Prof.Dr. C. Bessenrodt
Universität Hannover
Institut für Mathematik

ALGEBRA I

Wintersemester 2003/2004

Inhalt von Prof.Dr. C. Bessenrodt, überarbeitet von Alexander Seifert.
Wenn ihr Fehler im Skript findet, schickt die Seitenzahl und Stelle an alexseifert@gmx.net.

Inhaltsverzeichnis

Kapitel 1

Konstruktion mit Zirkel und Lineal (Teil 1)

In diesem ersten Abschnitt werden einige klassische Konstruktionsprobleme beschrieben. Sie werden uns im Folgenden als Testfälle bei der Entwicklung der Körpertheorie begleiten. Wir werden später sehen, dass einige der Probleme bereits mit relativ elementaren algebraischen Mitteln zu lösen sind, während wir für andere über die Algebra hinausgehen müssen.

1.1 Was bedeutet „Konstruktion mit Zirkel und Lineal“?

Gegeben ist zunächst eine Menge M von mindestens zwei Punkten in der (euklidischen) Ebene. Mit dem ersten Punkt legen wir einen Ursprung fest und mit dem zweiten eine Längeneinheit (hat M nur einen Punkt, so können wir keine weiteren Punkte konstruieren).
Es sei $G(M)$ die Menge aller Geraden in der reellen Ebene $\mathbb{R}^2$, die durch zwei Punkte aus M gehen und $K(M)$ die Menge aller Kreise, deren Mittelpunkte die Punkte von M und deren Radien gleich den Abständen je zweier Punkte aus M sind. Die Geraden betrachten wir als konstruierbar aus M mit Hilfe des Lineals (ohne Verwendung der Markierungen), die Kreise als konstruierbar aus M mit Hilfe des Zirkels. Zu beachten ist, dass wir hier einen **nichtkollabierenden** Zirkel verwenden, mit dem wir den Abstand zweier Punkte aus M abgreifen und an einen dritten Punkt aus M übertragen können. In den ursprünglichen geometrischen Konstruktionsproblemen wurde ein **kollabierender** Zirkel verwendet, mit dem nur unmittelbar ein Kreis um einen Punkt aus M mit einem weiteren Punkt aus M auf dem Umfang gezeichnet werden konnte. Tatsächlich können auch mit einem kollabierenden Zirkel und einem Lineal alle Kreise konstruiert werden, die mit einem nichtkollabierenden Zirkel gezeichnet werden können.
Über die Konstruktion von Geraden und Kreisen können wir nun weitere Punkte konstruieren, die ursprünglich nicht in M lagen, und zwar genauer durch folgende Operationen:

1. Schnitt zweier verschiedener Geraden aus $G(M)$.
2. Schnitt einer Geraden aus $G(M)$ mit einem Kreis aus $K(M)$.
3. Schnitt zweier verschiedener Kreise aus $K(M)$.

Unter der Hinzunahme dieser Schnittpunkte erhalten wir eine neue Menge von Punkten, die wir mit M' bezeichnen.
Setze $M_0 = M$. Ist M_n für $n \geq 0$ schon definiert, so sei

$$M_{n+1} = M_n'$$

die Menge der Punkte, die in M_n liegen oder aus M_n durch die obigen drei Operationen konstruiert werden können.

Definition 1.1

$\widehat{M} = \bigcup_{n=0}^{\infty} M_n$ heißt die Menge der aus M mit Zirkel und Lineal konstruierbaren Punkte.

Offenbar lässt sich jeder Punkt aus $\widehat{M}$ bereits mit endlich vielen Operationen aus M erzeugen. Außerdem werden in einem Konstruktionsschritt nur endlich viele Punkte aus M_n verwendet, also ist auch $(\widehat{M})' = \widehat{M}$.

Beispiel 1.2

Wir setzen stets voraus, dass M die Zahlen 0 und 1 enthält und damit enthält $\widehat{M}$ alle Gitterpunkte in $\mathbb{Z}\times\mathbb{Z}$.

0. **Dreieckskonstruktionen**

   Es wird vorausgesetzt, dass ein Dreieck mit spezifischen Bestimmungsstücken existiert, und es ist das Problem zu behandeln, ob und wie das Dreieck zu konstruieren ist. Dabei sind typischerweise drei Bestimmungsstücke des Dreiecks als Strecken (Kanten, Seitenhalbierende, Winkelhalbierende, Höhen, Mittelsenkrechten, Innenkreisradien, Umkreisradien, ...) und Winkel gegeben. Strecken können auf einer gegebenen Geraden g von einem gegebenen Punkt P aus abgetragen werden, für einen Winkel α muss relativ zu diesen Daten ein weiterer Punkt Q auf dem zweiten Schenkel mit Scheitel in P zu α angegeben werden.

   Die Bestimmungsstücke sind damit also durch eine endliche Punktemenge M gegeben, und es sind drei Punkte in $\widehat{M}$ gesucht, die das (bzw. ein) Dreieck mit diesen Bestimmungsstücken definieren.

   Sind z.B. die drei Kantenlängen des Dreiecks als Strecken PA, PB und PC auf g gegeben, so ist hier $M=\{P,A,B,C\}$. Mit Zirkel und Lineal konstruieren wir das gesuchte Dreieck dann folgendermaßen:

   Wir schlagen um P einen Kreis mit Radius PB und um A einen Kreis mit Radius PC. Da wir voraussetzen, dass ein Dreieck mit den gegebenen Daten existiert, schneiden sich diese beiden Kreise in zwei Punkten (sonst haben wir nur ein entartetes Dreieck), etwa in X und Y. Die beiden Dreiecke PXA und PYA sind dann Lösungen des Konstruktionsproblems.

1. **Das Delische Problem der Würfelverdopplung**

   Gegeben sei ein Würfel. Zu konstruieren ist ein Würfel mit dem doppelten Volumen.

   Ein Würfel ist durch seine Kantenlänge bestimmt, also ist hier $M=\{P,Q\}$, wobei die Strecke PQ die Kantenlänge a bestimmt.

   Ein Würfel mit doppeltem Volumen hat die Kantenlänge $\sqrt[3]{2}a$. Das Problem ist hier also, ob es einen Punkt Q' im Abstand $\sqrt[3]{2}a$ von P in $\widehat{M}$ gibt.

2. **Dreiteilung des Winkels**

   Ein Winkel φ sei wie oben beschrieben durch drei Punkte P,Q_1,Q_2 gegeben, d.h. PQ_1 und PQ_2 beschreiben die Schenkel des Winkels. Zu konstruieren ist der Winkel $\frac{\varphi}{3}$, d.h. wir müssen einen Punkt $X\in\widehat{M}$ finden, so dass der von den Schenkeln PX und PQ_1 eingeschlossene Winkel $\frac{\varphi}{3}$ ist.

   (Demonstration: (angenäherte) Winkeldreiteilung durch Papierfalten)

3. **Quadratur des Kreises**

   Zu einem gegebenen Kreis soll ein Quadrat mit demselben Flächeninhalt konstruiert werden.

   Hier ist also $M=\{P,Q\}$, wobei der Abstand von P zu Q genau der Radius r des Kreises ist. Gesucht ist ein Quadrat mit Flächeninhalt πr^2, d.h. wir müssen eine Strecke der Länge $r\sqrt{\pi}$ konstruieren können, also einen Punkt X mit Abstand $r\sqrt{\pi}$ von P in $\widehat{M}$ finden.

4. **Konstruktion des regulären n-Ecks**

   Gegeben ist wieder ein Kreis durch $M=\{P,Q\}$, wobei P der Mittelpunkt des Kreises sei. Diesem Kreis soll ein reguläres n-Eck einbeschrieben werden, d.h. es ist auf dem Umfang des Kreises ein Punkt $X\in\widehat{M}$ zu suchen, so dass der von PQ und PX eingeschlossene Winkel $\frac{2\pi}{n}$ ist.

   Für $n=3,4,5$ war die Konstruktion bereits den griechischen Mathematikern des Altertums gelungen. Da Winkel leicht halbiert werden können, können also auch alle $2^k\cdot n$-Ecke für $k\in\mathbb{N}$, $n\in\{3,4,5\}$ konstruiert werden. Erst Gauß gelang (etwa 1795) die Konstruktion des regulären 17-Ecks. Außerdem führte er die allgemeine Konstruktionsaufgabe auf ein zahlentheoretisches Problem zurück, das auch bis heute noch nicht vollständig gelöst ist. Insbesondere hat er gezeigt, dass das reguläre 7-Eck **nicht** mit Zirkel und Lineal konstruiert werden kann. Wir kommen später darauf zurück.

Die Konstruktion des einbeschriebenen 3-Ecks sei einer Übung überlassen. Die Konstruktion des regulären einbeschriebenen 5-Ecks hängt eng mit der Konstruktion des Goldenen Schnitts zusammen. Wir wollen dies kurz beschreiben.
Gegeben sei ein Kreis mit Mittelpunkt P und Radius AP. Wir konstruieren zunächst den Goldenen Schnitt des Radius'. Dazu errichten wir in P die Senkrechte auf AP. Es sei R der (ein) Schnittpunkt dieser Senkrechten mit dem Kreis. Ist AB der Durchmesser des Kreises, dann sei Q der Mittelpunkt der Strecke PB. Wir zeichnen nun einen Kreis um Q mit Radius RQ. Der Schnittpunkt dieses Kreises mit der Strecke AP sei T. Dieser Punkt liefert den Goldenen Schnitt von AP.
Wir erhalten nun die Eckpunkte des regulären 5-Ecks, indem wir die Strecke RT als Sehne auf dem Kreis wiederholt abtragen (Beweis: Übung). Das 10-Eck erhalten wir dann durch Abtragen der Strecke PT.

1.2 Algebraische Formalisierung des Konstruktionsproblems

Ist eine Ausgangsmenge M mit mindestens zwei Punkten gegeben, so können wir mit Hilfe von zwei Punkten O, P in der Ebene ein kartesisches Gitter konstruieren: O sei der Ursprung des Gitters und OP definiere die Längeneinheit 1. Damit ist zunächst die Gerade g durch O und P mit ganzzahligen Koordinaten $(n,0)$ versehen. Anschließend konstruieren wir in jedem Punkt $(n,0)$ die Lotgerade zu g: wir bringen die beiden Kreise um $(n-1,0)$ und $(n+1,0)$ vom Radius 2 zum Schnitt, die durch die beiden Punkte definierte Gerade ist die gewünschte Lotgerade. Wir versehen auch alle diese Geraden mit ganzzahligen Koordinaten. Damit stehen uns nun also alle Punkte des kartesischen Gitters zur Verfügung, d.h. $\mathbb{Z}\times\mathbb{Z} \subseteq \widehat{M} \subseteq \mathbb{R}\times\mathbb{R}$.
Es stellt sich als nützlich heraus, den $\mathbb{R}^2$ mit der Gaußschen Zahlenebene zu identifizieren und Punkte $(x,y) \in \mathbb{R}^2$ mit den zugehörigen komplexen Zahlen $x+iy$ zu identifizieren. Wir wollen die mit obigen Operationen konstruierbaren Punkte algebraisch untersuchen. Ziel ist es, im wesentlichen folgendes zu zeigen:
Die aus M mit Zirkel und Lineal konstruierbaren Punkte in $\mathbb{R}^2$ sind genau die Punkte, deren Koordinaten aus den Koordinaten der Punkte von M durch endlich viele Anwendungen der folgenden Operationen konstruiert werden können: Bildung der Summe, der Differenz, des Produkts, des Quotienten und Ziehen der Quadratwurzel.
Die ersten vier Operationen sind genau die Operationen, die wir in beliebigen Körpern (bzw. Schiefkörpern) durchführen können. Körper wurden bereits in der Linearen Algebra definiert. Wir erinnern nur an ...

Beispiel 1.3

(i) Die Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
(ii) Ist p eine Primzahl, dann ist $\mathbb{Z}_p$ ein Körper mit p Elementen (der Restklassenring nach p).

Über die aus M konstruierbaren Zahlen können wir zunächst folgende Aussage machen:

Satz 1.4

Sei M eine Menge der komplexen Zahlen, die 0 und 1 enthält. Dann ist die Menge $\widehat{M}$ der aus M konstruierbaren Zahlen ein Teilkörper von $\mathbb{C}$, d.h. ein in $\mathbb{C}$ enthaltener Körper.

Beweis

Wir müssen zeigen: sind $z_1, z_2 \in M$, so auch die Zahlen z_1+z_2, $-z_2$, $z_1\cdot z_2$ und für $z_2 \neq 0$ auch $\frac{1}{z_2}$.
Die Addition komplexer Zahlen erhält man durch das Parallelogramm der zugehörigen Vektoren. Den Punkt z_1+z_2 findet man als einen Schnittpunkt der beiden Kreise um z_i mit Radius z_j, $i \neq j$. Alternativ überlegt man sich zunächst allgemein, wie man Parallelen zu einer vorgegebenen Geraden in einem vorgegebenen Abstand konstruiert.
Die Konstruktion von $-z_2$ aus z_2 ist klar.

Nun zur Konstruktion des Produkts. Dazu betrachten wir zunächst den Fall: $r_1, r_2 \in \widehat{M} \cap \mathbb{R}^+$.
Wir konstruieren die Lotgeraden g_1 und g_2 zur x-Achse durch die Punkte 1 und r_2. Auf g_1 konstruieren wir im Abstand r_1 von 1 mit dem Zirkel einen weiteren Punkt von $\widehat{M}$. Durch diesen Punkt und 0 legen wir eine Gerade, die g_2 in einem Punkt X schneiden muss. Nach dem Strahlensatz hat dann X den Abstand $r_1 \cdot r_2$ zum Punkt r_2 auf der x-Achse. Die Strecke muss nun noch mit dem Zirkel von 0 aus auf die x-Achse übertragen werden, um $r_1 \cdot r_2 \in \widehat{M}$ zu zeigen.
Im allgemeinen Fall sind $z_1, z_2 \in \widehat{M}$ durch Polarkoordinaten gegeben:

$$z_k = r_k (\cos\varphi_k + i \cdot \sin\varphi_k) = r_k e^{i\varphi_k}.$$

Wobei $r_k = |r_k|$ die Länge des zu z_k gehörigen Vektors und φ_k dessen Winkel zur reellen Achse ist. Es ist dann

$$z_1 z_2 = r_1 r_2 e^{i(\varphi_1+\varphi_2)}.$$

Da mit z_k auch r_k zu $\widehat{M}$ gehört (Abtragen der Länge auf der reellen Achse), können wir nach dem oben Beschriebenen $r_1 r_2$ konstruieren. Außerdem können zwei Winkel leicht mit Zirkel und Lineal addiert werden. Abtragen von $r_1 r_2$ auf dem zu $\varphi_1 + \varphi_2$ gehörenden Strahl liefert dann $z_1 z_2$.
Zuletzt muss noch zu $z_2 \neq 0$ in $\widehat{M}$ $\frac{1}{z_2}$ konstruiert werden. Wir benutzen wieder Polarkoordinaten und erhalten

$$\frac{1}{z_2} = \frac{1}{r_2} e^{-i\varphi_2}.$$

Nun konstruieren wir $-\varphi_2$ durch Spiegelung an der reellen Achse und r_2^{-1} wieder mit dem Strahlensatz.
Damit ist insgesamt $\widehat{M}$ als Teilkörper von $\mathbb{C}$ nachgewiesen. □

Bemerkung 1.5

Jeder Teilkörper K von $\mathbb{C}$ enthält den Körper $\mathbb{Q}$ der rationalen Zahlen. Tatsächlich haben wir im obigen Beweis auch explizit gezeigt, wie die rationalen Zahlen mit Zirkel und Lineal aus der Menge $\{0,1\}$ konstruiert werden.

Als nächstes wollen wir zeigen, dass mit jeder komplexen Zahl in M auch ihre Wurzel konstruierbar ist.

Satz 1.6

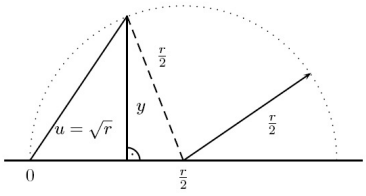
Für $z \in \widehat{M}$ ist auch $\sqrt{z} \in \widehat{M}$.

Beweis

Für $z = re^{i\varphi}$, $r \in \mathbb{R}^+$, $-\pi < \varphi \leq \pi$ gilt

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

Da wir Winkel halbieren können, müssen wir nur zeigen: $\sqrt{r} \in \widehat{M}$ für $r \in \widehat{M} \cap \mathbb{R}^+$.
Dies erreichen wir durch folgende Konstruktion. Wir können annehmen, dass $r \neq 0$ und dann sogar $\frac{r}{2} > 1$ gilt, sonst konstruieren wir zunächst $\frac{1}{r}$. Mit dem Zirkel konstruieren wir den Halbkreis über der Strecke von 0 nach r mit dem Radius $\frac{r}{2}$. Auf dieser Strecke im Punkt 1 errichten wir die Lotgerade. Diese schneidet den Kreis im Abstand y von der reellen Achse. Die Strecke von 0 zu diesem Schnittpunkt hat nach Pythagoras die Länge $u = \sqrt{1+y^2}$. Da der Punkt $(1, y)$ auf dem Kreis mit der Gleichung $(X - \frac{r}{2})^2 + Y^2 = (\frac{r}{2})^2$ liegt, gilt



$$1 - r + (\tfrac{r}{2})^2 + y^2 = (\tfrac{r}{2})^2,$$

also $r = 1 + y^2$ und damit $u = \sqrt{r}$. □

Definition 1.7

Ein Teilkörper K von $\mathbb{C}$ heißt **quadratisch abgeschlossen**, falls $\sqrt{z} \in K$ für alle $z \in K$ gilt.

Nach dem bisher Gezeigten ist also $\widehat{M}$ ein quadratisch abgeschlossener Teilkörper von $\mathbb{C}$.
Bevor wir weitere Eigenschaften von $\widehat{M}$ nachweisen, müssen wir noch einige Begriffe aus der Körpertheorie einführen.

Lemma 1.8

Sei $\{K_\lambda\}_{\lambda\in\Lambda}$ eine Familie von Teilkörpern von K. Dann ist auch $\bigcap_{\lambda\in\Lambda} K_\lambda$ ein Teilkörper von K.

Beweis

Liegen x,y in allen K_λ, so offenbar auch $x+y$, $x-y$, $x\cdot y$ und für $y\neq 0$ auch $\frac{x}{y}$.

Definition 1.9

Sei K ein Körper und $M\subseteq K$. Dann heißt der Durchschnitt aller M enthaltenen Teilkörper von K der **von M erzeugte Teilkörper** von K, und wir bezeichnen ihn kurz (M).
Ist K_0 ein Teilkörper von K, dann bezeichnen wir mit $K_0(M)$ den Teilkörper $(K_0\cup M)$ von K und sagen: $K_0(M)$ entsteht aus K_0 **durch Adjunktion von** M. Für $M=\{x_1,\dots,x_n\}$ schreiben wir $K_0(x_1,\dots,x_n)$ statt $K_0(\{x_1,\dots,x_n\})$.
Der von $M=\{0,1\}$ (oder auch von $M=\emptyset$!) erzeugte Teilkörper P von K heißt der **Primkörper** von K.

Bemerkung 1.10

(i) Der Primkörper P ist nach Definition in jedem Teilkörper von K enthalten, und für jedes $M\subseteq K$ ist $P(M)=(M)$.

(ii) Der Primkörper von $\mathbb{R}$ und $\mathbb{C}$ ist $\mathbb{Q}$.

(iii) In einem Körper von Charakteristik 2, d.h. in einem Körper mit $1+1=0$ ist bereits $P=\{0,1\}$ selbst ein Teilkörper. Für jede Primzahl p ist $\mathbb{Z}_p$ ein Primkörper. Allgemein gilt: Ein Körper hat genau dann die Charakteristik $p>0$, wenn sein Primkörper $\mathbb{Z}_p$ ist. Er hat die Charakteristik 0 genau dann, wenn sein Primkörper $\mathbb{Q}$ ist.

