ein Normalteiler.

Die Gruppe V_4 enthält 3 Doppeltranspositionen. Die Konjugation mit Elementen von S_4 permutiert diese 3-elementige Menge $V_4 \setminus \{\mathrm{id}\}$. Diese Operation definiert daher einen Gruppenhomomorphismus

$$f : S_4 \to S_3.$$

Der Kern besteht genau aus den Elementen $\sigma \in S_4$, die mit allen Elementen von V_4 vertauschen. Da V_4 abelsch ist, gilt sicher

$$V_4 \subseteq \ker(f).$$

Betrachen wir die Transposition $(12) \in S_4$. Dann kommt (12) in genau einer Doppeltransposition vor. Aus (17.1) folgt, daß Konjugation mit (12) genau die beiden anderen Doppeltranspositionen vertauscht. Damit ist $f((12))$ eine Transposition. Ersetzen wir (12) durch eine beliebige Transposition, so zeigt dies, daß jede beliebige Transposition aus S_3 im Bild von f liegt. Da die Transpositionen die symmetrische Gruppe erzeugen, ist f surjektiv. Nach dem Satz von Lagrange und dem Homomorphiesatz folgt

$$\#\ker(f) = \frac{\#S_4}{\#S_3} = 24/6 = 4 = \#V_4$$

und deshalb $V_4 = \ker(f)$. □

Da S_n für $n \geq 3$ aufgrund des Normalteilers $A_n \subseteq S_n$ nicht einfach ist, behandeln wir als nächstes die alternierende Gruppe A_n.

Lemma 293. *Die alternierende Gruppe A_n wird von den 3-Zykeln in S_n erzeugt.*

[15] Die Fälle $n = 1$ und $n = 2$ sind trivial: $S_1 = 1$ ist die triviale Gruppe und wird nicht betrachtet (formal gesehen nicht einfach), und $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$ ist zyklisch von Primzahlordnung, also einfach.

Beweis. Ein 3-Zykel ist ein Produkt zweier Transpositionen und damit eine gerade Permutation, also in A_n.

Die ersten $n-2$ Einträge einer beliebigen Permutation $\pi \in S_n$ können sukzessive durch 3-Zykel erreicht werden:

$$\pi = \tau\sigma_{n-2}\sigma_{n-3}\ldots\sigma_2\sigma_1$$

wobei der 3-Zykel σ_i für das richtige Bild von i sorgt und die Elemente $\pi(1), \ldots, \pi(i-1)$ fix läßt. Das Element τ ist entweder id oder die Transposition der letzen beiden Bilder $(\pi(n-1), \pi(n))$ je nach Bedarf.

Damit ist jedes Element in S_n bis auf höchstens eine Transposition ein Produkt von 3-Zykeln. Anwenden von $\mathrm{sign} : S_n \to \{\pm 1\}$ zeigt, daß für $\pi \in A_n$

$$1 = \mathrm{sign}(\pi) = \mathrm{sign}(\tau)\prod_{i=1}^{n-2}\mathrm{sign}(\sigma_i) = \mathrm{sign}(\tau),$$

also die Transposition nicht vorkommt. □

Lemma 294. *Sei $n \geq 5$. Dann sind in A_n alle 3-Zykel konjugiert.*

Beweis. Seien $\sigma_1 = (a, b, c)$, und $\sigma_2 = (\alpha, \beta, \gamma)$ zwei 3-Zykel. Dann gibt es $\pi \in S_n$ mit

$$\pi(a) = \alpha, \quad \pi(b) = \beta, \quad \pi(c) = \gamma$$

und nach (17.1) gilt $\pi\sigma_1\pi^{-1} = \sigma_2$. Damit sind alle 3-Zykel konjugiert in S_n.

Sei τ eine Transposition mit Träger disjunkt zu $\{a, b, c\}$. Ein solches τ gibt es, da $n \geq 5$ ist. Dann gilt auch

$$(\pi\tau)\sigma_1(\pi\tau)^{-1} = \pi(\tau\sigma_1\tau^{-1})\pi^{-1} = \pi\sigma_1\pi^{-1} = \sigma_2.$$

Da $\mathrm{sign}(\pi) \neq \mathrm{sign}(\pi\tau)$ liegt einer der beiden Elemente π oder $\pi\tau$ sogar in A_n. □

Theorem 295 (Galois)**.** *Die alternierende Gruppe A_n ist einfach genau für $n = 3$ und $n \geq 5$.*

Beweis. Die Fälle $n \leq 4$ erledigen wir durch Inspektion. $A_1 = A_2 = 1$ ist trivial, $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ ist einfach und A_4 enthält den Normalteiler V_4, also nicht einfach.

Sei $n \geq 5$. Wir beweisen, daß ein Normalteiler $1 \neq N \lhd A_n$ einen 3-Zykel enthält. Diese Behauptung beweist das Theorem, denn nach Lemma 294 enthält N dann alle 3-Zykel und wegen Lemma 293 gilt $N = A_n$.

Der Fall $n = 5$: Wir zeigen, daß ein nichttrivialer Normalteiler $N \lhd A_5$ einen 3-Zykel enthält.

Die 5-Sylowgruppe von A_5 ist zyklisch und wird von einem 5-Zykel erzeugt. Von den 5-Zyklen gibt es $5!/5 = 24$ in A_5, somit enthält die Vereinigung der 5-Sylows in A_5 genau 25 Elemente: die 1 und die 5-Zykel. Wenn $5 \mid \#N$, dann enthält N eine 5-Sylowgruppe von A_5. Weil die 5-Sylowgruppen alle unter A_5 konjugiert sind, enthält A_5 dann aber alle 5-Sylowgruppen von A_5. Dann folgt $\#N \geq 25$ und als nichttrivialer Teiler der Gruppenordnung bleibt nur $\#N = 30$. Wenn 3 ein Teiler von $\#N$ ist, dann enthält N aber ein Element der Ordnung 3 und damit einen 3-Zykel.

Wir sind also fertig, wenn 5 oder 3 ein Teiler von $\#N$ ist. Es bleibt der Fall daß N eine 2-Gruppe ist. Nach den Sylow-Sätzen gibt es dann eine 2-Sylowgruppe $P \subseteq A_5$ mit $N \subseteq P$. Da N normal ist, gilt für alle $\pi \in A_5$

$$N = \pi N\pi^{-1} \subseteq \pi P\pi^{-1}.$$

Als normale 2-Gruppe ist dann N nach den Sylow-Sätzen in jeder 2-Sylowgruppe von A_5 enthalten. Die 2-Sylowgruppen von A_5 sind konjugiert zu

$$P = V_4 \subseteq A_4 \subseteq A_5$$

Dabei fixiert P das Element 5. Die konjugierte $\sigma P\sigma^{-1}$ von P fixieren $\sigma(5)$, also für geeignetes σ ein belibiges Elemente aus $\{1, \ldots, 5\}$. Eine Gruppe, die in allen 2-Sylowgruppen enthalten ist, muß demnach alle Elemente fixieren, also $N = 1$.

Der Fall $n > 5$: Sei $1 \neq \pi \in N$ und $\sigma = (a, b, c)$ ein beliebiger 3-Zykel in A_n. Da N Normalteiler ist, gilt auch $\sigma\pi^{-1}\sigma^{-1} \in N$ und damit enthält N das Element

$$\tau = \pi(\sigma\pi^{-1}\sigma^{-1}) = (\pi\sigma\pi^{-1})\sigma^{-1} = (\pi(a), \pi(b), \pi(c))(a, c, b).$$

Wir können nun a, b, c so wählen, daß

$$4 \leq \#\{a, b, c, \pi(a), \pi(b), \pi(c)\} \leq 5. \tag{17.2}$$

Das geht, weil $\pi \neq 1$ und damit ein a existiert mit $a \neq \pi(a)$. Wir setzen $b = \pi(a)$. Wenn $\{a, b, \pi(b)\}$ aus bereits 3 Elementen besteht, dann wählen wir c beliebig aber davon verschieden. Im andern Fall gilt $\pi(b) = a$ und die Zykelschreibweise von π enthält die Transposition (a, b). Da $\pi \in A_n$ selbst keine Transposition ist, gibt es ein von a, b verschiedenes c mit $\pi(c) \neq c$.

Aus der Bedingung (17.2) folgt sofort, daß $\tau \neq 1$ ein nichttriviales Element mit Träger enthalten in einer 5-elementigen Teilmenge $M \subseteq \{1, \ldots, n\}$ ist. Die entsprechende Untergruppe $A_M \subseteq A_n$ der Permutationen, die alle $i \notin M$ fest lassen, ist isomorph zu A_5. Der Schnitt $N \cap A_M$ enthält τ und ist demnach ein nichttrivialer Normalteiler von $A_M \simeq A_5$. Der Fall $n = 5$ zeigt $A_M = N \cap A_M \subseteq N$, und da es 3-Zykel in A_M gibt, gibt es auch 3-Zykel in N. □

Bemerkung 296. Die einfachen endlichen Gruppen sind vollständig klassifiziert. Wenn man bedenkt, daß das Klassifikationstheorem der einfachen endlichen Gruppen sich auf viele Publikationen mit insgesamt wohl mehr als 10.000 Seiten erstreckt, wundert es nicht, daß die Meinung darüber, ob das Theorem endgültig als bewiesen anzusehen ist, in den Jahren 1983–2008 zwischen den beiden Möglichkeiten hin und her oszillierte.

Die Klassifikation der endlichen einfachen Gruppen behauptet, daß die folgende Liste vollständig ist:

- die Familie der zyklische Gruppe von Primzahlordnung $\mathbb{Z}/p\mathbb{Z}$,
- die Familie der alternierende Gruppe A_n für $n \geq 5$,
- 16 Familien einfacher Gruppen vom Lie-Typ (Beispiel $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$ für $q \geq 4$ Primpotenz und $n \geq 1$),
- 26 sporadische Gruppen (die größte davon wird das **Monster** genannt und hat $\approx 8 \cdot 10^{53}$ Elemente).

Dabei bedeutet sporadisch, daß man für diese Gruppen keinen Platz in einer der 18 Familien finden kann.

17.2. **Kompositionsreihen.**

Definition 297. Sei G eine Gruppe und $\mathrm{F}^\bullet(G)$ eine Subnormalreihe

$$G = \mathrm{F}^0(G) \supseteq \mathrm{F}^1(G) \supseteq \ldots \supseteq \mathrm{F}^{n-1}(G) \supseteq \mathrm{F}^n(G) = 1.$$

(1) Die Subnormalreihe $\mathrm{F}^\bullet(G)$ heißt **wiederholungsfrei**, wenn $\mathrm{F}^i(G) \neq \mathrm{F}^{i+1}(G)$ für alle $0 \leq i < n$.

(2) Die Subnormalreihe $\tilde{\mathrm{F}}^\bullet(G)$

$$G = \tilde{\mathrm{F}}^0(G) \supseteq \tilde{\mathrm{F}}^1(G) \supseteq \ldots \supseteq \tilde{\mathrm{F}}^{m-1}(G) \supseteq \tilde{\mathrm{F}}^m(G) = 1.$$

ist eine **Verfeinerung** von $F^\bullet(G)$, wenn es eine monotone Injektion

$$\sigma : \{0, \ldots, n\} \hookrightarrow \{0, \ldots, m\}$$

gibt mit

$$\mathrm{F}^i(G) = \tilde{\mathrm{F}}^{\sigma(i)}(G)$$

für alle $0 \leq i \leq n$.

(3) Eine **Kompositionsreihe** ist eine wiederholungsfreie Subnormalreihe, die keine echte wiederholungsfreie Verfeinerung zuläßt.

(4) Zwei Subnormalreihen $\mathrm{F}^\bullet(G)$ der Länge n und $\mathrm{H}^\bullet(G)$ der Länge m heißen äquivalent, wenn
(i) $n = m$,

(ii) es gibt ein $\sigma \in S_n$, und
(iii) es gibt Isomorphismen $\mathrm{gr}^i_{\mathrm{F}}(G) \simeq \mathrm{gr}^{\sigma(i)}_{\mathrm{H}}(G)$.

Bemerkung 298. Eine Subnormalreihe $\mathrm{F}^\bullet(G)$ ist genau dann Kompositionsreihe, wenn ihre Faktoren einfache Gruppen sind. Das liegt daran, daß die Normalteiler von $\mathrm{gr}^i_{\mathrm{F}} G$ genau den Normalteilern von $\mathrm{F}^i(G)$ entsprechen, die $\mathrm{F}^{i+1}(G)$ enthalten.

In der Regel ist das Erzeugnis zweier Untergruppen $A, B \subseteq G$ größer als das naive elementweise Produkt der Teilmengen

$$AB := \{ab \ ; \ a \in A, b \in B\} \subseteq \langle A, B \rangle \subseteq G.$$

Aber es gibt eine wichtige Ausnahme.

Lemma 299. *Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler von G. Dann gilt*

$$NH = \langle N, H \rangle.$$

Beweis. Offensichtlich ist NH im Erzeugnis von N und H enthalten. Das Erzeugnis enthält aber auch längere Produkte mit Faktoren aus N und H. Zum Beweis reicht es nun aus, wenn für alle $a \in N$ und $h \in H$ es ein $b \in N$ und $g \in H$ gibt mit

$$ha = bg,$$

denn dann kann man die Faktoren aus N induktiv nach links durchreichen. Das wird realisiert durch $g = h$ und $b = hah^{-1}$. Es ist $b \in N$, da N ein Normalteiler ist und

$$bg = (hah^{-1})h = ha.$$

□

Lemma 300 (Lemma von Zassenhaus — Schmetterlingslemma[16])**.** *Sei G eine Gruppe und seien $N \subseteq H \subseteq G$ und $M \subseteq K \subseteq G$ Untergruppen mit N normal in H und M normal in K. Dann gilt:*

(1) *$N(H \cap M)$ ist normal in $N(H \cap K)$.*
(2) *$M(N \cap K)$ ist normal in $M(H \cap K)$.*
(3)

$$(N(H \cap M)) \cap (H \cap K) = (H \cap M)(N \cap K) = (M(N \cap K)) \cap (H \cap K).$$

(4) *Es gibt einen Isomorphismus*

$$\frac{N(H \cap K)}{N(H \cap M)} \simeq \frac{M(H \cap K)}{M(N \cap K)}.$$

Beweis. (1) Sei $\pi : H \to H/N$ die kanonische Projektion. Dann ist

$$A := N(H \cap M) = \pi^{-1}(\pi(H \cap M)),$$
$$B := N(H \cap K) = \pi^{-1}(\pi(H \cap K)).$$

Als Kern des natürlichen Homomorphismus

$$H \cap K \to K/M$$

ist $H \cap M$ ein Normalteiler in $H \cap K$, daher ist auch A ein Normalteiler in B. Dies zeigt (1) und wegen Symmetrie auch (2).

Wir zeigen nun die Behauptung (3). Da $H \cap M$ und $N \cap K$ Normalteiler in $H \cap K$ sind, ist das Produkt

$$C := (H \cap M)(N \cap K)$$

ein Normalteiler von $H \cap K$. Außerdem ist C offensichtlich in A enthalten. Das zeigt die Inkusion der mittleren Gruppe C in der linken $A \cap (H \cap K)$.

[16]Das zugehörige Diagramm in Schmetterlingsform ist bei Wikipedia zu sehen.

Für die umgekehrte Inklusion schreiben wir ein Element $g \in A \cap (H \cap K)$ mittels $a \in N$, $h \in H \cap M$ als

$$g = ah.$$

Wir müssen zeigen, daß auch $a \in K$ gilt. Das folgt sofort aus

$$a = gh^{-1}.$$

Die Gleichheit mit der rechten Gruppe folgt wieder aus Symmetrie.

(4) Nach dem Homomorphiesatz angewandt auf den Normalteiler $A = N(H \cap M)$ von $B = N(H \cap K)$ und die Untergruppe $H \cap K$ gilt

$$\frac{N(H \cap K)}{N(H \cap M)} = \frac{A(H \cap K)}{A} \simeq \frac{H \cap K}{A \cap (H \cap K)} = \frac{H \cap K}{(H \cap M)(N \cap K)},$$

wobei die letzte Gleichheit (3) verwendet. Aus Symmetrie folgt (4). □

Theorem 301. *(Schreier) Zu je zwei Subnormalreihen derselben Gruppe gibt es äquivalente Verfeinerungen.*

Beweis. Sei $\mathrm{F}^\bullet(G)$ eine Subnormalreihe von G der Länge n und sei $N \subseteq H \subseteq G$ zwei Untergruppen mit N normal in H. Dann induziert $\mathrm{F}^\bullet(G)$ durch

$$A^i = N \cdot (\mathrm{F}^i(G) \cap H)$$

eine Filtrierung

$$H = A^0 \supseteq A^1 \supseteq \ldots \supseteq A^n = N.$$

Dabei ist A^{i+1} ein Normalteiler von A^i für alle $i = 0, \ldots, n-1$ nach Lemma 300 (1).

Sei $\mathrm{H}^\bullet(G)$ eine weitere Subnormalreihe der Länge m von G. Dann wenden wir die obige Konstruktion auf alle Schritte $\mathrm{H}^{j+1}(G) \subseteq \mathrm{H}^j(G)$ an. Zusammengenommen finden wir eine Subnormalreihe von G der Länge nm, welche $\mathrm{H}^\bullet(G)$ verfeinert. Mit vertauschten Rollen erhalten wir eine Subnormalreihe von G der Länge nm, welche $\mathrm{F}^\bullet(G)$ verfeinert.

Nach Lemma 300 (4) gibt es einen Isomorphismus der Faktoren

$$\frac{\mathrm{F}^{i+1}(G)(\mathrm{F}^i(G) \cap \mathrm{H}^j(G))}{\mathrm{F}^{i+1}(G)(\mathrm{F}^i(G) \cap \mathrm{H}^{j+1}(G))} \simeq \frac{\mathrm{H}^{j+1}(G)(\mathrm{F}^i(G) \cap \mathrm{H}^j(G))}{\mathrm{H}^{j+1}(G)(\mathrm{F}^{i+1}(G) \cap \mathrm{H}^j(G))}$$

und dies zeigt, daß die beiden Verfeinerungen äquivalente Subnormalreihen sind. □

Korollar 302 (Jordan–Hölder)**.** *Je zwei Kompositionsreihen einer Gruppe sind äquivalent.*

Beweis. Zu zwei Kompositionsreihen von G gibt es nach Theorem 301 äquivalente Verfeinerungen. Da man Kompositionsreihen nur durch Wiederholungen verfeinern kann, bekommt man die Kompositionsreihen zurück, indem man die Wiederholungen ausläßt, also aus der Liste der Faktoren die trivialen Gruppen streicht. Da die Schritte mit trivialem Faktor in den äquivalenten Verfeinerungen gleich oft vorkommen, sind damit auch die um die Wiederholungen bereinigten ursprünglichen Kompositionsreihen äquivalent. □

Definition 303. Eine Gruppe G hat **endliche Länge**, wenn es eine Kompositionsreihe gibt. Nach Korollar 302 ist die Länge einer solchen Kompositionsreihe wohldefiniert und wird **Länge** der Gruppe genannt. Ebenso ist die Liste der einfachen Gruppen bis auf Isomorphie aber möglicherweise Mehrfachnennung, die als Faktoren einer Kompositionsreihe von G auftreten von der Wahl einer solchen Kompositionsreihe unabhängig. Diese Faktoren werden **Kompositionsfaktoren** der Gruppe G genannt.

Beispiel 304. (1) Jede endliche Gruppe hat endliche Länge. Das ist klar, denn es gibt überhaupt nur endlich viele Untergruppen.

(2) Eine p-Gruppe G der Ordnung p^n besitzt eine Kompositionsreihe der Länge n. Jeder Faktor ist zyklisch von Ordnung p. Dies haben wir in Satz 278 bewiesen.

Proposition 305. *Eine Gruppe ist genau dann endlich, wenn sie endliche Länge mit endlichen Gruppen als Faktoren hat.*

Beweis. Das ist trivial nach dem Satz von Lagrange: Die Ordnung der Gruppe ist das Produkt der Ordnungen der Faktoren. ☐

Satz 306. *Sei G eine Gruppe und N ein Normalteiler. Wenn N und G/N eine Kompositionsreihe besitzen, dann hat auch G eine Kompositionsreihe. In diesem Fall gilt:*

(1) Die Länge ist additiv: die Länge von G ist die Summe von den Längen von N und von G/N.
(2) Die Faktoren von G sind die Faktoren von N und G/N betrachtet als Menge mit Vielfachheiten.

Beweis. Das ist klar: Die Urbilder bezüglich der kanonische Projektion $\pi : G \to G/N$ einer Kompositionsreihe von G/N führt zu einer Verlängerung einer Kompositionsreihe von N zu einer von G. ☐

17.3. **Auflösbare Gruppen.**

Definition 307. Eine Gruppe ist **auflösbar**, wenn sie eine Subnormalreihe mit abelschen Faktoren besitzt.

Bemerkung 308. Ein wichtiger 256-Seiten langer Baustein im Beweis der Klassifikation der endlichen einfachen Gruppen ist das *Odd Order Theorem* von Feit und Thompson: Jede Gruppe ungerader Ordnung ist auflösbar.

Beispiel 309. (1) Abelsche Gruppen sind auflösbar.
(2) Die alternierende Gruppe A_n ist nicht auflösbar für $n \geq 5$. Algemeiner ist keine nicht-abelsche einfache Gruppe G auflösbar. Der erste Schritt einer Subnormalreihe ist ein Normalteiler, daher gleich 1, weil G keine echten Normalteiler hat. Damit hat G einen einzigen Faktor, nämlich G selbst, und dieser Faktor ist nicht abelsch.

Satz 310. *Sei G eine Gruppe H eine Untergruppe und N ein Normalteiler. Dann gilt:*

(1) Wenn G auflösbar ist, dann ist H auflösbar.
(2) Wenn G auflösbar ist, dann ist G/N auflösbar.
(3) Wenn N und G/N auflösbar sind, dann ist G auflösbar.

Beweis. (1) Wen wir eine Subnormalreihe $\mathrm{F}^\bullet(G)$ von G mit H schneiden, dann erhalten wir eine Subnormalreihe von H, deren Faktoren in die jeweiligen Faktoren von G einbetten. Da Untergruppen von abelschen Gruppen wieder abelsch sind, ist H auch auflösbar.

(2) Wenn wir eine Subnormalreihe mit der kanonischen Projektion $\pi : G \to G/N$ abbilden, dann erhalten wir eine Subnormalreihe von G/N, deren Faktoren Quotienten der jeweiligen Faktoren von G sind. Da Quotienten abelscher Gruppen wieder abelsch sind, ist G/N auch auflösbar.

Teil (3) folgt wie bei Satz 306. ☐

Korollar 311. *Die symmetrische Gruppe S_n ist nicht auflösbar genau für $n \geq 5$.*

Beweis. Für $n \geq 5$ hat S_n einen einfachen nicht-abelschen Normalteiler A_n und kann daher nicht auflösbar sein (denn A_n ist nicht auflösbar, weil einfach nach Theorem 295). Die Fälle $n = 1, 2, 3$ sind offensichtlich auflösbar (A_3 ist abelsch). Und S_4 ist auflösbar wegen der kurzen exakten Sequenz

$$1 \to V_4 \to S_4 \to S_3 \to 1$$

aus Proposition 292, denn V_4 ist abelsch und S_3 ist auflösbar. ☐

17.4. Kommutatoren und Kommutatorfaktorgruppe.

Definition 312. Der **Kommutator** zweier Elemente g, h in einer Gruppe G ist das Element
$$[g, h] = ghg^{-1}h^{-1}.$$
Die **Kommutatorgruppe** $G' = [G, G]$ einer Gruppe G ist die Untergruppe von G, die von allen Kommutatoren in G erzeugt wird:
$$[G, G] = \langle [x, y]\ ;\ x, y \in G\rangle.$$

Bemerkung 313. Vorsicht: Gruppentheoretiker schreiben gerne
$$(g, h) = g^{-1}h{-}1gh$$
was nichts anderes ist als
$$(g, h) = [g^{-1}, h^{-1}].$$

Proposition 314. *Sei G eine Gruppe. Die Kommutatorgruppe $[G, G]$ ist ein Normalteiler. Die Quotientenabbildung $\pi : G \to G^{\mathrm{ab}}$ auf die* ***Kommutatorfaktorgruppe*** *(oder auch* ***Abelisierung*** *von G)*
$$G^{\mathrm{ab}} = G/[G, G]$$
hat die folgende universelle Eigenschaft:

(i) *G^{ab} ist eine abelsche Gruppe, und*
(ii) *Jeder Homomorphismus $f : G \to A$ nach einer abelschen Gruppe A faktorisiert eindeutig über G^{ab}, d.h., es gibt ein eindeutiges $\varphi : G^{\mathrm{ab}} \to A$ mit $f = \varphi \circ \pi$.*

Beweis. Sei $g, x, y \in G$. Dann gilt
$$g[x, y]g^{-1} = g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = [gxg^{-1}, gyg^{-1}].$$
Damit ist das definierende Erzeugendensystem von $[G, G]$ invariant unter Konjugation, somit auch das Erzeugnis $[G, G]$. Die Kommutatorgruppe ist also ein Normalteiler.

in $G^{\mathrm{ab}} = G/[G, G]$ kommutieren alle Elemente, denn der Unterschied von xy und yx ist gerade $[x, y]$. Wenn $f : G \to A$ ein Gruppenhomomorphismus ist mit A abelsch, dann gilt für alle $x, y \in G$
$$f([x, y]) = f(xyx^{-1}y^{-1}) = [f(x), f(y)] = 0.$$
Es folgt
$$[G, G] \subseteq \ker(f)$$
und aus der universellen Eigenschaft der Quotientenabbildung die Existenz eines Homomorphismus
$$\varphi : G^{\mathrm{ab}} \to A$$
mit den geforderten Bedingungen. Da π surjektiv ist, ist φ eindeutig. □

Definition 315. Die **abgeleitete Reihe** einer Gruppe G ist die (eventuell unendliche Filtrierung $\mathrm{K}^\bullet(G)$ die rekursiv durch
$$\begin{aligned} \mathrm{K}^0(G) &= G \\ \mathrm{K}^{i+1}(G) &= [\mathrm{K}^i(G), \mathrm{K}^i(G)] \text{ für alle } i \geq 0. \end{aligned}$$
definiert wird.

Satz 316. *Sei G eine Gruppe.*

(1) *Die abgeleitete Reihe von G ist eine Subnormalreihe mit abelschen Faktoren.*
(2) *Sei $\mathrm{F}^\bullet(G)$ eine Subnormalreihe von G mit abelschen Faktoren. Dann gilt $\mathrm{K}^i(G) \subseteq \mathrm{F}^i(G)$ für alle $i \geq 0$.*
(3) *G ist auflösbar genau dann, wenn für $i \gg 0$ gilt $\mathrm{K}^i(G) = 1$.*

Beweis. (1) Das ist klar aus der Definition der abgeleiteten Reihe.

