Skript zur Vorlesung

Algebra I

Wintersemester 2004/2005

Prof. Dr. Annette Werner

Inhaltsverzeichnis

Einf¨uhrung

Das Wort "Algebra" kommt aus dem Arabischen und bedeutet soviel wie das Rechnen mit Gleichungen. Dabei interessiert man sich in der Algebra vor allem für Polynomgleichungen, also etwa

$$3x^4 + x^2 + 2x + 3 = 0, \tag{1}$$

wobei x eine unbekannte Größe ist.
Man kann auch Gleichungen in mehreren unbekannten Größen betrachten, wie etwa

$$y^2 = x^3 + 2xy + 1.$$

Kommt in jedem Summanden nur eine unbekannte Größe mit dem Exponenten 1 vor, so nennt man die Gleichung linear, wie z.B.

$$3x + 5y + 1 = 0.$$

Systeme solcher linearen Gleichungen studiert man in der linearen Algebra.
In der Algebra interessieren wir uns für die Lösungen von Polynomgleichungen in einer unbekannten Größe x wie in (1).
Der größte Exponent, mit dem x in einer solchen Gleichung auftritt, heißt der Grad der Gleichung (oder auch der Grad des Polynoms auf der linken Seite).
Lineare Gleichungen, also Gleichungen vom Grad 1, zu lösen, stellt keine besondere Herausforderung dar:

$$x + a = 0 \Leftrightarrow x = -a.$$

Quadratische Gleichungen, also Gleichungen vom Grad 2, lernt man in der Schule zu lösen:

$$x^2 + ax + b = 0 \Leftrightarrow x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}.$$

Bei kubischen Gleichungen, also Gleichungen vom Grad 3, fängt es an, interessant zu werden. Schon in dem speziellen Fall

$$x^3 + ax = b \text{ mit } a, b > 0$$

bedurfte es einiger Anstrengungen, bis im 16. Jahrhundert eine Lösung

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

gefunden wurde.

Lange Zeit haben sich Mathematiker mit dem Finden solcher Lösungen für konkret gegebene Gleichungen beschäftigt. Wie die komplizierte Lösungsformel für die kubische Gleichung schon ahnen lässt, kommt man so nicht sehr weit. Über Gleichungen vom Grad ≥ 5 war lange sehr wenig bekannt. Noch zu Leibniz' Zeiten (1646 - 1716) war nicht einmal bekannt, ob Gleichungen 5. Grades überhaupt eine Lösung besitzen, die sich durch sukzessives Wurzelziehen erhalten lässt. Dies ist die Frage nach der "Auflösbarkeit algebraischer Gleichungen durch Radikale": Für welche Gleichungen lassen sich Lösungen durch wiederholte Anwendungen von Addition, Subtraktion Multiplikation, Division und Wurzelziehen aus den Koeffizienten gewinnen?
Der richtige Hebel zum Studium der algebraischen Gleichungen in einer unbekannten Größe wurde schließlich von Evariste Galois um 1830 angesetzt. Mit Hilfe der Galoistheorie kann man die Lösungen solcher Gleichungen mit Hilfe von Gruppentheorie beschreiben. Durch diese Theorie lassen sich viele Fragen, wie etwa die der Auflösbarkeit algebraischer Gleichungen durch Radikale, beantworten. Die Galoistheorie ist ein Beispiel dafür, dass ein mathematisches Problem oft erst mit einem abstrakten Zugang und den richtigen Begriffen zugänglich wird. Wir beginnen dementsprechend erst einmal mit etwas Theorie über Gruppen und Polynomringe.
Wir schreiben $\mathbb{Z}$ für die Menge der ganzen Zahlen, $\mathbb{N} = \{1, 2, \dots\}$ für die Menge der natürlichen Zahlen und setzen $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
Mit $\mathbb{Q}$, $\mathbb{R}$ bzw. $\mathbb{C}$ bezeichnen wir die rationalen, reellen bzw. komplexen Zahlen.
An manchen Stellen finden Sie ein (ÜA) für Übungsaufgabe. Dann sollten Sie sich unbedingt mit Papier und Bleistift von der Richtigkeit des Behaupteten überzeugen.

1 Gruppentheorie

Zuerst einige Definitionen:

Definition 1.1 Eine Menge M zusammen mit einer Abbildung

$$\cdot : M \times M \to M \text{ (Multiplikation)}$$

heißt **Monoid**, falls

i) $(ab)c = a(bc)$ für alle $a, b, c \in M$ ($\cdot$ ist assoziativ).

ii) Es gibt ein $e \in M$, so dass $ea = ae = a$ für alle $a \in M$ (neutrales Element)

In einem Monoid kann man also für endlich viele Elemente $a_1, \dots, a_n \in M$ das Produkt $\prod_{i=1}^{n} a_i = a_1 \cdots a_n$ definieren sowie für alle $a \in M$ und $n \in \mathbb{N}$ die n-te Potenz $a^n = \prod_{i=1}^{n} a$. Zusätzlich setzen wir $a^0 = e$.

Definition 1.2 Eine **Gruppe** ist ein Monoid G, so dass jedes Element von G ein Inverses besitzt. Mit anderen Worten, eine Gruppe ist eine Menge G zusammen mit einer Abbildung

$$\cdot : G \times G \to G,$$

die wir oft einfach als $ab = a \cdot b$ schreiben, so dass gilt

i) $\cdot$ ist assoziativ

ii) es gibt ein $e \in G$, so dass $ae = ea = a$ für alle $a \in G$

iii) zu jedem $a \in G$ gibt es ein $b \in G$, so dass $ab = e = ba$.

G heißt kommutativ oder abelsch, falls zusätzlich gilt

iv) $ab = ba$ für alle $a, b \in G$.

Bemerkung: Man kann in Definition 1.2 die Bedingungen ii) bzw. iii) durch die folgenden Bedingungen ii') bzw. iii') ersetzen:

ii') es gibt ein $e \in G$ mit $ea = a$ für alle $a \in G$ und

iii') zu jedem $a \in G$ existiert ein $b \in G$ mit $ba = e$

Man kann ferner zeigen, dass das neutrale Element e sowie das inverse Element zu jedem a eindeutig bestimmt sind. Letzteres bezeichnet man mit a^{-1}. Das neutrale Element bezeichnen wir meist einfach mit 1. Oft schreibt man die Verknüpfung in einer Gruppe in additiver Form, also $a + b$, $\sum_{i=1}^{n} a_i$ und na. Dann bezeichnet man das neutrale Element mit 0 und das inverse Element zu a mit $-a$.

Beispiel:

i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind abelsche Gruppen bezüglich der Addition.

ii) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ und $\mathbb{Q}_{>0} = \{x \in \mathbb{Q} : x > 0\}$ sowie $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ sind abelsche Gruppen bezüglich der Multiplikation.

iii) $\mathbb{N}$ und $\mathbb{Z}$ sind bezüglich der Multiplikation Monoide, aber keine Gruppen.

iv) Ist X eine Menge, so ist die Menge $S(X) = \{f : X \to X \text{ bijektiv}\}$ bezüglich der Hintereinanderausführung von Abbildungen eine Gruppe. Hat X mehr als zwei Elemente, so ist $S(X)$ nicht abelsch.

v) Ist X eine Menge und G eine Gruppe, so ist die Menge $G^X := \mathbf{Abb}(X, G)$ der Abbildungen von X nach G eine Gruppe, wenn man $(f \cdot g)(x) = f(x) \cdot g(x)$ setzt. Das neutrale Element ist die konstante Abbildung $f(x) = 1$.

vi) Ist I eine Indexmenge und $(G_i)_{i\in I}$ eine Familie von Gruppen. Dann wird $\prod_{i\in I} G_i$ zu einer Gruppe, wenn wir

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_i h_i)_{i\in I}$$

setzen.

$\prod_{i\in I} G_i$ heißt das Produkt der Gruppen G_i. Im Falle $G_i = G$ für alle i ist $\prod_{i\in I} G \simeq G^I$ aus v).

Definition 1.3 Es sei G ein Monoid. Eine Teilmenge $H \subset G$ heißt **Untermonoid**, falls gilt:

i) $e \in H$

ii) $a, b \in H \Rightarrow ab \in H$.

Ist G sogar eine Gruppe, so heißt $H \subset G$ **Untergruppe**, falls i), ii) und

iii) $a \in H \Rightarrow a^{-1} \in H$

gilt.

Beispiel:

i) In jeder Gruppe G ist G selbst sowie $\{e\}$ eine Untergruppe.

ii) Alle $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ für $m \in \mathbb{Z}$ sind Untergruppen von $\mathbb{Z}$.
$m\mathbb{Z}$ ist die "von m erzeugte zyklische Untergruppe von $\mathbb{Z}$".

Definition 1.4 Seien G, G' Monoide mit den neutralen Elementen e, e'. Eine Abbildung $\varphi : G \to G'$ heißt **Monoidhomomorphismus**, falls gilt:

i) $\varphi(e) = e'$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$.

Sind G und G' sogar Gruppen, so heißt φ auch **Gruppenhomomorphismus**.

Lemma 1.5 Eine Abbildung $\varphi : G \to G'$ zwischen Gruppen ist genau dann ein Gruppenhomomorphismus, wenn

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ für alle } a, b \in G$$

gilt.

Beweis : Wir müssen i) aus Definition 1.4 zeigen. Es gilt $\varphi(e) \overset{e \cdot e = e}{=} \varphi(ee) = \varphi(e)\varphi(e)$, nach Multiplikation mit $\varphi(e)^{-1}$ folgt $e' = \varphi(e)$. □

Lemma 1.6 Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, so gilt für alle $a \in G$:

$$\varphi(a^{-1}) = (\varphi(a))^{-1}.$$

Die Abbildung φ vertauscht also mit Inversenbildung.

Beweis : Es ist $\varphi(a)\varphi(a^{-1}) = \varphi(e) = e$. □

Weitere Begriffe:
Ein Gruppenhomomorphismus $\varphi : G \to G'$ heißt **Isomorphismus**, falls φ ein Inverses besitzt, d.h. falls es einen Gruppenhomomorphismus $\psi : G' \to G$ mit

$$\psi \circ \varphi = \mathrm{id}_G \text{ und } \varphi \circ \psi = \mathrm{id}_{G'}$$

gibt. Äquivalent dazu ist, dass der Homomorphismus φ bijektiv ist.
Ein injektiver Gruppenhomomorphismus heißt **Monomorphismus**, ein surjektiver Gruppenhomomorphismus heißt **Epimorphismus**.
Einen Homomorphismus $\varphi : G \to G$ von G nach G bezeichnet man auch als **Endomorphismus**, ein Isomorphismus $\varphi : G \to G$ von G nach G heißt **Automorphismus**.
Sind $\varphi : G \to G'$ und $\psi : G' \to G''$ Gruppenhomomorphismen, so ist auch die Verknüpfung $\psi \circ \varphi : G \to G''$ ein Gruppenhomomorphismus.
Zu jedem Gruppenhomomorphismus $\varphi : G \to G'$ gehört die Untergruppe

$$\mathbf{Kern}\,\varphi = \{x \in G : \varphi(x) = e'\}$$

von G, wobei e' das neutrale Element von G' ist, und die Untergruppe

$$\begin{aligned} \mathbf{Bild}\,\varphi &= \varphi(G) \\ &= \{y \in G' : \text{ es gibt ein } x \in G \text{ mit } \varphi(x) = y\} \end{aligned}$$

von G'.

Ein Gruppenhomomorphismus $\varphi : G \to G'$ ist injektiv genau dann, wenn

$$\text{Kern } \varphi = \{e\}$$

ist und surjektiv genau dann, wenn

$$\text{Bild } \varphi = G'$$

ist, wie man leicht nachrechnet (ÜA).

Definition 1.7 Es sei G eine Gruppe und $H \subset G$ eine Untergruppe. Eine **Linksnebenklasse** von H in G ist eine Teilmenge von G der Gestalt

$$aH := \{ab : b \in H\}.$$

Lemma 1.8 Für zwei Linksnebenklassen aH und bH von H in G sind äquivalent:

i) $aH = bH$

ii) $aH \cap bH \neq \emptyset$

iii) $a \in bH$

iv) $b^{-1}a \in H$

Beweis : i) $\Rightarrow$ ii) ist klar, da $a \cdot 1 \in aH$ ist und somit $aH \neq \emptyset$ gilt.
ii) $\Rightarrow$ iii): Es existiere ein $c \in aH \cap bH$, also $c = ah_1 = bh_2$ für $h_1, h_2 \in H$. Daraus folgt $a = bh_2h_1^{-1} \in bH$.
iii) $\Rightarrow$ iv) folgt durch Multiplikation mit b^{-1}
iv) $\Rightarrow$ i): Aus $b^{-1}a \in H$ folgt $a \in bH$, also $aH \subset bH$. Da H eine Untergruppe von G ist, enthält sie mit $b^{-1}a$ auch $(b^{-1}a)^{-1} = a^{-1}b$. Also folgt $b \in aH$ und somit $bH \subset aH$. Insgesamt also $aH = bH$. □

Satz 1.9 Zwischen je zwei Linksnebenklassen von H in G gibt es eine bijektive Abbildung. (Man sagt auch, sie sind gleichmächtig.)
Zwei Linksnebenklassen sind entweder disjunkt oder gleich. G ist disjunkte Vereinigung aller Linksnebenklassen.

Beweis : Für $a, b \in G$ vermittelt die Abbildung

$$\begin{aligned} \varphi : \quad & G \to G \\ & g \mapsto ba^{-1}g \end{aligned}$$

eine Bijektion $\varphi : aH \to bH$.
Die zweite Behauptung folgt aus Lemma 1.8.
Da jedes $a \in G$ in der Linksnebenklasse aH liegt, folgt auch die dritte Behauptung. □

Die Elemente einer Linksnebenklasse aH werden auch als **Vertreter** (oder **Repräsentanten**) dieser Linksnebenklasse bezeichnet. Für jeden Vertreter a' von aH (also jedes $a' \in aH$) gilt $aH = a'H$ nach Lemma 1.8.
Mit G/H bezeichnen wir die Menge der Linksnebenklassen von H in G.
Ganz analog kann man auch **Rechtsnebenklassen** Ha definieren, nämlich als Teilmengen von G der Form

$$Ha = \{ha : h \in H\}.$$

Die bijektive Abbildung $G \to G$, die g auf g^{-1} schickt, induziert eine Bijektion zwischen der Menge der Linksnebenklassen G/H und der Menge der Rechtsnebenklassen, die wir mit $H\backslash G$ bezeichnen (ÜA).

Definition 1.10 Die Anzahl der Elemente in G/H bezeichnen wir als

$$G : H,$$

und nennen diese Zahl den **Index von** H **in** G.
Mit $\mathrm{ord}(G)$ bezeichnen wir die **Ordnung** von G, d.h. die Anzahl der Elemente in G.

Korollar 1.11 (Satz von Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe von G. Dann gilt

$$\mathrm{ord}(G) = \mathrm{ord}(H) \cdot (G : H).$$

Beweis : Das folgt aus Satz 1.9. □

Definition 1.12 Eine Untergruppe $H \subset G$ heißt **Normalteiler** oder normale Untergruppe von G, wenn $aH = Ha$ für alle $a \in G$ gilt, d.h. wenn für jedes $a \in G$ die zugehörige Linksnebenklasse mit der Rechtsnebenklasse übereinstimmt.
Wir nennen in diesem Fall die Nebenklasse $aH = Ha$ auch Restklasse von a modulo H.

Bemerkung 1.13 i) H ist Normalteiler in G
$\Leftrightarrow$ für alle $a \in G$ ist $aHa^{-1} = H$
$\Leftrightarrow$ für alle $a \in G$ ist $aHa^{-1} \subset H$

ii) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler

iii) Der Kern eines Gruppenhomomorphismus $\varphi : G \to G'$ ist stets ein Normalteiler von G.

Beweis :

i) H Normalteiler, $\Rightarrow aHa^{-1} = H$ für alle $a \in G$, $\Rightarrow aHa^{-1} \subset H$ für alle $a \in G$.
Falls $aHa^{-1} \subset H$ für alle $a \in G$, so gilt auch $a^{-1}Ha \subset H$ für alle $a \in G$. Also ist $aH \subset Ha$ und $Ha \subset aH$, d.h. $aH = Ha$.

ii) klar

iii) Kern φ ist eine Untergruppe von G. Nach i) genügt es, für alle $a \in G$ zu zeigen: $a(\text{ Kern } \varphi)a^{-1} \subset \text{ Kern } \varphi$.
Sei also $x \in$ Kern φ. Dann ist

$$\begin{aligned} \varphi(axa^{-1}) &\overset{1.5}{=} \varphi(a)\varphi(x)\varphi(a^{-1}) \\ &\overset{1.6}{=} \varphi(a)\underbrace{\varphi(x)}_{=1}\varphi(a)^{-1} \\ &= 1, \end{aligned}$$

also $axa^{-1} \in$ Kern φ.

□

Nun wollen wir zeigen, dass es umgekehrt zu jedem Normalteiler $N \subset G$ einen Gruppenhomomorphismus $\varphi : G \to G'$ mit Kern $\varphi = N$ gibt.
Dazu definieren wir eine Gruppenstruktur auf der Menge G/N der Linksnebenklassen.

Lemma 1.14 Definiert man die Multiplikation von Teilmengen X und Y von G durch $XY = \{xy : x \in X, y \in Y\} \subset G$, so ist das Produkt der Linksnebenklassen aN und bN die Linksnebenklasse abN. Mit dieser Multiplikation wird G/N eine Gruppe mit neutralem Element $1N$ und inversem Element $a^{-1}N$ zu aN. Wir nennen sie die Faktor- oder Restklassengruppe von G modulo N.
Die Abbildung

$$\begin{aligned} \pi : \quad & G \to G/N, \\ & a \mapsto aN \end{aligned}$$

ist ein Gruppenhomomorphismus mit Kern $\pi = N$.

Beweis : $(aN)(bN) \overset{\text{Ass.}}{=} a(Nb)N \overset{N \text{ Normalteiler}}{=} a(bN)N \overset{\text{Ass.}}{=} (ab)(NN) \overset{N \text{ Untergr.}}{=} (ab)N.$

Die Gruppenaxiome aus Definition 1.12 lassen sich leicht nachrechnen (ÜA). Außerdem folgt sofort, dass π ein Gruppenhomomorphismus ist. Es ist

$$\begin{aligned} \text{Kern } (\pi) &= \{a \in G : \pi(a) = 1 \text{ in } G/N\} \\ &= \{a \in G : aN = 1N\} \\ &\overset{1.8}{=} N \end{aligned}$$

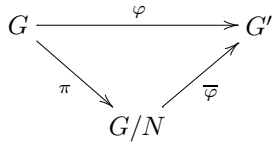
□

Wie viele algebraische Konstruktionen hat auch der Homomorphismus $\pi : G \to G/N$ eine universelle Eigenschaft:

Satz 1.15 (Homomorphiesatz) Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und $N \subset G$ ein Normalteiler mit $N \subset$ Kern φ.
Dann existiert genau ein Gruppenhomomorphismus

$$\overline{\varphi} : G/N \to G',$$

so dass



kommutiert. Mit anderen Worten, es ist $\varphi = \overline{\varphi} \circ \pi$.
Es gilt Bild$\overline{\varphi} =$ Bildφ, Kern$\overline{\varphi} = \pi$(Kernφ), Kern$\varphi = \pi^{-1}($ Kern $\overline{\varphi})$.
Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $N =$ Kern φ gilt.

Beweis : Für jede Abbildung $\overline{\varphi}$ mit $\varphi = \overline{\varphi} \circ \pi$ gilt $\overline{\varphi}(aN) = \varphi(a)$. Daher ist $\overline{\varphi}$ eindeutig bestimmt, falls es existiert. Wo liegt hier das Problem? Wir können doch einfach definieren $\overline{\varphi}(aN) = \varphi(a)$. Das macht aber nur dann Sinn, wenn aus $aN = bN$ schon $\varphi(a) = \varphi(b)$ folgt. Diese sogenannte Wohldefiniertheit von φ wollen wir jetzt zeigen. Aus $aN = bN$ folgt $b^{-1}aN = N$, also $b^{-1}a \in N \subset$ Kern φ. Somit gilt $1 = \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a)$, also in der Tat $\varphi(a) = \varphi(b)$.
$\overline{\varphi}$ ist also wohldefiniert. Aus $(aN)(bN) = (ab)N$ folgt, dass $\overline{\varphi}$ ein Homomorphismus ist. Offenbar ist Bild $(\overline{\varphi}) =$ Bild (φ) und Kern $\overline{\varphi} = \pi($ Kern $\varphi)$. Wir zeigen noch

$$\text{Kern } \varphi = \pi^{-1}(\text{ Kern } \overline{\varphi})$$

„$\subset$“ : Ist $\varphi(a) = 1$, so ist $\overline{\varphi}(\pi a) = \overline{\varphi}(aN) = 1$.

„$\supset$“ : Sei $a \in G$ ein Element mit $\pi(a) \in$ Kern $\overline{\varphi}$, d.h. $\overline{\varphi}(aN) = \overline{\varphi}(\pi a) = 1$, so folgt $\varphi(a) = 1$.

□

Korollar 1.16 Ist $\varphi : G \to G'$ ein Epimorphismus, so ist $G' \simeq G/$ Kern φ mit einem kanonischen („ausgezeichneten“) Isomorphismus.

Beweis : Nach Satz 1.15 existiert ein eindeutig bestimmter Homomorphismus $\overline{\varphi}$: $G/$ Kern $\varphi \to G'$ mit $\varphi = \overline{\varphi} \circ \pi$. Da Kern $\overline{\varphi} = \pi($ Kern $\varphi) = 1$ und Bild $\overline{\varphi} =$ Bild $\varphi = G'$ ist, ist $\overline{\varphi}$ bijektiv und somit ein Isomorphismus. □

Nun können wir die Isomorphinesätze für Gruppen beweisen.

Satz 1.17 (1. Isomorphiesatz) Es sei G eine Gruppe, $H \subset G$ eine Untergruppe und $N \subset G$ ein Normalteiler. Dann ist HN eine Untergruppe von G mit Normalteiler N, und $H \cap N$ ist ein Normalteiler von H. Die durch $H \subset HN$ induzierte Abbildung

$$H/H \cap N \to HN/N$$

ist ein Ismorphismus

Beweis : HN enthält 1 und ist abgeschlossen unter der Multiplikation, da für $h_1, h_2 \in H$ und $n_1, n_2 \in N$ gilt:

$$(h_1 n_1)(h_2 n_2) = h_1(n_1 h_2)n_2 \in h_1 h_2 N,$$

da $n_1 h_2 \in N h_2 = h_2 N$ ist. Da N ein Normalteiler in G ist, so ist N erst recht ein Normalteiler in HN.
Der Homomorphismus

$$H \hookrightarrow HN \to HN/N$$

ist surjektiv und hat offenbar den Kern $H \cap N$ (ÜA). Nach Bemerkung 1.13 ist $H \cap N$ also ein Normalteiler in H. Ferner folgt aus Korollar 1.16 der Isomorphismus

$$H/H \cap N \to HN/N.$$

□

Satz 1.18 (2. Isomorphiesatz) Es sei G eine Gruppe und N, H zwei Normalteiler in G mit $N \subset H$. Dann ist N auch Normalteiler in H und man kann H/N als Normalteiler von G/N auffassen. Der kanonische Gruppenhomomorphismus

$$(G/N)/(H/N) \to G/H$$

ist ein Isomorphismus.

Beweis : N ist normal in G, also auch in H. Die Inklusion $H \hookrightarrow G$ vermittelt den Gruppenhomomorphismus

$$\psi : H \hookrightarrow G \xrightarrow{\pi} G/N.$$

Dieser hat den Kern N. Nach Satz 1.15 gibt es also einen eindeutig bestimmten Gruppenhomomorphismus

$$\overline{\psi} : H/N \to G/N,$$

der

$$\begin{array}{ccc} H & \longrightarrow & G \\ \downarrow & & \downarrow \\ H/N & \xrightarrow{\overline{\psi}} & G/N \end{array}$$

kommutativ macht. Ebenfalls nach Satz 1.15 ist $\overline{\psi}$ injektiv. Mit Hilfe dieses injektiven Homomorphismus $\overline{\psi}$ identifzieren wir H/N mit der Untergruppe Bild $\overline{\psi}$ von G/N. Ferner induziert der Epimorphismus

$$G \to G/H$$

wegen $N \subset H$ einen Epimorphismus

$$G/N \to G/H,$$

dessen Kern mit dem Bild von H unter der Quotientenabbildung $G \to G/N$, d.h. mit Bild $\overline{\psi}$ übereinstimmt. Dieses haben wir oben mit H/N identifziert. Nach Korollar 1.16 ist also

$$(G/N)/(H/N) \xrightarrow{\sim} G/H$$

□

Definition 1.19 i) Ist H eine Teilmenge der Gruppe G, so ist die Menge

$$\langle H \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : n \in \mathbb{N}, x_1, \ldots, x_n \in H, \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}$$

eine Gruppe (ÜA).

Diese heißt die **von** H **erzeugte Untergruppe** von G.

ii) G heißt **endlich erzeugt**, wenn es eine endliche Teilmenge $H \subset G$ mit $\langle H \rangle = G$ gibt.

iii) G heißt **zyklisch**, falls es ein $x \in G$ mit $\langle \{x\} \rangle = G$ gibt. Dafür schreiben wir auch $\langle x \rangle$.

Offenbar ist jede zyklische Gruppe abelsch. Außerdem gilt

Satz 1.20 i) Eine Gruppe G ist genau dann zyklisch, wenn es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$ gibt.

ii) Für eine zyklische Gruppe G gilt:

$$G \simeq \mathbb{Z}, \text{ falls } \mathrm{ord}(G) = \infty$$
$$G \simeq \mathbb{Z}/m\mathbb{Z}, \text{ falls } \mathrm{ord}(G) = m \text{ für } m \in \mathbb{N}.$$

Hier ist $m\mathbb{Z} = \langle m \rangle$ die von $m \in \mathbb{N}$ erzeugte zyklische Untergruppe von $\mathbb{Z}$. Da $\mathbb{Z}$ abelsch ist, ist $m\mathbb{Z}$ ein Normalteiler in $\mathbb{Z}$.

Beweis :

i) Ist $G = \langle x \rangle = \{x^m : m \in \mathbb{Z}\}$, so definiert $m \mapsto x^m$ einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$.

Ist umgekehrt $\psi : \mathbb{Z} \to G$ ein surjektiver Gruppenhomomorphismus, so ist $G = \langle x \rangle$ für $x = \psi(1)$ (ÜA).

ii) Es sei $\psi : \mathbb{Z} \to G$ der surjektive Gruppenhomomorphismus aus i). Dann ist nach Korollar 1.16

$$\mathbb{Z}/\text{ Kern } \psi \simeq G.$$

Wir untersuchen die Struktur der Untergruppe $H :=$ Kern $\psi \subset \mathbb{Z}$. Wir nehmen zunächst $H \neq 0$ an. Dann gibt es in H positive ganze Zahlen. Sei

$$m = \min\{k \in H : k > 0\}.$$

Wir zeigen $m\mathbb{Z} = H$. Die Inklusion $m\mathbb{Z} \subset H$ ist klar. Sei $k \in H$. Mit Division durch m mit Rest ist

$$k = qm + r$$

für ein $r \in \{0, 1, \ldots, m-1\}$. Dann ist $r = k - qm \in H$. Aufgrund der Minimalität von m folgt $r = 0$, also $k \in m\mathbb{Z}$.

Dieser Beweis zeigt auch, dass die Nebenklassen von $m\mathbb{Z}$ in $\mathbb{Z}$ genau die

$$r + m\mathbb{Z}, r = 0, \ldots, m-1$$

sind. Somit ist $\mathrm{ord}(G) = \mathrm{ord}(\mathbb{Z}/m\mathbb{Z}) = m$. Ist $\mathrm{ord}(G) = \infty$, so folgt demnach Kern $\psi = 0$ und $\mathbb{Z} \simeq G$. Ist $\mathrm{ord}(G) = m$, so folgt $m = \mathrm{ord}(\mathbb{Z}/\text{ Kern } \psi)$, also Kern $\psi = m\mathbb{Z}$.

□

Satz 1.21 i) Ist G eine zyklische Gruppe, so ist auch jede Untergruppe $H \subset G$ zyklisch.

ii) Ist G zyklisch und $\varphi : G \to G'$ ein Gruppenhomomorphismus, so sind auch Kern φ und Bild φ zyklisch.

Beweis :

i) Es sei $\psi : \mathbb{Z} \to G$ ein Epimorphismus. Dann ist $\psi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ (ÜA), also wie in Satz 1.20 gezeigt:

$$\begin{aligned} \psi^{-1}(H) &= 0 \text{ oder} \\ \psi^{-1}(H) &= m\mathbb{Z} \text{ für ein } m \in \mathbb{N}. \end{aligned}$$

In jedem Fall ist $\psi^{-1}(H)$ zyklisch.

Ist $\psi^{-1}(H)$ von a erzeugt, so ist $\psi(\psi^{-1}H)$ von $\psi(a)$ erzeugt. Bilder zyklischer Gruppen sind also wieder zyklisch. Somit ist $H = \psi(\psi^{-1}H)$ zyklisch, da ψ surjektiv ist.

ii) Wir haben schon gesehen, dass Bilder zyklischer Gruppen wieder zyklisch sind. Da Kern $\varphi \subset G$ eine Untergruppe ist, ist Kern φ nach i) zyklisch.

□

Definition 1.22 Sei G eine Gruppe und $a \in G$. Die **Ordnung von** a ist definiert als die Ordnung von $\langle a \rangle$, der von a erzeugten zyklischen Untergruppe von G. Wir bezeichnen sie mit $\text{ord}(a)$.

Wir haben schon gesehen, dass

$$\begin{aligned} \psi : \mathbb{Z} &\to \langle a \rangle, \\ k &\mapsto a^k \end{aligned}$$

einen Epimorphismus definiert, und dass gilt

$$\mathbb{Z} \simeq \langle a \rangle, \text{ falls } \text{ord}(a) = \infty$$

sowie

$$\mathbb{Z}/m\mathbb{Z} \simeq \langle a \rangle, \text{ falls } \text{ord}(a) = m \in \mathbb{N}.$$

Ist $\text{ord}(a) = m \in \mathbb{N}$, so folgt aus diesem Isomorphismus:

$$a^k = 1 \Leftrightarrow k \in m\mathbb{Z}.$$

Insbesondere ist $m = \text{ord}(a)$ also die kleinste positive Zahl k mit $a^k = 1$. Ferner gilt

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{m-1}\}.$$

Satz 1.23 (Kleiner Fermat'scher Satz) Sei G eine endliche Gruppe und $a \in G$. Dann ist $\text{ord}(a)$ ein Teiler von $\text{ord}(G)$, und es gilt

$$a^{\text{ord}(G)} = 1.$$

Beweis : Aus dem Satz von Lagrange folgt $\text{ord}(G) = \text{ord}(a) \cdot (G : \langle a \rangle)$. Also gilt $\text{ord}(a) \mid \text{ord}(G)$. Daraus folgt $a^{\text{ord}(G)} = 1$. □

Korollar 1.24 Es sei G eine Gruppe, so dass $\text{ord}(G) = p$ eine Primzahl ist. Dann ist G zyklisch, $G \simeq \mathbb{Z}/p\mathbb{Z}$ und für jedes $a \in G$ mit $a \neq 1$ gilt $\text{ord}(a) = p$. Jedes $a \neq 1$ aus G ist ein Erzeuger von G.

Beweis : Es sei $a \neq 1$ ein Element in G. Dann ist $\text{ord}(a) > 1$ und nach Satz 1.23 ist $\text{ord}(a)$ ein Teiler von $\text{ord}(G) = p$. Also ist $\text{ord}(a) = p$. Somit ist $\langle a \rangle$ eine Untergruppe von G mit $p = \text{ord}(G)$ Elementen. Daraus folgt $\langle a \rangle = G$. Somit ist a ein Erzeuger von G, G ist zyklisch und nach Satz 1.20 folgt $G \simeq \mathbb{Z}/p\mathbb{Z}$. □

2 Ringe

Definition 2.1 Ein **Ring** (manchmal auch Ring mit Eins genannt) ist eine Menge R zusammen mit zwei Abbildungen:

$$\begin{aligned} + : &\quad R \times R \to R \quad \text{(Addition) und} \\ \cdot : &\quad R \times R \to R \quad \text{(Multiplikation),} \end{aligned}$$

so dass gilt

i) $(R, +)$ ist eine abelsche Gruppe

ii) $(R, \cdot)$ ist ein Monoid

iii) für alle $a, b, c \in R$ gilt

$$\begin{aligned} (a+b)c &= ac + bc \quad \text{und} \\ c(a+b) &= ca + cb \end{aligned}$$

(Distributivgesetze)

Wie gewohnt, soll immer die Multiplikation vor der Addition ausgeführt werden, d.h. wir schreiben $ac + bc = (ac) + (bc)$.
R heißt **kommutativ**, falls die Multiplikation kommutativ ist.

Wir werden hier im wesentlichen kommutative Ringe betrachten. Das neutrale Element bezüglich der Addition bezeichnen wir mit 0, das neutrale Element bezüglich der Multiplikation mit 1. Der kleinste Ring ist der Nullring $\{0\}$, den wir auch mit 0 bezeichnen. In diesem gilt $1 = 0$.

Lemma 2.2 In jedem Ring R gilt

i) $0a = a0 = 0$ für alle $a \in R$

ii) $(-a)b = -(ab) = a(-b)$ für alle $a, b \in R$

iii) Hat R mindestens zwei Elemente, so ist $1 \neq 0$.

Beweis :

i) Aus den Distributivgesetzen folgt $0a = (0+0)a = 0a+0a$, also $0a = 0$. Genauso folgt $a0 = 0$.

ii) $(-a)b + (ab) = (-a + a)b = 0b \overset{\text{i)}}{=} 0$. Die zweite Gleichung folgt genauso.

iii) Enthält R ein $a \neq 0$, so gilt $0a \overset{\text{i)}}{=} 0 \neq a$, daher kann 0 nicht das Einselement sein. □

Im allgemeinen gilt **nicht**, dass aus $ab = ac$ schon $b = c$ folgt!

Definition 2.3 Eine Teilmenge S des Ringes R heißt **Unterring** von R, falls S bezüglich der Addition eine Untergruppe von $(R, +)$ und bezüglich der Multiplikation ein Untermonoid von $(R, \cdot)$ ist.
Insbesondere ist S mit den eingeschränkten Verknüpfungen selbst ein Ring. Wir nennen $S \subset R$ dann auch eine Ringerweiterung. Für jeden Ring R bezeichnen wir mit

$$R^* = \{a \in R : \text{ es existiert ein } b \in R \text{ mit } ab = 1\}.$$

die Menge der multiplikativ invertierbaren Elemente. R^* ist eine Gruppe bzgl. der Multiplikation (ÜA). Wir bezeichnen sie auch als **Einheitengruppe**.
R heißt **Schiefkörper**, falls $R \neq 0$ und $R^* = R \setminus \{0\}$ gilt. Das heißt, es ist $1 \neq 0$ und jedes Element $\neq 0$ ist multiplikativ invertierbar.
Ein kommutativer Schiefkörper heißt **Körper**.

Ein Element $a \in R$ heißt **Nullteiler**, falls es ein $b \neq 0$ in R gibt mit $ab = 0$ oder $ba = 0$.
In Schiefkörpern oder Körpern ist das Nullelement der einzige Nullteiler (ÜA).
Ein kommutativer Ring $R \neq 0$ heißt **nullteilerfrei** oder **Integritätsring**, wenn R außer 0 keine Nullteiler enthält.
In Integritätsringen gilt die Kürzungsregel, d.h. aus $ab = ac$ für $a \neq 0$ folgt $b = c$ (ÜA).

Beispiel:

i) $\mathbb{Z}$ ist ein Integritätsring, $\mathbb{Z}^* = \{1, -1\}$.

ii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.

iii) Für jeden Körper K ist

$$K^{n\times n} = \{n \times n\text{-Matrizen über } K\}$$

ein Ring mit Einheitengruppe

$$\mathrm{GL}(n, K) = \{A \in K^{n\times n}, \det A \neq 0\}.$$

Dieser Ring ist für $n \geq 2$ nicht kommutativ und besitzt Nullteiler $\neq 0$.

iv) Für eine Menge X und einen Ring R ist

$$R^X = \{f : X \to R\}$$

ein Ring, wenn man die Addition und Multiplikation von Funktionen wie gewohnt als $(f + g)(x) = f(x) + g(x)$ und $(fg)(x) = f(x)g(x)$ definiert.

v) Ist I eine Indexmenge und $(R_i)_{i\in I}$ eine Familie von Ringen, so ist

$$\prod_{i\in I} R_i = \{(x_i)_{i\in I} : x_i \in R_i\}$$

ein Ring bezüglich der komponentenweisen Addition und Multiplikation.

Von nun an betrachten wir nur noch kommutative Ringe. **Daher ist ab sofort mit „Ring" immer „kommutativer Ring" gemeint.**
Eine Abbildung $\varphi : S \to R$ zwischen zwei Ringen heißt **Ringhomomorphismus**, falls φ ein Homomorphismus der abelschen Gruppen bezüglich der Addition und ein Monoidhomomorphismus bezüglich der Multiplikation ist. Mit anderen Worten, es gilt $\varphi(a + b) = \varphi(a) + \varphi(b), \varphi(1) = 1$ und $\varphi(ab) = \varphi(a)\varphi(b)$.

Definition 2.4 (Polynomring) Es sei R ein Ring. Der zugehörige Polynomring $R[X]$ in einer Unbestimmten X besteht aus allen formalen Summen

$$\sum_{i=0}^{n} a_i X^i, \quad n \in \mathbb{N}_0, a_i \in R.$$

Addition und Multiplikation werden gegeben durch

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i,$$

und

$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{i=0}^{m} b_i X^i\right) = \sum_{i=0}^{n+m} \left(\sum_{p+q=i} a_p b_q\right) X^i.$$

Hier setzen wir

$$\begin{aligned} a_i &= 0 \quad \text{für} \quad i \geq n+1 \text{ und} \\ b_i &= 0 \quad \text{für} \quad i \geq m+1. \end{aligned}$$

Das Nullelement ist das Nullpolynom $0 = 0X^0$, das Einselement das Polynom $1 = 1X^0$.