(iv) Der Körper $K_0(M)$ ist offenbar der kleinste Teilkörper von K, der K_0 und M enthält. Wir werden ihn etwas später auch explizit beschreiben.

(v) Sei $d\in\mathbb{Q}$ mit $\sqrt{d}\notin\mathbb{Q}$. Dann ist
$$\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\},$$
denn die Zahlen der Form $a+b\sqrt{d}$ bilden einen Körper:
$$\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-b^2d}.$$

Ist eine Teilmenge M von $\mathbb{C}$ gegeben, die 0 und 1 enthält, so sind durch Spiegelung an der reellen Achse auch alle konjugiert komplexen Elemente der Zahlen aus M konstruierbar. Wir bezeichnen diese Menge mit $\overline{M}$. Also gilt: $\mathbb{Q}(M\cup\overline{M})\subseteq\widehat{M}$. Tatsächlich bleibt dieser Körper fest unter komplexer Konjugation:

Lemma 1.11

Sei $M\subseteq\mathbb{C}$ mit 0 und 1 in M und sei $K_0=\mathbb{Q}(M\cup\overline{M})$. Dann ist $K_0=\overline{K_0}$.

Beweis

Die komplexe Konjugation bildet Teilkörper von $\mathbb{C}$ auf Teilkörper von $\mathbb{C}$ ab. Also ist auch $\overline{K_0}$ ein Teilkörper von $\mathbb{C}$. Da außerdem $\overline{\overline{z}}=z$ für alle $z\in\mathbb{C}$ gilt, ist $\overline{K_0}$ auch der kleinste Teilkörper, der $\overline{M}$ und M umfasst, also ist $\overline{K_0}=K_0$. □

Wir halten für das Folgende einen solchen Teilkörper L von $\mathbb{C}$ mit $\overline{L}=L$ fest.

Die Geraden durch Punkte von L seien mit $G(L)$, die Kreise mit Mittelpunkt in L und Radius in L seien mit $K(L)$ bezeichnet. Da $\overline{L} = L$, gehören insbesondere mit jedem $z = x + iy \in L$ auch x und iy zu L. Zunächst zeigen wir, dass Geradenschnitte nicht aus L hinausführen.

Lemma 1.12

Ist z Schnittpunkt zweier Geraden aus $G(L)$, so gilt $z \in L$.

Beweis

Die beiden Geraden seien gegeben in der Form

$$z_0 + \lambda z_1 \ \ (z_0, z_1 \in L),$$

$$z_0' + \mu z_1' \ \ (z_0', z_1' \in L),$$

wobei $\lambda, \mu \in \mathbb{R}$. Wir spalten die Gleichung $z_0 + \lambda z_1 = z_0' + \mu z_1'$ für den Schnittpunkt in die beiden Gleichungen für den Real- und Imaginärteil auf, wobei $z_k = x_k + iy_k$ und entsprechend für z_k':

$$x_0 + \lambda x_1 = x_0' + \mu x_1',$$

$$iy_0 + \lambda iy_1 = iy_0' + \mu iy_1'.$$

Mit z_k gehören natürlich auch x_k und iy_k zu L, da $\overline{L} = L$. Durch Auflösen des Gleichungssystems folgt dann auch: $\lambda, \mu \in L$ und damit ist der Schnittpunkt $z_0 + \lambda z_1 \in L$. □

Für die Schnittpunkte von Geraden und Kreisen über L ist unter Umständen die Adjunktion von Wurzeln notwendig:

Lemma 1.13

Ist z Schnittpunkt einer Geraden aus $G(L)$ mit einem Kreis aus $K(L)$ oder ein Schnittpunkt zweier Kreise aus $K(L)$, dann ist $z \in L(\sqrt{w})$ für ein geeignetes $w \in L$.

Beweis

Es sei z zunächst Schnittpunkt einer Geraden aus $G(L)$ mit einem Kreis aus $K(L)$. Die Gerade sei wieder durch $z_0 + \lambda z_1$ gegeben mit $z_0, z_1 \in L$. Der Kreis habe den Mittelpunkt z_2 und Radius r. Real- und Imaginärteile von z_0, z_1, z_2 seien wie vorher. Die Punkte $x + iy$ des Kreises erfüllen die Gleichung

$$(x - x_2)^2 - (iy - iy_2)^2 = r^2.$$

Insbesondere gilt für den Schnittpunkt $z = z_0 + \lambda z_1$:

$$(x - \lambda x_1 - x_2)^2 - (iy - \lambda iy_1 - iy_2)^2 = r^2.$$

Ist diese Gleichung linear in λ, so ist λ und damit auch z in L. Ist die Gleichung quadratisch in λ, etwa

$$\lambda^2 + p\lambda + q = 0, \ \ p, q \in L,$$

so gilt

$$\lambda = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q},$$

also ist $\lambda \in L(\sqrt{w})$ für $w = \frac{p^2}{4} - q \in L$ und damit auch $z \in L(\sqrt{w})$.

Sei nun z Schnittpunkt zweier Kreise aus $K(L)$, die durch die folgenden Gleichungen gegeben sind:

$$(x - x_0)^2 - (iy - iy_0)^2 = r_0^2,$$

$$(x - x_1)^2 - (iy - iy_1)^2 = r_1^2.$$

Durch Subtraktion erhalten wir eine in x und y lineare Gleichung der Form

$$ax + biy = c,$$

wobei $a, b, c \in L$ und a, b nicht beide Null, da wir von zwei sich schneidenden Kreisen ausgegangen sind. Diese Gleichung liefert eine Gerade in $G(L)$, und z ist Schnittpunkt dieser Geraden aus $G(L)$ mit einem Kreis aus $K(L)$, also nach den vorherigen Überlegungen ist $z \in L(\sqrt{w})$ für ein geeignetes $w \in L$. □

Um unseren Satz über die algebraische Charakterisierung von aus einer Menge M konstruierbaren Zahlen formulieren zu können, brauchen wir noch eine Definition:

Definition 1.14

Wir sagen, dass ein Körper L aus einem Teilkörper K durch **sukzessive Adjunktion von Quadratwurzeln** entsteht, wenn es Elemente $x_1,...,x_n \in L$ gibt, so dass gilt: $L = K(\{x_1,...,x_n\}) = K(x_1,...,x_n)$ und $x_1^2 \in K$, $x_{i+1}^2 \in K(x_1,...,x_i)$ für $i = 1,...,n-1$.

Satz 1.15

Eine Zahl $z \in \mathbb{C}$ ist genau dann aus einer vorgegebenen Menge M mit Zirkel und Lineal konstruierbar, wenn gilt: $z \in L$ für einen Teilkörper L von $\mathbb{C}$, der aus $K_0 = \mathbb{Q}(M \cup \overline{M})$ durch sukzessive Adjunktion von Quadratwurzeln entsteht.

Beweis

Da wir uns bereits überlegt haben, dass der Körper der aus M konstruierbaren Zahlen $\widehat{M}$ quadratisch abgeschlossen ist, enthält $\widehat{M}$ jeden Körper L, der aus K_0 durch sukzessive Adjunktion von Quadratwurzeln entsteht.

Wird umgekehrt eine Zahl z durch eine der erlaubten Konstruktionsmethoden erzeugt (Geradenschnitt, Kreis mit Gerade, Kreisschnitt), so existiert nach den obigen Lemmata $w \in K_0$ mit $z \in K_0(\sqrt{w})$.

Um die Lemmata im nächsten Schritt wieder anwenden zu können, muss der zugrunde liegende Körper invariant unter komplexer Konjugation sein. Da auch $\overline{w} \in K_0$, entsteht $K_1 = K_0(\sqrt{w}, \sqrt{\overline{w}})$ aus K_0 durch sukzessive Adjunktion von Quadratwurzeln, und $K_1 = \overline{K_1}$.

Jeder konstruierbare Punkt $z \in \widehat{M}$ entsteht durch endlich viele Anwendungen der Operationen aus M, also folgt die Behauptung mit Induktion.

Jedes Element aus $\widehat{M}$ kann demnach als rationale Funktion (über $\mathbb{Q}$) in den Elementen von $M \cup \overline{M}$ und geeigneten Quadratwurzeln (aus dem Körper des jeweiligen Konstruktionsschritts) dargestellt werden, und somit nach den vorher beschriebenen Methoden mit Zirkel und Lineal konstruiert werden.

Bezeichnen wir mit $\sqrt{K}$ die Menge aller Quadratwurzeln eines Körpers $K \subset \mathbb{C}$, so erhalten wir auch folgende Beschreibung von $\widehat{M}$:

Lemma 1.16

(i) Wir definieren induktiv einen Körperturm durch

$$K_0 = \mathbb{Q}(M \cup \overline{M}),\ K_{n+1} = K_n(\sqrt{K_n}).$$

Dann ist

$$\widehat{M} = \bigcup_{n=0}^{\infty} K_n .$$

(ii) Es ist $\widehat{M}$ der Durchschnitt aller quadratisch abgeschlossenen Teilkörper von $\mathbb{C}$, die K_0 enthalten, d.h. $\widehat{M}$ ist der kleinste quadratisch abgeschlossene Teilkörper von $\mathbb{C}$, der K_0 enthält.

Beweis

(i) Da $\widehat{M}$ quadratisch abgeschlossen ist, gilt $\widehat{M} \supseteq \bigcup_{n=0}^{\infty} K_n$. Die umgekehrte Inklusion folgt aus Satz 1.15.

(ii) Die Aussage (ii) folgt unmittelbar aus (i), da jeder quadratisch abgeschlossene Körper mit K_0 auch alle K_n enthält. □

Damit haben wir nun genau die Beschreibung der konstruierbaren Punkte bewiesen, die wir zu Beginn des Abschnitts als Ziel formuliert hatten.

Beispiel 1.17

1. **Würfelverdopplung**
   Wir können ohne Einschränkung $M = \{0,1\}$ annehmen und müssen also $\sqrt[3]{2}$ konstruieren. Die Frage ist also, ob $\sqrt[3]{2}$ in einem Teilkörper von $\mathbb{C}$ liegt, der aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln hervorgeht.
2. **Winkeldreiteilung**
   Gegeben ist ein Winkel φ, also eine Menge M mit drei Punkten, etwa $\{0,1,e^{i\varphi}\}$. Hier ist $K_0 = \mathbb{Q}(e^{i\varphi}, e^{-i\varphi}) = \mathbb{Q}(e^{i\varphi})$, und es ist zu klären, ob $e^{i\varphi/3}$ in einem Teilkörper von $\mathbb{C}$ liegt, der aus K_0 durch sukzessive Adjunktion von Quadratwurzeln hervorgeht.
   Einige Winkel lassen sich offensichtlich dritteln, z.B. $\varphi = \frac{\pi}{2}$. Dies folgt auch aus einer leichten algebraischen Betrachtung: $z = e^{i\pi/6}$ erfüllt die Gleichung
   $$X^2 - iX - 1 = 0\,,$$
   es ist also $z = \frac{1}{2}(i + \sqrt{3}) \in \mathbb{Q}(i, \sqrt{3})$ konstruierbar.
3. **Quadratur des Kreises**
   Aus $M = \{0,1\}$ ist $\sqrt{\pi}$ zu konstruieren. Dazu müsste es einen Teilkörper von $\mathbb{C}$ geben, der π enthält und aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln entsteht.
4. **Konstruktion regulärer n-Ecke**
   Aus $M = \{0,1\}$ ist $z_n = e^{2\pi i/n}$ zu konstruieren. Wir zeigen hier noch einmal algebraisch, dass reguläre Fünfecke mit Zirkel und Lineal konstruiert werden können.
   Setze $\xi = z_5$. Dann gilt
   $$0 = \xi^5 - 1 = (\xi - 1)(\xi^4 + \xi^3 + \xi^2 + \xi + 1),$$
   also
   $$0 = \xi^4 + \xi^3 + \xi^2 + \xi + 1 = \xi^2 + \xi(\xi^3 + \xi^2 + 1) + 1\,. \qquad \circledast$$
   Andererseits gilt
   $$(\xi + \xi^{-1})^2 = \xi^2 + \xi^{-2} + 2 = \xi^2 + \xi^3 + 2 = -(\xi + \xi^{-1}) + 1\,,$$
   also
   $$(\xi + \xi^{-1})^2 + (\xi + \xi^{-1}) - 1 = 0\,.$$
   Auflösen dieser quadratischen Gleichung für $\xi + \xi^{-1}$ ergibt
   $$\xi + \xi^{-1} = -\frac{1}{2}(1 - \sqrt{5})\,,\ \xi^2 + \xi^3 + 1 = \frac{1}{2}(1 - \sqrt{5})\,.$$
   Setzen wir dies in $\circledast$ ein, so erhalten wir
   $$\xi^2 + \frac{1}{2}(1 - \sqrt{5})\xi + 1 = 0\,.$$
   Nach ξ auflösen liefert die gesuchte Darstellung von ξ, die die Konstruierbarkeit beweist:
   $$\xi = \frac{1}{4}(\sqrt{5} - 1 + \sqrt{-10 - 2\sqrt{5}}) \in \mathbb{Q}(\sqrt{5}, \sqrt{-10 - 2\sqrt{5}})\,.$$

Kapitel 2

Polynomringe

Grundlagen der Ringtheorie wurden bereits in der Linearen Algebra behandelt. Insbesondere haben wir uns in der LA II bereits intensiv mit Polynomen befasst. Es sei hier an einige wichtige Begriffe und Ergebnisse erinnert: wir werden dabei auch bereits einige Ergänzungen hinzufügen, die im Weiteren benötigt werden.

Definition 2.1

Sei R eine nichtleere Menge mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt:

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

(ii) $(R,\cdot)$ ist eine Halbgruppe.

(iii) Für alle $a,b,c \in R$ gilt:

$$a(b+c) = ab + ac\,,\ (b+c)a = ba + ca\,. \quad \text{(Distributivgesetze)}$$

Dann heißt R (bzw. genauer: das Tripel $(R,+,\cdot)$) ein **Ring**. Der Ring R heißt **kommutativ**, wenn $(R,\cdot)$ kommutativ ist. Hat $(R,\cdot)$ ein neutrales Element, so wird es als 1 bezeichnet und heißt **Einselement** von R. Im Fall, dass R ein kommutativer Ring mit 1 ist, setzen wir

$$R^* := \{a \in R \mid \exists b \in R : ab = 1\}\,.$$

R^* ist eine multiplikative Gruppe, die **Einheitengruppe** von R. (Ist $R^* = R \setminus \{0\}$, so ist R ein Körper.)

Ist für alle $a,b \in R \setminus \{0\}$ auch das Produkt $ab \neq 0$, so heißt R **nullteilerfrei**. Ein kommutativer nullteilerfreier Ring mit 1 heißt **Integritätsring**.

Beispiel 2.2

(i) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer, nullteilerfreier Ring mit 1, also ein Integritätsring. Die Einheitengruppe ist $\mathbb{Z}^* = \{1,-1\}$.

(ii) Die Menge $M_n(R)$ der $n \times n$-Matrizen über einem Ring R bildet mit der gewöhnlichen Matrizenaddition und -multiplikation einen Ring, der für $n > 1$ nicht kommutativ ist. Hat R eine 1, so hat auch $M_n(R)$ ein Einselement, nämlich die Einheitsmatrix.

Ist K ein Körper, so ist die Einheitengruppe die allgemeine lineare Gruppe: $M_n(K)^* = \mathrm{GL}_n(K)$.

(iii) Jeder Körper ist ein kommutativer nullteilerfreier Ring mit 1.

Definition 2.3

Eine Abbildung $\varphi : R \to \widetilde{R}$ zwischen zwei Ringen R und $\widetilde{R}$ heißt **Ringhomomorphismus**, wenn für alle $a,b \in R$ gilt:

$$\varphi(a+b) = \varphi(a) + \varphi(b)\,,\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)\,,$$

d.h. φ ist ein (Gruppen-)Homomorphismus zwischen den additiven Gruppen $(R,+)$ und $(\widetilde{R},+)$ bzw. ein (Halbgruppen-)Homomorphismus zwischen den multiplikativen Halbgruppen $(R,\cdot)$ und $(\widetilde{R},\cdot)$.

Haben die Ringe jeweils ein Einselement, so verlangen wir auch $\varphi(1_R) = 1_{\widetilde{R}}$.

Ist φ injektiv (bzw. surjektiv oder bijektiv), so heißt φ ein **Monomorphismus** (bzw. **Epimorphismus** oder **Isomorphismus**). Zwei Ringe heißen **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

Polynome sind „formale Ausdrücke“ der Form

$$f = a_0 + a_1X + a_2X^2 + ... + a_nX^n\,,\ a_0,a_1,...,a_n \in R\,,$$

wobei R ein kommutativer Ring mit 1 ist, die a_i sind die Koeffizienten von f und X ist eine „Unbestimmte“ über R.
Wir haben bereits in der Linearen Algebra gesehen, wie sich diese vage Beschreibung präzise fassen lässt und erinnern kurz daran.
Sei

$$R[X] \coloneqq \left\{ (a_i)_{i\in\mathbb{N}_0} \mid a_i \in R,\, a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0 \right\}$$

die Menge der abbrechenden Folgen über R.
Definiere auf $R[X]$ eine Addition und eine Multiplikation durch:

$$(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_0}$$

$$(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} = (c_i)_{i\in\mathbb{N}_0} \text{ mit } c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Damit ist $(R[X],+,\cdot)$ ein kommutativer Ring mit $1 = (1,0,0,...)$.
Wir betten R nach $R[X]$ ein durch

$$\iota : R \to R[X],\ a \mapsto (a,0,0,...)$$

(dies ist ein injektiver Ringhomomorphismus!) und identifizieren die Elemente aus R mit den entsprechenden Elementen in $R[X]$.
Sei e_k die Folge mit genau einer 1 an der Position $k \in \mathbb{N}_0$ und Nullen überall sonst. Setze $X \coloneqq (0,1,0,0,...) = e_1$. Dann ist $X^k = e_k$. Jedes $f \in R[X]$ lässt sich dann schreiben in der Form

$$f = \sum_{k=0}^{n} a_k X^k\,,\ a_0,...,a_n \in R\,.$$

Hier sind die Koeffizienten $a_i \in R$ eindeutig bestimmt. Es sind gerade die ersten $n+1$ Komponenten der Folge f, die danach nur noch Nullen hat.

Der Ring $R[X]$ erfüllt die folgende Definition für Polynomringe, die die Substitutionseigenschaft zur Charakterisierung heranzieht:

Definition 2.4

Sei R ein kommutativer Ring mit 1. Ein Tripel $(R[X],X,\iota)$, wobei $R[X]$ ein Ring ist, $X \in R[X]$ ein ausgezeichnetes Element und $\iota : R \to R[X]$ ein Homomorphismus, heißt **Polynomring über R in der Unbestimmten X**, wenn folgende **universelle Eigenschaft** erfüllt ist:
Zu jedem Ring S, $s \in S$ und Homomorphismus $\varphi : R \to S$ gibt es genau einen Homomorphismus $\Phi : R[X] \to S$ mit $\Phi(X) = s$ (**Substitution** von X) und $\Phi \circ \iota = \varphi$. Die Elemente in $R[X]$ heißen **Polynome** mit Koeffizienten in R in der Unbestimmten X.

Satz 2.5

$(R[X],X,\iota)$ wie oben ist ein Polynomring über R in der Unbestimmten X.