(2) Dies zeigen wir per Induktion nach i. Für $i = 0$ haben wir $\mathrm{K}^0(G) = G = \mathrm{F}^0(G)$. Sei also die Aussage (2) bis i bewiesen. Dann ist

$$\mathrm{K}^{i+1}(G) = [\mathrm{K}^i(G), \mathrm{K}^i(G)] \subseteq [\mathrm{F}^i(G), \mathrm{F}^i(G)] \subseteq \ker(\mathrm{F}^i(G) \to \mathrm{gr}^i_{\mathrm{F}}(G)) = \mathrm{F}^{i+1}(G).$$

(3) Wenn die abgeleitete Reihe die 0 für endliches i erreicht, ist die abgeleitete Reihe eine Subnormalreihe mit abelschen Faktoren und G somit auflösbar. Ist umgekehrt G auflösbar und $\mathrm{F}^\bullet(G)$ eine Subnormalreihe mit abelschen Faktoren, die dies beweist. Dann ist nach (2) $\mathrm{K}^\bullet(G)$ für jeden Index nach oben durch $\mathrm{F}^\bullet(G)$ beschränkt. Wenn $\mathrm{F}^i(G) = 1$ erreicht ist, dann gilt auch $\mathrm{K}^i(G) = 1$. □

Übungsaufgaben zu §17

Übungsaufgabe 17.1. Beschreiben Sie alle Normalteiler von A_4 und S_4.

Übungsaufgabe 17.2. Bestimmen Sie eine Kompositionsreihen und die Faktoren für die Gruppen $\mathrm{SL}_2(\mathbb{F}_2)$ und $\mathrm{SL}_2(\mathbb{F}_3)$.

Tipp: Lassen Sie für $K = \mathbb{F}_2$ und $\mathbb{F}_3$ die Gruppen via

$$\mathrm{SL}_2(K) \subseteq \mathrm{GL}_2(K) \to \mathrm{PGL}_2(K)$$

auf $\mathbb{P}^1(K)$ mittels Möbiustransformationen operieren. Es gilt $\#\mathbb{P}^1(\mathbb{F}_q) = q + 1$. Dies führt zu Homomorphismen $\mathrm{SL}_2(\mathbb{F}_2) \to S_3$ und $\mathrm{SL}_2(\mathbb{F}_3) \to S_4$.

Übungsaufgabe 17.3. Sei K ein Körper und $\mathrm{Aff}^1(K)$ die Gruppe der affin linearen Tranformationen von K, also der Abbildungen $f : K \to K$ der Form

$$f(x) = ax + b$$

für ein $a \in K^\times$ und $b \in K$. Ist $\mathrm{Aff}^1(K)$ auflösbar?

Übungsaufgabe 17.4. Sei K ein Körper und $n \in \mathbb{N}$. Wir bezeichnen mit $N \subseteq \mathrm{GL}_n(K)$ die Gruppe der unipotenten oberen Dreiecksmatrizen (unipotent bedeutet, daß auf der Diagonalen nur 1 steht). Zeigen Sie, daß N auflösbar ist.

Übungsaufgabe 17.5. Bestimmen Sie die Kompositionsfaktoren von S_n für alle $n \in \mathbb{N}$.

Übungsaufgabe 17.6. Sei K ein Körper, $N \subseteq \mathrm{SL}_2(K)$ die Gruppe der oberen unipotenten Dreiecksmatrizen, $N^t \subseteq \mathrm{SL}_2(K)$ die dazu transponierte Untergruppe, und $D \subseteq \mathrm{SL}_2(K)$ die Gruppe der Diagonalmatrizen mit Determinante 1.

(1) Zeigen Sie

$$\mathrm{SL}_2(K) = \langle N, D, N^t \rangle.$$

(2) Berechnen Sie

$$\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & -x \\ & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & \\ & a \end{pmatrix} =$$

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

$$\begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} =$$

(Die dritte Identität geht auf Whitehead zurück.)

(3) Bestimmen Sie die Kommutatorfaktorgruppe von $\mathrm{SL}_2(K)$.

(4) Für welche K ist $\mathrm{SL}_2(K)$ auflösbar?

Tipp: Verwenden Sie Aufgabe 17.2 für die Ausnahmekörper $\mathbb{F}_2$ und $\mathbb{F}_3$.

Übungsaufgabe 17.7. Für welche Körper K und welche $n \in \mathbb{N}$ ist $\mathrm{GL}_n(K)$ auflösbar?

Tipp: Für $n \geq 2$ ist $\mathrm{SL}_2(K)$ eine Untergruppe von $\mathrm{GL}_2(K)$. Verwenden Sie nun Aufgabe 17.6.

18. Radikalerweiterungen

Wir wenden uns nun der Auflösbarkeit im Sinne der Körpererweiterungen zu.

18.1. **Galoistheorie des Wurzelziehens.** Wir wenden uns nun der Galoistheorie der Polynome $T^n - a$ mit $a \in K^\times$ zu. Dieses Polynom ist genau dann separabel, wenn n kein Vielfaches der Charakteristik von K ist, denn die Ableitung nT^{n-1} hat dann nur die Nullstelle $T = 0$.

Zunächst behandeln wir den Fall einer Primzahl.

Proposition 317. *Sei p eine Primzahl, K ein Körper und $a \in K$. Dann ist*
$$T^p - a \in K[T]$$
genau dann irreduzibel, wenn $a \notin K^p$.

Beweis. Wenn $a \in K^p$ ist, dann hat $T^p - a$ eine Nullstelle in K und ist sicher nicht irreduzibel.

Sei nun $a \notin K^p$ und α eine Nullstelle von $T^p - a$ in einem algebraischen Abschluß $\overline{K}$ von K. Sei $L = K(\alpha)$ und $d = [L : K]$. Dann ist
$$N_{L/K}(\alpha)^p = N_{L/K}(\alpha^p) = N_{L/K}(a) = a^d.$$
Wenn $d < p$, dann ist d teilerfremd zu p, somit gibt es $r, s \in \mathbb{Z}$ mit $rp + sd = 1$ und
$$a = a^{rp+sd} = \left(a^r N_{L/K}(\alpha)^s\right)^p \in K^p$$
im Widerspruch zur Annahme. Daher gilt $[L : K] = p$ und $T^p - a$ ist irreduzibel. □

Satz 318. *Sei K ein Körper und $0 < n \in \mathbb{N}$. Sei $a \in K$. Dann ist*
$$T^n - a$$
genau dann irreduzibel, wenn gilt:

(i) Für keinen Primteiler p von n ist $a \in K^p$.

(ii) Wenn $4 \mid n$, dann ist a nicht von der Form $a = -4b^4$ für ein $b \in K$.

Beweis. Wir zeigen zunächst, daß die Bedingungen notwendig sind für irreduzibilität. Sei daher $n = p \cdot m$ und $a = b^p$. Dann ist
$$T^m - b \mid T^n - a,$$
also $T^n - a$ nicht irreduzibel. Sei weiter $n = 4m$ und $a = -4b^4$, dann nutzen wir die Identität von Sophie Germain
$$\begin{aligned} A^4 + 4B^4 &= (A^4 + 4A^2B^2 + 4B^4) - 4A^2B^2 = (A^2 + 2B^2)^2 - (2AB)^2 \\ &= (A^2 + 2AB + 2B^2)(A^2 - 2AB + 2B^2), \end{aligned}$$
woraus
$$T^n - a = (T^m)^4 + 4b^4 = (T^{2m} + 2bT^m + 2b^2)(T^{2m} - 2bT^m + 2b^2)$$
folgt. Wieder ist $T^n - a$ nicht irreduzibel.

Wir müssen nun zeigen, daß dies die einzigen Szenarien sind, die zu Faktorisierungen führen. Wir nehmen daher nun (i) und (ii) an, und beweisen per Induktion nach n, daß $T^n - a$ irreduzibel ist. Der Induktionsanfang $n = 1$ ist klar. Sei
$$n = p \cdot m$$
mit einer Primzahl p, und sei $T^m - a$ irreduzibel. Sei α eine Nullstelle von $T^n - a$ und dann $\beta = \alpha^p$ eine Nullstelle von $T^m - a$. Sei
$$L = K(\alpha) \supseteq M = K(\beta) \supseteq K,$$
so daß $[M : K] = m$ gilt per Induktion und wir $[L : K] = n$ bzw. $[L : M] = p$ zu zeigen haben. Die Erweiterung L/M adjungiert eine Nullstelle von
$$T^p - \beta$$

und ist nach Proposition 317 vom Grad p genau dann, wenn β keine p-te Potenz in M ist. Angenommen $\beta = \gamma^p$ mit $\gamma \in M$. Dann gilt

$$-a = (-1)^m N_{M/K}(\beta) = (-1)^m N_{M/K}(\gamma)^p. \tag{18.1}$$

Wenn p ungerade ist, dann ist $-1 \in K^p$, und somit $a \in K^p$ im Widerspruch zur Voraussetzung. Es bleibt der Fall $p = 2$. Indem wir zunächst alle ungeraden Primfaktoren mit diesem Argument loswerden, dürfen wir nun annehmen, daß

$$n = 2^t$$

eine 2-er Potenz ist. Der Fall $n = 2$ ist durch Proposition 317 abgedeckt. Sei also $t \geq 2$.

Sei α, $\beta = \alpha^2$, $L = K(\alpha)$ und $M = K(\beta)$ wie oben, und per Induktion schon $[M : K] = 2^{t-1}$. Wir sind fertig, falls β kein Quadrat in M ist. Andernfalls wird (18.1) zu

$$-a \in K^2.$$

Falls $\operatorname{char}(K) = 2$, ist dies bereits ein Widerspruch zu $a \notin K^2$. Ansonsten wird mit $\sqrt{a} = \alpha^{n/2}$

$$K' := K(\alpha^{n/2}) = K(\sqrt{a}) = K(i)$$

mit $i^2 = -1$. Dies ist wegen $a \notin K^2$ nach Proposition 317 eine quadratische Erweiterung von K. Wir wollen nun die Induktionsvoraussetzung für $\sqrt{a} \in K'$ und

$$T^{n/2} - \sqrt{a}$$

anwenden. In K' ist -1 ein Quadrat und daher (ii) eine Konsequenz von (i), denn $-4b^4 = (2ib^2)^2$. Bleibt zu zeigen, daß $\sqrt{a}$ kein Quadrat in K' ist. Ansonsten ist für geeignete $x, y \in K$

$$\sqrt{a} = (x + iy)^2$$

also nach Binomischer Formel

$$a = \sqrt{a}^2 = (x + iy)^4 = (x^4 - 6x^2y^2 + y^4) + 4xy(x^2 - y^2) \cdot i.$$

Weil $a \in K$ muß $xy(x^2 - y^2) = 0$ sein. Wenn $x = 0$ oder $y = 0$, so ist $a = y^4$ oder x^4 ein Quadrat, Widerspruch. Bleibt $x^2 = y^2$ und dann ist

$$a = x^4 - 6x^2y^2 + y^4 = -4x^4$$

ebenfalls ein Widersruch (und endlich der Grund für die besondere Bedingung (ii)).

Per Induktion folgt nun, daß $[L : K'] = n/2$ und damit $[L : K] = n$ wie behauptet: $T^n - a$ ist irreduzibel. □

Korollar 319. *Sei K ein Körper, $a \in K$ und $0 < n \in \mathbb{N}$. Sei -1 ein Quadrat in K. Dann ist*

$$T^n - a$$

genau dann irreduzibel, wenn für keinen Primteiler p von n gilt $a \in K^p$.

Beweis. Da $-1 \in K^2$, folgt $-4b^4 \in K^2$ für alle $b \in K$. Damit ist Bedingung (ii) von Satz 318 eine Folge von Bedingung (i). □

Sei $a \in K$ und L Zerfällungskörper von $T^n - a$. Als Quotient von zwei Nullstellen von $T^n - a$ enthält L alle n-ten Einheitswurzeln. Sei α eine Nullstelle von $T^n - a$, dann ist

$$L = K(\alpha, \mu_n).$$

Die Erweiterung L/K ist galoissch genau dann, wenn die Charakteristik von K kein Teiler von n ist. In diesem Fall ist ein $\sigma \in \operatorname{Gal}(L/K)$ durch die Werte

$$\sigma(\zeta) = \zeta^{\chi_n(\sigma)},$$
$$\sigma(\alpha) = \zeta_n^{a_\sigma}\alpha$$

eindeutig bestimmt, wobei ζ_n eine fixierte primitive n-te Einheitswurzel ist,

$$a_\sigma \in \mathbb{Z}/n\mathbb{Z}$$

und

$$\chi_n : \mathrm{Gal}(L/K) \to \mathrm{Gal}(K(\mu_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

die Restriktion auf $K(\mu_n)$ gefolgt vom zyklotimischen Charakter ist. Wir haben nun einen injektiven Gruppenhomomorphsimus

$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$
$$\sigma \mapsto \begin{pmatrix} \chi_n(\sigma) & a_\sigma \\ 0 & 1 \end{pmatrix}$$

Das rechnet am besten jeder zur Übung selbst nach!

Proposition 320. *Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$ kein Vielfaches der Charakteristik von K. Sei L der Zerfällungskörper über K des Polynoms*

$$T^n - a.$$

(1) Die Galoisgruppe $\mathrm{Gal}(L/K)$ ist eine auflösbare Gruppe.
(2) Wenn K die n-ten Einheitswurzeln enthält, dann ist L/K eine zyklische Erweiterung von Grad ein Teiler von n.

Beweis. Die Voraussetzungen an n bedeuten, daß $T^n - a$ ein separables Polynom ist. Damit ist L/K galoissch.

(1) Nach obiger Diskussion ist die fragliche Galoisgruppe eine Untergruppe von

$$G = \left\{ \begin{pmatrix} a & b \\ & 1 \end{pmatrix} \ ; \ a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Nach Satz 310 reicht es aus, wenn G auflösbar ist. Die Abbildung

$$\begin{pmatrix} a & b \\ & 1 \end{pmatrix} \mapsto a$$

definiert einen Homomorphismus $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ mit Kern $N \simeq \mathbb{Z}/n\mathbb{Z}$. Daher ist $1 \subseteq N \subseteq G$ eine Subnomralreihe mit abelschen Faktoren, und G ist auflösbar.

(2) Wenn $\mu_n \subseteq K$, dann ist $\chi_n : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ der triviale Homomorphismus: $\chi_n(\sigma) = 1$ für alle σ. Daher ist $\mathrm{Gal}(L/K)$ sogar eine Untergruppe von

$$\mathbb{Z}/n\mathbb{Z} \simeq \left\{ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \ ; \ b \in \mathbb{Z}/n\mathbb{Z} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$
$$b \mapsto \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}.$$

Die Aussage folgt sofort. □

18.2. **Zyklische Erweiterungen.**

Definition 321. Eine **abelsche Erweiterung** ist eine galoissche Erweiterung mit abelscher Galoisgruppe. Eine **zyklische Erweiterung** ist eine galoissche Erweiterung mit zyklischer Galoisgruppe.

Beispiel 322. (1) $\mathbb{C}/\mathbb{R}$ ist zyklisch. Ebenso jede separable quadratische Erweiterung.
(2) Jede Zwischenerweiterung einer abelschen Erweiterung ist abelsch.
(3) Die Kreisteilungskörper sind abelsche Erweiterungen $\mathbb{Q}(\mu_n)/\mathbb{Q}$. Ein wichtiger Satz der Zahlentheorie, der Satz von Dedekind und Weber, besagt, daß jede abelsche Erweiterung von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten ist.
(4) Jede Erweiterung endlicher Körper ist zyklisch.

Zyklische Erweiterungen lassen sich übersichtlich beschreiben, wenn es die entsprechenden Einheitswurzeln im Grundkörper gibt.

Satz 323. *Sei K ein Körper der Charakteristik $p \geq 0$ und $n \in \mathbb{N}$. Sei $p = 0$ oder $p \nmid n$. Sei $\zeta_n \in K$ eine primitive n-te Einheitswurzel.*

Sei L/K eine zyklische Galoiserweiterung vom Grad n und $\sigma \in \mathrm{Gal}(L/K)$ ein Erzeuger. Dann gibt es $\alpha \in L$ mit

(1) $a = \alpha^n \in K$, *und* $\sigma(\alpha) = \zeta_n \alpha$,
(2) $L = K(\alpha)$ *ist Zerfällungskörper des irreduziblen Polynoms* $T^n - a \in K[T]$.

Beweis. Wir betrachten die **Lagrange–Resolvente**

$$\lambda = \sum_{i=0}^{n-1} \zeta_n^{-i} \sigma^i : L \to L.$$

Aus der linearen unabhängigkeit der Charaktere folgt, daß es ein $x \in L$ gibt, so daß

$$\alpha = \lambda(x) \neq 0.$$

Wir rechnen für (1)

$$\sigma(\alpha) = \sigma\big(\sum_{i=0}^{n-1} \zeta_n^{-i} \sigma^i(x)\big) = \sum_{i=0}^{n-1} \zeta_n^{-i} \sigma^{i+1}(x) = \zeta_n \cdot \sum_{i=0}^{n-1} \zeta_n^{-i-1} \sigma^{i+1}(x) = \zeta_n \cdot \sum_{i=0}^{n-1} \zeta_n^{-i} \sigma^i(x) = \zeta_n \alpha$$

und

$$\sigma(a) = (\sigma(\alpha))^n = (\zeta_n \alpha)^n = a.$$

Somit ist a invariant unter $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ und damit aus K.

Wir zeigen nun die entscheidende Aussage (2). Die Konjugierten von α sind $\sigma^i(\alpha) = \zeta_n^i \alpha$ für $i = 0, \ldots n-1$. Damit gibt es n Konjugierte und das Minimalpolynom von α hat Grad n. Da α eine Nullstelle von $T^n - a$ ist, muß das Minimalpolynom

$$P_{\alpha, L/K} = T^n - a$$

sein, und $T^n - a$ ist als ein Minimalpolynom ein irreduzibeles Polynom. Damit hat $K(\alpha)$ den Grad $[L : K] = n$ über K, somit gilt $L = K(\alpha)$. Und dies zeigt (2). □

18.3. **Zyklische p-Erweiterungen in Charakteristik p.** Teilt die Charakteristik den Grad einer zyklischen Erweiterung, so wird es im Allgemeinen schwierig; nicht so der einfachste Fall. Dies ist nun keine (multiplikative) Frage der Einheitswurzeln, p-te Einheitswurzeln gibt es in Charakteristik p sowieso nicht, sondern mehr eine additive Frage.

Im Folgenden wird das Artin–Schreier Polynom

$$\wp(T) = T^p - T$$

eine Rolle Spielen. Wenn K Charakteristik p hat, dann hat $\wp(T) \in K[T]$ genau $\mathbb{F}_p \subseteq K$ als Menge der Nullstellen, und

$$\wp(T) = \prod_{n=0}^{p-1} (T - n). \tag{18.2}$$

Satz 324. *Sei K ein Körper der Charakteristik $p > 0$. Sei L/K eine zyklische Galoiserweiterung vom Grad p mit Galoisgruppe erzeugt von $\sigma \in \mathrm{Gal}(L/K)$.*

(1) *Es gilt:*

$$\ker(\mathrm{tr}_{L/K}) = \{\sigma(x) - x \ ; \ x \in L\} = \mathrm{im}(\sigma - 1 : L \to L),$$

mit anderen Worten ist die Sequenz von K-Vektorräumen

$$0 \to K \to L \xrightarrow{\sigma - 1} L \xrightarrow{\mathrm{tr}_{L/K}} K \to 0.$$

exakt.

(2) *Es gibt ein $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1$,*

$$\wp(\alpha) = \alpha^p - \alpha = a \in K$$

und Minimalpolynom

$$P_{\alpha/K} = T^p - T - a.$$

Insbesondere gilt $L = K(\alpha) = K(\wp^{-1}(a))$.

Beweis. (1) Es gilt $\ker(\sigma - 1) = L^{\langle\sigma\rangle} = K$ nach dem Hauptsatz der Galoistheorie. Weiter ist $\mathrm{tr}_{L/K}$ surjektiv, da L/K separabel ist. Damit gilt

$$\dim(\mathrm{im}(\sigma - 1)) = [L : K] - 1 = \dim(\ker(\mathrm{tr}_{L/K})).$$

Es reicht nun zu zeigen, daß $\mathrm{im}(\sigma - 1) \subseteq \ker(\mathrm{tr}_{L/K})$. Dies folgt aus: für alle $x \in L$

$$\mathrm{tr}_{L/K} \circ (\sigma - 1)(x) = (1 + \sigma + \ldots + \sigma^{p-1})(\sigma - 1)(x) = (1 - \sigma^p)(x) = 0.$$

(2) Da $\mathrm{tr}_{L/K}(1) = p = 0$, liegt 1 nach (1) im Bild von $\sigma - 1$. Es gibt also ein $\alpha \in L$ mit $1 = \sigma(\alpha) - \alpha$, andersherum

$$\sigma(\alpha) = \alpha + 1.$$

Per Induktion berechnet man die Konjugierten

$$\sigma^i(\alpha) = \alpha + i.$$

Dieses α hat p Konjugierte, also sein Minimalpolynom den Grad p. Das Minimalpolynom von α über K ist daher via (18.2)

$$P_{\alpha/K} = \prod_{n=0}^{p-1}(T - (\alpha + n)) = \prod_{n=0}^{p-1}((T - \alpha) - n) = (T - \alpha)^p - (T - \alpha) = T^p - T - \wp(\alpha)$$

Wir schließen daraus, daß $a = \wp(\alpha) \in K$ und

$$L = K(\wp^{-1}(a))$$

mit der Galoiswirkung von σ auf

$$\wp^{-1}(a) = \{\alpha, \alpha + 1, \ldots, \alpha + (p - 1)\}$$

durch $x \mapsto x + 1$. □

18.4. **Eine Anwendung.** Als Anwendung der Sätze über zyklische Galoiserweiterungen dsikutieren wir nun Körper mit endlicher Galoistheorie.

Theorem 325 (Artin)**.** *Sei K ein Körper mit algebraischem Abschluß $\overline{K}$. Wenn $\overline{K}/K$ endlich ist, dann ist*

$$[\overline{K} : K] \leq 2$$

und $\overline{K} = K(i)$ für eine Nullstelle i von $T^2 + 1$.

Beweis. Schritt 1, K ist perfekt: Sei L/K eine endliche Erweiterung in Charakteristik p. Der Frobenius ist ein Isomorphismus von L/K mit L^p/K^p. Daher gilt $[K : K^p]$ ist endlich genau dann wenn $[L : L^p]$ endlich ist und dann gilt

$$[K : K^p] = \frac{[L : K^p]}{[L : K]} = \frac{[L : K^p]}{[L^p : K^p]} = [L : L^p].$$

Dies wenden wir hier auf $L = \overline{K}$ an und erhalten

$$[K : K^p] = [\overline{K} : \overline{K}^p] = 1.$$

Schritt 2: Wir schließen, daß $\overline{K}/K$ endlich separabel und offensichtlich auch normal ist. Damit ist $\overline{K}/K$ eine endliche Galoiserweiterung. Wie setzen nun $G = \mathrm{Gal}(\overline{K}/K)$.

Schritt 3, oBdA ist -1 ein Quadrat in K: Wenn K Charakteristik 2 hat, ist nichts zu tun: $-1 = 1^2$. Ansonsten ersetzen wir K durch $K(i)$ mit $i^2 = -1$, und haben nun zu zeigen, daß $\overline{K} = K$. Wir nehmen daher an, daß $G \neq 1$ und führen dies zu einem Widerspruch.

Schritt 4: Sei p ein Primteiler von $\#G$ und nicht die Charakteristik von K. Dann gibt es $g \in G$ von Ordnung p. Wir ersetzen G durch $H = \langle g \rangle$ und K durch $\overline{K}^H$. Wir dürfen also oBdA annehmen, daß G zyklisch von Ordnung p ist.

Dann enthält K die p-ten Einheitswurzeln, denn die Erweiterung $K(\mu_p)/K$ ist galoissch mit Galoisgruppe eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$. Damit ist $[K(\mu_p) : K]$ ein Teiler von $p-1$ und teilerfremd zu $[\overline{K} : K] = p$, also nach dem Gradsatz $[K(\mu_n) : K] = 1$. Damit enthält K die p-ten Einheitswurzeln und Satz 323 findet Anwendung: Es gibt ein $a \in K$ mit $\overline{K} = K(\sqrt[p]{a})$. Daraus folgt, daß a in K keine p-te Potenz ist. Nach Korollar 319 ist dann auch $T^{p^n} - a$ irreduzibel für alle $n \geq 1$, wobei wir nutzen, daß -1 ein Quadrat in K ist. Damit gibt es algebraische Erweiterungen von Grad p^n für alle $n \in \mathbb{N}$. Dies ist ein Widerspruch zu $[\overline{K} : K] = p$.

Schritt 5: Es bleibt der Fall, daß K von Charakteristik p ist, und G eine p-Gruppe. Wir ersetzen wieder K durch den Fixkörper einer zyklischen Untergruppe der Ordnung p. Dann ist $\overline{K} = K(\alpha)$ mit

$$\wp(\alpha) = \alpha^p - \alpha = a \in K.$$

Da $\wp = \mathrm{Frob} - \mathrm{id}$ und Frob und id mit jedem Körperautomorphismus kommutieren, und $\mathrm{tr}_{\bar{K}/K}$ nach Satz 245 eine Summe von Körperautomorphismen ist, gilt

$$\begin{aligned}\mathrm{tr}_{\bar{K}/K} \circ \wp = \mathrm{tr}_{\bar{K}/K} \circ (\mathrm{Frob} - \mathrm{id}) &= \mathrm{tr}_{\bar{K}/K} \circ \mathrm{Frob} - \mathrm{tr}_{\bar{K}/K} \\ &= \mathrm{Frob} \circ \mathrm{tr}_{\bar{K}/K} - \mathrm{tr}_{\bar{K}/K} = (\mathrm{Frob} - \mathrm{id}) \circ \mathrm{tr}_{\bar{K}/K} = \wp \circ \mathrm{tr}_{\bar{K}/K}.\end{aligned}$$

Da $\overline{K}/K$ separabel ist, gibt es ein $\beta \in \overline{K}$ mit

$$\mathrm{tr}_{\bar{K}/K}(\beta) = a.$$

Da $\overline{K}$ algebraisch abgeschlossen ist, gibt es $x \in \overline{K}$ mit $\wp(x) = \beta$. Aber dann ist

$$a = \mathrm{tr}_{\bar{K}/K}(\beta) = \mathrm{tr}_{\bar{K}/K}(\wp(x)) = \wp(\mathrm{tr}_{\bar{K}/K}(x)) \in \wp(K).$$

Die Lösungen von $\wp(T) = a$ sind gegeben durch $\alpha + n$ für $n \in \mathbb{F}_p$. Daher sind mit einer Lösung automatisch alle in K. Es folgt $\alpha \in K$, ein Widerspruch. $\square$

18.5. **Auflösbarkeit von Gleichungen durch Radikale.** Der Begriff *Auflösbarkeit* kommt ursprünglich nicht aus der Gruppentheorie sondern aus der Theorie des Lösens von Polynomgleichungen.

Bemerkung 326. Eine quadratische Gleichung

$$T^2 + pT + q = 0$$

mit $p, q \in K$ und $2 \in K^\times$ hat bekanntlich die Lösungen

$$t_{1/2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2},$$

die durch Quadratwurzeln der Diskriminante $p^2 - 4q$ des quadratischen Polynoms dargestellt werden können. In (unzulässiger) Verallgemeinerung werden daher auch allgemeiner Nullstellen von Polynomen als **Wurzeln** des Polynoms bezeichnet.