Die natürliche Abbildung

$$\begin{aligned} R &\to R[X] \\ a &\mapsto aX^0 \end{aligned}$$

ist ein injektiver Ringhomomorphismus (ÜA). Sie identifiziert R mit dem Unterring

$$\{aX^0 : a \in R\} \subset R[X]$$

Wir schreiben daher auch einfach $a = aX^0$.

Lemma 2.5 Für eine Ringerweiterung $R \subset R'$ und ein Element $c \in R'$ ist die Abbildung

$$\begin{aligned} \varphi : R[X] &\to R' \\ f(X) = \sum_{i=0}^{n} a_i X^i &\mapsto f(c) = \sum_{i=0}^{n} a_i c^i \end{aligned}$$

ein Ringhomomorphismus. Dieser heißt **Einsetzungshomomorphismus**.

Beweis : Offenbar ist $f(c) + g(c) = (f + g)(c)$ für alle $f, g \in R[X]$. Ferner gilt für $f(X) = \sum_{i=0}^{n} a_i X^i$ und $g(X) = \sum_{j=0}^{m} b_j X^j$:

$$\begin{aligned} f(c)g(c) &= \left(\sum_{i=0}^{n} a_i c^i\right)\left(\sum_{j=0}^{m} b_j c^j\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i c^i b_j c^j \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j c^{i+j} \\ &= (fg)(c). \end{aligned}$$

Hier ist es wichtig, dass R' - wie alle unsere Ringe nun - kommutativ ist.
Da außerdem $\varphi(1X^0) = 1$ gilt, ist φ ein Ringhomomorphismus. □

Für ein Polynom $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ nennen wir a_i den Koeffizienten vom Grad i von f. Der Koeffizient vom Grad 0 heißt auch **Absolutkoeffizient.** Außerdem definieren wir den **Grad** von f als

$$\text{grad } (f) := \max\{i : a_i \neq 0\},$$

falls $f \neq 0$ ist. Ist $f = 0$, so setzen wir $\text{grad}(f) = -\infty$. Ist $f \neq 0$ und $n = \text{grad}(f)$, so heißt a_n höchster Koeffizient oder **Leitkoeffizient** von f. Ist $a_n = 1$, so heißt f **normiert.** Jedes $f \in R[X] \setminus \{0\}$, dessen Leitkoeffizient a_n eine Einheit in R ist, lässt sich durch Multiplikation mit a_n^{-1} normieren.

Bemerkung 2.6 Für $f, g \in R[X]$ gilt

$$\begin{aligned} \text{grad}(f+g) &\leq \max(\text{grad}(f), \text{grad}(g)) \\ \text{grad}(fg) &\leq \text{grad}(f) + \text{grad}(g). \end{aligned}$$

Ist R ein Integritätsring, so gilt sogar

$$\text{grad}(fg) = \text{grad}(f) + \text{grad}(g).$$

Hier setzen wir $(-\infty) + (-\infty) = -\infty$ und $(-\infty) + n = -\infty$ für alle $n \in \mathbb{N}_0$.

Beweis : Falls f oder g das Nullpolynom ist, stimmt die Behauptung offenbar. Wir können also annehmen $n = \text{grad}(f) \geq 0$ und $m = \text{grad}(g) \geq 0$. Ist $f(X) = \sum_{i=0}^{n} a_i X^i$

und $g(X) = \sum_{i=0}^{m} b_i X^i$, so ist $a_i + b_i = 0$ für $i > \max(m, n)$, also folgt

$$\text{grad}(f + g) \leq \max(\text{grad}(f), \text{grad}(g)).$$

Außerdem ist $\sum_{p+q=i} a_p b_q = 0$ für $i > m + n$, also $\text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g)$. Der Koeffizient vom Grad $m + n$ in fg ist $a_n b_m$. Ist R ein Integritätsring, so ist $a_n b_m \neq 0$, also

$$\text{grad}(fg) = m + n = \text{grad}(f) + \text{grad}(g).$$

□

Bemerkung 2.7 Es sei R ein Integritätsring. Dann ist auch der Polynomring $R[X]$ ein Integritätsring. Ferner gilt $R[X]^* = R^*$.

Beweis : $f \in R[X]$ sei ein Nullteiler in $R[X]$ mit $fg = 0$ für ein $g \neq 0$. Da R ein Integritätsring ist, folgt aus Bemerkung 2.6: $-\infty = \text{grad}(0) = \text{grad}(f) + \text{grad}(g)$. Da $\text{grad}(g) \geq 0$ ist, muss hier $\text{grad}(f) = -\infty$, d.h. $f = 0$ sein.
Wir zeigen jetzt $R[X]^* = R^*$. Die Inklusion „$\supset$“ ist klar. Sei also $f \in R[X]^*$, d.h. es existiert ein $g \in R[X]$ mit $fg = 1$. Aus Bemerkung 2.6 folgt wieder $0 = \text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$, also $f, g \in R$. □

In Polynomringen lässt sich eine **Division mit Rest** durchführen:

Satz 2.8 Sei R ein Ring und $g = \sum_{i=0}^{d} a_i X^i \in R[X]$ mit $a_d \in R^*$. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit

$$f = qg + r, \quad \text{grad}(r) < d.$$

Beweis : Ist q ein Polynom vom Grad n mit Leitkoeffizient $c_n \neq 0$, so ist der Koeffizient vom Grad $n + d$ in qg gerade $a_d c_n$. Da a_d eine Einheit ist, folgt $a_d c_n \neq 0$. Also ist

$$\text{grad}(qg) = \text{grad}(q) + \text{grad}(g).$$

Wir zeigen zunächst die Eindeutigkeit der Division mit Rest. Gilt

$$f = qg + r = q'g + r'$$

mit grad $r < d$ und grad $r' < d$, so folgt

$$0 = (q - q')g + (r - r'),$$

also

$$\begin{aligned} d > \text{grad}(r - r') &= \text{grad}((q - q')g) \\ &\overset{\text{s.o.}}{=} \text{grad}(q - q') + \text{grad}(g) \\ &= \text{grad}(q - q') + d. \end{aligned}$$

Das kann nur stimmen, wenn $q - q' = 0$, also $q = q'$ ist. Daraus folgt $r = r'$ und somit die Eindeutigkeit.
Die Existenz zeigen wir mit Induktion nach $n = \text{grad}(f)$. Für grad $(f) < d$ können wir $q = 0$ und $r = f$ nehmen. Ist $f = \sum_{i=0}^{n} c_n X^i$ mit $c_n \neq 0$ und $n \geq d$, so ist

$$f_1 = f - c_n a_d^{-1} X^{n-d} g$$

ein Polynom mit $\text{grad}(f_1) < n$. Dies besitzt nach Induktionsvoraussetzung eine Zerlegung

$$f_1 = q_1 g + r_1$$

mit $q_1, r_1 \in R[X]$, $\text{grad}(r_1) < d$. Aus

$$f = (q_1 + c_n a_d^{-1} X^{n-d})g + r_1$$

folgt die gewünschte Zerlegung von f. □

Der Beweis gibt uns auch ein Verfahren zur Bestimmung von q und r an die Hand, das wir an einem Beispiel vorführen wollen.
Beispiel $f = X^5 + 3X^4 + X^3 - 6X^2 - X + 1$, $g = X^3 + 2X^2 + X - 1$ in $\mathbb{Z}[X]$

$$\begin{array}{lrl} & (X^5 & +3X^4 + X^3 - 6X^2 - X + 1) : (X^3 + 2X^2 + X - 1) = X^2 + X - 2 = q(X) \\ - & \underline{(X^5} & \underline{+2X^4 + X^3 - X^2)} \\ & X^4 & -5X^2 - X + 1 \\ & - \quad \underline{(X^4} & \underline{+2X^3 + X^2 - X)} \\ & & -2X^3 - 6X^2 + 1 \\ & & - \quad \underline{(2X^3 - 4X^2 - 2X + 2)} \\ & & -2X^2 + 2X - 1 = r(X) \end{array}$$

Also ist $f(X) = (X^2 + X - 2)g(X) + (-2X^2 + 2X - 1)$

Wir lernen nun Ideale in Ringen kennen. Diese haben eine ähnliche Funktion wie Normalteiler in Gruppen, man kann nämlich in der Welt der Ringe Quotienten nach Idealen bilden. Allerdings sind Ideale im allgemeinen keine Unterringe.

Definition 2.9 Es sei R ein Ring (kommutativ, wie immer!). Eine Teilmenge $\mathfrak{a} \subset R$ heißt **Ideal** in R, falls gilt

i) $\mathfrak{a}$ ist eine additive Untergruppe von R

ii) für alle $r \in R, a \in \mathfrak{a}$ gilt $ra \in \mathfrak{a}$.

Jeder Ring enthält die trivialen Ideale $\{0\}$ (auch mit 0 bezeichnet) und R. Ist R ein Körper, so sind dies die einzigen Ideale (ÜA). Für Ideale $\mathfrak{a}, \mathfrak{b} \subset R$ sind auch folgende Teilmengen von R Ideale (ÜA):

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &:= \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\} \\ \mathfrak{a}\mathfrak{b} &:= \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N} \right\} \\ \mathfrak{a} \cap \mathfrak{b} & \end{aligned}$$

Offenbar ist $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ sowie $\mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}$, $\mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$ (ÜA).
Analog ist das Produkt von endlich vielen Idealen in R wieder ein Ideal. Auch der Schnitt beliebig vieler Ideale $(\mathfrak{a}_i)_{i \in I}$ sowie die Summe beliebig vieler Ideale.

$$\sum_{i \in I} \mathfrak{a}_i = \{ \sum_{i \in I} a_i : a_i \in \mathfrak{a}_i \text{ für alle } i \in I, \text{ fast alle } a_i = 0 \}$$

sind Ideale in R (ÜA). Hier schreiben wir „ fast alle“ für „ alle bis auf endlich viele“.
Für jedes $a \in R$ nennt man

$$(a) := Ra = \{ra : r \in R\}$$

das von a erzeugte **Hauptideal**.
Für endlich viele Elemente $a_1, \ldots, a_n \in R$ ist

$$(a_1, \ldots, a_n) := Ra_1 + \cdots + Ra_n = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$$

ein Ideal in R. Es heißt das von $a_1, \ldots, a_n$ erzeugte Ideal und ist das kleinste Ideal in R, das $a_1, \ldots, a_n$ enthält. Mit anderen Worten, jedes Ideal $\mathfrak{a}$ mit $\{a_1, \ldots, a_n\} \subset \mathfrak{a}$ erfüllt $(a_1, \ldots, a_n) \subset \mathfrak{a}$. (ÜA).
Analog erzeugen beliebig viele Elemente $a_i, i \in I$ aus R ein Ideal:

$$(\{a_i : i \in I\}) := \sum_{i \in I} Ra_i = \left\{ \sum_{i \in I} r_i a_i : r_i \in R, \text{ fast alle } r_i = 0 \right\}.$$

Definition 2.10 Es sei $\mathfrak{a}$ ein Ideal des Ringes R. Eine Familie $(a_i)_{i\in I}$ von Elementen aus $\mathfrak{a}$ heißt **Erzeugendensystem** von $\mathfrak{a}$, wenn $\mathfrak{a} = \sum_{i\in I} Ra_i$ gilt. $\mathfrak{a}$ heißt **endlich erzeugt**, wenn $\mathfrak{a}$ ein endliches Erzeugendensystem besitzt. Ferner heißt $\mathfrak{a}$ **Hauptideal**, wenn $\mathfrak{a}$ von einem einzigen Element erzeugt ist, d.h. wenn $\mathfrak{a} = (a)$ für ein $a \in R$ gilt.
Ist R ein Integritätsring, in dem jedes Ideal ein Hauptideal ist, so nennen wir R einen **Hauptidealring**.

Beispiel:

i) In jedem Ring sind die trivialen Ideale $0 = (0)$ und $R = (1)$ Hauptideale.

ii) In $\mathbb{Z}$ sind die Untergruppen $m\mathbb{Z}$ auch Ideale, und zwar Hauptideale, da $m\mathbb{Z} = (m)$ ist. Da jedes Ideal von $\mathbb{Z}$ eine additive Untergruppe ist, gibt es nach dem Beweis von Satz 1.20 keine weiteren Ideale. Der Ring $\mathbb{Z}$ ist also ein Hauptidealring.

Bemerkung 2.11 In einem Integritätsring R sind zwei Hauptideale $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$ genau dann gleich, wenn es ein $c \in R^*$ mit $b = ca$ gibt.

Beweis : Es sei $\mathfrak{a} = \mathfrak{b}$. Wir können annehmen $\mathfrak{b} \neq 0$, also $b \neq 0$. Da $b \in \mathfrak{a}$ ist, existiert ein $c \in R$ mit $b = ca$. Analog existiert wegen $a \in \mathfrak{b}$ ein $c' \in R$ mit $a = c'b$. Damit folgt $b = ca = cc'b$, also

$$(1 - cc')b = 0.$$

Da R ein Integritätsring ist, ist $b \neq 0$ kein Nullteiler, also folgt $1 = cc'$. Somit ist $c \in R^*$. Ist umgekehrt $b = ca$ für $c \in R^*$, so folgt $a = c^{-1} \cdot b$, also $(b) \subset (a)$ und $(a) \subset (b)$. □

Wir nennen zwei Elemente a, b eines Ringes R **assoziiert**, wenn es ein $c \in R^*$ mit $b = ca$ gibt.

Beispiel: Wir betrachten den Polynomring $\mathbb{Z}[X]$. Dieser ist ein Integritätsring nach Bemerkung 2.7. $\mathbb{Z}[X]$ enthält die Hauptideale

$$(X) = \left\{ \sum_{i=1}^{n} a_i X^i : n \in \mathbb{N}, a_i \in \mathbb{Z} \right\}$$

und

$$(2) = \left\{ \sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}_0, a_i \in 2\mathbb{Z} \right\}.$$

Das Ideal $(2, X)$ erfüllt

$$(2, X) = \left\{ \sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}, a_0 \in 2\mathbb{Z} \right\} \quad \text{(ÜA)}.$$

Es ist allerdings kein Hauptideal. Sonst gäbe es nämlich ein $f \in \mathbb{Z}[X]$ mit $2 \in (f)$ und $X \in (f)$, d.h.

$$2 = fg \text{ und } X = fh$$

für gewisse $g, h \in \mathbb{Z}[X]$. Aus der ersten Gleichung folgt nach Bemerkung 2.6 aber $f \in \mathbb{Z}$ und $g \in \mathbb{Z}$. Da $(2, X) \neq \mathbb{Z}[X]$, kann f nicht ± 1 sein. Also folgt $f = \pm 2$ im Widerspruch zur zweiten Gleichung $X = fh$.
Somit ist $\mathbb{Z}[X]$ kein Hauptidealring.
Jetzt wollen wir - analog zu Faktorgruppen - auch Faktorringe definieren. Dazu untersuchen wir zunächst Ringhomomorphismen.

Lemma 2.12 Es sei $\varphi : R \to R'$ ein Ringhomomorphismus. Dann gilt

i) Kern$(\varphi) := \{a \in R : \varphi(a) = 0\}$ ist ein Ideal in R.

ii) Bild $(\varphi) = \varphi(R)$ ist ein Unterring von R'.

iii) φ induziert einen Gruppenhomomorphismus $R^* \to R'^*$ zwischen den Einheitengruppen

Beweis :

i) Kern (φ) ist einfach der Kern der Abbildung φ, betrachtet als Gruppenhomomorphismus der zugehörigen abelschen Gruppen Also ist Kern(φ) eine Untergruppe von $(R, +)$. Für $r \in R$ und $a \in$ Kern (φ) gilt $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, also $ra \in$ Kern (φ). Somit ist Kern(φ) ein Ideal in R.

ii) Wie in i) folgt, dass Bild (φ) mit der eingeschränkten Addition eine Untergruppe von $(R', +)$ ist. Wegen $\varphi(1) = 1$ liegt $1 \in$ Bild (φ). Da $\varphi(a)\varphi(b) = \varphi(ab)$ ist, ist Bild (φ) abgeschlossen unter der Multiplikation, also ein Untermonoid von $(R', \cdot)$.

iii) Ist $a \in R^*$ mit $ab = 1$, so ist $\varphi(a)\varphi(b) = 1$, also $\varphi(a) \in R'^*$. Somit vermittelt φ eine Abbildung $R^* \to R'^*$. Diese ist ein Gruppenhomomorphismus, da $\varphi(ab) = \varphi(a)\varphi(b)$ gilt.

□

Man muss zwischen Idealen und Unterringen unterscheiden. Ein Ideal $\mathfrak{a} \subset R$ ist nur dann ein Unterring, wenn $1 \in \mathfrak{a}$ ist, woraus schon $\mathfrak{a} = R$ folgt.
Ein Unterring hingegen muss nicht abgeschlossen sein unter Multiplikation mit beliebigen Elementen in R. So wird auch das Bild eines Ringhomomorphismus im allgemeinen kein Ideal sein (ÜA: Wann ist es eins?).

Bemerkung 2.13 Es sei K ein Körper und R ein Ring, $R \neq 0$. Dann ist jeder Ringhomomorphismus

$$\varphi : K \to R$$

injektiv. Insbesondere ist jeder Ringhomomorphismus zwischen Körpern injektiv. Einen Ringhomomorphismus zwischen Körpern nennt man auch **Körperhomomorphismus**

Beweis : Kern(φ) ist ein Ideal in K, das wegen $\varphi(1) = 1 \neq 0$ nicht ganz K ist. Da K nur die Ideale 0 und K enthält, folgt also Kern $(\varphi) = 0$. □

Beispiel Zu jedem Ring R gibt es den Ringhomomorphismus

$$\varphi : \mathbb{Z} \to R$$

mit

$$\varphi(n) = n \cdot 1 = (\underbrace{1 + \cdots + 1}_{n\text{-mal}})$$

und

$$\varphi(-n) = -\varphi(n) \qquad \text{für } n \geq 0.$$

φ ist der einzige Ringhomomorphismus $\mathbb{Z} \to R$ (ÜA).

Definition 2.14 Es sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Da $\mathfrak{a}$ insbesondere eine Untergruppe der abelschen Gruppe $(R, +)$ ist, existiert die **Faktorgruppe** $R/\mathfrak{a}$, siehe Lemma 1.14. Dort haben wir die Gruppenoperation multiplikativ geschrieben. In additive Schreibweise übersetzt, besteht $R/\mathfrak{a}$ aus allen Nebenklassen der Form $x + \mathfrak{a}$, $x \in R$, wobei die Addition definiert ist als

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}.$$

Zusätzlich definieren wir eine Multiplikation auf $R/\mathfrak{a}$ durch

$$(x + \mathfrak{a})(y + \mathfrak{a}) = (xy) + \mathfrak{a}.$$

Lemma 2.15 Mit dieser Multiplikation wird $R/\mathfrak{a}$ zu einem Ring. Die Abbildung

$$\begin{array}{rcl} \pi : R & \to & R/\mathfrak{a} \\ x & \mapsto & x + \mathfrak{a} \end{array}$$

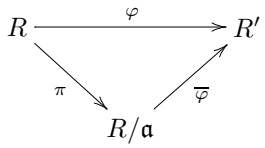
ist ein Ringhomomorphismus mit Kern$(\pi) = \mathfrak{a}$. Der Ring $R/\mathfrak{a}$ heißt auch **Faktorring** und π heißt auch die **Projektionsabbildung** von R nach $R/\mathfrak{a}$.

Beweis : Wir wissen aus Lemma 1.14, dass die Addition von Restklassen wohldefiniert ist. Um zu zeigen, dass auch die Multiplikation wohldefiniert ist, sei $x+\mathfrak{a} = x'+\mathfrak{a}$ und $y + \mathfrak{a} = y' + \mathfrak{a}$, d.h. $x' - x = a \in \mathfrak{a}$ und $y' - y = b \in \mathfrak{a}$.
Dann ist

$$x'y' = (x + a)(y + b) = xy + bx + ay + ab \in xy + \mathfrak{a}$$

Nun rechnet man leicht nach, dass $R/\mathfrak{a}$ ein Ring mit Einselement $1 + \mathfrak{a}$ ist (ÜA). Die kanonische Projektion π ist nach Lemma 1.14 ein surjektiver Gruppenhomomorphismus mit Kern $(\pi) = \mathfrak{a}$. Da $\pi(x)\pi(y) = (x+\mathfrak{a})(y+\mathfrak{a}) = xy+\mathfrak{a} = \pi(xy)$ und $\pi(1) = 1+\mathfrak{a}$ gilt, ist π ein Ringhomomorphismus. □

Satz 2.16 (Homomorphiesatz für Ringe) Es sei $\varphi : R \to R'$ ein Ringhomomorphismus und $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{a} \subset$ Kern (φ). Dann existiert genau ein Ringhomomorphismus $\overline{\varphi} : R/\mathfrak{a} \to R'$, so dass das Diagramm



kommutiert. Es gilt

$$\begin{aligned} \text{Bild } (\overline{\varphi}) &= \text{Bild } (\varphi) \\ \text{Kern } (\overline{\varphi}) &= \pi(\text{ Kern } \varphi) \\ \text{Kern } (\varphi) &= \pi^{-1}(\text{ Kern } \overline{\varphi}). \end{aligned}$$

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $\mathfrak{a} =$ Kern φ gilt.

Beweis : Nach Satz 1.15 existiert ein eindeutig bestimmter Gruppenhomomorphismus $\overline{\varphi} : R/\mathfrak{a} \to R'$ mit $\varphi = \overline{\varphi} \circ \pi$, der die Aussagen über Kern $\overline{\varphi}$ und Bild $\overline{\varphi}$ erfüllt.
Es ist

$$\begin{aligned} \overline{\varphi}((x + \mathfrak{a}) \cdot (y + \mathfrak{a})) &= \overline{\varphi}(\pi(x) \cdot \pi(y)) \\ &= \overline{\varphi}(\pi(xy)) \\ &= \varphi(xy) \\ &= \varphi(x) \cdot \varphi(y) \\ &= \overline{\varphi}(\pi(x)) \cdot \overline{\varphi}(\pi(y)) \\ &= \overline{\varphi}(x + \mathfrak{a}) \cdot \overline{\varphi}(y + \mathfrak{a}), \end{aligned}$$

also ist $\overline{\varphi}$ ein Ringhomomorphismus. Damit ist alles gezeigt. □

Korollar 2.17 Ist $\varphi : R \to R'$ ein surjektiver Ringhomomorphismus, so ist R' kanonisch isomorph zu $R/\text{Kern}\varphi$.

Beweis : φ ist insbesondere ein surjektiver Gruppenhomomorphismus, also ist nach Korollar 1.16 der eindeutig bestimmte (kanonische) Gruppenhomomorphismus $\overline{\varphi}$: $R/\text{Kern}\varphi \to R'$ mit $\varphi = \overline{\varphi} \circ \pi$ ein Isomorphismus Nach Satz 2.16 ist $\overline{\varphi}$ ein Ringhomomorphismus. Als bijektiver Ringhomomorphismus ist $\overline{\varphi}$ nach dem folgenden Lemma aber auch ein Isomorphismus von Ringen. □

Lemma 2.18 Es sei $\varphi : R \to R'$ ein bijektiver Ringhomomorphismus. Dann ist φ ein **Isomorphismus von Ringen**, d.h. es existiert ein Ringhomomorphismus $\psi : R' \to R$ mit $\psi \circ \varphi = \text{id}_R$ und $\varphi \circ \psi = \text{id}_{R'}$.

Beweis : Wir definieren $\psi(y)$ als das eindeutig bestimmte Urbild von φ in R. Dann rechnet man leicht nach, dass ψ mit der Addition und der Mutliplikation verträglich ist und $\varphi(1) = 1$ sowie $\psi \circ \varphi = \text{id}_R$ und $\varphi \circ \psi = \text{id}_{R'}$ erfüllt. □

Die Isomorphiesätze 1.17 und 1.18 lassen sich auch für Ringe formulieren, wenn man überall Untergruppe und Normalteiler durch Ideal ersetzt. Diese Aussagen folgen dann aus den Sätzen 1.17 und 1.18, indem man nachrechnet, dass alle Gruppenhomorphismen auch Ringhomomorphismen sind (ÜA).

Beispiel: Die zuvor betrachtete Untergruppe $m\mathbb{Z} \subset \mathbb{Z}$ für $m \in \mathbb{N}$ ist sogar ein Ideal von $\mathbb{Z}$, und zwar das von m erzeugte Hauptideal. Der Faktorring $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring mit m Elementen.

Satz 2.19 Für $m \in \mathbb{N}$ sind äquivalent

i) m ist eine Primzahl

ii) $\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring

iii) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper

Beweis : Wir schreiben kurz $\overline{x} = x + m\mathbb{Z}$ für die Restklasse von x modulo $m\mathbb{Z}$.
i) $\Rightarrow$ ii) Ist p prim, so ist $p > 1$ und $\mathbb{Z}/p\mathbb{Z}$ als Ring mit p Elementen nicht der Nullring. Gilt $\overline{a} \cdot \overline{b} = 0$ in $\mathbb{Z}/p\mathbb{Z}$, so ist $ab \in p\mathbb{Z}$, d.h. $ab = pk$, für ein $k \in \mathbb{Z}$. Aufgrund der Primfaktorzerlegung in $\mathbb{Z}$ ist p ein Teiler von a oder von b, somit ist $\overline{a} = 0$ oder $\overline{b} = 0$. $\mathbb{Z}/p\mathbb{Z}$ ist also nullteilerfrei.

ii) $\Rightarrow$ iii) Für jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$ betrachten wir die Abbildung.

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ \overline{x} &\mapsto \overline{a} \cdot \overline{x}. \end{aligned}$$

Dies ist ein Homomorphismus der additiven Gruppen (aber *kein* Ringhomomorphismus!), der injektiv ist, da $\overline{a}$ kein Nullteiler ist. Da auf beiden Seiten m-elementige Mengen stehen, ist er somit bijektiv. Also existiert ein $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ mit $\overline{a} \cdot \overline{b} = 1$. Daher ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper.
iii) $\Rightarrow$ i) Ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, so ist $m \geq 2$. Es sei $m = d \cdot a$. Daraus folgt $\overline{d} \cdot \overline{a} = 0$, aufgrund der Nullteilerfreiheit von $\mathbb{Z}/m\mathbb{Z}$, also $\overline{d} = 0$ oder $\overline{a} = 0$. Somit ist m ein Teiler von d, woraus $m = d$ und $a = 1$ folgt, oder ein Teiler von a, woraus $m = a$ und $d = 1$ folgt. Daher ist m eine Primzahl □

Definition 2.20 Für jede Primzahl p sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dies ist ein Körper mit p Elementen.

Wir verallgemeinern jetzt den Begriff einer Primzahl in $\mathbb{Z}$.

Definition 2.21 Es sei R ein Ring.

i) Ein Ideal $\mathfrak{p} \subset R$ heißt **prim** oder **Primideal**, wenn $\mathfrak{p} \neq R$ ist und wenn für alle $a, b \in R$ aus $ab \in \mathfrak{p}$ schon $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

ii) Ein Ideal $\mathfrak{m} \subset R$ heißt **maximal**, wenn $\mathfrak{m} \neq R$ ist und wenn für alle Ideale $\mathfrak{a} \subset R$ mit $\mathfrak{m} \subset \mathfrak{a}$ gilt: $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Beispiel: Das Ideal $m\mathbb{Z} \subset \mathbb{Z}$, $m \in \mathbb{N}_0$ ist genau dann ein Primideal, wenn $m = 0$ oder m eine Primzahl ist. $m\mathbb{Z} \subset \mathbb{Z}$ ist ein maximales Ideal genau dann, wenn m eine Primzahl ist. (ÜA)

Satz 2.22 Es sei R ein Ring.

i) Ein Ideal $\mathfrak{p} \subset R$ ist prim genau dann, wenn $R/\mathfrak{p}$ ein Integritätsring ist. Insbesondere ist 0 ein Primideal genau dann, wenn R ein Integritätsring ist.

ii) Ein Ideal $\mathfrak{m} \subset R$ ist genau dann ein maximales Ideal, wenn $R/\mathfrak{m}$ ein Körper ist. Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis :

i) „$\Rightarrow$“: Ist $\mathfrak{p} \subset R$ ein Primideal, so ist $\mathfrak{p} \neq R$, d.h. $R/\mathfrak{p} \neq 0$. Gilt für $a, b \in R$, dass $\overline{a} \cdot \overline{b} = 0$ in $R/\mathfrak{p}$ ist, so ist $ab \in \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d.h. $\overline{a} = 0$ oder $\overline{b} = 0$.

„$\Leftarrow$“: Da $R/\mathfrak{p} \neq 0$ ist, ist $\mathfrak{p} \neq R$. Sei $ab \in \mathfrak{p}$, dann ist $\overline{a}\overline{b} = 0$. Da $R/\mathfrak{p}$ nullteilerfrei ist, folgt $\overline{a} = 0$ oder $\overline{b} = 0$, d.h. $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

ii) folgt aus Lemma 2.23.

□

Lemma 2.23 i) Ein Ideal $\mathfrak{m} \subset R$ ist genau dann maximal, wenn das Nullideal in $R/\mathfrak{m}$ maximal ist.

ii) Das Nullideal $0 \subset R$ ist maximal genau dann, wenn R ein Körper ist.

Beweis :

i) Für jedes Ideal $\mathfrak{a} \supset \mathfrak{m}$ ist das Bild $\pi(\mathfrak{a})$ unter der Restklassenabbildung $\pi : R \to R/\mathfrak{m}$ ein Ideal in $R/\mathfrak{m}$. Umgekehrt ist für jedes Ideal $\mathfrak{b} \subset R/\mathfrak{m}$ das Urbild $\pi^{-1}(\mathfrak{b})$ ein Ideal in R, das $\mathfrak{m}$ enthält. (ÜA). Diese Abbildungen vermitteln eine Bijektion (ÜA):

$$\begin{aligned} \{ \text{ Ideale } \mathfrak{a} \subset R \text{ mit } \mathfrak{m} \subset \mathfrak{a} \} &\to \{ \text{ Ideale in } R/\mathfrak{m} \} \\ \mathfrak{a} &\mapsto \pi(\mathfrak{a}) \\ \pi^{-1}(\mathfrak{b}) &\hookleftarrow \mathfrak{b}. \end{aligned}$$

Daraus folgt sofort die Behauptung.

ii) Wir haben oben schon gesehen, dass ein Körper R nur die Ideale 0 und R enthält, die außerdem verschieden sind. Also ist 0 ein maximales Ideal in R. Sei umgekehrt R ein Ring, so dass 0 ein maximales Ideal in R ist. Wir müssen zeigen, dass $R \neq 0$ und dass jedes $a \in R \setminus \{0\}$ invertierbar ist. Ersteres folgt, da das maximale Ideal $0 \neq R$ ist. Sei ferner $a \in R \setminus \{0\}$. Dann ist

$$0 \subsetneq (a) \subset R,$$

wegen der Maximalität von 0 also $(a) = R$. Daher ist $1 \in (a)$, d.h. es existiert ein $b \in R$ mit $ab = 1$.

□

Satz 2.24 (Chinesischer Restsatz) Sei R ein Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ paarweise teilerfremde Ideale, d.h. es gelte $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Sei $\pi_i : R \to R/\mathfrak{a}_i$ die kanonische Projektion. Dann ist der Homomorphismus

$$\begin{aligned} \varphi : R &\to \prod_{i=1}^{n} R/\mathfrak{a}_i \\ x &\mapsto (\pi_1(x), \ldots, \pi_n(x)). \end{aligned}$$

surjektiv, und es gilt Kern$\varphi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Daher induziert φ einen Isomorphismus

$$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i,$$

Beweis : $\prod_{i=1}^{n} R/\mathfrak{a}_i$ bezeichnet hier das Produkt von Ringen, also das kartesische Produkt mit komponentenweiser Addition und Multiplikation. Wir zeigen zunächst, dass für alle $j = 1, \ldots, n$ auch die Ideale $\mathfrak{a}_j$ und $\bigcap_{i \neq j} \mathfrak{a}_i$ teilerfremd sind, d.h. dass

$$\mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i = R$$

gilt. Da für alle $i \neq j$ gilt $\mathfrak{a}_j + \mathfrak{a}_i = R$, gibt es für alle $i \neq j$ Elemente $a_i \in \mathfrak{a}_j$ und $a_i' \in \mathfrak{a}_i$ mit $a_i + a_i' = 1$. Somit ist

$$1 = \prod_{i \neq j} (a_i + a_i') = \sum_{i \neq j} a_i r_i + \prod_{i \neq j} a_i'$$

für gewisse $r_i \in R$ nach Ausmultiplizieren. Da alle a_i in $\mathfrak{a}_j$ liegen und $\prod_{i \neq j} a_i' \in \prod_{i \neq j} \mathfrak{a}_i \subset \bigcap_{i \neq j} \mathfrak{a}_i$ ist, folgt $1 \in \mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i$. Somit ist in der Tat $\mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i = R$.
Wir finden also für jedes $j = 1, \ldots, n$ Elemente $d_j \in \mathfrak{a}_j$ und $e_j \in \bigcap_{i \neq j} \mathfrak{a}_i$ mit $d_j + e_j = 1$. Dann ist $\pi_i(e_j) = 0$ für $i \neq j$ und $\pi_j(e_j) = \pi_j(1 - d_j) = \pi_j(1)$.
Jetzt können wir zeigen, dass φ surjektiv ist. Sei $y = (y_1, \ldots, y_n) \in \prod_{i=1}^{n} R/\mathfrak{a}_i$. Wir wählen für alle i ein beliebiges $x_i \in R$ mit $\pi(x_i) = y_i$ und setzen $x = \sum_{i=1}^{n} x_i e_i$. Dann ist

$$\begin{aligned} \varphi(x) &= \left(\pi_1 \left(\sum_{i=1}^{n} x_i e_i \right), \ldots, \pi_n \left(\sum_{i=1}^{n} x_i e_i \right) \right) \\ &= (x_1, \ldots, x_n). \end{aligned}$$

Offenbar ist $\varphi(x) = 0$ genau dann, wenn $\pi_1(x) = \cdots = \pi_n(x) = 0$ ist, d.h. genau dann, wenn $x \in \bigcap_{i=1}^{n} \mathfrak{a}_i$ ist. Somit ist Kern $\varphi = \bigcap_{i=1}^{n} \mathfrak{a}_1$ ist. Die letzte Behauptung folgt aus Korollar 2.17. □

Ist $\mathfrak{a} \subset R$ ein Ideal, so nennen wir $x, a \in R$ kongruent modulo $\mathfrak{a}$ und schreiben $x \equiv y \mod \mathfrak{a}$, wenn die Restklassen $x + \mathfrak{a}$ und $y + \mathfrak{a}$ in $R/\mathfrak{a}$ gleich sind. Also ist $x \equiv y \mod \mathfrak{a}$ genau dann, wenn $x - y \in \mathfrak{a}$ gilt. Für $\mathfrak{a} = (a)$ schreiben wir auch „mod a“ statt „mod $\mathfrak{a}$“.
Dann bedeutet die Surjektivität der Abbildung φ in Satz 2.24, dass es zu beliebigen $x_1, \ldots, x_n \in R$ ein $x \in R$ mit

$$x \equiv x_i \mod \mathfrak{a}_i \text{ für alle } i = 1, \ldots, n$$

gibt.
Für $R = \mathbb{Z}$ sagt der Chinesische Restsatz:

Korollar 2.25 Es seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremde ganze Zahlen. Dann gibt es für alle $x_1, \ldots, x_n \in \mathbb{Z}$ ein $x \in \mathbb{Z}$ mit

$$x \equiv x_i \mod a_i \text{ für alle } i = 1, \ldots, n.$$

Zwei solche Lösungen x und x' sind jeweils kongruent modulo $a_1 \cdots a_n$.

Beweis : Teilerfremde ganze Zahlen $a, b \in \mathbb{Z}$ erzeugen teilerfremde Ideale, d.h. es gilt

$$(a) + (b) = \mathbb{Z}.$$

Wir wissen nämlich, dass jedes Ideal in $\mathbb{Z}$ von der Form $(m) = m\mathbb{Z}$ ist. Also ist $(a) + (b) = (m)$ für ein $m \in \mathbb{Z}$. Aus $(a) \subset (a) + (b) = (m)$ und $(b) \subset (a) + (b) = (m)$ folgt, dass m sowohl a als auch b teilt. Da a und b teilerfremd sind, ist $m = \pm 1$, also $(m) = \mathbb{Z}$.
Ferner gilt für teilerfremde Zahlen $a, b \in \mathbb{Z}$, dass

$$(ab) = (a) \cap (b).$$

ist. Die Inklusion „$\subset$“ ist hier klar. Sei $m \in (a) \cap (b)$, d.h. a und b teilen m. Da a und b teilerfremd sind, folgt ab teilt m, also $m \in (ab)$. Somit ist auch „$\supset$ “gezeigt. Die Behauptung folgt jetzt aus Satz 2.24. □

Viele Eigenschaften des Ringes $\mathbb{Z}$ oder des Polynomrings $K[X]$ beruhen darauf, dass in diesen Ringen eine Division mit Rest möglich ist, vgl. Satz 2.8. Diese Eigenschaft wollen wir jetzt allgemein untersuchen:

Definition 2.26 Ein Integritätsring R mit einer Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}_0$ heißt **euklidischer Ring**, wenn gilt:

Zu allen $f, g \in R$ mit $g \neq 0$ gibt es Elemente $q, r \in R$ mit

$$f = q \cdot g + r \text{ und } (\delta(r) < \delta(g) \text{ oder } r = 0).$$

Die Abbildung δ wird als Grad- oder Normabbildung des euklidischen Rings R bezeichnet.