Beweis

Sei $\varphi : R \to S$ ein Ringhomomorphismus, $s \in S$, $f = \sum_{k=0}^{n} a_k X^k$.
Ist $\Phi : R[X] \to S$ ein Ringhomomorphismus mit $\Phi(X) = s$ und $\Phi \circ \iota = \varphi$, dann folgt

$$\Phi(f) = \Phi\Big(\sum_{k=0}^{n} a_k X^k\Big) = \sum_{k=0}^{n} \Phi(a_k)\Phi(X)^k = \sum_{k=0}^{n} \varphi(a_k)\, s^k\,. \qquad \circledast$$

Der Homomorphismus Φ ist also durch die geforderten Bedingungen bereits eindeutig festgelegt! Wird Φ durch $\circledast$ definiert, so ist leicht nachzurechnen, dass Φ tatsächlich ein Ringhomomorphismus mit den gewünschten Eigenschaften ist. □

Satz 2.6

(i) Je zwei Polynomringe über R in einer Unbestimmten sind isomorph.

(ii) Ist $(R[Y],Y,\varepsilon)$ ein Polynomring über R, dann ist ε injektiv und zu jedem $g \in R[Y] \setminus \{0\}$ gibt es eindeutig bestimmte Elemente $n \in \mathbb{N}$, $a_0,...,a_n \in R$ mit $a_n \neq 0$ und $g = \sum_{i=0}^{n} \varepsilon(a_i) Y^i$.

Beweis

Übung. □

Ein wichtiger Parameter von Polynomen ist ihr Grad:

Definition 2.7

Ist $f = \sum_{i \in \mathbb{N}_0} a_i X^i \in R[X]$, dann heißt

$$\deg f := \begin{cases} \max\{ i \in \mathbb{N}_0 \mid a_i \neq 0 \} & \text{falls } f \neq 0 \\ -\infty & \text{falls } f = 0 \end{cases}$$

der **Grad** von f. Gilt $\deg f = n \in \mathbb{N}_0$, dann heißt a_n der **Leitkoeffizient** von f. Ist $a_n = 1$, so heißt f **normiert**.

Definition 2.8

Durch Iteration konstruieren wir den Polynomring $R[X_1,...,X_n]$ in den Unbestimmten $X_1,...,X_n$:

$$R \subset R[X_1] \subset R[X_1,X_2] \subset ... \subset R[X_1,...,X_n].$$

Jedes $f \in R[X_1,...,X_n]$, $f \neq 0$ lässt sich dann eindeutig schreiben als

$$f = \sum_{(i_1,...,i_n) \in I} a_{i_1,...,i_n} X_1^{i_1} \cdot ... \cdot X_n^{i_n}$$

mit $a_{i_1,...,i_n} \in R \setminus \{0\}$, $I \subset \mathbb{N}_0^n$ endlich.

Wir können diese Polynomringe benutzen, um die versprochene explizite Beschreibung von Körpern der Form $K(M)$ zu geben, die aus einem Grundkörper K durch Adjunktion der Menge M entstehen:

Lemma 2.9

Seien $K \subseteq L$ Körper und $M \subseteq L$. Dann gilt

$$K(M) = \left\{ \frac{f(x_1,...,x_n)}{g(y_1,...,y_m)} \mid n,m \in \mathbb{N},\ f \in K[X_1,...,X_n],\ g \in K[X_1,...,X_m],\ x_1,...,y_m \in M,\ g(y_1,...,y_m) \neq 0 \right\}.$$

Beweis

Setze

$$Q = \left\{ \frac{f(x_1,...,x_n)}{g(y_1,...,y_m)} \mid n,m \in \mathbb{N},\ f \in K[X_1,...,X_n],\ g \in K[X_1,...,X_m],\ x_1,...,y_m \in M,\ g(y_1,...,y_m) \neq 0 \right\}.$$

Dann ist offenbar Q ein Teilkörper von L, der in $K(M)$ enthalten ist. Wegen $K \cup M \subseteq Q$ ist aber auch $K(M) \subseteq Q$. Also folgt $Q = K(M)$. □

Definition 2.10

Seien R,S kommutative Ringe mit 1, $R \subseteq S$ und $f = \sum_{i\in\mathbb{N}_0} a_i X^i \in R[X]$ ein Polynom. Die Abbildung $S \to S,\ t \mapsto f(t) = \sum_i a_i t^i$ heißt **Polynomfunktion** zum Polynom f. Ein Element $s \in S$ heißt **Nullstelle** von f, wenn

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

gilt.

Satz 2.11

Sei R ein kommutativer Ring mit 1, $f,g \in R[X]$. Dann gilt:

(i) $\deg(fg) \le \deg(f) + \deg(g)$.

(ii) Sind $f,g \neq 0$ mit Leitkoeffizienten a,b, so dass $ab \neq 0$ gilt, dann gilt

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

Beweis

Für $f = 0$ oder $g = 0$ ist (i) klar. Sei also $f \neq 0 \neq g$, $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$, $a_m =: a \neq 0$, $b_n =: b \neq 0$. Dann gilt

$$fg = \sum_{i=0}^{m+n} c_i X^i,\ c_i = \sum_{j+k=i} a_j b_k,$$

also $\deg(fg) \le m+n$. Da $c_{m+n} = a_m b_n = ab$, folgt auch (ii). □

In der Linearen Algebra haben wir uns vor allem mit den Polynomringen $K[X]$, K Körper, beschäftigt. In der Algebra werden wir uns mit allgemeineren Polynomringen befassen. Während in $K[X]$ Division mit Rest stets möglich ist, müssen wir bei allgemeineren Ringen R vorsichtiger sein:

Satz 2.12 (Division mit Rest)

Sei R ein kommutativer Ring mit 1, und seien $f,g \in R[X]\setminus\{0\}$, $m = \deg f$, $n = \deg g$, $k := \max\{0, m-n+1\}$, b der Leitkoeffizient von g. Dann gibt es $q,r \in R[X]$ mit $b^k \cdot f = qg + r$, $\deg r < \deg g$.

Ist $b \in R^*$, so gibt es genau ein $q \in R[X]$ und genau ein $r \in R[X]$ mit $f = qg + r$, $\deg r < \deg g$.

Beweis

Vollständige Induktion nach m. Für $m < n$ ist $k = 0$, $f = 0 \cdot g + f$ eine Zerlegung wie gewünscht.

Wir können also jetzt $m \ge n$ annehmen. Für $m = 0$ ist die Aussage offenbar richtig. Nach Induktionsvoraussetzung sei die Behauptung für alle Polynome vom Grad $< m$ richtig.

Sei a der Leitkoeffizient von f.

Dann ist

$$m' := \deg(bf - aX^{m-n}g) \le m-1,$$

also gibt es nach Induktion $q', r \in R[X]$, $\deg r < \deg g$ mit

$$b^{(m-1)-n+1}(bf - aX^{m-n}g) = q'g + r$$

(beachte, dass $\max\{0, m'-n+1\} \le \max\{0,(m-1)-n+1\}$). Daher gilt

$$b^{m-n+1} f = (\underbrace{ab^{m-n}X^{m-n} + q'}_{=:q})g + r.$$

Ist $b \in R^*$, so ist $f = (\underbrace{b^{-k}q}_{\hat{q}})g + \underbrace{b^{-k}r}_{\hat{r}}$. Ist auch $f = \tilde{q}g + \tilde{r}$, $\deg\tilde{r} < \deg g$, so ist $(\tilde{q} - \hat{q})g = \hat{r} - \tilde{r}$. Da $b \in R^*$, gilt

$$\deg(\tilde{q} - \hat{q}) + \deg g = \deg(\hat{r} - \tilde{r}) < \deg g,$$

also ist $\tilde{q} = \hat{q}$ und dann auch $\tilde{r} = \hat{r}$. □

Satz 2.13

Sei R ein kommutativer Ring mit 1.

(i) Ist $f \in R[X]$, $a \in R$ eine Nullstelle von f, dann gilt $f = (X-a)\tilde{f}$ für ein $\tilde{f} \in R[X]$.

(ii) Sei R ein Integritätsring. Ist $f \in R[X] \setminus \{0\}$, dann hat f höchstens $\deg f$ Nullstellen in R.

Beweis

(i) Nach Satz 2.12 gibt es $q,r \in R[X]$, $\deg r \leq 0$ mit $f = q(X-a) + r$. Dann gilt

$$0 = f(a) = q(a) \cdot 0 + r(a),$$

also ist $r = 0$.

(ii) Seien $a_1,\ldots,a_k$ verschiedene Nullstellen von f. Da R ein Integritätsring ist, folgt dann nach (i):

$$f = \prod_{i=1}^{k} (X - a_i) \cdot \hat{f}$$

für ein geeignetes $\hat{f} \in R[X]$. Also ist $\deg f = k + \deg \hat{f} \geq k$. □

Warum geht (ii) oben schief, wenn der Ring kein Integritätsring ist? Dazu betrachten wir folgendes ...

Beispiel 2.14

Sei $R = \mathbb{Z}_6$ und $f = (X-2)(X-3) = X^2 + X = X(X+1) \in R[X]$. Dann hat f die vier Nullstellen $2,3,0,5$, aber $\deg f = 2$.

Kapitel 3

Algebraische Gleichungen

Im Rahmen der Linearen Algebra sind bereits ausführlich lineare Gleichungssysteme behandelt worden. Die Probleme, die dabei gelöst wurden, waren z.B. die Frage nach der Lösbarkeit eines solchen Gleichungssystems, die Struktur der Lösungsmenge und das Auffinden der Lösungsgesamtheit.
In der Linearen Algebra werden ähnliche Fragestellungen für den allgemeineren Fall eines algebraischen Gleichungssystems behandelt, d.h. eines Gleichungssystems der Form

$$f_i(X_1,...,X_n) = 0 \text{ für } i = 1,...,m\,,$$

wobei die f_i Polynome sind.
Wir werden im Rahmen dieser Vorlesung nur die Anfänge dieser Theorie behandeln können, die im Rahmen der algebraischen Geometrie in diesem Jahrhundert eine außerordentliche Entwicklung genommen hat und ein sehr aktives Gebiet der heutigen Mathematik ist.
Selbst in einfachsten Beispielen hat die Lösungsmenge – im Gegensatz zu den Lösungsgesamtheiten linearer Systeme – oft eine hochgradig komplexe Struktur.

Beispiel 3.1

1. Sei $f(X,Y) = (X^2+Y^2)^5 - 16X^2Y^2(X^2-Y^2)^2$, dann ist die Nullstellenmenge von f in $\mathbb{R}^2$ eine Rosettenkurve.
2. Nullstellenmengen von Gleichungen vom Grad 2 sind gerade die Kegelschnitte.
3. Für ein System von zwei Gleichungen
$$f(X,Y) = 0\,,\ g(X,Y) = 0$$
ist die Lösungsmenge die Schnittpunktmenge der zu f und g gehörenden Kurven. Im vorhergehenden Abschnitt haben wir z.B. für Geraden und Kreise die Schnittpunktmengen bestimmt. Im allgemeinen Fall sind solche Kurvenschnitte natürlich wesentlich komplizierter zu beschreiben oder gar zu berechnen.

Bisher haben wir die Koeffizienten der Polynome bzw. den Zahlenbereich, in dem die Lösungen zu suchen sind, weitgehend außer acht gelassen. Es ist ein Thema der Zahlentheorie, genauer der arithmetischen oder diophantischen Geometrie, insbesondere für Polynome $f_i \in \mathbb{Z}[X_1,...,X_n]$ bzw. $f_i \in \mathbb{Q}[X_1,...,X_n]$ nach Lösungen in $\mathbb{Z}^n$ bzw. $\mathbb{Q}^n$ zu fragen.
Ein bekanntes Beispiel ist das Fermatproblem (1637), das besagt, dass die Gleichung

$$X^n + Y^n = Z^n$$

für $n \geq 3$ keine nichttrivialen ganzzahligen Lösungen hat. Mit tief liegenden Methoden hat Faltings (1983) gezeigt, dass es zumindest nur endlich viele solcher Lösungen geben kann. Wiles hat 1993 einen Beweis des Fermatproblems angekündigt. In seiner Arbeit folgt dieser Beweis aus seinem Beweis eines Spezialfalles der sehr tief liegenden Taniyama-Shimura-Weil-Vermutung, deren Bedeutung weit über das Fermatproblem hinausgeht. Es wurden im Beweis von Wiles zunächst noch Lücken entdeckt, die sich aber 1994 von ihm in Zusammenarbeit mit Taylor schließen ließen. Der endgültige Beweis von Wiles erschien 1996 in den „Annals of Mathematics“.

Im Rahmen der Algebra werden wir uns hier hauptsächlich mit algebraischen Gleichungen in einer Variable beschäftigen. Der „Fundamentalsatz der Algebra“, der auf viele verschiedene Arten bewiesen wurde (wobei der Beweis stets einen analytischen Anteil hat), besagt, dass eine Gleichung

$$a_n X^n + ... + a_1 X + a_0 = 0 \text{ mit } a_i \in \mathbb{C}$$

stets eine Lösung besitzt, falls $n > 0$ und $a_n \neq 0$. Zählt man Vielfachheiten mit, so gibt es sogar stets genau n Lösungen.

Für kleineren Grad n kann man die Lösungen unmittelbar aus den Koeffizienten ausrechnen. Lineare Gleichungen brauchen wir natürlich nicht mehr zu betrachten. Auch für die quadratischen Gleichungen ist die Antwort wohlbekannt: wir teilen zunächst durch $a_2 \neq 0$, um die Normalform

$$X^2 + pX + q = 0$$

zu erhalten. Die Lösungen dieser Gleichung sind dann durch folgende Formel gegeben:

$$-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}\,.$$

Die Formeln für die Gleichungen 3. Grades sind ebenfalls lange bekannt, wenn auch weniger häufig geläufig. Es sind die Cardanoschen Formeln (1545 in einem Buch von Cardano veröffentlicht), die wir jetzt kurz vorstellen wollen.

Nach Division durch a_3 können wir wieder annehmen, dass der Leitkoeffizient $a_3 = 1$ ist. Durch die Transformation $X \mapsto X - \frac{a_2}{3}$ bringen wir den quadratischen Term zum Verschwinden, so dass wir von folgender Normalform ausgehen können:

$$X^3 + pX + q = 0,\ p,q \in \mathbb{C}\,. \qquad \circledast$$

Wir setzen nun

$$D = -4p^3 - 27q^2$$

(**Diskriminante** der Gleichung) und

$$A = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}},$$
$$B = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}.$$

Dabei sollen die dritten Wurzeln so bestimmt sein, dass $AB = -3p$ gilt. Setzen wir nun noch

$$\rho = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3})\,,\ \overline{\rho} = \frac{1}{2}(-1 - \sqrt{-3})\,,$$

so erhalten wir die Lösungen von $\circledast$ als

$$x_1 = \frac{1}{3}(A + B),$$
$$x_2 = \frac{1}{3}(\rho^2 A + \rho B) = \frac{1}{3}(\overline{\rho} A + \rho B),$$
$$x_3 = \frac{1}{3}(\rho A + \rho^2 B) = \frac{1}{3}(\rho A + \overline{\rho} B).$$

Dies sind die Cardanoschen Formeln. Man prüft durch Einsetzen nach, dass es sich wirklich um Lösungen handelt. Wir werden später sehen, wie die Galoistheorie bei der Aufstellung solcher Formeln hilft. Bemerkenswert ist, dass auch im Fall von nur reellen Nullstellen die unterwegs zu berechnenden Werte A und B im Allgemeinen komplex sind. Dass dieser „Umweg“ über die komplexen Zahlen nötig ist, kam damals als Überraschung und hat zur weiteren Anerkennung der Bedeutung der komplexen Zahlen geführt.

Nun zu Gleichungen 4. Grades.

$$a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0 = 0\,,\ a_4 \neq 0$$

Ohne Einschränkung können wir wieder $a_4 = 1$ annehmen. Wir bringen den Term vom Grad 3 wieder durch eine geeignete Substitution zum Verschwinden: $X \mapsto X - \frac{a_3}{4}$. Die Gleichung hat dann die Form

$$X^4 + pX^2 + qX + r = 0\,,\ p,q,r \in \mathbb{C}\,. \qquad \circledcirc$$

Die Lösungen dieser Gleichung gehen auf Ferrari zurück. Zunächst betrachtet man eine zu ◎ gehörende Gleichung 3. Grades, die **kubische Resolvente**:

$$X^3 - 2pX^2 + (p^2 - 4r)X + q^2 = 0\,.$$

Deren Lösungen y_1, y_2, y_3 können wir mit den Cardano-Formeln berechnen. Die Lösungen von ◎ erhält man daraus in der Form:

$$x_1 = \frac{1}{2}(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}),\ x_2 = \frac{1}{2}(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}),$$
$$x_3 = \frac{1}{2}(\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}),\ x_4 = \frac{1}{2}(\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}),$$

wobei die Wurzeln so gewählt sein müssen, dass $\sqrt{-y_1} \cdot \sqrt{-y_2} \cdot \sqrt{-y_3} = -q$ gilt. Durch langwieriges Nachrechnen prüft man nach, dass es sich tatsächlich um Lösungen handelt.
Das Charakteristische an den oben angegebenen Lösungsformeln ist, dass die Lösungen – ähnlich wie im vorherigen geometrischen Konstruktionsproblem – aus den Koeffizienten der Gleichung nur durch Addition, Subtraktion, Multiplikation, Division und Wurzelziehen berechnet werden. Solche Ausdrücke heißen **Radikale**. Wir definieren:

Definition 3.2

Ein Körper L heißt **Radikalerweiterung** eines Teilkörpers $K \subseteq L$, wenn gilt:
(i) Es gibt $w_1,...,w_n \in L$ mit $L = K(w_1,...,w_n)$.
(ii) Es ist $w_1^{r_1} \in K$ und $w_{i+1}^{r_{i+1}} \in K(w_1,...,w_i)$, $1 \leq i \leq n-1$ für geeignete $r_1,...,r_n \in \mathbb{N}$.

Radikalerweiterungen entstehen also durch sukzessive Adjunktion von Wurzeln. Wir erinnern daran, dass beim geometrischen Konstruktionsproblem des vorherigen Paragraphen nur **Quadratwurzeln** adjungiert wurden.

Definition 3.3

Ist ein Polynom $f \in K[X]$ gegeben, so heißt die Gleichung $f = 0$ **durch Radikale auflösbar**, wenn das Polynom f in einer Radikalerweiterung L von K eine Nullstelle besitzt.

Nach dem bisher in diesem Paragraphen Gesagten sind also die Polynome $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $n \leq 4$ durch Radikale über $K = \mathbb{Q}(a_0,...,a_n)$ auflösbar. Genauer haben wir sogar Formeln für die Lösungen angegeben.
Die Geschichte der Galoistheorie beginnt mit dem überraschenden Resultat, dass es solche allgemeinen Lösungsformeln für $n = 5$ nicht mehr geben kann (Abel, 1802-1829). Insbesondere hat Galois (1811-1832) konkrete Gleichungen 5. Grades angegeben, die nicht durch Radikale auflösbar sind. Diese Ergebnisse werden wir erst herleiten können, nachdem wir die Galoistheorie sehr weit entwickelt haben. Es sei hier schon gesagt, dass die Auflösbarkeit durch Radikale mit der gruppentheoretisch definierten Auflösbarkeit der zu f assoziierten, so genannten Galoisgruppe verknüpft ist.
Zunächst werden wir uns mit dem Studium von Körpererweiterungen befassen. Bereits relativ schnell werden wir dann einige der klassischen Konstruktionsprobleme beantworten können.

Kapitel 4

Körpererweiterungen (Grundlagen)

Ist L ein Körper und K ein Teilkörper von L, so nennen wir L einen **Erweiterungskörper** von K und sprechen von einer **Körpererweiterung** L/K. Wesentlich ist für unsere Untersuchungen die Beobachtung, dass in dieser Situation L insbesondere auch ein K-Vektorraum ist (evtl. von unendlicher Dimension) und wir damit das Instrumentarium der Linearen Algebra zur Verfügung haben.