Notation 327. Wir vereinbaren die Notation

$$\sqrt[\infty]{K}$$

für eine Erweiterung des Körpers K, die von den Nullstellen aller Polynome $T^n - a$ mit $n \in \mathbb{N}$ und $a \in K$ erzeugt wird. Da $\sqrt[\infty]{K}/K$ per Definition ein Zerfällungskörper ist, so ist die Erweiterung bis auf isomorphie eindeutig.

Definition 328. Sei K ein Körper.

(1) Der **Körper der Radikalausdrücke n-ter Stufe** für $n \in \mathbb{N}_0$ wird induktiv definiert über

$$K_0 := K,$$
$$K_{n-\text{solv}} := \sqrt[\infty]{K_{(n-1)-\text{solv}}} \quad \text{für } n \geq 1.$$

Der **Körper der Radikalausdrücke** über K ist dann

$$K_{\text{solv}} := \bigcup_{n \geq 0} K_{n-\text{solv}}$$

(2) Für ein Polynom $f \in K[T]$ heißt die Polynomgleichung

$$f(T) = 0$$

auflösbar (durch Radikale), wenn alle Wurzeln von f in K_{solv} liegen.

(3) Eine von **auflösbare Körpererweiterung** ist eine Körpererweiterung L/K, die von Elementen aus K_{solv} erzeugt werden kann.

Bemerkung 329. (1) Der Wortstamm *Radikal* entstammt dem lateinischen *radix*, zu deutsch Wurzel.

(2) Notation 327 und Definition 328 sind etwas unsauber. Besser wäre es, zunächst einen algebraischen Abschluß Ω/K zu wählen und dann alle Körper als Teilkörper von Ω zu definieren.

(3) Offensichtlich ist L/K genau dann durch Radikale erzeugt, wenn $L \subseteq K_{\text{solv}}$. Ist L/K zudem endlich, so ist dies äquivalent zur Existrenz eines Körperturms

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$$

mit $L \subseteq K_n$ der folgenden Form: für alle $0 \leq i \leq n-1$ gibt es Elemente $a_i \in K_i$ und $m_i \in \mathbb{N}$, so daß K_{i+1} als Erweiterung von K_i durch Adjunktion einer Nullstelle von $T^{m_i} - a_i$ entsteht.

(4) Die Gleichungen der Form $T^n - 1 = 0$ werden auch betrachtet. Daher gilt

$$K(\mu_\infty) \subseteq K_{1-\text{solv}} \subseteq K_{\text{solv}}.$$

Proposition 330. *Sei L/K eine Körpererweiterung und M, M_1, M_2 Zwischenkörper.*

(1) L/K ist auflösbar genau dann, wenn L/M und M/K auflösbar sind.

(2) Sind M_1/K und M_2/K auflösbar, dann auch das Kompositum M_1M_2/K.

(3) Ist L/K rein inseparabel, so ist L/K auflösbar.

(4) Eine endliche Erweiterung L/K ist auflösbar genau dann, wenn ihre normale Hülle auflösbar ist.

Beweis. (1) Sei L/K auflösbar. Dann ist $M \subseteq L \subseteq K_{\text{solv}}$ und daher M/K auflösbar. Außerdem gilt $L \subseteq K_{\text{solv}} \subseteq M_{\text{solv}}$ und daher L/M auflösbar.

Sein nun L/M und M/K auflösbar. Dann gibt es $n, m \in \mathbb{N}$ mit $M \subseteq K_{n-\text{solv}}$ und $L \subseteq M_{m-\text{solv}}$. Es folgt dann offensichtlich

$$L \subseteq M_{m-\text{solv}} \subseteq (K_{n-\text{solv}})_{m-\text{solv}} = K_{n+m-\text{solv}}$$

und somit L/K auflösbar.

(2) Nach Voraussetzung ist $M_i \subseteq K_{\text{solv}}$ für $i = 1, 2$. Damit ist auch das Kompositum M_1M_2 in K_{solv} enthalten und damit über K auflösbar.

(3) Rein inseparable Erweiterungen in Charakteristik $p > 0$ lassen sich nach Korollar 171 induktiv über einfache Erweiterungen mit Minimalpolynom der Form $T^p - a$ erzeugen. Damit sind sie auflösbar.

(4) Sei Ω ein algebraischer Abschluß von L und $\tilde{L}$ die normale Hülle von L/K in Ω. Wenn $\tilde{L}/K$ auflösbar ist, dann auch nach (1) die Teilerweiterung L/K.

Sei umgekehrt nun L/K auflösbar. Für jede K-Einbettung $\sigma : L \to \Omega$ ist $\sigma(L)/K$ per Strukturtransport mit σ ebenfalls auflösbar. Die normale Hülle $\tilde{L}$ ist das Kompositum in Ω der endlich vielen Körper $\sigma(L)$ und damit nach (2) ebenfalls auflösbar. □

Der folgende Satz bringt die Begriffe *auflösbar* aus der Welt der Polynomgleichungen, der Körpererweiterungen und der Gruppen zusammen.

Satz 331. *Sei K ein Körper der Charakteristik 0, L/K eine endliche Erweiterung und $f \in K[T]$ ein Polynom.*

(1) Das Polynom f ist auflösbar durch Radikale genau dann, wenn der Zerfällungskörper von f eine auflösbare Erweiterung von K ist.
(2) L/K is auflösbar genau dann, wenn die Galoisgruppe $\mathrm{Gal}(\tilde{L}/K)$ der galoisschen Hülle $\tilde{L}$ von L/K eine auflösbare Gruppe ist.

Bemerkung 332. Wir müssen annehmen, daß K ein Körper der Charakteristik 0 ist, denn die angestrebte Form der Adjunktion von Radikalen gilt nicht für zyklische Erweiterungen vom Grad p in Charakeristik p, obwohl diese offensichtlich auflösbare Galoisgruppen haben. Dazu siehe Satz 324. Eine Radikalerweiterung vom Grad p wäre rein inseparabel, während zyklische Erweiterungen galoissch und damit separabel sind.

Beweis. Aussage (1) folgt sofort aus der Definition. Wir zeigen nun (2). Sei dazu zunächst L/K auflösbar und $\tilde{L}$ eine galoissche Hülle. Nach Proposition 330 (4) ist auch $\tilde{L}/K$ auflösbar. Wir dürfen also oBdA von Anfang an annehmen, daß L/K eine Galoiserweiterung ist. Das tun wir nun zur Vereinfachung der Notation.

Es gibt einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$$

mit

$$L \subseteq K_n$$

und für alle $0 \le i \le n-1$ Elementen $a_i \in K_i$, so daß K_{i+1} für ein $m_i \in \mathbb{N}$ aus K_i durch Adjunktion einer Nullstelle von $T^{m_i} - a_i$ entsteht.

Wir setzen N für das kleinste gemeinsame Vielfache der $m_1, \ldots, m_{n-1}$ und betrachten

$$L' = LK(\mu_N).$$

Als Kompositum zweier Galoiserweiterungen ist L'/K auch galoissch. Da die Restriktion

$$\mathrm{Gal}(L'/K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

surjektiv ist, reicht es aus zu zeigen, daß $\mathrm{Gal}(L'/K)$ eine auflösbare Gruppe ist.

Wir betrachten nun für alle $i = 0, \ldots, n-1$ die Körper $K_i' = K_i(\mu_N)$ und den Turm

$$K = K_{-1}' \subseteq K_0' \subseteq K_1' \subseteq \ldots \subseteq K_n'$$

mit

$$L' \subseteq K_n'.$$

Die Erweiterungen

$$K_i'/K_{i-1}'$$

sind für alle $i = 0, \ldots n-1$ abelsch: für $i = 0$ ist dies $K(\mu_N)/K$ und für $i > 0$ ziehen wir die m_i-te Wurzel über einem Körper der die N-ten Einheitswurzeln und damit auch die m_i-ten Einheitswurzeln enthält. Dies ist zyklisch (also insbesondere abelsch) nach Proposition 320 (2).

Wir setzen nun $L_i' = L' \cap K_i'$. Dies ist ein Körperturm

$$K = L_{-1}' \subseteq L_0' \subseteq L_1' \subseteq \ldots \subseteq L_n' = L'.$$

Wir werden zeigen, daß die Untergruppen

$$\mathrm{F}^i(G) := \mathrm{Gal}(L'/L_{i-1}')$$

eine Subnormalreihe von $G = \mathrm{Gal}(L'/K)$ mit abelschen Faktoren bilden. Dazu betrachten wir das Diagramm von Körpererweiterungen

$$\begin{tikzcd}
& L'K'_{i+1} \arrow[dl, dash] \arrow[dr, dash] & & \\
L' \arrow[dr, dash] & & K'_{i+1} \arrow[dl, dash] \arrow[dr, dash] & \\
& L'_{i+1} \arrow[dr, dash] & & K'_i \arrow[dl, dash] \\
& & L'_i \arrow[d, dash] & \\
& & K &
\end{tikzcd}$$

Die Erweiterung $L'K'_{i+1}/K'_i$ ist galoissch als Kompositum der galoisschen Erweiterungen K'_{i+1} und $L'K'_i/K'_i$; letztere ist separabel und normal, weil L'/K separabel und normal ist. Wir bestimmen das Bild der Restriktionsabbildung

$$r : \mathrm{Gal}(L'K'_{i+1}/K'_i) \to \mathrm{Gal}(L'/K)$$

durch den vom Bild beschriebenen Fixkörper:

$$L'^{\,\mathrm{im}(r)} = L' \cap (L'K'_{i+1})^{\mathrm{Gal}(L'K'_{i+1}/K'_i)} = L' \cap K'_i = L'_i.$$

Das Bild ist also die Untergruppe $\mathrm{Gal}(L'/L'_i)$. Wir zeigen nun, daß L'_{i+1}/L'_i galoissch ist. Dazu müssen wir für jedes $\sigma \in \mathrm{Gal}(L'/L'_i)$ zeigen: $\sigma(L'_{i+1}) = L'_{i+1}$. Sei $\tilde{\sigma} \in \mathrm{Gal}(L'K'_{i+1}/K'_i)$ eine beliebige Fortsetzung von σ. Dann ist

$$\sigma(L'_{i+1}) \subseteq \sigma(L') = L'$$

und

$$\sigma(L'_{i+1}) \subseteq \tilde{\sigma}(K'_{i+1}) = K'_{i+1}$$

also insgesamt

$$\sigma(L'_{i+1}) \subseteq L' \cap K'_{i+1} = L'_{i+1}.$$

Galoistheorie liefert das folgende Diagramm von Gruppen

$$\begin{tikzcd}
\mathrm{Gal}(L'K'_{i+1}/K'_i) \arrow[r, two heads, "r"] \arrow[d, two heads] & \mathrm{Gal}(L'/L'_i) \arrow[d, two heads] \\
\mathrm{Gal}(K'_{i+1}/K'_i) \arrow[r, dotted, "\rho"] & \mathrm{Gal}(L'_{i+1}/L'_i)
\end{tikzcd}$$

Der Homomorphismus ρ existiert wegen der universellen Eigenschaft der Faktorgruppe (linker vertikaler Homomorphismus) als Quotient, denn alle $\tilde{\sigma} \in \mathrm{Gal}(L'K'_{i+1}/K'_{i+1})$ wirken als Identität auf K'_{i+1} und demnach auch auf L'_{i+1}.

Das Bild von ρ bestimmen wir wieder wie eben durch das Betrachten des entsprechenden Fixkörpers

$$(L'_{i+1})^{\mathrm{im}(\rho)} = L'_{i+1} \cap (L'K'_{i+1})^{\mathrm{Gal}(L'K'_{i+1}/K'_i)} = L'_{i+1} \cap (L')^{\mathrm{Gal}(L'/L'_i)} = L'_i.$$

Daher ist ρ surjektiv und

$$\mathrm{F}^{i+1}(G)/\,\mathrm{F}^{i+2}(G) = \mathrm{Gal}(L'/L'_i)/\,\mathrm{Gal}(L'/L'_{i+1}) = \mathrm{Gal}(L'_{i+1}/L'_i)$$

als Quotient der abelschen Gruppe $\mathrm{Gal}(K'_{i+1}/K'_i)$ selbst abelsch. Die beweist die Behauptung über die Filtrierung $\mathrm{F}^\bullet(G)$, und deshalb ist $\mathrm{Gal}(L'/K)$ auflösbar im Sinne von Gruppen.

Wir müssen nun die andere Richtung zeigen. Sei dazu $\tilde{L}/K$ die galoissche Hülle von L/K und $\mathrm{Gal}(\tilde{L}/K)$ eine auflösbare Gruppe der Ordnung N. Wenn wir zeigen, daß $\tilde{L}/K$ auflösbar ist, dann gilt das auch für die Teilerweiterung L/K nach Proposition 330 (1). Wir dürfen also oBdA annehmen, daß L/K selbst bereits galoissch ist. Das tun wir nun wieder zur Vereinfachung der Notation.

Sei $N = [L : K]$ die Ordnung von $G = \mathrm{Gal}(L/K)$. Und sei $\mathrm{F}^\bullet(G)$ eine Subnormalreihe von G mit abelschen Faktoren. Weil jede abelsche Gruppe eine Subnormalreihe mit zyklischen Faktoren besitzt (Übungsaufgabe!), dürfen wir nach Verfeinerung annehmen, daß alle Faktoren zyklisch sind. Sei

$$K = K_0 \subseteq \ldots \subseteq K_i = L^{\mathrm{F}^i(G)} \subseteq \ldots \subseteq K_n = L$$

der ensprechende Turm der Fixkörper. Da $\mathrm{F}^\bullet(G)$ Subnormalreihe ist, sind die Teilerweiterungen K_i/K_{i-1} sämtlich galoissch. Und da die Faktoren zyklisch sind, sind die K_i/K_{i-1} zyklische Erweiterungen vom Grad m_i ein Teiler von N.

Wir betrachten nun den Turm

$$K = K'_{-1} \subseteq K'_0 \subseteq \ldots \subseteq K'_n = L' = L(\mu_N)$$

mit $K'_i = K_i(\mu_N)$. Per Restriktion ist

$$\mathrm{Gal}(K'_i/K'_{i-1}) \hookrightarrow \mathrm{Gal}(K_i/K_{i-1})$$

injektiv, und daher auch zyklisch von Ordnung einem Teiler m'_i von N. Der Schritt K'_0/K'_{-1} ist zyklotomisch, also auflösbar. Jeder weitere Schritt K'_i/K'_{i-1} mit $i \geq 1$ ist zyklisch in Gegenwart der entsprechenden Einheitswurzeln, also auch auflösbar nach Proposition 320. Als Turm auflösbarer Erweiterungen ist L'/K auflösbar, und damit auch die Teilerweiterung L/K auflösbar. $\square$

Beispiel 333. Das Polynom

$$f = T^5 - 4T + 2 \in \mathbb{Q}[T]$$

ist nicht auflösbar durch Radikale. Wir haben in Beispiel 239 gesehen, daß

$$\mathrm{Gal}(f) \simeq S_5$$

und S_5 ist keine auflösbare Gruppe nach Korollar 311.

18.6. **Kummertheorie.** Kummertheorie beschreibt abelsche Erweiterungen vom Exponent n für gewisse Körper K.

Definition 334. Der **Exponent** einer Gruppe ist das kleinste gemeinsame Vielfache der Ordnungen der Elemente von G, sofern dieses kgV existiert.

Man sagt (ungenau), daß eine Gruppe G *vom Exponenten n ist*, wenn der Exponent von G ein Teiler von n ist.

Für den Begriff der Paarung abelscher Gruppen und Pontrajagin–Dualität sei Auf Anhang C verwiesen.

Satz 335 (Kummertheorie I)**.** *Sei K ein Körper, $1 \leq n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $\mu_n \subseteq K$. Sei L/K eine endliche abelsche Erweiterung mit Galoisgruppe $\mathrm{Gal}(L/K)$ vom Exponenten n.*

(1) Zu $a \in \Delta_L := (L^\times)^n \cap K^\times$ und $\alpha \in L^\times$ mit $\alpha^n = a$ definiert

$$\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}$$

einen Gruppenhomomorphismus

$$\chi_a : \mathrm{Gal}(L/K) \to \mu_n,$$

der unabhängig von der Wahl von α ist. Der Fixkörper von $\ker(\chi_a)$ ist $K(\alpha)$.

(2) *Die Abbildung*

$$\begin{aligned}\mathrm{Gal}(L/K) \times \Delta_L/(K^\times)^n &\to \mu_n\\ (\sigma, a) &\mapsto \chi_a(\sigma),\end{aligned}$$

ist eine perfekte Paarung endlicher abelscher Gruppen vom Exponenten n.

(3) *L/K wird als Erweiterung von der Menge*

$$\sqrt[n]{\Delta_L} := \{\alpha \in L^\times \; ; \; \alpha^n \in K^\times\}$$

erzeugt.

(4) *Es gelten*

$$\begin{aligned}\mathrm{Gal}(L/K) &\simeq \mathrm{Hom}(\Delta_L/(K^\times)^n, \mu_n),\\ \Delta_L/(K^\times)^n &\simeq \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n).\end{aligned}$$

Beweis. (1) Zunächst sind die $a \in \Delta_L$ genau diejenigen Elemente von $K^\times$ für die es ein $\alpha \in L^\times$ mit der geforderten Eigenschaft gibt.

Wegen $(\sigma(\alpha)/\alpha)^n = \sigma(a)/a = 1$ ist $\sigma(\alpha)/\alpha \in \mu_n$. Wählt man statt α eine andere n-te Wurzel α' von a, dann geibt es $\zeta \in \mu_n \subseteq K$ mit $\alpha' = \zeta\alpha$ und

$$\frac{\sigma(\alpha')}{\alpha'} = \frac{\sigma(\zeta\alpha)}{\zeta\alpha} = \frac{\zeta \cdot \sigma(\alpha)}{\zeta\alpha} = \frac{\sigma(\alpha)}{\alpha}.$$

Damit ist $\chi_a(\sigma) \in \mu_n$ unabhängig von der Wahl der n-ten Wurzel α.

Für $\sigma, \tau \in \mathrm{Gal}(L/K)$ gilt

$$\chi_a(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)} \cdot \frac{\tau(\alpha)}{\alpha} = \chi_a(\sigma) \cdot \chi_a(\tau),$$

denn auch $\alpha' = \tau(\alpha)$ ist zur Berechnung von $\chi_a(\sigma)$ geeignet. Damit ist χ_a ein Gruppenhomomorphismus. Es gilt

$$\sigma \in \ker(\chi_a) \iff \sigma(\alpha) = \alpha \iff \sigma \in \mathrm{Gal}(L/K(\alpha)),$$

somit ist $K(\alpha)$ der Fixkörper zum Kern von χ_a.

(2) Aus (1) folgt, daß $\chi_a(\sigma)$ additiv in σ ist. Seien $a, b \in \Delta_L$ und $\alpha, \beta \in L^\times$ mit $\alpha^n = a$ und $\beta^n = b$. Dann gilt $(\alpha\beta)^n = ab$ und

$$\chi_{ab}(\sigma) = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\sigma(\beta)}{\beta} = \chi_a(\sigma) \cdot \chi_b(\sigma).$$

Damit ist $(\sigma, a) \mapsto \chi_a(\sigma)$ eine Paarung abelscher Gruppen

$$\mathrm{Gal}(L/K) \times \Delta_L \to \mu_n.$$

Für $a \in \Delta_L$ und $\alpha \in L^\times$ mit $\alpha^n = a$ gilt

$$\begin{aligned}&\chi_a(\sigma) = 1 \text{ für alle } \sigma \in \mathrm{Gal}(L/K)\\ \iff &\sigma(\alpha) = \alpha \text{ für alle } \sigma \in \mathrm{Gal}(L/K)\\ \iff &\alpha \in L^{\mathrm{Gal}(L/K)} = K\\ \iff &a \in (K^\times)^n.\end{aligned}$$

Es folgt, daß $(\sigma, a) \mapsto \chi_a(\sigma)$ eine Paarung abelscher Gruppen

$$\mathrm{Gal}(L/K) \times \Delta_L/(K^\times)^n \to \mu_n$$

induziert, die überdies rechts-nichtausgeartet ist. Die zugehörige adjungierte Abbildung

$$\rho : \Delta_L/(K^\times)^n \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n),$$

$\rho(a) = \chi_a$, ist damit injektiv mit Werten in einer endliche Gruppe $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \simeq \mathrm{Gal}(L/K)^\vee$. Beide Gruppen der Paarung sind somit endlich. Weil offensichtlich $\Delta_L^n \subseteq (K^\times)^n$, sind beide Seiten außerdem vom Exponenten n.

Wir müssen noch zeigen, daß die Paarung perfekt ist. Dazu zeigen wir, daß ρ auch surjektiv ist, und verwenden dann Satz 413. Sei $\varphi : \mathrm{Gal}(L/K) \to \mu_n$ ein Gruppenhomomorphismus. Der Fixkörper zu $\ker(\varphi)$ sei der Zwischenkörper M. Dann induziert φ einen injektiven Gruppenhomomorphismus

$$\bar{\varphi} : \mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)/\ker(\varphi) \hookrightarrow \mu_n.$$

Daher ist M/K zyklisch von Grad d, einem Teiler von n. Mit μ_n ist auch $\mu_d \subseteq K$. Sei $\zeta \in \mu_d \subseteq \mu_n$ ein Erzeuger des Bildes von φ (oder $\bar{\varphi}$) und $\bar{\sigma} \in \mathrm{Gal}(M/K)$ mit $\bar{\varphi}(\bar{\sigma}) = \zeta$.

Nach Satz 323 gibt es dann ein $b \in K$ und ein $\alpha \in M$ mit

(i) $\alpha^d = b$, und
(ii) $\bar{\sigma}(\alpha) = \zeta\alpha$, und
(iii) $M = K(\alpha)$.

Sei $n = dm$. Wir setzen $a = b^m$ und haben damit $\alpha^n = a$. Dann gilt

$$\rho(a) = \chi_a = \varphi.$$

In der Tat, haben χ_a und φ den gleichen Kern, nämlich die Untergruppe, die zu $M = K(\alpha)$ gehört, und es reicht die induzierten Homomorphismen $\bar{\varphi}, \bar{\chi}_a : \mathrm{Gal}(M/K) \to \mu_n$ zu vergleichen. Weil $\mathrm{Gal}(M/K)$ zyklisch ist, reicht es weiter χ_a und φ auf einem Erzeuger von $\mathrm{Gal}(M/K)$ zu vergleichen:

$$\bar{\chi}_a(\bar{\sigma}) = \frac{\bar{\sigma}(\alpha)}{\alpha} = \frac{\zeta\alpha}{\alpha} = \zeta = \bar{\varphi}(\bar{\sigma}).$$

Dies zeigt nun die behauptete Surjektivität von ρ.

(3) Sei M der Zwischenkörper von L/K, der von $\sqrt[n]{\Delta_L}$ erzeugt wird. Dann gilt

$$\mathrm{Gal}(L/M) = \{\sigma \ ; \ \sigma(\alpha) = \alpha \text{ für alle } \alpha \in \sqrt[n]{\Delta_L}\} = \{\sigma \ ; \ \chi_a(\sigma) = 1 \text{ für alle } a \in \Delta_L\}.$$

Das ist die triviale Untergruppe, da die Paarung in (2) perfekt, also insbesondere links-nicht-ausgeartet ist. Per Galoiskorrespondenz folgt $L = M$.

Aussage (4) folgt sofort aus der Perfektheit der Paarung in (2) und Satz 413, wobei Bemerkung 417 zu beachten ist. $\square$

Satz 336 (Kummertheorie II)**.** *Sei K ein Körper und $1 \leq n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$ und $\mu_n \subseteq K$. Sei Ω ein algebraischer Abschluß von K. Die Abbildung*

$$M \mapsto \Delta_M = (M^\times)^n \cap K^\times$$

definiert eine Bijektion

$$\left\{ M/K \ ; \ \begin{array}{c} M \subseteq \Omega, \ \textit{endlich galoissch } /K \textit{ mit} \\ \mathrm{Gal}(M/K) \ \textit{ abelsch, Exponent teilt } n \end{array} \right\} \to \left\{ (K^\times)^n \subseteq \Delta \subseteq K^\times \ ; \ \begin{array}{c} \Delta/(K^\times)^n \\ \textit{endlich erzeugt} \end{array} \right\}$$

mit inverser Abbildung

$$\Delta \mapsto K(\sqrt[n]{\Delta}),$$

wobei $\sqrt[n]{\Delta} = \{\alpha \in \Omega \ ; \ \alpha^n \in \Delta\}$.

Beweis. Wir schließen aus Satz 335, daß zu M/K wie im Satz die Gruppe $\Delta_M = (M^\times)^n \cap K^\times$ die geforderten Eigenschaften hat, somit die Abbildung wohldefiniert ist.

Da K die n-ten Einheitswurzeln enthält, und da $K(\sqrt[n]{\Delta})$ bereits als Erweiterung von K durch die n-ten Wurzeln von Vertretern der Erzeuger von $\Delta/(K^\times)^n$ erzeugt wird, beschreibt $M_\Delta := K(\sqrt[n]{\Delta})$ tatsächlich eine endlich erzeugte Teilerweiterung von K in Ω. Die Erweiterung

M_Δ/K ist offenbar ein gemeinsamer Zerfällungskörper der separablen Polynome $T^n - a$ für alle $a \in \Delta$. Daher ist M_Δ/K galoissch. Die Zuordnung

$$\begin{gathered}\mathrm{Gal}(M_\Delta/K) \to \mathrm{Hom}(\Delta/(K^\times)^n, \mu_n)\\ \sigma \mapsto (a \mapsto \chi_a(\sigma))\end{gathered}$$

ist ein Gruppenhomomorphismus (wie aus Satz 335 bekannt) und offenbar injektiv. Daher ist M_Δ/K eine abelsche Erweiterung und die angegebene Umkehrabbildung wohldefiniert.

Es bleibt zu zeigen, daß die angegebenen Abbildungen zueinander invers sind. Es gilt

$$M = K(\sqrt[n]{\Delta_M})$$

nach Satz 335(3). Weiter ist offenbar

$$\Delta \subseteq \Delta_{M_\Delta}.$$

Wir betrachten die zu $\bar{\Delta} = \Delta/(K^\times)^n$ orthogonale Gruppe bezüglich der Paarung der Kummertheorie

$$\mathrm{Gal}(M_\Delta/K) \times \Delta_{M_\Delta}/(K^\times)^n \to \mu_n.$$

Es gilt

$$\bar{\Delta}^\perp = \{\sigma \in \mathrm{Gal}(M_\Delta/K)\ ;\ \sigma(\alpha) = \alpha \text{ für alle } \alpha \in \sqrt[n]{\Delta}\} = \mathrm{Gal}(M_\Delta/K(\sqrt[n]{\Delta})) = 1.$$

Daher ist nach Satz 416

$$\bar{\Delta} = (\bar{\Delta}^\perp)^\perp = (1)^\perp = \Delta_{M_\Delta}/(K^\times)^n,$$

und daher auch $\Delta = \Delta_{M_\Delta}$. Das war zu zeigen. $\square$

Teil 4. Funktionenkörper

19. Funktionenkörper in mehreren Variablen

Zu einem Ring R gibt es den Polynomring in einer Variablen $R[X]$.