Beispiel:

i) Jeder Körper ist zusammen mit der Abbildung $\delta = 0$ ein euklidischer Ring.

ii) Ist K ein Körper, so ist $K[X]$ mit der Abbildung $\delta(g) = \text{grad}(g)$ ein euklidischer Ring nach Satz 2.8.

iii) $\mathbb{Z}$ ist ein euklidischer Ring mit $\delta(a) = |a|$ und der gewöhnlichen Division mit Rest.

iv) Wir betrachten $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. $\mathbb{Z}[i]$ ist ein Unterring von $\mathbb{C}$ (ÜA). Wir definieren eine Gradabbildung

$$\begin{aligned} \delta : \mathbb{Z}[i] \setminus \{0\} &\to \mathbb{N} \\ (a + ib) &\mapsto |a + ib|^2 = a^2 + b^2. \end{aligned}$$

Für alle $x, y \in \mathbb{R}$ finden wir offenbar $a, b \in \mathbb{Z}$ mit $|x - a| \leq \frac{1}{2}, |y - b| \leq \frac{1}{2}$. Es sei $z = x + iy \in \mathbb{C}$.

Dann gilt für $a + ib \in \mathbb{Z}[i]$:

$$|z - (a + ib)|^2 = |(x - a) + i(y - b)|^2 \leq 2 \cdot \frac{1}{4} < 1.$$

Insbesondere gibt es für beliebiges $f, g \in \mathbb{Z}[i]$ mit $g \neq 0$ ein $q = a + ib \in \mathbb{Z}[i]$ mit

$$\left| \frac{f}{g} - q \right|^2 < 1.$$

Setzen wir $r = f - qg$, so gilt, falls $r \neq 0$ ist, $\delta(r) = |f - qg|^2 < |g|^2 = \delta(g)$.

$\mathbb{Z}[i]$ heißt der **Ring der ganzen Gauß'schen Zahlen.**

v) Allgemeiner sei $d \neq 0, 1$ eine quadratfreie ganze Zahl, d.h. kein Quadrat eines $n > 1, n \in \mathbb{N}$, ist ein Teiler von d. Dann ist

$$R_d = \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z}, & \text{falls } d \equiv 2, 3 \mod 4 \\ \mathbb{Z} + \frac{1}{2}(1 + \sqrt{d})\mathbb{Z}, & \text{falls } d \equiv 1 \mod 4. \end{cases}$$

ein Unterring von $\mathbb{C}$. Für $d = -1$ gilt $R_{-1} = \mathbb{Z}[i]$. Die Ringe R_d sind in der Zahlentheorie von besonderem Interesse. Insbesondere möchte man wissen, ob R_d euklidisch oder faktoriell (s.u.) ist.

Satz 2.27 Jeder euklidische Ring ist ein Hauptidealring.

Beweis : Es sei $\mathfrak{a} \subset R$ ein Ideal. Wir können annehmen, dass $\mathfrak{a} \neq 0$ ist. Wir wählen unter den Elementen $a \neq 0$ aus $\mathfrak{a}$ eines mit minimalem Grad $\delta(a)$. Jetzt zeigen wir $\mathfrak{a} = (a)$. Die Inklusion „$\supset$“ ist trivial. Sei also $b \in \mathfrak{a}$. Dann können wir b schreiben als $b = q \cdot a + r$ mit $q, r \in R$, so dass $r = 0$ oder $\delta(r) < \delta(a)$ ist. Es ist

$$r = b - q \cdot a \in \mathfrak{a},$$

also gilt aufgrund der Definition von a schon $\delta(r) \geq \delta(a)$, woraus $r = 0$ folgt. Daher ist $b = q \cdot a \in (a)$. □

Korollar 2.28 Die Ringe $\mathbb{Z}, \mathbb{Z}[i]$ und der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe auch Hauptidealringe.

Als nächstes wollen wir Primfaktorzerlegungen in Hauptidealringen studieren. Wir sagen, dass in einem Integritätsring R ein Element $x \in R$ das Element $y \in R$ teilt und schreiben $x \mid y$, falls $y = x \cdot a$ für ein $a \in R$ gilt. Also ist $x \mid y$ äquivalent zu $y \in (x)$. Ist diese Bedingung nicht erfüllt, so schreiben wir $x \nmid y$.

Definition 2.29 Es sei R ein Integritätsring und $p \in R \setminus \{0\}$ keine Einheit

i) p heißt **irreduzibel**, falls für jede Zerlegung $p = xy$ mit $x, y \in R$ gilt: $x \in R^*$ oder $y \in R^*$. Ein nicht irreduzibles Element nennen wir auch **reduzibel**.

ii) p heißt **prim** oder **Primelement**, falls für alle $x, y \in R$ aus $p \mid xy$ schon $p \mid x$ oder $p \mid y$ folgt, mit anderen Worten, falls das Hauptideal (p) ein Primideal ist (ÜA).

Beispiel: In $\mathbb{Z}$ entsprechen die irreduziblen Elemente genau den Primelementen. Dies sind die Zahlen $\pm p, p$ Primzahl.

Bemerkung 2.30 Es sei R ein Integritätsring und $p \in R \setminus \{0\}$ keine Einheit.

i) Ist $(p) \subset R$ ein maximales Ideal, so ist p ein Primelement.

ii) Primelemente sind irreduzibel.

Beweis :

i) Maximale Ideale sind prim nach Satz 2.22.

ii) Sei p ein Primelement und gelte $p = xy$ in R. Dann teilt p das Produkt xy, woraus $p \mid x$ oder $p \mid y$ folgt. Ist $x = pa$, so folgt $p = xy = pay$, also, da R ein Integritätsring ist, $ay = 1$. Somit ist $y \in R^*$. Falls $p \mid y$, so folgt mit demselben Argument $x \in R^*$.

□

In Hauptidealringen gilt sogar

Satz 2.31 Sei R ein Hauptidealring und $p \in R \setminus \{0\}$ keine Einheit. Dann sind äquivalent:

i) p ist irreduzibel.

ii) p ist Primelement.

iii) (p) ist ein maximales Ideal.

Beweis : iii) $\Rightarrow$ ii) $\Rightarrow$ i) folgt allgemein mit Bemerkung 2.30.
i) $\Rightarrow$ iii): Angenommen, p ist irreduzibel und $\mathfrak{a} \subset R$ ist ein Ideal mit $(p) \subset \mathfrak{a}$. Da R ein Hauptidealring ist, ist $\mathfrak{a} = (a)$ für ein $a \in R$. Also existiert ein $c \in R$ mit $p = ac$, woraus $a \in R^*$ oder $c \in R^*$ folgt. Im ersten Fall ist $\mathfrak{a} = (a) = R$, im zweiten Fall ist $\mathfrak{a} = (a) = (p)$. Daher ist (p) maximal □

Als nächstes wollen wir zeigen, dass in Hauptidealringen stets ein Analogon der Primfaktorzerlegung in $\mathbb{Z}$ existiert.

Definition 2.32 i) Ein Element a eines Ringes R besitzt eine **Zerlegung in irreduzible Faktoren**, wenn sich a schreiben lässt als

$$a = \varepsilon p_1 \cdots p_r$$

mit $\varepsilon \in R^*$ und irreduziblen $p_1, \ldots p_r$ in R, $r \in \mathbb{N}_0$.

ii) Wir sagen, $a \in R$ hat eine **eindeutige Zerlegung in irreduzible Faktoren**, falls a eine Zerlegung in irreduzible Faktoren hat, die in folgender Weise eindeutig ist: Sind $a = \varepsilon p_1 \cdots p_r$ und $a = \varepsilon' q_1 \cdots q_s$ zwei Zerlegungen in irreduzible Faktoren, so gilt $r = s$ und nach geeigneter Umnummerierung ist für alle $i = 1, \ldots, r$ das Element p_i assoziiert zu q_i.

iii) Ein Integritätsring R heißt **faktoriell**, falls jedes $a \neq 0$ aus R eine eindeutige Zerlegung in irreduzible Faktoren besitzt.

Satz 2.33 Es sei R ein Integritätsring.

i) R ist faktoriell genau dann, wenn sich jedes Element $a \neq 0$, das keine Einheit ist, als Produkt von Primelementen schreiben kann.

ii) Ist R faktoriell, so ist $a \in R$ genau dann irreduzibel, wenn es prim ist.

Beweis : Wir zeigen zuerst

ii) Alle Primelemente sind irreduzibel nach Bemerkung 2.30. Sei umgekehrt $a \in R$ irreduzibel. Falls $a \mid xy$ gilt, so müssen wir $a \mid x$ oder $a \mid y$ zeigen. Wir können annehmen, dass weder x noch y Einheiten sind. Es seien $x = \varepsilon x_1 \cdots x_r$ und $y = \varepsilon' y_1 \cdots y_s$ Zerlegungen in irreduzible Elemente. Es gibt ein $z \in R$ mit $xy = az$, das wir ebenfalls in irreduzible Elemente zerlegen können. Aus der Eindeutigkeit der Zerlegung folgt dann, dass das irreduzible Element a assoziiert zu einem x_i oder zu einem y_i ist. Also folgt $a \mid x$ oder $a \mid y$.

i) Ist R faktoriell, so ist nach ii) jedes irreduzible Element prim. Daher ist jedes $a \neq 0$, das keine Einheit ist, ein Produkt von Primelementen.

Umgekehrt nehmen wir an, dass sich jede Nichteinheit $a \neq 0$ in R schreiben lässt als

$$a = \pi_1 \cdots \pi_r.$$

mit Primelementen π_i. Da die π_i nach Bemerkung 2.30 irreduzibel sind, ist das insbesondere eine Zerlegung von a in irreduzible Elemente. Gilt $a = \varepsilon p_1 \cdots p_s$ mit $\varepsilon \in R^*$ und $p_1, \ldots, p_s$ irreduzibel, so folgt aus $\pi_1 \mid \varepsilon p_1 \cdots p_s$, dass $\pi_1 \mid \varepsilon$ oder $\pi_1 \mid p_j$ für ein $j = 1, \ldots, s$ gilt. Da π_1 keine Einheit ist, gibt es ein $j = 1, \ldots, s$ und ein $c \in R$ mit $p_j = \pi_1 \cdot c$. Da p_j irreduzibel und $\pi_1 \notin R^*$ ist, folgt hieraus $c \in R^*$. Also ist π_1 assoziiert zu p_j. Da R ein Integritätsring ist, folgt $\pi_2 \cdots \pi_r = \varepsilon' \prod_{i \neq j} p_i$ für ein $\varepsilon' \in R^*$. Setzt man das Verfahren induktiv fort, so ergibt sich die Eindeutigkeit der Zerlegung von a.

□

Korollar 2.34 Jeder Hauptidealring ist faktoriell.
Insbesondere ist also jeder euklidische Ring faktoriell, für jeden Körper K also etwa der Ring $K[X]$.

Für den Beweis dieser Aussage benötigen wir das folgende Lemma.

Lemma 2.35 Jeder Hauptidealring R ist noethersch, d.h. jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset R$ wird stationär in dem Sinne, dass es ein $n \in \mathbb{N}$ mit $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$ gibt.

Beweis : Die Vereinigung $\bigcup_{i\geq 1} \mathfrak{a}_i = \mathfrak{a}$ einer aufsteigenden Kette von Idealen ist ein Ideal in R (ÜA). Nach Voraussetzung existiert ein $a \in R$ mit $\mathfrak{a} = (a)$. Es gibt ein $n \geq 1$ mit $a \in \mathfrak{a}_n$. Also gilt

$$(a) \subset \mathfrak{a}_n \subset \mathfrak{a} = (a),$$

woraus $\mathfrak{a} = \mathfrak{a}_n$ folgt. Somit ist $\mathfrak{a}_i = \mathfrak{a}_n$ für $n \geq i$, die Idealkette wird also stationär. □

Beweis von 2.34 : Es sei S die Menge der Hauptideale in R, die von all denjenigen $a \neq 0$ erzeugt werden, die keine Zerlegung in irreduzible Faktoren besitzen. Ist $S = \emptyset$, so hat jedes $a \neq 0$ in R eine Zerlegung in irreduzible Faktoren. Nach Satz 2.31 lässt sich dann jede Nichteinheit $a \neq 0$ als Produkt von Primelementen schreiben, und nach Satz 2.33 ist R daher faktoriell. Also müssen wir nur $S = \emptyset$ zeigen.
Wir nehmen an, $S \neq \emptyset$. Dann hat S ein maximales Element $\mathfrak{a}$, d.h. für alle Ideale $\mathfrak{b}$ in R mit $\mathfrak{a} \subsetneq \mathfrak{b}$ ist $\mathfrak{b} \notin S$. Gäbe es nämlich kein solches maximales Element, so könnte man eine Kette von Idealen

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_i \subsetneq \ldots$$

für $i \in \mathbb{N}$ konstruieren, so dass alle $\mathfrak{a}_i \in S$ sind. Da R nach Lemma 2.35 noethersch ist, wird diese Kette stationär, d.h. für ein $n \in \mathbb{N}$ ist $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots = \mathfrak{a}_i = \ldots$ Das steht im Widerspruch zur Konstruktion der $\mathfrak{a}_i$.
Das maximale Element $\mathfrak{a}$ von S ist ein Hauptideal, also $\mathfrak{a} = (a)$. Definitionsgemäß kann a keine Einheit und nicht irreduzibel sein. Also können wir a als Produkt $a = bc$ mit $b, c \in R \setminus R^*$ schreiben. Wegen $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$ ist. $(b) \notin S$ und $(c) \notin S$. Somit haben b und c eine Zerlegung in irreduzible Faktoren. Dann hat aber auch das Produkt $a = bc$ eine Zerlegung zu irreduziblen Faktoren, was zu einem Widerspruch führt. □

Man kann die Primfaktorzerlegung in einem faktoriellen Ring R weiter standardisieren, indem man ein Vertretersystem P der Primelemente modulo Assoziiertheit auswählt. Man wählt also aus jeder Äquivalenzklasse bezüglich der Äquivalenzrelation

$$p \sim q \text{ genau dann, wenn } p \text{ assoziiert zu } q \text{ ist,}$$

genau ein Element aus.
Dann hat jedes $a \in R \setminus \{0\}$ eine Zerlegung

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)}$$

mit eindeutig bestimmten $\varepsilon \in R^*$ und $v_p(a) \in \mathbb{N}_0$, so dass fast alle $v_p(a) = 0$ sind.

In $\mathbb{Z}$ etwa nimmt man üblicherweise $P =$ Menge der Primzahlen. In $K[X]$ kann man $P =$ Menge der irreduziblen normierten Polynome nehmen, da $K[X]^* = K^*$ nach Bemerkung 2.7 gilt.

Definition 2.36 Sei R ein Integritätsring und $x_1, \ldots, x_n \in R$.

i) $d \in R$ heißt **größter gemeinsamer Teiler** von $x_1, \ldots, x_n$, d.h. $d = \text{ggT}(x_1, \ldots x_n)$, falls $d \mid x_i$ für alle $i = 1, \ldots, n$ und falls aus $a \mid x_i$ für alle $i = 1, \ldots, n$ schon $a \mid d$ folgt.

ii) $v \in R$ heißt **kleinstes gemeinsames Vielfaches** von $x_1, \ldots, x_n$, d.h. $v = \text{kgV}(x_1, \ldots, x_n)$, falls $x_i \mid v$ für alle $i = 1, \ldots, n$ und falls aus $x_i \mid a$ für alle $i = 1, \ldots, n$ schon $v \mid a$ folgt.

Falls der ggT oder das kgV existieren, so sind sie eindeutig bestimmt bis auf Assoziiertheit (ÜA).

Satz 2.37 Es sei R faktoriell und P ein Vertretersystem der Primelemente von R. Zu beliebigen $x_1, \ldots, x_n \in R$ existieren $\text{ggT}(x_1, \ldots, x_n)$ und $\text{kgV}(x_1, \ldots, x_n)$. Ist $x_i = \varepsilon_i \prod\limits_{p \in P} p^{v_p(x_i)}$ für $i = 1, \ldots, n$, so ist (bis auf Assoziiertheit)

$$\begin{aligned} \text{ggT}(x_1, \ldots, x_n) &= \prod_{p \in P} p^{\min(v_p(x_1), \ldots, v_p(x_n))} \\ \text{kgV}(x_1, \ldots, x_n) &= \prod_{p \in P} p^{\max(v_p(x_1), \ldots, v_p(x_n))} \end{aligned}$$

Beweis : Geht genau wie für $R = \mathbb{Z}$ (ÜA). □

Satz 2.38 Seien $x_1, \ldots, x_n$ Elemente eines Integritätsringes R.

i) Falls $(x_1, \ldots, x_n) = (d)$ ein Hauptideal ist, so ist $d = \text{ggT}(x_1, \ldots, x_n)$.

ii) Falls $(x_1) \cap \cdots \cap (x_n) = (v)$ ein Hauptideal ist, so ist $v = \text{kgV}(x_1, \ldots, x_n)$.

Beweis :

i) Ist $(x_1, \ldots, x_n) = (d)$, so gilt $d \mid x_i$ für alle i. Da $d \in (x_1, \ldots, x_n)$ ist, gilt $d = a_1 x_1 + \cdots + a_n x_n$ für $a_1, \ldots, a_n \in R$. Jeder gemeinsame Teiler der x_i teilt also d.

ii) Ist $(x_1) \cap \cdots \cap (x_n) = (v)$, so ist $v \in (x_i)$ für alle i, d.h. $x_i \mid v$. Falls a ein gemeinsames Vielfaches aller x_i ist, so ist $a \in (x_1) \cap \cdots \cap (x_n) = (v)$, d.h. $v \mid a$.

□

In Euklidischen Ringen gibt es ein konstruktives Verfahren zur Bestimmung des ggT.

Satz 2.39 (Euklidischer Algorithmus) Sei R ein euklidischer Ring. Für $x, y \in R \setminus \{0\}$ betrachten wir die Folge $(z_n)_n \in R$, definiert als

$$\begin{aligned} z_0 &= x \\ z_1 &= y \\ z_{i+1} &= \begin{cases} \text{Rest bei Division von } z_{i-1} \text{ durch } z_i, & \text{falls } z_i \neq 0. \\ 0, & \text{falls } z_i = 0 \end{cases} \end{aligned}$$

Dann gibt es einen kleinsten Index $n \in \mathbb{N}_0$ mit $z_{n+1} = 0$. Für dieses n gilt $z_n = \text{ggT}(x, y)$.

Beweis : Sei $\delta : R \setminus \{0\} \to \mathbb{N}_0$ die Gradabbildung. Definitionsgemäß ist für alle $i \geq 1$ mit $z_i \neq 0$:

$$\delta(z_{i+1}) < \delta(z_i) \text{ oder } z_{i+1} = 0$$

Daher ist die Folge $\delta(z_i)$ streng monoton fallend auf der Menge aller i mit $z_{i+1} \neq 0$. Somit können nur endlich viele $z_{i+1} \neq 0$ sein. Also gibt es ein minimales n mit $z_{n+1} = 0$. Da z_0 und z_1 nicht Null sind, ist $n \geq 1$. Nach Konstruktion gilt $z_0 = q_1 z_1 + z_2,\ z_1 = q_2 z_2 + z_3, \ldots, z_{n-2} = q_{n-1} z_{n-1} + z_n,\ z_{n-1} = q_n z_n$. Daher teilt z_n alle z_i für $0 \leq i \leq n-1$. Insbesondere gilt $z_n \mid x$ und $z_n \mid y$. Ist a ein gemeinsamer Teiler von $x = z_0$ und $y = z_1$, so folgt $x \mid z_2$, $x \mid z_3, \ldots, x \mid z_n$. Daher ist $z_n = \text{ggT}(x, y)$. □

Der Euklidische Algorithmus liefert außer einem ggT d von x und y auch $a, b \in R$ mit $d = ax + by$. Es ist nämlich $z_{n-2} = q_{n-1} z_{n-1} + z_n$, also $z_n = q_{n-1} z_{n-1} + z_{n-2}$. Hier kann man jetzt induktiv die Gleichungen $z_i = q_{i-1} z_{i-1} + z_{i-2}$ für $i \leq n-1$ einsetzen.

Beispiel: Wir haben gesehen, dass euklidische Ringe Hauptidealringe und dass Hauptidealringe faktoriell sind. Insbesondere ist für jeden Körper K der Polynomring $K[X]$ ein Hauptidealring. Jedes irreduzible Polynom $f \in K[X]$ erzeugt also nach Satz 2.31 ein maximales Ideal, d.h.

$$L = K[X]/(f)$$

ist ein Körper. Der kanonische Ringhomomorphismus

$$K \to K[X] \to K[X]/f$$

ist nach Bemerkung 2.13 injektiv. Man kann K also als Teilkörper von L auffassen. Ist $a = X + (f)$ die Restklasse von X in L, so gilt: $f(a)$ (ausgerechnet in L) stimmt mit

der Restklasse von $f(X)$ überein, d.h. $f(a) = 0$. In L existiert also eine Nullstelle des irreduziblen Polynoms f. Beispielsweise gilt

$$\begin{aligned} \mathbb{R}[X]/(X^2+1) &\simeq \mathbb{C} \\ \text{vermöge } X &\mapsto i. \end{aligned}$$

Solche Körpererweiterungen werden wir später noch genauer studieren.

3 Polynomringe

Sei R ein Ring. Durch Iteration kann man für n Unbekannte $X_1, \ldots, X_n$, den Polynomring über R in n Variablen konstruieren:

$$\begin{aligned} R[X_1, X_2] &= (R[X_1])[X_2] \\ R[X_1, X_2, X_3] &= (R[X_1, X_2])[X_3] \\ &\vdots \\ R[X_1, X_2, \ldots, X_n] &= (R[X_1, \ldots, X_{n-1}])[X_n]. \end{aligned}$$

Die Elemente in $R[X_1, \ldots, X_n]$ sind genau die formalen Summen

$$f(X_1, \ldots, X_n) = \sum_{I=(i_1,\ldots,i_n)\in\mathbb{N}_0^n} a_I X_1^{i_1} \cdots X_n^{i_n}$$

mit Koeffizienten $a_I \in R$, die fast alle verschwinden.

Lemma 3.1 Ist R ein Integritätsring, so auch $R[X_1, \ldots, X_n]$.

Beweis : Das folgt mit Induktion aus Bemerkung 2.7, wo wir gesehen haben, dass für einen Integritätsring R auch $R[X]$ ein Integritätsring ist □

Für $I = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ sei $|I| = i_1 + \cdots + i_n$. Außerdem schreiben wir $X^I = X_1^{i_1} \cdots X_n^{i_n}$. Dann nennen wir für $f = \sum_{I\in\mathbb{N}_0^n} a_I X_1^{i_1} \cdots X_n^{i_n} = \sum_{I\in\mathbb{N}_0^n} a_I X^I$ in $R[X_1, \ldots, X_n]$ das Polynom

$$f_k := \sum_{|I|=k} a_I X^I$$

den homogenen Bestandteil von f vom Grad k für alle $k \geq 0$. f heißt homogen vom Grad k, falls $f = f_k$ gilt. Für jedes homogene Polynom $f \neq 0$ ist der Grad eindeutig bestimmt, das Nullpolynom jedoch ist homogen vor jedem Grad $k \geq 0$.

Ferner heißt

$$\text{grad}(f) = \begin{cases} \max\{k : f_k \neq 0\} = \max\{|I| : a_I \neq 0\}, & f \neq 0 \\ -\infty & , f = 0 \end{cases}$$

der Totalgrad von f. Dann gilt

Satz 3.2 Seien $f, g \in R[X_1, \ldots, X_n]$. Dann gilt

$$\begin{aligned} \text{grad}(f+g) &\leq \max(\text{grad}(f), \text{grad}(g)) \\ \text{grad}(fg) &\leq \text{grad}(f) + \text{grad}(g) \end{aligned}$$

und sogar

$$\text{grad}(fg) = \text{grad}(f) + \text{grad}(g),$$

falls R ein Integritätsring ist.

Beweis : Ohne Einschränkung sind f und g ungleich Null. Seien $f = \sum_{k=0}^{r} f_k$ und $g = \sum_{k=0}^{s} g_k$ die Zerlegungen in homogene Summanden, wobei $r = \text{grad}(f)$ und $s = \text{grad}(g)$ sei. Dann folgt sofort $\text{grad}(f+g) \leq \max(r, s)$. Außerdem ist $fg = f_r g_s +$ (homogene Bestandteile vom Grad $< rs$). Also ist $\text{grad}(f \cdot g) \leq r + s = \text{grad}(f) + \text{grad}(g)$. Ist R ein Integritätsring, so folgt aus $f_r \neq 0$ und $g_s \neq 0$ nach Lemma 3.1 auch $f_r g_s \neq 0$, also grad $(fg) = r + s$. □

Korollar 3.3 Ist R ein Integritätsring, so gilt

$$(R[X_1, \ldots, X_n])^* = R^*.$$

Beweis : Das folgt sofort aus der letzten Formel von Satz 3.2 □

Satz 3.4 Es sei $\psi : R \to R'$ ein Ringhomomorphismus und $c_1, \ldots, c_n \in R'$. Dann existiert genau ein Ringhomomorphismus $\varphi : R[X_1, \ldots, X_n] \to R'$ mit $\varphi(X_i) = c_i$ für $i = 1, \ldots, n$ und $\varphi|_R = \psi$.

Beweis : Für $f = \sum_{I \in \mathbb{N}_0^n} a_I X^I \in R[X_1, \ldots, X_n]$ definieren wir $\varphi(f) = \sum_I \psi(a_I) c_1^{i_1} \cdots c_n^{i_n} \in R'$. Man rechnet leicht nach, dass φ ein Ringhomomorphismus ist (vgl. Lemma 2.5). Ist $\varphi' : R[X_1, \ldots, X_n] \to R'$ ein Ringhomomorphismus mit $\varphi'|_R = \psi$ und $\varphi'(X_i) = c_i$, so muss $\varphi'(f) = \sum_I \psi(a_I) c_1^{i_1} \cdots c_n^{i_n}$ gelten, da φ' mit der Addition und der Multiplikation vertauscht. Das zeigt die Eindeutigkeit □

Die Abbildung φ aus Satz 3.4 nennt man Einsetzungshomomorphismus. Ist R ein Unterring von R' und $\psi : R \hookrightarrow R'$ die Inklusion, so bezeichnen wir das Bild von $f = \sum a_I X^I$ auch mit

$$f(c_1, \ldots, c_n) = \sum_I a_I c_1^{i_1} \cdots c_n^{i_n}.$$

Gilt $f(c_1, \ldots, c_n) = 0$, so heißt $(c_1, \ldots, c_n)$ Nullstelle von f. Ferner schreiben wir

$$\begin{aligned} R[c_1, \ldots, c_n] &:= \varphi(R[X_1, \ldots, X_n]) \\ &= \left\{ \sum_{I \in \mathbb{N}_0^n} a_I c_1^{i_1} \cdots c_n^{i_n} : a_I \in R, \text{ fast alle } a_I = 0 \right\} \end{aligned}$$

$R[c_1, \ldots, c_n]$ ist der kleinste Unterring von R', der R und die Elemente $c_1, \ldots, c_n$ enthält (ÜA). (Beispiel: $\mathbb{Z}[i]$).

Definition 3.5 Es sei $R \subset R'$ eine Ringerweiterung und $c_1, \ldots, c_n \in R'$. Das System $(c_1, \ldots, c_n)$ heißt **algebraisch unabhängig** oder **transzendent** über R, falls der Einsetzungshomomorphismus $\varphi : R[X_1, \ldots, X_n] \to R'$ mit $\varphi(X_i) = c_i$ injektiv ist und somit einen Isomorphismus $R[X_1, \ldots, X_n] \xrightarrow{\sim} R[c_1, \ldots, c_n]$ induziert. Andernfalls heißt $(c_1, \ldots, c_n)$ **algebraisch abhängig.**

Beispiel:

i) $(1, i)$ ist algebraisch abhängig über $\mathbb{Z}$.

ii) Die Zahl $\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$.

Ist $R' = R/\mathfrak{a}$ für ein Ideal $\mathfrak{a}$, so gibt es einen Einsetzungshomomorphismus

$$\varphi : R[X_1, \ldots, X_n] \to (R/\mathfrak{a})[X_1, \ldots, X_n],$$

der die kanonische Projektion $R \to R/\mathfrak{a}$ fortsetzt und X_i auf X_i abbildet. φ reduziert alle Koeffizienten eines Polynoms modulo dem Ideal $\mathfrak{a}$. So können wir etwa für jede Primzahl p den Homomorphismus $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ betrachten.

Man kann auch Polynome in unendlich vielen Variablen betrachten. Ist $\mathcal{X} = (X_\sigma)_{\sigma \in \Sigma}$ ein durch eine beliebige Indexmenge Σ indiziertes System von Unbestimmten, so besteht $R[\mathcal{X}]$ aus allen formalen Summen $\sum_{I \in \mathbb{N}_0^{(\Sigma)}} a_I \mathcal{X}^I$, wobei $\mathbb{N}_0^{(\Sigma)} = \{I = (i_\sigma)_{\sigma \in \Sigma} \in \mathbb{N}_0^\Sigma : i_\sigma = 0 \text{ für fast alle } \sigma\}$ und $\mathcal{X}^I = \prod_\sigma X_\sigma^{i_\sigma}$ gesetzt wird, und die $a_I \in R$ fast alle verschwinden.

Wir setzen

$$\sum_{I\in\mathbb{N}_0^{(\Sigma)}} a_I\mathcal{X}^I + \sum_{I\in\mathbb{N}_0^{(\Sigma)}} b_I\mathcal{X}^I = \sum_{I\in\mathbb{N}_0^{(\Sigma)}} (a_I+b_I)\mathcal{X}^I$$

und

$$\left(\sum_{I\in\mathbb{N}_0^{(\Sigma)}} a_I\mathcal{X}^I\right)\cdot\left(\sum_{I\in\mathbb{N}_0^{(\Sigma)}} b_I\mathcal{X}^I\right) = \sum_{I\in\mathbb{N}_0^{(\Sigma)}} c_I\mathcal{X}^I$$

mit $c_I = \sum_{J+K=I} a_J b_K$, wobei für $J, K \in \mathbb{N}_0^{(\Sigma)}$ die Summe $J+K \in \mathbb{N}_0^{(\Sigma)}$ komponentenweise definiert ist. Dann ist $R[\mathcal{X}]$ ein Ring, der Polynomring in den Unbestimmten $(X_\sigma)_{\sigma\in\sum}$.
Wir betrachten jetzt wieder den Polynomring $K[X]$ in einer Unbestimmten über dem Körper K. Da $K[X]$ euklidisch ist (Satz 2.8), existieren zu jedem $f \in K[X]$ und zu jedem $\alpha \in K$ Polynome $q, r \in K[X]$ mit

$$f(X) = q(X)(X-\alpha) + r(X)$$

mit $\text{grad}(r) < 1$, d.h. $r \in K$. Dann ist $f(\alpha) = r(\alpha) = r$. Daher ist α eine Nullstelle von f genau dann, wenn $r = 0$ ist. Das Polynom $(X-\alpha)$ ist aus Gradgründen irreduzibel (ÜA). α heißt Nullstelle der Vielfachheit r von f, wenn in der Primfaktorzerlegung von f das Polynom $(X-\alpha)$ genau mit dem Exponenten r auftritt.

Satz 3.6 Es sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geq 0$. Dann hat f, mit Vielfachheiten gezählt, höchstens n Nullstellen in K. f hat genau dann n Nullstellen mit Vielfachheit gezählt, wenn f in $K[X]$ vollständig in Linearfaktoren zerfällt, d.h. sich als Produkt von Polynomen vom Grad 1 schreiben lässt.

Beweis : Da in $K[X]$ der Grad eines Produktes von Polynomen gleich der Summe der Grade der Faktoren ist, folgt die Behauptung aus Gradgründen aus der Primfaktorzerlegung von f. □

Daraus folgt, dass ein Polynom mit mehr Nullstellen als sein Grad angibt, bereits das Nullpolynom sein muss. Ist daher K ein unendlicher Körper, so gilt für $f \in K[X]$:

$$f = 0 \text{ in } K[X] \Leftrightarrow f(\alpha) = 0 \text{ für alle } \alpha \in K.$$

Das stimmt über endlichen Körpern nicht mehr. So ist etwa $f(X) = \prod_{a\in\mathbb{F}_p}(X-a) \in \mathbb{F}_p[X]$ ein Polynom $f \neq 0$ mit $f(\alpha) = 0$ für alle $\alpha \in \mathbb{F}_p$.
Wir können mit Hilfe der Ableitung von f ein Kriterium für das Vorliegen mehrfacher Nullstellen zeigen. Dazu müssen wir zunächst die Ableitung eines Polynoms rein

algebraisch definieren, damit wir über beliebigen Körpern arbeiten können. Dazu betrachten wir

$$\begin{aligned} D : K[X] &\to K[X], \text{ definiert durch} \\ \sum_{i=0}^{n} c_i X^i &\mapsto \sum_{i=1}^{n} i c_i X^{i-1}, \end{aligned}$$

wobei wie üblich $ic_i = \underbrace{c_i + \cdots + c_i}_{i\text{-mal}}$ in K gilt.

D ist kein Ringhomomorphismus, sondern eine Derivation, d.h. es gilt

i) $D(af + bg) = aD(f) + bD(g)$ für $a, b \in K$ und $f, g \in K[X]$ (d.h. D ist linear).

ii) $D(fg) = fD(g) + gD(f)$ (ÜA).

Wir bezeichnen $D(f)$ auch mit $f'(X)$ und nennen f' die erste Ableitung von f.

Satz 3.7 Es sei $f \in K[X]$, $f \neq 0$, ein Polynom mit Koeffizienten in einem Körper K. Eine Nullstelle α von f ist genau dann eine mehrfache Nullstelle (d.h. eine Nullstelle mit Vielfachheit ≥ 2), wenn $f'(\alpha) = 0$ gilt.

Beweis : Es sei r die Vielfachheit der Nullstelle α von f. Dann liefert die Zerlegung von f in irreduzible Faktoren, dass

$$f(X) = (X - \alpha)^r g(X)$$

mit einem $g \in K[X]$, für das $g(\alpha) \neq 0$ gilt. Nun ist

$$\begin{aligned} f'(X) &= D(f) = D((X - \alpha)^r g) \\ &= (X - \alpha)^r g' + r(X - \alpha)^{r-1} g, \end{aligned}$$

denn mit Induktion nach r zeigt man leicht, dass $D((X - \alpha)^r) = r(X - \alpha)^{r-1}$ gilt. Ist α eine mehrfache Nullstelle von f, d.h. gilt $r \geq 2$, so folgt $f'(\alpha) = 0$. Umgekehrt folgt aus $f'(\alpha) = 0$, dass auch $(r(X - \alpha)^{r-1} g)(\alpha) = 0$ ist. Da $g(\alpha) \neq 0$ ist, muss also $r \geq 2$ sein. □

Korollar 3.8 Ein $\alpha \in K$ ist genau dann mehrfache Nullstelle von $f \in K[X] \setminus \{0\}$, wenn α Nullstelle von ggT(f, f') ist.

Beweis : α ist nach Satz 3.7 genau dann mehrfache Nullstelle, wenn $f(\alpha)$ und $f'(\alpha)$ Null sind, also genau dann, wenn $(X - \alpha)$ in der Primfaktorzerlegung von f und f' vorkommt. Nach Satz 2.37 ist das äquivalent dazu, dass $(X - \alpha)$ in der Primfaktorzerlegung von ggT(f, f') vorkommt. □

Beispiel: Ist p eine Primzahl, so hat $f(X) = X^p - X \in \mathbb{F}_p[X]$ keine mehrfachen Nullstellen. Es gilt nämlich

$$f'(X) = p \cdot X^{p-1} - 1 = -1 \text{ in } \mathbb{F}_p[X].$$

Wir steuern jetzt auf den berühmten Satz von Gauß zu, der besagt, dass für einen faktoriellen Ring R auch $R[X]$ faktoriell ist. Zum Beweis benötigen wir noch ein paar technische Hilfsmittel.
Zunächst wollen wir in einem allgemeinen Rahmen Bruchringe konstruieren. Das verallgemeinert die Konstruktion des Körpers $\mathbb{Q}$ aus dem Ring $\mathbb{Z}$ als Menge aller Brüche $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $b \neq 0$. Da im allgemeinen unsere Ringe Nullteiler enthalten können, müssen wir etwas mehr aufpassen.
Sei R ein Ring und S ein multiplikatives Untermonoid von R, d.h. eine Teilmenge $S \subset R$ mit $1 \in S$ und $ab \in S$, falls $a \in S$ und $b \in S$ gilt. Wir definieren eine Relation $\sim$ auf $R \times S$ wie folgt:

$$(a, s) \sim (b, t) \Leftrightarrow \text{ es gibt ein } u \in S \text{ mit } (at - bs)u = 0.$$

Die Relation ist offenbar reflexiv und symmetrisch. Um zu zeigen, dass sie auch transitiv ist, seien $(a, s) \sim (b, t)$ und $(b, t) \sim (c, u)$ in $R \times S$ gegeben. Dann gibt es $v, w \in S$ mit $(at - bs)v = 0$ und $(bu - ct)w = 0$. Daraus folgt (nach Multiplikation der ersten Gleichung mit uw und der zweiten mit sv) $(au - cs)tvw = 0$. Da S multiplikativ abgeschlossen ist, gilt $tvw \in S$, also $(a, s) \sim (c, u)$.
Also ist $\sim$ eine Äquivalenzrelation. Wir bezeichnen mit a/s die Äquivalenzklasse von (a, s), und mit $S^{-1}A$ die Menge der Äquivalenzklassen. Jetzt definieren wir eine Ringstruktur auf $S^{-1}A$, indem wir genauso rechnen, wie wir es von Brüchen gewohnt sind:

$$(a/s) + (b/t) = (at + bs)/st$$

und

$$(a/s)(b/t) = ab/st$$

Lemma 3.9 Diese Definitionen sind unabhängig von der Wahl der Vertreter (a, s) und (b, t). Zusammen mit dieser Addition und Multiplikation wird $S^{-1}R$ zu einem Ring mit Nullelement $0/1$ und Einselement $1/1$. Die Abbildung $f : R \to S^{-1}R$ mit $f(a) = a/1$ ist ein Ringhomomorphismus.