Definition 4.1

Die Vektorraumdimension von L über K heißt der **Grad** von L über K, geschrieben $|L:K|$. Ist $|L:K|$ endlich, so heißt die Körpererweiterung L/K **endlich**.

Bemerkung 4.2

1. Es ist $|L:K|=1$ genau dann, wenn $L=K$.
2. $|\mathbb{C}:\mathbb{R}|=2$, da $1,i$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist.
3. $|\mathbb{Q}(\sqrt{d}):\mathbb{Q}|=2$ für $d\in\mathbb{Q}$ mit $\sqrt{d}\notin\mathbb{Q}$, da $1,\sqrt{d}$ eine $\mathbb{Q}$-Basis für $L=\mathbb{Q}(\sqrt{d})$ ist. Verwende dazu die früher bereits gezeigte Beschreibung
$$\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d}\mid a,b\in\mathbb{Q}\}.$$
4. $|\mathbb{R}:\mathbb{Q}|=\infty$, da jeder endlich-dimensionale $\mathbb{Q}$-Vektorraum nur abzählbar viele Elemente hat.

Erweiterungen eines Teilkörpers $K\subseteq\mathbb{C}$ vom Grad 2 (in $\mathbb{C}$) können wir vollständig beschreiben:

Satz 4.3

Sei $L\subseteq\mathbb{C}$ ein Erweiterungskörper von K.
Dann gilt $|L:K|=2$ genau dann, wenn L aus K durch Adjunktion einer Quadratwurzel entsteht, die nicht in K liegt.

Beweis

Sei $|L:K|=2$ und sei $x\in L\setminus K$. Dann ist $1,x$ eine K-Basis von L und x erfüllt daher eine Gleichung
$$x^2+a_1x+a_0=0 \text{ mit } a_1,a_0\in K.$$
Also ist $x=-\frac{1}{2}\big(a_1\pm\sqrt{a_1^2-4a_0}\big)$ und daher ist $w=\sqrt{a_1^2-4a_0}$ eine Quadratwurzel, die in $L\setminus K$ liegt. Offenbar gilt außerdem $K(w)=K(x)=L$.
Ist $L=K(w)$ für eine Quadratwurzel $w\in L\setminus K$, dann folgt mit demselben Argument wie früher, dass $K(w)$ die Beschreibung
$$K(w)=\{a+bw\mid a,b\in K\}$$
hat und daher $|K(w):K|=2$ ist. □

Die algebraische Charakterisierung der aus einer vorgegebenen Menge konstruierbaren Elemente können wir nun folgendermaßen umformulieren:

Satz 4.4

Sei $M \subseteq \mathbb{C}$, $0,1 \in M$. Dann ist eine Zahl $z \in \mathbb{C}$ genau dann aus M mit Zirkel und Lineal konstruierbar, wenn gilt: $z \in L$ für einen Teilkörper L von $\mathbb{C}$, der aus $K_0 = \mathbb{Q}(M \cup \overline{M})$ durch endlich viele Erweiterungen vom Grad 2 entsteht, d.h. es gibt eine Kette $K_0 \subset ... \subset K_m = L$ mit $|K_i : K_{i-1}| = 2$ für $i \in \{1,...,m\}$.

Definition 4.5

Ein Teilkörper $F \subseteq L$ mit $K \subseteq F$ heißt **Zwischenkörper** von L/K.

Ein äußerst nützlicher Satz ist die so genannte ...

Satz 4.6 (Gradformel)

Für jeden Zwischenkörper F von L/K gilt:

$$|L : K| = |L : F| \cdot |F : K|.$$

Beweis

Ist $|F : K|$ oder $|L : F|$ unendlich, so erst recht $|L : K|$, also ist die Gradformel (bei kanonischer Interpretation) in diesem Fall gültig.

Wir nehmen also nun an, dass $|L : F|$ und $|F : K|$ beide endlich sind. Sei etwa $\{w_1,...,w_r\}$ eine F-Vektorraum-Basis von L und $\{v_1,...,v_s\}$ eine K-Vektorraum-Basis von F.

Wir können dann jedes Element von L in der Form

$$y = \lambda_1 w_1 + ... + \lambda_r w_r$$

schreiben, mit $\lambda_1,...,\lambda_r \in F$. Die λ_i können dann bezüglich der K-Basis von F als

$$\lambda_i = \kappa_{i1} v_1 + ... + \kappa_{is} v_s$$

mit $\kappa_{ij} \in K$ dargestellt werden. Setzen wir dies oben ein, so ergibt sich:

$$y = \sum_{\substack{1 \le i \le r \\ 1 \le j \le s}} \kappa_{ij} v_j w_i .$$

Also ist $\{v_j w_i \mid 1 \le i \le r, 1 \le j \le s\}$ ein K-Erzeugendensystem von L. Dieses System ist aber auch linear unabhängig über K, denn eine Relation

$$\sum_{\substack{1 \le i \le r \\ 1 \le j \le s}} \alpha_{ij} v_j w_i = 0$$

mit $\alpha_{ij} \in K$ zieht zunächst

$$\sum_{j=1}^{s} \alpha_{ij} v_j = 0, \ 1 \le i \le r$$

nach sich, da die w_i's linear unabhängig sind und dann wegen der linearen Unabhängigkeit der v_j's auch $\alpha_{ij} = 0$ für alle i, j.

Also folgt $|L : K| = r \cdot s = |L : F| \cdot |F : K|$. □

Folgerung 4.7

Sei L ein Teilkörper von $\mathbb{C}$, der aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht. Dann ist $|L : K|$ eine 2-Potenz.

Folgerung 4.8

Sei $M \subseteq \mathbb{C}$, $0,1 \in M$, $K_0 = \mathbb{Q}(M \cup \overline{M})$. Ist eine Zahl $z \in \mathbb{C}$ aus M mit Zirkel und Lineal konstruierbar, dann ist $|K_0(z) : K_0|$ eine 2-Potenz.

Beweis
Ist $z \in \mathbb{C}$ aus M mit Zirkel und Lineal konstruierbar, dann liegt z in einem Erweiterungskörper L von K_0, der durch sukzessive Adjunktion von Quadratwurzeln entsteht. Also ist $|L : K_0|$ eine 2-Potenz. Da $K_0(z)$ ein Zwischenkörper von L/K_0 ist, folgt dann aus der Gradformel, dass auch $|K_0(z) : K_0|$ eine 2-Potenz sein muss. □

Unmöglichkeitsbeweise für die geometrischen Konstruktionsaufgaben können wir also z.B. dadurch führen, dass wir für die zu testenden Elemente z nachweisen, dass der Grad $|K_0(z) : K_0|$ keine 2-Potenz ist. Dazu müssen wir uns nun Erweiterungen der Form $K(z)/K$ genauer ansehen.

Kapitel 5

Algebraische und transzendente Körpererweiterungen

Sei L/K eine Körpererweiterung (für den Rest des Paragraphen festgehalten).

Definition 5.1

Ein Element $a \in L$ heißt **algebraisch** über K, falls es ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$ gibt. Falls es kein solches f gibt, heißt a **transzendent** über K.
Die über $\mathbb{Q}$ algebraischen Elemente von $\mathbb{C}$ heißen **algebraische Zahlen**.
Die Körpererweiterung L/K heißt **algebraisch**, wenn alle Elemente $a \in L$ algebraisch über K sind. Ist L/K nicht algebraisch, so heißt L/K **transzendente Körpererweiterung**.

Bemerkung 5.2

1. Als Nullstelle des Polynoms $X^3 - 2$ ist $\sqrt[3]{2}$ eine algebraische Zahl.
2. Die n **-ten Einheitswurzeln** $e^{(2\pi i/n)m}$, $m = 0,...,n-1$ sind als Nullstellen des Polynoms $X^n - 1$ ebenfalls algebraisch über $\mathbb{Q}$.
3. Die Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch, denn jede komplexe Zahl $z = a + bi$, $a,b \in \mathbb{R}$ ist Nullstelle eines Polynoms in $\mathbb{R}[X]$:
$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} = X^2 - 2aX + (a^2 + b^2).$$

Satz 5.3

Die Menge der algebraischen Zahlen ist abzählbar.
Beweis
Die Menge der Polynome vom Grad $\leq n$ in $\mathbb{Q}[X]$ ist abzählbar, da jedes solche Polynom eindeutig seinem Koeffizientenvektor in $\mathbb{Q}^{n+1}$ zugeordnet werden kann, und $\mathbb{Q}^{n+1}$ ist abzählbar. Als abzählbare Vereinigung von abzählbaren Mengen ist daher auch $\mathbb{Q}[X]$ abzählbar. Da jedes Polynom in $\mathbb{Q}[X]$ nur endlich viele Nullstellen besitzt, ist die Gesamtmenge aller Nullstellen, also gerade die Menge der algebraischen Zahlen, ebenfalls abzählbar.
Da in jedem offenen Intervall von $\mathbb{R}$ überabzählbar viele Zahlen liegen, folgt daher unmittelbar:

Folgerung 5.4

In jedem offenen Intervall von $\mathbb{R}$ liegen überabzählbar viele transzendente Zahlen. Insbesondere sind also $\mathbb{R}$ und $\mathbb{C}$ transzendente Körpererweiterungen von $\mathbb{Q}$.

Trotz dieser Reichhaltigkeit an transzendenten Zahlen ist es schwer, für eine gegebene Zahl die Transzendenz nachzuweisen!

Ohne Beweis (die Beweise benötigen nur relativ elementare Hilfsmittel aus der Linearen Algebra und Analysis, sind aber leider etwas technisch) zitieren wir:

Satz 5.5

(i) (Hermite 1873) Die Eulersche Zahl e ist transzendent.
(ii) (Lindemann 1882) Die Kreiszahl π ist transzendent.

Für ein Element $a \in L$ definieren wir

$$K[a] = \left\{ \sum_{i=0}^{m} c_i a^i \mid m \in \mathbb{N}_0,\, c_i \in K,\, i = 0,...,m \right\} = \{ f(a) \mid f \in K[X] \}.$$

Dann ist $K[a] \subseteq L$ ein Ring und offenbar auch ein K-Vektorraum. Es ist $K[a]$ gerade das Bild des von der Einbettung $K \subseteq L$ und der Substitution $X \mapsto a$ induzierten Ringhomomorphismus $\Phi : K[X] \to L$.

Um die Dimension von $K[a]$ zu bestimmen, suchen wir nach der kleinsten Relation zwischen den Potenzen von a – für ein algebraisches Element a ist diese gerade durch das **Minimalpolynom** gegeben:
Ist ein über K algebraisches Element $a \in L$ gegeben, so gibt es ein Polynom $f \in K[X] \setminus \{0\}$ von kleinstem Grad mit $f(a) = 0$. Wir können annehmen, dass der Leitkoeffizient des Polynoms 1 ist, da wir anderenfalls f durch den Leitkoeffizienten dividieren können. Durch diese Normierung wird das nichtkonstante Polynom vom kleinsten Grad mit Nullstelle a eindeutig bestimmt: falls es ein zweites normiertes Polynom vom selben Grad mit Nullstelle a gäbe, würden wir durch Subtraktion ein Polynom kleineren Grades mit Nullstelle a bekommen. Wir können daher jetzt definieren:

Definition 5.6

Ist $a \in L$ algebraisch über K, so heißt das normierte Polynom $f \in K[X] \setminus \{0\}$ vom kleinsten Grad mit $f(a) = 0$ das **Minimalpolynom** von a über K, geschrieben $f = \operatorname{minpol}_K a$. Der Grad von f heißt auch der **Grad** von a über K. Ist $a \in L$ transzendent über K, so setzen wir $\operatorname{minpol}_K a = 0$ und definieren den Grad von a als ∞.

Beispiel 5.7

(i) Die Elemente vom Grad 1 über K sind genau die Elemente von K.
(ii) Der Grad von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist ≤ 3.
(iii) Der Grad der n-ten Einheitswurzeln über $\mathbb{Q}$ ist $\leq n-1$ (für $n \geq 2$), da

$$X^n - 1 = (X-1)(X^{n-1} + ... + X + 1).$$

Ist a algebraisch über K mit Minimalpolynom

$$f = X^n + c_{n-1}X^{n-1} + ... + c_1 X + c_0 \in K[X],$$

dann lässt sich a^n darstellen als

$$a^n = -(c_{n-1}a^{n-1} + ... + c_1 a + c_0).$$

Also lassen sich alle Ausdrücke der Form $\sum_{i=0}^{n} r_i a^i$ bereits in der Form $\sum_{i=0}^{n-1} s_i a^i$ schreiben, d.h.

$$K[a] = \left\{ \sum_{i=0}^{n-1} c_i a^i \mid c_i \in K,\, i = 0,...,n-1 \right\} = \left\{ g(a) \mid g \in K[X],\, \deg g \leq n-1 \right\}.$$

Es ist also $\dim_K K[a] \leq n$.

Für unsere Konstruktionsprobleme waren wir aber nicht auf den Ring $K[a]$, sondern auf den von a und K erzeugten Teilkörper $K(a)$ von L geführt worden.
Wir wollen nun zeigen, dass für ein über K algebraisches Element a der Ring $K[a]$ bereits ein Körper ist und daher in diesem Fall $K[a] = K(a)$ gilt. Dies verallgemeinert die frühere Beschreibung der Körper $K(\sqrt{d})$ als $\{a + b\sqrt{d} \mid a,b \in K\} = K[\sqrt{d}]$.

Satz 5.8

Sei L/K eine Körpererweiterung, $a \in L$. Dann sind äquivalent:

(i) Das Element a ist algebraisch über K.

(ii) $K[a]\,(= K\langle a\rangle)$ ist ein Körper.

(iii) $|K\langle a\rangle : K|$ ist endlich.

(iv) $|K[a] : K|$ ist endlich.

Ist $f = \operatorname{minpol}_K a$, so gilt in diesem Fall:

$$|K[a] : K| = |K\langle a\rangle : K| = \deg f$$

und $\{1, a, a^2, ..., a^{n-1}\}$ mit $n = \deg f$ ist eine K-Basis von $K\langle a\rangle = K[a]$.

Beweis

(i) $\Rightarrow$ (ii): Sei $a \in L$ algebraisch über K, $f = \operatorname{minpol}_K a \in K[X]$, $\deg f = n$. Da f vom Grad n ist, sind $1, a, a^2, ..., a^{n-1}$ linear unabhängig über K, und es ist

$$K[a] = \Big\{\sum_{i=0}^{n-1} c_i a^i \mid c_i \in K,\ i = 0, ..., n-1\Big\} = \big\{g\langle a\rangle \mid g \in K[X],\ \deg g \le n-1\big\}$$

ein n-dimensionaler K-Vektorraum. Wir zeigen nun, dass $K[a]$ ein Körper ist.

Offenbar ist $K[a]$ abgeschlossen bezüglich Addition, Subtraktion und Multiplikation. Wir müssen nun noch für gegebenes $y \in K[a] \setminus \{0\}$ nachweisen, dass $y^{-1} \in K[a]$ gilt. Da $K[a]$ endlich-dimensional über K ist, muss auch y algebraisch über K sein, da sonst $1, y, y^2, ...$ eine unendliche Menge K-linear-unabhängiger Elemente in $K[a]$ wäre. Also erfüllt y eine algebraische Gleichung über K, sei etwa

$$X^m + c_{m-1}X^{m-1} + ... + c_1 X + c_0$$

mit $c_0, ..., c_{m-1} \in K$ das Minimalpolynom von y über K (aus Dimensionsgründen muss genauer $m \le n$ sein). Dann ist $c_0 \neq 0$ und aus der Gleichung

$$y^m + c_{m-1}y^{m-1} + ... + c_1 y + c_0 = 0$$

erhalten wir nach Division durch $c_0 y$:

$$y^{-1} = -\frac{1}{c_0}\big(y^{m-1} + c_{m-1}y^{m-2} + ... + c_1\big) \in K[a].$$

Also ist $K[a]$ ein in $K\langle a\rangle$ enthaltener Teilkörper von L. Da aber $K\langle a\rangle$ der kleinste Teilkörper von L ist, der K und a enthält, muss bereits $K[a] = K\langle a\rangle$ gelten.

(ii) $\Rightarrow$ (iii): Sei $K[a] = K\langle a\rangle$. Da $a^{-1} \in K[a]$, gibt es $m \in \mathbb{N}_0$ und $c_0, ..., c_m \in K$, $c_m \neq 0$, mit

$$a^{-1} = \sum_{i=0}^{m} c_i a^i\,.$$

Dann ist

$$a^{m+1} = \frac{1}{c_m}\Big(1 - \sum_{i=0}^{m-1} c_i a^{i+1}\Big),$$

also ist $1, a, a^2, ..., a^m$ bereits ein K-Erzeugendensystem für $K\langle a\rangle$.

(iii) $\Rightarrow$ (iv): Dies ist wegen $K[a] \subseteq K\langle a\rangle$ klar.

(iv) $\Rightarrow$ (i): Dies folgt sofort mit dem bereits in (i) $\Rightarrow$ (ii) verwendeten Argument. □

Definition 5.9

Erweiterungen L/K der speziellen Form $L = K\langle a\rangle$ (für ein geeignetes $a \in L$) heißen **einfache Körpererweiterungen**.

Wir gehen auf diese speziellen Körpererweiterungen im nächsten Abschnitt noch ausführlich ein.

Bemerkung 5.10

Ist $|L:K|$ endlich, so ist L/K algebraisch. Genauer gilt in diesem Fall: $|K(a):K| = |K[a]:K| \leq |L:K|$ für alle $a \in L$. Dies folgt unmittelbar mit dem im Beweis oben schon benutzten Argument. Aus der Gradformel folgt dann sogar: $|K(a):K| \,|\, |L:K|$ für alle $a \in L$.
Die Umkehrung gilt nicht: es gibt unendliche algebraische Körpererweiterungen, die wir z.B. als Körpertürme konstruieren können. Dazu sei $(I,<)$ eine linear geordnete Indexmenge, K_i, $i \in I$ eine Familie von Teilkörpern eines Körpers K, so dass für $i < j$ die Inklusion $K_i \subset K_j$ besteht. Dann heißt $\{K_i\}_{i\in I}$ ein **Körperturm**. Man überlegt sich leicht, dass dann $\bigcup_{i\in I} K_i$ ein Teilkörper von K ist.
Wählen wir z.B. $K_i = \mathbb{Q}(2^{1/2^i})$ für $i \in \mathbb{N}$, so ist $\{K_i\}_{i\in\mathbb{N}}$ ein Körperturm in $\mathbb{R}$, und $\bigcup_{i\in\mathbb{N}} K_i$ ist eine unendliche algebraische Erweiterung von $\mathbb{Q}$ (Übung).

Eine andere potentiell unendliche algebraische Erweiterung haben wir früher bereits kennen gelernt:

Folgerung 5.11

Sei $M \subseteq \mathbb{C}$, $0,1 \in M$, $K_0 = \mathbb{Q}(M \cup \overline{M})$. Dann ist die Erweiterung $\widehat{M}/K_0$ algebraisch.

Folgerung 5.12

Die Quadratur des Kreises mit Zirkel und Lineal ist unmöglich.

Beweis

Dies folgt sofort daraus, dass die Zahl π transzendent ist. □

Wir können nun die Beschreibung der Körpererweiterungen vom Grad 2 verallgemeinern und alle endlichen Körpererweiterungen über die Adjunktion von (endlich vielen) Elementen charakterisieren:

Satz 5.13

Für eine Körpererweiterung L/K sind folgende Aussagen äquivalent:

(i) L/K ist eine endliche Erweiterung.

(ii) L/K ist algebraisch, und es gibt $a_1,...,a_n \in L$ mit $L = K(a_1,...,a_n)$.

(iii) Es gibt $a_1,...,a_n \in L$ mit $L = K(a_1,...,a_n)$, wobei a_1 algebraisch über K und a_{i+1} algebraisch über $K(a_1,...,a_i)$, $1 \leq i \leq n-1$ ist.