19.1. **Polynome in mehreren Variablen.** Iteriert man diese Konstruktion so bekommt man induktiv

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

den Polynomring in n Variablen mit Koeffizienten in R. Es ist wichtig, die dieser induktiven Konstruktion fehlende Symmetrie zwischen den vairablen wiederherzustellen. Dazu benutzen wir Multiindizes für eine kompakte Notation. Ein Multiindex

$$I = (i_1, \ldots, i_n)$$

der Länge n besteht aus $i_\alpha \in \mathbb{N}_0$ für $\alpha = 1, \ldots, n$. Der Grad des Multiindex ist

$$\deg(I) = \#I = \sum_{\alpha=1}^{n} i_\alpha$$

und das zu I gehörende Monom ist

$$X^I = \prod_{\alpha=1}^{n} X_\alpha^{i_\alpha}.$$

Es gelten zur Notation passende Rechenregeln wie

$$X^I \cdot X^J = X^{I+J},$$

wobei die Multiindizes wie Elemente von $\mathbb{Z}^n$ addiert werden.

Ein Element $f \in R[X_1, \ldots, X_n]$ hat nun eine eindeutige Darstellung als endliche Summe

$$f = \sum_I a_I X^I \tag{19.1}$$

mit $a_I \in R$, fast alle 0, und I läuft über alle möglichen Multiindizes. Die Multiplikation auf solchen Summen ist die, die man sich denkt.

Der **Grad** von $f \neq 0$ mit Darstellung wie in (19.1) ist

$$\deg(f) = \max\{\deg(I) \; ; \; a_I \neq 0\}.$$

Darüberhinaus nennt man f **homogen vom Grad** d, wenn $a_I \neq 0$ nur für Multiindizes I mit $\deg(I) = d$ gilt.

Als kurze Notation, wenn die verwendeten Variablen klar aus dem Kontext hervorgehen, vereinbaren wir

$$R[\underline{X}] = R[X_1, \ldots, X_n].$$

Bemerkung 337. Der Polynomring erfüllt die folgende universelle Eigenschaft: Sei A eine R-Algebra. Dann gibt es eine natürliche Bijektion

$$\begin{aligned} \mathrm{Hom}_R(R[X_1, \ldots, X_n], A) &\xrightarrow{\sim} A^n \\ \big(\varphi : R[X_1, \ldots, X_n] \to A\big) &\mapsto \big(\varphi(X_1), \ldots, \varphi(X_n)\big) \end{aligned}$$

von R-Algebrenmorphismen $R[X_1, \ldots, X_n] \to A$ zu n-Tupel aus A durch Auswertung in den Variablen. Kurz: ein solcher Homomorphismus ist eindeutig durch seine Werte auf den Variablen gegeben und jede Vorgabe solcher Werte führt zu einem Homomorphismus. Der zu $(a_1, \ldots, a_n) \in A^n$ gehörende Homomorphismus wertet ein Polynom f in den $X_i = a_i$ aus, und das schreiben wir

$$f(a_1, \ldots, a_n).$$

19.2. **Der rationale Funktionenkörper in mehreren Variablen.** Der Polynomring über einem Integritätsring bleibt ein Integritätsring.

Definition 338. Der **rationale Funktionenkörper in n Variablen** über dem Körper K ist der Quotientenkörper

$$K(X_1, \ldots, x_n) = \mathrm{Quot}(K[X_1, \ldots, X_n])$$

des Polynomrings in n Variabelen.

Diese Definition erweitert die Definition des rationalen Funktionenkörpers in einer Variablen.

19.3. **Symmetrische Polynome.** Die Darstellung der Elemente in (19.1) offenbart eine Symmetrie auf dem Polynomring in n Variablen: zu $\sigma \in S_n$ gehört die Permutation der Variablen

$$X_i \mapsto X_{\sigma(i)},$$

die zu einem Automorphismus

$$\begin{aligned} \sigma : R[X_1, \ldots, X_n] &\to R[X_1, \ldots, X_n] \\ F(X_1, \ldots, X_n) &\mapsto \sigma(F) = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \end{aligned}$$

führt. (Hier verwenden wir das Einsetzen des permutierten Variablensatzes in das Polynom F). Insgesamt wird in natürlicher Weise S_n zu einer Untergruppe

$$S_n \subseteq \mathrm{Aut}_R(R[X_1, \ldots, X_n])$$

der Automorphismengruppe des Polynomrings als R-Algebra.

Aus der universellen Eigenschaft des Quotientenkörpers folgt, daß für $R = K$ ein Körper auch

$$S_n \subseteq \mathrm{Aut}_K\big(K(X_1, \ldots, X_n)\big)$$

die symmetrische Gruppe eine natürliche Gruppe von K-Automorphsimen des rationalen Funktionenkörpers in n Variablen ist.

Definition 339. Ein **symmetrisches Polynom** in n Variablen ist ein S_n-invariantes Polynom aus $R[X_1, \ldots, X_n]$.

Eine **symmetrische rationale Funktion** in n-Variablen mit Koeffizienten in einem Körper K ist ein Element der S_n-Invarianten

$$K(X_1, \ldots, X_n)^{S_n}.$$

Wir konstruieren nun zuerst ein paar symmetrische Polynome. Dazu benutzen wir die Idee aus dem Beweis der Charakterisierung endlicher galoisscher Erweiterungen, Theorem 202. Der S_n-Orbit von X_1 ist

$$\{X_1, \ldots, X_n\}$$

und das führt zum Polynom

$$\prod_{i=1}^{n}(T - X_i) = T^n - \sigma_1 T^{n-1} \pm \ldots \pm \sigma_n = \sum_{i=0}^{n}(-1)^i \sigma_i T^{n-i}$$

dessen Koeffizienten automatisch per Konstruktion S_n-invariant sind. Das ist zwar auch aus der folgenden direkten Definition (per Ausmultiplizieren äquivalent zur ersten) ersichtlich, aber der Weg über die Koeffizienten hat den Charme, diese wichtige Konstruktion zu wiederholen.

Definition 340. Die **elementarsymmetrischen Polynome** in n-Variablen sind für $1 \leq i \leq n$ die S_n-invarianten Polynome

$$\sigma_i = \sigma_i(X_1, \ldots, X_n) = \sum_{I \subseteq \{1, \ldots, n\}, \#I = i} X^I.$$

Wir setzen außerdem $\sigma_0 = 1$, aber betonen, daß σ_0 nicht zu den elementarsymmetrischen Polynomen gehört.

Es gilt offenbar für $m \leq n$

$$\sigma_i(X_1, \ldots, X_m) = \sigma_i(X_1, \ldots, X_m, 0, \ldots, 0).$$

Satz 341. *Sei K ein Körper.*

(1) *Der Körper der symmetrischen rationalen Funktionen ist*

$$K(X_1, \ldots, X_n)^{S_n} = K(\sigma_1, \ldots, \sigma_n).$$

(2) *$K(X_1, \ldots, X_n)$ ist der Zerfällungskörper des Polynoms*

$$T^n - \sigma_1 T^{n-1} \pm \ldots + (-1)^n \sigma_n$$

über $K(\sigma_1, \ldots, \sigma_n)$.

(3) *Im Körperturm*

$$L_{n+1} = K(\underline{\sigma}) \subseteq L_n = K(\underline{\sigma}, X_n) \subseteq \ldots \subseteq L_i = K(\underline{\sigma}, X_i, \ldots, X_n) \subseteq \ldots \subseteq L_1 = K(\underline{X}).$$

ist das Minimalpolynom von $X_m \in L_m$ über L_{m+1} das Polynom

$$\prod_{i=1}^{m} (T - X_i) = \sum_{i=0}^{m} (-1)^i \sigma_i(X_1, \ldots, X_m) T^{m-i}.$$

Beweis. Die Erweiterung

$$K(X_1, \ldots, X_n)/K(X_1, \ldots, X_n)^{S_n}$$

ist galoissch mit Galoisgruppe S_n, also vom Grad $n!$. Der Fixkörper enthält

$$K(\sigma_1, \ldots, \sigma_n).$$

Aussage (2) ist offensichtlich. Die Abschätzung des Grads eines Zerfällungskörpers zeigt

$$[K(X_1, \ldots, X_n) : K(\sigma_1, \ldots, \sigma_n)] \leq n!$$

woraus Aussage (1) sofort folgt. Es folgt sogar mehr, denn die Abschätzung ist scharf genau dann, wenn durch Hinzunahme der Nullstellen $X_m, \ldots, X_n$ genau die Linearfaktoren $(T - X_i)$ mit $m \leq i \leq n$ von

$$T^n - \sigma_1 T^{n-1} \pm \ldots + (-1)^n \sigma_n = \prod_{i=m+1}^{n} (T - X_i) \cdot \sum_{i=0}^{m} (-1)^i \sigma_i(X_1, \ldots, X_m) T^{m-i}$$

abgespalten werden können und das verbleibende Polynom irreduzibel über L_{m+1} bleibt. Dies zeigt (3). ☐

Bemerkung 342. Für $n \geq 5$ haben wir in der S_n-Erweiterung

$$K(X_1, \ldots, X_n)/K(\sigma_1, \ldots, \sigma_n)$$

eine weitere galoissche Erweiterung, die nicht auflösbar ist gefunden.

Das Resultat über die S_n-Invarianten rationalen Funktionen ist in Wirklichkeit Folge des stärkeren Resultats über symmetrische Polynome mit beliebigen Koeffizienten.

Satz 343. *Sei R ein Ring. Der Ring der S_n-invarianten Polynome in n Variabeln mit Koeffizienten aus R wird erzeugt von den elementarsymmetrischen Polynomen $\sigma_1, \ldots, \sigma_n$.*

Beweis. Per Induktion nach der Anzahl der Variablen n. Der Fall $n = 1$ ist trivial, denn $\sigma_1(X_1) = X_1$ und alles ist S_1-Invariant.

Wir nehmen nun an, der Satz sei für weniger als n Variablen bereits gezeigt, und argumentieren per Induktion nach dem Grad. Wenn $\deg(f) = 0$ ist, dann haben wir ein konstantes Polynom f und alles ist klar. Sei $f \in R[X_1, \ldots, X_n]^{S_n}$. Dann ist

$$f(X_1, \ldots, X_{n-1}, 0) \in R[X_1, \ldots, X_{n-1}]$$

Invariant unter S_{n-1}, dem Stabilisator von $n \in \{1,\dots,n\}$. Es gibt daher ein Polynom P mit Koeffizienten aus R in $n-1$-Variablen, so daß

$$f(X_1,\dots,X_{n-1},0) = P\big(\sigma_1(X_1,\dots,X_{n-1}),\dots,\sigma_{n-1}(X_1,\dots,X_{n-1})\big).$$

Wir betrachten nun

$$Q = f - P\big(\sigma_1(X_1,\dots,X_n),\dots,\sigma_{n-1}(X_1,\dots,X_n)\big) \in R[X_1,\dots,X_n].$$

Als Kombination aus dem symmetrischen Polynom f und dem Polynom P ausgewertet in den elementar symmetrischen Polynomen ist auch Q symmetrisch. Per Konstruktion folgt

$$Q(X_1,\dots,X_{n-1},0) = 0.$$

Aufgrund der eindeutigen Darstellung als Summe von Monomen folgt daraus, daß in Q nur Monome mit Koeffizient $\neq 0$ auftreten, in denen X_n vorkommt:

$$X_n \mid Q.$$

Als symmetrisches Polynom gilt dann für alle $\sigma \in S_n$

$$X_{\sigma(n)} = \sigma(X_n) \mid \sigma(Q) = Q.$$

Wieder aus der eindeutigen Darstellung als Summe von Monomen folgt dann

$$\sigma_n(X_1,\dots,X_n) = X_1 \cdot \ldots \cdot X_n \mid Q.$$

Wir schreiben $Q = \sigma_n \cdot Q_0$. Erneut aus der eindeutigen Darstellung als Summe von Monomen folgt, daß auch Q_0 ein symmetrisches Polynom ist. Per Induktion nach dem Grad des Polynoms gilt dann der Satz für Q und damit auch für $f = P(\underline{\sigma}) + Q$. □

Bemerkung 344. Der Beweis von Satz 343 ist konstruktiv. Er gibt einen Algorithmus an, mit dem man im Prinzip die Darstellung als Polynom in den elementarsymmetrischen Polynomen bestimmen kann.

Beispiel 345. Das Polynom

$$S_m = X_1^m + \ldots + X_n^m$$

in $\mathbb{Z}[X_1,\dots,X_n]$ ist ersichtlich symmetrisch. Wir bestimmen den Ausdruck in den elementarsymmetrischen Polynomen, der S_m entspricht.

Die Variablen X_i sind alle Lösungen von

$$T^n - \sigma_1 T^{n-1} \pm \ldots (-1)^n \sigma_n = 0.$$

Substituieren wir $T = X_i$, multiplizieren mit X_i^m und addieren über $1 \leq i \leq n$ ergibt die Rekursion

$$S_{m+n} = \sigma_1 S_{m+n-1} - \sigma_2 S_{m+n-2} \pm \ldots - (-1)^n \sigma_n S_m.$$

Es bleibt die Aufgabe, S_m für $m < n$ darzustellen. Es gilt

$$S_0 = n$$
$$S_1 = \sigma_1$$

und wir behaupten daß für alle $m < n$:

$$S_m = \sigma_1 S_{m-1} - \sigma_2 S_{m-2} \pm \ldots - (-1)^m m\sigma_m.$$

Dies zeigen wir per Induktion nach n. Für $n = 0$ und $n = 1$ ist dies klar. Angenommen, die Formel gilt für alle Variablenanzahlen $< n$. Dann verschwindet die Differenz, wenn man $X_n = 0$ setzt. Es gilt also

$$X_n \mid S_m - \big(\sigma_1 S_{m-1} - \sigma_2 S_{m-2} \pm \ldots - (-1)^m m\sigma_m\big)$$

in $\mathbb{Z}[X_1,\dots,X_n]$. Wegen Symmetrie ist dies sogar ein Vielfaches von σ_n. Aus der eindeutigen Schreibweise als Summe von Monomen folgt

$$S_m - \big(\sigma_1 S_{m-1} - \sigma_2 S_{m-2} \pm \ldots - (-1)^m m\sigma_m\big) = \sigma_n \cdot Q$$

für ein $Q \in \mathbb{Z}[X_1, \ldots, X_n]$. Die linke Seite hat nur Monome vom Grad $< n$, während die rechte Seite nur Monome vom Grad $\geq n$ besitzt. Koeffizientenvergleich zeigt dann $Q = 0$ und beweist die Behauptung.

Übungsaufgaben zu §19

Übungsaufgabe 19.1. Jede endliche Gruppe G ist Galoisgruppe einer geeigneten Körpererweiterung L/K. (Satz von Cayley: jede endliche Gruppe G ist Untergruppe der symmetrischen Gruppe.)

Übungsaufgabe 19.2. Sei K ein Körper.
(a) Zeigen Sie $\mathrm{Aut}_K(K(T)) = \mathrm{PGL}_2(K)$.
(b) Bestimmen Sie für unendliche K die Invarianten $K(T)^{\mathrm{PGL}_2(K)}$. Ist $K(T)/K$ galoissch?

Übungsaufgabe 19.3. Schreiben Sie das Polynom $X^3 + Y^3 + Z^3 \in \mathbb{Z}[X, Y, Z]$ als Polynom in den elementarsymmetrischen Polynomen.

20. Der Transzendenzgrad

Wir wenden uns nun den Körpererweiterungen zu, die über algebraische Elemente hinausgehen.

20.1. **Algebraische Unabhängigkeit.**

Definition 346. Sei R ein Ring und A eine R-Algebra.
(1) Die Elemente $\alpha_1, \ldots, \alpha_n \in A$ heißen **über R algebraisch unabhängig**, wenn der Auswertungshomomorphismus $R[X_1, \ldots, X_n] \to A$ mit $X_i \mapsto \alpha_i$ injektiv ist.
Das bedeutet, daß die einzige algebraische Relation
$$P(\alpha_1, \ldots, \alpha_n)$$
mit $P \in R[X_1, \ldots, X_n]$ durch das Nullpolynom $P = 0$ gegeben ist.
(2) Eine Menge $M \subseteq A$ heißt **über R algebraisch unabhängig**, wenn jede endliche Teilmenge von M über R algebraisch unabhängig ist.

Proposition 347. *(1) Sei R ein Ring und A eine R-Algebra. Die Elemente $\alpha_1, \ldots, \alpha_n \in A$ sind über R algebraisch unabhängig genau dann, wenn die von $\alpha_1, \ldots, \alpha_n$ erzeugte R-Unteralgebra durch die Auswertung $X_i \mapsto \alpha_i$ isomorph zum Polynomring $R[X_1, \ldots, X_n]$ ist.*
(2) Sei L eine Körpererweiterung von K. Die Elemente $\alpha_1, \ldots, \alpha_n \in L$ sind über K algebraisch unabhängig genau dann, wenn der von den $\alpha_1, \ldots, \alpha_n$ über K erzeugte Körpererweiterung in L durch die Auswertung $X_i \mapsto \alpha_i$ isomorph zum rationalen Funktionenkörper $K(X_1, \ldots, X_n)$ ist.

Beweis. (1) ist klar, denn die von $\alpha_1, \ldots, \alpha_n$ erzeugte R-Unteralgebra ist gerade das Bild der Auswertungsabbildung.

(2) Aus (1) folgt, daß $K[X_1, \ldots, X_n] \simeq K[\alpha_1, \ldots, \alpha_n]$. Dies impliziert die behauptete Isomoprhie der Quotientenkörper. Die Umkehrung ist offensichtlich. □

Definition 348. Eine **Transzendenzbasis** einer Körpererweiterung L/K ist eine über K algebraisch unabhängige Teilmenge $\mathscr{T} \subseteq L$, die maximal bezüglich Inklusion unter allen über K algebraisch unabhängige Teilmengen von L ist.

Proposition 349. *Eine Teilmenge $\mathscr{T} \subseteq L$ ist eine Transzendenzbasis von L/K genau denn, wenn*
(i) $\mathscr{T}$ über K algebraisch unabhängig ist, und
(ii) $L/K(\mathscr{T})$ eine algebraische Erweiterung ist.

Beweis. Das ist klar. Man kann ein algebraisch unabhängiges $\mathscr{T}$ genau dann nicht algebraisch unabhängig vergrößern, wenn jedes Element von L algebraisch über $K(\mathscr{T})$ ist: Multipliziere mit dem Hauptnenner der Koeffizienten einer algebraischen Gleichung. □

Korollar 350. *Eine Körpererweiterung ist genau dann algebraisch, wenn die leere Menge eine Transzendenzbasis ist.*

Beweis. Trivial. □

Proposition 351. *(1) Jede Körpererweiterung L/K besitzt eine Transzendenzbasis.*
(2) Sei L/K eine Körpererweiterung und $\mathscr{T}_0 \subseteq L$ eine über K algebraisch unabhängige Menge. Dann gibt es eine Transzendenz Basis $\mathscr{T}$ von L/K, die $\mathscr{T}_0$ enthält.

Beweis. (1) folgt sofort aus (2) angewandt auf $\mathscr{T}_0 = \emptyset$.

Der Beweis von Aussage (2) benötigt das Auswahlaxiom oder das dazu äquivalente Zorn'sche Lemma. Sei

$$M = \{S \subseteq L\ ;\ \mathscr{T}_0 \subseteq S \text{ und } S \text{ ist über } K \text{ algebraisch unabhängig}\}.$$

Dann ist M bezüglich Inklusion induktiv geordnet. Die obere Schranke einer totalgeordneten Teilmenge S_i, $i \in I$ ist durch die Vereinigung $\bigcup_{i\in I} S_i$ gegeben, denn jede algebraische Relation benötigt nur endlich viele Elemente. Daher fänden wir eine algebraische Relation zwischen Elementen der Vereinigung schon bei einer genügend großen Teilmenge S_i.

Das Lemma von Zorn garantiert nun die Existenz maximaler Elemente in M, und das sind genau die gesuchten Transzendenzbasen. □

Wir sagen die Variable X_α kommt in einem Polynom

$$f = \sum_I a_I X^I \in K[X_1, \ldots, X_n]$$

vor, wenn es einen Multiindex $I = (i_1, \ldots, i_n)$ mit $i_\alpha \geq 1$ und $a_I \neq 0$ gibt. Das ist äquivalent dazu, daß f aufgefaßt als Polynom in X_α über dem rationalen Funktionenkörper in der restlichen Variablen

$$K(X_1, \ldots, \widehat{X_\alpha}, \ldots, X_n)$$

einen positiven Grad hat.

20.2. **Der Transzendenzbasensatz.**

Theorem 352. *Je zwei Transzendenzbasen einer Körpererweiterung sind gleichmächtig.*

Beweis. Dieser Satz kann formal genauso aus einem Austauschargument bewiesen werden wie der Satz über die Gleichmächtigkeit zweier Basen eines Vektorraums. Wir behandeln nur den Fall endlicher Transzendenzbasen. Dieser folgt sofort aus dem folgenden Satz 353. In der Tat, sind A und B Transzendenzbasen und $\#A < \infty$, dann sagt Satz 353 B ist auch endlich und $\#B \leq \#A$. Weil B auch endlich ist, können wir Satz 353 mit vertauschten Rollen anwenden und erhalten $\#A \leq \#B$. □

Satz 353. *Sei L/K eine Körpererweiterung und $A = (a_1, \ldots, a_n) \subseteq L$ eine Transzendenzbasis von L/K. Sei $B = (b_1, \ldots, b_m) \subseteq L$ algebraisch unabhängig über K. Dann gilt*

$$\#B \leq \#A.$$

Beweis. Schritt 1, algebraische Relation: Da A Transzendenzbasis ist, sind die b_i als Elemente von L algebraisch über $K(A)$. Es gibt daher für $b = b_1$ ein Polynom $0 \neq P \in K[X_1, \ldots, X_n, Y]$ mit

$$P(a_1, \ldots, a_n, b) = 0.$$

Da A algebraisch unabhängig ist, kommt Y in P vor. Da b als Element von B nicht über K algebraisch sein kann, kommt auch mindestens eines der X_α vor. Dies sei oBdA die Variable X_1. Es folgt, daß a_1 algebraisch über

$$K(b, a_2, \ldots, a_n)$$

ist.

Schritt 2, Austausch: Wir zeigen nun, daß $A' = (b, a_2, \ldots, a_n)$ auch über K algebraisch unabhängig ist. Angenommen, es gäbe eine nichttriviale algebraische Relation über K, dann muß darin b vorkommen, denn die $a_2, \ldots, a_n$ sind algebraisch unabhängig über K. Dann ist

$$K(a_2, \ldots, a_n) \subseteq K(b, a_2, \ldots, a_n) \subseteq K(b, a_1, a_2, \ldots, a_n)$$

ein Turm algebraischer Erweiterungen, und somit a_1 algebraisch über $K(a_2, \ldots, a_n)$. Dies wiederspricht der algebraischen Unabhängigkeit von A.

Außerdem ist A' auch Transzendenzbasis von L/K, denn $L/K(A, b) = K(A', a_1)/K(A')$ ist ein Turm algebraischer Erweiterungen und damit $L/K(A')$ algebraisch.

Schritt 3, Induktion: Wir betrachten nun $M = K(b)$ und die Erweiterung L/M. Wir zeigen, daß $\hat{A} = (a_2, \ldots, a_n)$ und $\hat{B} = (b_2, \ldots, b_m)$ über M algebraisch unabhängig sind. Dann schließen wir, daß $\hat{A}$ eine Transzendenzbasis von L/M der Größe $n-1$ ist, denn $L/M(a_2, \ldots, a_n) = K(A')$ ist algebraisch, und weiter per Induktion, daß

$$\#\hat{B} \leq \#\hat{A}.$$

Aber dann gilt auch

$$\#B = \#\hat{B} + 1 \leq \#\hat{A} + 1 = \#A,$$

was zu beweisen war.

Schritt 4, algebraische Unabhängigkeit: Da Argument für $\hat{A}$ und $\hat{B}$ ist dasselbe. Sei also $0 \neq P \in M[X_2, \ldots, X_n]$ mit

$$P(a_2, \ldots, a_n) = 0.$$

Wir schreiben

$$P = \sum_I f_I X^I$$

mit $f_I \in M = K(b)$. Da b algebraisch unabhängig über K ist, ist $K(b)$ ein rationaler Funktionenkörper in einer Variablen. Es gibt daher $0 \neq h \in K[Y]$ und für jeden Multiindex ein $g_I \in K[Y]$ mit

$$f_I = \frac{g_I(b)}{h(b)}.$$

Nach Durchmultiplizieren mit dem Hauptnenner finden wir

$$Q = \sum_I g_I(Y) X^I \in K[Y, X_2, \ldots, X_n]$$

mit

$$Q(b, a_2, \ldots, a_n) = 0.$$

Da $A' = (b, a_2, \ldots, a_n)$ über K algebraisch unabhängig ist, folgt $Q = 0$. Da die Multiindexschreibweise eindeutig ist, folgt $g_I = 0$ für alle I, somit $f_I = 0$ und $P = 0$, der gesuchte Widerspruch. $\square$

Korollar 354. *Sei L/K eine Körpererweiterung und $A = (a_1, \ldots, a_n) \subseteq L$ eine Transzendenzbasis von L/K. Sei $B = (b_1, \ldots, b_m) \subseteq L$ algebraisch unabhängig über K. Dann gibt es Elemente*

$$b_{m+1}, \ldots, b_n \in A$$

so daß $(b_1, \ldots, b_n)$ eine Transzendenzbasis von L/K ist.

Beweis. Wir betrachten eine maximale über K algebraisch unabhängige Teilmenge $C \subseteq A \cup B$, die B enthält. Dann ist A algebraisch über $K(C)$ und daher $L/K(A, C)/K(C)$ algebraisch. Daher ist C eine Transzendenzbasis und nach Theorem 352 genauso groß wie A. □

Damit ist der folgende Begriff wohldefiniert.

Definition 355. Der **Transzendenzgrad** einer Körpererweiterung L/K ist die Mächtigkeit einer (oder aller) Transzendenzbasen von L/K und wird mit

$$\operatorname{trdeg}(L/K)$$

bezeichnet.

Proposition 356. *Seien L/M und M/K Körpererweiterungen. Dann gilt:*

(1) $\operatorname{trdeg}(M/K) \leq \operatorname{trdeg}(L/K)$,
(2) $\operatorname{trdeg}(L/K) = \operatorname{trdeg}(M/K) + \operatorname{trdeg}(L/M)$,
(3) $\operatorname{trdeg}(L/K) = 0$ *dann und nur dann, wenn L/K algebraisch ist.*

Beweis. Da der Transzendenzgrad stets nicht-negativ ist, folgt (1) aus (2).

Wir zeigen nun Aussage (2). Sei $A = (a_1, \ldots, a_n)$ eine Transzendenzbasis von M/K und $B = (b_1, \ldots, b_m)$ eine von L/M. Dann ist L algebraisch über $K(A \cup B)$, denn beide Schritte $L/M(B)$ und $M(B)/K(A \cup B)$ sind algebraisch. Eine maximale über K algebraisch unabhängige Teilmenge von $A \cup B$ ist daher eine Transzendenzbasis von L/K. Wir müssen daher zeigen, daß $A \cap B = \emptyset$ und $A \cup B$ algebraisch unabhängig über K ist. Angenommen $0 \neq P \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ ist eine nichttriviale Relation für $X_i \mapsto a_i$ und $Y_j \mapsto b_j$. Wir können P schreiben als

$$P = \sum_J f_J Y^J$$

mit $f_J \in K[X_1, \ldots, X_n]$. Mit $a_J = f_J(a_1, \ldots, a_n) \in M$ verschwindet daher das Polynom

$$Q = \sum_J a_J Y^J \in M[Y_1, \ldots, Y_m]$$

unter $Y_j \mapsto b_j$. Da B über M algebraisch unabhängig ist, muß $Q = 0$ und daher $a_J = 0$ sein für alle Multiindizes J. Da aber A algebraisch unahängig über K ist, folgt aus $f_J(a_1, \ldots, a_n) = a_J = 0$ schon $f_J = 0$. Daher ist $P = 0$ das triviale Polynom im Widerspruch zu unserer Annahme. Das zeigt (2).