Beweis : Wir zeigen die Unabhängigkeit der Addition von der Vertreterwahl. Sei $(a_1, s_1) \sim (a_2, s_2)$, d.h. $u(a_1 s_2 - a_2 s_1) = 0$ für ein $u \in S$. Wir müssen zeigen, dass für $(b, t) \in R \times S$ gilt: $(a_1 t + bs_1, s_1 t) \sim (a_2 t + bs_2, s_2 t)$. Das folgt aus

$$u(a_1 s_2 t^2 + bs_1 s_2 t - a_2 s_1 t^2 - bs_1 s_2 t) = t^2 u(a_1 s_2 - a_2 s_1) = 0.$$

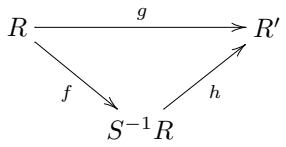
Analog zeigt man die Wohldefiniertheit der Multiplikation. Das Nachrechnen der Ringaxiome ist Routine. Wir betrachten nun die Abbildung f. Offenbar gilt $f(a+b) = (a+b)/1 = (a/1) + (b/1) = f(a) + f(b)$, $f(1) = 1$ und $f(ab) = (ab)/1 = f(a)f(b)$. $\square$

Enthält S Nullteiler von R, so ist f nicht injektiv, denn aus $as = 0$ für $a \in R \setminus \{0\}$ und $s \in S$ folgt $f(a) = a/1 = 0/1 = 0$, da $s(a-0) = sa = 0$ gilt.
Der Ring $S^{-1}R$ heißt auch Bruchring. Ist R ein Integritätsring und $0 \notin S$, so vereinfacht sich die Äquivalenzrelation $\sim$ zum üblichen Kürzen von Brüchen: $(a,s) \sim (b,t) \Leftrightarrow at - bs = 0$. $S^{-1}R$ hat folgende universelle Eigenschaft:

Satz 3.10 Es sei $g : R \to R'$ ein Ringhomomorphismus, so dass für alle $s \in S$ das Bild $g(s)$ eine Einheit in R' ist. Dann gibt es genau einen Ringhomomorphismus

$$h : S^{-1}R \to R',$$

der das Diagramm



kommutativ macht.

Beweis :

i) Eindeutigkeit: Existiert ein h mit $g = h \circ f$, so gilt für alle $a \in R$:

$$g(a) = h(f(a)) = h(a/1).$$

Für jedes $s \in S$ gilt $(s/1)(1/s) = (s/s) = 1$ in $S^{-1}R$, also folgt $1 = h(1) = h(s/1)h(1/s) = g(s)h(1/s)$, d.h. es gilt $h(1/s) = g(s)^{-1}$ in R'. Daraus folgt für alle $a \in R$, $s \in S$: $h(a/s) = h((a/1)(1/s)) = h(a/1)h(1/s) = g(a)g(s)^{-1}$. Somit ist h eindeutig festgelegt.

ii) Existenz: Wir definieren $h(a/s) = g(a)g(s)^{-1}$. Das ist möglich, da $g(s)$ eine Einheit in R' ist. Wir müssen nachrechnen, dass h wohldefiniert ist. Angenommen $a/s = b/t$, d.h. es existiert ein $u \in S$ mit $(at - bs)u = 0$. Dann gilt $(g(a)g(t) - g(b)g(s))g(u) = 0$. Da $g(u)$ eine Einheit in R' ist, folgt $g(a)g(s)^{-1} = g(b)g(t)^{-1}$. Jetzt kann man leicht nachrechnen, dass h ein Ringhomomorhpismus mit $g = h \circ f$ ist.

$\square$

Aus den Rechnungen in diesem Beweis folgt auch, dass für alle $s \in S$ das Element $f(s) \in S^{-1}R$ eine Einheit ist, und dass jedes Element in $S^{-1}R$ die Form $f(a)f(s)^{-1}$ für ein $a \in R$ und ein $s \in S$ hat.

Beispiele:

i) Sei R ein Ring und $a \in R \setminus \{0\}$. Dann ist $S = \{1, a, a^2, \dots\} \subset R$ eine multiplikative Teilmenge. In $S^{-1}R$ sind als Nenner dann genau die Potenzen von a zugelassen.

ii) Sei R ein Ring und $\mathfrak{p} \subset R$ ein Primideal. Dann ist $S = R \setminus \mathfrak{p}$ eine multiplikative Teilmenge von R, da $1 \notin \mathfrak{p}$ liegt und für $a \notin \mathfrak{p}$ und $b \notin \mathfrak{p}$ auch $ab \notin \mathfrak{p}$ gilt. In diesem Fall bezeichnen wir $S^{-1}R$ auch mit $R_{\mathfrak{p}}$ und nennen diesen Ring die Lokalisierung von R nach $\mathfrak{p}$. Als Nenner sind alle Elemente, die nicht in $\mathfrak{p}$ liegen, zugelassen.

iii) Ist R ein Integritätsring, so betrachten wir die multiplikative Teilmenge $S = R \setminus \{0\}$. In diesem Fall vereinfacht sich die Äquivalenzrelation $\sim$ zu

$$(a, s) \sim (b, t) \Leftrightarrow at - bs = 0,$$

also zum gewohnten Kürzen von Brüchen, und der Homomorphismus $f : R \to S^{-1}R$ ist injektiv. Ist $(a/s) \neq 0$ in $S^{-1}R$, d.h. ist $a \in R \setminus \{0\}$ und $s \in S = R \setminus \{0\}$, so liegt auch (s/a) in $S^{-}R$, und es gilt

$$(a/s)(s/a) = (1/0) = 1.$$

Somit ist $S^{-1}R$ sogar ein Körper. Wir bezeichnen ihn mit Quot(R), den Quotientenkörper von R. Vermöge des injektiven Ringhomomorphismus f fassen wir R als Unterring von Quot(R) auf, wir identifzieren also $a \in R$ mit $(a/1) \in$ Quot(R). Wir schreiben ferner einfach $\frac{a}{b}$ für die Äquivalenzklasse a/b.

Für $R = \mathbb{Z}$ ist Quot$(\mathbb{Z}) = \mathbb{Q}$. Ist K ein Körper, so bezeichnen wir mit $K(X) =$ Quot$(K[X])$ und mit $K(X_1, \dots, X_n) =$ Quot$(K[X_1 \dots, X_n])$ die Quotientenkörper der entsprechenden Polynomringe. $K(X_1, \dots, X_n)$ heißt auch Körper der rationalen Funktionen in den Variablen $X_1, \dots, X_n$ über K.

Lemma 3.11 Es sei R ein faktorieller Ring und P ein Vertretersystem der irreduziblen Elemente von R. Dann besitzt jedes $\frac{a}{b} \in$ Quot$(R)^*$ eine eindeutige Darstellung

$$\frac{a}{b} = \varepsilon \prod_{p \in P} p^{v_p}$$

mit $\varepsilon \in R^*$ und $v_p \in \mathbb{Z}$, so dass fast alle $v_p = 0$ sind. Insbesondere ist $\frac{a}{b} \in R$ genau dann, wenn $v_p \geq 0$ für alle $p \in P$.

Beweis : Für $v_p < 0$ ist hier mit p^{v_p} natürlich das Inverse von $p^{-v_p} \in R$ gemeint. Die Existenz der geforderten Darstellung folgt sofort aus der Primfaktorzerlegung von a und b. Gilt $\varepsilon \prod\limits_{p\in P} p^{v_p} = \varepsilon' \prod\limits_{p\in P} p^{v'_p}$, so folgt nach Multiplikation mit $\prod\limits_{p\in P} p^{m_p}$ für

$$m_p = \begin{cases} -\min\{v_p, v'_p\}, & \text{falls } \min\{v_p, v'_p\} < 0 \\ 0, & \text{sonst} \end{cases}$$

dass

$$\varepsilon \prod_{p\in P} p^{v_p+m_p} = \varepsilon' \prod_{p\in P} p^{v'_p+m_p}$$

gilt. Hier stehen auf beiden Seiten Elemente in R. Aus der Eindeutigkeit der Primfaktorzerlegung in R folgt also $\varepsilon = \varepsilon'$ und $v_p + m_p = v'_p + m_p$, also $v_p = v'_p$ für alle $p \in P$. □

In der Situation von Lemma 3.11 schreiben wir, wenn nötig, auch genauer $v_p(\frac{a}{b}) = v_p$ für den Exponenten von p in der Zerlegung von $\frac{a}{b}$. Ferner setzen wir $v_p(0) := \infty$ für alle $p \in P$.
Für ein Polynom $f = \sum\limits_{i=0}^{n} a_i X^i \in \text{Quot}(R)[X]$ definieren wir $v_p(f) := \min\limits_i\{v_p(a_i)\}$. Dann ist $f = 0$ genau dann, wenn $v_p(f) = \infty$. Außerdem gilt $f \in R[X]$ genau dann, wenn $v_p(f) \geq 0$ für alle $p \in P$.

Lemma 3.12 (Lemma von Gauß) Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für alle $f, g \in \text{Quot}(R)[X]$:

$$v_p(fg) = v_p(f) + v_p(g).$$

Beweis : Ist $f = a_0 \in \text{Quot}(R)$ ein konstantes Polynom und $g = \sum\limits_{i=o}^{m} b_i X^i$, so ist

$$\begin{aligned} v_p(fg) &= v_p(a_0 g) \\ &= \min_i\{v_p(a_0 b_i)\} \\ &= \min_i\{v_p(a_0) + v_p(b_i)\} \\ &= v_p(a_0) + \min_i\{v_p(b_i)\} \\ &= v_p(f) + v_p(g). \end{aligned}$$

In diesem Fall stimmt die Behauptung also. Ist $f = \sum\limits_{i=1}^{n} a_i X^i \in \text{Quot}(R)[X]$ ein Polynom vom Grad ≥ 1, so existiert ein $r \in R$ mit $ra_i \in R$ und $rb_i \in R$ für alle Koeffizienten a_i und b_i. Also gilt $rf \in R[X]$ und $rg \in R[X]$. Nach dem oben Gezeigten ist $v_p(rfrg) = 2v_p(r) + v_p(fg)$, also genügt es, die Behauptung für $f, g \in R[X]$ zu zeigen.

Zu $f = \sum_{i=1}^{n} a_i X^i$ betrachten wir $d = \text{ggT}(a_0, \ldots, a_n) \in R$. Dann ist $f = df_1$ für ein $f_1 \in R[X]$, dessen Koeffizienten keinen gemeinsamen Teiler haben. Für jedes $p \in P$ gibt es also einen Koeffizienten von f_1, der nicht von p geteilt wird, d.h. es ist

$$v_p(f_1) = 0$$

Aus der Beobachtung am Anfang des Beweises folgt wieder, dass wir die Behauptung nur für f_1 und g zeigen müssen. Also können wir annehmen, $f, g \in R[X]$ und $v_p(f) = 0, v_p(g) = 0$. Zu zeigen ist $v_p(fg) = 0$. Dazu betrachten wir die Projektion $R \to R/(p)$. Diese vermittelt einen Ringhomomorphismus

$$\varphi : R[X] \to R/(p)[X]$$

mit $\varphi(X) = X$, der einfach Reduktion aller Koeffizienten modulo (p) ist. Kern(φ) besteht aus allen Polynomen, deren sämtliche Koeffizienten in (p) liegen, d.h. Kern$(\varphi) = \{f \in R[X] : v_p(f) > 0\}$. Aus $v_p(f) = 0$ und $v_p(g) = 0$ folgt also $\varphi(f) \neq 0$ und $\varphi(g) \neq 0$. Da p irreduzibel ist, ist p auch ein Primelement nach Satz 2.33, d.h. (p) ist ein Primideal. Mit $R/(p)$ ist nach Bemerkung 2.7 auch $R/(p)[X]$ ein Integritätsring. Also ist

$$\varphi(fg) = \varphi(f)\varphi(g) \neq 0,$$

woraus $v_p(fg) = 0$ folgt. □

Korollar 3.13 Sei R ein faktorieller Ring und $h \in R[X]$ ein normiertes Polynom. Ist dann $h = fg$ eine Zerlegung von h in normierte Polynome $f, g \in \text{Quot}(R)[X]$, so gilt bereits $f, g \in R[X]$.

Beweis : Da $h(X) = a_0 + a_1 X + \cdots + a_d X^d$ mit $a_i \in R$ ist, gilt

$$v_p(h) = \min_i \{v_p(a_i)\} = 0.$$

Analog folgt für die normierten Polynome $f, g \in \text{Quot}(R)[X]$, dass $v_p(f) \leq 0$ und $v_p(g) \leq 0$ ist. Aus dem Lemma von Gauß folgt $v_p(f) + v_p(g) = v_p(h) = 0$, also ist $v_p(f) = v_p(g) = 0$ für alle $p \in P$. Somit liegen alle Koeffizienten von f und g in R, d.h. es gilt $f, g \in R[X]$. □

Ist R faktoriell, so heißt $f \in R[X]$ primitiv, wenn der größte gemeinsame Teiler seiner Koeffizienten 1 ist. Also ist f primitiv genau dann, wenn $v_p(f) = 0$ für alle $p \in P$ gilt, wobei P wieder ein Vertretersystem der irreduziblen Elemente in R ist.
Ist $f \in \text{Quot}(R)[X]$ ein Polynom $\neq 0$, so ist für $a = \prod_{p \in P} p^{v_p(f)} \in \text{Quot}(R)^*$ das Polynom $a^{-1}f$ ein primitives Polynom in $R[X]$, da $v_p(a^{-1}f) = 0$ für alle $p \in P$ gilt. Wir können nun den berühmten Satz von Gauß zeigen:

Satz 3.14 (Gauß) Es sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell. Ein Polynom $q \in R[X]$ ist genau dann ein Primelement in $R[X]$, wenn gilt:

i) q ist ein Primelement in R oder

ii) q ist primitiv in $R[X]$ und ein Primelement in Quot$(R)[X]$.

Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann prim in $R[X]$, wenn es prim in Quot$(R)[X]$ ist.

Beweis : Wir zeigen zunächst, dass die Elemente aus i) und ii) Primelemente in $R[X]$ sind. Ist q ein Primelement von R, so ist R/qR ein Integritätsring. Also ist auch $R[X]/qR[X] \simeq (R/qR)[X]$ ein Integritätsring, d.h. q ist ein Primelement in $R[X]$.
Ist $q \in R[X]$ ein primitives Polynom, das in Quot$(R)[X]$ ein Primelement ist, so nehmen wir $q \mid fg$ in $R[X]$ mit $f, g \in R[X]$ an. Dann gilt $q \mid fg$ auch in Quot$(R)[X]$. Da q in Quot$(R)[X]$ ein Primelement ist, teilt q einen der beiden Faktoren in Quot$(R)[X]$. Wir nehmen an, $q \mid f$ (der andere Fall geht genauso). Dann existiert ein $h \in$ Quot$(R)[X]$ mit $f = qh$. Nach dem Lemma von Gauß gilt für jedes Primelement p von R dann

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

Da $f \in R[X]$ ist, gilt $v_p(f) \geq 0$, da q primitiv ist, gilt $v_p(q) = 0$. Somit ist $v_p(h) \geq 0$ für alle Primelemente p von R, woraus $h \in R[X]$ folgt. Also teilt q das Polynom f auch in $R[X]$. Somit ist q wirklich ein Primelement in $R[X]$.
Jetzt zeigen wir, dass $R[X]$ faktoriell ist und nur die Primelemente aus i) und ii) besitzt. Nach Satz 2.33 genügt es zu zeigen, dass sich jedes $f \in R[X]$, das weder Null noch eine Einheit ist, als Produkt von Primelementen der Gestalt i) oder ii) schreiben lässt. Dazu schreiben wir $f = a\tilde{f}$ mit dem ggT $a \in R$ aller Koeffizienten von f und einem Polynom $\tilde{f} \in R[X]$, das primitiv sein muss, da der ggT seiner Koeffizienten 1 ist. R ist faktoriell, also ist a Produkt von Primelementen in R, d.h. von Elementen vom Typ i). Es genügt also zu zeigen, dass $\tilde{f}$ eine Zerlegung als Produkt von primitiven Polynomen in $R[X]$, die prim in Quot$(R)[X]$ sind, besitzt. Da Quot$(R)[X]$ faktoriell ist (Satz 2.8), können wir $\tilde{f}$ zerlegen als

$$\tilde{f} = cq_1 \cdots q_r$$

mit $c \in$ Quot$(R)[X]^* =$ Quot$(R)^*$ und Primelementen q_i in Quot$(R)[X]$.
Wie oben gezeigt, existiert zu jedem $q_i \in$ Quot$(R)[X]$ ein $\tilde{c}_i \in$ Quot$(R)^*$, so dass $\tilde{q}_i := \tilde{c}_i^{-1} q_i$ ein primitives Polynom in $R[X]$ ist. Also ist für $d = c\tilde{c}_1 \ldots \tilde{c}_r$:

$$\tilde{f} = d\tilde{q}_1 \cdots \tilde{q}_r.$$

Die primitiven Polynome $\tilde{q}_i \in R[X]$ sind jeweils assoziiert zu q_i, also Primelemente in Quot$(R)[X]$ und somit Elemente vom Typ ii). Wir müssen nur noch die Konstante d untersuchen. Für jedes Primelement p von R gilt nach dem Lemma von Gauß:

$$v_p(\tilde{f}) = v_p(d) + v_p(\tilde{q}_1) + \cdots + v_p(\tilde{q}_r)$$

Da $\tilde{f}, \tilde{q}_1, \ldots, \tilde{q}_r$ alle primitiv sind, ist $v_p(\tilde{f}) = v_p(\tilde{q}_1) = \cdots = v_p(\tilde{q}_r) = 0$, woraus $v_p(d) = 0$ folgt. Somit ist d eine Einheit in R und $\tilde{f}$ ein Produkt von Elementen des Typs ii). □

Es sei R ein faktorieller Ring und $K =$ Quot(R) sein Quotientenkörper. Wir wollen jetzt Kriterien dafür herleiten, wann ein Polynom $f \in K[X] \setminus \{0\}$ irreduzibel ist (bzw. prim, das ist ja in faktoriellen Ringen dasselbe).
Zu $f \in K[X]$ existiert ein $c \in K$, so dass $\tilde{f} = cf$ ein primitives Polynom in $R[X]$ ist. Nach dem Satz von Gauss ist f (und somit $\tilde{f}$) genau dann irreduzibel in $K[X]$, wenn $\tilde{f}$ irreduzibel in $R[X]$ ist. Also kann die Irreduzibilität von Polynomen in $K[X]$ auf die Irreduzibilität primitiver Polynome in $R[X]$ zurückgeführt werden.

Satz 3.15 (Eisenstein'sches Irreduzibilitätskriterium) Es sei R ein faktorieller Ring und $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ ein primitives Polynom vom Grad $n > 0$. Außerdem sei $p \in R$ ein Primelement mit $p \nmid a_n,\ p \mid a_i$ für $i < n$ und $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$ und somit auch in Quot$(R)[X]$.

Beweis : Angenommen, f ist reduzibel in $R[X]$, d.h. $f = gh$ mit Polynomen $g = \sum_{i=0}^{r} b_iX^i$, $h = \sum_{i=0}^{s} c_iX^i$ vom Grad $r > 0$ bzw. $s > 0$. Da R ein Integritätsring ist, gilt $n = r + s$. Es folgt außerdem $a_n = b_rc_s$ und $a_0 = b_0c_0$. Daher gilt $p \nmid b_r$ und $p \nmid c_s$ und p teilt genau eine der Zahlen b_0 und c_0. Wir nehmen an, $p \mid b_0$ und $p \nmid c_0$, der andere Fall geht analog. Sei $t < r$ der Index mit $p \mid b_0, \ldots, p \mid b_t$, aber $p \nmid b_{t+1}$. Setzen wir $b_i = 0$ für $i > r$ und $c_i = 0$ für $i > s$, so ist

$$a_{t+1} = b_0c_{t+1} + b_1c_t + \cdots + b_tc_1 + b_{t+1}c_0.$$

p teilt $b_0, \ldots, b_t$, aber weder c_0 noch b_{t+1}, d.h. p teilt alle Summanden bis auf den letzten. Daher kann p kein Teiler von a_{t+1} sein. Nach Voraussetzung folgt daraus $t + 1 = n$, d.h. $r \geq t + 1 = n = r + s$. Das ist ein Widerspruch zu $s > 0$. □

Satz 3.16 (Reduktionskriterium) Es sei R ein faktorieller Ring und $p \in R$ ein Primelement. Ferner sei $0 \neq f \in R[X]$ ein Polynom, dessen höchster Koeffizient nicht von p geteilt wird. Weiter sei

$$\varphi : R[X] \to R/(p)[X]$$

der Homomorphismus, der die Projektion $R \to R/(p)$ fortsetzt und X auf X abbildet. Ist $\varphi(f)$ irreduzibel in $R/(p)[X]$, so ist f irreduzibel in Quot$(R)[X]$. Falls f zusätzlich primitiv ist, so ist f sogar irreduzibel in $R[X]$.

Beweis : Wir nehmen zunächst an, dass $f \in R[X]$ primitiv ist. Ist f reduzibel in $R[X]$, d.h. gibt es eine Zerlegung $f = gh$ mit grad$(g) > 0$ und grad$(h) > 0$ in $R[X]$, so ist das Produkt der höchsten Koeffizienten von g und h gerade der höchste Koeffizient von f. Da dieser nicht von p geteilt wird, werden auch die höchsten Koeffizienten von g und h nicht von p geteilt. Also ist grad$(\varphi(g)) =$ grad$(g) > 0$ und grad$(\varphi(h)) =$ grad$(h) > 0$. Aus

$$\varphi(f) = \varphi(g)\varphi(h)$$

folgt somit, dass f auch reduzibel in $R/(p)[X]$ ist. Daher folgt umgekehrt aus der Irreduzibilität von $\varphi(f)$ die Irreduzibilität von f.
Im allgemeinen Fall schreiben wir $f = c\tilde{f}$ mit $c \in R$ (gewonnen als ggT der Koeffizienten von f) und einem primitiven $\tilde{f} \in R[X]$. Nach Voraussetzung teilt p nicht den höchsten Koeffizienten von f, also weder c noch den höchsten Koeffizienten von $\tilde{f}$. Ist $\varphi(f)$ irreduzibel, so auch $\varphi(\tilde{f})$. Nach dem zuvor Gezeigten folgt, dass $\tilde{f}$ irreduzibel in $R[X]$ ist. Mit dem Satz von Gauß (Satz 3.14) folgt, dass $\tilde{f}$ irreduzibel in Quot$(R)[X]$ ist. Dann ist auch das in Quot$(R)[X]$ zu $\tilde{f}$ assoziierte Polynom f irreduzibel in Quot$(R)[X]$. □

Das Eisenstein'sche Irreduzibililtätskriterium folgt aus dem Reduktionskriterium. Ist f nämlich ein Polynom wie in Satz 3.15 mit einer Zerlegung $f = gh$ in $R[X]$, so ist für $\varphi : R[X] \to R/(p)[X]$:

$$0 \neq \overline{a}_n X^n = \varphi(f) = \varphi(g)\varphi(h).$$

Diese Zerlegung gilt auch in dem faktoriellen Ring Quot$(R/(p))[X]$. Betrachtet man hier die Zerlegungen von $\varphi(g)$ und $\varphi(h)$ in irreduzible Faktoren, so sieht man, dass $\varphi(g)$ und $\varphi(h)$ bis auf Faktoren in $R/(p)$ Potenzen von X sind. Da grad$(\varphi(g)) +$ grad$(\varphi(h)) = n =$ grad $g +$ grad h gilt, so ist entweder eines von ihnen konstant (dann sind wir fertig) oder g und h haben beide die Eigenschaft, dass ihr Absolutkoeffizient durch p teilbar ist. Dann ist aber der Absolutkoeffizient von f (also a_0) durch p^2 teilbar. Dies ist also unmöglich.
Beispiel:

i) Sei K ein Körper und $K = k(t)$ der Körper der rationalen Funktionen in der Variablen t über k. Dann ist für $n \geq 1$ das Polynom $X^n - t \in K[X]$ irreduzibel. Es ist nämlich $K =$ Quot(R) für den faktoriellen Ring $R = k[t]$. Mit dem Primelement $t \in R$ können wir das Eisensteinsche Kriterium auf $X^n - t$ anwenden.

ii) Sei p eine Primzahl. Dann wollen wir zeigen, dass

$$f(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

irreduzibel in $\mathbb{Q}[X]$ ist.

Dazu genügt es zu zeigen, dass $f(X+1)$ irreduzibel ist, denn jede Zerlegung von $f(X)$ gibt auch eine von $f(X+1)$ und umgekehrt. Es ist

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{X+1-1} \\ &= \frac{1}{X}((X+1)^p - 1) \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-1}. \end{aligned}$$

Nun ist für $\nu = 1, \ldots, p-1$: $\binom{p}{\nu} = \frac{p(p-1)\cdots(p-\nu+1)}{1\cdots\nu}$. Im Zähler steht hier der Primfaktor p, im Nenner nicht, daher wird die ganze Zahl $\binom{p}{\nu}$ von p geteilt. Der Absolutkoeffizient ist $\binom{p}{p-1} = p$, also ist das primitive Polynom $f(X+1)$ irreduzibel nach dem Eisensteinschen Kriterium.

iii) Wir zeigen, dass $f(X) = X^3 + 6X^2 - 4X - 1$ irreduzibel in $\mathbb{Q}[X]$ ist. f ist ein primitives Polynom in $\mathbb{Z}[X]$. Reduktion modulo (2) ergibt $X^3 - 1 \in \mathbb{F}_2[X]$. Dieses Polynom wird von $(X-1)$ geteilt, ist also nicht irreduzibel. Daraus können wir erst einmal nichts schließen!

Reduktion modulo (3) ergibt $X^3 - X - 1 \in \mathbb{F}_3[X]$. Das ist irreduzibel, denn es hat keine Nullstelle in $\mathbb{F}_3$, wie man durch Einsetzen von 0, 1, 2 nachprüfen kann. Also ist f irreduzibel in $\mathbb{Q}[X]$.

4 Algebraische Körpererweiterungen

Für jeden Integritätsring R gibt es genau einen Ringhomomorphismus

$$\varphi : \mathbb{Z} \to R$$

(siehe das Beispiel nach Bemerkung 2.13) Dieser bildet n auf $n \cdot 1$ ab. Aufgrund des Homomorphiesatzes 2.16 induziert φ einen injektiven Ringhomomorphismus

$$\overline{\varphi} : \mathbb{Z}/\operatorname{Kern}\varphi \to R$$

Also ist $\mathbb{Z}/\operatorname{Kern}\varphi$ ein Integritätsring. d.h. Kern $\varphi \subset \mathbb{Z}$ ist ein Primideal in $\mathbb{Z}$. Also gilt $\operatorname{Kern}\varphi = (0)$ oder $\operatorname{Kern}\varphi = (p)$ für eine Primzahl p.

Definition 4.1 Die Zahl $p \in \mathbb{N}_0$ mit Kern$\varphi = (p)$ heißt **Charakteristik** des Integritätsrings R:

$$p = \text{ char}(R)$$

Die Charakteristik eines Integritätsring ist also genau dann Null, wenn φ injektiv ist. Das ist etwa für $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ der Fall.

Offenbar gilt char$(\mathbb{F}_p) = p$ für jede Primzahl p.
Wir nennen einen Unterring T eines Körpers K, der selbst wieder ein Körper ist, auch einen Teilkörper von K. Dann gilt char$(T) =$ char(K).
Der Schnitt P aller Teilkörper eines Körpers K ist wieder ein Körper (ÜA). P ist der kleinste in K enthaltene Teilkörper und wird Primkörper von K genannt.

Satz 4.2 Es sei K ein Körper und $P \subset K$ der Primkörper von K. Dann gilt

i) char$(K) = p > 0 \Leftrightarrow P \simeq \mathbb{F}_p$ mit einer Primzahl p.

ii) char$(K) = 0 \Leftrightarrow P \simeq \mathbb{Q}$.

Es gibt also bis auf Isomorphie nur die Primkörper $\mathbb{F}_p$ und $\mathbb{Q}$.

Beweis : In beiden Fällen ist „$\Leftarrow$“ klar.
„$\Rightarrow$“: Wir betrachten $\varphi : \mathbb{Z} \to K$. Ist $\varphi_0 : \mathbb{Z} \to P$ die entsprechende Abbildung für P, so gilt $\varphi = i \circ \varphi_0$ mit $i : P \hookrightarrow K$ der Inklusion. Also ist Bild$\varphi \subset P$. Ist char$(K) = p$ eine Primzahl, so gilt: Bild$\varphi \simeq \mathbb{Z}/$Kern$\varphi = \mathbb{F}_p$ ist ein Körper. Wegen der Minimalität von P folgt $P \subset$ Bildφ. Insgesamt ist $P =$ Bild$\varphi \simeq \mathbb{F}_p$.
Gilt char$(K) = 0$, so ist Bild$\varphi \simeq \mathbb{Z}$. Somit ist mit Bild$\varphi$ auch Quot(Bildφ) in P enthalten. Andererseits folgt wieder aus der Minimalität von P, dass $P =$ Quot(Bildφ) $\simeq \mathbb{Q}$ gilt. □

In Charakteristik p lässt sich manchmal einfacher rechnen als in Charakteristik Null:

Lemma 4.3 Es sei p eine Primzahl und R ein Integritätsring der Charakteristik p. Dann gilt für $a, b \in R$ und $r \in \mathbb{N}$:

$$\begin{aligned} (a+b)^{p^r} &= a^{p^r} + b^{p^r} \text{ und} \\ (a-b)^{p^r} &= a^{p^r} - b^{p^r}. \end{aligned}$$

Beweis : Mit vollständiger Induktion reduziert man auf den Fall $r = 1$. Wir haben am Ende von § 3 schon nachgerechnet, dass p ein Teiler von $\binom{p}{\nu}$ für $\nu = 1, \ldots, p-1$ ist. Da

$$(a+b)^p = a^p + \sum_{\nu=1}^{p-1} \binom{p}{\nu} a^{p-\nu} b^\nu + b^p$$

ist, folgt die erste Behauptung. Die zweite ergibt sich durch Einsetzen von $(-b)$:

$$(a+(-b))^p = a^p + (-b)^p = \begin{cases} a^p + b^p & p \text{ gerade} \\ a^p - b^p & p \text{ ungerade} \end{cases}.$$

Der erste Fall (p gerade) tritt nur ein, wenn $p = 2$ ist. Dann ist $b^p = -b^p$, so dass auch hier die Behauptung folgt. □

Definition 4.4 Ist K ein Körper der Charakteristik $p > 0$, so ist nach Lemma 4.3 die Abbildung

$$\begin{aligned} \sigma : K &\to K \\ a &\mapsto a^p \end{aligned}$$

ein Homomorphismus von Ringen. σ heißt **Frobenius-Homomorphismus** von K.

Wir nennen einen Körper L zusammen mit einem Teilkörper $K \subset L$ auch eine Körpererweiterung. Die Multiplikation auf L lässt sich zu einer Multiplikation

$$K \times L \to L$$

einschränken. Gemeinsam mit dieser Abbildung ist L ein K-Vektorraum (ÜA).
Wir schreiben statt $K \subset L$ auch manchmal L/K für eine Körpererweiterung. Damit ist dann nicht der Faktorring oder die Faktorgruppe gemeint!
E heißt **Zwischenkörper** der Körpererweiterung L/K, falls E ein Körper mit

$$K \subset E \subset L$$

ist.

Definition 4.5 Es sei $K \subset L$ eine Körpererweiterung. Der Grad von L über K ist definiert als die Dimension des K-Vektorraums L. Wir bezeichnen ihn mit $[L : K]$.
Die Körpererweiterung $K \subset L$ heißt **endlich (bzw. unendlich)**, wenn $[L : K]$ endlich (bzw. unendlich) ist. Offenbar ist $[L : K] = 1 \Leftrightarrow L = K$ (ÜA).

Satz 4.6 (Gradsatz) Es seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt

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

falls alle drei Grade endlich sind. Ferner ist $[M : K]$ unendlich genau dann, wenn einer der Grade $[M : L]$ oder $[L : K]$ unendlich ist.

Beweis : Wir nehmen zunächst an, alle Grade seien endlich. Es sei dann $x_1, \ldots, x_m$ eine K-Basis des K-Vektorraums L und $y_1, \ldots, y_n$ eine L-Basis des L-Vektorraums M. Es genügt zu zeigen, dass $x_i y_j$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ eine K-Basis des K-Vektorraums M ist. Wir zeigen zunächst die lineare Unabhängigkeit. Angenommen

$$\sum_{i,j} c_{ij} x_i y_j = 0 \text{ für } c_{ij} \in K$$

Dann gilt

$$\sum_{j=1}^{n} \underbrace{\left(\sum_{i=1}^{m} c_{ij} x_i \right)}_{\in L} y_j = 0$$

Da $y_1, \ldots, y_n$ linear unabhängig über L sind, folgt $\sum_{i=1}^{n} c_{ij} x_i = 0$ für alle $j = 1, \ldots, m$. Da $x_1, \ldots, x_m$ linear unabhängig über K sind, folgt hieraus $c_{ij} = 0$ für alle i und j. Also sind die $x_i y_i$ linear unabhängig über K. Es bleibt zu zeigen, dass sie außerdem ein Erzeugendensystem von M sind. Zunächst hat jedes $z \in M$ eine Darstellung

$$z = \sum_{j=1}^{n} c_j y_j \text{ mit } c_1 \ldots, c_n \in L$$

bezüglich der L-Basis $y_1, \ldots, y_n$ von M. Jedes c_i lässt sich schreiben als

$$c_i = \sum_{i=1}^{m} c_{ij} x_i \text{ mit } c_{ij} \in K$$

bezüglich der K-Basis $x_1, \ldots, x_m$ von L. Also ist $z = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij} x_i y_j$ eine Linearkombination der $x_i y_j$. Damit ist die Behauptung im Fall endlicher Grade gezeigt.
Sind allgemein $x_1, \ldots, x_m$ aus L linear unabhängig über K und $y_1, \ldots, y_n$ aus M linear unabhängig über L, so haben wir oben gezeigt, dass $(x_i y_j)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}$ linear unabhängig über K sind. Also folgt aus $[L : K] \geq m$ und $[M : L] \geq n$, dass $[M : K] \geq m \cdot n$ ist. Also ist $[M : K]$ unendlich, falls einer der Grade $[L : K]$ oder $[M : L]$ dies ist. Sind umgekehrt $[L : K]$ und $[M : L]$ beide endlich, so haben wir oben gezeigt, dass dann auch $[M : K]$ endlich ist. □

Korollar 4.7 Sind $K \subset L \subset M$ Körpererweiterungen und ist $p = [M : K]$ eine Primzahl, so folgt $L = K$ oder $L = M$.

Beweis : $[M : L]$ und $[L : K]$ sind nach Satz 4.6 Teiler von p. □

Beispiel:

i) $\mathbb{R} \subset \mathbb{C}$ ist eine endliche Körpererweiterung; $[\mathbb{C} : \mathbb{R}] = 2$.

ii) $\mathbb{Q} \subset \mathbb{R}$ ist eine unendliche Körpererweiterung, ebenso $K \subset K(X) = \text{Quot}(K[X])$ für einen beliebigen Körper K.

Definition 4.8 Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$. Dann heißt α algebraisch über K, wenn α eine algebraische Gleichung

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha + c_n = 0$$

mit $c_1 \ldots, c_n \in K$ erfüllt. Es gibt also ein normiertes Polynom $f \in K[X]$, so dass das Bild von f unter dem Einsetzungshomomorphismus $\varphi : K[X] \to L$, $\varphi(g) = g(\alpha)$, verschwindet. α ist daher algebraisch über K genau dann, wenn φ nicht injektiv ist.
Ist α nicht algebraisch über K, so heißt α transzendent über K.
Eine Körpererweiterung $K \subset L$ heißt **algebraisch**, falls jedes $\alpha \in L$ algebraisch über K ist.

Beispiel:

1) $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ und über $\mathbb{Q}$, denn i ist Nullstelle von $X^2+1 \in \mathbb{Q}[X]$.

2) Die reellen Zahlen π und e sind transzendent über $\mathbb{Q}$.

Lemma 4.9 Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes normiertes Polynom kleinsten Grades $f \in K[X]$ mit $f(\alpha) = 0$.
Es gilt Kern $\varphi = (f)$ für den Einsetzungshomomorphismus $\varphi : K[X] \to L$, $\varphi(g) = g(\alpha)$. Insbesondere ist f prim, also irreduzibel. f heißt das Minimalpolynom von α über K. Wir schreiben auch $f = \text{Mipo}_K(\alpha)$.

Beweis : Da $K[X]$ ein Hauptidealring ist, gibt es ein $f \in K[X]$ mit Kern$\varphi = (f)$. Da α algebraisch ist, gilt $f \neq 0$. Der Erzeuger f ist bis auf einen Faktor in K^* eindeutig bestimmt. Daher gibt es genau ein normiertes f mit Kern$\varphi = (f)$. Dies ist das eindeutig bestimmte normierte Polynom kleinsten Grades mit $f(\alpha) = 0$. Bild$\varphi \subset L$ ist ein Integritätsring, somit ist Kern$\varphi = (f)$ ein Primideal, d.h. f ein Primelement und somit irreduzibel. □

Satz 4.10 Es sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K mit $f = \text{Mipo}_K(\alpha)$. Bezeichnet $K[\alpha]$ den von α und K erzeugten Unterring von L, also

das Bild des Einsetzungshomomorphismus $\varphi : K[X] \to L$, $\varphi(g) = g(\alpha)$, so induziert φ einen Isomorphismus

$$K[X]/(f) \simeq K[\alpha]$$

$K \subset K[\alpha]$ ist eine Körpererweiterung vom Grad$[K[\alpha] : K] = \text{grad}(f)$. Wir bezeichnen den Körper $K[\alpha]$ auch mit $K(\alpha)$ (siehe unten).