Beweis

(i) $\Rightarrow$ (ii): Dass L/K algebraisch ist, haben wir bereits oben bemerkt.
Wir beweisen die zweite Aussage nun durch Induktion nach $d = |L:K|$. Ist $d = 1$, so ist $L = K$ und wir sind wir fertig. Sei also $d > 1$. Dann gibt es ein $a \in L \setminus K$, also ist $|K(a):K| > 1$ und $|L:K(a)| = \frac{|L:K|}{|K(a):K|} < d$. Nach Induktion ist dann $L = K(a)(a_2,...,a_n) = K(a,a_2,...,a_n)$ für geeignete $a_2,...,a_n \in L$.
(ii) $\Rightarrow$ (iii): trivial.
(iii) $\Rightarrow$ (i): Setze $K_0 = K$ und $K_i = K(a_1,...,a_i)$ für $1 \leq i \leq n$. Da a_{i+1} algebraisch über K_i ist, ist $|K_{i+1}:K_i| = d_i$ endlich. Also ist nach der Gradformel auch $|L:K| = \prod_{i=0}^{n-1} d_i$ endlich.

Folgerung 5.14 (Transitivität der Algebraizität)

Sei k ein Zwischenkörper der Körpererweiterung L/K. Dann ist L/K genau dann algebraisch, wenn L/k und k/K algebraisch sind.

Beweis

Ist L/K algebraisch, so sind offenbar auch L/k und k/K algebraisch. Seien nun L/k und k/K algebraisch, $a \in L$. Ist $0 \neq f \in k[X]$ mit $f(a) = 0$, so erhält man durch Adjunktion der Koeffizienten $b_0,...,b_n$ von f an K: a ist algebraisch über $K(b_0,...,b_n)$, also gilt

$$|K(a) : K| \leq |K(a)(b_0,...,b_n) : K(b_0,...,b_n)| \cdot |K(b_0,...,b_n) : K| < \infty$$

und damit a algebraisch über K.

Folgerung 5.15

Sei L/K eine beliebige Körpererweiterung.

(i) Die Menge $\overline{K}$ aller über K algebraischen Elemente von L ist ein Zwischenkörper von L/K.

(ii) $\overline{K}/K$ ist eine algebraische Körpererweiterung.

(iii) Ist $a \in L$ algebraisch über $\overline{K}$, so ist $a \in \overline{K}$.

Beweis

Sind $x,y \in L$ algebraisch über K, so ist nach obigem Satz $K(x,y)/K$ eine algebraische Körpererweiterung. Also sind auch $x+y, x-y, x \cdot y$ bzw. y^{-1} (falls $y \neq 0$) als Elemente von $K(x,y)$ algebraisch über K.
Die zweite Aussage folgt aus den Definitionen.
Ist $a \in L$ algebraisch über $\overline{K}$, so ist $\overline{K}(a)/\overline{K}$ algebraisch und daher nach der vorhergehenden Folgerung $\overline{K}(a)/K$ algebraisch, also a algebraisch über K.

Beispiel 5.16

Sei $z = a + bi \in \mathbb{C}$, $a,b \in \mathbb{R}$, und sei z algebraisch über $\mathbb{Q}$, $f = \text{minpol}_{\mathbb{Q}}\, z$. Dann ist auch $f(\overline{z}) = 0$, also ist auch $\overline{z}$ algebraisch über $\mathbb{Q}$. Damit folgt, dass auch $a = \frac{1}{2}(z + \overline{z}) \in \mathbb{Q}(z,\overline{z})$ algebraisch über $\mathbb{Q}$ ist. Da auch i algebraisch über $\mathbb{Q}$ ist, ist außerdem auch $b = \frac{1}{2i}(z - \overline{z}) \in \mathbb{Q}(z,\overline{z},i)$ algebraisch über $\mathbb{Q}$.

Definition 5.17

Der Körper $\overline{K}$ der über K algebraischen Elemente von L heißt der **algebraische Abschluss** von K in L. Für $K = \mathbb{Q}$ und $L = \mathbb{C}$ heißt der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ der **Körper der algebraischen Zahlen**.

(Achtung: für $K \subseteq \mathbb{C}$ nicht den algebraischen Abschluss $\overline{K}$ mit der Menge der komplex konjugierten Elemente zu K verwechseln!)

Zuletzt wollen wir noch einen sehr nützlichen Begriff einführen, der zu zwei Zwischenkörpern einen neuen Körper bildet und die Vererbung von Eigenschaften auf den neuen Körper untersuchen.

Definition 5.18

Seien E_1 und E_2 zwei Zwischenkörper der Erweiterung L/K. Dann heißt

$$E_1E_2 = E_1(E_2) = E_2(E_1) = K(E_1 \cup E_2)$$

das **Körperkompositum** von E_1 und E_2 in L.

Satz 5.19

Seien L/K, E_1, E_2 wie oben. Dann gilt:

(i) Ist E_1/K algebraisch, so auch E_1E_2/E_2.

(ii) Ist E_1/K endlich, so auch E_1E_2/E_2. Genauer gilt: $|E_1E_2 : E_2| \leq |E_1 : K|$.

(iii) Sind E_1/K und E_2/K algebraisch, so auch E_1E_2/K.

(iv) Sind E_1/K und E_2/K endlich, so auch E_1E_2/K. Sind $|E_1 : K|$ und $|E_2 : K|$ teilerfremd, so ist $|E_1E_2 : K| = |E_1 : K| \cdot |E_2 : K|$.

Beweis

Übung. □

Kapitel 6

Einfache Körpererweiterungen

Wir wollen nun die Struktur der einfachen Körpererweiterungen $K(a)/K$ genauer untersuchen. Einige Eigenschaften hatten wir im vorhergehenden Paragraphen bereits gezeigt, insbesondere hatten wir einen qualitativen Unterschied zwischen algebraischen und transzendenten Elementen festgestellt. In diesem Abschnitt wollen wir einen genaueren Vergleich zwischen $K[a]$ bzw. $K(a)$ und dem Polynomring $K[X]$ ziehen.

Definition 6.1

Ein Element $a \in L$ heißt ein **primitives Element** der einfachen Körpererweiterung L/K, falls $L = K(a)$.

Für das Rechnen in $K[a]$ bzw. $K(a)$ kommt es auf die algebraischen Relationen an, die das Element a erfüllt.

Sei im Folgenden L/K stets eine Körpererweiterung und $a \in L$.

Zentral für das Rechnen mit a sind die polynomialen Relationen für a, also die Menge

$$I = I_a = \{ g \in K[X] \mid g(a) = 0 \}.$$

Diese Menge I ist genau der Kern des Einsetzungshomomorphismus'

$$\varphi_a : K[X] \to L,\ \textstyle\sum_i c_i X^i \mapsto \sum_i c_i a^i .$$

Kerne von Ringhomomorphismen haben als Teilmengen des sie enthaltenden Ringes besondere Eigenschaften. Der folgende Begriff kam bereits in der Linearen Algebra vor, dort allerdings nur für den Fall kommutativer Ringe:

Definition 6.2

Sei R ein Ring mit 1. Eine nichtleere Teilmenge $I \subseteq R$ heißt ein (zweiseitiges) **Ideal** von R, wenn gilt:

(i) Sind $a,b \in I$, dann ist auch $a + b \in I$.

(ii) Ist $a \in I$, dann sind für alle $r \in R$ auch $ar, ra \in I$.

Schreibweise: $I \trianglelefteq R$.

Ideale sind also additive Untergruppen von R, die nicht nur bezüglich Multiplikation innerhalb der Untergruppe abgeschlossen sind, sondern sogar bezüglich Multiplikation mit beliebigen Ringelementen.

Beispiel 6.3

(i) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, für alle $n \in \mathbb{Z}$.

(ii) Ist L/K eine Körpererweiterung und $V \subseteq L$, dann ist

$$I_V = \{ f \in K[X] \mid f(x) = 0 \text{ für alle } x \in V \}$$

ein Ideal des Polynomrings $K[X]$, das **Verschwindungsideal** zu V.

Das oben definierte Ideal $I_a = \operatorname{Kern} \varphi_a$ hat – je nach Kontext – unterschiedliche Bezeichnungen, es heißt Verschwindungsideal von a oder auch Relationenideal von a.

Wie oben schon bemerkt, sind Kerne von Ringhomomorphismen Ideale, und auch die Umkehrung ist richtig. Wir wollen dazu eine entsprechende Ringkonstruktion wie im kommutativen Fall durchführen.
Wir starten also mit einem Ring mit 1 und einem (zweiseitigen) Ideal I von R. Auf R wird eine Relation $\sim$ definiert durch

$$\text{für } a,b \in R: \quad a \sim b \iff a - b \in I .$$

Da I eine additive Untergruppe von R ist, definiert dies eine Äquivalenzrelation. Statt $a \sim b$ wird auch

$$a \equiv b \bmod I$$

geschrieben. Die Äquivalenzklassen dieser Relation sind

$$\overline{a} := \{b \in R \mid b \sim a\} = \{a + c \mid c \in I\} =: a + I .$$

Die Äquivalenzklasse $\overline{a}$ heißt die **Restklasse** von a modulo I. Die Menge der Äquivalenzklassen wird dann mit R/I bezeichnet.
Wir betrachten nun die kanonische Abbildung

$$\pi : R \to R/I, \ a \mapsto \overline{a}$$

und zeigen: es gibt auf R/I genau eine Ringstruktur, so dass π ein Ringhomomorphismus ist.

Damit π ein Ringhomomorphismus ist, müssen wir setzen:

$$\overline{a} + \overline{b} = \overline{a + b}, \ \overline{a} \cdot \overline{b} = \overline{a \cdot b} .$$

Nachzuweisen bleibt nun, dass dies eine wohl definierte Setzung ist.
Seien also $a,a',b,b' \in R$ mit $a \sim a'$, $b \sim b'$. Dann gibt es $x,y \in I$ mit $a = a' + x$, $b = b' + y$. Also folgt

$$a + b = a' + b' + (x + y), \ ab = a'b' + (a'y + xb' + xy) .$$

Da I ein Ideal in R ist, liegen $x + y$ bzw. $a'y + xb' + xy$ in I, also folgt

$$a + b \sim a' + b', \ ab \sim a'b'$$

und damit ist die Wohldefiniertheit gezeigt.
Die Ringeigenschaften lassen sich leicht überprüfen.
Der Ring R/I mit der oben definierten Addition und Multiplikation heißt der **Restklassenring von R modulo I** (oder auch: **nach I**). Die Abbildung π heißt der **kanonische Restklassenhomomorphismus** oder auch die **kanonische Abbildung** von R nach R/I. Das Ideal I von R ist dann genau der Kern von π.

Beispiel 6.4

Für alle $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$, und $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ist der Restklassenring von $\mathbb{Z}$ nach $n\mathbb{Z}$.

Wir können mit Hilfe geeigneter Restklassenringe jeden Ringhomomorphismus in „gute“ Homomorphismen zerlegen. Auch diese Zerlegung ist uns bereits in der Linearen Algebra begegnet:

Satz 6.5 (Homomorphiesatz)

Seien R, R' Ringe (mit 1), und sei $\varphi : R \to R'$ ein Ringhomomorphismus. Weiter sei $\pi : R \to R/\operatorname{Kern}\varphi$ der kanonische Restklassenhomomorphismus.
Dann gibt es genau einen Ringhomomorphismus

$$\Phi : R/\operatorname{Kern}\varphi \to R'$$

mit $\varphi = \Phi \circ \pi$, d.h. für den das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\Phi} & \\ & R/\mathrm{Kern}\,\varphi & \end{array}$$

kommutativ ist, nämlich $\Phi : \overline{a} \mapsto \varphi(a)$.
Außerdem ist Φ ein Monomorphismus mit $\mathrm{Bild}\,\Phi = \mathrm{Bild}\,\varphi$, und daher gilt die Isomorphie

$$R/\mathrm{Kern}\,\varphi \cong \mathrm{Bild}\,\varphi\,.$$

Beweis
Der Beweis verläuft genauso wie aus der Linearen Algebra bereits bekannt. □

Wenden wir die obigen allgemeinen Ergebnisse auf unsere Ausgangssituation an (wobei für φ dann der Einsetzungshomomorphismus mit $X \mapsto a$ gewählt wird), so erhalten wir:

Folgerung 6.6

Sei L/K eine Körpererweiterung, $a \in L$, I_a das Relationenideal von a in $K[X]$, dann gilt:

$$K[a] \cong K[X]/I_a\,.$$

Unser früheres Ergebnis für algebraische Elemente (Satz 5.6) können wir äquivalent für transzendente Elemente formulieren:

Satz 6.7

Sei L/K eine Körpererweiterung, $a \in L$. Dann sind äquivalent:
(i) a ist transzendent über K, d.h. a erfüllt keine algebraische Relation über K.
(ii) $K[a] \cong K[X]$.
(iii) $K[a]$ ist ein Körper.

Wir werden etwas später noch darauf eingehen, wie der Körper $K(a)$ im Fall eines über K transzendenten Elementes a aussieht.

Kehren wir nun zurück zum Fall eines über K algebraischen Elementes a, bei dem das Relationenideal also nichttrivial ist. Wir untersuchen das Relationenideal nun genauer:

Satz 6.8

Sei L/K eine Körpererweiterung, $a \in L$, $f = \mathrm{minpol}_K\, a$. Dann gilt:

$$I_a = K[X]f = \{hf \mid h \in K[X]\}\,.$$

Beweis
Nach Definition ist $f \in I_a$ und damit ist auch $K[X]f \subseteq I_a$, da I_a ein Ideal ist.
Sei umgekehrt $g \in I_a$. Da wir in $K[X]$ Division mit Rest durchführen können, gibt es Polynome $q,r \in K[X]$ mit

$$g = qf + r \text{ und } \deg r < \deg f\,.$$

Dann folgt

$$0 = g(a) = q(a)f(a) + r(a) = r(a),$$

also ist auch $r \in I_a$. Aber da f das Minimalpolynom von a über K ist, folgt dann $r = 0$. Also ist $g = qf \in K[X]f$, wie zu zeigen war. □

Wir erinnern uns daran, dass Ideale mit dieser besonders einfachen Struktur einen speziellen Namen haben:

Definition 6.9

Sei R ein kommutativer Ring mit 1. Für $a \in R$ setzen wir

$$\langle a \rangle = Ra = \{ra \mid r \in R\}.$$

Das Ideal(!) $\langle a \rangle$ heißt das von a erzeugte **Hauptideal** von R.
Für den Restklassenring $R/\langle a \rangle$ wird in diesem Fall gelegentlich auch R/a geschrieben.
Der Ring R heißt **Hauptidealring**, wenn alle seine Ideale Hauptideale sind.

Bereits in der Linearen Algebra hatten wir gezeigt, dass $\mathbb{Z}$ und die Polynomringe $K[X]$ über Körpern K Hauptidealringe sind. Wir werden dies im nächsten Abschnitt im Kontext der euklidischen Ringe noch einmal aufgreifen.

Wir können für die algebraischen Elemente nun folgern:

Satz 6.10

Sei L/K eine Körpererweiterung, $a \in L$ algebraisch über K, $f = \operatorname{minpol}_K a$. Dann gilt:

$$K\langle a \rangle = K[a] \cong K[X]/fK[X] =: K[X]/f,$$

wobei der Isomorphismus durch den Einsetzungshomomorphismus $X \mapsto a$ induziert ist.

Wir können an dieser Stelle auch das Delische Problem der Würfelverdopplung beantworten:

Folgerung 6.11

Die Würfelverdopplung ist mit Zirkel und Lineal nicht möglich.

Beweis

Wir hatten bereits als notwendiges Kriterium hergeleitet, dass $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$ eine 2-Potenz sein muss.
Für $a = \sqrt[3]{2}$ ist $g = X^3 - 2 \in I_a$. Ist $f = \operatorname{minpol}_K a$, dann ist $g = fh$ für ein geeignetes $h \in \mathbb{Q}[X]$. Also ist $\deg f \leq 3$. Da $\sqrt[3]{2} \notin \mathbb{Q}$, ist $\deg f > 1$. Da $X^3 - 2$ keine Nullstelle in $\mathbb{Q}$ hat, kann auch h nicht vom Grad 1 sein. Also folgt $f = g$, und damit ist

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

Da dieser Grad also keine 2-Potenz ist, ist damit die Würfelverdopplung mit Zirkel und Lineal als unmöglich nachgewiesen. □

Wir haben nun noch zu klären, wie die von transzendenten Elementen erzeugten einfachen Körpererweiterungen aussehen.
Sei also L/K eine Körpererweiterung, $a \in L$ transzendent. Dann wissen wir bereits:

$$R := K[a] \cong K[X].$$

In L können wir $K\langle a \rangle$ leicht beschreiben, nämlich als

$$K\langle a \rangle = \left\{ \frac{f(a)}{g(a)} \mid f, g \in K[X],\ g(a) \neq 0 \right\}.$$

Ist R ein beliebiger Teilring von L, dann heißt der von R erzeugte Körper in L

$$\left\{ \frac{r}{s} \mid r, s \in R,\ s \neq 0 \right\}$$

auch der **Körper der Brüche von R in L**.

Startet man mit einem beliebigen Ring R mit 1, der nicht bereits als Teilring eines Körpers gegeben ist (z.B. mit dem Polynomring $K[X]$), dann stellt sich die Frage, ob es überhaupt einen Körper gibt, der R enthält. Falls es einen solchen Körper gibt, dann muss der Ring R notwendig kommutativ sein, und es kann in R keine Gleichung

$$ab = 0 \text{ mit } a,b \in R\,,\ a,b \neq 0$$

gelten, d.h. der Ring R muss nullteilerfrei sein.
Wir gehen also jetzt von einem Integritätsring R aus. Der Körper, den wir zu R konstruieren wollen, soll in einem zu präzisierenden Sinn minimal sein. Wir formulieren dies wieder als Lösung eines universellen Problems:

Satz 6.12

Sei R ein Integritätsring. Dann gibt es einen Körper K und einen Ringmonomorphismus $\iota : R \to K$ mit folgender (universeller) Eigenschaft: Zu jedem Körper L und Ringmonomorphismus $\tau : R \to L$ gibt es genau einen Ringhomomorphismus $\psi : K \to L$ mit $\tau = \psi \circ \iota$, d.h. das folgende Diagramm ist kommutativ:

$$\begin{array}{ccc} R & \xrightarrow{\ \tau\ } & L \\ & {\scriptstyle\iota}\searrow \quad \nearrow{\scriptstyle\psi} & \\ & K & \end{array}$$

Ein solcher Körper ist der Körper der Brüche von $\iota(R)$ in K. K heißt ein **Quotientenkörper** von R.