Aussage (3) ist eine triviale Folge von Korollar 350. □

Bemerkung 357. Der Beweis von Proposition 356 (2) zeigt genauer, daß man Transzendenzbasen für eine iterierte Erweiterung als Vereinigung der einzelnen Transzendenzbasen bekommt.

Definition 358. Die **Konstantenerweiterung** des Funktionenkörpers $K(X_1, \ldots, X_n)$ zur Körpererweiterung L/K ist die Erweiterung

$$L(X_1, \ldots, X_n)/K(X_1, \ldots, X_n),$$

die aus der Inklusion

$$K[X_1, \ldots, X_n] \subseteq L[X_1, \ldots, X_n]$$

durch Übergang zu den Quotientenkörpern entsteht.

Lemma 359. *Sei L/K eine endliche Körpererweiterung. Dann ist die Konstantenkörpererweiterung mit L/K auch endlich und*

$$[L : K] = [L(X_1, \ldots, X_n) : K(X_1, \ldots, X_n)].$$

Beweis. Per Induktion über n wir reduzieren auf den Fall $n = 1$ und $L = K(\alpha)$. Wir músse n zeigen, daß $P_{\alpha/K}$ auch das Minimalpolynom von α über $K(X)$ ist. Angenommen es gibt $f_i \in K(X)$ und $e < [L : K]$ mit

$$\alpha^e + f_1\alpha^{e-1} + \ldots + \alpha f_{e-1} + f_e = 0,$$

Dann gibt es (nach Durchmultiplizieren mit dem Hauptnenner) Polynome $P_i \in K[X]$, nicht alle 0 und

$$P_0\alpha^e + P_1\alpha^{e-1} + \ldots + P_{e-1}\alpha + P_e = 0.$$

Dies ist eine Gleichung in $L[X]$ und Koeffizientenvergleich zeigt, da $1, \ldots, \alpha^e$ linear unabhängig über K sind, daß alle $P_i = 0$ sind, ein Widerspruch. □

Proposition 360. *Sei L/K eine Körpererweiterung und M ein Zwischenkörper. Dann sind äquivalent:*

(a) *L/K ist endlich erzeugt.*
(b) *L/M und M/K sind endlich erzeugt.*

Beweis. Wenn L/M und M/K endlich erzeugt sind, etwa durch die endlichen Mengen $A \subseteq L$ und $B \subseteq M$, also $L = M(A)$ und $M = K(B)$ gilt, dann gilt

$$L = M(A) = K(B)(A) = K(A \cup B)$$

und L ist über K endlich erzeugt.

Sei nun L/K endlich erzeugt, etwa $A \subseteq L$ endlich mit $L = K(A)$. Dann gilt auch $L = M(A)$ und L/M ist endlich erzeugt.

Es bleibt zu zeigen, daß auch M/K endlich erzeugt ist. Aus Proposition 356 folgt, daß

$$\mathrm{trdeg}(M/K) \leq \mathrm{trdeg}(L/K)$$

endlich ist. Wir dürfen K durch eine endlich erzeugte Teilerweiterung von M/K ersetzen. Wir tun dies mit der von einer Transzendenzbasis von M/K erzeugten Teilerweiterung und nehmen daher von nun an oBdA an, daß M/K algebraisch ist.

Sei dann $x_1, \ldots, x_n$ eine Transzendenzbasis von L/K. Wir betrachten das Diagramm von Körpern

$$\begin{tikzcd}[arrows=dash]
 & L \arrow[d] & \\
 & M(x_1, \ldots, x_n) \arrow[dl] \arrow[dr] & \\
M \arrow[dr] & & K(x_1, \ldots, x_n) \arrow[dl] \\
 & K &
\end{tikzcd}$$

Es ist $x_1, \ldots, x_n$ auch eine Transzendenzbasis von L/M, denn sonst wäre

$$n = \mathrm{trdeg}(L/K) = \mathrm{trdeg}(L/M(x_1, \ldots, x_n)) + \mathrm{trdeg}(M(x_1, \ldots, x_n)/M) + \mathrm{trdeg}(M/K) < n$$

ein Widerspruch. Daher sind $K(x_1, \ldots, x_n)$ und $M(x_1, \ldots, x_n)$ isomorph zu rationalen Funktionenkörpern in n Variablen und die Körpererweiterung $M(x_1, \ldots, x_n)/K(x_1, \ldots, x_n)$ isomorph zur Konstantenerweiterung

$$M(X_1, \ldots, X_n)/K(X_1, \ldots, X_n).$$

Es gilt dann mit Lemma 359

$$[M : K] = [M(X_1, \ldots, X_n) : K(X_1, \ldots, X_n)] = [M(x_1, \ldots, x_n) : K(x_1, \ldots, x_n)] \leq [L : K(\mathscr{T})],$$

und das ist nach Voraussetzung endlich. Daher ist M/K endlich erzeugt. □

20.3. **Die allgemeine Gleichung.** Wir haben das Polynom

$$\prod_{i=1}^{n}(T - X_i) = T^n - \sigma_1 T^{n-1} \pm \dots (-1)^n \sigma_n$$

mit Variablen X_i als Polynom mit allgemeinen Wurzeln kennen gelernt. In der Tat, alles was wir über dieses Polynom und seine Wurzeln in $\mathbb{Z}[X_1, \dots, X_n]$ aussagen können, gilt so auch für ein beliebiges spezielles Polynom f mit Wurzeln $\alpha_1, \dots, \alpha \in R$. Dazu betrachten wir einfach den Auswertungshomorphismus $\mathbb{Z}[X_1, \dots, X_n] \to R$

$$X_i \mapsto \alpha_i.$$

Typischerweise kennen wir aber nur die Koeffizienten unseres Polynoms und nicht die Wurzeln. Das allgemeine Polynom hat daher Varablen als Koeffizienten und spezialisiert vermöge Auswertung auf jedes beliebige Polynom.

Satz 361.

(1) *Die elementarsymmetrischen Polynome $\sigma_1, \dots, \sigma_n \in \mathbb{Z}[X_1, \dots, X_n]$ sind algebraisch unabhängig.*

(2) *Für einen Körper K ist*

$$K(\sigma_1, \dots, \sigma_n)$$

ein rationaler Funktionenkörper in den $\sigma_1, \dots, \sigma_n$.

Beweis. (1) folgt aus (2) für $K = \mathbb{Q}$. Wir zeigen daher nun (2). Die Erweiterung

$$K(X_1, \dots, X_n)/K(\sigma_1, \dots, \sigma_n)$$

ist algebraisch. Daher gilt nach Proposition 356(2)

$$\operatorname{trdeg}(K(\sigma_1, \dots, \sigma_n)/K) = \operatorname{trdeg}(K(X_1, \dots, X_n)/K) = n.$$

In der erzeugenden Menge $\sigma_1, \dots, \sigma_n$ ist eine Transzendenzbasis enthalten. Da alle Transzendenzbasen n Elemente haben, muß $\sigma_1, \dots, \sigma_n$ bereits eine Transzendenzbasis sein. $\square$

Satz 361 erlaubt uns einen Perspektivwechsel. Die **allgemeine Gleichung** wird gegeben durch

$$T^n - \sigma_1 T^{n-1} \pm \dots + (-1)^n \sigma_n = 0$$

wobei nun die σ_i zunächst als unabhängige Variablen aufzufassen sind. Der Zerfällungskörper über $K(\sigma_1, \dots, \sigma_n)$ ist gegeben durch die schon bekannte Erweiterung

$$K(X_1, \dots, X_n)/K(\sigma_1, \dots, \sigma_n),$$

wobei nun wieder X_i Variablen und die σ_i elmentarsymmetrische Polynome in den X_i sind. Die Tatsache, daß die Nullstellen der allgemeinen Gleichung algebraisch unabhängig sind, zeigt, daß keine allgemeingültigen algebraischen Abhängigkeiten zwischen den Nullstellen eines Polynoms vom Grad n bestehen. Ferner ist die Galoisgruppe der allgemeinen Gleichung vom Grad n die volle symmetrische Gruppe S_n. Jede Abhängigkeit der Nullstellen bei einem speziellen Polynom, die dann die Galoisgruppe zu einer Untergruppe von S_n macht, ist ein Artefakt des speziellen Polynoms.

Bemerkung 362. Wie verhält sich die Galoisgruppe, wenn man die Koeffizienten $(-1)^i \sigma_i$ der allgemeinen Gleichung vom Grad n (mit Galoisgruppe S_n) durch zufällige Werte $a_i \in K$ ersetzt (spezialisiert)?

$$\begin{array}{ccccc}
K(X_1, \dots, X_n) & \supseteq & K[X_1, \dots, X_n] & \xrightarrow{X_i \mapsto \alpha_i} & K(\alpha_1, \dots, \alpha_n) \\
\bigcup & & \bigcup & & \bigcup \\
K(\sigma_1, \dots, \sigma_n) & \supseteq & K[\sigma_1, \dots, \sigma_n] & \xrightarrow{\sigma_i \mapsto (-1)^i a_i} & K
\end{array}$$

Diese Frage benötigt zunächst eine Präzisierung des *zufälligen*, und wird selbst danach noch von der arithemtischen Natur des Körpers K abhängen.

- Wenn K algebraisch abgeschlossen ist, wird als Galoisgruppe stets 1 herauskommen: das spezialisierte Polynom ist $(n > 1)$ nicht einmal mehr irreduzibel.
- Wenn $K = \mathbb{F}_q$ ein endlicher Körper ist, dann wird — Irreduzibilität der Spezialisierung vorausgesetzt — die Galoisgruppe $\mathbb{Z}/n\mathbb{Z}$ werden.
- Es ist eine Eigenschaft gewisser Körper, **hilbertsch** genannt, daß die Galoisgruppe die volle S_n bleibt, sofern die Koeffizienten außerhalb einer *dünnen* Menge von Koeffizientenwerten spezialisiert werden. Endliche Erweiterungen von $\mathbb{Q}$, also insbesondere $\mathbb{Q}$ selbst, sind hilbertsch. Von einem zufällig dahingeworfenen Polynom vom Grad n in $\mathbb{Q}[T]$ erwarten wir also die Galoisgruppe S_n.

21. Algorithmische Bestimmung der Galoisgruppe eines Polynoms

Sei L/K eine endliche Galoiserweiterung, der Zerfällungskörper des Polynoms $f \in K[T]$ mit den Wurzeln $\alpha_1, \ldots, \alpha_n \in L$. Wir betrachten die Galoisgruppe natürlich als Permutationsgruppe auf der Menge der Wurzeln von f. Dies ist ein injektiver Gruppenhomomorphismus

$$\rho : \mathrm{Gal}(L/K) \hookrightarrow S_n$$

definiert für $g \in \mathrm{Gal}(L/K)$ durch

$$g(\alpha_i) = \alpha_{\rho(g)(i)}.$$

Der Auswertungshomomorphismus

$$\begin{aligned} K[X_1, \ldots, X_n] &\to L \\ F(X_1, \ldots, X_n) &\mapsto F(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

wird so $\mathrm{Gal}(L/K)$-äquivariant, wenn man $\mathrm{Gal}(L/K)$ mittels ρ auf Polynomen operieren läßt: für alle $g \in \mathrm{Gal}(L/K)$ und $F \in K[X_1, \ldots, X_n]$ gilt

$$\begin{aligned} g(F(\underline{\alpha})) &= F(g(\alpha_1), \ldots, g(\alpha_n)) = F(\alpha_{\rho(1)}, \ldots, \alpha_{\rho(n)}) \\ &= (F(X_{\rho(g)(1)}, \ldots, X_{\rho(g)(n)})(\underline{\alpha}) = \big(\rho(g)(F)\big)(\underline{\alpha}). \end{aligned} \tag{21.1}$$

21.1. Die Diskriminante.

Definition 363. (1) Sei K ein Körper. Die **Diskriminante** $\mathrm{disc}(f)$ eines normierten Polynoms $f \in K[T]$ vom Grad $n \geq 1$ berechnet sich aus den Wurzeln $\alpha_1, \ldots, \alpha_n$ von f in einem algebraischen Abschluß von K (mit Vielfachheit) als

$$\mathrm{disc}(f) = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

(2) Die **Diskriminante** der allgemeinen Gleichung

$$f = T^n - \sigma_1 T^{n-1} \pm \ldots (-1)^n \sigma_n \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n][T]$$

ist

$$\Delta = (-1)^{\binom{n}{2}} \prod_{i \neq j} (X_i - X_j),$$

wobei die X_i die Variablen sind, mit $\sigma_i = \sigma_i(X_1, \ldots, X_n)$.

Die Diskriminante Δ ist per Definition offensichtlich ein homogenes Polynom vom Grad $\binom{n}{2}$.

Lemma 364. *Sei K ein Körper und $f = T^n + a_1 T^{n-1} + \ldots + a_n \in K[T]$ ein normiertes Polynom vom Grad $n \geq 1$. Es gelten die folgenden Aussagen.*

(1) $\Delta \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n]$.

(2) $\mathrm{disc}(f) \in K$, *und* $\mathrm{disc}(f)$ *ist unabhängig von der Wahl des algebraischen Abschlusses, aus dem die Wurzeln stammen, mit denen man* $\mathrm{disc}(f)$ *berechnet.*

(3) Das Polynom f ist separabel genau dann, wenn $\mathrm{disc}(f) \neq 0$.

Beweis. (1) Das Polynom Δ ist offensichtlich S_n-invariant. Damit kann man Δ nach Satz 343 als Polynom in den elementarsymmetrischen Polynomen ausdrücken.

(2) Der Auswertungshomomorphismus $F(\underline{X}) \mapsto F(\underline{\alpha})$

$$\varphi : \mathbb{Z}[X_1, \ldots, X_n] \to L$$

führt zu $\sigma_i(\underline{\alpha}) = (-1)^i a_i$ und leistet daher

$$\mathrm{disc}(f) = \Delta(\underline{\alpha}) \in \varphi(\mathbb{Z}[\sigma_1, \ldots, \sigma_n]) \subseteq K.$$

Die Aussage über die Unabhängigkeit ist damit auch klar.

(3) Das ist offensichtlich. □

Satz 365. *Seien $\alpha_1, \ldots, \alpha_n$ die Wurzeln von f in einem algebraischen Abschluß von K. Sei* $\mathrm{disc}(f) \neq 0$ *und $L = K(\alpha_1, \ldots, \alpha_n)$ der Zerfällungskörper von f. Wir betrachten* $\mathrm{Gal}(L/K)$ *via der Operation auf den Wurzeln von f als Permutationsgruppe*

$$\mathrm{Gal}(L/K) \subseteq S_n.$$

Dann ist

$$\mathrm{Gal}(L/K) \subseteq A_n \iff \mathrm{disc}(f) \textit{ ist ein Quadrat in } K.$$

Beweis. Zum Quotienten $\mathrm{sign} : S_n \to \{\pm 1\}$ mit Kern A_n gehört eine quadratische Zwischenerweiterung

$$\mathbb{Q}(X_1, \ldots, X_n) \supseteq \mathbb{Q}(X_1, \ldots, X_n)^{A_n} \supseteq \mathbb{Q}(\sigma_1, \ldots, \sigma_n).$$

Diese bestimmen wir jetzt. Sei $\delta \in \mathbb{Z}[X_1, \ldots, X_n]$ definiert durch

$$\delta = \prod_{i<j} (X_i - X_j).$$

Dann ist offensichtlich

$$\delta^2 = \Delta$$

und mit der Definition

$$\mathrm{sign}(\sigma) = (-1)^{\#\{i<j\ ;\ \sigma(i)>\sigma(j)\}}$$

offenbar

$$\sigma(\delta) = \mathrm{sign}(\sigma)\delta.$$

Damit ist der Kummercharakter zu Δ der Homomorphismus

$$\begin{aligned} \chi_\Delta : \mathrm{Gal}(\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)) = S_n &\to \mu_2 = \{\pm 1\} \\ \sigma \mapsto \frac{\sigma(\delta)}{\delta} = \mathrm{sign}(\sigma) \end{aligned}$$

nichts anderes als das Signum der Permutation. Via Kummertheorie, oder direkt in diesem einfachen Fall, gehört zu $\mathrm{sign} = \chi_\Delta$ als Fixkörper des Kerns die quadratische Erweiterung

$$\mathbb{Q}(X_1, \ldots, X_n)^{A_n} = \mathbb{Q}(\sigma_1, \ldots, \sigma_n, \delta)$$

von $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$.

Im konkreten Fall ist nun

$$\delta(\underline{\alpha}) \in L$$

mit

$$\delta(\underline{\alpha})^2 = \Delta(\underline{\alpha}) = \mathrm{disc}(f).$$

Beschreibe $\rho : \mathrm{Gal}(L/K) \subseteq S_n$ die Wirkung auf $\alpha_1, \ldots, \alpha_n$. Wir rechnen mittels (21.1) für alle $g \in \mathrm{Gal}(L/K)$

$$\frac{g(\delta(\underline{\alpha}))}{\delta(\underline{\alpha})} = \frac{\rho(g)(\delta)}{\delta}(\underline{\alpha}) = \mathrm{sign}(\rho(g)).$$

Daher gilt

$$\begin{aligned} \mathrm{disc}(f) \in K^2 &\iff \delta(\underline{\alpha}) \in K \\ &\iff g(\delta(\underline{\alpha})) = \delta(\underline{\alpha}) \text{ für alle } g \in \mathrm{Gal}(L/K) \\ &\iff \mathrm{sign}(\rho(g)) = 1 \text{ für alle } g \in \mathrm{Gal}(L/K) \\ &\iff \mathrm{Gal}(L/K) \subseteq A_n \end{aligned}$$

vermöge der Identifikation $\mathrm{Gal}(L/K) \subseteq S_n$ mittels ρ. □

Beispiel 366. Die Diskriminante läßt sich nach Lemma 364 und Satz 343 als Polynom in den elementarsymmetrischen Polynomen ausdrücken.

(1) $n = 1$: Trivial!

$$\Delta = 1.$$

(2) $n = 2$: Das ist leicht.

$$\Delta = (X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 = \sigma_1^2 - 4\sigma_2.$$

(3) $n = 3$: Das ist schon anstrengend. Zunächst berechnen wir bei $X_3 = 0$

$$\Delta(X_1, X_2, 0) = (X_1 - X_2)^2(X_1X_2)^2 = (\sigma_1^2 - 4\sigma_2)\sigma_2^2.$$

Daher gilt

$$\Delta = (\sigma_1^2 - 4\sigma_2)\sigma_2^2 + \sigma_3 \cdot P$$

mit einem symmetrischen homogenen Polynom P vom Grad 3. Ein Monom $\sigma_1^r\sigma_2^s\sigma_3^t$ hat als Polynom in $X_1, \ldots, X_3$ betrachtet den Grad

$$r + 2s + 3t.$$

Daher gilt für gewisse $a, b, c \in \mathbb{Z}$

$$P = a \cdot \sigma_1^3 + b \cdot \sigma_1\sigma_2 + c \cdot \sigma_3.$$

Einsetzen von exlpiziten Werten aus $\mathbb{Z}$ führt zu linearen Gleichungssystemen für a, b, c, die man leicht auflösen kann:

$$\Delta = (\sigma_1^2 - 4\sigma_2)\sigma_2^2 + \sigma_3 \cdot (-4\sigma_1^3 + 18\sigma_1\sigma_2 - 27\sigma_3).$$

Als Spezialfall ergibt sich für Polynome vom Grad 3 mit $\sigma_1 = 0$, also für

$$f(T) = T^3 + BT + C$$

die Diskriminante

$$\mathrm{disc}(f) = -4B^3 - 27C^2.$$

21.2. **Die Methode von Stauduhar.** Die Diskriminante Δ oder besser ihre kanonische Wurzel $\delta \in \mathbb{Z}[X_1, \ldots, X_n]$ kontrolliert, ob die Galoisgruppe des Zerfällungskörpers eines separablen Polynoms vom Grad n als Permutationsgruppe auf den Wurzeln in der alternierenden Gruppe A_n landet. Die Methode von Stauduhar zur Bestimmung von Galoisgruppen benutzt denselben Ansatz für eine beliebige Untergruppe von S_n. Wir skizzieren eine vereinfachte Version.

Zu einem $F \in \mathbb{Z}[X_1, \ldots, X_n]$ bezeichnen wir den Stabilisator von F unter der S_n-Operation mit

$$G_F := \{\tau \in S_n \ ; \ \tau(F) = F\} \subseteq S_n.$$

Lemma 367. *Zu jeder Untergruppe $G \subseteq S_n$ gibt es ein $F \in \mathbb{Z}[X_1, \ldots, X_n]$ mit $G = G_F$.*

Beweis. Es gilt $G = G_F$ genau denn, wenn F ein primitives Element für die Erweiterung

$$\mathbb{Q}(X_1, \ldots, X_n)^G/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$$

ist. Das folgt sofort aus Galoistheorie, denn

$$\mathrm{Gal}\left(\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n, F)\right) = G_F.$$

Jede separable Erweiterung besitzt nach dem Satz vom primitiven Element, Theorem 161, ein primitives Element. Daher gibt es $F \in \mathbb{Q}(X_1, \ldots, X_n)$ mit der gewünschten Stabilisatoreigenschaft. Das ist nur ein erster Schritt, denn wir wollen ein Polynom mit Koeffizienten aus $\mathbb{Z}$. Das ist aber nicht schwer zu korrigieren. Wir schreiben $F = P/Q$ mit $P, Q \in \mathbb{Z}[X_1, \ldots, X_n]$. Dann ist

$$H = F \cdot \prod_{\sigma \in S_n} \sigma(Q) = P \cdot \prod_{\sigma \neq 1} \sigma(Q) \in \mathbb{Z}[X_1, \ldots, X_n]$$

offensichtlich auch ein primitives Element. □

Definition 368. Die **(Galois)-Resolvente** zu einem Polynom $F \in \mathbb{Z}[X_1, \ldots, X_n]$ ist das Polynom

$$R_F(T) = \prod_{\sigma \in S_n/G_F} (T - \sigma(F)) \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n][T].$$

Der Ausdruck $\sigma(F)$ hängt von $\sigma \in S_n$ nur über seine Nebenklasse $\sigma G_F \in S_n/G_F$ ab. Daher ist $\sigma(F)$ in der Definition der Galois-Resolvente eindeutig bestimmt. Die Koeffizienten von $R_F(T)$ sind invariante Polynome, weil für alle $\tau \in S_n$

$$\tau(R_F) = \prod_{\sigma \in S_n/G_F} (T - \tau\sigma(F)) = R_F.$$

Durch Multiplikation mit τ von links werden die Nebenklassen S_n/G_F nur permutiert.

Proposition 369. *Für jedes $F \in \mathbb{Z}[X_1, \ldots, X_n]$ ist die Galois-Resolvente R_F das Minimalpolynom von F über $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$.*

Beweis. Es gilt $R_F(F) = 0$, also ist R_F ein Vielfaches des Minimalpolynoms. Andererseits gilt

$$\begin{aligned}
\deg(P_{F/\mathbb{Q}(\sigma_1,\ldots,\sigma_n)}) &= [\mathbb{Q}(\sigma_1, \ldots, \sigma_n, F) : \mathbb{Q}(\sigma_1, \ldots, \sigma_n)] \\
&= [\mathbb{Q}(X_1, \ldots, X_n)^{G_F} : \mathbb{Q}(\sigma_1, \ldots, \sigma_n)] \\
&= \frac{[\mathbb{Q}(X_1, \ldots, X_n) : \mathbb{Q}(\sigma_1, \ldots, \sigma_n)]}{[\mathbb{Q}(X_1, \ldots, X_n) : \mathbb{Q}(X_1, \ldots, X_n)^{G_F}]} = \frac{\# S_n}{\# G_F} \\
&= \#(S_n/G_F) = \deg(R_F).
\end{aligned}$$

Als sich teilende normierte Polynome gleichen Grades gilt dann $R_F = P_{F/\mathbb{Q}(\sigma_1,\ldots,\sigma_n)}$. □

Sei $f = T^n + a_1 T^{n-1} + \ldots + a_n \in K[T]$ separabel mit Nullstellen $\alpha_1, \ldots, \alpha_n$ in einem algebraischen Abschluß, und sei $L = K(\alpha_1, \ldots, \alpha_n)/K$ der Zerfällungskörper von f. Wir schreiben

$$\rho : \mathrm{Gal}(f) = \mathrm{Gal}(L/K) \hookrightarrow S_n$$

für die übliche Struktur als Permutationsgruppe auf $\{\alpha_1, \ldots, \alpha_n\}$.

Sei $G \subseteq S_n$ eine Untergruppe und $F \in \mathbb{Z}[X_1, \ldots, X_n]$ mit $G_F = G$. Die Auswertung der Galois-Resolvente R_F in $X_i \mapsto \alpha_i$

$$R_{F,\underline{\alpha}}(T) = \prod_{\sigma \in S_n/G} (T - \sigma(F)(\underline{\alpha}))$$

ist ein Polynom in $K[T]$. In der Tat entsteht $R_{F,\underline{\alpha}}(T)$ aus $R_F(T)$ durch Auswertung der Koeffizienten mittels $\sigma_i \mapsto (-1)^i a_i$.

Satz 370. *Im obigen Kontext nehmen wir an, daß $R_{F,\underline{\alpha}}(T)$ ein separables Polynom in $K[T]$ ist. Dann sind äquivalent:*

(a) *Es gibt ein $\tau \in S_n$ mit*
$$\rho(\mathrm{Gal}(L/K)) \subseteq \tau G \tau^{-1}.$$
(b) *Die Galois-Resolvente $R_{F,\underline{\alpha}}(T)$ hat eine Nullstelle in K.*

Beweis. Es ist $\mathrm{Gal}(L/K)$ in einer zu G konjugierten Untergruppe enthalten, genau dann, wenn $\rho(\mathrm{Gal}(L/K))$ auf der Menge der
$$\sigma(F)(\underline{X})$$
mit $\sigma \in S_n/G_F$ einen Fixpunkt hat, denn der Stabilisator von F ist G und damit der Stabilisator von $\tau(F)$ gerade $\tau G \tau^{-1}$.

Für die Auswertung in $\underline{\alpha}$ gilt nach (21.1) für alle $g \in \mathrm{Gal}(L/K)$ und $P \in K[X_1,\ldots,X_n]$
$$g(P(\underline{\alpha})) = \big(\rho(g)(P)\big)(\underline{\alpha}).$$
Angewandt auf $P = \tau(F)$ und angesichts dessen, daß die Galois-Resolvente separabel bleiben soll nach Auswertung in $\alpha_1,\ldots,\alpha_n$, gibt es einen Fixpunkt genau dann, wenn es $\tau \in S_n$ gibt mit
$$\tau(F)(\underline{\alpha})$$
ist $\mathrm{Gal}(L/K)$-invariant, also ein Element von K. Die Menge der $\tau(F)(\underline{\alpha})$ sind genau die Menge der Nullstellen von $R_{F,\underline{\alpha}}$ (im Zerfällungskörper L/K). □

Aus Satz 370 kann man nun im Prinzip einen Algorithmus bauen, mit dem man $\mathrm{Gal}(f)$ als Permutationsgruppe in S_n bestimmen kann (bis auf Konjugation, was einer Umnummerierung der Nullstellen entspricht). Dazu muß man

- wissen, daß es stets ein F gibt, so daß $R_{F,\underline{\alpha}}$ separabel bleibt, und
- über einem Körper K arbeiten, für den sich algorithmisch entscheiden läßt, ob die Galois-Resolvente $R_{F,\underline{\alpha}}$ eine Nullstelle in K hat.