Beweis : Den Ring $K[\alpha]$ haben wir nach Satz 3.4 definiert. Es ist

$$K[\alpha] = \text{Bild}(\varphi) \simeq K[X]/\text{Kern}\varphi$$

nach dem Homomorphiesatz. Also ist $K[X]/(f) \simeq K[\alpha]$. Da $f \neq 0$ ein Primelement in einem Hauptidealring ist, ist nach Satz 2.31 (f) sogar maximal, d.h. $K[X]/(f)$ und $K[\alpha]$ sind Körper. Wir müssen noch

$$\dim_K(K[X]/(f)) = \text{grad}(f)$$

zeigen. Sei $f = X^n + c_1X^{n-1} + \cdots + c_n$ ein Polynom vom Grad n. Wir behaupten, dass die Restklassen $1, \overline{X}, \ldots, \overline{X}^{n-1}$ von $1, X, \ldots, X^{n-1}$ modulo (f) eine K-Basis von $K[X]/(f)$ bilden. Ist $\overline{g} \in K[X]/(f)$ die Restklasse eines beliebigen $g \in K[X]$, so ist $g = qf + r$ mit einem Polynom r vom Grad $< n$. In $K[X]/(f)$ gilt also $\overline{g} = \overline{r}$. Also ist $\overline{g}$ eine Linearkombination von $1, \overline{X}, \ldots, \overline{X}^{n-1}$. Somit bilden $1, \overline{X}, \ldots, \overline{X}^{n-1}$ ein Erzeugendensystem von $K[X]/(f)$ über K.
Gilt $\sum_{i=0}^{n-1} \alpha_i \overline{X}^i = 0$ in $K[X]/(f)$, so liegt das Polynom $\sum_{i=0}^{n-1} \alpha_i X_i$ in (f), ist also ein Vielfaches von f. Da grad $\left(\sum_{i=0}^{n-1} \alpha_i X_i\right) < n = \text{grad}(f)$ gilt, muss $\sum_{i=0}^{n-1} \alpha_i X_i = 0$ sein. Somit ist $\alpha_0 = \cdots = \alpha_{n-1} = 0$. Also sind $1, \overline{X}, \ldots, \overline{X}^{n-1}$ auch linear unabhängig und daher eine Basis. Daher gilt $\dim_K(K[X]/(f)) = n = \text{grad}(f)$. □

Unter $\varphi : K[X]/(f) \xrightarrow{\sim} K[\alpha]$ wird $\overline{X}^i$ auf α^i abgebildet. Daher folgt aus dem obigen Beweis, dass $1, \alpha, \ldots, \alpha^{n-1}$ eine K-Basis von $K[\alpha]$ ist.
Beispiel: Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist $\sqrt[n]{p} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, da $\sqrt[n]{p}$ Nullstelle von

$$f = X^n - p \in \mathbb{Q}[X]$$

ist. f ist irreduzibel nach Eisenstein und normiert, also folgt $f = \text{Mipo}_{\mathbb{Q}}(\sqrt[n]{p})$ (ÜA). Somit gilt $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \text{grad}(f) = n$. Da $\mathbb{R}$ alle Zahlen $\sqrt[n]{p}$ enthält, folgt insbesondere, dass $\mathbb{Q} \subset \mathbb{R}$ eine unendliche Körpererweiterung ist.

Satz 4.11 Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.

Beweis : Es sei $[L : K] = n$ und $\alpha \in L$. Dann müssen die $(n+1)$ Elemente $1, \alpha, \alpha^2, \ldots, \alpha^n$ in dem K-Vektorraum L linear abhängig sein. Es gibt also $c_0, \ldots, c_n \in K$, nicht alle 0, mit

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

Ist i der kleinste Index mit $c_i \neq 0$, so kann man diese Gleichung durch c_i teilen und erhält eine algebraische Gleichung

$$\alpha^{n-i} + \cdots + \frac{c_{n-1}}{c_i}\alpha + \frac{c_n}{c_i} = 0.$$

Daher ist α algebraisch über K. □

Die Umkehrung dieses Satzes ist nicht richtig, wie wir weiter unten sehen werden.
Ist $K \subset L$ eine Körpererweiterung und $\mathfrak{a} = (a_i)_{i \in I}$ ein System von Elementen aus L, so sei

$$K(\mathfrak{a}) = \bigcap_{\substack{M \subset L \text{ Teilkörper} \\ K \subset M, a_i \in M \forall i \in I}} M \subset L.$$

$K(\mathfrak{a})$ ist ein Teilkörper von L (ÜA). Ferner ist $K(\mathfrak{a})$ der kleinste Teilkörper von L, der K und alle a_i enthält, d.h. er ist in jedem Teilkörper $M \subset L$ mit dieser Eigenschaft enthalten.
Für eine Körpererweiterung $K \subset L$ existiert immer ein System $\mathfrak{a}$ mit $L = K(\mathfrak{a})$, etwa das System $\mathfrak{a}$ aller Elemente aus L.

Definition 4.12 i) Eine Körpererweiterung $K \subset L$ heißt **einfach**, falls es ein $\alpha \in L$ mit $L = K(\alpha)$ gibt. Der Grad $[K(\alpha) : K]$ wird auch als Grad von α übers K bezeichnet.

ii) Eine Körpererweiterung L/K heßt **endlich erzeugt**, wenn es endlich viele $\alpha_1, \ldots, \alpha_n \in L$ gibt mit $L = K(\alpha_1, \ldots, \alpha_n)$.

Eine endlich erzeugte Körpererweiterung ist im allgemeinen nicht algebraisch, also auch nicht endlich. Ist $L = K(\alpha_1, \ldots, \alpha_n)$ endlich erzeugt, so enthält L den Ring $K[\alpha_1, \ldots, \alpha_n]$ (also das Bild des Einsetzungshomomorphismus $K[X_1, \ldots, X_n] \to L$), denn die Elemente in $K[\alpha_1, \ldots, \alpha_n]$ sind polynomiale Ausdrücke in $\alpha_1, \ldots, \alpha_n$. Daher ist auch Quot$(K[\alpha_1, \ldots, \alpha_n]) \subset L$ (ÜA). Umgekehrt ist Quot $(K[\alpha_1, \ldots, \alpha_n])$ ein Teilkörper von L, der K und alle α_i enthält, also gilt auch die andere Inklusion. Insgesamt folgt

$$K(\alpha_1, \ldots, \alpha_n) = \text{Quot}(K[\alpha_1, \ldots, \alpha_n])$$

Satz 4.13 Es sei $L = K(\alpha_1, \dots \alpha_n)$ eine endlich erzeugte Körpererweiterung von K. Sind $\alpha_1, \dots \alpha_n$ algebraisch über K, so gilt:

i) $L = K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$

ii) L ist eine endliche und somit eine algebraische Körpererweiterung von K.

Beweis : durch Induktion nach n.
Ist $n = 1$, so folgt die Behauptung aus Satz 4.10 und Satz 4.11.
Sei also $n > 1$. Nach Induktionsvoraussetzung ist $K(\alpha_1, \dots, \alpha_{n-1}) = K[\alpha_1, \dots \alpha_{n-1}]$ eine endliche Körpererweiterung von K. Da α_n erst recht algebraisch über $K[\alpha_1, \dots, \alpha_{n-1}]$ ist, ist nach Satz 4.10 $K[\alpha_1, \dots \alpha_{n-1}][\alpha_n]$ ein Körper, und zwar eine endliche Erweiterung von $K[\alpha_1 \dots, \alpha_{n-1}]$. Es ist $K[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] \simeq K[\alpha_1, \dots, \alpha_n]$ (ÜA). Also ist $K[\alpha_1, \dots \alpha_n]$ ein Körper und daher gleich seinem Quotientenkörper $K(\alpha_1, \dots, \alpha_n)$, woraus i) folgt.
Da $K[\alpha_1, \dots, \alpha_n]$ endlich über $K[\alpha_1, \dots, \alpha_{n-1}]$ und $K[\alpha_1, \dots, \alpha_{n-1}]$ endlich über K ist, folgt ii) mit Satz 4.6. □

Aus dem Satz folgt, dass eine einfache Körpererweiterung L/K, die von einem $\alpha \in L$ erzeugt wird, das algebraisch über K ist, selbst algebraisch ist. Jedes Element $\beta \in L = K(\alpha)$ ist also algebraisch, d.h. es genügt einer algebraischen Gleichung.

Korollar 4.14 Es sei L/K eine Körpererweiterung. Dann sind äquivalent

i) L/K ist endlich

ii) L wird über K von endlich vielen algebraischen Elementen erzeugt.

iii) L ist eine endlich erzeugte algebraische Körpererweiterung von K.

Beweis : i) $\Rightarrow$ ii). Ist $\alpha_1, \dots, \alpha_n$ eine K-Basis von L, so ist offenbar $L = K(\alpha_1, \dots, \alpha_n)$, d.h. L wird über K von endlich vielen Elementen erzeugt, die nach Satz 4.11 algebraisch sind.
ii) $\Rightarrow$ iii) und ii) $\Rightarrow$ i) folgen aus Satz 4.13.
iii) $\Rightarrow$ ii) ist klar. □

Ist $\mathfrak{a} = (\alpha_i)_{i \in I}$ ein Erzeugendensystem einer Körpererweiterung L/K, so ist L die Vereinigung aller Teilkörper $K(\alpha_{i_1}, \dots, \alpha_{i_n})$ für $\{i_1, \dots, i_n\} \subset I$, $n \in \mathbb{N}$. Die Vereinigung all dieser Teilkörper ist nämlich ein Teilkörper von L (ÜA), der offenbar K und alle α_i enthält.

Korollar 4.15 Es sei L/K eine Körpererweiterung. Dann sind äquivalent:

i) L/K algebraisch

ii) $L = K(\mathfrak{a})$, $\mathfrak{a} = (\alpha_i)_{i\in I}$ ein System algebraischer Elemente $\alpha_i \in L$.

Beweis : i) $\Rightarrow$ ii) Da alle $\alpha \in L$ algebraisch über K sind, gilt ii) etwa mit dem System aller $\alpha \in L$.
ii) $\Rightarrow$ i). Für endlich viele $\alpha_{i_1}, \ldots, \alpha_{i_n}$ ist nach Satz 4.13 $K(\alpha_{i_1}, \ldots \alpha_{i_n})$ eine algebraische Körpererweiterung von K. L ist als Vereinigung aller $K(\alpha_{i_1}, \ldots, \alpha_{i_n})$ für $\{i_1, \ldots, i_n\} \subset I$ ebenfalls algebraisch über K. □

Satz 4.16 Es seien $K \subset L \subset M$ Körpererweiterungen. Ist $\alpha \in M$ algebraisch über L und L/K algebraisch, so ist α auch algebraisch über K. Insbesondere ist M/K genau dann algebraisch, wenn M/L und L/K algebraisch sind.

Beweis : Angenommen, L/K ist algebraisch. Sei $\alpha \in M$ algebraisch über L und $f(X) = X^n + c_1X^{n-1} + \cdots + c_{n-1}X + c_n \in L[X]$ das Minimalpolynom von α über L. Da alle Koeffizienten von f in $K(c_1, \ldots, c_n)$ liegen, ist α auch algebraisch über dem Teilkörper $K(c_1, \ldots, c_n) \subset L$. Nach Satz 4.10 folgt

$$[K(c_1, \ldots, c_n, \alpha) : K(c_1, \ldots, c_n] < \infty.$$

Da nach Satz 4.13 $K(c_1, \ldots, c_n)$ eine endliche Erweiterung von K ist, ist nach dem Gradsatz 4.6 auch $K(c_1, \ldots, c_n, \alpha)$ eine endliche Erweiterung von K, also algebraisch nach Satz 4.11. Daher ist α algebraisch über K.
Somit ist mit M/L und L/K auch M/K eine algebraische Körpererweiterung. Ist umgekehrt M/K algebraisch, so folgt sofort aus den Definitionen, dass M/L und L/K algebraisch sind (ÜA). □

Beispiel: Es sei $L = \{\alpha \in \mathbb{C} : \alpha \text{ ist algebraisch über } \mathbb{Q}\}$. L ist ein Teilkörper von $\mathbb{C}$, denn für $\alpha, \beta \in L$ wird $\mathbb{Q}(\alpha, \beta)$ von algebraischen Elementen erzeugt, ist also nach Satz 4.13 eine algebraische Erweiterung von $\mathbb{Q}$. Somit ist $\alpha + \beta \in L$, $\alpha\beta \in L$. Definitionsgemäß ist $L/\mathbb{Q}$ algebraisch.
Für jede Primzahl p und alle $n \in \mathbb{N}$ ist $\sqrt[n]{p} \in L$, also $\mathbb{Q}(\sqrt[n]{p}) \subset L$. Wir haben oben gesehen, dass $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$ ist. Also enthält $L/\mathbb{Q}$ Zwischenkörper von beliebig hohem Grad $n \in \mathbb{N}$, daher ist $[L : \mathbb{Q}] = \infty$. Wir nennen L den algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$ und schreiben $L = \overline{\mathbb{Q}}$.

Wir wollen nun zu jedem Körper K einen algebraischen Abschluss $\overline{K}$ konstruieren. Zuerst zeigen wir, wie man für ein nicht-konstantes Polynom $f \in K[X]$ einen Erweiterungskörper L/K konstruiert, so dass f eine Nullstelle in L besitzt.

Satz 4.17 (Verfahrenvon Kronecker) Es sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad ≥ 1. Dann existiert eine algebraische Körpererweiterung L/K, so dass f eine Nullstelle in L besitzt. Ist f irreduzibel, so hat

$$L := K[X]/(f)$$

diese Eigenschaft.

Beweis : Ist f irreduzibel, so ist (f) nach Satz 2.31 ein maximales Ideal im Hauptidealring $K[X]$. Also ist $L = K[X]/(f)$ ein Körper. Der Homomorphismus

$$K \hookrightarrow K[X] \xrightarrow{\pi} K[X]/(f) = L$$

ist als Homomorphismus zwischen Körpern injektiv. Wir identifzieren K mit seinem Bild in L und fassen so L als Erweiterungskörper von K auf. Sei $x = \pi(X) \in L$. Mit $f = \sum_{i=0}^{n} c_i X^i$ gilt dann:

$$f(x) = \sum_{i=0}^{n} c_i x_i = \sum_{i=0}^{n} c_i \pi(X)^i = \pi\left(\sum_{i=0}^{n} c_i X^i\right) = \pi(f) = 0$$

Also ist $x \in L$ eine Nullstelle von f. Ist f nicht irreduzibel, so sei g einer der irreduziblen Faktoren von f. Dann hat g, und somit auch f, eine Nullstelle in $K[X]/(g)$. $\square$

Wir sagen, L entsteht aus K durch Adjunktion einer Nullstelle von f. Man kann dann über L einen Linearfaktor von f abspalten und das Verfahren solange fortsetzen, bis ein Erweiterungskörper K' von K gefunden ist, über dem f vollständig in Linearfaktoren zerfällt.

Definition 4.18 Ein Körper K heißt **algebraisch abgeschlossen**, falls jedes nichtkonstante Polynom $f \in K[X]$ eine Nullstelle in K besitzt. Mit anderen Worten, K ist algebraisch abgeschlossen, falls jedes f in $K[X]$ vollständig in Linearfaktoren zerfällt, d.h. dass f von der Form

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

mit $c \in K^*$ und $\alpha_1, \ldots, \alpha_n \in K$ ist.

Lemma 4.19 Ein Körper K ist genau dann algebraisch abgeschlossen, wenn er keine echten algebraischen Körpererweiterungen L/K besitzt.

Beweis : Sei K algebraisch abgeschlossen und L/K eine algebraische Erweiterung. Ist dann $\alpha \in L$ und $f = \text{Mipo}_K(\alpha)$, so zerfällt f über K in Linearfaktoren. Da f irreduzibel ist, ist f ein lineares Polynom in $K[X]$ mit Nullstelle α. Also ist $\alpha \in K$, d.h. $K = L$.
Umgekehrt sei K ein Körper ohne echte algebraische Erweiterungen und $f \in K[X]$ ein Polynom vom Grad ≥ 1. Nach dem Kronecker-Verfahren aus Satz 4.17 gibt es eine algebraische Erweiterung L/K, so dass f eine Nullstelle in L besitzt. Dann muss gemäß der Annahme $K = L$ gelten, d.h. f hat eine Nullstelle in K. □

Satz 4.20 Zu jedem Körper existiert ein algebraisch abgeschlossener Erweiterungskörper L.

Zum Beweis benötigen wir folgende Aussagen.

Satz 4.21 Sei R ein Ring und $\mathfrak{a} \subsetneq R$ ein echtes Ideal. Dann besitzt R ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m}$. Insbesondere besitzt also jeder Ring $R \neq 0$ ein maximales Ideal.

Beweis von Satz 4.21 : Wir benötigen das Zornsche Lemma: Eine partiell geordnete Menge $M \neq \emptyset$, in der jede total geordnete Teilmenge eine obere Schranke hat, besitzt ein maximales Element, d.h. ein Element $a \in M$, so dass aus $a \leq x$ schon $a = x$ folgt.
Sei $M = \{\mathfrak{b} : \mathfrak{b} \text{ Ideal in } M, \mathfrak{a} \subset \mathfrak{b} \subsetneq M\}$. M ist partiell geordnet mit der Relation

$$\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b},$$

denn es gilt

i) $\mathfrak{a} \leq \mathfrak{a}$ für alle $\mathfrak{a} \in M$

ii) $\mathfrak{a} \leq \mathfrak{b}$, $\mathfrak{b} \leq \mathfrak{c} \Rightarrow \mathfrak{a} \leq \mathfrak{c}$

iii) $\mathfrak{a} \leq \mathfrak{b}$, $\mathfrak{b} \leq \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b}$.

Sei $\emptyset \neq N \subset M$ eine total geordnete Teilmenge. Wir zeigen, dass dann $\mathfrak{c} = \bigcup_{\mathfrak{b} \in N} \mathfrak{b} \in M$ eine obere Schranke ist. $\mathfrak{c}$ ist ein Ideal in M, denn aus $x \in \mathfrak{c}$, $a \in R$ folgt $ax \in \mathfrak{c}$ und aus $x \in \mathfrak{c}$, $y \in \mathfrak{c}$ folgt $x \in \mathfrak{b}_1$, $y \in \mathfrak{b}_2$ für $\mathfrak{b}_1, \mathfrak{b}_2 \in N$. Da N total geordnet ist, gilt $\mathfrak{b}_1 \subset \mathfrak{b}_2$ oder $\mathfrak{b}_2 \subset \mathfrak{b}_1$, also $x + y \in \mathfrak{b}_2$ oder $\mathfrak{b}_1$, mithin in $\mathfrak{c}$.
Ferner ist $\mathfrak{a} \subset \mathfrak{c} \neq R$, denn aus $1 \in \mathfrak{c}$ würde $1 \in \mathfrak{b}$ für ein $\mathfrak{b} \in N$ folgen. Somit besitzt M ein maximales Element $\mathfrak{m}$. Definitionsgemäß ist dies ein maximales Ideal, das $\mathfrak{a}$ enthält. □

Beweis von Satz 4.20 : Wir konstruieren einen Erweiterungskörper von K, in dem jedes Polynom $f \in K[X]$ vom Grad ≥ 1 eine Nullstelle besitzt. Sei

$$I = \{f \in K[X] : \text{grad} f \geq 1\}$$

und $\mathcal{X} = (X_f)_{f \in I}$ ein System von Variablen indiziert durch I. Im Polynomring $K[\mathcal{X}]$ betrachten wir das Ideal

$$\mathfrak{a} = (\{f(X_f) : f \in I\})$$

Angenommen, $\mathfrak{a} = K[\mathcal{X}]$. Dann ist $1 \in \mathfrak{a}$, d.h. es existiert eine Gleichung

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

für gewisse $g_i \in K[\mathcal{X}]$ und $f_1, \ldots, f_n \in I$.
Nach dem Kronecker-Verfahren Satz 4.17 gibt es einen Erweiterungskörper K' von K, so dass jedes f_i eine Nullstelle $\alpha_i \in K'$ hat. Wir setzen α_i für X_{f_i} ein und erhalten $\sum_{i=1}^{n} g_i f(\alpha_i) = 0$ in K', im Widerspruch zur Darstellung der 1. Also ist $\mathfrak{a}$ ein echtes Ideal in $K[\mathcal{X}]$. Nach Satz 4.21 existiert ein maximales Ideal $\mathfrak{m} \subset K[\mathcal{X}]$, das $\mathfrak{a}$ enthält. Dann ist $L_1 = K[\mathcal{X}]/\mathfrak{m}$ ein Körper, den man mit der injektiven Abbildung

$$K \to K[\mathcal{X}] \to K[\mathcal{X}]/\mathfrak{m} = L_1$$

als Erweiterungskörper von K auffassen kann. Zu $f \in I$ sei $\overline{X}_f$ die Restklasse von X_f in L_1. Ist $f = \sum_{i=0}^{n} c_i X^i \in K[X]$, so gilt in L_1:

$$f(\overline{X}_f) = \sum_{i=0}^{n} c_i \overline{X}_f = \overline{\sum_{i=0}^{n} c_i X_f} = \overline{f(X_f)} = 0,$$

da $f(X_f) \in \mathfrak{a} \subset \mathfrak{m}$ ist. f hat also eine Nullstelle in L_1. Somit haben wir einen Körper L_1konstruiert, in dem jedes nicht-konstante Polynom in $K[X]$ eine Nullstelle hat. Dasselbe Verfahren wenden wir auf L_1 an. Durch Iteration dieser Konstruktion erhalten wir Körper $K \subset L_1 \subset L_2 \subset L_3 \subset \ldots$ mit der Eigenschaft, dass jedes nicht-konstante Polynom in $L_n[X]$ eine Nullstelle in L_{n+1} hat. Es sei $L = \bigcup_{n=1}^{\infty} L_n$. Dann ist L ein Körper (ÜA). Sei $f \in L[X]$ vom Grad ≥ 1. f hat nur endlich viele nicht-triviale Koeffizienten, also existiert ein n mit $f \in L_n[X]$. Nach Konstruktion hat f eine Nullstelle in $L_{n+1} \subset L$. Somit ist L ein algebraisch abgeschlossener Erweiterungskörper von K. □

Korollar 4.22 Sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Erweiterungskörper $\overline{K}$ von K, der algebraisch über K ist. Jeden solchen Körper nennt man einen algebraischen Abschluss von K.

Beweis : Der Körper L aus Satz 4.20 ist algebraisch über K, da jede Erweiterung L_n/L_{n-1} von der Familie algebraischer Elemente $(\overline{X}_f)_{f\in I}$ erzeugt wird. Induktiv folgert man so mit Satz 4.16, dass alle L_n/K algebraisch sind.
Ein anderer Beweis ergibt sich wie folgt:
Ist L ein beliebiger algebraisch abgeschlossener Erweiterungskörper, so sei

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

$\overline{K}$ ist ein Körper, da mit $\alpha, \beta \in \overline{K}$ auch $K(\alpha, \beta) \subset \overline{K}$ gilt, also $\alpha \cdot \beta$, $\alpha + \beta$ etc. in $\overline{K}$ liegen. $\overline{K}$ ist offenbar algebraisch über K. $\overline{K}$ ist auch algebraisch abgeschlossen, denn jedes $f \in \overline{K}[X]$ mit $\text{grad}(f) \geq 1$ hat eine Nullstelle γ in L. Diese ist algebraisch über $\overline{K}$ und nach Satz 4.16 auch über K. Also hat f die Nullstelle $\gamma \in \overline{K}$. □

Der soeben konstruierte Körper $\overline{K} \subset L$ heißt auch algebraischer Abschluss von K in L. Insbesondere ist

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraisch über } \mathbb{Q}\}$$

ein algebraischer Abschluss von $\mathbb{Q}$, da $\mathbb{C}$ algebraisch abgeschlossen ist, wie wir später zeigen werden.
Wir wollen jetzt zeigen, dass alle algebraischen Abschlüsse eines Körpers isomorph sind. Ist $\sigma : K \to L$ ein Körperhomomorphismus und $K[X] \to L[X]$ der induzierte Homomorphismus, der $f = \sum a_i X^i$ auf $f^\sigma := \sum_i \sigma(a_i) X^i$ abbildet. Dann ist für alle $\alpha \in K$:

$$f^\sigma(\sigma\alpha) = \sum_i \sigma(a_i)\sigma(\alpha)^i = \sigma\left(\sum_i a_i \alpha^i\right) = \sigma(f(\alpha)).$$

Insbesondere ist für jede Nullstelle α von f das Element $\sigma(\alpha)$ eine Nullstelle von f^σ.

Lemma 4.23 Sei K ein Körper und $K' = K(\alpha)$ eine einfache algebraische Körpererweiterung mit $f = \text{Mipo}_K(\alpha) \in K[X]$. Weiter sei $\sigma : K \to L$ ein Körperhomomorphismus.

i) Ist $\sigma' : K' \to L$ ein Körperhomomorphismus, der σ fortsetzt, so ist $\sigma'(\alpha)$ Nullstelle von f^σ.

ii) Umgekehrt gibt es zu jeder Nullstelle $\beta \in L$ von $f^\sigma \in L[X]$ genau eine Fortsetzung $\sigma' : K' \to L$ von σ mit $\sigma'(\alpha) = \beta$.

Insbesondere ist die Anzahl der verschiedenen Fortsetzungen σ' von σ gleich der Anzahl der verschiedenen Nullstellen von f^σ in L, also $\leq$ grad(f).

Beweis :

i) haben wir oben gesehen.

ii) Da nach Satz 4.10 $K' = K(\alpha) = K[\alpha]$ ist, ist die Fortsetzung σ' von σ mit $\sigma'(\alpha) = \beta$ eindeutig, falls sie existiert. Um die Existenz zu zeigen, betrachten wir die Einsetzungshomomorphismen

$$\begin{array}{rcccc} \varphi : K[X] & \to & K[\alpha], & \varphi(g) & = & g(\alpha) \\ \text{und } \psi : K[X] & \to & L, & \psi(g) & = & g^\sigma(\beta). \end{array}$$

Nach Satz 4.10 gilt Kern$\varphi = (f)$ und $K[X]/(f) \simeq K[\alpha]$. Da $f^\sigma(\beta) = 0$ ist, ist außerdem $(f) \subset$ Kernψ. Bezeichnen wir mit $\pi : K[X] \to K[X]/(f)$ die Projektion, so gibt es nach dem Homomorphiesatz einen Homomorphismus $\overline{\psi} : K[X]/(f) \to L$, so dass $\overline{\psi} \circ \pi = \psi$ ist. Also liefert $\sigma' : K[\alpha] \simeq K[X]/(f) \xrightarrow{\overline{\psi}} L$ einen Homomorphismus $K' \to L$ mit $\sigma'(\alpha) = \overline{\psi}(\pi(X)) = \psi(X) = \beta$, der für $a \in K$ gerade $\sigma'(a) = \overline{\psi}(\pi(a)) = \psi(a) = \sigma(a)$ liefert.

□

Satz 4.24 Es sei K'/K eine algebraische Körpererweiterung und $\sigma : K \to L$ ein Körperhomomorphismus mit Bild in einem algebraisch abgeschlossenen Körper L. Dann besitzt σ eine Fortsetzung $\sigma' : K' \to L$. Ist zusätzlich K' algebraisch abgeschlossen und L algebraisch über $\sigma(K)$ so ist jede Fortsetzung σ' von σ ein Isomorphismus.

Beweis : Wir wenden das Zorn'sche Lemma an. Sei

$$\begin{array}{rcl} M & = & \{(F, \tau) : F \text{ ein Zwischenkörper von } K'/K \\ & & \text{und } \tau : F \to L \text{ eine Fortsetzung von } \sigma\} \end{array}$$

Dann ist M partiell geordnet unter der Relation $(F, \tau) \leq (F', \tau')$, falls $F \subset F'$ und $\tau'|_F = \tau$ gilt. Da $(K, \sigma) \in M$ ist, ist $M \neq \emptyset$. Ist $N \subset M$ eine total geordnete Teilmenge, so liefert die Vereinigung F_0 aller F mit $(F, \tau) \in N$ mit der Abbildung $\tau_0 : F \to L$, die alle diese τ fortsetzt, eine obere Schranke von N (ÜA). Also enthält M ein maximales Element (F, τ). Gilt $F \neq K'$, so existiert ein $\alpha \in K' \setminus F$. Der algebraisch abgeschlossene Körper L enthält eine Nullstelle des Polynoms $(\text{Mipo}_F(\alpha))^\tau \in L[X]$. Also gibt es nach Lemma 4.23 eine Fortsetzung von τ auf $F(\alpha)$, was der Maximalität von (F, τ) widerspricht. Somit existiert tatsächlich eine Fortsetzung $\sigma' : K' \to L$ von σ.

Ist zusätzlich K' algebraisch abgeschlossen, so ist auch $\sigma'(K')$ algebraisch abgeschlossen (ÜA). Ist zusätzlich $L/\sigma(K)$ algebraisch, so ist L auch über dem größeren Körper $\sigma'(K')$ algebraisch, woraus nach Lemma 4.19 $L = \sigma'(K')$ folgt. τ' ist also surjektiv, und somit als Körperhomomorphismus schon ein Isomorphismus. □

Korollar 4.25 Seien $\overline{K}_1$ und $\overline{K}_2$ algebraische Abschlüsse von K. Dann existiert ein (i.a. nicht-kanonischer) Isomorphismus $\varphi : \overline{K}_1 \simeq \overline{K}_2$, so dass $\varphi|_K = \mathrm{id}_K$ ist.

Beweis : Das folgt direkt aus Satz 4.24. □

5 Normale und separable Erweiterungen

Sind L/K und L'/K zwei Erweiterungen von K, so nennen wir einen Körperhomomorphismus $\sigma : L \to L'$ einen K-Homomorphismus, falls $\sigma|_K$ die Identität auf K ist.

Definition 5.1 Sei $\mathcal{F} = (f_i)_{i\in I}$, $f_i \in K[X]$ eine Familie nicht-konstanter Polynome. Ein Erweiterungskörper L/K heißt Zerfällungskörper von $\mathcal{F}$ über K, wenn gilt:

i) Jedes f_i zerfällt über L vollständig in Linearfaktoren und

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

Ein Zerfällungskörper L/K ist also algebraisch über K. Ist $\mathcal{F} = (f)$ ein einziges Polynom mit den Nullstellen $a_1, \ldots, a_n$ in einem algebraichen Abschluss $\overline{K}$ von K, so ist $L = K(a_1, \ldots, a_n)$ ein Zerfällungskörper von f über K.
Analog zeigt man, dass auch für eine beliebige Familie $\mathcal{F}$ stets ein Zerfällungskörper von f über K existiert. Man wählt einen algebraischen Abschluss $\overline{K}$ von K. Über $\overline{K}$ zerfallen alle $f_i \in \mathcal{F}$ vollständig in Linearfaktoren. Der Teilkörper L von $\overline{K}$, der über K von allen Nullstellen der f_i erzeugt wird, ist dann ein Zerfällungskörper von $\mathcal{F}$ über K.
Ist $\mathcal{F} = (f_1, \ldots, f_n)$ endlich, so ist jeder Zerfällungskörper von $\mathcal{F}$ auch einer von dem Produkt $f_1 \cdots f_n$ und umgekehrt.

Satz 5.2 Seien L_1 und L_2 zwei Zerfällungskörper einer Familie $\mathcal{F}$ nicht-konstanter Polynome $f_i \in K[X]$ über K. Dann lässt sich jeder K-Homomorphismus

$$\overline{\sigma} : L_1 \to \overline{L}_2$$

in einem algebraischen Abschluss $\overline{L}_2$ von L_2 zu einem Isomorphismus $\sigma : L_1 \xrightarrow{\sim} L_2$ einschränken.

Beweis : Ist $\mathcal{F} = (f)$, so können wir annehmen, dass f normiert ist. Seien $a_1, \ldots, a_n$ die Nullstellen von f in L_1 und $b_1, \ldots, b_n$ die Nullstellen von f in $L_2 \subset \overline{L}_2$, so gilt $f = \prod_i (X - a_i)$ in $L_1[X]$ und $f = \prod_i (X - b_i)$ in $L_2[X]$. Also ist $f^{\overline{\sigma}} = \prod_i (X - \overline{\sigma}(a_i))$ in $L_2[X]$. Andererseits ist $f^{\overline{\sigma}} = f$, da f Koeffizienten in K hat. Also gilt in $\overline{L}_2[X]$:

$$f^{\overline{\sigma}} = \prod_i (X - b_i).$$

Daher bildet $\overline{\sigma}$ die Menge $\{a_1, \ldots, a_n\}$ bijektiv auf $\{b_1, \ldots, b_n\}$ ab und es folgt

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

Also vermittelt die Einschränkung von $\overline{\sigma}$ auf L_1 einen surjektiven Körperhomomorphismus und damit einen Isomorphismus nach L_2.
Da für $\mathcal{F} = (f_1, \ldots, f_n)$ wie oben gesehen L_1 und L_2 Zerfällungskörper von $f = f_1 \cdots f_n$ sind, folgt die Behauptung auch für endliche Familien $\mathcal{F}$.
Eine beliebige Familie $\mathcal{F}$ können wir als Vereinigung aller endlichen Teilfamilien schreiben. Ein Zerfällungskörper L von $\mathcal{F}$ ist dann die Vereinigung von Zerfällungskörpern aller endlichen Teilfamilien (ÜA). Daher folgt auch hier die Behauptung. □

Korollar 5.3 Je zwei Zerfällungskörper L_1 und L_2 einer Familie nicht konstanter Polynome in $K[X]$ sind über K isomorph.

Beweis : Die Inklusion $K \hookrightarrow \overline{L}_2$ lässt sich nach Satz 4.24 zu einem K-Homomorphismus $\overline{\sigma} : L_1 \to \overline{L}_2$ fortsetzen. Nach Satz 5.2 folgt $\overline{\sigma} : L_1 \xrightarrow{\sim} L_2$. □

Satz 5.4 Es sei K ein Körper und L/K algebraisch. Dann sind äquivalent:

i) Jeder K-Homomorphismus $L \to \overline{L}$ in einem algebraischen Abschluss $\overline{L}$ von L vermittelt einen Automorphismus von L.

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

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

Beweis : i) $\Rightarrow$ iii): Sei $f \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle von f. Ist $b \in \overline{L}$ eine weitere Nullstelle von f, so existiert nach Lemma 4.23 ein K-Homomorphismus $\sigma : K(a) \to \overline{L}$ mit $\sigma(a) = b$. Nach Satz 4.24 lässt sich σ zu einem K-Homomorphismus

$\sigma : L \to \overline{L}$ fortsetzen Gilt i), so folgt $\sigma(L) = L$, d.h. $b = \sigma(a) \in L$. Also sind alle Nullstellen von f bereits in L enthalten.
iii) $\Rightarrow$ ii): Sei $L = K((a_i)_{i\in I})$ und $f_i = \text{Mipo}_K(a_i)$. Nach iii) zerfallen alle f_i über L vollständig in Linearfaktoren. Also ist L Zerfällungskörper von $\mathcal{F} = (f_i)_{i\in I}$.
ii) $\Rightarrow$ i): Sei L Zerfällungskörper von $\mathcal{F}$ und $\sigma : L \to \overline{L}$ ein K-Homomorphismus. Wie im Beweis von Satz 5.2 zeigt man, dass σ die Nullstellen der Polynome aus $\mathcal{F}$ in sich abbildet. Da L von diesen Nullstellen erzeugt wird, gilt $\sigma(L) = L$. □

Definition 5.5 Eine algebraische Körpererweiterung L/K heißt **normal**, wenn die äquivalenten Bedingungen aus Satz 5.4 erfüllt sind.

Beispiel: Körpererweiterungen vom Grad 2 sind nach Satz 5.4 ii) stets normal (ÜA).

Lemma 5.6 Ist $K \subset L \subset M$ mit M/K normal, so ist auch M/L normal.

Beweis : Das folgt aus Satz 5.4 ii). □

Sind die Körpererweiterungen L/K und M/L normal, so muss M/K nicht normal sein (ÜA). Ist M/K normal, so muss L/K nicht normal sein (s.u.).
Ist L/K eine algebraische Körpererweiterung, so nennen wir einen algebraischen Erweiterungskörper L' von L, so dass L'/K normal, aber kein Zwischenkörper $L \subset M \subset L'$ mit $M \neq L'$ normal über K ist, eine **normale Hülle** von L/K.

Satz 5.7 Sei L/K eine algebraische Körpererweiterung.

i) Zu L/K gibt es eine normale Hülle L'/K. Diese ist bis auf Isomorphie eindeutig bestimmt.

ii) Ist L/K endlich, so auch L'/K.

iii) Ist M/L eine algebraische Erweiterung, so dass M/K normal ist, so ist $L' = K(\mathfrak{b})$ mit $\mathfrak{b} = \{\sigma(a) : a \in L, \sigma : L \to M \ K\text{-Homomorphismus}\}$ eine normale Hülle von L/K. Sie heißt normale Hülle von L in M.

Beweis : Nach Korollar 4.15 ist $L = K(\mathfrak{a})$ für eine Familie $\mathfrak{a} = (a_j)_{j\in J}$ von algebraischen Elementen. Setze $f_j = \text{Mipo}_K(a_j)$. Die f_j zerfallen über einem algebraischen Abschluss $\overline{L}$ von L vollständig in Linearfaktoren. Sei L' der von den Nullstellen der f_j erzeugte Teilkörper von $\overline{L}/L$. Dann ist L' ein Zerfällungskörper der Familie (f_j). Offenbar ist L'/K eine normale Hülle von L/K (ÜA). Nach Konstruktion ist L'/K endlich, falls L/K endlich ist. Mit Korollar 5.3 folgt die Eindeutigkeit bis auf Isomorphie.

Zu iii): Wir konstruieren wie in i) $L' \subset \overline{M}$. Jeder K-Homomorphismus $\sigma : L \to M$ überführt nach Lemma 4.23 a_j in eine Nullstelle von f_j, somit ist $\sigma(a_j) \in L'$. Daher folgt $\sigma(L) \subset L'$, also $K(\mathfrak{b}) \subset L'$. Andererseits können wir zu jeder Nullstelle $a'_j \in L'$ von $f = \text{Mipo}_K(a_j)$ nach Lemma 4.23 einen K-Homomorphismus $\sigma : K(a_j) \to L'$ mit $\sigma(a_j) = a'_j$ finden. Dieser lässt sich nach Satz 4.24 zu $\sigma : M \to \overline{M}$ fortsetzen und vermittelt nach Satz 5.4 einen Automorphismus von M, da M/K normal ist. Somit gilt $a'_j = \sigma(a_j) \in K(\mathfrak{b})$. Da $L \subset K(\mathfrak{b})$ ist, folgt $L' \subset K(\mathfrak{b})$, so dass $L' = K(\mathfrak{b})$ gilt. □

Lemma 5.8 Es sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann gilt:

i) $a \in \overline{K}$ ist mehrfache Nullstelle von f.
   $\Leftrightarrow f(a) = 0$ und $f'(a) = 0$
   $\Leftrightarrow \text{ggT}(f, f')(a) = 0$.

ii) Ist f irreduzibel, so hat f genau dann mehrfache Nullstellen in $\overline{K}$, wenn $f' = 0$ gilt.