Bemerkung 6.13

Aus der universellen Eigenschaft folgt, dass die Quotientenkörper von R alle zueinander isomorph sind (Übung). Wir sprechen daher von **dem** Quotientenkörper von R und bezeichnen ihn mit $Q(R)$. Außerdem identifizieren wir R mit $\iota(R) \subseteq Q(R)$. Nach dem obigen Satz gilt dann

$$Q(R) = \left\{ \frac{r}{s} \mid r,s \in R,\ s \neq 0 \right\}.$$

Beweis (Satz 6.12)
Die Konstruktion eines Körpers K wie im Satz orientiert sich an der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.
Wir betrachten die Menge

$$\mathcal{M} = \left\{ (r,s) \mid r,s \in R,\ s \neq 0 \right\}$$

und die folgende Relation auf $\mathcal{M}$:

$$(r,s) \sim (u,v) \iff rv = su\,.$$

Es ist leicht nachzurechnen, dass $\sim$ eine Äquivalenzrelation auf $\mathcal{M}$ definiert. Auf der Menge $K = \mathcal{M}/\!\sim$ der Äquivalenzklassen definieren wir nun eine Addition und Multiplikation. Wir bezeichnen die Äquivalenzklasse von (r,s) bezüglich $\sim$ mit r/s und setzen

$$r/s + u/v = (rv + su)/sv\,,\ r/s \cdot u/v = ru/sv\,.$$

Es ist wieder zu überprüfen, dass diese Setzung wohl definiert ist. Wir kontrollieren dies hier für die Addition, die Multiplikation sei als Übung überlassen.
Seien also $(r',s'),(u',v') \in \mathcal{M}$ mit $(r,s) \sim (r',s')$ und $(u,v) \sim (u',v')$. Dann ist $rs' = sr'$ und $uv' = vu'$. Also folgt

$$(rv + su)s'v' = rs'vv' + ss'uv' = sr'vv' + ss'vu' = (r'v' + s'u')sv\,,$$

was $(rv + su, sv) \sim (r'v' + s'u', s'v')$ und damit die Behauptung zeigt.
Da R ein kommutativer Ring ist, ist auch K ein kommutativer Ring. Außerdem sind $0/1$ und $1/1$ die Null bzw. die Eins in K (hätte R keine 1 enthalten, so hätten wir die Eins in K an dieser Stelle als r/r für $0 \neq r \in R$ erhalten). Für jedes $0 \neq r/s \in K$ ist offenbar s/r ein Inverses in K. Also ist K ein Körper.
Eine Einbettung $\iota : R \to K$ definieren wir durch $\iota(r) = r/1$. Dies ist offenbar ein Ringmonomorphismus. Der Körper der Brüche von $\iota(R)$ in K ist dann

$$\big\{(r/1)/(s/1) \mid r,s \in R,\, s \neq 0\big\} = \big\{r/s \mid r,s \in R,\, s \neq 0\big\} = K\,,$$

wie behauptet.

Wir haben noch zu zeigen, dass K mit ι tatsächlich eine Lösung des im Satz beschriebenen universellen Problems ist.

Sei also L ein Körper und $\tau : R \to L$ ein Ringmonomorphismus.

Ist $\psi : K \to L$ ein Ringhomomorphismus mit $\tau = \psi \circ \iota$, dann ist $\psi(r/1) = \tau(r)$ und daher

$$\psi(r/s) = \psi(r/1)\psi\big((s/1)^{-1}\big) = \psi(r/1)(\psi(s/1))^{-1} = \tau(r)(\tau(s))^{-1}\,,$$

d.h. ψ ist dann eindeutig festgelegt. Umgekehrt lässt sich aber leicht nachrechnen, dass die obige Gleichung einen Ringhomomorphismus ψ mit $\tau = \psi \circ \iota$ definiert. □

Beispiel 6.14

$\mathbb{Q} = Q(\mathbb{Z})$ ist der Quotientenkörper von $\mathbb{Z}$.

Mit der obigen Konstruktion erhalten wir insbesondere einen Quotientenkörper für den Polynomring $K[X]$, da $K[X]$ ein Integritätsring ist.

Definition 6.15

Sei K ein Körper, $K[X]$ der Polynomring über K in der Unbestimmten X. Dann heißt

$$K(X) = Q(K[X])$$

der **rationale Funktionenkörper** über K in der Unbestimmten X. Die Elemente in $K(X)$ heißen **rationale Funktionen**.

Nach dem vorhergehenden Satz können wir $K(X)$ explizit so beschreiben:

$$K(X) = \left\{\frac{f}{g} \mid f,g \in K[X],\, g \neq 0\right\},$$

d.h. jede rationale Funktion ist Quotient zweier Polynome.

Folgerung 6.16

Sei L/K eine Körpererweiterung, $a \in L$ transzendent über K. Dann induziert der Einsetzungshomomorphismus $X \mapsto a$ einen Isomorphismus von Körpern:

$$K(a) \cong K(X)\,.$$

Sind umgekehrt diese Körper isomorph, so ist a transzendent über K.

Beweis

Ist a transzendent, so induziert der Einsetzungshomomorphismus $X \mapsto a$ einen Isomorphismus $\tau : K[X] \to K[a]$. Der Ringhomomorphismus τ lässt sich wegen der Eindeutigkeit und universellen Eigenschaft des Quotientenkörpers dann eindeutig zu einem Isomorphismus $\hat{\tau} : K(X) \to K(a)$ fortsetzen.

Da bereits $K[X] \subset K(X)$ unendlich-dimensional über K ist, folgt die zweite Behauptung aus den bereits gezeigten Eigenschaften algebraischer bzw. transzendenter Elemente. □

Kapitel 7

Teilbarkeitstheorie in kommutativen Ringen

Unsere geometrischen Konstruktionsprobleme haben wir in die algebraische Frage übersetzt, ob eine gegebene Zahl $a \in \mathbb{C}$ in einem speziellen Zwischenkörper $\mathbb{C}/K$ liegt, wobei K der durch die vorgegebene Punktemenge M bestimmte Grundkörper ist.
Grundlegend ist die Bestimmung des Grades $|K(a):K|$. Wir haben ja bereits gesehen, dass damit bereits erfolgreich die Unmöglichkeit einiger Konstruktionsaufgaben gezeigt werden konnte. Dazu müssen wir das Minimalpolynom von a über K bestimmen. Oft ist es einfach, ein Polynom $\in K[X]\setminus\{0\}$ mit Nullstelle a zu finden. Dann ist zu entscheiden, ob dieses Polynom von minimalem Grad ist.

Beispiel 7.1

Für die Konstruktion regulärer n-Ecke hatten wir $a = e^{2\pi i/n}$ über $K = \mathbb{Q}$ zu untersuchen. Es ist a Nullstelle von

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + ... + X + 1) \in \mathbb{Q}[X].$$

Das Minimalpolynom $f = \text{minpol}_{\mathbb{Q}}\, a$ teilt also $X^{n-1} + X^{n-2} + ... + X + 1$. Dieses Polynom zerfällt aber i.A. noch weiter in Faktoren.
Da wir bereits wissen, dass das Verschwindungsideal

$$I_a = (f) \text{ mit } f = \text{minpol}_K\, a$$

ist, wird jedes Polynom mit Nullstelle a von f geteilt. Unsere Aufgabe ist es also, zu entscheiden, ob sich das gefundene Polynom faktorisieren lässt bzw. wie die Faktorisierung aussieht.
Wir wollen zunächst allgemeine Grundlagen aus der Teilbarkeitstheorie kommutativer Ringe behandeln, bevor wir dann wieder zu Polynomringen zurückkehren und die dort spezifischen Methoden weiter entwickeln. (Diese Themen wurden zum Teil bereits in der Linearen Algebra II angesprochen.)

Sei im Folgenden R stets ein kommutativer Ring mit 1.

Sind $a,b \in R$, dann heißt b ein **Teiler** von a, wenn es ein $c \in R$ mit $a = bc$ gibt. Wir schreiben kurz $b|a$. Ist b kein Teiler von a, so wird $b\nmid a$ geschrieben.

Bemerkung 7.2

(a) Die Eigenschaften
   (i) Es gilt für alle $a \in R$: $a|a$.
   (ii) Gilt $b|a$ und $c|b$, dann folgt $c|a$.
   (iii) Für alle $a \in R$ gilt: $1|a$ und $a|0$.

   besagen, dass die Teilbarkeitsrelation eine teilweise Ordnung mit einem größten und kleinsten Element ist.

(b) Die Teilbarkeitseigenschaften sind außerdem verträglich mit den Ringoperationen:
   (i) Gilt $b|a$ und $d|c$, dann gilt auch $bd|ac$.
   (ii) Gilt $b|a$ und $b|c$, dann gilt auch $b|a+c$.

(c) Teilbarkeit ist immer nur von Interesse **modulo Einheiten**, denn ist x invertierbar in R, dann gilt:

$$b|a \iff bx|a\,.$$

Nach Definition können wir die invertierbaren Elemente in R als Teiler von 1 identifizieren:

$$R^* = \{x \in R \mid x|1\}\,.$$

Definition 7.3

Sind $a,b \in R$ mit $a|b$ und $b|a$, dann heißen a,b zueinander **assoziierte** Elemente von R, kurz: $a \sim b$.

Bemerkung 7.4

Assoziiertheit ist eine Äquivalenzrelation. Ist R ein Integritätsring, dann haben die Assoziiertenklassen die Form:

$$\{b \in R \mid b \sim a\} = R^*a\,.$$

Beispiel 7.5

(i) Die Assoziiertenklassen in $\mathbb{Z}$ sind $\{a,-a\}$ für $a \in \mathbb{Z}$.

(ii) Für einen Körper K ist nach Definition $K^* = K \setminus \{0\}$, also hat K nur die zwei Assoziiertenklassen $\{0\}$ und K^*.

(iii) Für einen Integritätsring R ist auch $R[X]$ ein Integritätsring, und es gilt $R[X]^* = R^*$.

(iv) Einheiten in $\mathbb{Z}/6\mathbb{Z}$ sind nur die Restklassen von 1 und 5.

Die Teilbarkeitsbeziehung lässt sich idealtheoretisch formulieren:

$$b|a \iff Ra = (a) \subseteq Rb = (b)\,.$$

Für assoziierte Elemente gilt damit:

$$a \sim b \iff (a) = (b)\,.$$

In der Sprache der Ideale lassen sich auch die Begriffe des (größten) gemeinsamen Teilers und des (kleinsten) gemeinsamen Vielfachen sehr gut untersuchen.
Wir wollen zunächst diese Begriffe in allgemeinen kommutativen Ringen definieren:

Definition 7.6

Seien $a_1,...,a_n \in R$.

(a) Ein Element $d \in R$ heißt ein **größter gemeinsamer Teiler** von $a_1,...,a_n$ (kurz: $\mathrm{ggT}(a_1,...,a_n)$), wenn gilt:

(i) d ist ein gemeinsamer Teiler von $a_1,...,a_n$.

(ii) Ist t ein gemeinsamer Teiler von $a_1,...,a_n$, so gilt $t|d$.

Ist 1 ein ggT von $a_1,...,a_n$, so heißen $a_1,...,a_n$ zueinander **teilerfremd**.

(b) Ein Element $v \in R$ heißt ein **kleinstes gemeinsames Vielfaches** von $a_1,...,a_n$ ($\mathrm{kgV}(a_1,...,a_n)$), wenn gilt:

(i) v ist ein gemeinsames Vielfaches von $a_1,...,a_n$.

(ii) Ist u ein gemeinsames Vielfaches von $a_1,...,a_n$, so gilt $v|u$.

Bemerkung 7.7

Die ggT 's von $a_1,...,a_n$ bzw. die kgV 's von $a_1,...,a_n$ bilden jeweils eine Assoziiertenklasse in R. Da Teilbarkeit nur **modulo Einheiten** untersucht wird, macht es also Sinn, von **dem** ggT bzw. kgV zu sprechen – falls diese Elemente überhaupt existieren (s.u.).

Bevor wir die ggT - und kgV -Beziehung nun mit Hilfe der Ideale umformulieren, benötigen wir noch ein ...

Lemma 7.8

(i) Ist I_λ, $\lambda \in \Lambda$ eine Familie von Idealen in R, dann ist auch $\bigcap_{\lambda\in\Lambda} I_\lambda$ ein Ideal in R.

(ii) Seien $I_1,...,I_n$ Ideale von R, dann ist auch

$$I_1 + ... + I_n = \left\{a_1 + ... + a_n \mid a_j \in I_j,\ j = 1,...,n\right\}$$

ein Ideal in R (die **Summe** der Ideale $I_1,...,I_n$).

Definition 7.9

Ist $M \subseteq R$, dann ist

$$(M) := \bigcap\left\{I \mid I \text{ Ideal von } R,\ M \subseteq I\right\}$$

ein Ideal von R. Es heißt das **von** M **erzeugte Ideal**. Für $M = \{a_1,...,a_n\}$ schreiben wir für das von M erzeugte Ideal: $(a_1,...,a_n)$.

Bemerkung 7.10

Es gilt mit den obigen Bezeichnungen:

$$(a_1,...,a_n) = (a_1) + ... + (a_n) = \left\{\sum_{i=1}^n r_i a_i \mid r_i \in R,\ i = 1,...,n\right\}.$$

Wir kommen nun zu ggT und kgV zurück:

d ist ein gemeinsamer Teiler von $a_1,...,a_n \in R$ genau dann, wenn für alle i gilt: $(a_i) \subseteq (d)$, also: $(a_1) + ... + (a_n) = (a_1,...,a_n) \subseteq (d)$.

Ist $(a_1,...,a_n) = (d)$ ein Hauptideal, so ist also d ein ggT von $a_1,...,a_n$. Nach der obigen Bemerkung lässt sich d dann als R-Linearkombination von $a_1,...,a_n$ schreiben:

$$d = r_1a_1 + ... + r_na_n.$$

Die hier auftretenden Koeffizienten $r_1,...,r_n$ heißen **Bezout-Koeffizienten**.

v ist ein gemeinsames Vielfaches von $a_1,...,a_n \in R$ genau dann, wenn für alle i gilt: $(a_i) \supseteq \langle v\rangle$, also: $(a_1) \cap .... \cap (a_n) \supseteq \langle v\rangle$.

Hier gilt nun (Beweis!):

v ist ein kgV von $a_1,...,a_n$ genau dann, wenn $\langle v\rangle = (a_1) \cap ... \cap (a_n)$ ist.

Insbesondere muss also das Durchschnittsideal ein Hauptideal sein.

Nach den obigen Überlegungen ist die Existenz von ggT und kgV also gesichert, wenn R ein Hauptidealring ist.

In der Linearen Algebra haben wir bereits gezeigt, dass $\mathbb{Z}$ ein Hauptidealring ist.

Wesentlich für den Beweis dieser Tatsache war die Existenz einer „guten“ Gradfunktion bezüglich der Division mit Rest. Wir erinnern an die Definition der Ringe, in denen eine solche Division mit Rest durchgeführt werden kann:

Definition 7.11

Ein Integritätsring R heißt **euklidischer Ring**, wenn es eine Abbildung

$$\delta : R \setminus \{0\} \to \mathbb{N}_0$$

gibt mit folgender Eigenschaft:

Für $0 \neq a,b \in R$ gibt es stets $q,r \in R$ mit

$$b = qa + r \text{, wobei } \delta\langle r\rangle < \delta\langle a\rangle \text{ oder } r = 0.$$

Eine solche Abbildung heißt eine **(euklidische) Gradfunktion** (oder auch: **Normfunktion**) auf R.

Beispiel 7.12

(i) $R = \mathbb{Z}$ mit der Betragsfunktion als Gradfunktion δ ist ein euklidischer Ring.

(ii) Ist K ein Körper, so ist $R = K[X]$ mit der Abbildung $\delta = \deg$ ein euklidischer Ring.

Allgemein gilt nun:

Satz 7.13

Sei R ein euklidischer Ring mit Gradfunktion δ. Sei $I \neq (0)$ ein Ideal in R. Dann ist $I = (a)$ für $0 \neq a \in I$ mit

$$\delta(a) = \min\{\delta(x) \mid x \in I, x \neq 0\}.$$

Insbesondere ist jeder euklidische Ring ein Hauptidealring.

Beweis

Sei $I \neq (0)$ ein Ideal von R. Sei $0 \neq a \in I$ von minimalem Grad, also $\delta(a) = \min\{\delta(x) \mid x \in I, x \neq 0\}$.

Wir wollen zeigen: $I = (a)$.

Die Inklusion $(a) \subseteq I$ ist klar. Sei also nun $b \in I$. Dann gibt es $q, r \in R$ mit

$$b = qa + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(a).$$

Da aber $r = b - qa \in I$, folgt aus der Definition von a, dass $r = 0$ gelten muss. Also ist $b = qa \in (a)$, und damit ist $I = (a)$ gezeigt. □

Wie schon oben angedeutet, existiert der ggT nicht immer. Insbesondere gibt es also Ringe, die keine Hauptidealringe sind. Die folgenden Beispiele zeigen auch, dass beim Nachweis der Eigenschaften einer Gradfunktion Sorgfalt geboten ist.

Beispiel 7.14

(i) Sei $R = \mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$ der Ring der ganzen Gaußschen Zahlen.

Auf $\mathbb{C}$ haben wir die Abstandsquadrat-Funktion

$$\delta : \mathbb{C} \to \mathbb{R}_{\geq 0},\ x + iy \mapsto x^2 + y^2.$$

Wir schränken δ auf $\mathbb{Z}[i]$ ein und zeigen: R ist mit

$$\delta : R \setminus \{0\} \to \mathbb{N},\ m + in \mapsto m^2 + n^2$$

ein euklidischer Ring.

Seien $z, w \in R \setminus \{0\}$. Dann ist $\frac{z}{w} = a + ib$ für geeignete $a, b \in \mathbb{R}$. Dann gibt es $m, n \in \mathbb{Z}$ mit $|a - m| \leq \frac{1}{2}$, $|b - n| \leq \frac{1}{2}$.

Also folgt:

$$\delta(z - (m + in)w) = \delta\Big(w \cdot \Big(\frac{z}{w} - (m + in)\Big)\Big) = \circledast$$

Nun benutzen wir, dass unsere Funktion δ sogar auf $\mathbb{C}$ definiert ist und auf $\mathbb{C}$ multiplikativ ist, d.h. $\delta(uv) = \delta(u)\delta(v)$ gilt:

$$\circledast = \delta(w)\delta\Big(\frac{z}{w} - (m + in)\Big) = \delta(w)\underbrace{\delta((a - m) + i(b - n))}_{\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}} < \delta(w).$$

Damit ist $z = (m + in)w + (z - (m + in)w)$ mit $m, n \in \mathbb{Z}$ wie oben eine Division mit Rest in R wie erforderlich.

(ii) Sei $R = \mathbb{Z}[\sqrt{-5}]$. Wir schränken wieder die Abstandsquadrat-Funktion δ von oben auf R ein und erhalten diesmal:

$$\delta : R \setminus \{0\} \to \mathbb{N},\ m + i\sqrt{5}n \mapsto m^2 + 5n^2.$$

Da, wie oben bereits angesprochen, die Abbildung δ multiplikativ ist, folgt insbesondere: sind $a, b \in R$ mit $b \mid a$, dann gilt auch $\delta(b) \mid \delta(a)$.

Wir wollen nun untersuchen, ob es zu $a = 6$ und $b = 2(1+\sqrt{-5})$ einen ggT in R gibt. Wir nehmen an, dass d ein solcher ggT sei.
Da wir die folgende Faktorisierung in R haben

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

sind 2 und $1+\sqrt{-5}$ gemeinsame Teiler von a und b, also muss gelten: $2|d$ und $1+\sqrt{-5}|d$, und daher gilt:

$$4|\delta(d) \text{ und } 6|\delta(d), \text{ also: } 12|\delta(d).$$

Andererseits folgt aus $d|6$ und $d|2(1+\sqrt{-5})$:

$$\delta(d)|36 \text{ und } \delta(d)|24.$$

Also ist $\delta(d) = 12$. Aber 12 ist nicht von der Form $m^2 + 5n^2$ für $m, n \in \mathbb{Z}$. Dieser Widerspruch zeigt, dass $a = 6$ und $b = 2(1+\sqrt{-5})$ in R keinen ggT haben.
Insbesondere ist also R kein Hauptidealring und damit erst recht kein euklidischer Ring.

Bemerkung 7.15

In euklidischen Ringen kann der ggT (und auch zugehörige Bezout-Koeffizienten) effizient mit dem euklidischen Algorithmus berechnet werden.

Kapitel 8

Primelemente, irreduzible Elemente und faktorielle Ringe

Bezüglich der Teilbarkeit sind die kleinsten (nichttrivialen) Bausteine in $\mathbb{Z}$ die Primzahlen in $\mathbb{N}$, die dadurch definiert sind, dass sie genau zwei positive Teiler haben, nämlich 1 und sich selbst, d.h., es sind die positiven Zahlen, die sich nur trivial faktorisieren lassen.
Elemente mit dieser Unzerlegbarkeitseigenschaft bezüglich Produkten betrachten wir nun in einem beliebigen Ring R (stets als kommutativ und mit 1 vorausgesetzt):

Definition 8.1
Ein Element $a \in R$ heißt **irreduzibel**, wenn a weder 0 noch eine Einheit in R ist und außerdem gilt:
Sind $u, v \in R$ mit $a = uv$, dann ist u oder v eine Einheit in R.