Die Effektivität des Verfahrens hängt maßgeblich davon ab, zu jeder Untergruppe $G \subseteq S_n$ geeignete Polynome F möglichst kleinen Grades zu finden mit $G = G_F$. Verbessern läßt sich der skizzierte Ansatz, indem man relative Galois-Resolventen benutzt. Diese entscheiden für ein Paar
$$H \subseteq G$$
von Untergruppen von S_n, bei denen man bereits $\mathrm{Gal}(L/K) \subseteq G$ weiß, ob die Galoisgruppe sogar eine Untergruppe einer G-konjugierten von H ist.

Beispiel 371. Das Polynom
$$\Theta = X_1X_3 + X_2X_4$$
hat als Stabilisator der S_4-Operation die 2-Sylowgruppe D_4, die Diedergruppe des Quadrats
$$\begin{tikzcd} 1 \arrow[r, dash] \arrow[d, dash] & 2 \arrow[d, dash] \\ 4 \arrow[r, dash] & 3 \end{tikzcd}$$
wie man sieht, wenn man alle (i,j) verbindet, so daß X_iX_j in Θ als Summand vorkommen, und bemerkt, daß diese Konfiguration von D_4 erhalten bleibt.

Es gilt $(S_4 : D_4) = 3$, somit hat die Galois-Resolvente R_Θ den Grad 3. Eine kurze Rechnung zeigt
$$R_\Theta(T) = T^3 - \sigma_2 T + (\sigma_1\sigma_3 - 4\sigma_4)T + 4\sigma_2\sigma_4 - \sigma_1^2\sigma_4 - \sigma_3^2.$$
Dieses kubische Polynom hat als Wurzeln
$$\Theta = X_1X_3 + X_2X_4,\ \ \Theta' = X_1X_2 + X_3X_4,\ \ \Theta'' = X_1X_4 + X_2X_3,$$

deren Stabilisatoren den drei 2-Sylowgruppen von S_4 entsprechen. Der Zerfällungskörper von $R_\Theta(T)$ ist die galoissche S_3-Zwischenerweiterung die zum Schnitt aller 2-Sylowuntergruppen, also zum Normalteiler

$$V_4 \subseteq S_4$$

gehört.

Es gilt nun für ein irreduzibles Polynom 4. Grades

$$T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$$

unter der Annahme, daß

$$R_{\Theta,\underline{a}} = T^3 - a_2T^2 + (a_1a_3 - 4a_4)T + 4a_2a_4 - a_1^2a_4 - a_3^2 \in K[T]$$

separabel ist, daß

- $\mathrm{Gal}(f) = V_4 \iff R_\Theta(T)$ zerfällt in $K[T]$ in Linearfaktoren.
- $\mathrm{Gal}(f) \simeq D_4$ oder $\mathrm{Gal}(f) \simeq \mathbb{Z}/4\mathbb{Z} \iff R_\Theta(T)$ hat genau eine Nullstelle in K.
- $\mathrm{Gal}(f)$ enthält einen 3-Zykel $\iff R_\Theta(T)$ ist irreduzibel. Da $\mathrm{Gal}(f)$ auch transitiv auf $\{\alpha_1, \dots, \alpha_4\}$ operiert, bedeutet das $\mathrm{Gal}(f) = A_4$ oder $\mathrm{Gal}(f) = S_4$. In welchem Fall man sich befindet, entscheidet sich durch das Diskriminantenkriterium aus Satz 365.

Beispiel 372. Die transitiven Untergruppen von S_4 sind bis auf Konjugation

$$V_4, \mathbb{Z}/4\mathbb{Z}, D_4, A_4, S_4,$$

wobei $\mathbb{Z}/4\mathbb{Z}$ durch einen 4-Zykel erzeugt wird und die D_4 eine 2-Sylowgruppe ist. Die V_4 und A_4 sind eindeutig als Normalteiler. Man beachte aber, daß es auch eine nicht-transitive Kopie von V_4 in S_4 gibt: zum Beispiel erzeugt von (12) und (12)(34).

Die folgenden Polynome in $X_1, \dots, X_4$ realisieren diese Untergruppen als Stabilisatoren.

- $\delta = \prod_{i<j}(X_i - X_j)$ für A_4,
- $\Theta = X_1X_3 + X_2X_4$ für D_4,
- $\Theta + \delta$ für V_4.
- $X_1^2X_2 + X_2^2X_3 + X_3^2X_4 + X_4^2X_1$ für $\mathbb{Z}/4\mathbb{Z} = \langle(1234)\rangle$.
- unwichtig: $X_1+X_2+X_3+X_4$ oder jedes andere Polynom in den elementarsymmetrischen Polynomen für S_4.

21.3. **Die Lösungsformel für Grad 3.** Sei K ein Körper der nicht Charakteristik 2 oder 3 hat, und sei

$$f = T^3 + a_1T^2 + a_2T + a_3 \in K[T]$$

ein kubisches Polynom mit den zu bestimmenden Wurzeln $\alpha_1, \dots, \alpha_3$. Durch Verschieben um $a_1/3$ dürfen wir oBdA annehmen, daß

$$a_1 = 0.$$

Die Diskriminante berechnet sich dann einfach(er) als

$$\mathrm{disc}(f) = -4a_2^3 - 27a_3^2.$$

Wenn $\mathrm{disc}(f) = 0$, so ist f nicht separabel und eine erste Nullstelle bekommt man als Nullstelle von $\mathrm{ggT}(f, f')$. Wir nehmen also an, daß $\mathrm{disc}(f) \neq 0$. Sei

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

Dann gilt $\delta^2 = \mathrm{disc}(f)$ oder

$$\delta = \sqrt{-4a_2^3 - 27a_3^2}.$$

Wir betrachten weiter eine dritte Einheitswurzel $\zeta = \frac{-1+\sqrt{-3}}{2}$, d.h.

$$1 + \zeta + \zeta^2 = 0 \tag{21.2}$$

und die Körper

$$\begin{tikzcd}
 & L(\zeta) \arrow[dl, dash] \arrow[d, dash] \\
L = K(\alpha_1, \ldots, \alpha_3) \arrow[d, dash] & M(\zeta) \arrow[dl, dash] \\
M = K(\delta) \arrow[d, dash] & \\
K &
\end{tikzcd}$$

Aus Satz 365 folgt, daß $\mathrm{Gal}(L/M) \subseteq A_3$. Wenn f nicht irreduzibel ist, dann hat $\mathrm{Gal}(f) \subseteq S_3$ einen Fixpunkt und ist entweder trivial oder zyklisch der Ordnung 2. In jedem Fall ist dann $L = M$. Wenn hingegen f irreduzibel ist, dann ist $\mathrm{Gal}(f) \subseteq S_3$ entweder A_3 oder S_3, in jedem Fall allerdings ist dann

$$L(\zeta)/M(\zeta)$$

zyklisch von Ordnung 3. Die Methode der Lagrange-Resolvente führt dann zur Struktur einer Radikalerweiterung. Wir machen daher den Ansatz

$$\begin{aligned}
A &= \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 \\
B &= \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3
\end{aligned}$$

und erinnern uns an

$$0 = -a_1 = \alpha_1 + \alpha_2 + \alpha_3.$$

Wir erwarten nun Formeln für A^3 und B^3 aus $M(\zeta)$: aus (21.2) folgt

$$\begin{aligned}
A + B &= 3\alpha_1 && (21.3)\\
A + \zeta B &= 3\zeta^2\alpha_3 && (21.4)\\
A + \zeta^2 B &= 3\zeta\alpha_2 && (21.5)\\
A - B &= (\zeta - \zeta^2)(\alpha_2 - \alpha_3) \\
A - \zeta B &= (1 - \zeta)(\alpha_1 - \alpha_2) \\
A - \zeta^2 B &= (\zeta^2 - 1)(\alpha_3 - \alpha_1).
\end{aligned}$$

Somit

$$\begin{aligned}
A^3 + B^3 &= (A + B)(A + \zeta B)(A + \zeta^2 B) \\
&= 27\alpha_1\alpha_2\alpha_3 = -27a_3, \\
A^3 - B^3 &= (A - B)(A - \zeta B)(A - \zeta^2 B) \\
&= (\zeta - \zeta^2)(\alpha_2 - \alpha_3)(1 - \zeta)(\alpha_1 - \alpha_2)(\zeta^2 - 1)(\alpha_3 - \alpha_1) \\
&= 3(\zeta^2 - \zeta)\delta.
\end{aligned}$$

folglich (Wenn man stattdessen $-\delta$ als Wurzel von $\mathrm{disc}(f)$ gewählt hat, dann vertauschen an dieser Stelle A und B. Das permutiert die Nullstellen nur.)

$$\begin{aligned}
A^3 &= -\frac{27}{2}a_3 + \frac{3}{2}(\zeta^2 - \zeta)\delta, \\
B^3 &= -\frac{27}{2}a_3 - \frac{3}{2}(\zeta^2 - \zeta)\delta.
\end{aligned}$$

Die dritten Wurzeln A und B sind allerdings nicht ganz unabhängig zu wählen. Der Ansatz führt durch Ausmultiplizieren auf

$$AB = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_3\alpha_1 = (\sigma_1^2 - 3\sigma_2)(\underline{\alpha}) = -3a_2$$

so daß die Wahl von

$$A = \sqrt[3]{-\frac{27}{2}a_3 + \frac{3}{2}(\zeta^2 - \zeta)\delta}$$

die Wahl von

$$B = \frac{-3a_2}{A}$$

bedingt. Die finale Lösungsformel für die α_i ergibt sich dann aus (21.3) – (21.5). Man kann die Formeln noch ein wenig polieren:

Satz 373 (Cardanosche Formel)**.** *Sei K ein Körper nicht von Charakteristik 2 oder 3, und sei*

$$f(T) = T^3 + a_2T + a_3$$

ein kubisches Polynom aus $K[T]$. Es sei ζ eine primitive dritte Einheitswurzel. Wir wählen in algebraischen Erweiterungen von K

$$\begin{aligned} z &= \left(\frac{a_2}{3}\right)^3 + \left(\frac{a_3}{2}\right)^2 \\ \xi &= \sqrt{z} \\ u &= \sqrt[3]{-\frac{a_3}{2} + \xi} \\ v &= \sqrt[3]{-\frac{a_3}{2} - \xi} \end{aligned}$$

mit der Bedingung

$$uv = -\frac{a_2}{3}.$$

Dann sind die Lösungen von $f(T) = 0$ gegeben durch

$$\begin{aligned} \alpha_1 &= u + v, \\ \alpha_2 &= \zeta u + \zeta^2 v, \\ \alpha_3 &= \zeta^2 u + \zeta v. \end{aligned}$$

Beweis. Den verbesserten Formeln liegt die Subsitution $u = A/3$, $v = B/3$ zugrunde. Der Rest folgt durch Nachrechnen, etwa $z = -\operatorname{disc}(f)/(4 \cdot 27)$ und

$$(\zeta^2 - \zeta)\delta/9 = -(1 + 2\zeta)\delta/9 = -\sqrt{-\operatorname{disc}(f)/27} = -2\xi$$

etc. □

Übungsaufgaben zu §21

Übungsaufgabe 21.1. Sei $G \subseteq S_n$ eine Untergruppe. Zeigen Sie, daß

$$F = \sum_{\sigma \in G} \left(\prod_{i=1}^{n} X_{\sigma(i)}^i\right)$$

ein primitives Element für die Erweiterung

$$K(X_1, \ldots, X_n)^G / K(\sigma_1, \ldots, \sigma_n)$$

ist.

Teil 5. Appendix

Anhang A. Das Zornsche Lemma

Um zu beweisen, daß jeder Körper in einem algebraisch abgeschlossenen Körper enthalten ist, brauchen wir etwas mathematische Logik.

A.1. **Das Auswahlaxiom.**

Zu einer Menge M bezeichnen wir mit
$$\mathscr{P}(M)^{\times} = \{S \subseteq A \ ; \ S \neq \emptyset\}$$
die Menge aller nichtleeren Teilmengen von A, also die Potenzmenge von A ohne die leere Menge.

Definition 374. Eine **Auswahlfunktion** auf einer Menge M ist eine Abbildung
$$f : \mathscr{P}(M)^{\times} \to M$$
mit der Eigenschaft, daß
$$f(A) \in A$$
für alle $A \in \mathscr{P}(M)^{\times}$. Die Funktion f stellt also für jede nichtleere Teilmenge A von M ein Element aus A bereit.

Auswahlfunktionen sind nichts anderes als Elemente des katesischen Produkts von Mengen
$$\prod_{\emptyset \neq A \subseteq M} A.$$

Axiom 1 (Auswahlaxiom)**.** Zu jeder Menge gibt es eine Auswahlfunktion.

Mittels der Interpretation als Elemente des kartesischen Produkts besagt das Auswahlaxiom also letztlich nur, daß das Produkt nichtleerer Mengen wieder nicht leer ist.

Dies klingt plausibel, muß aber im Rahmen der Mengenlehre axiomatisch gefordert werden. Wir verweisen auf mathematische Logik zur Klärung der logischen Zusammenhänge und beschränken uns hier darauf, die Äquivalenz zum Wohlordnungssatz und zum Lemma von Zorn zu beschreiben.

A.2. **Der Wohlordnungssatz.**

Definition 375. (1) Eine **(partielle) Ordnung** auf einer Menge M ist eine Relation $\leq$ auf der Menge M, so daß für alle $x, y, z \in M$ gilt:
   (i) transitiv: Wenn $x \leq y$ und $y \leq z$, dann gilt $x \leq z$.
   (ii) antisymmetrisch: Wenn $x \leq y$ und $y \leq x$, dann gilt $x = y$.
   (iii) reflexiv: $x \leq x$.

(2) Eine **totale Ordnung** auf einer Menge M ist eine partielle Ordnung auf M, so daß zusätzlich
   (iv) $x \leq y$ oder $y \leq x$ gilt.

(3) Eine **Wohlordnung** auf einer Menge M ist eine partielle Ordnung $\leq$ auf M, so daß für jede nichtleere Teilmenge $S \subseteq M$ ein kleinstes Element bezüglich $\leq$ gibt, d.h. es gibt $x \in S$ so daß für alle $y \in S$:
$$x \leq y.$$
Eine Menge kann **wohlgeordnet** werden, wenn es auf ihr eine Wohlordnung gibt.

Beispiel 376. (1) Die Potenzmenge einer Menge M hat eine partielle Ordnung: die Inklusion. Diese partielle Ordnung ist im Allgemeinen nicht total geordnet.

(2) Die Menge $\mathbb{Z}$ ist bezüglich der üblichen $\leq$-Relation total geordnet, aber nicht wohlgeordnet. Aber $\mathbb{Z}$ kann wohlgeordnet werden, indem man etwa setzt
$$0 \preceq 1 \preceq -1 \preceq 2 \preceq -2 \preceq 3 \preceq -3 \preceq \ldots$$

(3) Die Menge $\mathbb{N}$ mit der üblichen $\leq$-Relation ist wohlgeordnet, aber $\mathbb{R}_+ = \{r \in \mathbb{R} \; ; \; r > 0\}$ mit $\leq$ nicht.

(4) Die folgende Menge rationaler Zahlen

$$M = \{m - \frac{1}{n} \; ; \; n, m \in \mathbb{N}\}$$

mit der üblichen $\leq$-Ordnung ist wohlgeordnet.

Lemma 377. *Jede wohlgeordnete Menge ist total geordnet.*

Beweis. Sei M wohlgeordnet und $x, y \in M$ beliebig. Dann hat $\{x, y\}$ ein kleinstes Element, oBdA x, somit $x \leq y$. □

Axiom 2 (Wohlordnungssatz)**.** Jede Menge kann wohlgeordnet werden.

Das ist schon weniger plausibel als das Auswahlaxiom.

A.3. **Das Lemma von Zorn.**

Definition 378. (1) Sei M bezüglich $\preceq$ partiell geordnet. Ein Element $x \in M$ heißt **obere Schranke** für die Teilmenge $S \subseteq M$, wenn $y \preceq x$ für alle $y \in S$ gilt.

(2) Die Menge M heißt bezüglich der Ordnung $\preceq$ **induktiv geordnet**, wenn jede total geordnete Teilmenge $S \subseteq M$ eine obere Schranke in M besitzt.

(3) Ein Element $x \in M$ einer bezüglich $\preceq$ partiell geordneten Menge M heißt **maximales Element**, wenn für alle $y \in M$ mit $x \preceq y$ schon $x = y$ gilt.

Beispiel 379. (1) Sei M eine Menge. Die Menge der Teilmengen von M ist bezüglich der Inklusion induktiv geordnet. Eine Obere Schranke ergibt sich als Vereinigung.

(2) Sei M eine Menge. Die Menge der echten Teilmengen $U \subset M$, also $U \neq M$, ist bezüglich Inklusion partiell geordnet. Für jedes $a \in M$ ist $U_a = M \setminus \{a\}$ ein maximales Element.

Axiom 3 (Lemma von Zorn)**.** Sei M eine nicht-leere, bezüglich $\preceq$ induktiv geordnete Menge. Dann hat M bezüglich $\preceq$ ein maximales Element.

Notation 380. Sei M eine bezüglich $\preceq$ partiell geordnete Menge $x, y \in M$ und $S \subseteq M$ eine Teilmenge.

(1) Mit $x \prec y$ bezeichenen wir '$x \preceq y$ und $x \neq y$'.

(2) Weiter setzen wir

$$S_{\preceq x} = \{s \in S \; ; \; s \preceq x\}$$
$$S_{\prec x} = \{s \in S \; ; \; s \prec x\}.$$

A.4. **Auswahlaxiom, Wohlordnungssatz und das Lemma von Zorn.** Wir zeigen nun die logische Äquivalenz dieser drei Aussagen.

Theorem 381. *Die folgenden Aussagen sind äquivalent.*

(a) Es gilt das Lemma von Zorn.
(b) Es gilt der Wohlordnungssatz.
(c) Es gilt das Auswahlaxiom.

Beweis. (a) $\Longrightarrow$ (b): Sei M eine Menge. Wir definieren die Menge

$$\mathscr{W} = \{(A, \preceq) \; ; \; A \subseteq M, \; \preceq \text{ ist Wohlordnung auf } A\}$$

der mit einer Wohlordnung ausgestatteten Teilmengen von M. Die Menge $\mathscr{W}$ ist partiell geordnet durch

$$(A, \preceq_A) \leq (B, \preceq_B)$$

wenn

(i) $A \subseteq B$,

(ii) $\preceq_B$ setzt $\preceq_A$ fort: für alle $x, y \in A$ gilt $x \preceq_A y \iff x \preceq_B y$,
(iii) für alle $a \in A$ und $b \in B \setminus A$ gilt $a \preceq b$.

Dann ist $\mathscr{W}$ mit $\leq$ induktiv geordnet: sei $(A_i, \preceq_i)_{i \in I}$ eine total geordnete Teilmenge von $\mathscr{W}$. Eine obere Schranke wird gegeben durch

$$A = \bigcup_{i \in I} A_i$$

mittels für alle $a, b \in A$

$$a \preceq b \iff a \preceq_i b \text{ sofern } a, b \in A_i.$$

Dies ist wohldefiniert und eine partielle Ordnung, da die $\preceq_i$ einander fortsetzen. Die Vereinigung A ist mit $\preceq$ wohlgeordnet: sei $S \subseteq A$ eine nicht-leere Teilmenge. Dann gibt es $i \in I$ mit $S_i := S \cap A_i \neq \emptyset$. Da A_i bezüglich $\preceq_i$ wohlgeordnet ist, gibt es ein kleinstes Element $x \in S_i$. Dieses ist auch kleinstes für S, da alle Elemente aus $S \setminus S_i$ sowieso größer sind. Hier geht die strenge Eigenschaft (iii) der Ordnung $\leq$ auf $\mathscr{W}$ ein.

Die Menge $\mathscr{W}$ ist nicht leer, da $\emptyset \subseteq M$ eine Teilmenge ist, die wohlgeordnet werden kann.

Nach dem Lemma von Zorn gibt es demnach ein maximales Element in $\mathscr{W}$. Dies sei $(A, \preceq)$. Wenn $A \neq M$, dann gibt es $x \in M \setminus A$ und auf $A \cup \{x\}$ die Wohlordnung, die $\preceq$ fortsetzt durch $a \leq x$ für alle $a \in A$. Dies ist ein Widerspruch zur Maximalität. Somit muß $A = M$ sein und M besitzt eine Wohlordnung.

(b) $\Longrightarrow$ (c): Sei M eine Menge. Auf dieser existiert nach Voraussetzung eine Wohlordnung $\preceq$. Wir definieren nun eine Auswahlfunktion für nicht-leere Teilmengen A von M durch

$$f(A) := \text{kleinstes Element von } A \text{ bezüglich } \preceq.$$

Damit erfüllte M das Auswahlaxiom.

(c) $\Longrightarrow$ (a) *nach Grayson, Kneser und Zermelo*: Wir beweisen dies durch Widerspruch. Wir nehmen also an, daß es eine bezüglich $\preceq$ induktiv geordnete, nicht-leere Menge M ohne maximale Elemente gibt.

Schritt 1, Auswahl oberer Schranken: Zu jeder totalgeordneten Teilmenge $T \subseteq M$ ist die Menge der oberen Schranken außerhalb T

$$U_T = \{x \in M \; ; \; t \prec x \text{ für alle } t \in T\} \neq \emptyset$$

nicht leer, denn es gibt eine obere Schranke x_0 von T, die nach Voraussetzung nicht maximal sein kann, was durch ein $x_0 \prec x$ bezeugt wird. Dieses x liegt in U_T.

Nach dem Auswahlaxiom gibt es nun eine Auswahlfunktion, die simultan aus allen U_T ein Element auswählt. Damit konstruieren wir

$$f : \{T \subseteq M \; ; \; T \text{ total geordnet}\} \to M$$

mit $f(T) \in U_T$.

Schritt 2, Beweisidee: Wir machen nun intuitiv das folgende. Die leere Menge ist total geordnet und $f(\emptyset) = x_0 \in M$ ein Element (spätestens hier brauchen wir, daß M nicht leer ist). Dann ist $\{x_0\}$ total geordnet, und $x_1 = f(\{x_0\})$. Wegen $x_0 \prec x_1$ ist auch $\{x_0, x_1\}$ total geordnet. Induktiv konstruieren wir

$$x_{n+1} = f(\{x_0, \ldots, x_n\})$$

und weiter, wenn die natürlichen Zahlen zu Ende sind

$$x_{\mathbb{N}} = f(\{x_0, x_1, \ldots\}).$$

Weiter geht es dann mit

$$x_{\mathbb{N}+1} = f(\{x_0, x_1, \ldots\} \cup \{x_{\mathbb{N}}\}).$$

Diese Konstruktion hört nie auf und liefert eine Abbildung aller Ordnialzahlen injektiv in M. Das geht nicht, da irgendwann die Ordnialzahlen eine größere Mächtigkeit haben als M. Mit der Theorie der Ordinalzahlen wären wir nun fertig. Ohne sie müssen wir noch ein wenig arbeiten.

Schritt 3, f-Mengen: Wohlgeordnete Teilmengen sind insbesondere nach Lemma 377 total geordnete Teilmengen. Wir sagen, daß eine wohlgeordnete Teilmenge $W \subseteq M$ eine f-Menge ist, wenn

(i) für alle $x \in W$ gilt
$$f(W_{\prec x}) = x,$$

(ii) und $x_0 = f(\emptyset) \in W$.

Die eben konstruierten Mengen $\{x_0, x_1, \ldots, x_n\}$ sind Beispiele von f-Mengen.

Schritt 4, die Menge aller f-Mengen ist total geordnet: Zu f-Mengen V und W betrachten wir die Vereinigung T aller Mengen $S \subseteq V \cap W$ für die es $v \in V$ und $w \in W$ gibt mit
$$V_{\preceq v} = S = W_{\preceq w}.$$
Die Menge T ist somit die Vereinigung der in V und W gleichen 'Anfangsstücke'.

Für alle $t \in T$ gilt dann
$$V_{\preceq t} \subseteq T \text{ und } W_{\preceq t} \subseteq T, \tag{A.1}$$
denn es gibt S, $v \in V$ und $w \in W$ wie oben mit $t \in S = V_{\preceq v} = W_{\preceq w} \subseteq T$, und dann ist auch
$$V_{\preceq t} \subseteq V_{\preceq v} = S \subseteq T$$
und analog für $W_{\preceq t}$. Wenn also $a \in V \setminus T$, dann gilt (und analog für W):
$$T \subseteq V_{\prec a}, \tag{A.2}$$
denn sonst gibt es $t \in T$ mit $a \preceq t$ und dann einen Widerspruch $a \in T$ aus (A.1).

Wir behaupten nun, daß die Menge der f-Mengen bezüglich Inklusion total geordnet ist, genauer behaupten wir $T = V$ oder $T = W$. Angenommen $T \subsetneq V$ und $T \subsetneq W$. Jetzt brauchen wir, daß V, W wohlgeordnet sind, denn damit sind wohldefiniert
$$a_0 = \min V \setminus T \text{ und } b_0 = \min W \setminus T.$$
Folglich gilt
$$V_{\prec a_0} \subseteq T$$
was zusammen mit (A.2) (und analog für W)
$$T = V_{\prec a_0} = W_{\prec b_0}$$
ergibt. Die f-Mengen Eigenschaft führt nun zu einem Widerspruch, denn
$$t_0 = a_0 = f(V_{\prec a_0}) = f(T) = f(W_{\prec b_0}) = b_0$$
bedeutet, daß $T \cup \{t_0\} \subseteq V \cap W$ und
$$T \cup \{t_0\} = V_{\prec a_0} \cup \{a_0\} = V_{\preceq a_0}$$
und analog $T \cup \{t_0\} = W_{\preceq b_0}$. Damit ist $S = T \cup \{t_0\}$ eine der Mengen, deren Vereinigung T ist, also $t_0 \in T$: Widerspruch.

Schritt 5, Vereinigung aller f-Mengen: Wir setzen nun
$$F = \bigcup_{W \text{ ist } f\text{-Menge}} W$$
Dies ist selbst eine f-Menge, denn

(1) F ist wohlgeordnet: für alle $\emptyset \neq S \subseteq F$ ist
$$\min S = \min_{S \cap W \neq \emptyset, W \text{ ist } f\text{-Menge}} S \cap W.$$
Mindestens ein $S \cap W$ ist nicht die leere Menge, und die Minima sind unabhängig vom gewählten W, weil je zwei f-Mengen V, W das gleiche Anfangsstück T haben.

(2) Zu jedem $x \in F$ ist
$$F_{\prec x} = W_{\prec x},$$
sofern W eine f-Menge ist mit $x \in W$. Daher gilt auch
$$x = f(W_{\prec x}) = f(F_{\prec x}).$$

Schritt 6, Der Widerspruch: Die Menge
$$F \cup \{f(F)\}$$
enthält echt die Menge F und ist selbst eine f-Menge. Das geht nicht, denn jede f-Menge ist in F enthalten. Widerspruch. $\square$

Anhang B. Mehr über Permutationsgruppen

Ziel dieses Anhangs ist ein Satz von Jordan über primitive Permutationsgruppen.