Beweis :

i) folgt aus Satz 3.7 und Korollar 3.8, angewandt auf $f \in \overline{K}[X]$. Man muss nur nachrechnen, dass $\text{ggT}_{K[X]}(f, f') = \text{ggT}_{\overline{K}[X]}(f, f')$ ist. Da $K[X]$ und $\overline{K}[X]$ Hauptidealringe sind, folgt das aus Satz 2.37 (ÜA).

ii) Ohne Einschränkung sei f normiert. Ist f irreduzibel und $a \in \overline{K}$ eine mehrfache Nullstelle von f, so ist einerseits $f = \text{Mipo}_K(a)$ und andererseits folgt aus i), dass $f'(a) = 0$ ist. Da $\text{grad}(f') < \text{grad}(f)$ ist, muss $f' = 0$ sein. Ist umgekehrt $f' = 0$, so ist jede Nullstelle von f nach i) eine mehrfache Nullstelle

□

Beispiel

i) Ist $\text{char}(K) = 0$, so gilt für jedes nicht-konstante $f \in K[X] : f' \neq 0$.

ii) Es sei p eine Primzahl, t eine Unbestimmte und $K = \mathbb{F}_p(t) = \text{Quot}(\mathbb{F}_p[t])$. Dann ist $f = X^p - t \in K[X]$ irreduzibel nach Eisenstein, denn t ist ein Primelement in $\mathbb{F}_p[t]$. Es ist $f' = pX^{p-1} = 0$ in $\mathbb{F}_p[t]$.

Definition 5.9 Ein nicht-konstantes Polynom $f \in K[X]$, das keine mehrfachen Nullstellen in $\overline{K}$ hat, heißt **separabel**. Ein irreduzibles Polynom f ist also genau dann separabel, wenn $f' = 0$ ist.

Satz 5.10 Sei K ein Körper und $f \in K[X]$ irreduzibel.

i) Ist $\text{char}(K) = 0$, so ist f separabel.

ii) Ist $\text{char}(K) = p > 0$, so sei $r \in \mathbb{N}_0$ maximal mit der Eingenschaft, dass es ein $g \in K[X]$ mit $f(X) = g\left(X^{p^r}\right)$ gibt. Dann hat jede Nullstelle von f die Vielfachheit p^r und g ist irreduzibel und separabel. Die Nullstellen von f sind gerade die p^r-ten Wurzeln der Nullstellen von g.

Beweis :

i) ist schon gezeigt.

ii) Sei $f = \sum_{i=0}^{n} c_i X^i$, also $f' = \sum_{i=1}^{n} i \cdot c_i X^{i-1}$. $f' = 0$ ist äquivalent zu $i \cdot c_i = 0$ für alle $i = 1, \ldots, n-1$, d.h. $p|i$ oder $c_i = 0$. Also ist $f' = 0$ genau dann, wenn es ein $h \in K[X]$ mit $f(X) = h(X^p)$ gibt.

Gilt $f(X) = g\left(X^{p^r}\right)$ wie in der Behauptung, so liefert dasselbe Argument, auf g angewandt, dass $g' \neq 0$ ist, d.h. g ist separabel. Aus der Irreduzibilität von f folgt offenbar die Irreduzibilität von g. Ist $\overline{K}$ ein algebraischer Abschluss von K, so gilt $g = d \cdot \prod_i (X - a_i)$ in $\overline{K}[X]$ mit paarweie verschiedenen $a_i \in \overline{K}$ und einem $d \in \overline{K}$.

Für alle i sei $c_i \in \overline{K}$ ein Element mit $c_i^{p^r} = a_i$. Dann gilt

$$f = d \prod_i (X^{p^r} - c_i^{p^r}) = d \prod_i (X - c_i)^{p^r} \text{ nach Lemma 4.3.}$$

Somit haben alle Nullstellen von f die Ordnung p^r.

□

Definition 5.11 Sei L/K algebraisch.

i) Dann heißt $\alpha \in L$ **separabel** über K, falls α Nullstelle eines separablen Polynoms in $K[X]$ ist.

ii) L/K heißt **separabel**, falls jedes $\alpha \in L$ separabel über K ist.

iii) K heißt **vollkommen**, wenn jede algebraische Erweiterung von K separabel ist.

Bemerkung:

i) Offenbar ist $\alpha \in L$ separabel über K genau dann, wenn $\text{Mipo}_K(\alpha) \in K[X]$ ein separables Polynom ist (ÜA).

ii) Jeder Körper der Charakteristik 0 ist vollkommen.

iii) Der Körper $\mathbb{F}_p(t)[X]/(X^p - t)$ ist nicht separabel über $\mathbb{F}_p(t)$.

iv) Ist für algebraische Körpererweiterungen $K \subset L \subset M$ M/K separabel, so auch M/L.

Definition 5.12 Sei L/K algebraisch und $\mathrm{Hom}_K(L, \overline{K})$ sei die Menge der K-Homomorphismen von L in einen algebraischen Abschluss $\overline{K}$ von K. Dann ist der Separabilitätsgrad von L/K definiert als

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

Nach Korollar 4.25 ist $[L : K]_s$ unabhängig von der Wahl eines algebraischen Abschlusses $\overline{K}$.

Lemma 5.13 Sei $L = K(\alpha)$ und $f = \mathrm{Mipo}_K(\alpha)$.

i) $[L : K]_s$ ist gleich der Anzahl der verschiedene Nullstellen von f in einem algebraischen Abschluss $\overline{K}$.

ii) α ist genau dann separabel über K, wenn $[L : K]_s = [L : K]$ gilt.

iii) Ist $\mathrm{char} K = p > 0$ und p^r die Vielfachheit der Nullstelle α von f, so folgt $[L : K] = p^r [L : K]_s$.

Beweis :

i) folgt sofort aus Lemma 4.23.

ii) Sei $n = \mathrm{grad}(f)$. Ist α separabel, so hat f keine mehrfachen Nullstellen, sondern n paarweise verschiedene. Aus i) folgt $[L : K]_s = n = \mathrm{grad}(f) = [L : K]$. Gilt umgekehrt $[L : K]_s = [L : K] = n$, so hat f nach i) n verschiedene Nullstellen, ist also separabel.

iii) Nach Satz 5.10 ii) ist $f(X) = g(X^{p^r})$ mit einem separablen irreduziblen Polynom g. Also ist $[L : K] = \mathrm{grad}(f) = p^r \cdot \mathrm{grad}(g)$. Da g keine mehrfachen Nullstellen hat, ist $[L : K]_s = \mathrm{grad}(g)$, woraus die Behauptung folgt.

□

Satz 5.14 Sind $K \subset L \subset M$ algebraische Körpererweiterungen, so gilt

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

Beweis : Es sei $\overline{K}$ ein algebraischer Abschluss von M. Dann ist $\overline{K}$ auch ein algebraischer Abschluss von K und L (ÜA). Ferner sei $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i : i \in I\}$ und $\mathrm{Hom}_L(M, \overline{K}) = \{\tau_j : j \in J\}$ mit jeweils paarweise verschiedenen σ_i ($i \in I$) und τ_j ($j \in J$). Nach Satz 4.24 lässt sich σ_i zu einem K-Automorphismus

$$\overline{\sigma}_i : \overline{K} \to \overline{K}$$

fortsetzen. Für alle j ist dann $\overline{\sigma}_i \circ \tau_j \in \mathrm{Hom}_K(M, \overline{K})$. Angenommen $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$ für $i, i' \in I$ und $j, j' \in J$. Da $\tau_j|_L = \tau_{j'}|_L = \mathrm{id}$ ist, folgt nach Einschränken auf L, dass $\sigma_i = \sigma_{i'}$, also $i = i'$ ist. Daraus folgt $\tau_j = \tau_{j'}$, also $j = j'$. Die $\overline{\sigma}_i \circ \tau_j$ sind also paarweise verschieden. Sei $\tau \cdot M \to \overline{K}$ ein beliebiger K-Homomorphismus. Dann ist $\tau|_L \in \mathrm{Hom}_K(L, \overline{K})$, also $\tau|_L = \sigma_i$ für ein $i \in I$. Daraus folgt $\overline{\sigma}_i^{-1} \circ \tau|_L = \mathrm{id}_L$, also $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$. Somit ist $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$ für ein $j \in J$. Es folgt $\tau = \overline{\sigma}_i \circ \tau_j$. Daher ist $\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j : i \in I, j \in J\}$ und $[M : K]_s = \#I \cdot \#J = [M : L]_s \cdot [L : K]_s$. □

Satz 5.15 Sei L/K endlich.

i) Ist L/K separabel, so folgt $[L : K]_s = [L : K]$.

ii) Ist $\mathrm{char} K = p > 0$, so existiert ein $r \in \mathbb{N}_0$ mit $[L : K] = p^r \cdot [L : K]_s$. Insbesondere ist $[L : K]_s$ ein Teiler von $[L : K]$.

Beweis :

i) Ist L/K endlich und separabel, also $L = K(a_1, \ldots, a_n)$, so ist für alle $i = 1, \ldots, n-1$ das Element a_{i+1} separabel über K, also auch über $K(a_1, \ldots, a_i)$ (vgl. obige Bemerkung). Aus Lemma 5.13 ii) folgt

$$[K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots a_i)]_s = [K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots, a_i)].$$

Aufgrund des Gradsatzes und Satz 5.14 folgt $[L : K]_s = [L \cdot K]$.

ii) folgt aus Lemma 5.13 ii) angewandt auf alle $K(a_1, \ldots, a_{i+1})/K(a_1, \ldots, a_i)$.

□

Satz 5.16 Sei L/K endlich. Ist $[L : K]_s = [L : K]$, so ist L/K separabel.

Beweis : Ist $\mathrm{char}(K) = 0$, so ist nichts zu zeigen. Ist $\mathrm{char}(K) = p > 0$, so sei $a \in L$ und $f = \mathrm{Mipo}_K(a)$. Nach Lemma 5.13 iii) gilt für die Vielfachheit r der Nullstelle a

$$[K(a) : K] = p^r \cdot [K(a) : K]_s.$$

Also ist

$$\begin{aligned}[L:K] &= [L:K(a)]\cdot[K(a):K] \\ &\geq [L:K(a)]_s \cdot p^r [K(a):K]_s \\ &= p^r [L:K]_s \text{ (nach Satz 5.14).}\end{aligned}$$

Aus $[L:K] = [L:K]_s$ folgt $r = 0$, d.h. f hat nur einfache Nullstellen. Somit ist a separabel über K. □

Lemma 5.17 Seien $K \subset L \subset M$ algebraische Körpererweiterungen. Dann ist M/K genau dann separabel, wenn M/L und L/K separabel sind.

Beweis : Ist M/K separabel, so auch M/L und L/K (ÜA). Sei umgekehrt M/L und L/K separabel und $a \in M$ gegeben. Es sei L' der Zwischenkörper von L/K, der von den Koeffizienten von

$$f = \text{Mipo}_L(a) \in L[X]$$

erzeugt wird. Da M/L separabel ist, so ist f separabel. Somit ist $L'(a)/L'$ separabel. Da L/K separabel ist, ist auch L'/K separabel. Ferner sind L'/K und $L'(a)/K$ endlich. Also gilt

$$\begin{aligned}[L'(a):K]_s &\overset{5.14}{=} [L'(a)L']_s \cdot [L':K]_s \\ &\overset{5.15}{=} [L'(a):L']\cdot[L':K] \\ &\overset{\text{Gradsatz}}{=} [L'(a):K].\end{aligned}$$

Nach Satz 5.16 ist $L'(a)/K$ separabel, also a separabel über K. □

Satz 5.18 (Satz vom primitiven Element) Es sei L/K endlich und separabel. Dann existiert ein primitives Element, d.h. ein $a \in L$ mit $L = K(a)$.

Beweis : 1. Fall: K ist endlich. Dann ist wegen $[L:K] < \infty$ auch L endlich. Nach Satz 5.20 (s.u.) ist L^* eine zyklische Gruppe. Ist $a \in L$ ein Erzeuger, so gilt $L = K(a)$.
2. Fall: K ist unendlich. Mit einem Induktionsargument genügt es zu zeigen, dass jede endliche Erweiterung $K(a,b)/K$ ein primitives Element besitzt (ÜA). Sei $n = [K(a,b):K]$ und $\text{Hom}_K(K(a,b), \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Wir betrachten das Polynom

$$P = \prod_{i \neq j} [(\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))X]$$

Für $i \neq j$ ist $\sigma_i \neq \sigma_j$, also $\sigma_i(a) \neq \sigma_j(a)$ oder $\sigma_i(b) \neq \sigma_j(b)$. Somit ist $P \neq 0$. Da K unendlich viele Elemente besitzt, gibt es ein $c \in K$ mit $P(c) \neq 0$. Dann ist für

$i \neq j$ also $\sigma_i(a) - \sigma_j(a) \neq -c(\sigma_i(b) - \sigma_j(b))$, d.h. $\sigma_i(a + cb) \neq \sigma_j(a + cb)$. Ist $f = \text{Mipo}_K(a+cb) \in K[X]$, so hat f die n paarweise verschiedenen Nullstellen $\sigma_i(a+cb)$, $i = 1, \ldots, n$. Also folgt:

$$[K(a,b) : K]_s = n \leq \text{grad}(f) = [K(a + cb) : K] \leq [K(a,b) : K].$$

Da $K(a,b)/K$ separabel ist, gilt aber $[K(a,b) : K] = [K(a,b) : K]_s$, woraus $K(a+cb) = K(a,b)$ folgt. □

Wir zeigen jetzt, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

Lemma 5.19 Seien a, b Elemente endlicher Ordnung in einer abelschen Gruppe G. Sei $\text{ord}(a) = m$ und $\text{ord}(b) = n$. Dann existiert in G ein Element der Ordnung $\text{kgV}(m,n)$.

Beweis : Wir nehmen zunächst an, dass $\text{ggT}(m,n) = 1$ gilt und zeigen, dass dann ab die Ordnung mn hat. Es gilt $(ab)^{mn} = (a^m)^n(b^n)^m = 1$. Aus $(ab)^t = 1$ folgt $a^{nt} = a^{nt}b^{nt} = 1$, also $m \mid nt$, woraus wegen $\text{ggT}(m,n) = 1$ dann $m \mid t$ folgt. Analog zeigt man $n \mid t$, woraus $mn \mid t$ folgt. Also ist $\text{ord}(ab) = mn$. Im allgemeinen Fall sei $\text{kgV}(m,n) = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung von $\text{kgV}(m,n)$. Wir definieren m_0 als das Produkt aller $p_i^{\nu_i}$, die m teilen und n_0 als das Produkt aller $p_i^{\nu_i}$, die m nicht teilen. Dann gilt $m_0 \mid m$ und $n_0 \mid n$, d.h. es ist $m = m_0m'$ und $n = n_0n'$ für gewisse Zahlen m' und n'. Außerdem ist $\text{ggT}(m_0, n_0) = 1$. Da $\text{ord}(a^{m'}) = m_0$ und $\text{ord}(b^{n'}) = n_0$ gilt, hat $a^{m'}b^{n'}$ nach dem oben Gezeigten die Ordnung $m_0n_0 = \text{kgV}(m,n)$. □

Satz 5.20 Es sei K ein Körper und H eine endliche Untergruppe der multiplikativen Gruppe K^*. Dann ist H zyklisch.

Beweis : Sei $a \in H$ ein Element maximaler Ordnung m und H_m die Untergruppe aller Elemente von H, deren Ordnung m teilt. Alle Elemente von H_m sind dann Nullstellen des Polynoms $X^m - 1$ in K, so dass $\#H_m \leq m$ gilt. Andererseits enthält H_m die zyklische Untergruppe $\langle a \rangle$ der Ordnung m, woraus $H_m = \langle a \rangle$ folgt. Es genügt also zu zeigen, dass $H_m = H$ gilt. Angenommen, $b \in H \setminus H_m$, d.h. $\text{ord}(b)$ teilt nicht m. Dann besitzt H nach Lemma 5.19 ein Element der Ordnung $\text{kgV}(m, \text{ord}(b)) > m$ in Widerspruch zur Wahl von a. □

Definition 5.21 Sei L/K eine algebraische Erweiterung. L/K heißt **rein inseparabel**, wenn $[L : K]_s = 1$ gilt.

6 Endliche Körper

Bisher haben wir die endlichen Körper $\mathbb{F}_p$, $p > 0$ eine Primzahl kennengelernt. Wir wollen nun untersuchen, welche weiteren endlichen Körper es gibt.

Lemma 6.1 Sei $\mathbb{F}$ ein endlicher Körper. Dann ist $p = \text{char}(\mathbb{F}) > 0$. Ferner enthält $\mathbb{F}$ genau $q = p^n$ Elemente mit $n = [\mathbb{F} : \mathbb{F}_p]$. $\mathbb{F}$ ist ein Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$, die Erweiterung $\mathbb{F}/\mathbb{F}_p$ ist also normal.

Beweis : Da $\mathbb{F}$ endlich ist, ist auch der Primkörper von $\mathbb{F}$ endlich, also nach Satz 4.2 isomorph zu einem $\mathbb{F}_p$, $p = \text{char}(\mathbb{F}) > 0$. Ferner muss $n = [\mathbb{F} : \mathbb{F}_p] < \infty$ sein. Als n-dimensionaler Vektorraum über $\mathbb{F}_p$ enthält $\mathbb{F}$ also $q = p^n$ Elemente (ÜA). Also hat $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ die Ordnung $q - 1$, d.h. jedes Element $a \in \mathbb{F}^*$ erfüllt $a^{q-1} = 1$. Somit ist jedes Element aus $\mathbb{F}^*$ Nullstelle von $X^{q-1} - 1 \in \mathbb{F}_p[X]$, also auch von $X^q - X \in \mathbb{F}_p[X]$, das zusätzlich die Nullstelle 0 besitzt. Somit besteht $\mathbb{F}$ aus $q = p^n$ verschiedenen Nullstellen von $X^q - X$, also aus allen Nullstellen von $X^q - X$ in $\overline{\mathbb{F}}_p$. Daher zerfällt $X^q - X$ in $\mathbb{F}$ vollständig in Linearfaktoren. Da $\mathbb{F}$ außerdem von den Nullstellen von $X^q - X$ über $\mathbb{F}_p$ erzeugt wird, ist $\mathbb{F}$ ein Zerfällungskörper dieses Polynoms. □

Satz 6.2 Sei p eine Primzahl. Dann existiert zu jedem $n \in \mathbb{N} \setminus \{0\}$ ein Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit $q = p^n$ Elementen. $\mathbb{F}_q$ ist bis auf Isomorphie eindeutig bestimmt als Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$. Ferner beseht $\mathbb{F}_q$ genau aus den q Nullstellen von $X^q - X$.
Jeder endliche Körper der Charakteristik p ist isomorph zu genau einem $\mathbb{F}_q$.

Beweis : Es sei $q = p^n$ und $f(X) = X^q - X$. Da $f' = -1$ ist, hat f nach Lemma 5.8 keine mehrfachen Nullstellen in einem algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Also hat f genau q paarweise verschiedene Nullstellen in $\overline{\mathbb{F}}_p$. Sind $a, b \in \overline{\mathbb{F}}_p$ zwei Nullstellen von f, so gilt nach Lemma 4.3

$$(a \pm b)^q = a^q \pm b^q = a - b,$$

d.h. $a \pm b$ ist ebenfalls eine Nullstelle von f. Außerdem ist ab sowie a^{-1} eine Nullstelle von f. So sieht man, dass die Menge der Nullstellen von f in $\overline{\mathbb{F}}_p$ einen Körper $\mathbb{F}_q$ mit q Elementen bilden. Offenbar ist $\mathbb{F}_q$ ein Zerfällungskörper von f. Das zeigt die Existenz von $\mathbb{F}_q$. Ist $\mathbb{F}$ ein beliebiger endlicher Körper, so ist $\mathbb{F}$ nach Lemma 6.1 ein Zerfällungskörper von $X^q - X$ für $q = p^{[\mathbb{F}:\mathbb{F}_p]}$. Also ist nach Korollar 5.3 $\mathbb{F} \simeq \mathbb{F}_q$. □

Korollar 6.3 Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Für alle $n \geq 1$ können wir $\mathbb{F}_{p^n}$ nach $\overline{\mathbb{F}}_p$ einbetten. Das Bild dieser Einbettung ist eindeutig bestimmt, wir bezeichnen es ebenfalls mit $\mathbb{F}_{p^n}$. Dann ist

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \Leftrightarrow n \mid m$$

Die Erweiterungen $\mathbb{F}_{q^m}/\mathbb{F}_{q^n}$ für $n \mid m$ sind bis auf Isomorphie die einzigen Erweiterungen endlicher Körper der Charakteristik p.

Beweis : Nach Satz 4.24 existiert ein $\mathbb{F}_p$-Homomorphismus $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$. Da $\mathbb{F}_{p^n}/\mathbb{F}_p$ normal ist, ist sein Bild eindeutig bestimmt (vgl. Satz 5.2). Ist $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, so gilt für $\nu = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$:

$$p^m = \#\mathbb{F}_{p^m} = (\#\mathbb{F}_{p^n})^\nu = p^{n\nu}, \text{ also } n \mid m.$$

Umgekehrt folgt aus $m = n\nu$, dass jedes $a \in \mathbb{F}_{p^n}$ die Gleichung $a^{p^m} = a^{p^{n\nu}} = \underbrace{(\dots(a^{p^n})^{p^n}\dots)^{p^n}}_{\nu\text{-mal}} \overset{a\in\mathbb{F}_{p^n}}{=} a$ erfüllt. Somit ist $a \in \mathbb{F}_{p^m}$ nach Satz 6.2.
Ist $\mathbb{F}'/\mathbb{F}$ eine Erweiterung endlicher Körper, so können wir $\mathbb{F}_p \hookrightarrow \overline{\mathbb{F}}_p$ nach Satz 4.24 zu einem $\mathbb{F}_p$-Homomorphismus $\sigma : \mathbb{F}' \hookrightarrow \overline{\mathbb{F}}_p$ fortsetzen. Also sind $\sigma(\mathbb{F})$ und $\sigma(\mathbb{F}')$ endliche Teilkörper von $\overline{\mathbb{F}}_p$, woraus die Behauptung folgt. □

Korollar 6.4 Jede algebraische Erweiterung eines endlichen Körpers ist normal und separabel. Insbesondere sind endliche Körper vollkommen.

Beweis : Sei K ein endlicher Körper. Nach Satz 6.2 ist $K \simeq \mathbb{F}_q$ mit $q = p^n$. Ist L/K eine endliche Erweiterung, so ist nach Korollar 6.3 $L \simeq \mathbb{F}_{p^m}$ für ein Vielfaches m von n. $\mathbb{F}_{p^m}$ ist Zerfällungskörper von $X^{p^m} - X$ über $\mathbb{F}_p$, also auch über $\mathbb{F}_{p^n} = K$, somit ist L/K normal. Da $X^{p^m} - X$ separabel ist, ist L/K auch separabel.
Eine beliebige algebraische Erweiterung L/K ist Vereinigung von endlichen Teilerweiterungen L_i/K, die alle normal und separabel sind. Daher ist jedes Element in L separabel über K, d.h. L/K ist separabel. Mit Satz 5.4 iii) ist L/K auch normal. □

Satz 6.5 Ist $q = p^n$, so ist die multiplikative Gruppe $\mathbb{F}_q^\times$ zyklisch von der Ordnung $q - 1$.

Beweis : Das folgt aus Satz 5.20. □

Es sei $q = p^n$ und $q' = p^m$ mit $m = n\nu$. Dann ist $\mathbb{F}_{q'}/\mathbb{F}_q$ eine Erweiterung endlicher Körper vom Grad ν. Es sei $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ die Gruppe der Körperautomorphismen von

$\mathbb{F}_{q'}$, die $\mathbb{F}_q$ festlassen. Sei $\overline{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_{q'}$. Dann ist wegen der Normalität von $\mathbb{F}_{q'}/\mathbb{F}_q$ nach Satz 5.4 i)

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q'}, \overline{\mathbb{F}}_p).$$

Da $\mathbb{F}_{q'}/\mathbb{F}_q$ separabel ist, gilt

$$\#\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = [\mathbb{F}_{q'} : \mathbb{F}_q]_s = [\mathbb{F}_{q'} : \mathbb{F}_q] = \nu.$$

Es sei

$$\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \sigma(a) = a^p$$

der Frobeniushomomorphismus aus Definition 4.4.

Satz 6.6 Sei $q = p^n$ und $q' = p^m$ mit $m = n\nu$. $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$ ist eine zyklische Gruppe der Ordnung $\nu = [\mathbb{F}_{q'} : \mathbb{F}_q]$. Sie wird erzeugt von σ^n.

Beweis : Für $a \in \mathbb{F}_q, q = p^n$, ist $\sigma^n(a) = a^{p^{\cdots^p}} = a^q = a$, d.h. σ^n lässt $\mathbb{F}_q$ invariant. Also ist $\sigma^n \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$.
Da für alle $a \in \mathbb{F}_{q'}$

$$(\sigma^n)^\nu(a) = \sigma^m(a) = a^{q'} = a$$

gilt, ist $(\sigma^n)^\nu = \mathrm{id}$ in $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'})$, d.h. $\mathrm{ord}(\sigma^n)$ teilt ν. Ist $\mu = \mathrm{ord}\,(\sigma^n)$, so gilt für alle $a \in \mathbb{F}_{q'}$: $a^{p^{n\mu}} = \sigma^{n\mu}(a) = a$, d.h. alle $a \in \mathbb{F}_{q'}$ sind Nullstellen von $X^{p^{n\mu}} - X$. Dieses Polynom hat nach Satz 6.2 $p^{n\mu}$ verschiedene Nullstellen, also folgt $q' = p^m = p^{n\nu} \leq p^{n\mu}$, woraus $\nu \leq \mu$, also insgesamt $\mu = \nu$ folgt. Also hat σ^n die Ordnung ν, woraus wegen $\#\,\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = \nu$ dann $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q'}) = \langle\sigma^n\rangle$ folgt. □

7 Galoistheorie

Definition 7.1 Eine algebraische Körpererweiterung L/K heißt **galoissch**, wenn sie normal und separabel ist. In diesem Fall bezeichnen wir

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$$

als die Galoisgruppe der Erweiterung L/K.

Beispiel: Jede algebraische Erweiterung $\mathbb{F}/\mathbb{F}_q$ eines endlichen Körpers $\mathbb{F}_q$ ist nach Korollar 6.4 galoissch. Ist $\mathbb{F}/\mathbb{F}_q$ endlich und $q = p^n$, so ist nach Satz 6.6
$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) = \langle\sigma^n\rangle$ eine zyklische Gruppe der Ordnung $[\mathbb{F} : \mathbb{F}_q]$.

Proposition 7.2 Es sei L/K galoissch und E ein Zwischenkörper von L/K. Dann gilt:

i) L/E ist galoissch und $\mathrm{Gal}(L/E)$ ist in natürlicher Weise eine Untergruppe von $\mathrm{Gal}(L/K)$.

ii) Ist auch E/K galoissch, so ist für jedes $\tau \in \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ die Einschränkung $\tau|_E$ ein K-Automorphismus von L. Die Abbildung K

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \\ \tau & \mapsto & \tau_E \end{array}$$

ist ein surjektiver Gruppenhomomorphismus.

Beweis :

i) Nach Lemma 5.6 und Lemma 5.17 ist E/L galoissch. Jeder E-Automorphismus von L ist insbesondere ein K-Automorphismus, also ist $\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L)$ eine Untergruppe von $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

ii) Da E/K normal ist, vermittelt nach Satz 5.4 für jedes $\tau \in \mathrm{Aut}_K(L)$ die Einschränkung

$$\tau|_E : E \to L$$

einen Automorphismus von E.

Die Abbildung $\tau \mapsto \tau|_E$ vermittelt offenbar einen Gruppenhomomorphismus

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K).$$

Ist $\sigma \in \mathrm{Gal}(E/K) = \mathrm{Aut}_K(E)$, so lässt sich σ nach Satz 4.24 zu einem K-Homomorphismus $\sigma' : L \to \overline{E}$ fortsetzen. Da L/K normal ist, vermittelt σ' nach Satz 5.4 einen K-Automorphismus τ von L. Dieser erfüllt $\tau|_L = \sigma$. Der Homomorphismus zwischen den Galoisgruppen ist also surjektiv.

□

Proposition 7.3 Ist L/K endlich und normal, so ist

$$\mathrm{ord}\ \mathrm{Aut}_K(L) = [L : K]_s \leq [L : K]$$

Insbesondere gilt $\mathrm{ord}\ \mathrm{Aut}_K(L) = [L : K]$ genau dann, wenn L/K zusätzlich separabel ist. Für jede Galoiserweiterung L/K ist also $\mathrm{ord}\ \mathrm{Gal}(L/K) = [L : K]$.

Beweis : Da L/K normal ist, gilt mit Satz 5.4 $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Aut}_K(L)$, also folgt mit Satz 5.15 $\mathrm{ord}\ (\mathrm{Aut}_K(L)) = [L : K]_s \leq [L : K]$. Mit Satz 5.15 und Satz 5.16 folgt der Rest der Behauptung □

Definition 7.4 Ist L ein Körper und G eine Untergruppe der Körperautomorphismen $\mathrm{Aut}(L)$, so ist

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

der sogenannte **Fixkörper** von G.

Man muss hier natürlich nachrechnen, dass L^G tatsächlich ein Körper ist (ÜA). Offenbar ist L^G ein Teilkörper von L.

Satz 7.5 Es sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}(L)$.

i) Ist G endlich, so ist L/L^G eine endliche Galoiserweiterung vom Grad $[L : L^G] = \mathrm{ord}\ G$ mit Galoisgruppe $\mathrm{Gal}(L/L^G) = G$.

ii) Ist G nicht endlich, so ist L/L^G eine unendliche Galoiserweiterung und G eine Untergruppe von $\mathrm{Gal}(L/L^G)$.

Beweis : Wir zeigen zunächst, dass L/L^G separabel ist. Sei $a \in L$. Dann ist nach Lemma 4.23 für jedes $\sigma \in G$ das Element $\sigma(a) \in L$ eine Nullstelle von $\mathrm{Mipo}_{L^G}(a)$. Somit gibt es endlich viele, paarweise verschiedene $\sigma_1, \ldots, \sigma_r \in G$ mit

$$\{\sigma_1(a), \ldots, \sigma_r(a)\} = \{\sigma(a) : a \in G\}.$$

Jedes $\sigma \in G$ vermittelt eine Abbildung

$$\begin{aligned} \{\sigma_1(a), \ldots, \sigma_r(a)\} &\to \{\sigma_1(a), \ldots, \sigma_r(a)\} \\ \sigma_i(a) &\mapsto \sigma \circ \sigma_i(a). \end{aligned}$$

Da $\mathrm{id}(a) = a$ ist, ist ferner $a \in \{\sigma_1(a), \ldots, \sigma_r(a)\}$. Wir betrachten das Polynom

$$f = \prod_{i=1}^{r} (X - \sigma_i(a)).$$

Offenbar ist für alle $\sigma \in G$:

$$f^\sigma = \prod_{i=1}^{r} (X - \sigma \circ \sigma_i(a)) = f,$$

d.h. alle Koeffizienten von f werden von σ festgehalten. Somit ist $f \in L^G[X]$.
Ferner ist f nach Konstruktion ein separables Polynom mit $f(a) = 0$. Somit ist a separabel über L^G, d.h. L/L^G ist separabel. Ferner ist L/L^G normal, da L Zerfällungskörper aller Polynome f des obigen Typs über L^G ist (ÜA). Somit ist L/L^G galoissch.

Sei $n = \text{ ord}(G)$ für $n \in \mathbb{N}$. Dann gilt für jeden Teilkörper E von L/L^G mit E/L^G endlich, dass E/L^G separabel, nach dem Satz vom primitiven Element also einfach ist, d.h. $E = L^G(a)$. Nach dem oben Gezeigten ist $[E : L^G] = \deg \text{Mipo}_{L^G}(a) \leq \text{ ord}(G) = n$. L ist Vereinigung aller Teilkörper E mit E/L^G endlich. Es sei E ein solcher Teilkörper, für den $[E : L^G]$ maximal ist. Dann erfüllt jedes $a \in L : [E(a) : L^G] \leq [E : L^G]$, also $E(a) = E$. Somit ist $L = E$ endlich über L^G mit $[L : L^G] \leq n$. Jedes $\sigma \in G$ lässt L^G fest, d.h. G ist auch eine Untergruppe von $\text{Gal}(L/L^G)$. Somit folgt aus Proposition 7.3

$$n = \text{ ord } G \leq \text{ ord Gal}(L/L^G) = [L : L^G] \leq n,$$

d.h. insgesamt folgt $n = [L : L^G]$ und $G = \text{ Gal}(L/L^G)$.
Ist G nicht endlich, so zeigt dasselbe Argument, dass auch L/L^G nicht endlich sein kann und dass G eine Untergruppe von L/L^G ist (ÜA). □

Korollar 7.6 Es sei L/K eine normale algebraische Erweiterung mit $G = \text{ Aut}_K(L)$. Dann gilt

i) L/L^G ist galoissch mit $\text{Gal}(L/L^G) = G$

ii) L^G/K ist rein inseparabel.

iii) Ist L/K separabel und damit galoissch, so ist $L^G = K$.

Beweis :

i) folgt aus Satz 7.5, angewandt auf $G = \text{ Aut}_K(L)$. Da $\text{Aut}_K(L) = \text{ Aut}_{L^G}(L)$ ist, muss hier in jedem Fall (endlich oder unendlich) $\text{Gal}(L/L^G) = \text{ Aut}_{L^G}(L) = G$ sein.

ii) Da sich jeder K-Homomorphismus $\sigma : L^G \to \overline{K}$ mit Satz 4.24 nach L fortsetzen lässt und mit Satz 5.4 ein $\sigma' \in \text{ Aut}_K(L) = G$ vermittelt, ist $\sigma = \sigma'|_{L^G} = \text{id}$. Somit folgt
$$[L^G : K]_s = \#\,\text{Hom}_K(L^G, \overline{K}) = 1,$$
d.h. L^G/K ist rein inseparabel.

iii) Ist L/K separabel, so ist nach Lemma 5.17 auch L^G/K separabel, nach ii) muss also $[L^G : K] = [L^G : K]_s = 1$ sein, woraus $K = L^G$ folgt.

□

Jetzt können wir einen der wichtigsten Sätze dieser Vorlesung beweisen, den sogenannten Hauptsatz der Galoistheorie.

Satz 7.7 (Hauptsatz der Galoistheorie) Es sei L/K eine endliche Galoiserweiterung und $G = \text{Gal}(L/K)$. Dann sind die Zuordnungen

$$\begin{array}{ccc} \{ \text{ Untergruppen von } G\} & \begin{array}{c}\xrightarrow{\Phi}\\ \xleftarrow{\Psi}\end{array} & \{ \text{ Zwischenkörper von } L/K\} \\ H & \overset{\Phi}{\longmapsto} & L^H \\ \text{Gal}(L/E) & \longmapsto & E, \end{array}$$

welche einer Untergruppe $H \subset G$ ihren Fixkörper L^H bzw. einem Zwischenkörper E die Galoisgruppe von L/E zuordnen, bijektiv und invers zueinander.
L^H ist genau dann normal und damit galoissch über K, wenn H ein Normalteiler in G ist. In diesem Fall hat der surjektive Gruppenhomomorphismus

$$\begin{array}{ccc} G & \to & \text{Gal}(L^H/K) \\ \sigma & \mapsto & \sigma|_{L^H} \end{array}$$

den Kern H und induziert somit einen Isomorphismus $G/H \xrightarrow{\sim} \text{Gal}(L^H/K)$.

Beweis : Offenbar ist für jede Untergruppe H von G der Fixkörper L^H ein Zwischenkörper von L/K Mit G ist auch H endlich. Nach Korollar 7.6 i) ist L/L^H galoissch mit $\text{Gal}(L/L^H) = H$. Somit ist $\Psi(\Phi(H)) = H$.
Für jeden Zwischenkörper E von L/K ist nach Proposition 7.2 L/E galoissch und $H = \text{Gal}(L/E)$ eine Untergruppe von G. Nach Korollar 7.6 iii) ist $L^H = E$, d.h.

$$\Phi(\Psi(E)) = E.$$

Somit sind Φ und Ψ bijektiv und invers zueinander.
Angenommen, H ist eine Untergruppe, so dass der Fixkörper L^H normal über K ist. Dann ist L^H/K galoissch, nach Proposition 7.2 ii) ist also

$$\begin{array}{ccc} \varphi : G = \text{Gal}(L/K) & \to & \text{Gal}(L^H/K) \\ \sigma & \mapsto & \sigma|_{L^H} \end{array}$$

ein surjektiver Gruppenhomomorphismus. Es ist $\sigma \in \text{Kern}(\varphi)$ genau dann, wenn $\sigma|_{L^H} = \text{id}$ gilt. Also ist $\text{Kern}(\varphi) = \text{Aut}_{L^H}(L) = \text{Gal}(L/L^H) = H$. Als Kern eines Gruppenhomomorphismus ist H also ein Normalteiler von G. Umgekehrt sei H ein Normalteiler von G. Wir wählen einen algebraischen Abschluss $\overline{L}$ von L, dieser ist

gleichzeitig ein algebraischer Abschluss von K und von L^H. Es sei $\sigma : L^H \to \overline{L}$ ein K-Homomorphismus. Mit Satz 4.24 lässt sich σ zu einem K-Homomorphismus $\sigma_L : L \to \overline{L}$ fortsetzen, der aufgrund der Normalität von L den Körper L in sich überführt. Also ist $\sigma_L \in \mathrm{Aut}_K(L) = G$ und $\sigma = \sigma_L|_{L^H}$ faktorisiert als $\sigma : L^H \to L \hookrightarrow \overline{L}$. Sei $a \in L^H$ und $b = \sigma(a) = \sigma_L(a) \in L$. Da H ein Normalteiler von G ist, gilt $H\sigma_L = \sigma_L H$. Für jedes $\tau \in H$ existiert also ein $\tau' \in H$ mit $\tau\sigma_L = \sigma_L\tau'$. Daher ist $\tau b = \tau\sigma_L(a) = \sigma_L\tau'(a) \overset{a\in L^H}{=} \sigma_L(a) = b$, d.h. $b = \sigma(a) \in L^H$. Somit ist $\sigma(L^H) \subset L^H$. Mit Satz 4.24 lässt sich $\sigma^{-1} : \sigma(L^H) \to L^H$ zu einem K-Homomorphismus $\rho : L^H \to \overline{L}$ fortsetzen. Auf diesen wenden wir dasselbe Argument an und erhalten $\rho(L^H) \subset L^H$. Da auch $L^H \subset \rho(L^H)$ gilt, folgt $L^H = \rho(L^H)$ bzw. $\sigma(L^H) = L^H$. Also vermittelt jeder K-Homomorphismus $\sigma : L^H \to \overline{L}$ einen Automorphismus von L^H. L^H/K ist somit normal. □

Korollar 7.8 Jede endliche separable Körpererweiterlung L/K besitzt nur endlich viele Zwischenkörper.