Bemerkung 8.2
(i) Die irreduziblen Elemente in $\mathbb{Z}$ sind genau die Primzahlen und ihre Negativen.
(ii) Da nach dem Fundamentalsatz der Algebra jedes nichtkonstante Polynom in $\mathbb{C}[X]$ eine Nullstelle in $\mathbb{C}$ hat, sind in $\mathbb{C}$ nur die linearen Polynome $aX + b$, $a \in \mathbb{C}^*$, $b \in \mathbb{C}$ irreduzibel.
(iii) Irreduzible Polynome in $\mathbb{R}[X]$ sind vom Grad 1 oder 2.

Die Primzahlen in $\mathbb{Z}$ haben die Eigenschaft, dass sich jede andere ganze Zahl als Produkt von Primzahlen (und eventuell einem Faktor -1) schreiben lässt. Auch diese Eigenschaft wollen wir uns für den Ring R ansehen. Sie spielte bereits im Rahmen der Linearen Algebra eine Rolle.

Wir sagen, dass ein Element $0 \neq a \in R$ eine Zerlegung in irreduzible Faktoren hat, wenn sich a in der Form

$$a = \varepsilon u_1 u_2 \cdot \ldots \cdot u_r$$

schreiben lässt, wobei $\varepsilon \in R^*$ ist und $u_1, \ldots, u_r$ irreduzible Elemente in R sind (dabei ist der Fall $r = 0$, d.h. $a \in R^*$, zugelassen).
Eine solche Zerlegung nennen wir **eindeutig**, wenn sie bis auf die Reihenfolge der Faktoren und die alternative Wahl assoziierter Faktoren eindeutig ist.

Wann haben Elemente Zerlegungen in irreduzible Elemente? Wir wollen dazu wieder die zugehörigen Ideale betrachten.

Definition 8.3
Eine Folge $(r_n)_{n \in \mathbb{N}}$ in R heißt eine **Teilerkette** in R, wenn für alle $n \in \mathbb{N}$ gilt: $r_{n+1} | r_n$. Äquivalent dazu ist die Eigenschaft, dass die zugehörigen Hauptideale eine aufsteigende Idealkette in R bilden:

$$(r_1) \subseteq (r_2) \subseteq \ldots \subseteq (r_n) \subseteq (r_{n+1}) \subseteq \ldots$$

In R gilt **der Teilerkettensatz für Elemente**, wenn es für jede solche Teilerkette ein n_0 gibt, so dass $r_n \sim r_{n+1}$ für alle $n \geq n_0$ gilt. Für die Idealkette bedeutet dies, dass die Kette ab einem n_0-ten Glied stationär wird, also $(r_n) = (r_{n+1})$ für alle $n \geq n_0$ gilt.

Beispiel 8.4

In $\mathbb{Z}$ gilt der Teilerkettensatz für Elemente.

Satz 8.5 (Euklid)

Gilt in R der Teilerkettensatz für Elemente, dann hat jedes Element in $R \setminus \{0\}$ eine Zerlegung in irreduzible Elemente.

Beweis

Aus dem Teilerkettensatz für Elemente folgt, dass es in jeder nichtleeren Teilmenge $\mathcal{M} \subseteq R$ ein Element gibt, das keinen echten Teiler (d.h. weder Einheit noch assoziiert) in $\mathcal{M}$ hat (sonst könnten wir ja eine unendliche echte Teilerkette in R konstruieren).

Wir betrachten nun die Menge

$$\mathcal{M} = \{r \in R \setminus \{0\} \mid r \text{ hat keine Zerlegung in irreduzible Elemente}\}$$

und haben zu zeigen, dass $\mathcal{M}$ leer ist.

Falls nicht, so gibt es nach der vorstehenden Beobachtung ein Element $r \in \mathcal{M}$, das keine echten Teiler in $\mathcal{M}$ hat. Nach Definition von $\mathcal{M}$ ist r nicht irreduzibel, hat also eine Faktorisierung $r = uv$ mit echten Teilern $u, v \in R$. Da $u, v \notin \mathcal{M}$, haben u und v Zerlegungen in irreduzible Elemente. Dann liefern diese Zerlegungen aber auch eine Zerlegung von r in irreduzible Elemente. □

Bevor wir die Eindeutigkeit dieser Zerlegung genauer untersuchen, brauchen wir noch einen weiteren Begriff. Die Primzahlen in $\mathbb{Z}$ lassen sich auch durch eine weitere Eigenschaft definieren: teilt eine Primzahl ein Produkt, dann teilt sie bereits einen der Faktoren (dies ist eine nichttriviale Eigenschaft der Primzahlen!).

Wir definieren allgemein:

Definition 8.6

Ein Element $a \in R \setminus \{0\}$, das keine Einheit ist, heißt **Primelement** in R, wenn gilt:

Sind $u, v \in R$ mit $a \mid uv$, dann folgt $a \mid u$ oder $a \mid v$.

Bemerkung 8.7

Jedes Primelement eines Integritätsrings ist irreduzibel.

Beispiel 8.8

Die Primelemente in $\mathbb{Z}$ sind die Zahlen $\pm p$, $p \in \mathbb{N}$ Primzahl.

Analog zur Sprechweise für Zerlegungen von Elementen in irreduzible Faktoren sprechen wir auch von der Zerlegung von Elementen in Primelemente.

Lemma 8.9

Sei R ein Integritätsring. Hat ein Element $a \in R \setminus \{0\}$ eine Zerlegung in Primelemente, dann ist die Zerlegung in Primelemente eindeutig.

Die Frage ist also, wann jedes Element eine Zerlegung in Primelemente hat; auch mit diesem Thema hatten wir uns schon etwas in der Linearen Algebra beschäftigt.

Definition 8.10

Ein Integritätsring R heißt **faktoriell** (oder **ZPE-Ring**), wenn jedes $a \in R \setminus \{0\}$ eine (eindeutige) Zerlegung in Primelemente hat.

Beispiel 8.11

$\mathbb{Z}$ ist ein faktorieller Ring.

Die Eigenschaft der Primzahlen, nicht nur irreduzibel, sondern sogar Primelement zu sein, gilt für irreduzible Elemente in allen faktoriellen Ringen, außerdem gilt dann die Eindeutigkeit der Zerlegung in irreduzible Elemente:

Satz 8.12

Sei R ein Integritätsring, in dem jedes Element $0 \neq a \in R$ eine Zerlegung in irreduzible Elemente hat. Dann sind äquivalent:

(i) Jedes Element in $R \setminus \{0\}$ hat eine eindeutige Zerlegung in irreduzible Elemente.

(ii) Jedes irreduzible Element in R ist ein Primelement in R.

(iii) Der Ring R ist faktoriell.

Beweis

Sei zunächst (i) vorausgesetzt. Sei $a \in R$ irreduzibel, und seien $u, v \in R$ mit $a \mid uv$, also $uv = ab$ für ein $b \in R$. Dann besitzen u, v, b Zerlegungen in irreduzible Elemente, etwa

$$u = \varepsilon u_1 u_2 \cdot \ldots \cdot u_r\,,\ v = \varepsilon' v_1 v_2 \cdot \ldots \cdot v_s\,,\ b = \varepsilon'' b_1 b_2 \cdot \ldots \cdot b_t$$

mit Einheiten $\varepsilon, \varepsilon', \varepsilon''$ und irreduziblen Elementen u_i, v_j, b_k. Dann gilt

$$\varepsilon u_1 u_2 \cdot \ldots \cdot u_r \varepsilon' v_1 v_2 \cdot \ldots \cdot v_s = a \varepsilon'' b_1 b_2 \cdot \ldots \cdot b_t\,.$$

Aufgrund der Eindeutigkeit der Zerlegung gilt dann o.E. $a \sim u_i$ für ein i und damit folgt $a \mid u$.

Sei nun (ii) angenommen, also dass jedes irreduzible Element in R ein Primelement ist. Dann hat nach Definition jedes Element eine Zerlegung in Primelemente, also ist R faktoriell.

Sei nun (iii) gegeben, also R als faktoriell vorausgesetzt, und wir wollen (i) zeigen.

Ist $a \in R^*$, dann ist die triviale Zerlegung von a die eindeutige Zerlegung von a. Wir beweisen die Behauptung nun durch Induktion über die Länge der Zerlegung in Primelemente. Seien also

$$a = \varepsilon u_1 u_2 \cdot \ldots \cdot u_r = \varepsilon' v_1 v_2 \cdot \ldots \cdot v_s$$

mit $\varepsilon, \varepsilon' \in R^*$, die u_i Primelemente und die v_j irreduzible Elemente. Da $u_r \mid a = \varepsilon' v_1 v_2 \cdot \ldots \cdot v_s$ und u_r ein Primelement ist, folgt, dass $u_r \mid v_i$ für ein i, o.E. ist $i = s$. Da v_s irreduzibel ist, muss dann aber $u_r \sim v_s$ gelten. Nach Division durch u_r erhalten wir also

$$a' = \varepsilon u_1 u_2 \cdot \ldots \cdot u_{r-1} = \varepsilon'' v_1 v_2 \cdot \ldots \cdot v_{s-1}\,,$$

wobei $\varepsilon'' \in R^*$. Nach Induktionsannahme ist die Zerlegung von a' eindeutig, also folgt die Behauptung. □

Beispiel 8.13

Der bereits früher untersuchte Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell! Wir zeigen dies, indem wir irreduzible Elemente finden, die keine Primelemente sind.

Die Einheiten in R sind mit Hilfe der früher bereits benutzten Gradfunktion δ leicht zu ermitteln. Es ist:

$$R^* = \{1, -1\} = \{\, x \in R \mid \delta(x) = 1 \,\}\,.$$

Wir betrachten nun wieder die Faktorisierung

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Es ist $\delta(2) = 4$, also muss für jeden Teiler a von 2 in R gelten: $\delta(a) | 4$. Für jeden echten Teiler a von 2 folgt dann bereits: $\delta(a) = 2$. Da $\delta(a) = 2$ aber nicht möglich ist, folgt, dass 2 irreduzibel in R ist.
Da $\delta(1+\sqrt{-5}) = \delta(1-\sqrt{-5}) = 6$ ist, folgt aber: $2 \nmid 1 \pm \sqrt{-5}$. Also ist 2 kein Primelement in R.
Ganz entsprechend ergibt sich, dass 3 und $1 \pm \sqrt{-5}$ irreduzible Elemente sind, die keine Primelemente sind. Die beiden angegebenen Faktorisierungen von 6 sind also zwei wesentlich verschiedene Zerlegungen von 6 in irreduzible Faktoren. Insbesondere hat 6 im Ring R **keine** Zerlegung in Primelemente.

Aus den vorhergehenden Sätzen erhalten wir nun folgende Charakterisierung faktorieller Ringe:

Satz 8.14

Sei R ein Integritätsring. Dann sind äquivalent:
(i) R ist faktoriell.
(ii) In R gilt der Teilerkettensatz für Elemente, und jedes irreduzible Element in R ist ein Primelement.

Beweis
Die Richtung (ii) $\Rightarrow$ (i) folgt aus Satz 8.5 und Satz 8.12.
Sei nun vorausgesetzt, dass R faktoriell ist. Dann ist die Voraussetzung von Satz 8.12 erfüllt, und damit ist jedes irreduzible Element ein Primelement in R. Wegen der Eindeutigkeit der Zerlegung in Primelemente sind die Teiler eines Elementes $0 \neq a \in R$ leicht anzugeben. Ist

$$a = \varepsilon u_1 u_2 \cdot \ldots \cdot u_r$$

mit $\varepsilon \in R^*$ und Primelementen u_i, dann sind die Teiler von a von der Form

$$\varepsilon' u_{i_1} u_{i_2} \cdot \ldots \cdot u_{i_s} \text{ mit } \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}$$

Also gibt es – bis auf Assoziiertheit – nur endlich viele echte Teiler von a, und daher wird jede Teilerkette – bis auf Assoziiertheit – stationär. □

Wir können damit nun eine große Klasse von Ringen als faktoriell nachweisen:

Satz 8.15

Sei R ein Integritätsring. Ist R ein Hauptidealring, dann ist R faktoriell.

Beweis
Wir verwenden das oben bewiesene Kriterium. Sei

$$(r_1) \subseteq (r_2) \subseteq \ldots \subseteq (r_n) \subseteq (r_{n+1}) \subseteq \ldots$$

eine Kette von Hauptidealen in R. Dann ist $I = \bigcup_{i \geq 1} (r_i)$ ein Ideal in R, also ist $I = (a)$ für ein $a \in R$.
Aus $a \in I$ folgt $a \in (r_{n_0})$ für ein $n_0 \in \mathbb{N}$, also $(a) \subseteq (r_{n_0}) \subseteq I = (a)$ und damit $(r_{n_0}) = (a) = (r_n)$ für alle $n \geq n_0$, d.h. die Kette wird bei n_0 stationär.
Sei $x \in R$ irreduzibel, und seien $u, v \in R$ mit $x | uv$. Gilt $x \nmid u$, dann sind x und u teilerfremd (da x irreduzibel ist!), also existieren $s, t \in R$ mit $1 = xs + ut$. Dann folgt

$$v = xsv + uvt,$$

und damit $x | v$. Also ist x ein Primelement in R. □

Bemerkung 8.16

(i) Die Umkehrung gilt nicht! Wir werden später sehen, dass $\mathbb{Z}[X]$ ein faktorieller Ring ist, aber $\mathbb{Z}[X]$ ist kein Hauptidealring.
(ii) Alle euklidischen Ringe sind faktoriell.

Im Ring $\mathbb{Z}$ wird für jedes Element üblicherweise eine „Standardzerlegung“ der Form

$$a = \pm\prod_{i=1}^{r} p_i^{r_i}$$

angegeben, wobei $p_1,...,p_r$ die verschiedenen Primzahlen sind, die a teilen, und $r_i \in \mathbb{N}$, $i = 1,...,r$. Diese Zerlegung ist die **Primfaktorzerlegung** von a in $\mathbb{Z}$.

Eine solche Zerlegung wollen wir für Elemente in einem beliebigen **faktoriellen** Ring R angeben. Dazu wählen wir ein **(vollständiges) Repräsentantensystem $\mathcal{P}$ für die Assoziiertenklassen von Primelementen in R** (beachte: eine solche Wahl ist nach dem Auswahlaxiom möglich!). Für $R = \mathbb{Z}$ würden wir also z.B. $\mathcal{P}$ als die Menge der Primzahlen wählen.

Dann gilt:

Jedes $a \in R \setminus \{0\}$ hat eine eindeutige Darstellung der Form

$$a = \varepsilon \prod_{p\in\mathcal{P}} p^{\nu_p}$$

mit $\varepsilon \in R^*$ und $\nu_p \in \mathbb{N}_0$, wobei nur endlich viele ν_p von 0 verschieden sind.

Diese Zerlegung heißt dann die **normierte Primelementzerlegung zum Repräsentantensystem $\mathcal{P}$**. Der Exponent $\nu_p(a)$ heißt die **Ordnung von a an der Stelle p**.

Die Funktion $\nu_p : R \setminus \{0\} \to \mathbb{N}_0$ heißt **Ordnungsfunktion an der Stelle** p oder auch zu p **gehörende Exponentialbewertung**.

Bemerkung 8.17

Es gilt auch die Umkehrung: ist die obige Eigenschaft gegeben, dann ist R ein faktorieller Ring und $\mathbb{P}$ ein Repräsentantensystem für die Assoziiertenklassen von Primelementen in R.

Wir betrachten die Abbildungen ν_p, $p \in \mathcal{P}$ noch etwas genauer. Die folgenden Eigenschaften sind leicht nachzuweisen:

Bemerkung 8.18

Seien $a,b \in R \setminus \{0\}$.

(i) $a|b \iff \nu_p(a) \le \nu_p(b)$ für alle $p \in \mathcal{P}$.

(ii) $\#\{\text{Assoziiertenklassen von Teilern von } a\} = \prod_{p\in\mathcal{P}}(1+\nu_p(a))$.

(iii) Es ist $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(iv) Ist $a+b \neq 0$, dann ist $\nu_p(a+b) \ge \min\{\nu_p(a),\nu_p(b)\}$,
und falls $\nu_p(a) < \nu_p(b)$, so ist $\nu_p(a+b) = \nu_p(a)$.

Bei gegebenen Zerlegungen in Primelemente lassen sich ggT und kgV sofort angeben:

Satz 8.19

Sei R ein faktorieller Ring, $\mathcal{P}$ wie oben.

Dann existieren zu beliebigen Elementen $a_1,...,a_n \in R \setminus \{0\}$ stets ihr ggT und kgV, und es gilt

$$\mathrm{ggT}(a_1,...,a_n) \sim \prod_{p\in\mathcal{P}} p^{\min\{\nu_p(a_1),...,\nu_p(a_n)\}}$$

$$\mathrm{kgV}(a_1,...,a_n) \sim \prod_{p\in\mathcal{P}} p^{\max\{\nu_p(a_1),...,\nu_p(a_n)\}}$$

Bemerkung 8.20

Sind $a,b \in R$, so gilt

$$a \cdot b \sim \mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b).$$

Für einen faktoriellen Ring R können wir seinen Quotientenkörper $K = Q(R)$ bilden. Dann lässt sich die Abbildung ν_p, $p \in \mathcal{P}$ fortsetzen zu einer Abbildung, die wir mit demselben Namen bezeichnen:

$$\nu_p : K \to \mathbb{Z} \cup \{\infty\},$$

wobei wir $\nu_p(0) = \infty$ setzen und für $a,b \in R \setminus \{0\}$ definieren:

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b).$$

(Beachte, dass aufgrund von Eigenschaft (iii) diese Setzung wohl definiert ist!)

Bemerkung 8.21

Es gelten folgende Eigenschaften:

(i) Jedes $a \in K^*$ hat eine (eindeutige) Darstellung

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p}$$

mit $\varepsilon \in R^*$ und $\nu_p \in \mathbb{Z}$, wobei nur endlich viele ν_p von 0 verschieden sind.

(ii) Sei $a \in K^*$. Dann ist $a \in R \setminus \{0\}$ genau dann, wenn $\nu_p(a) \geq 0$ für alle $p \in \mathcal{P}$.

Kapitel 9

Primideale und maximale Ideale

Was bedeuten die Elementeigenschaften irreduzibel und Primelement idealtheoretisch und wie lassen sie sich sinnvoll für Ringe verallgemeinern, in denen keine Zerlegung in irreduzible Elemente bzw. Primelemente gegeben ist? Wir beginnen zunächst mit einigen allgemeinen ringtheoretischen Eigenschaften.

Definition 9.1

Sei R ein (nicht notwendig kommutativer) Ring. Dann heißt R **einfach**, wenn R nur die beiden trivialen Ideale (0) und $R(\neq (0))$ hat.

Beispiel 9.2

(i) Jeder Körper ist ein einfacher Ring (enthält ein Ideal eine Einheit, so ist es bereits gleich dem ganzen Ring!).

(ii) Der Matrizenring $M_n(K)$, K ein Körper, $n \in \mathbb{N}$, ist einfach (Übung).

Satz 9.3

Sei R ein kommutativer Ring mit 1. Dann ist R genau dann einfach, wenn R ein Körper ist.

Beweis

Sei R ein einfacher Ring, und sei $a \in R \setminus \{0\}$. Dann ist $(a) \neq (0)$, also muss nach Definition $(a) = R$ gelten. Wegen $1 \in (a) = Ra$ gibt es also $b \in R$ mit $1 = ab$, also ist a invertierbar.