Definition 382. Ein **Block** für eine Permutationsgruppe $G \hookrightarrow S_M$ ist eine Teilmenge $B \subseteq M$, so daß für alle $g \in G$

(a) $g(B) = B$, oder
(b) $g(B) \cap B = \emptyset$.

Beispiel 383. (1) Es gibt stets die trivialen Blöcke bestehend aus einem Element, oder bestehend aus der ganzen Menge.
(2) Betrachtet man beim Rubik's Cube nur die Wirkung der Drehungen auf den Eckenplättchen, dann sind je drei davon die Farben einer Ecke. Diese bleiben stets zusammen und bilden daher einen Block.

Proposition 384. *Sei B ein Block für eine transitive Permutationsgruppe $G \hookrightarrow S_M$.*
(1) Für alle $g \in G$ ist auch $g(B)$ ein Block.
(2) Wir setzen $G_B := \{g \in G \ ; \ g(B) = B\}$ für den Stabilisator des Blocks als Teilmenge. Dann ist
$$M = \bigcup_{g \in G/B_B} g(B)$$
eine disjunkte Zerlegung in Blöcke.
(3) Es gilt ist # ein Teiler von $\#G$ und
$$\#M = \#B \cdot (G : G_B).$$

Beweis. (1) Wir müssen zeigen, daß für alle $h \in G$ aus $hg(B) \cap g(B) \neq \emptyset$ folgt $hg(B) = g(B)$. Dazu operieren wir mit g^{-1} und schon folgt alles aus der entsprechenden Eigenschaft von B.

(2) Dies ist einfach nur die Vereinigung der Translate von B ohne Mehrfachnennung. Die Vereinigung ist disjunkt nach (1). Weil G transitiv operiert, ist dies ganz M.

(3) folgt aus der Zerlegung in (2), weil für alle $g \in G$ gilt $\#g(B) = \#B$. $\square$

Wenn eine transitive Permutationsgruppe, wie dies $\mathrm{Gal}(f)$ für irreduzibles f so ist, einen Block $B \subseteq M$ besitzt, dann kann man eine kleinere Untergruppe von S_M angeben, in der G enthalten ist. Dies ist die Untergruppe der Permutationen, welche die Blockzerlegung $M = \bigcup_{i \in I} B_i$ in Translate $B_i = g_i(B)$ von B respektieren:
$$S_{M,B} := \{\sigma \in S_M \ ; \ \text{für alle } i \in I \text{ gibt es ein } j \in I \text{ mit } \sigma(B_i) = B_j\}.$$
Diese Gruppe hat einen Normalteiler
$$\prod_{i \in I} S_{B_i} = \{\sigma \in S_M \ ; \ \text{für alle } i \in I \text{ gilt } \sigma(B_i) = B_i\}$$

und die Faktorgruppe ist natürlich isomorph zu S_I, der Permutationsgruppe der Blöcke als ganzes. Wir haben eine kurze exakte Sequenz

$$1 \to \prod_{i \in I} S_{B_i} \to S_{M,B} \to S_I \to 1$$

und $G \subseteq S_{M,B}$.

Definition 385. Eine **primitive** Permutationsgruppe ist eine transitive Permutationsgruppe, die nur die trivialen Blöcke hat. Andernfalls, wenn es nichttriviale Blöcke gibt, dann nennt man die transitive Permutationsgruppe **imprimitiv**.

Lemma 386. *Eine transitive Permutationsgruppe $G \hookrightarrow S_M$ ist primitiv genau dann, wenn der Punkt-Stabilisator*

$$G_a = \{g \in G \quad g(a) = a\}$$

für ein (äquivalent für alle) $a \in M$ eine maximale Untergruppe von G ist.

Beweis. Wegen $G_{\sigma(a)} = \sigma G_a \sigma^{-1}$ sind die Punkt-Stabilisatoren sämtliche konjugiert. Daher sind entweder alle oder keine der Gruppen G_a maximal in G.

Angenommen, es gibt einen nichttrivialen Block $B \subseteq M$. Wir wählen $a \in B$. Dann sind die Inklusionen in

$$G_a \subseteq G_B = \{\sigma \in G \ ; \ \sigma(a) \in B\} \subseteq G$$

jeweils echt, da G transitiv auf M operiert. Somit ist G_a nicht maximal.

Sei umgekehrt G_a nicht maximal und $G_a \subseteq H \subseteq G$ eine echte Zwischengruppe. Der Orbit $B = Ha \subseteq M$ ist dann ein nicht-trivialer Block. Wenn nämlich für $g \in G$ der Schnitt $g(B) \cap B$ nicht leer ist, dann gibt es $h, k \in H$ mit

$$gh(a) = k(a)$$

also $k^{-1}gh \in G_a \subseteq H$. Daher gilt auch $g \in H$ und $g(B) = g(Ha) = Ha = B$. Somit ist B in der Tat ein Block. □

Lemma 387. *Sei $G \hookrightarrow S_M$ eine transitive Permutationsgruppe. Dann sind äquivalent.*

(1) *G ist 2-transitiv.*
(2) *Es gibt ein $a \in M$, für das der Stabilisator*

$$G_a = \{g \in G \quad g(a) = a\}$$

auf $M \setminus \{a\}$ transitiv operiert.

Beweis. (2) $\Longrightarrow$ (1): Es reicht aus, für ein festes $b \in M \setminus \{a\}$ das Paar (a, b) auf ein beliebiges Paar (x, y) mit $x \neq y$ abzubilden. Da die Operation transitiv ist, gibt es ein $g \in G$ mit $g(a) = x$. Dann ist $g^{-1}(y) \in M \setminus \{a\}$ und somit gibt es ein $h \in G_a$ mit $h(b) = g^{-1}(y)$. Dann gilt $gh(a, b) = (x, y)$.

(1) $\Longrightarrow$ (2): Seien $b, c \in M \setminus \{a\}$. Dann gibt es ein $g \in G$ mit $g(a, b) = (a, c)$, oder anders ausgedrückt $g \in G_a$ und $g(b) = c$. Also ist die Operation von G_a auf $M \setminus \{a\}$ transitiv. □

Lemma 388. *Sei $G \hookrightarrow S_M$ eine transitive Permutationsgruppe, und $\Delta \subsetneq M$ eine echte Teilmenge. Dann ist für alle $a \in M$*

$$\Delta_a := \bigcap_{\sigma, \ a \in \sigma(\Delta)} \sigma(\Delta). \tag{B.1}$$

ein Block von M.

Beweis. Erst einmal ist $a \in \Delta_a$ und Δ_a nicht leer. Sei $g \in G$ ein Element. Dann gilt offensichtlich sofort aus der Definition

$$g(\Delta_a) = \bigcap_{\sigma, \ a \in \sigma(\Delta)} g\sigma(\Delta) = \bigcap_{g\sigma, \ g(a) \in g\sigma(\Delta)} g\sigma(\Delta) = \Delta_{g(a)}.$$

Wenn $b \in \Delta_a$, dann gilt offensichtlich

$$\Delta_b \subseteq \Delta_a,$$

da höchstens über mehr Teilmengen geschnitten wird. Weil aber die G-Operation transitiv ist, gibt es $g \in G$ mit $b = g(a)$ und daher ist

$$\#\Delta_b = \#\Delta_{g(a)} = \#\Delta_a.$$

Als gleichmächtige Teilmenge gilt demnach

$$\Delta_b = \Delta_a.$$

Seien nun $a \in M$ beliebig. Wenn es ein $c \in \Delta_a \cap g(\Delta_a) = \Delta_a \cap \Delta_{g(a)}$ gibt, dann ist

$$\Delta_a = \Delta_c = \Delta_g(a) = g(\Delta_a).$$

Daher ist Δ_a ein Block von $G \hookrightarrow S_M$. □

Satz 389 (Jordan)**.** *Sei $G \hookrightarrow S_M$ eine primitive Permutationsgruppe. Wenn es ein $T \subseteq M$ gibt mit*

(i) $\#T \geq 2$ und $S = M \setminus T$ hat $\#S \geq 1$, und

(ii) Die Untergruppe $F_S = \{g \in G \ ; \ g(s) = s$ für alle $s \in S\}$ operiert transitiv auf T,

dann ist G eine 2-fach transitive Permutationsgruppe.

Beweis. Schritt 1: Wir zeigen zunächst, wie wir T größer machen können. Angenommen es gibt ein $g \in G$ mit

- $T' = T \cup g(T) \neq M$, und
- $T \cap g(T) \neq \emptyset$.

Dann können wir T durch T' ersetzen. Es gilt dann $S' = M \setminus T' = S \cap g(S)$. Es operiert

$$gF_Sg^{-1} = F_{g(S)}$$

transitiv auf $g(T)$ (durch Strukturtransport mittels Translation mit g von der transitiven Operation von F_S auf T). Wegen

$$F_S \text{ und } F_{g(S)} \subseteq F_{S'}$$

operiert $F_{S'}$ schon mal mit höchstens zwei Bahnen auf T', nämlich eine die T und eine Bahn die $g(T)$ enthält. Diese Mengen schneiden sich nach Voraussetzung, so daß es nur eine Bahn geben kann.

Schritt 2:

Weil G primitiv ist, gibt es ein $g \in G$ mit $g(T) \cap T \neq \emptyset$ und $g(T) \neq T$. Solange $T \cup g(T) \neq M$ gilt, können wir also T durch T' wie oben ersetzen und T vergrößern. Wir dürfen also annehmen, daß für alle $g \in G$ gilt

- $g(T) = T$ oder
- $T \cup g(T) = M$.

Schritt 3: Wir wenden nun Lemma 388 für ein $a \notin T$ auf $\Delta = S = M \setminus T$ and. Weil

$$a \in \Delta_a$$

ein Block von G auf M ist, aber G primitiv ist, so gilt

$$\Delta_a = \{a\}$$

und als Komplement dazu

$$M \setminus \{a\} = \bigcup_{\sigma, \ a \notin \sigma(T)} \sigma(T).$$

Wenn es dabei ein σ gibt, mit $\sigma(T) \neq T$, dann muß wegen Schritt 2 schon $T \cup \sigma(T) = M$ sein, ein Widerspruch. Daher gilt für alle σ, über die vereinigt wird, schon $\sigma(T) = T$. Somit gilt

$$T = M \setminus \{a\},$$

und $G_a = F_{M\setminus T}$ operiert transitiv auf $T = M\setminus\{a\}$. Nach Lemma 387 ist G somit 2-transitiv. $\square$

Korollar 390 (Jordan)**.** *Eine primitive Permutationsgruppe $G \hookrightarrow S_M$, die eine Transposition von S_M enthält, ist notwendig bereits $G = S_M$.*

Beweis. Sei $\tau_{a,b} \in G$ die Transposition von $a, b \in M$. Dann erfüllt $T = \{a, b\} \subseteq M$ die Voraussetzung von Satz 389, und G ist 2-transitiv.

Seien x, y zwei verschiedene Elemente in M. Dann gibt es ein $g \in G$ mit $g(a) = x$ und $g(b) = y$. Wir sehen, daß die Transposition von x, y

$$\tau_{x,y} = g\tau_{a,b}g^{-1}$$

auch in G enthalten ist. Damit enthält G alle Transpositionen aus S_M, also ein Erzeugendensystem von S_M. $\square$

Übungsaufgaben zu §B

Übungsaufgabe B.1. Wir betrachten eine endliche Gruppe G als Permutationsgruppe durch Linkstranslation auf sich selbst: $G \hookrightarrow S_G$. Bestimmen Sie die Blöcke dieser Permutationsgruppe. Für welche G ist dies eine primitive Permutationsgruppe?

Anhang C. Struktursätze für abelsche Gruppen

In diesem Anhang behandeln wir die Klassifikation endlich erzeugter abelscher Gruppen und beweisen Pontrjagin–Dualität für endliche abelsche Gruppen.

C.1. **Endlich erzeugte abelsche Gruppen.** Was wir in diesem Abschnitt über abelsche Gruppen lernen, funktioniert so direkt analog auch für Modul über Hauptidealringen.

C.1.1. *Freie abelsche Gruppen.*

Definition 391. Eine **Basis** für eine abelsche Gruppe A ist eine Tupel $(x_i)_{i\in I}$ von Elementen $x_i \in A$ so daß jedes $g \in A$ auf eindeutige Art und Weise als endliche Summe

$$a = \sum_i a_i x_i$$

mit $a_i \in \mathbb{Z}$ und fast alle $a_i = 0$ geschrieben werden kann.

Eine **freie abelsche Gruppe** ist eine Gruppe, die eine Basis besitzt.

Beispiel 392. (1) Die Gruppe $\mathbb{Z}^n$ der Zeilen mit Einträgen aus $\mathbb{Z}$ ist eine freie Gruppe mit Basis der $e_i \in \mathbb{Z}^n$ für $i = 1, \ldots, n$ dem Vektor mit 1 im i-ten Eintrag und 0 sonst.

(2) Sei I eine Menge und $\mathbb{Z}^{(I)} = \bigoplus_{i\in I} \mathbb{Z}$ die mit I indizierte direkte Summe von Kopien von $\mathbb{Z}$. Dann ist $\mathbb{Z}^{(I)}$ per Konstruktion eine freie Gruppe mit der Basis bestehend aus den Elementen $e_i \in \mathbb{Z}^{(I)}$ deren i ter Eintrag 1 und alle anderen Einträge 0 sind.

(3) Sei A eine freie Gruppe mit Basis $(x_i)_{i\in I}$. Dann ist

$$\mathbb{Z}^{(I)} \to A, \quad (a_i) \mapsto \sum_{i\in I} a_i x_i,$$

ein Gruppenisomorphismus (die auftretenden Summen sind endliche Summen!).

Umgekehrt für ein solcher Isomorphismus durch das Bild der Basis $(e_i)_{I\in I}$ auf eine Basis von A.

Definition 393. Der **Rang** einer freien abelschen Gruppe A ist die Mächtigkeit einer Basis von A und wird mit

$$\mathrm{rg}(A) = \mathrm{rg}_{\mathbb{Z}}(A)$$

bezeichnet.

Man muß sich überlegen, daß die Definition des Rangs wohldefiniert ist. Für freie abelsche Gruppen endlichen Rangs ist das leicht. Hat A eine Basis von Mächtigkeit n, dann ist $A \simeq \mathbb{Z}^n$ und daher

$$\#(A/2A) = \#(\mathbb{Z}^n/2\mathbb{Z}^n) = \#(\mathbb{Z}/2\mathbb{Z})^n = 2^n.$$

Somit bestimmt A über $A/2A$ den Wert von n, dieser ist somit unabhängig von der gewählten Basis.

Ein Basiswechsel der Standardbasis $e_1, \ldots, e_n$ von $\mathbb{Z}^n$ zu einer neuen Basis $b_1, \ldots, b_n$ entspricht einem Automorphismus $S : \mathbb{Z}^n \to \mathbb{Z}^n$ definiert durch $e_i \mapsto S(e_i) = b_i$, der neue Koordinaten auf alte Koordinaten abbildet. Der Automorphismus wird durch die ganzzahlige $n \times n$-Matrix

$$S = (b_1, \ldots, b_n) \in \mathrm{M}_n(\mathbb{Z})$$

und Matrixmultiplikation vermittelt. Die Invertierbarkeit bedeutet, daß $S \in \mathrm{GL}_n(\mathbb{Z})$, also

$$\det(S) = \pm 1.$$

Definition 394. Die **allgemeine lineare Gruppe** der Größe n über dem Ring R ist die Gruppe bezüglich Matrixmultiplikation der Matrizen

$$\mathrm{GL}_n(R) = \{A \in \mathrm{M}_n(R) \ ; \ \det(R) \in R^\times\}.$$

Es ist zu überlegen, warum $\mathrm{GL}_n(R)$ eine Gruppe ist. Neutrales Element ist die Einheitsmatrix E_n, Assoziativität folgt aus der Assoziativität im Ring der Matrizen $\mathrm{M}_n(R)$. Einzig fraglich ist die Existenz des Inversen. Sei $\hat{A}_{ij}$ die Matrix, die aus A entsteht durch Löschen der i-ten Zeile und der j-ten Spalte. Sei weiter $A^\#$ die Matrix mit

$$(A^\#)_{ij} = (-1)^{i+j} \det(A_{ji}).$$

Wichtig ist, daß $A^\#$ sich durch Polynome in den Einträgen von A ausdrücken läßt. Dann gilt

$$A \cdot A\# = A^\# \cdot A = \det(A) \cdot E_n.$$

Dies gilt bekanntermaßen, wenn R ein Körper ist, und sofort auch, wenn nur R ein Teilring eines Körpers ist. Damit gilt es für die allgemeine Matrix $\mathscr{X} = (X_{ij})$ in der die Einträge Variablen X_{ij} in dem Polynomring $\mathbb{Z}[X_{ij}; 1 \le i, j \le n]$ sind, denn der Polynomring ist als Integritätsring in seinem Quotientenkörper enthalten. Der allgemeine Fall folgt durch Einsetzen der Einträge von $A = (a_{ij})$ also durch Anwendung des Homomorphismus nach R, der auf den Vairablen durch $X_{ij} \mapsto a_{ij}$ definiert ist.

Da wir für $A \in GL_n(R)$ fordern, daß $\det(A) \in R^\times$ invertierbar ist, und weil

$$\det(A)^{n-1} = \det(\det(A) \cdot E_n)/\det(A) = \det(A \cdot A^\#)/\det(A) = \det(A^\#)$$

auch invertierbar ist, so ist auch

$$A^{-1} = \det(A)^{-1} \cdot A^\# \in \mathrm{GL}_n(R),$$

und überdies das gesuchte Inverse zu A.

Lemma 395. *Es gilt vermöge Matrixmultiplikation*

$$\mathrm{Aut}(\mathbb{Z}^n) = \mathrm{GL}_n(\mathbb{Z}).$$

Beweis. Das ist nun klar. □

C.1.2. *Untergruppen von freien abelschen Gruppen.*

Lemma 396. *Eine Untergruppe B einer endlich erzeugten abelschen Gruppe A ist wieder endlich erzeugt.*

Beweis. Das folgt sofort aus der Tatsache, daß $\mathbb{Z}$ ein noetherscher Ring ist, soll hier aber direkt bewiesen werden.

Sei $x_1, \dots, x_n$ ein endliches Erzeugendensystem für A. Wir setzen $A_i = \langle x_1, \dots, x_i \rangle$ und erhalten eine aufsteigende Firltrierung durch Untergruppen $A_i \subseteq A$. Der Quotienten A_i/A_{i-1} wird vom Bild von x_i erzeugt und ist daher zyklisch. Sei $B_i = B \cap A_i$. Dann ist

$$B_i/B_{i-1} \hookrightarrow A_i/A_{i-1}$$

als Untergruppe einer zyklischen Gruppe ebenso zyklisch. Sei $y_i \in B_i$ ein Urbild eines Erzeugers von B_i/B_{i-1}. Dann folgt per Induktion nach i daß $y_1, \dots, y_i$ die Gruppe B_i erzeugen. Da $B_n = B$ folgt die Behauptung. $\square$

Nun zu Untergruppen von freien abelschen Gruppen.

Satz 397. *Jede Untergruppe B einer freien abelschen Gruppe A ist wieder frei. Es gilt*

$$\mathrm{rg}(B) \le \mathrm{rg}(A).$$

Genauer gibt es eine Basis $(x_i)_{i \in I}$ von A und $d_i \in \mathbb{N}_0$ für alle $i \in I$, so daß

$$(d_i x_i)_{i \in I}$$

eine Basis von B ist.

Wir zeigen Satz 397 nur für freie abelsche Gruppen von endlichem Rang.

Beweis von Satz 397. Nach Lemma 396 ist B endlich erzeugt, etwa durch $b_1, \dots, b_m$. Nach Wahl einer Basis von A, also einem Isomorphismus $A \simeq \mathbb{Z}^n$ kann man die b_i als Spalten einer Matrix M auffassen, die eine Abbidlung durch Matrixmultiplikation

$$M \cdot : \mathbb{Z}^m \to \mathbb{Z}^n$$

liefert. Das Bild ist als Erzeugnis der Spalten dann gerade B, bzw. das Bild von B in $A \simeq \mathbb{Z}^n$. Ein Wechsel der Basis von A entspricht der Multiplikation SM mit einem $S \in \mathrm{GL}_n(\mathbb{Z})$. Analog entspricht MT mit $T \in \mathrm{GL}_n(\mathbb{Z})$ einem Wechsel der Erzeuger $b_1, \dots, b_m$ (allerdings keinem beliebigen, denn die Anzahl bleibt ja gleich, aber das tut nichts zur Sache). Nach dem Elementarteilersatz 404 angewandt auf den Hauptidealring $R = \mathbb{Z}$ findet man nun S und T, so daß

$$SMT$$

Diagonalgestalt hat. Damit hat man die gesuchte Basis gefunden und der Rest folgt sofort. $\square$

C.1.3. *Größter gemeinsamer Teiler und Matrixmultiplikation.* Bevor wir den Elemetarteilersatz beweisen können, brauchen wir ein paar Vorarbeiten.

Definition 398. Sei A eine Matrix mit Einträgen aus einem Hauptidealring. Es bezeichne $\mathrm{ggT}(A)$ den größten gemeinsamen Teiler der Einträge der Matrix A.

Lemma 399. *Sei R ein Hauptidealring und $A \in \mathrm{M}_{m \times n}(R)$, $S \in \mathrm{M}_m(R)$ und $T \in \mathrm{M}_n(R)$. Dann gilt:*

(1) $\mathrm{ggT}(A)$ *teilt* $\mathrm{ggT}(SA)$ *und* $\mathrm{ggT}(AT)$.
(2) *Sind S, T invertierbar, so gilt* $\mathrm{ggT}(A) = \mathrm{ggT}(SA) = \mathrm{ggT}(AT)$.

Beweis. (1) Die Einträge von SA und AT sind Linearkombinationen der Einträge von A, daher Vielfache von $\mathrm{ggT}(A)$.

(2) Wir wenden (1) auf Multiplikation mit S und mit S^{-1} an. Es folgt

$$\mathrm{ggT}(A) \mid \mathrm{ggT}(SA) \mid \mathrm{ggT}(S^{-1}SA) = \mathrm{ggT}(A)$$

und daher die gewünschte Gleichheit $\mathrm{ggT}(A) = \mathrm{ggT}(SA)$. Die Aussage für AT folgt analog. $\square$

Lemma 400. *(1) Sei $w = (a_1, \ldots, a_m) \in R^m$ ein Zeilenvektor und $d = \mathrm{ggT}(w)$. Dann gibt es eine invertierbare Matrix $T \in \mathrm{GL}_m(R)$ mit $wT = (d, 0 \ldots, 0)$.*

(2) Analog gibt es für einen Spaltenvektor v der Länge n eine invertierbare Matrix $S \in \mathrm{GL}_n(R)$ so, daß in Sv die erste Zeile d ist und alle anderen Einträge verschwinden.

Beweis. Offenbar sind die Aussagen (1) und (2) durch Transponieren zueinander äquivalent. Daher beweisen wir nur (2). Wir verwenden Induktion nach der Größe n des Vektors. Für $n = 1$ ist nichts zu zeigen. Des weiteren ist die Behauptung des Lemmas für Vektoren v und Bv äquivalent, wenn B eine invertierbare Matrix ist, denn nach Lemma 399 gilt $\mathrm{ggT}(v) = \mathrm{ggT}(Bv)$.

Sei $v = \binom{a_1}{v'}$ mit einem Spaltenvektor v' der Länge $n-1$. Per Induktionsvoraussetzung gibt es eine Matrix $S' \in \mathrm{GL}_{n-1}(R)$ so daß $S'v'$ nur noch einen nichtverschwindenden Eintrag d' in der ersten Zeile hat. Dann ist die Blockmatrix

$$B = \begin{pmatrix} 1 & 0 \\ 0 & S' \end{pmatrix}$$

invertierbar, und es hat Bv nur noch nichtverschwindende Einträge in den ersten beiden Zeilen. Jetzt reicht es offenbar, den Fall $n = 2$ zu beherrschen.

Sei $n = 2$ und $v = \binom{a_1}{a_2}$. Nach dem Satz von Bézout gibt es in R eine Relation

$$x_1 a_1 + x_2 a_2 = d.$$

Damit erfüllt die Matrix

$$S = \begin{pmatrix} x_1 & x_2 \\ -a_2/d & a_1/d \end{pmatrix}$$

das Gewünschte: $Sv = \binom{d}{0}$. Es ist $d = \mathrm{ggT}(Sv) = \mathrm{ggT}(v)$ nach Lemma 399. $\square$

C.1.4. *Fitting-Ideale.* Die Eindeutigkeitsaussage im Elementarteilersatz folgt schnell aus der Theorie der Fittingideale, von der wir nur das nötigste beweisen.

Definition 401. Sei $A \in \mathrm{M}_{n\times m}(R)$ eine Matrix mit Einträgen in einem beliebigen kommutativen Ring R. Für $\nu \geq 0$ ist das **ν-te Fittingideal** von A dasjenige Ideal

$$\mathrm{Fitt}_\nu(A) \subseteq R,$$

welches von den Minoren der Größe $n - \nu$ der Matrix A, also den Determinanten von quadratischen $(n-\nu) \times (n-\nu)$-Untermatrizen von A, erzeugt wird. Wir setzten

$$\mathrm{Fitt}_n(A) = R$$

(Minoren der Größe 0 sind per Konvention alle 1), und

$$\mathrm{Fitt}_\nu(A) = (0),$$

sobald $n - \nu > \min\{n, m\}$ und damit keine quadratischen Untermatrizen der Größe $n - \nu$ in A Platz finden.

Bemerkung 402. (1) Da ein $(r+1)$-Minor eine Linearkombination von r-Minoren ist, bilden die Fittingideale einer Matrix $A \in \mathrm{M}_{n\times m}(R)$ eine aufsteigende Kette von Idealen

$$(0) \subseteq \mathrm{Fitt}_0(A) \subseteq \mathrm{Fitt}_1(A) \subseteq \ldots \subseteq \mathrm{Fitt}_{n-1}(A) \subseteq \mathrm{Fitt}_n(A) = R$$

von R. Dabei ist $\mathrm{Fitt}_{n-1}(A)$ gerade das von den Einträgen von A erzeugte Ideal.

(2) Die Nummerierung der Fittingideale ist auf den ersten Blick merkwürdig, hat aber einen tieferen geometrischen Sinn. Es geht um die Struktur des Quotientenmodules

$$M = R^n / AR^m.$$

Der Quotienten $R \twoheadrightarrow R/\mathrm{Fitt}_\nu(A)$ beschreibt den Ort in $\mathrm{Spec}(R)$, an dem M einen Rang $> \nu$ hat.