Beweis : Sei M/K eine normale Hülle von L/K (vgl. Satz 5.7). Nach Satz 5.7 ii) ist M/K endlich. In 5.7 haben wir gesehen, dass für $L = K(a_1, \ldots, a_n)$ und $\{\sigma_1, \ldots, \sigma_m\} = \mathrm{Hom}_K(L, \overline{K})$

$$M \simeq K(\{\sigma_j(a_i) : i = 1, \ldots, n, j = 1, \ldots, m\})$$

gilt. Da für alle $i = 1, \ldots, n$ und alle $j = 1, \ldots, m$

$$\mathrm{Mipo}_K(\sigma_j(a_i)) = \mathrm{Mipo}_K(a_i)$$

gilt (ÜA), sind mit a_i auch alle $\sigma_j(a_i)$ separabel über K. Also ist M/K separabel. M/K ist also eine endliche Galoiserweiterung mit Zwischenkörper L. Es genügt zu zeigen, dass M/K endlich viele Zwischenkörper besitzt. Nach Definition 7.4 entsprechen die Zwischenkörper von M/K bijektiv den Untergruppen der endlichen Gruppe $\mathrm{Gal}(M/K)$. Davon gibt es endlich viele. □

Definition 7.9 Es seien E, E' Teilkörper von L. Das **Kompositum** EE' ist definiert als der kleinste Teilkörper von L, der E und E' enthält. Mit anderen Worten, es ist

$$EE' = E(\{a : a \in E'\}) = E'(\{b : b \in E\}).$$

Korollar 7.10 Sei L/K eine endliche Galois-Erweiterung mit Zwischenkörpern E und E'. Für $H = \mathrm{Gal}(L/E)$ und $H' = \mathrm{Gal}(L/E')$ gilt dann:

i) $E \subset E' \Leftrightarrow H' \subset H$

ii) $EE' = L^{H \cap H'}$

iii) $E \cap E' = L^{\langle H, H' \rangle}$, wobei $\langle H, H' \rangle$ die von H und H' erzeugte Untergruppe von G ist.

Beweis :

i) Für $E \subset E'$ ist offenbar $H' = \mathrm{Gal}(L/E') = \mathrm{Aut}_{E'}(L) \subset \mathrm{Aut}_E(L) = \mathrm{Gal}(L/E) = H$. Umgekehrt gilt für $H' \subset H$ mit Satz 7.7: $E = L^H \subset L^{H'} = E'$.

ii) Offenbar ist $EE' \subset L^{H \cap H'}$. Aus $E \subset EE'$ und $E' \subset EE'$ folgt mit i) $\mathrm{Gal}(L/EE') \subset \mathrm{Gal}\,(L/E) \cap \mathrm{Gal}(L/E') = H \cap H'$. Daraus folgt, wieder mit i),

$$L^{H \cap H'} \subset EE'.$$

iii) Offenbar ist $L^{\langle H, H' \rangle} = L^H \cap L^{H'}$, also folgt $L^{\langle H, H' \rangle} = E \cap E'$.

□

Definition 7.11 Eine Galoiserweiterung L/K heißt **abelsch** bzw. **zyklisch**, wenn $\mathrm{Gal}(L/K)$ abelsch bzw. zyklisch ist.

Nach Satz 6.6 ist jede Erweiterung endlicher Körper zyklisch und damit abelsch.

Korollar 7.12 Ist L/K eine endliche abelsche (bzw. zyklische) Galoiserweiterung, so ist für jeden Zwischenkörper E von L/K auch E/K eine endliche abelsche (bzw. zyklische) Erweiterung.

Beweis : Zyklische Gruppen sind abelsch. In jedem Fall ist also $\mathrm{Gal}(L/E)$ ein Normalteiler in $\mathrm{Gal}(L/K)$. Nach Satz 7.7 ist also E/K galoissch und $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$. Als Quotient einer endlichen abelschen (bzw. zyklischen) Gruppe ist auch $\mathrm{Gal}(E/K)$ endlich abelsch (bzw. zyklisch). □

Satz 7.13 Es sei L/K eine Körpererweiterung mit Zwischenkörpern E und E', so dass E/K und E'/K endliche Galoiserweiterungen sind. Dann gilt:

i) EE'/K ist endlich galoissch und der Homomorphismus

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(EE'/E) & \to & \mathrm{Gal}(E'/E \cap E') \\ & \sigma & \mapsto & \sigma|_{E'} \end{array}$$

ist bijektiv.

ii) Der Homomorphismus

$$\begin{aligned} \psi : \text{ Gal}(EE'/K) &\rightarrow \text{ Gal}(E/K) \times \text{ Gal}(E'/K) \\ \sigma &\mapsto (\sigma|_E, \sigma|_{E'}) \end{aligned}$$

ist injektiv. Ist $E \cap E' = K$, so ist ψ bijektiv.

Beweis :

i) Da $EE' = K(E, E')$ ist, ist EE' endlich, normal und separabel über K (ÜA). Ist $\sigma \in \text{ Gal}(EE'/E)$ mit $\sigma|_{E'} = \text{id}$, so gilt auch $\sigma|_E = \text{id}$, d.h. $\sigma = \text{id}$ auf ganz EE'. Somit ist φ injektiv.

$H = \text{ Bild}(\varphi)$ ist eine Untergruppe von $\text{Gal}(E'/E \cap E')$. Wir zeigen $E'^H = E \cap E'$. Ist $a \in E \cap E'$ und $\tau = \varphi(\sigma) = \sigma|_{E'}$ in H, so lässt σ den Körper E invariant, also folgt $\tau(a) = a$, d.h. $a \in E'^H$.

Gilt umgekehrt $a \in E'^H$, so folgt für jedes $\sigma \in \text{ Gal}(EE'/E)$: $\sigma(a) = \sigma|_{E'}(a) = \varphi(\sigma)(a) \overset{a \in E'^H}{=} a$, d.h. $a \in EE'^{\text{Gal}(EE'/E)} = E$. Insgesamt gilt also $a \in E \cap E'$. Aus $E'^H = E \cap E'$ folgt mit Satz 7.7:

$$H = \text{ Gal}(E'/E'^H) = \text{ Gal}(E'/E \cap E').$$

Also ist φ auch surjektiv.

ii) Sei $\sigma \in \text{ Gal}(EE'/K)$ im Kern von ψ. Dann sind $\sigma|_E$ und $\sigma|_{E'}$ trivial. Daher ist σ auf ganz EE' die Identität. Also ist ψ injektiv.

Angenommen, $E \cap E' = K$ und $(\sigma, \sigma') \in \text{ Gal}(E/K) \times \text{ Gal}(E'/K)$. Nach i) existiert eine Fortsetzung $\tilde{\sigma} \in \text{ Gal}(EE'/E')$ von σ und eine Fortsetzung $\tilde{\sigma}' \in \text{ Gal}(EE'/E)$ von σ'. Dann gilt für $\tilde{\sigma} \circ \tilde{\sigma}' \in \text{ Aut}_K(EE') = \text{ Gal}(EE'/K)$:

$$\tilde{\sigma} \circ \tilde{\sigma}'|_E = \tilde{\sigma}|_E \circ \tilde{\sigma}'|_E = \tilde{\sigma}|_E = \sigma$$

und

$$\tilde{\sigma} \circ \tilde{\sigma}'|_{E'} = \tilde{\sigma}|_{E'} \circ \tilde{\sigma}'|_{E'} = \tilde{\sigma}'|_{E'} = \sigma'$$

□

Wir wollen jetzt noch die Galoistheorie unendlicher Erweiterungen studieren. Hier kommt ein neues Phänomen ins Spiel, nämlich eine Topologie auf der Galoisgruppe. **Erinnerung:** Eine **Topologie** auf einer Menge X besteht aus einem System $\mathcal{T} = (U_i)_{i \in I}$ von Teilmengen von X (den sogenannten offenen Mengen), so dass folgende Bedingungen erfüllt sind:

i) $\emptyset, X$ sind offen.

ii) Die Vereinigung beliebig vieler offener Teilmengen ist offen.

iii) Der Schnitt endlich vieler offener Teilmengen ist offen.

Das Paar $(X, \mathcal{T})$ heißt dann **topologischer Raum.**
Ist $U_i \in \mathcal{T}$ offen, so heißt $X \setminus U_i$ abgeschlossen. Für jedes $x \in U_i$ wird U_i auch als offene Umgebung von x bezeichnet.
Eine Abbildung zwischen topologischen Räumen ist **stetig,** wenn Urbilder offener Mengen offen sind.

Definition 7.14 Eine topologische Gruppe ist eine Gruppe G, die eine Topologie $\mathcal{T}$ trägt, so dass die Gruppenverknüpfung

$$\begin{array}{rcl} G \times G & \to & G \\ (a, b) & \mapsto & ab \end{array}$$

und die Inversenbildung

$$\begin{array}{rcl} G & \to & G \\ a & \mapsto & a^{-1} \end{array}$$

stetig sind.

Sei uns L/K eine beliebige Galoiserweiterung und $\mathcal{L} = (L_i)_{i \in I}$ das System aller Zwischenkörper L_i, für die L_i/K endlich galoissch ist. Dann ist

$$\begin{array}{rcl} f_i : \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(L_i/K) \\ \sigma & \mapsto & \sigma|_{L_i} \end{array}$$

ein Gruppenhomomorphismus, der nach Proposition 7.2 surjektiv ist.
Wir definieren jetzt eine Topologie auf $\mathrm{Gal}(L/K)$.

Definition 7.15 Eine Teilmenge $U \subset \mathrm{Gal}(L/K)$ ist offen, wenn es zu jeden $\sigma \in U$ ein $i \in I$ mit $f_i^{-1}(f_i(\sigma)) \subset U$ gibt.

Lemma 7.16 $\mathrm{Gal}(L/K)$ ist eine topologische Gruppe.

Beweis : Offenbar sind $\emptyset$ und X offen sowie die Vereinigung beliebig vieler offener Teilmengen offen. Sind $U_1, \ldots, U_r$ offene Teilmengen, so existieren zu jedem $\sigma \in U_1 \cap \cdots \cap U_r$ Indizes $i_1, \ldots, i_r$ mit $f_{i_j}^{-1}(f_{i_j}(\sigma)) \subset U_j$ für alle $j = 1, \ldots, r$. Es sei L_k/K eine

endliche galoissche Erweiterung, die $L_{j_1}, \ldots, L_{j_r}$ enthält. (ÜA: Wieso existiert eine solche Erweiterung?) Dann ist $f_k^{-1}(f_k(\sigma))$ in allen $f_{i_j}^{-1}(f_{i_j}(\sigma))$ enthalten, also auch in $U_1 \cap \cdots \cap U_r$. Somit ist der Schnitt endlich vieler offener Mengen offen.
Sei $U \subset \text{Gal}(L/K)$ offen und $m : \text{Gal}(L/K) \times \text{Gal}(L/K) \to \text{Gal}(L/K)$ die Multiplikation. Für $(x, y) \in m^{-1}(U)$ existiert ein i, so dass $f_i^{-1}(f_i(xy)) \subset U$ gilt. Wir behaupten, dass $f_i^{-1}(f_i(x)) \times f_i^{-1}(f_i(y)) \subset \text{Gal}(L/K) \times \text{Gal}(L/K)$ in $m^{-1}(U)$ enthalten ist. Sei also $(a, b) \in f_i^{-1}(f_i(x)) \times f_i^{-1}(f_i(y))$, d.h. $f_i(a) = f_i(x)$ und $f_i(b) = f_i(y)$. Dann ist $f_i(ab) = f_i(a)f_i(b) = f_i(x)f_i(y) = f_i(xy)$, d.h. $ab \in f_i^{-1}(f_i(xy)) \subset U$, also $(a, b) \in m^{-1}(U)$. Also gibt es zu jedem $(x, y) \in m^{-1}(U)$ einen Index i mit $f_i^{-1}(f_i(x)) \times f_i^{-1}(f_i(y)) \subset m^{-1}(U)$. Somit ist $m^{-1}(U)$ offen in $\text{Gal}(L/K) \times \text{Gal}(L/K)$, die Multiplikation ist also stetig. Ein ähnliches Argument zeigt, dass die Inversenbildung stetig ist (ÜA). □

Man kann übrigens zeigen, dass die topologische Gruppe $\text{Gal}(L/K)$ kompakt ist.

Satz 7.17 (Hauptsatz der Galoistheorie für beliebige Erweiterungen) Es sei L/K eine Galoiserweiterung mit $G = \text{Gal}(L/K)$. Dann sind die Zuordnungen

$$\begin{array}{ccc} \{ \text{ abgeschlossene Untergruppen von } G\} & \begin{array}{c}\xrightarrow{\Phi}\\ \xleftarrow{\Psi}\end{array} & \{ \text{ Zwischenkörper von } L/K\} \\ H & \xmapsto{\Phi} & L^H \\ \text{Gal}(L/E) & \xmapsto{\Psi} & E \end{array}$$

bijektiv und invers zueinander.
Es ist L^H genau dann normal über K, wenn H ein abgeschlossener Normalteiler von G ist. In diesem Fall gilt:

$$G/H \simeq \text{Gal}(L^H/K).$$

Beweis : Aus Korollar 7.6 folgt, dass für jeden Zwischenkörper E von L/K $\Phi \circ \Psi(E) = E$ gilt. Wir zeigen jetzt, dass $\Psi(E) = \text{Gal}(L/E)$ abgeschlossen in G ist. Dazu sei $\sigma \in G \setminus \text{Gal}(L/E)$. Dann existiert ein $a \in E$ mit $\sigma(a) \neq a$. Da $K(a)/K$ endlich ist, ist die normale Hülle von $K(a)/K$ in L endlich galoissch über K. Somit existiert ein $i \in I$ mit $a \in L_i$. Sei nun $\tau \in f_i^{-1}(f_i(\sigma))$, d.h. es ist $\tau|_{L_i} = f_i(\tau) = f_i(\sigma) = \sigma|_{L_i}$. Somit ist

$$\tau(a) = \sigma(a) \neq a,$$

d.h. $\tau \notin \text{Gal}(L/E)$. Also gilt $f_i^{-1}(f_i(\sigma)) \subset G \setminus \text{Gal}(L/E)$, d.h. das Komplement von $\text{Gal}(L/E)$ ist offen und somit Gal (L/E) abgeschlossen.
Jetzt zeigen wir für jede abgeschlossene Untergruppe $H \subset \text{Gal}(L/K) : \Psi(\Phi(H)) = H$, d.h. $\text{Gal}(L/L^H) = H$. Für alle $i \in I$ sei $H_i = f_i(H) \subset \text{Gal}(L_i/K)$. Offenbar ist

$L_i^{H_i} \subset L^H \cap L_i$. Ist umgekehrt $x \in L^H \cap L_i$, d.h. $\sigma(x) = x$ für alle $\sigma \in H$, so folgt $f_i(\sigma)(x) = x$ und somit $x \in L_i^{H_i}$. Also gilt $L_i^{H_i} = L^H \cap L_i$.
Wir behaupten nun, dass $\mathrm{Gal}(L/L^H) = \bigcap_i f_i^{-1}(H_i)$ gilt.
Ist $\sigma \in \mathrm{Gal}(L/L^H)$, so ist für alle $i \in I$ $f_i(\sigma) = \sigma|_{L_i} \in \mathrm{Gal}(L_i/L^H \cap L_i) = \mathrm{Gal}(L^i/L_i^{H_i}) = H_i$ nach dem Hauptsatz für endliche Galoiserweiterungen. Ist umgekehrt $f_i(\sigma) \in H_i$ für alle $i \in I$, so lässt $\sigma|_{L_i}$ alle Körper $L_i^{H_i} = L^H \cap L_i$ fest. Also lässt σ ganz $L^H = \bigcup_i (L^H \cap L_i)$ fest, d.h. $\sigma \in \mathrm{Gal}(L/L^H)$.
Definitionsgemäß ist $H \subset \bigcap_{i \in I} f_i^{-1}(H_i)$. Wir zeigen nun auch die andere Inklusion. Ist nämlich σ in der offenen Teilmenge $G \setminus H$, so existiert ein $i \in I$ mit $f_i^{-1} f_i(\sigma) \subset G \setminus H$. Aus $f_i(\sigma) = f_i(\tau)$ folgt also $\tau \in G \setminus H$. Somit folgt $\sigma \notin f_i^{-1} f_i(H)) = f_i^{-1}(H_i)$. Insgesamt folgt $H = \bigcap_{i \in I} f_i^{-1}(H_i)$, also in der Tat $\mathrm{Gal}\,(L/L^H) = H$. Die Abbilungen Φ und Ψ sind also bijektiv und invers zueinander. Der Zusatz über Normalteiler lässt sich genau wie im endlichen Fall beweisen. □

8 Sylowsätze

Wir wollen jetzt noch einige Hilfsmittel kennenlernen, um (Galois-)Gruppen zu untersuchen.

Definition 8.1 Eine Operation einer Gruppe G auf einer Menge X ist eine Abbildung

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

mit

i) $1x = x$ für alle $x \in X$ und

ii) $(gh)x = g(hx)$ für alle $g, h \in G, x \in X$.

Beispiel: G operiert auf sich selbst durch Konjugation:

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto ghg^{-1}. \end{aligned}$$

Ist G abelsch, so ist dies die triviale Operation $(g, h) \mapsto h$.

Definition 8.2 Ist $G \times X \to X$ eine Operation von G auf X, so heißt $Gx = \{gx : g \in G\} \subset X$ die **Bahn** von $x \in X$. Ferner heißt $G_x = \{g \in G : gx = x\} \subset G$ die Isotropiegruppe von x oder der Stabilisator von x. G_x ist eine Untergruppe von G (ÜA).

Zwei Bahnen Gx und Gy sind entweder disjunkt oder gleich, denn aus $gx = hy \in Gx \cap Gy$ folgt $x = g^{-1}hy$, also $Gx \subset Gy$, und $y = h^{-1}gx$, also $Gy \subset Gx$. Also ist X die disjunkte Vereinigung aller Bahnen.

Lemma 8.3 Sei $G \times X \to X$ eine Operation von G auf X. Für jedes $x \in X$ induziert die Abbildung

$$\begin{array}{rcl} \varphi : G & \to & X \\ g & \mapsto & gx \end{array}$$

eine Bijektion $G/G_x \xrightarrow{\sim} Gx$, wobei G/G_x die Menge der Linksnebenklassen bezeichnet. Insbesondere ist

$$\text{ord}\,(Gx) = G : G_x.$$

Beweis : Es ist $\varphi(g) = \varphi(h) \Leftrightarrow gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$. Also vermittelt φ eine injektive Abbildung $G/G_x \to Gx$. Die Surjektivität ist klar. □

Sei X eine endliche Menge, auf der G operiert. Wir nennen $x_1, \ldots, x_r \in X$ ein Vertretersystem der Bahnen von X, falls X die disjunkte Vereinigung von Bahnen $B_1, \ldots, B_r$ ist und $x_i \in B_i$ für alle i gilt. In dieser Situation gilt

Satz 8.4 (Bahnengleichung)

$$\text{ord}(X) = \sum_{i=1}^{r} \text{ord}\,(Gx_i) = \sum_{i=1}^{r} (G : G_{x_i}),$$

wobei $\text{ord}(X)$ die Anzahl der Elemente in X bezeichnet.

Beweis : Es ist X die disjunkte Vereinigung der Bahnen B_i mit $B_i = Gx_i$. Dann gilt:

$$\begin{array}{rcl} \text{ord}(X) & = & \displaystyle\sum_{i=1}^{r} \text{ord}(Gx_i) \\ & = & \displaystyle\sum_{i=1}^{r} (G : G_{x_i}) \end{array}$$

nach Lemma 8.3. □

Wir wollen die Bahnengleichung auf die Operation von G auf sich vermöge Konjugation anwenden. Dazu definieren wir

Definition 8.5 Sei G eine Gruppe und $S \subset G$ eine Teilmenge von G.

i) $Z_S = \{h \in G : hs = sh \text{ für alle } s \in S\}$ heißt **Zentralisator** von S.

ii) $N_S = \{h \in G : hS = Sh\}$ heißt **Normalisator** von S.

iii) $Z = Z_G = \{h \in G : hg = gh \text{ für alle } g \in G\}$ heißt **Zentrum** von G.

Man rechnet leicht nach, dass Z_S und N_S Untergruppen von G sind (ÜA). Offenbar gilt für alle $g \in G$ die Gleichung $gZ = Zg$, d.h. $Z \subset G$ ist ein Normalteiler.

Satz 8.6 (Klassengleichung) Sei G eine endliche Gruppe und $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen von $G \setminus Z$ unter der Konjugationsoperation von G auf sich. Dann ist

$$\text{ord}(G) = \text{ord}(Z) + \sum_{i=1}^{r} G : Z_{\{x_i\}}.$$

Beweis : Für $z \in Z$ ist $gzg^{-1} = z$, d.h. $Gz = \{z\}$. Somit operiert G durch Konjugation auf dem Komplement $G \setminus Z$. Die Bahnen der Operation von G auf sich selbst sind also alle $\{z\}, z \in Z$ sowie $Gx_1, \ldots, Gx_r$. Die Behauptung folgt somit aus Satz 8.4, wenn wir noch $G_{x_i} = \{g \in G : gx_ig^{-1} = x_i\} = Z_{\{x_i\}}$ berücksichtigen. □

Jetzt wollen wir einige Resultate über die Existenz von Untergruppen mit gewissen Eigenschaften zeigen.

Definition 8.7 Sei G eine endliche Gruppe und p eine Primzahl.

i) G heißt p-Gruppe, falls $\text{ord}(G)$ eine p-Potenz ist.

ii) Eine Untergruppe $H \subset G$ heißt p-Sylowgruppe, wenn H eine p-Gruppe ist, so dass $p \nmid (G : H)$ gilt.

Eine p-Sylowgruppe ist also eine maximale p-Untergruppe von G.
Für $p \nmid \text{ord}(G)$ ist offenbar $\{1\}$ eine p-Sylowgruppe von G.

Satz 8.8 Es sei p prim und $\text{ord}(G) = p^k$ für ein $k \geq 1$. Dann ist p ein Teiler von $\text{ord}(Z)$, d.h. insbesondere ist $Z \neq 1$.

Beweis : Nach Satz 8.6 ist $p^k = \text{ord}(G) = \text{ord}(Z) + \sum_{i=1}^{r} G : Z_{\{x_i\}}$ für ein Vertretersystem $x_1, \ldots, x_r$ der Bahnen von $G \setminus Z$. Nach dem Satz von Lagrange gilt $G : Z_{\{x_i\}} \mid \text{ord}(G)$. Da $x_i \notin Z$, gilt $Z_{x_i} \neq G$, d.h. $G : Z_{\{x_i\}} \neq 1$. Da $\text{ord}(G)$ eine p-Potenz ist, ist dann p ein Teiler von $G : Z_{\{x_i\}}$. Somit muss auch p ein Teiler von $\text{ord}(Z)$ sein. □

Korollar 8.9 Sei p eine Primzahl und G eine p-Gruppe der Ordnung p^k, $k \geq 1$. Dann gibt es Untergruppen

$$G = G_k \supset G_{k-1} \supset \cdots \supset G_0 = \{1\}$$

in G, so dass für $l = 1, \ldots, k$ ord $G_l = p^l$ ist und G_{l-1} ein Normalteiler in G_l ist. Insbesondere gibt es für alle $l = 1, \ldots, k$ eine Untergruppe der Ordnung p^l, also auch ein Element der Ordnung p.

Beweis : Wir schließen mit Induktion nach k. Der Fall $k = 1$ ist trivial. Sei also $k > 1$. Nach Satz 8.8 ist $Z \neq 1$, also existiert ein $a \in Z$. Da $\text{ord}(a)$ ein Teiler von p^k ist, ist $\text{ord}(a) = p^r$ für ein $r \geq 1$, also $\text{ord}(a^{p^{r-1}}) = p$. Für $b = a^{p^{r-1}} \in Z$ ist $\langle b \rangle \subset G$ ein Normalteiler. Die Faktorgruppe $\overline{G} = G/\langle b \rangle$ hat die Ordnung p^{k-1}. Nach Induktionsvoraussetzung gibt es also Untergruppen

$$\overline{G} = \overline{G}_k \supset \overline{G}_{k-1} + \supset \cdots \supset \overline{G}_1 = 1$$

mit ord $\overline{G}_l = p^{l-1}$, so dass $\overline{G}_{l-1} \subset \overline{G}_l$ ein Normalteiler ist. Für die Projektion $\pi : G \to G/\langle b \rangle = \overline{G}$ setzen wir $G_l = \pi^{-1}(\overline{G}_l)$. Dann hat

$$G = G_k \supset G_{k-1} \supset \cdots \supset G_1 \supset \{1\}$$

die gewünschten Eigenschaften (ÜA). □

Satz 8.10 (Sylowsätze) Es sei G eine endliche Gruppe und p eine Primzahl.

i) Zu jeder p-Untergruppe $H \subset G$ existiert eine p-Sylowgruppe $S \subset G$ mit $H \subset S$. Insbesondere enthält G eine p-Sylowgruppe.

ii) Ist $S \subset G$ eine p-Sylowgruppe, so auch gSg^{-1} für jedes $g \in G$. Umgekehrt sind je zwei p-Sylowgruppen S_1 und S_2 konjugiert zueinander, d.h. es gibt ein $g \in G$ mit $gS_1g^{-1} = S_2$.

iii) Ist s_p die Anzahl der p-Sylowgruppen in G, so gilt $s_p \mid \text{ord}(G)$ und $s_p \equiv 1 \mod p$.

Zum Beweis des Satzes verwenden wir folgendes Lemma:

Lemma 8.11 Sei G eine Gruppe der Ordnung $n = p^k m$ mit einer Primzahl p und einer Zahl m. Dann gilt für die Anzahl s der p-Untergruppen $H \subset G$ mit ord$(H) = p^k$:

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

Beweis : Sei X die Menge aller p^k-elementigen Teilmengen von G. Dann ist ord$(X) = \binom{n}{p^k}$. Die Gruppe G operiert via $(g, U) \mapsto gU = \{gu : u \in U\}$ auf X (ÜA). $G(U) = \{gU : g \in G\}$ ist die Bahn von U unter G. Die Isotropiegruppe $G_U = \{g \in G : gU = U\}$ operiert via $(g, x) \mapsto gx$ auf der Menge U. Die Bahnen dieser Operation sind gewisse Rechtsnebenklassen $G_U x$ von G_U in G. Sie sind also paarweise disjunkt und haben alle (ord G_U)-viele Elemente. Somit ist ord G_U ein Teiler von ord$(U) = p^k$, d.h. ord$G_U = p^{k'}$ für ein $k' \leq k$.
Sei $(U_i)_{i=1,\ldots,r}$ ein Vertretersystem aller G-Bahnen auf X. Nach Satz 8.4 gilt

$$\binom{n}{p^k} = \text{ ord}(X) = \sum_{i=1}^{r} \text{ ord } G(U_i) = \sum_{i=1}^{r} (G : G_{U_i}).$$

Es ist ord$G_{U_i} = p^{k_i}$, nach dem Satz von Lagrange also $(G : G_{U_i}) = mp^{k-k_i}$. Für $I = \{i \in \{1, \ldots, r\} : k_i = k\} \subset \{1, \ldots, r\}$ gilt

$$\begin{aligned} \text{ord}(I)m &= \sum_{i \in I} (G : G_{U_i}) \\ &= \binom{n}{p^k} - \underbrace{\sum_{i \notin I} (G : G_{U_i})}_{=mp^{\geq 1}} \\ &\equiv \binom{n}{p^k} \mod (mp). \end{aligned}$$

Es genügt also nun zu zeigen, dass ord(I) mit der Anzahl s aller p-Untergruppen $H \subset G$ der Ordnung p^k überstimmt.
Sei $H \subset G$ eine solche p-Untergruppe. Dann ist $(G : H) = m$. Die G-Bahn von H, d.h. $G(H) = \{gH : g \in G\}$, besteht genau aus den Linksnebenklassen von H in G, hat also m Elemente. Also ist $G(H)$ eines der U_i mit $i \in I$. Ist $G(H_1) = G(H_2)$, so gilt $gH_1 = H_2$ für ein $g \in G$, woraus $gh = 1$ für ein $h \in H_1$, also $g = h^{-1} \in H_1$ folgt. Daher ist $H_1 = H_2$. Die p-Untergruppen H der Ordnung p^k liefern also verschiedene G-Bahnen $G(H) = U_i$ auf X mit $i \in I$. Umgekehrt gilt für jedes U_i mit $i \in I$, dass ord$(G_{U_i} = p^k$ ist. U_i ist eine Rechtsnebenklasse von G_{U_i} in G, d.h. $U_i = G_{U_i} u_i$ für ein $u_i \in U_i$. Also gilt

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

für die Untergruppe $H = u_i^{-1} G_{U_i} u_i$ der Ordnung $\text{ord}(H) = \text{ ord}(G_{U_i}) = p^k$ Somit ist jedes U_i für $i \in I$ von der Form $U_i = G(H)$ für eine eindeutig bestimmte Untergruppe H der Ordnung p^k. Also ist $s = \text{ ord}(I)$. □

Jetzt können wir die Sylowsätze beweisen.
Beweis von Satz 8.10 :

i) Ist $n = \text{ ord}(G) = mp^k$ mit $(p, m) = 1$, so gilt nach Lemma 8.11 für die Anzahl s_p der p-Sylowgruppen von G:

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

Um diese Zahl zu berechnen, wenden wir Lemma 8.11 auf die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ an, deren Untergruppen wir kennen. $\mathbb{Z}/n\mathbb{Z}$ enthält nämlich für jeden Teiler d von n genau eine zyklische Untergruppe $\frac{n}{d}\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ der Ordnung d. Also gilt

$$1 \equiv \binom{n-1}{p^k-1} \mod p,$$

und somit auch $s_p \equiv 1 \mod p$.

Insbesondere ist $s_p \neq 0$, d.h. G enthält eine p-Sylowgruppe S.

Ist $H \subset G$ eine beliebige p-Untergruppe, so betrachten wir die folgende Operation von H auf der Menge G/S der Linksnebenklassen von S in G:

$$\begin{aligned} H \times G/S &\to G/S \\ (h, gS) &\mapsto (hg)S. \end{aligned}$$

Die Bahnengleichung besagt, dass für ein Vertretersystem $x_1, \ldots, x_r$ der Bahnen gilt:

$$\text{ord } G/S = \sum_{i=1}^{r} \text{ ord}(Hx_i).$$

Nun ist $\text{ord } (G/S) = \text{ ord } G/ \text{ ord}(S) = \frac{n}{p^k} = m$. Die Ordnung der H-Bahnen Hx_i ist nach Lemma 8.3 gerade $(H : H_{x_i})$, also als Teiler von $\text{ord}(H)$ eine p-Potenz. Da $p \nmid m = \text{ ord}(G/S)$, muss es mindestens eine H-Bahn Hx_i der Ordnung $p^0 = 1$ geben. Dann ist $Hx_i = \{gS\}$ für ein $g \in G$, d.h. $hgS = gS$ für alle $h \in H$. Daher folgt $hg \in gS$, d.h. $h \in gSg^{-1}$. Somit gilt $H \subset gSg^{-1}$. Offenbar ist $gSg^{-1} \subset G$ eine Untergruppe (ÜA) und wegen $\text{ord}(gSg^{-1}) = \text{ ord}(S)$ auch eine p-Sylowgruppe von G.

ii) Wir haben schon gesehen, dass mit S auch gSg^{-1} eine p-Sylowgruppe ist. Ist S' eine weitere p-Sylowgruppe in G, so existiert nach i) ein $g \in G$ mit $S' \subset gSg^{-1}$. Da ord(S') = ord(S) = ord$(gSg^{-1}$ gilt, folgt $S' = gSg^{-1}$. Daher sind alle p-Sylowgruppen zueinander konjugiert.

iii) Wir haben schon gezeigt, dass $s_p \equiv 1 \bmod p$ gilt. Sei X die Menge der p-Sylowgruppen von G. Nach ii) ist die Konjugationsoperation

$$\begin{aligned} G \times X &\to X \\ (g, S) &\mapsto gSg^{-1} \end{aligned}$$

transitiv, d.h. sie hat nur eine Bahn. Daher folgt nach Lemma 8.3

$$\text{ord}X = G : G_S$$

mit

$$\begin{aligned} G_S &= \{g \in G : gSg^{-1} = S\} \\ &= N_S \end{aligned}$$

für den Normalisator N_S von S in G.

Also ist $s_p = (G : G_S)$ ein Teiler von ord(G).

□

Wir wollen jetzt an einem Beispiel zeigen, wie die Sylowsätze zur Untersuchung von Galoisgruppen eingesetzt werden können.
Beispiel: Sei E der Zerfällungskörper von $f = X^3 - 2$ über $\mathbb{Q}$. Für $\zeta = \exp \frac{2\pi i}{3} \in \mathbb{C}$ hat f die Nullstellen $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$, wobei $\sqrt[3]{2}$ die reelle Nullstelle von f ist. f ist irreduzibel nach Eisenstein, also ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Da Mipo$_{\mathbb{Q}}(\zeta) = X^2 + X + 1 = \frac{x^3-1}{x-1}$ gilt, folgt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$. Diese Grade sind teilerfremd, also folgt für $E = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, dass $[E : \mathbb{Q}] = 6$ gilt. Somit ist $G =$ Gal$(E/\mathbb{Q})$ eine Gruppe der Ordnung 6. Die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist normal, da $\zeta^2 \in \mathbb{Q}(\zeta)$, also ist Gal$(E/\mathbb{Q}(\zeta))$ ein Normalteiler der Ordnung 3 in G. Somit ist Gal$(E/\mathbb{Q}(\zeta))$ die einzige 3-Sylow-Gruppe in G. Gal$(E/\mathbb{Q}\sqrt[3]{2}))$ ist eine 2-Sylowgruppe, aber kein Normalteiler. Somit ist $s_2 > 1$. Andererseits gilt $s_2 \mid 6$ und $s_2 \equiv 1 (\text{mod } 2)$, also folgt $s_2 = 3$. G besitzt also außer den trivialen Untergruppen genau eine Untergruppe der Ordnung 3 und drei Untergruppen der Ordnung 2. Weitere kann es nach dem Satz von Lagrange nicht geben. Die zugehörigen Zwischenkörper sind $\mathbb{Q}, \mathbb{Q}(\zeta), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta\sqrt[3]{2}), \mathbb{Q}(\zeta^2\sqrt[3]{2})$ und E, wie man leicht zeigen kann.
Wir wollen jetzt die Sylowsätze anwenden, um den Fundamentalsatz der Algebra zu beweisen.

Satz 8.12 (Fundamentalsatz der Algebra) Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

Beweis : Wir benutzen hier folgende aus der Analysis bekannte Tatsachen über den Körper $\mathbb{R}$ der reellen Zahlen.

i) Jedes Polynom $f \in \mathbb{R}[X]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.

ii) Jedes $a \in \mathbb{R}_{\geq 0}$ besitzt eine Quadratwurzel in $\mathbb{R}$.

Wir zeigen zunächst, dass $\mathbb{C}$ keine Erweiterung vom Grad 2 besitzt. Angenommen, $f(X) = X^2 + uX + v \in \mathbb{C}[X]$ ist ein normiertes Polynom vom Grad 2. Dann ist $f(X) = \left(X + \frac{u}{2}\right)^2 + w$ mit $w = v - \frac{u^2}{4} \in \mathbb{C}$. Wir schreiben $w = r + is$ für $r, s \in \mathbb{R}$. Da $||w|| = \sqrt{r^2 + s^2} \geq \pm r$ ist, gibt es reelle Zahlen a, b mit $a^2 = \frac{||w|| - r}{2}$ und $b^2 = \frac{||w|| + r}{2}$. Für diese gilt $a^2 - b^2 = -r$ und $2|ab| = 2\sqrt{\frac{||w||^2 - r^2}{4}} = |s|$.
Wählen wir die Vorzeichen von a und b so, dass $2ab = -s$ gilt, so folgt $(a+ib)^2 + w = a^2 + 2iab - b^2 + w = 0$. Also hat f eine Nullstelle in $\mathbb{C}$, d.h. $\mathbb{C}$ besitzt keine Erweiterung vom Grad 2.
Sei nun $L/\mathbb{C}$ eine endliche Erweiterung von beliebigem Grad > 1. Dann gilt $2 \mid [L : \mathbb{R}]$, also ist $[L : \mathbb{R}] = 2^k m$ mit $k \geq 1$ und einer ungeraden Zahl m. Gal$(L/\mathbb{R})$ enthält nach Satz 8.10 eine 2-Sylowgruppe H, also eine Untergruppe der Ordnung 2^k. Dann ist $[L : L^H] = 2^k$ und $[L^H : \mathbb{R}] = m$. Ist a ein primitives Element von $L^H/\mathbb{R}$, so hat $f = \text{Mipo}_{\mathbb{R}}(a)$ als Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$. Also muss $m = 1$ sein. Somit ist $[L : \mathbb{R}] = 2^k$, also $[L : \mathbb{C}] = 2^{k-1}$, d.h. $k \geq 2$. Nach Korollar 8.9 existiert in der 2-Gruppe Gal$(L/\mathbb{C})$ eine Untergruppe H' der Ordnung 2^{k-2}. Für $L^{H'}$ ist dann $[L^{H'} : \mathbb{C}] = 2$. Das steht im Widerspruch zu der eingangs gezeigten Tatsache, dass $\mathbb{C}$ keine quadratischen Erweiterungen besitzt.
Also ist $\mathbb{C}$ algebraisch abgeschlossen. □

9 Einheitswurzeln

Es sei K ein Körper und $\overline{K}$ ein algebraischer Abschluss.