Lemma 403 (Fitting's Lemma). *Sei R ein Ring, $A \in \mathrm{M}_{n\times m}(R)$ und $S \in \mathrm{GL}_n(R)$ und $T \in \mathrm{GL}_m(R)$. Dann gilt*

$$\mathrm{Fitt}_\nu(A) = \mathrm{Fitt}_\nu(SA) = \mathrm{Fitt}_\nu(AT).$$

Beweis. Man hat nur

$$\mathrm{Fitt}_\nu(SA) \subseteq \mathrm{Fitt}_\nu(A)$$

nachzuweisen, denn dann gilt

$$\mathrm{Fitt}_\nu(A) = \mathrm{Fitt}_\nu(S^{-1}SA) \subseteq \mathrm{Fitt}_\nu(SA) \subseteq \mathrm{Fitt}_\nu(A).$$

Die Aussage für AT erhält man analog durch Transposition.

Berechnen wir den Minor derjenigen Untermatrix $(SA)_{IJ}$ von SA deren Zeilenindizes nur $i \in I$ und Spaltenindizes nur $j \in J$ durchlaufen ($\#I = \#J$). Wir stellen zunächst fest, daß die Zeilenvektoren von $(SA)_{IJ}$ Linearkombinationen der auf den Indexbereich $j \in J$ eingeschränkten Zeilenvektoren von A (alle Zeilen, nicht nur $i \in I$) sind. Dies folgt unmittelbar aus der Definition der Matrizenmultiplikation. Die Koeffizienten der Linearkombination stehen in der entsprechenden Zeile von S. Sodann berechnen wir die Determinate von $(SA)_{IJ}$ vermöge der Multilinearität in jeder Zeile als eine Linearkombination von Determinaten von auf den Bereich $j \in J$ eingeschränkten Zeilenvektoren von A, also entsprechende Minoren von A. Terme, in denen eine Zeile doppelt auftritt, verschwinden. Damit liegt $\det(SA)_{IJ}$ im entsprechenden Fittingideal von A. □

C.1.5. *Der Elementarteilersatz.*

Satz 404 (Elementarteilersatz). *Sei R ein Hauptidealring und $A \in \mathrm{M}_{n\times m}(R)$.*

Dann gibt es invertierbare Matrizen $S \in \mathrm{GL}_n(R)$ und $T \in \mathrm{GL}_m(R)$, so daß

$$SAT = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_s & \\ & & & \\ \end{pmatrix}$$

mit $s \leq \min\{n, m\}$ und sich steigend teilenden Elementen $d_1|d_2|\ldots|d_s$ des Rings R. (Alle restlichen Einträge der Matrix sind 0.)

Die natürliche Zahl s und die d_i bis auf Assoziertheit sind eindeutig bestimmt, d.h., sie hängen nicht von den Matrizen S, T ab.

Beweis. Wir werden versuchen, durch Multiplikation mit invertierbaren Matrizen von links und rechts die Matrix A auf die Blockform

$$\left(\begin{array}{c|ccc} d & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{C.1}$$

zu bringen, wobei $d = \mathrm{ggT}(A)$ gelten soll. Somit teilt d jeden Eintrag der Matrix A'. Wir schließen dann per Induktion nach der Größe $n+m$ der Matrix indem wir den Induktionsschritt auf die Matrix $\frac{1}{d}A' \in \mathrm{M}_{(n-1)\times(m-1)}(R)$ anwenden. Dabei ist wichtig, daß durch Multiplikation mit invertierbaren Matrizen von links und rechts sich der ggT nicht ändert, siehe Lemma 399. nichts ändert.

Der Induktionsanfang ($n = 1$ oder $m = 1$) wurde bereits in Lemma 400 bewiesen. Zum Induktionsschritt wenden wir Lemma 400 auf die erste Spalte von $A_0 = A$ an. Wir finden ein

$S \in \mathrm{GL}_m(R)$, so daß

$$A_1 = SA_0 = \left(\begin{array}{c|ccc} a_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & A_1' & \\ 0 & & & \end{array}\right) \tag{C.2}$$

Dabei ist a_1 als ggT der ersten Spalte ein Teiler des Eintrags von A_0 an derselben Stelle. Nun wenden wir Lemma 400 auf die erste Zeile von A_1 an, und finden $T \in \mathrm{GL}_n(R)$, so daß

$$A_2 = A_1 T = \left(\begin{array}{c|ccc} a_2 & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & A_2' & \\ * & & & \end{array}\right) \tag{C.3}$$

Diesmal ist a_2 der ggT der ersten Zeile und damit ein Teiler von a_1. Allerdings kontrollieren wir nicht, ob die Nullen in der ersten Spalte aus dem ersten Schritt erhalten bleiben.

Wir iterieren diese beiden Schritte alternierend und erhalten eine Folge von Matrizen A_i mit erstem Eintrag a_i oben links und

$$a_{i+1} \mid a_i.$$

Da in einem Hauptidealring kein Element beliebig oft Teiler mit weniger Primfaktoren haben kann, muß nach einer Weile a_{i+1} sich nur noch um eine Einheit von a_i unterscheiden. Das bedeutet, daß dann a_i schon der entsprechende ggT ist. In diesem Moment können wir die Nullen in der ersten Spalte und ersten Zeile durch elementare Spalten- (bzw. Zeilen-)transformationen erhalten, nämlich durch Addition eines Vielfachen der ersten Spalte (bzw. Zeile), die dann die bereits vorhandenen Nullen nicht wieder zerstören. Wir erhälten so eine Matrix der Gestalt

$$\left(\begin{array}{c|ccc} \delta & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{C.4}$$

Damit sind wir fast am Ziel. Wir kontrollieren nur noch nicht, daß δ alle Einträge von A' teilt. Dieses Problem ignorieren wir zunächst und schließen per Induktion nach $n+m$ auf eine Diagonalgestalt

$$\begin{pmatrix} \delta_1 & & & \\ & \ddots & & \\ & & \delta_s & \\ & & & \\ & & & \end{pmatrix} \tag{C.5}$$

Nun gehen wir einen Schritt rückwärts und Addieren per Zeilenoperation die $2 \le i \le s$-te Zeile zur ersten Zeile dazu. In der Matrix

$$\begin{pmatrix} \delta_1 & \ldots & \delta_s & \\ & \ddots & & \\ & & \delta_s & \\ & & & \\ & & & \end{pmatrix} \tag{C.6}$$

ist nun der ggT der ersten Zeile gleich $\mathrm{ggT}(A)$. Starten wir mit dieser Matrix das Verfahren erneut, wird die in (C.4) erreichte Matrix sogar die Eigenschaft haben, daß $\delta = \mathrm{ggT}(A)$ ein Teiler der Matrix A' ist, also das Ziel (C.1) erreicht ist. Wieder per Induktion nach $n+m$ folgt die Existenz der gewünschten Diagonalform.

Jetzt kümmern wir uns um die Eindeutigkeit der Elemente

$$d_1 \mid d_2 \mid \ldots \mid d_s$$

und der Zahl s. Nach Lemma 403 sind die Fittingideale von A und der erreichten Diagonalform SAT die gleichen. Wir berechnen mittels der diagonalen Form (in der nur sehr wenige Minoren von 0 verschieden sind!)

$$\mathrm{Fitt}_\nu(A) = \begin{cases} (\prod_{i=1}^{n-\nu} d_i) & \text{falls } n-\nu \leq s, \\ (0) & \text{falls } n-\nu > s. \end{cases}$$

Da dies Invarianten der Matrix A und nicht nur der diagonalen Form SAT sind, schließen wir, daß sich s und die Elemente d_i bis auf Assoziiertheit eindeutig aus den Fittingidealen von A und damit der Matrix A rekonstruieren lassen. Dies zeigt die Eindeutigkeit der Parameter der diagonalen Form. □

C.1.6. *Der Struktursatz.*

Theorem 405 (Struktursatz über endlich erzeugte abelsche Gruppen)**.** *Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{N}_0$ und $1 < d_1, \ldots d_s \in \mathbb{N}$ mit*

$$d_1 \mid d_2 \mid \ldots \mid d_s$$

und einen Isomorphismus

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

Die Zahlen $r, s \in \mathbb{N}_0$ und d_i für $1 \leq i \leq s$ sind eindeutig.

Beweis. Wir wählen ein Erzeugendensystem $x_1, \ldots, x_n$ von A minimaler Länge. Dazu gehört ein surjektiver Homomorphismus $\varphi : \mathbb{Z}^n \twoheadrightarrow A$, der durch $e_i \mapsto x_i$ definiert wird. Der Kern $B = \ker(\varphi)$ ist nach Lemma 396 endlich erzeugt und damit Bild eines Homomorphismus

$$M : \mathbb{Z}^m \to \mathbb{Z}^n$$

mittels Matrixmultiplikation mit $M \in \mathrm{M}_{n\times m}(\mathbb{Z})$. Wir wenden den Elementarteilersatz, Satz 404, auf die Matrix M an. Nach einem entsprechenden Basiswechsel von $\mathbb{Z}^n$ (das wechselt das Erzeugendensystem für A) und $\mathbb{Z}^m$ dürfen wir annehmen, daß M die diagonale Form aus Satz 404 hat. Da das ursprüngliche Erzeugendensystem minimale Länge hat, darf kein $d_i = \pm 1$ eine Einheit sein, denn sonst könnte man nach Basiswechsel und damit Wechsel des Erzeugendensystems das entsprechen Element weglassen und erhielte ein kürzeres Erzeugendensystem. Wir setzen noch $d_i = 0$ für alle $i > s$. Dann ist mit $r = n - s$

$$A \simeq \mathbb{Z}^n/M\mathbb{Z}^m \simeq \mathbb{Z}^n/\bigoplus_{i=1}^{n} d_i\mathbb{Z} \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

Es bleibt, die Eindeutigkeitsaussage zu zeigen. Leider folgt diese nicht direkt aus der Eindeutigkeit im Elementarteilersatz, da wir nicht wissen, ob sich durch grundsätzlichen Wechsel des anfänglichen Erzeugendensystems nicht eine gravierende Änderung ergeben kann. Wir haben letztlich die Theorie der Fitingideale nicht ausreichend betrieben.

Stattdessen berechnen wir die folgenden Invarianten von A für jedePrimzahl p und $t \geq 0$:

$$N_p(t) := \log_p(\#A/p^tA) = rt + \sum_{i=1}^{s} \log_p(d_i, p^t).$$

Dann gilt weiter

$$\Delta N_p(t) = N_p(t) - N_p(t-1) = r + \#\{i\ ;\ 1 \leq i \leq s \text{ und } p^t \mid d_i\}.$$

Aus $\Delta N_p(t) = r$ für $t \gg 0$ lesen wir r ab. Aus den Sprüngen der Funktion $\Delta N_p(t) - r$ lesen wir ab, wieviele der d_i genau durch p^t teilbar sind. Da die d_i sich gegenseitig teilen, legt das die p-Potenzfaktoren in der Primfaktorzerlegung der d_i fest. Das s ergibt sich anschließend aus der Anzahl der so konstruierten d_i, oder genauer als

$$s = \max_p \{\Delta N_p(1) - r\}.$$

Dies zeigt die behauptete Eindeutigkeit. $\square$

C.2. **Pontrjagin–Dualität.**

C.2.1. *Gruppen von Homomorphismen.* Für eine beliebige Gruppe G und eine abelsche Gruppe A ist

$$\mathrm{Hom}(G, A) = \{\varphi : G \to A \ ; \ \phi \text{ ist Gruppenhomomorphismus}\}$$

eine abelsche Gruppe durch werteweise Addition:

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g).$$

Dabei muß A abelsch sein, damit die so definierte Abbildung $\varphi + \psi$ wieder ein Gruppenhomomorphismus ist.

Bemerkung 406. Zu einem Homomorphismus $f : A \to B$ ist die Abbildung

$$f\circ : \mathrm{Hom}(G, A) \to \mathrm{Hom}(G, B)$$

definiert durch $\varphi \mapsto f \circ \varphi$ ein Gruppenhomomorphismus. Zu einem Homomorphismus $f : H \to G$ ist die Abbildung

$$\circ f : \mathrm{Hom}(G, A) \to \mathrm{Hom}(H, A)$$

definiert durch $\varphi \mapsto \varphi \circ f$ ein Gruppenhomomorphismus.

Bemerkung 407. Die universelle Eigenschaft der Abelisierung $\pi : G \to G^{\mathrm{ab}}$ zeigt, daß

$$\circ\pi : \mathrm{Hom}(G^{\mathrm{ab}}, A) \xrightarrow{\sim} \mathrm{Hom}(G, A)$$

bijektiv, und damit ein Isomorphismus von Gruppen.

Proposition 408. *Es seien A, B und T abelsche Gruppen. Dann sind die Abbildungen*

$$\begin{aligned} \mathrm{Hom}(A \oplus B, T) &\to \mathrm{Hom}(A, T) \oplus \mathrm{Hom}(B, T) \\ \varphi &\mapsto (\varphi \circ i_A, \varphi \circ i_B) \end{aligned}$$

und

$$\begin{aligned} \mathrm{Hom}(T, A \oplus B) &\to \mathrm{Hom}(T, A) \oplus \mathrm{Hom}(T, B) \\ \varphi &\mapsto (p_A \circ \varphi, p_B \circ \varphi) \end{aligned}$$

Isomorphismen von Gruppen. Dabei sind $i_A : A \to A \oplus B$ und $i_B : B \to A \oplus B$ die Inklusionen der Summanden, und die Abbildungen $p_A : A \oplus B \to A$ und $p_B : A \oplus B \to B$ sind die Projektionen.

Beweis. Die Abbildungen sind bijektiv als Konsequenz der definierenden universellen Eigenschaft der Summe zweier abelscher Gruppen als Summe bzw. als Produkt. Außerdem sind die Abbildungen Gruppenhomomorphismen und somit Isomorphismen von Gruppen. $\square$

C.2.2. *Paarungen von abelschen Gruppen.* Eine **Paarung** abelscher Gruppen A, B mit Werten in D ist eine biadditive Abbildung

$$f : A \times B \to D$$

das heißt für alle $a, a' \in A$ und $b, b' \in B$ gilt

$$f(a + a', b) = f(a, b) + f(a', b)$$
$$f(a, b + b') = f(a, b) + f(a, b').$$

Zu einer solchen Paarung gehören *adjungierte* Gruppenhomomorphismen

$$A \to \mathrm{Hom}(B, D)$$

definiert durch $a \mapsto \big(b \mapsto f(a, b)\big)$ und

$$B \to \mathrm{Hom}(A, D)$$

definiert durch $b \mapsto \big(a \mapsto f(a, b)\big)$.

Die Paarung f ist **rechts- (bzw. links-) nichtausgeartet**, wenn zu jedem $0 \neq a \in A$ (bzw. jedem $0 \neq b \in B$) ein $b \in B$ (bzw. ein $a \in A$) existiert mit

$$f(a, b) \neq 0.$$

Das ist offenbar äquivalent dazu, daß die adjungierte Abbildung $A \to \mathrm{Hom}(B, D)$ (bzw. $B \to \mathrm{Hom}(A, D)$) injektiv sind. Die Paarung heißt **nichtausgeartet**, wenn sie sowohl rechts- als auch links-nichtausgeartet ist. Anstelle von rechts-nichtausgeartet (bzw. links-nichtausgeartet) kann man auch in A (bzw. in B) nichtausgeartet sagen.

C.2.3. *Die Pontrjagin–duale Gruppe.* Für Pontrjagindualität ist die Gruppe $\mathbb{Q}/\mathbb{Z}$ nötig. Die Untergruppe $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ der Restklassen rationaler Zahlen, deren Nenner multiplikativ durch n beschränkt ist, eine zyklische Gruppe der Ordnung n mit einem ausgezeichneten Erzeuger $\frac{1}{n}$. Weiter besteht die Untergruppe $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ genau aus den Elemente, deren Ordnung ein Teiler von n ist. Es gilt

$$\mathbb{Q}/\mathbb{Z} = \bigcup_{n \geq 1} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Für eine abelsche Gruppe A bezeichnen wir

$$A^\vee := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

als die **Pontrjagin-duale Gruppe** zu A. Zu einem Homomorphismus $f : A \to B$ gehört der duale Homomrphismus

$$f^\vee = \circ f : B^\vee \to A^\vee.$$

Beispiel 409. (1) $\mathbb{Z}^\vee = \mathbb{Q}/\mathbb{Z}$ durch Auswertung von $\varphi : \mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ bei $1 \in \mathbb{Z}$.

(2) Es gilt $(\mathbb{Z}/n\mathbb{Z})^\vee = \mathbb{Z}/n\mathbb{Z}$, in dem wir $a \in \mathbb{Z}/n\mathbb{Z}$ den Homomorphimus

$$\varphi_a(x) = \frac{ax}{n} \in \mathbb{Q}/\mathbb{Z}$$

zuordnen. Der Isomorphismus ist kanonisch, da $\mathbb{Z}/n\mathbb{Z}$ und $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ einen kanonischen Erzeuger haben, und damit auch die duale Gruppe $(\mathbb{Z}/n\mathbb{Z})^\vee$ einen kanonischen Erzeuger φ_1 hat.

(3) Sei μ_n die Gruppe der n-ten Einheitswurzeln in einem algebraisch abgeschlossenen Körper dessen Charakteristik kein Teiler von n ist. Dann ist wohl

$$\mu_n^\vee \simeq (\mathbb{Z}/n\mathbb{Z})^\vee = \mathbb{Z}/n\mathbb{Z} \simeq \mu_n,$$

aber der Isomorphismus ist nicht kanonisch, denn er hängt zweimal (in sich nicht aufhebender Weise) von der Wahl einer primitiven n-ten Einheitswurzel ab.

Satz 410. *Sei A eine endliche abelsche Gruppe. Dann ist*

$$A^\vee \simeq A$$

und insbesondere $\#A = \#A^\vee$.

Beweis. Als Spezialfall von Proposition 408 haben wir für abelsche Gruppen A und B

$$(A \oplus B)^\vee = A^\vee \oplus B^\vee.$$

Da die Gruppenordnung multiplikativ bezüglich direkter Summen ist:

$$\#(A \oplus B) = \#A \cdot \#B$$

reicht es demnach die Aussage des Satzes für direkte Summanden einer Darstellung von A als direkte Summe zu beweisen.

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen, Theorem 405, ist jede solche eine direkte Summe von endlichen zyklischen Gruppen. Somit habe wir uns auf den Fall $A = \mathbb{Z}/n\mathbb{Z}$ reduziert. Diesen haben wir uns bereits als Beispiel angesehen. □

Satz 411. *Sei*

$$0 \to A' \xrightarrow{i} A \xrightarrow{p} A'' \to 0$$

eine kurze exakte Sequenz endlicher abelscher Gruppen. Dann ist die duale Sequenz

$$0 \to (A'')^\vee \xrightarrow{p^\vee} A^\vee \xrightarrow{i^\vee} (A')^\vee \to 0$$

ebenfalls exakt.

Beweis. Wir bestimmen den Kern von $i^\vee$ nach der universellen Eigenschaft der Quotientenabbildung $p : A \to A/A' \simeq A''$ als

$$\ker(i^\vee) = \{\varphi \in A^\vee \ ; \ \varphi \circ i = 0\} = \{\varphi \in A^\vee \ ; \ \varphi = \psi \circ p \text{ für ein } \psi \in (A'')^\vee\}.$$

Da die fraglichen ψ zudem eindeutig sind, ist $p^\vee$ injektiv und sein Bild mit $\ker(i^\vee)$ zu identifizieren. Damit fehlt nur noch zu zeigen, daß $p^\vee$ surjektiv ist. In jedem Fall wissen wir bereits, daß die von $p^\vee$ induzierte Abbildung

$$A^\vee/(A')^\vee \to (A'')^\vee$$

injektiv ist, und zu zeigen ist: sogar bijektiv. Das können wir nun mittels Satz 410 und den Satz von Lagrange durch Zählen erledigen:

$$\#(A'')^\vee = \#A'' = \frac{\#A}{\#A'} = \frac{\#A^\vee}{\#(A')^\vee} = \#(A^\vee/(A')^\vee)$$

und das war zu zeigen. □

Bemerkung 412. Die Aussage von Satz 411 gilt allgemeiner auch für nicht notwendig endliche abelsche Gruppen. Der Beweis bis auf die Surjektivität von $i^\vee$ ist der gleiche. Letzteres zeigt gerade Aufgabe C.1

C.2.4. *Dualität.* Wir betrachten nun speziell Paarungen mit Werten in der Gruppe $D = \mathbb{Q}/\mathbb{Z}$.

Satz 413 (Perfekte Paarung)**.** *Sei $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ eine Paarung endlicher abelscher Gruppen. Dann sind äquivalent*

(a) f ist nichtausgeartet.
(b) Die adjungierte Abbildung $A \to B^\vee$ ist ein Isomorphismus.
(c) Die adjungierte Abbildugn $B \to A^\vee$ ist ein Isomorphsimus.

*Wenn diese äquivalenten Bedingungen zutreffen, so nennen wir die Paarung eine **perfekte** Paarung.*

Beweis. Wenn die Paarung nichtausgeartet ist, dann sind die adjungierten Abbildungen injektiv und somit (mit Satz 410)

$$\#A \leq \#B^\vee = \#B \leq \#A^\vee = \#A.$$

Es herrscht daher Gleichheit und die adjungierten Abbildungen sind sogar bijektiv. Dies zeigt (a) $\Longrightarrow$ (b) und (c).

Für die ausstehenden Richtungen reicht per Symmetrie die Aussage (b) $\Longrightarrow$ (a). Da $A \to B^\vee$ injektiv ist, ist f in A nichtausgeartet. Wir müssen nur noch zeigen, daß f auch in B nichtausgeartet ist. Sei dazu $0 \neq b \in B$. Dann ist $U = \langle b \rangle \subseteq A$ eine zyklische Untergruppe, sagen wir der Ordnung $n > 1$. Dann gibt es ein nichttriviales

$$\varphi_0 : U \to \mathbb{Q}/\mathbb{Z}$$

mit $\varphi_0(b) \neq 0$. Nach Satz 411 ist die durch Einschränkung induzierte Abbildung

$$A^\vee \twoheadrightarrow U^\vee$$

surjektiv. Wir können daher φ_0 zu einem Homomorphismus $\varphi : A \to \mathbb{Q}/\mathbb{Z}$ fortsetzen. Da $A \to B^\vee$ surjektiv ist, gibt es ein $a \in A$ mit $\varphi = f(a, -)$, und für dieses gitl

$$f(a, b) = \varphi(b) = \varphi_0(b) \neq 0.$$

Damit ist f auch in B nichtausgeartet. □

Bemerkung 414. Wenn in einer Paarung $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ abelscher Gruppen a priori nur A als endlich bekannt ist, wohl aber f im Argument B, also rechts-nichtausgeartet ist, dann folgt automatisch, daß auch B endlich ist. Schließlich ist dann

$$B \to A^\vee$$

injektiv und $A^\vee$ ebenso endlich.

Korollar 415. *Sei A eine endliche Gruppe. Dann ist die natürliche Abbildung*

$$\begin{aligned} A &\to (A^\vee)^\vee \\ a &\mapsto \big(\varphi \mapsto \varphi(a)\big) \end{aligned}$$

ein Gruppenisomorphismus.

Beweis. Dies ist eine der adjungierten Abbildungen zur Auswertungspaarung

$$\begin{aligned} A \times A^\vee &\to \mathbb{Q}/\mathbb{Z} \\ (a, \varphi) &\mapsto \varphi(a). \end{aligned}$$

Diese Paarung ist perfekt nach Satz 413, da die andere adjungierte Abbildung die Identität auf $A^\vee$ ist. □

Sei $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ eine Paarung. Zu einer Untergruppe $U \subseteq A$ definieren wir den **Annihilator** von U (oder die zu U **orthogonale Untergruppe** als die Untergruppe von B

$$U^\perp = \{b \in B \ ; \ f(u, b) = 0 \text{ für alle } u \in U\}.$$

Wir verwenden die gleiche Terminologie und Notation, wenn A und B die Rollen tauschen, da Mißverständnisse ausgeschlossen sind.

Satz 416. *Sei $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ eine perfekte Paarung endlicher abelscher Gruppen. Dann definiert $U \mapsto U^\perp$ eine Bijektion zwischen den Untergruppen von A und den Untergruppen von B. Dabei gilt*

(1) $(U^\perp)^\perp = U$.
(2) Die Paarung f induziert einen Isomorphismus $A/U \simeq (U^\perp)^\vee$ und $U^\perp \simeq (A/U)^\vee$.
(3) Die Paarung f induziert einen Isomorphismus $U \simeq (B/U^\perp)^\vee$ und $B/U^\perp \simeq U^\vee$.

Beweis. Die Paarung f induziert eine Paarung

$$U \times B/U^{\perp} \to \mathbb{Q}/\mathbb{Z},$$

die per Definition in $B/U^{\perp}$ nichtausgeartet ist. Nichtausgeartet in U ist diese Paarung, weil ja schon f in A nichtausgeartet ist. Hieraus folgt bereits (3) nach Satz 413. Es folgt weiter

$$\#U \cdot \#U^{\perp} = \#(B/U^{\perp}) \cdot \#U^{\perp} = \#B = \#A.$$

Ein zweites Mal angewandt folgt

$$\#U = \#(U^{\perp})^{\perp}.$$

Da tautologisch bereits $U \subseteq (U^{\perp})^{\perp}$ folgt (1). Dann ist (2) eine Folge von (3) für $U^{\perp}$ andstelle von U. □

Bemerkung 417. Wenn bei einer perfekten Paarung $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ die Gruppen A und B einen Exponenten haben, der ein Teiler von n ist, dann nimmt die Paarung nur Werte in der Untergruppe $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$ an. Man kann daher die Paarung im Wertebreich auf diese Gruppe beschränlen: $f : A \times B \to \mathbb{Z}/n\mathbb{Z}$. Außerdem gilt dann

$$A^{\vee} = \mathrm{Hom}(A, \frac{1}{n}\mathbb{Z}/\mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Z}/n\mathbb{Z})$$

und genauso für $B^{\vee}$.

Wenn man nun eine perfekte Paarung $f : A \times B \to D$ hat in der D isomorph zu einer Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist, dann gelten die Sätze 413 und 416 sinngemäß weiter, nur hat man das Pontrjagin-dual $M^{\vee}$ für die verschiedensten Gruppen M durch

$$M^* := \mathrm{Hom}(M, D)$$

zu ersetzen. Diese Situation betrifft Kummertheorie vom Exponenten n mit $D = \mu_n$.

Übungsaufgaben zu §C

Übungsaufgabe C.1. Sei $i : A \subseteq B$ eine Inklusion abelscher Gruppen. Zeigen Sie, daß jeder Gruppenhomomorphismus $\varphi : A \to \mathbb{Q}/\mathbb{Z}$ sich zu einem Gruppenhomomorphismus $\psi : B \to \mathbb{Q}/\mathbb{Z}$ fortsetzt:

$$\psi \circ i = \varphi.$$

Tipp: Nutzen Sie das Lemma von Zorn.

Übungsaufgabe C.2. Sei $f : A \times B \to \mathbb{Q}/\mathbb{Z}$ eine Paarung abelscher Gruppen. Seien $\lambda : A \to B^{\vee}$ und $\rho : B \to A^{\vee}$ die adjungierten Abbildungen. Zeigen Sie, daß

$$\lambda^{\vee} = \rho \text{ und } \rho^{\vee} = \lambda$$

wenn man die kanonischen Isomorphismen $A = (A^{\vee})^{\vee}$ und $B = (B^{\vee})^{\vee}$ verwendet.

Jakob Stix, Institut für Mathematik, Johann Wolfgang Goethe–Universität Frankfurt, Robert-Mayer-Strasse 6–8, 60325 Frankfurt am Main, Germany

E-mail address: stix@math.uni-frankfurt.de