Definition 9.1 Die Nullstellen des Polynoms $X^n - 1$ in $\overline{K}$ heißen n-te **Einheitswurzeln** in $\overline{K}$. Sie bilden eine Untergruppe $U_n \subset \overline{K}^*$.

Für char$K \nmid n$ ist $x^n - 1$ separabel, d.h. U_n hat n Elemente. Gilt char$K = p$ und $n = mp^r$ mit ggT$(m, p) = 1$, so ist $X^n - 1 = (X^m - 1)^{p^r}$ und $U_n = U_m$. Somit kann man sich bei der Untersuchung von U_n oft auf den Fall char$K \nmid n$ beschränken.
Nach Satz 5.20 ist U_n als Untergruppe von $\overline{K}^*$ zyklisch.

Definition 9.2 Für char $K \nmid n$ heißt jeder Erzeuger der zyklischen Gruppe U_n **primitive** n-te Einheitswurzel.

Beispiel: In $\mathbb{C}$ ist $U_n = \{\exp \frac{2\pi ik}{n} : k = 0, \ldots, n-1\}$.

Definition 9.3 Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ mit

$$\varphi(n) = \text{ ord}(\mathbb{Z}/n\mathbb{Z})^*$$

heißt **Eulersche φ-Funktion**.

Da $(\mathbb{Z}/n\mathbb{Z})^* = \#\{d \mod n\mathbb{Z} : \text{ ggT}(d,n) = 1\}$ gilt, folgt $\varphi(n) = \#\{d \in \{1, \ldots, n\} : d$ teilerfremd zu $n\}$. Genau die Elemente in $(\mathbb{Z}/n\mathbb{Z})^*$ sind die Erzeuger der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$ (ÜA).

Satz 9.4 Es gelte char$(K) \nmid n$. Sei ζ eine primitive n-te Einheitswurzel. Dann ist ζ^k genau dann primitv, wenn ggT $(k,n) = 1$ ist. Insbesondere enthält U_n genau $\varphi(n)$ primitive Einheitswurzeln.

Beweis : Da $U_n = \langle\zeta\rangle$ gilt, ist $\mathbb{Z}/n\mathbb{Z} \simeq U_n$ vermöge $k \mapsto \zeta^k$. Da k genau dann ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ ist, wenn ggT$(k,n) = 1$ gilt, folgt die Behauptung. □

Satz 9.5 Es sei $\zeta \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoissch mit $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Der Körper $\mathbb{Q}(\zeta)$ heißt auch n-ter **Kreisteilungskörper**.

Beweis : Offenbar ist $X^n - 1$ ein separables Polynom in $\mathbb{Q}[X]$, dessen Nullstellen alle in $\mathbb{Q}(\zeta)$ liegen. Als Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist $\mathbb{Q}(\zeta)$ galoissch über $\mathbb{Q}$. Sei $f = \text{ Mipo}_{\mathbb{Q}}(\zeta)$. Jedes $\sigma \in \text{ Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ vermittelt einen Automorphismus von U_n (ÜA), insbesondere ist auch $\sigma(\zeta)$ primitiv. Da es zu jeder Nullstelle η von f nach Lemma 4.23 ein $\sigma \in \text{ Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $\sigma(\zeta) = \eta$ gibt, so ist η auch eine primitive Einheitswurzel. Also ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \text{ grad}(f) \leq \varphi(n)$. Als Minimalpolynom von ζ über $\mathbb{Q}$ teilt f das Polynom $X^n - 1$, d.h. es ist

$$X^n - 1 = f \cdot h$$

für ein $h \in \mathbb{Q}[X]$. Mit f ist auch h normiert, nach Korollar 1.13 gilt also $f, h \in \mathbb{Z}[X]$. Ist p eine Primzahl mit $p \nmid n$, so ist ζ^p eine primitive n-te Einheitswurzel. Angenommen $f(\zeta^p) \neq 0$. Dann folgt $h(\zeta^p) = 0$., d.h. ζ ist Nullstelle von $h(X^p)$. Also ist $h(X^p) = f(X)g(X)$ für ein Polynom $g(X)$. Mit f ist auch g normiert. Nach Korollar 3.13 gilt $f, g \in \mathbb{Z}[X]$. Unter dem Homomorphismus

$$\begin{aligned} \mathbb{Z}[X] &\to \mathbb{F}_p[X], \\ f &\mapsto \overline{f}, \end{aligned}$$

der die kanonische Projektion $\mathbb{Z} \to \mathbb{F}_p$ fortsetzt, gilt $\overline{h}^p = \overline{h(X^p)} = \overline{f}\overline{g}$, also sind $\overline{f}$ und $\overline{h}$ nicht teilerfremd in $\mathbb{F}_p[X]$. Also hat $X^n - 1 = \overline{f} \cdot \overline{h} \in \mathbb{F}_p[X]$ mehrfache Nullstellen in einem algebraischen Abschluss $\overline{\mathbb{F}}_p$. Da p kein Teiler von n ist, ist dies ein Widerspruch. Somit gilt $f(\zeta^p) = 0$.
Sei ζ' eine beliebige primitive m-te Einheitswurzel, also $\zeta' = \zeta^m$ mit ggT$(m, n) = 1$. Dann entsteht ζ' aus ζ durch wiederholtes Potenzieren mit den Primteilern von m. Nach dem oben gezeigten ist also $f(\zeta') = 0$.
Also sind alle primitiven n-ten Einheitswurzeln Nullstellen von f, so dass auch $\varphi(n) \leq$ grad(f), insgesamt also $\varphi(n) =$ grad(f) gilt. □

Satz 9.6 Es sei K ein Körper und $\zeta \in \overline{K}$ eine primitive n-te Einheitswurzel mit char$(K) \nmid n$.

i) $K(\zeta)/K$ ist eine endliche abelsche Galois-Erweiterung vom Grad $\leq \varphi(n)$.

ii) Zu jedem $\sigma \in$ Gal$(K(\zeta)/K)$, existiert eine natürliche Zahl $r(\sigma)$ mit $\sigma(\zeta) = \zeta^{r(\sigma)}$, wobei $\overline{r(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ eine Einheit ist, die nicht von der Wahl von ζ abhängt. Die Abbildung

$$\begin{array}{rccc} \psi: & \text{Gal}(K(\zeta)/K) & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ & \sigma & \mapsto & \overline{r(\sigma)} \end{array}$$

ist ein injektiver Gruppenhomomorphismus. Für $K = \mathbb{Q}$ ist ψ sogar ein Isomorphismus.

Beweis :

i) Als Zerfällungskörper des separablen Polynoms $X^n - 1 \in K[X]$ ist $K(\zeta)$ endlich und galoissch über K. Aus ii) folgt, dass $K(\zeta)/K$ abelsch ist und dass $[K(\zeta) : K] =$ ord Gal$(K(\zeta)/K) \leq$ ord$(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ ist. Also müssen wir nur noch ii) zeigen.

ii) Da $\sigma(\zeta)$ eine primitive Einheitswurzel ist, gilt $\sigma(\zeta) = \zeta^{r(\sigma)}$ für ein $r(\sigma)$, dessen Restklasse $\overline{r(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ eine Einheit ist. Ist ζ' eine weitere primitive Einheitswurzel, so gilt nach Satz 9.4, dass $\zeta' = \zeta^r$ für ein $r \in (\mathbb{Z}/n\mathbb{Z})^*$ ist. Also ist $\sigma(\zeta') = \sigma(\zeta)^r = \zeta^{r(\sigma)r} = (\zeta')^{r(\sigma)}$. Somit ist $\overline{r(\sigma)}$ unabhängig von der Wahl von ζ.

Offenbar ist ψ ein Gruppenhomomorphismus. Ist $\overline{r(\sigma)} = \overline{r(\tau)}$, so folgt $\sigma(\zeta) = \tau(\zeta)$, also $\sigma = \tau$. Somit ist ψ injektiv.

Für $K = \mathbb{Q}$ ist nach Satz 9.5

$$\text{ord}(\text{ Gal}(K(\zeta)/K)) = \varphi(n) = \text{ ord}((\mathbb{Z}/n\mathbb{Z})^*),$$

also ist hier ψ auch surjektiv.

□

Korollar 9.7 Es sei $\zeta \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine abelsche Erweiterung mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^*$.

Wir werden folgenden Satz für die Untersuchung zyklischer Erweiterungen brauchen, ihn allerdings hier nicht beweisen.

Satz 9.8 Sei L/K eine zyklische Galoiserweiterung vom Grad n.

i) Falls char$K \nmid n$ und K eine primitive n-te Einheitswurzel ζ enthält, so gibt es einen Erzeuger σ von Gal(L/K) und ein $a \in L^*$ mit $\sigma(a) = \zeta a$.

ii) Falls $n = \text{ char}(K) = p > 0$ gilt, so gibt es einen Erzeuger σ von Gal(L/K) und ein $a \in L^*$ mit $\sigma(a) - a = 1$.

Beweis : mit dem sogenannten Satz 90 von Hilbert, siehe [Bo], 4.7 und 4.8 □

Satz 9.9 Sei L/K eine endliche Körpererweiterung und $\zeta \in K$ eine primitive n-te Einheitswurzel.

i) Ist L/K zyklisch vom Grad n mit char$K \nmid n$, so ist $L = K(a)$ für ein $a \in L$ mit $\text{Mipo}_K(a) = X^n - c \in K[X]$.

ii) Ist $L = K(a)$ und a Nullstelle von $X^n - c \in K[X]$ mit char$K \nmid n$, so ist L/K zyklisch, $d = [L : K]$ ein Teiler von n und $\text{Mipo}_K(a) = X^d - a^d$.

Beweis :

i) Nach Satz 9.8 existiert ein Erzeuger σ von Gal(L/K) und ein $a \in L^*$ mit $\sigma(a) = \zeta a$. Also ist $\sigma^k(a) = \zeta^k(a)$ für $k = 1, \ldots, n$. Insbesondere sind dies k verschiedene Elemente, woraus $[K(a) : K] \geq n$ folgt. Also ist $L = K(a)$. Da $a^n = \zeta^n a^n = \sigma(a)^n = \sigma(a^n)$ gilt, folgt $a^n \in K$. Somit ist a Nullstelle von $X^n - a^n \in K[X]$. Da dieses Polynom den Grad $n = [K(a) : K]$ hat, folgt $\text{Mipo}_K(a) = X^n - a^n$.

ii) Ohne Einschränkung ist $a \neq 0$. Dann hat $X^n - c$ die n verschiedenen Nullstellen $a, \ldots, \zeta^{n-1}a$, so dass $L = K(a)$ ein Zerfällungskörper von $X^n - c$ ist. Da $\mathrm{char}K \nmid n$ gilt, ist $X^n - c$ separabel, L/K also galoissch. Für jedes $\sigma \in \mathrm{Gal}(L/K)$ ist auch $(\sigma(a))^n = c = a^n$, also ist $\sigma(a)/a = w_\sigma \in U_n \subset K$. Die Zuordnung $\sigma \mapsto \frac{\sigma(a)}{a}$ definiert offenbar eine injektive Abbildung $\mathrm{Gal}(L/K) \to U_n$, die wegen

$$\frac{\tau\sigma(a)}{a} = \frac{\tau(\sigma(a))}{\tau(a)}\frac{\tau(a)}{a} \overset{\frac{\sigma(a)}{a} \in K}{=} \frac{\sigma(a)}{a}\frac{\tau(a)}{a}$$

ein Gruppenhomomorphismus ist. Also ist $\mathrm{Gal}(L/K)$ als Untergruppe der zyklischen Gruppe U_n zyklisch der Ordnung d für ein $d \mid n$. Ist σ ein Erzeuger von $\mathrm{Gal}(L/K)$, so ist w_σ eine d-te Einheitswurzel, und es gilt

$$\sigma(a^d) = \sigma(a)^d = w_\sigma^d \cdot a^d = a^d.$$

Also ist $a^d \in K$ und a Nullstelle von $X^d - a^d \in K[X]$. Aus Gradgründen ist $X^d - a^d = \mathrm{Mipo}_K(a)$.

□

Satz 9.10 Es sei L/K eine Körpererweiterung mit $\mathrm{char}K = p > 0$.

i) Ist L/K zyklisch vom Grad p, so ist $L = K(a)$ für ein $a \in L$ mit $\mathrm{Mipo}_K(a) = X^p - X - c \in K[X]$.

ii) Ist $L = K(a)$ für eine Nullstelle a von $X^p - X - c \in K[X]$, so ist L/K zyklisch. Entweder zerfällt $X^p - X - c$ vollständig über K in Linearfaktoren oder es ist irreduzibel. Im letzteren Fall ist $[L : K] = p$.

Beweis :

i) Nach Satz 9.8 gibt es einen Erzeuger σ von $\mathrm{Gal}(L/K)$ und ein $a \in L$ mit $\sigma(a) - a = 1$. Es folgt mit Induktion, dass

$$\sigma^k(a) - a = k \text{ für } k = 0, \ldots, p-1$$

gilt. Da $a, \sigma(a), \ldots, \sigma^{p-1}(a)$ paarweise verschieden sind, so gilt $[K(a) : K] \geq p$, also $L = K(a)$. Außerdem ist

$$\begin{aligned} \sigma(a^p - a) &= \sigma(a)^p - \sigma(a) \\ &= (a+1)^p - (a+1) \\ &= a^p - a, \end{aligned}$$

also ist $c = a^p - a \in K$. Es folgt aus Gradgründen, dass $X^p - X - c \in K[X]$ das Minimalpolynom von a über K ist.

ii) siehe Aufgabe 50.

□

10 Auflösbare Erweiterungen

Wir wollen jetzt noch einmal auf die Frage zurückkommen, welche Gleichungen durch Radikale auflösbar sind. Dazu studieren wir zunächst die sogenannten auflösbaren Gruppen.

Definition 10.1 Ist G eine Gruppe, so heißt die von allen Elementen der Form $[a,b] := aba^{-1}b^{-1}$ mit $a,b \in G$ erzeugte Untergruppe von G die **Kommutatorgruppe**. Wir bezeichnen sie mit $[G,G]$. Das Element $[a,b]$ heißt Kommutator von a und b. Offenbar ist G abelsch genau dann, wenn $[G,G] = \{1\}$ ist.

Lemma 10.2 i) $[G,G]$ besteht aus allen endlichen Produkten von Elementen der Form $[a,b]$ für $a,b \in G$.

ii) $[G,G] \subset G$ ist ein Normalteiler, und zwar der kleinste unter allen Normalteilern N, so dasss G/N abelsch ist.

Beweis :

i) Es ist $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$. Somit bildet die Menge aller endlichen Produkte von Kommutatoren $[a,b]$ eine Untergruppe von G, die offenbar mit $[G,G]$ übereinstimmt.

ii) Es ist für alle $a,b,g \in G$:

$$\begin{aligned} g[a,b]g^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \\ &= [gag^{-1}, gbg^{-1}]. \end{aligned}$$

Also ist $[G,G]$ ein Normalteiler in G. Ist $N \subset G$ ein Normalteiler mit G/N abelsch, so sei $\pi : G \to G/N$ die Projektion. Dann ist $\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}) = 1$, also $[a,b] \in N$. Somit ist $[G,G] \subset N$. Dieselbe Rechnung zeigt, dass $G/[G,G]$ abelsch ist.

□

Definition 10.3 Sei G eine Gruppe. Eine Kette von Untergruppen

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

heißt eine **Normalreihe** von G, wenn G_{i+1} jeweils ein Normalteiler in G_i ist.
Die Quotienten G_i/G_{i+1} heißen Faktoren der Normalreihe.
G heißt **auflösbar**, wenn G eine Normalreihe mit abelschen Faktoren besitzt.

Beispiel: Wir definieren induktiv Untergruppen $D^iG \subset G$ durch

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

Die Kette $G = D^0G \supset D^1G \supset \ldots$ hat nach Lemma 10.2 die Eigenschaft, dass $D^iG \subset D^{i+1}G$ ein Normalteiler mit $D^{i+1}G/D^iG$ abelsch ist.

Satz 10.4 G ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}_0$ mit $D^nG = \{1\}$ gibt.

Beweis : Ist $D^nG = \{1\}$, so ist G offenbar auflösbar. Ist umgekehrt

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

eine Normalreihe mit abelschen Faktoren, so zeigen wir induktiv, dass $D^iG \subset G_i$ gilt. Für $i = 0$ stimmt das. Gelte also $D^iG \subset G_i$ für ein $i \geq 0$. Da G_i/G_{i+1} abelsch ist, ist nach Lemma 10.2 ii) $[G_i, G_i] \subset G_{i+1}$, also auch $D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i] \subset G_{i+1}$.
Somit muss mit G_n auch D^nG trivial sein. □

Beispiel:

i) Jede abelsche Gruppe ist auflösbar.

ii) Jede endliche p-Gruppe (p Primzahl) ist nach Korollar 8.9 auflösbar, da Gruppen der Ordnung p zyklisch und somit abelsch sind.

iii) Die Gruppe S_5 der Permutationen einer 5-elementigen Menge ist nicht auflösbar. Ist nämlich

$$A_5 = \{\pi \in S_5 : \text{ sgn}\pi = 1\}$$

die Untergruppe aller Permutationen, die sich als Produkt von einer geraden Anzahl von Transpositionen (Vertauschungen) schreiben lassen, so gilt $[A_5, A_5] = A_5$.

Ist nämlich τ_{ij} die Vertauschung von i und j für $i \neq j$, so gilt

$$\tau_{ij}\tau_{jk} = (\tau_{ik}\tau_{rs})(\tau_{jk}\tau_{rs})(\tau_{jk}\tau_{rs})^{-1}(\tau_{jk}\tau_{rs})^{-1},$$

wobei $\{i,j,k,r,s\} = \{1,2,3,4,5\}$. Für paarweise verschiedene i,j,k,l gilt $\tau_{ij}\tau_{kl} = (\tau_{il}\tau_{lk})(\tau_{ij}\tau_{jk})$, also nach dem soeben Gezeigten ebenfalls $\tau_{ij}\tau_{kl} \in [A_5, A_5]$. Daher ist jedes Element in A_5 Produkt von Kommutatoren. Somit ist A_5 nicht auflösbar, also auch nicht S_5, die A_5 als Normalteiler vom Index 2 enthält (siehe unten Satz 10.6).

Satz 10.5 Sei G eine endliche auflösbare Gruppe. Dann lässt sich in G jede echt absteigende Normalreihe mit abelschen Faktoren zu einer Normalreihe verfeinern, deren Faktoren zyklisch von Primzahlordnung sind.

Beweis : Ist $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = 1$ eine Normalreihe mit abelschen Faktoren, und G_i/G_{i+1} nicht zyklisch von Primzahlordnung, so sei $1 \neq \overline{a} \in G_i/G_{i+1}$. Dann ist $\langle\overline{a}\rangle \subsetneq G_i/G_{i+1}$ ein Normalteiler, das Urbild von $\langle\overline{a}\rangle$ unter $G_i \to G_i/G_{i+1}$ ist also ein Normalteiler H in G_i mit $G_{i+1} \subsetneq H \subsetneq G_i$. Offenbar ist G_{i+1} ein Normalteiler nicht nur in G_i, sondern auch in H. Also können wir die Normalreihe durch H verfeinern. Da H/G_{i+1} als Untergruppe von G_i/G_{i+1} und G_i/H als Quotient von G_i/G_{i+1} abelsch sind, hat auch die neue Normalreihe abelsche Faktoren. Wiederholt man dieses Verfahren, so gelangt man nach endlich vielen Schritten zu einer Normalreihe, deren Faktoren zyklisch von Primzahlordnung sind. □

Satz 10.6 Es sei G eine Gruppe und $H \subset G$ eine Untergruppe. Ist G auflösbar, so auch H. Ist H ein Normalteiler in G, so ist G genau dann auflösbar, wenn H und G/H auflösbar sind.

Beweis : Ist G auflösbar, so ist wegen $D^iH \subset D^iG$ auch jede Untergruppe H auflösbar. Ist H ein Normalteiler, so betrachten wir $\pi : G \to G/H$. Es ist $D^i(\pi(G)) = \pi(D^iG)$ (ÜA), also ist mit G auch $\pi(G) = G/H$ auflösbar.
Sind umgekehrt H und G/H auflösbar, so existiert ein $n \in \mathbb{N}$ mit $D^nH = \{1\}$ und $D^n(G/H) = \{1\}$. Es folgt

$$\pi(D^nG) = D^n(G/H) = \{1\},$$

d.h. $D^nG \subset H$. Also ist $D^{2n}G = D^n(D^nG) \subset D^nH = \{1\}$, d.h. G ist auflösbar. □

Definition 10.7 Eine endliche Körpererweiterung L/K heißt **durch Radikale auflösbar**, wenn es einen Erweiterungskörper E von L sowie eine Körperkette

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

gibt, so dass E_{i+1} jeweils aus E_i durch Adjunktion eines Elements des folgenden Typs entsteht:

i) einer Einheitswurzel oder

ii) einer Nullstelle von $X^n - a \in E_i[X]$ mit $\text{char}(K) \nmid n$, oder

iii) einer Nullstelle von $X^p - X - a \in E_i[X]$ mit $p = \text{ char}(K) > 0$.

Offenbar ist jede durch Radikale auflösbare Körpererweiterung separabel. Ist L/K durch Radikale auflösbar und char$K = 0$, so gibt es für jedes Element von L eine Formel, die mit den Grundrechenarten und Wurzelziehen auskommt.

Definition 10.8 Eine endliche Körpererweiterung L/K heißt **auflösbar**, wenn es einen Erweiterungskörper E von L gibt so dass E/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe ist (im Sinne von Definition 10.3).

Lemma 10.9 Ist L/K galoissch, so ist L/K genau dann auflösbar, wenn $\text{Gal}(L/K)$ auflösbar ist.

Beweis : Sei E ein Erweiterungskörper wie in Definition 10.8. Da L/K normal ist, ist $H = \text{ Gal}(E/L)$ ein Normalteiler in $G = \text{ Gal}(E/K)$ und

$$G/H \xrightarrow{\sim} \text{ Gal}(L/K).$$

Nach Satz 10.6 ist mit G dann auch $\text{Gal}(L/K)$ auflösbar. Die andere Richtung ist klar. □

Definition 10.10 Ist $f \in K[X]$ ein nicht-konstantes separables Polynom und L/K ein Zerfällungskörper von f. Dann heißt die algebraische Gleichung $f(X) = 0$ über K auflösbar bzw. durch Radikale auflösbar, falls L/K auflösbar bzw. durch Radikale auflösbar ist.

Lemma 10.11 Ist L/K eine endliche Körpererweiterung und F ein beliebiger Erweiterungskörper von K. Bettet man L mit einem K-Homomorphismus in den algebraischen Abschluss $\overline{F}$ ein, so sei FL das Kompositum in $\overline{F}$. Ist L/K auflösbar bzw. galoissch mit auflösbarer Galoisgruppe bzw. durch Radikale auflösbar bzw. durch eine Körperkette wie in Definition 10.7 ausschöpfbar, so hat FL/F dieselbe Eigenschaft.

Beweis : Ein K-Homomorphismus $L \hookrightarrow \overline{F}$ existiert nach Satz 4.24. Ist E/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe und $L \subset E$, so lässt sich diese Einbettung auf E fortsetzen. Nach dem Satz vom primitiven Element ist $E = K(a)$, also ist E Zerfällungskörper von $\text{Mipo}_K(a)$. Somit ist $EF = F(a)$ als

Zerfällungskörper des separablen Polynoms $\text{Mipo}_K(a)$ eine endliche Galoiserweiterung von F. Für jedes $\sigma \in \text{Gal}(EF/F)$ ist $\sigma(E)$ eine algebraische Erweiterung von $K = \sigma(K)$. Also folgt aus der Normalität von E/K, dass $\sigma(E) = E$ ist. Wir erhalten einen Homomorphismus.

$$\begin{array}{ccc} \text{Gal}(EF/F) & \to & \text{Gal}(E/K) \\ \sigma & \mapsto & \sigma|_E. \end{array}$$

Dieser ist wegen $EF = F(E)$ injektiv. Aus der Auflösbarkeit von $\text{Gal}(E/K)$ folgt also die von $\text{Gal}(EF/F)$ nach Satz 10.6.
Besitzt andererseits E/K eine Körperkette

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

wie in Definition 10.7, so ist

$$F \subset E_1F \subset E_2F \subset \cdots \subset E_mF = EF$$

eine analoge Körperkette von EF/F. Daraus folgt die Behauptung. □

Lemma 10.12 Ist $K \subset L \subset M$ eine Kette endlicher Körpererweiterungen, so ist M/K genau dann auflösbar (bzw. durch Radikale auflösbar), wenn M/L und L/K auflösbar (bzw. durch Radikale auflösbar) sind.

Beweis : Sei zunächst M/K auflösbar und M' ein Erweiterungskörper von M, für den M'/K galoissch mit auflösbarer Galoisgruppe ist. Definitionsgemäß ist dann auch L/K auflösbar. $\text{Gal}(M'/L)$ ist als Untergruppe von $\text{Gal}(M'/K)$ nach Satz 10.6 auflösbar. Also ist auch M/L auflösbar.
Umgekehrt seien L/K und M/L auflösbar. Sei $L' \supset L$ eine Erweiterung, so dass L'/K galoissch mit auflösbarer Galoisgruppe ist, und sei $M' \supset M$ eine Erweiterung, so dass M'/L galoissch mit auflösbarer Galoisgruppe ist. Dann ist nach Lemma 10.11 auch $L'M'/L'$ galoissch mit auflösbarer Galoisgruppe. Indem wir $L \subset M$ durch $L' \subset L'M'$ ersetzen, können wir annehmen, dass L/K und M/L galoissch mit auflösbarer Galoisgruppe sind.
Dann ist M/K separabel, eventuell aber nicht normal. Sei M'/K die normale Hülle von M/K. Dann ist M'/K endlich galoissch. Nach Satz 5.7 können wir M' folgendermaßen konstruieren: Sei $\overline{M}$ ein algebraischer Abschluss von M, so ist M' das Kompositum der $\sigma(M)$ in $\overline{M}$, wobei σ alle K-Homomorphismen $M \to \overline{M}$ durchläuft. Da L/K galoissch ist, gilt für jeden K-Homomorphismus $\sigma : M \to \overline{M}$,

dass $\sigma(L) = L$ ist. Also ist $\sigma(M)/L$ eine zu M/L isomorphe Galoiserweiterung, d.h. $\text{Gal}(\sigma(M)/L) \simeq \text{Gal}(M/L)$.
Wir behaupten, dass Gal (M'/K) auflösbar ist. Dazu betrachten wir die surjektive Restriktionsabbildung

$$\text{Gal}(M'/K) \to \text{Gal}(L/K)$$

mit Kern $\text{Gal}(M'/L)$. Da $\text{Gal}(L/K)$ auflösbar ist, genügt es nach Satz 10.6 zu zeigen, dass $\text{Gal}(M'/L)$ auflösbar ist. Nun ist M' das Kompositum der $\sigma(M)$. Aus Satz 7.13 folgt, dass

$$\begin{array}{rcl} \text{Gal}(M'/L) & \to & \displaystyle\prod_{\sigma \in \text{Hom}_K(M,\overline{M})} \text{Gal}(\sigma(M)/L) \\ \tau & \mapsto & (\tau|_{\sigma(M)})_\sigma \end{array}$$

injektiv ist. Nach Satz 10.6 müssen wir nur zeigen, dass das Produkt auf der rechten Seite auflösbar ist, d.h., dass $\prod_\sigma \text{Gal}(\sigma(M)/L)$ auflösbar ist. Dies zeigt man mit Induktion über die Anzahl der Faktoren unter Zuhilfenahme von Satz 10.6 (ÜA). Also ist M'/K und somit auch M/K auflösbar.
Es bleibt noch der Fall „durch Radikale auflösbar“ zu betrachten. Ist M/K durch Radikale auflösbar, so gilt dies trivialerweise auch für L/K. Indem man das Kompositum der Körperkette aus Definition 10.7 mit L betrachtet, ist auch M/L durch Radikale auflösbar.
Sind umgekehrt M/L und L/K durch Radikale auflösbar, so sei L'/L eine Erweiterung, für die L'/K durch eine Kette wie in Definition 10.7 ausgeschöpft wird. Es sei $L'M$ das Kompositum in einem algebraischen Abschluss von M. Dann ist $L'M/L'$ nach Lemma 10.11 durch Radikale auflösbar. Somit ist auch $L'M/K$ durch Radikale auflösbar, indem man zwei Körperketten zusammenfügt. Also ist M/K durch Radikale auflösbar. □

Jetzt können wir den folgenden wichtigen Satz zeigen.

Satz 10.13 Eine endliche Körpererweiterung L/K ist genau dann auflösbar, wenn sie durch Radikale auflösbar ist.

Beweis : Angenommen, L/K ist auflösbar. Nach Übergang zu einem Erweiterungskörper können wir annehmen, dass L/K galoissch mit auflösbarer Galoisgruppe ist. Sei m das Produkt aller Primzahlen $p \neq \text{char}(K)$ mit $p \mid [L : K]$. Ferner sei $F = K(\zeta_m)$ für eine primitive m-te Einheitswurzel ζ_m. Dann ist F/K durch Radikale auflösbar. Wir betten F in einen algebraischen Abschluss $\overline{L}$ von L ein und bilden dort das Kompositum FL. Dann ist $K \subset F \subset FL$, und es genügt nach Lemma 10.12 zu

zeigen, dass FL/F durch Radikale auflösbar ist. Nach Lemma 10.11 wissen wir, dass FL/F galoissch mit auflösbarer Galoisgruppe ist. Also gibt es nach Satz 10.5 eine Normalreihe

$$\text{Gal}(FL/F) = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

mit Faktoren G_i/G_{i+1}, die zyklisch von Primzahlordnung sind. Aufgrund des Hauptsatzes der Galoistheorie gehört dazu eine Kette von Zwischenkörpern

$$F = F_0 \subset F_1 \subset \ldots F_n = FL,$$

mit $F_i = (FL)^{G_i}$, so dass F_{i+1}/F_i galoissch mit $\text{Gal}(F_{i+1}/F_i) \simeq G_i/G_{i+1}$ zyklisch von der Ordnung p_i für eine Primzahl p_i ist. Da nach Satz 7.13

$$\text{Gal}(FL/F) \simeq \text{ Gal}(L/F \cap L)$$

gilt, ist $[FL : F]$ ein Teiler von $[L : K]$. Also ist p_i ein Teiler von m, so dass F eine primitive p_i-te Einheitswurzel enthält (nämlich eine geeignete Potenz von ζ_m). Damit enthält auch F_i eine primitive p_i-te Einheitswurzel, und nach Satz 9.9 entsteht F_{i+1} aus F_i durch Adjunktion einer Nullstelle eines Polynoms der Form $X^{p_i} - a \in F_i[X]$. Ist $p_i = \text{ char}(K)$, so folgt aus Satz 9.10, dass F_{i+1} aus F_i durch Adjunktion einer Nullstelle eines Polynoms der Form $X^{p_i} - X - a \in F_i[X]$ entsteht. Daher ist FL/F und somit auch L/K durch Radikale auflösbar.
Sei umgekehrt L/K durch Radikale auflösbar. Dann gibt es einen Erweiterungskörper E von L, so dass E/K durch eine Körperkette wie in Definition 10.7 ausschöpfbar ist. Wir können $E = L$ annehmen. Dann gibt es eine Kette

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L,$$

so dass K_{i+1}/K_i vom Typ i), ii) oder iii) aus Definition 10.7 ist. Um zu zeigen, dass L/K auflösbar ist, genügt es nach Lemma 10.12 zu zeigen, dass alle K_{i+1}/K_i auflösbar sind. Ist K_{i+1}/K_i vom Typ i), so ist K_{i+1}/K_i nach Satz 9.6 galoissch und abelsch. Ist K_{i+1}/K_i vom Typ iii), so ist $\text{Gal}(K_{i+1}/K_i)$ nach Satz 9.10 galoissch und zyklisch. In beiden Fällen ist K_{i+1}/K_i auflösbar.
Ist K_{i+1}/K_i vom Typ ii), also $K_{i+1} = K_i(c)$ für eine Nullstelle c des Polynoms $X^n - a \in K_i[X]$ mit $\text{char}(K) \nmid n$, so sei $F = K_i(\zeta_n)$ mit einer primitiven n-ten Einheitswurzel ζ_n. Wir betten F in einen algebraischen Abschluss von K_{i+1} ein und betrachten

$$K_i \subset F \subset FK_{i+1} = F(c).$$

Dann ist F/K_i nach Satz 9.6 galoissch und abelsch und $F(c)/F$ nach Satz 9.9 galoissch und zyklisch. Beide Erweiterungen sind also auflösbar und nach Lemma 10.12 ist auch $F(c)/K_i$ und somit auch K_{i+1}/K_i auflösbar. Insgesamt folgt also dass L/K auflösbar ist. □

Wir haben jetzt also ein gruppentheoretisches Kriterium dafür, wann eine Erweiterung durch Radikale auflösbar ist. Das wollen wir jetzt anwenden:

Satz 10.14 Die Gleichung $X^5 - 4X + 2 = 0$ ist über $\mathbb{Q}$ nicht durch Radikale auflösbar.

Es gibt also Polynomgleichungen vom Grad 5, für deren Lösung keine „Wurzelformel" existiert.

Beweis : $f = X^5 - 4X + 2$ ist nach Eisenstein irreduzibel über $\mathbb{Q}$. Sei $L/\mathbb{Q}$ ein Zerfällungskörper von f. Die Ableitung $f' = 5X^4 - 4$ hat genau zwei reelle Nullstellen, nach dem Satz von Rolle hat f also höchstens drei reelle Nullstellen. Da $f(-2) < 0, f(0) > 0, f(1) < 0$ und $f(2) > 0$ ist, hat f genau drei reelle Nullstellen $\alpha_3, \alpha_4, \alpha_5$. Mit jedem $z \in \mathbb{C}$ ist auch das komplex konjugierte $\overline{z}$ Nullstelle von f, also muss für die restlichen beiden komplexen Nullstellen α_1, α_2 von f die Gleichung $\overline{\alpha}_1 = \alpha_2$ gelten. Die komplexe Konjugation vermittelt also einen Automorphismus $\tau \in \text{Gal}(L/\mathbb{Q})$ der Ordnung 2.
Da f irreduzibel ist, gilt $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$, also gillt $5 \mid [L : K]$. Sei H eine 5-Sylowgruppe in $G = \text{Gal}(L/K)$. Da $\text{ord}(G)$ ein Teiler von 5! ist (siehe Aufgabe 42), ist $\text{ord}(H) = 5$. G enthält also ein Element der Ordnung 5. Nach Lemma 4.23 vermittelt jedes $\sigma \in G$ eine eindeutig bestimmte Permutation der Nullstellen $\alpha_1, \ldots, \alpha_5$ von f. Wir erhalten somit einen injektiven Gruppenhomomorphismus

$$G \to S_5,$$

vermöge dessen wir G als Untergruppe der S_5 auffassen. Somit ist H eine Untergruppe der S_5 der Ordnung 5. Betrachten wir ihre natürliche Operation auf der Menge $\{1, 2, 3, 4, 5\}$, so ist nach der Bahnengleichung

$$5 = \sum_i \text{ord}(Hx_i) = \sum_i (H : H_{x_i})$$

für ein Vertretersystem (x_i) der Bahnen. Da jedes $(H : H_{x_i})$ ein Teiler von $5 = \text{ord}(H)$ ist, gibt es eine Bahn der Ordnung 5. Ist $H = \langle h \rangle$, so ist also $\{1, 2, 3, 4, 5\} = \{1, h(1), h^2(1), h^3(1), h^4(1)\}$.
Die komplexe Konjugation in G vermittelt ein Element τ der Ordnung 2 in S_5, also eine Transposition. Es ist $\tau = (1\,2)$, da $\tau(\alpha_1) = \alpha_2$ gilt. Man zeigt leicht $h^{-k}\tau h^k = (h^k(1)\, h^k(2)) \in G$ für alle $k \in \mathbb{Z}$. Andererseits ist $2 = h^q(1)$ für ein $0 \leq q \leq 4$, d.h. für alle k ist $(h^k(1)\, h^{k+q}(1)) \in G$. Für jede beliebige Transposition τ' gibt es $m, n \in \{0, \ldots, 4\}$, so dass $\tau' = (h^m(1)\, h^n(1))$. Da q teilerfremd zu 5 ist, gibt es $r, s \in \mathbb{Z}$ mit $n - m = rq + s5$. Falls $q \geq 0$ ist, so ist

$$\tau' = (h^m(1)\, h^{m+q}(1))(h^{m+q}(1)\, h^{m+2q}(1)) \ldots (h^{m+(r-1)q}(1)\, h^n(1)) \in G$$

Für $q < 0$ wenden wir dasselbe Argument auf $m - n = r(-q) - 5s$ an.
Somit enthält G alle Transpositionen. Da jedes Element in S_5 Produkt von Transpositionen ist, folgt $G \simeq S_5$. Also ist G nicht auflösar. Nach Satz 10.13 ist L/K also nicht durch Radikale auflösbar. □

Literatur

[Bo] S. Bosch: Algebra. Springer 1992.