Die Definition von „einfach“ sagt, dass es oberhalb des Nullideals nur das triviale Ideal R gibt. Dies wollen wir nun zu einer „relativen“ Definition verallgemeinern:

Definition 9.4

Ein Ideal I von R heißt **maximales Ideal** von R, wenn $I \neq R$ ist und es kein Ideal I' mit $I \subset I' \subset R$ gibt.

Beispiel 9.5

Ist $p \in \mathbb{N}$ eine Primzahl, dann ist $p\mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$. Sei etwa I ein Ideal von $\mathbb{Z}$ mit $p\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, ist $I = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$, wobei wir sogar $n \in \mathbb{N}$ annehmen können. Also folgt $p = nt$ für ein $t \in \mathbb{Z}$. Da p eine Primzahl ist, folgt dann $n = 1$ oder $n = p$, also ist $I = \mathbb{Z}$ oder $I = p\mathbb{Z}$.

Ist $n \in \mathbb{N} \setminus \{1\}$ keine Primzahl, also etwa $n = ab$ mit $a,b \in \mathbb{N} \setminus \{1\}$, dann ist $n\mathbb{Z}$ kein maximales Ideal, da $n\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$.

Die obige Definition verallgemeinert die vorhergehende in folgendem Sinn: Herausfaktorisieren eines maximalen Ideals liefert einen einfachen Ring. Wir zeigen dazu eine allgemeinere Beziehung:

Satz 9.6

Sei R ein Ring, I ein Ideal von R, $\pi : R \to R/I$ der kanonische Restklassenepimorphismus. Dann induziert π eine Bijektion

$$\Phi : \{I' \mid I' \text{ Ideal von } R,\ I \subseteq I'\} \to \{J \mid J \text{ Ideal von } R/I\},\ I' \mapsto \pi(I').$$

Beweis

Surjektive Homomorphismen bilden stets Ideale auf Ideale ab! Die additiven Eigenschaften sind klar, zu zeigen ist nur: ist $b \in \pi(I')$, $t \in \pi(R) = R/I$, dann ist $bt \in \pi(I')$ (bzw. $tb \in \pi(I')$). Seien $a \in I'$, $r \in R$ mit $b = \pi(a)$, $t = \pi(r)$. Dann ist $ar \in I'$, da I' ein Ideal von R ist und daher $bt = \pi(a)\pi(r) = \pi(ar) \in \pi(I')$ (analog für tb).

Also ist die angegebene Abbildung Φ wohl definiert.

Wir zeigen die Bijektivität, indem wir die Umkehrabbildung angeben. Sei

$$\Psi : \{J \mid J \text{ Ideal von } R/I\} \to \{I' \mid I' \text{ Ideal von } R,\ I \subseteq I'\},\ J \mapsto \pi^{-1}(J).$$

Da $0 \in J$ für jedes Ideal J von R/I, ist $I = \pi^{-1}(0) \subseteq \pi^{-1}(J)$. Außerdem sind Urbilder von Idealen unter Homomorphismen stets wieder Ideale (Übung). Also ist Ψ wohl definiert.

Die Beziehung $\Phi\Psi(J) = \pi\pi^{-1}(J) = J$ gilt für jede Teilmenge $J \subseteq R/I$, da π surjektiv ist.

Andererseits gilt

$$\begin{aligned}\Psi\Phi(I') = \pi^{-1}\pi(I') &= \{x \in R \mid \pi(x) \in \pi(I')\}\\ &= \{x \in R \mid \exists a \in I' : \pi(x) = \pi(a)\}\\ &= \{x \in R \mid \exists a \in I' : x - a \in I\}\\ &= I',\end{aligned}$$

wobei die letzte Beziehung daraus folgt, dass $I \subseteq I'$.

Also haben wir insgesamt die Bijektivität gezeigt. □

Folgerung 9.7

Sei R ein Ring, I Ideal von R.

Dann ist I genau dann ein maximales Ideal von R, wenn R/I ein einfacher Ring ist.

Ist R ein kommutativer Ring mit 1, so ist also I ein maximales Ideal genau dann, wenn R/I ein Körper ist.

Folgerung 9.8

Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beispiel 9.9

(i) Sei $R = \mathcal{C}(\mathbb{R})$ die Menge der stetigen Funktionen auf $\mathbb{R}$. Dann ist R bezüglich der punktweisen Addition und Multiplikation von Funktionen ein Ring. Definiere für $a \in \mathbb{R}$:

$$\varphi_a : \mathcal{C}(\mathbb{R}) \to \mathbb{R},\ f \mapsto f(a).$$

Dann ist φ_a offenbar ein Epimorphismus mit $\operatorname{Kern}\varphi_a = I_a = \{f \in R \mid f(a) = 0\}$. Also gilt nach dem Homomorphiesatz: $R/I_a \cong \mathbb{R}$, d.h. der Faktorring nach I_a ist ein Körper, und damit ist I_a ein maximales Ideal in R.

(ii) Es gilt $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$, also ist (X^2+1) ein maximales Ideal in $\mathbb{R}[X]$.

Wir wissen bereits, dass X^2+1 irreduzibel in $\mathbb{R}[X]$ ist (dieses Polynom hat keine Nullstelle in $\mathbb{R}$). Wir wollen nun das Beispiel (ii) oben verallgemeinern und die Eigenschaft „irreduzibel“ idealtheoretisch fassen:

Satz 9.10

Sei R ein Integritätsring. Sei $p \in R$, $p \neq 0$ und $p \notin R^*$. Dann ist p irreduzibel in R genau dann, wenn aus $(p) \subset (a) \subseteq R$ mit $a \in R$ stets $(a) = R$, d.h. $a \in R^*$ folgt.
Ist R außerdem ein Hauptidealring, so ist also p irreduzibel in R genau dann, wenn (p) ein maximales Ideal in R ist.

Beweis

Sei $p \in R$ irreduzibel, und sei $a \in R$ mit $(p) \subseteq (a)$. Dann gibt es $x \in R$ mit $p = ax$. Da p irreduzibel ist, folgt dann $a \in R^*$, d.h. $(a) = R$ oder $(p) = (a)$.
Wir nehmen nun an, dass die Idealbedingung für (p) erfüllt sei. Sei $p = ab$ mit $a,b \in R$, o.E. sei $b \notin R^*$. Dann ist $(p) \subset (a) \subseteq R$, also folgt $a \in R^*$.
Die letzte Aussage folgt unmittelbar. □

Wir wollen nun auch die Eigenschaft „Primelement“ idealtheoretisch formulieren bzw. verallgemeinern. Zunächst brauchen wir noch den Begriff des Produktes von Idealen:

Definition 9.11

Sei R ein Ring, und seien A,B Ideale in R. Dann ist das Produkt von A und B definiert als das Ideal

$$AB = \left(\left\{ab \mid a \in A,\, b \in B\right\}\right).$$

Definition 9.12

Sei R ein Ring, $P \subset R$ ein Ideal von R.
Das Ideal P heißt **Primideal** von R, wenn gilt:
Sind A,B Ideale von R mit $AB \subseteq P$, dann ist $A \subseteq P$ oder $B \subseteq P$.

Bemerkung 9.13

Erfüllt das Ideal P von R die Bedingung:

$$\circledast \text{ Sind } a,b \in R \text{ mit } ab \in P, \text{ dann ist } a \in P \text{ oder } b \in P.$$

Dann heißt P auch ein **vollprimes Ideal** von R.
Vollprime Ideale sind stets Primideale:
Sei P vollprim in R, und seien A,B Ideale von R mit $AB \subseteq P$. Ist $A \not\subseteq P$, dann gibt es $a \in A$, $a \notin P$. Da $ab \in aB \subseteq P$ für alle $b \in B$, folgt dann $B \subseteq P$.
Ist R ein kommutativer Ring mit 1, dann ist auch umgekehrt jedes Primideal vollprim:
Sei P ein Primideal in R, und seien $a,b \in R$ mit $ab \in P$. Dann ist $(a)(b) = RaRb = Rab \subseteq P$, also folgt $(a) \subseteq P$ oder $(b) \subseteq P$, und damit ist $a \in P$ oder $b \in P$.
Wir können also in diesen Ringen auch mit der Elementbedingung $\circledast$ statt mit der Idealbedingung für Primideale arbeiten.

Beispiel 9.14

(i) Ein Ring R ist genau dann nullteilerfrei, wenn (0) ein vollprimes Ideal in R ist. Ein kommutativer Ring R ist also genau dann nullteilerfrei, wenn (0) ein Primideal von R ist.
Insbesondere ist (0) ein Primideal von $\mathbb{Z}$.

(ii) Ist p eine Primzahl, dann ist $p\mathbb{Z}$ ein Primideal in $\mathbb{Z}$.

Satz 9.15

Sei R ein kommutativer Ring mit 1, $I \subset R$ ein Ideal in R. Dann ist I genau dann ein Primideal, wenn R/I ein Integritätsring ist.

Beweis
Dies folgt aus den vorhergehenden Bemerkungen und der Multiplikation in R/I: $(a+I)(b+I) = ab+I$. □

Folgerung 9.16
Sei R ein kommutativer Ring mit 1. Dann ist jedes maximale Ideal von R ein Primideal.

Satz 9.17
Sei R ein Integritätsring, $p \in R$. Dann ist p ein Primelement von R genau dann, wenn $(p) \neq (0)$ und (p) ein Primideal von R ist.
Beweis
Sei $p \in R$ ein Primelement. Dann ist nach Definition $(p) \neq (0)$ und $(p) \neq R$. Sei nun $ab \in (p)$ für $a,b \in R$. Dann ist $ab = px$ für ein $x \in R$, und da p ein Primelement ist, folgt dann $p|a$ oder $p|b$, also $a \in (p)$ oder $b \in (p)$, und daher ist (p) ein Primideal von R .
Ist umgekehrt $(p) \neq (0)$ ein Primideal, dann ist $p \neq 0$ und $p \notin R^*$. Sind $a,b \in R$ mit $p|ab$, dann ist $ab \in (p)$, also $a \in (p)$ oder $b \in (p)$, und damit gilt $p|a$ oder $p|b$. □

Wir wollen noch einen Satz über die Existenz maximaler Ideale beweisen. Dazu müssen wir zunächst einiges bereitstellen bzw. wollen an einige Definitionen erinnern.

Definition 9.18
Eine Relation $\leq$ auf einer Menge X heißt eine **Halbordnung** auf X , wenn gilt:
(i) Für alle $x \in X$ gilt: $x \leq x$.
(ii) Für $x,y \in X$ folgt aus $x \leq y$ und $y \leq x$ stets $x = y$.
(iii) Für $x,y,z \in X$ folgt aus $x \leq y$ und $y \leq z$ stets $x \leq z$.
Eine Teilmenge $A \neq \emptyset$ von X heißt eine **Kette** (bzgl. $\leq$), wenn für je zwei Elemente $x,y \in A$ stets $x \leq y$ oder $y \leq x$ gilt.
Die Halbordnung $\leq$ heißt eine **Ordnung**, wenn X selbst eine Kette bzgl. $\leq$ ist.

Beispiel 9.19
(i) Die übliche $\leq$-Relation auf $\mathbb{R}$ ist eine Ordnung auf $\mathbb{R}$.
(ii) Für jede Menge X ist die Inklusionsrelation eine Halbordnung auf $\mathfrak{P}(X)$.
(iii) Die Teilbarkeitsrelation ist eine Halbordnung auf $\mathbb{N}$.

Definition 9.20
Sei X eine Menge mit einer Halbordnung $\leq$. Sei $A \subseteq X$. Ein Element $s \in X$ heißt **obere** (bzw. **untere**) **Schranke von** A , wenn für alle $a \in A$ gilt: $a \leq s$ (bzw. $s \leq a$).
Ein Element $t \in A$ heißt **größtes** (**kleinstes**) **Element von** A , wenn t obere (untere) Schranke von A ist.
Ein Element $m \in A$ heißt **maximales** (**minimales**) **Element von** A , wenn es kein $a \in A$, $a \neq m$ mit $m \leq a$ ($a \leq m$) gibt.
Die Menge X heißt **induktiv geordnet** (**bzgl.** $\leq$), wenn jede Kette in X eine obere Schranke in X besitzt.

Wir brauchen nun folgende Aussage, die äquivalent zum Auswahlaxiom ist:

Lemma 9.21 (Zornsches Lemma)
Jede nichtleere induktiv geordnete Menge besitzt ein maximales Element.

Satz 9.22
Sei R ein Ring mit 1, $I \neq R$ ein Ideal von R. Dann gibt es ein maximales Ideal m von R mit $I \subseteq m$. Insbesondere hat R ein maximales Ideal.

Beweis
Sei

$$X = \{ J \trianglelefteq R \mid I \subseteq J \subset R \}.$$

Dann ist $I \in X$, also X nichtleer, und die Inklusionsrelation $\subseteq$ ist eine Halbordnung auf X. Die maximalen Elemente bezüglich $\subseteq$ in X sind genau die gesuchten maximalen Ideale von R, die I enthalten.
Wir haben zu zeigen: X ist induktiv geordnet.
Sei $\mathcal{K} \neq \emptyset$ eine Kette in X. Setze

$$s(\mathcal{K}) = \bigcup_{B \in \mathcal{K}} B.$$

Wir wollen zeigen, dass $s(\mathcal{K})$ eine obere Schranke zu $\mathcal{K}$ in X ist.
Nach Konstruktion ist $B \subseteq s(\mathcal{K})$ für alle $B \in \mathcal{K}$.
Wir zeigen nun, dass die Menge $s(\mathcal{K})$ ein Ideal ist. Sind $x, y \in s(\mathcal{K})$, dann ist $x \in B_x$, $y \in B_y$ für geeignete $B_x, B_y \in \mathcal{K}$. Da $\mathcal{K}$ eine Kette ist, ist $B_x \subseteq B_y$ oder $B_y \subseteq B_x$, und damit jedenfalls $B_x \cup B_y$ ein Ideal, das in $s(\mathcal{K})$ enthalten ist. Also ist $x + y \in s(\mathcal{K})$. Außerdem ist für alle $a \in R$ auch $ax, xa \in B_x \subseteq s(\mathcal{K})$.
Zuletzt müssen wir noch $s(\mathcal{K}) \neq R$ zeigen. Wäre $s(\mathcal{K}) = R$, dann wäre $1 \in B$ für ein geeignetes $B \in \mathcal{K}$. Dann folgt aber $B = R$ im Widerspruch zu $B \in \mathcal{K} \subseteq X$.
Also ist tatsächlich $s(\mathcal{K})$ eine obere Schranke zu $\mathcal{K}$ in X.
Nach dem Zornschen Lemma existiert daher ein maximales Element $m \in X$ und damit ein maximales Ideal m von R, das I enthält. □

Die Ringe $\mathbb{Z}$ und $\mathcal{C}(\mathbb{R})$ haben, wie wir oben gesehen haben, „viele“ maximale Ideale. Insbesondere im Kontext der Algebraischen Geometrie werden oft Ringe betrachtet, die nur ein einziges maximales Ideal haben, das dann einem „Punkt“ in einer geometrischen Situation entspricht.

Definition 9.23
Ein kommutativer Ring mit 1, der genau ein maximales Ideal besitzt, heißt **lokaler Ring**.

Beispiel 9.24

(i) Sei $p \in \mathbb{N}$ eine Primzahl, $k \in \mathbb{N}$. Dann ist der Ring $\mathbb{Z}_{p^k}$ ein lokaler Ring mit maximalem Ideal $p\mathbb{Z}_{p^k} = {}^{p\mathbb{Z}}\!/_{p^k\mathbb{Z}}$.

(ii) Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \nmid b \right\} \subset \mathbb{Q}$$

ein lokaler Ring mit maximalem Ideal

$$p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \mid a,\ p \nmid b \right\}.$$

Das maximale Ideal in einem lokalen Ring lässt sich einfach beschreiben. Gleichzeitig liefert dies ein Kriterium für lokale Ringe:

Satz 9.25

Sei R ein kommutativer Ring mit 1. Dann ist R genau dann lokal, wenn $R \setminus R^*$ ein Ideal von R ist (und in diesem Fall ist es das maximale Ideal von R).

Beweis

Sei zunächst R als lokal angenommen, mit maximalem Ideal m.

Ist $a \in R \setminus R^*$, dann ist $Ra \subset R$, also folgt nach Satz 9.22 $a \in Ra \subseteq m$. Also ist $R \setminus R^* \subseteq m \subseteq R \setminus R^*$, und daher $m = R \setminus R^*$ ein Ideal von R.

Ist umgekehrt $R \setminus R^*$ ein Ideal, dann muss es maximal sein, da für jedes echte Ideal $I \subset RI \subseteq R \setminus R^*$ gilt. Außerdem ist es aus demselben Grund das einzige maximale Ideal. □

Kapitel 10

Faktorisierung in Polynomringen

Wir hatten uns bereits früher überlegt, dass die geometrischen Konstruktionsprobleme dazu führen, dass wir für komplexe Zahlen ihre Minimalpolynome über $\mathbb{Q}$ bzw. über Erweiterungskörpern von $\mathbb{Q}$ bestimmen müssen (zumindest ihre Grade). Oft ist ein Polynom bekannt, das das vorgegebene Element als Nullstelle hat, so dass wir die Frage nach der Faktorisierung dieses Polynoms bzw. seiner Irreduzibilität zu beantworten haben. In den vorhergehenden Paragraphen haben wir gesehen, dass in allgemeinen kommutativen Ringen Faktorisierungen in irreduzible Elemente durchaus nicht eindeutig sein müssen. Wir wollen also zunächst die Frage klären, wann ein Polynomring ein faktorieller Ring ist.

Unser Koeffizientenring R sei im Folgenden stets ein Integritätsring. Insbesondere ist dann also $R[X]$ auch ein Integritätsring.

Wir haben bereits gezeigt, dass jeder nullteilerfreie Hauptidealring faktoriell ist. Wir untersuchen nun zunächst, welche Polynomringe $R[X]$ Hauptidealringe bzw. sogar euklidische Ringe sind.

Satz 10.1

Sei R ein Integritätsring. Dann sind die folgenden Aussagen äquivalent:
(i) $R[X]$ ist mit der Gradfunktion $\deg$ ein euklidischer Ring.
(ii) $R[X]$ ist ein Hauptidealring.
(iii) R ist ein Körper.

Beweis

Die Implikationen (i)$\Rightarrow$(ii) und (iii)$\Rightarrow$(i) haben wir bereits gezeigt.
(ii)$\Rightarrow$(iii): Sei $R[X]$ ein Hauptidealring, und sei $a \in R \setminus \{0\}$. Offenbar sind a und X teilerfremd in $R[X]$. Also gibt es $f, g \in R[X]$ mit $1 = af + Xg$. Koeffizientenvergleich liefert dann sofort $1 = ac_0$, wobei c_0 das konstante Glied von f ist. Also ist a eine Einheit in R. □

Mit Satz 8.15 folgt daraus unmittelbar:

Folgerung 10.2

Ist K ein Körper, so ist $K[X]$ ein faktorieller Ring.

In $K[X]$ können wir also jedes Polynom eindeutig in irreduzible Faktoren bzw. Primelemente in $K[X]$ zerlegen.
Welche Polynomringe können überhaupt nur faktoriell sein? Wir zeigen zunächst:

Satz 10.3

Sei R ein Integritätsring. Sei $a \in R$. Dann ist a Primelement in R genau dann, wenn a Primelement in $R[X]$ ist.

Beweis
O.E. ist $a \neq 0$. Wir betrachten den vom Restklassenhomomorphismus $\pi : R \to R/\langle a \rangle$ induzierten Ringhomomorphismus:

$$\varphi : R[X] \to R/\langle a \rangle [X], \sum_i c_i X^i \mapsto \sum_i \pi(c_i) X^i .$$

Dann ist φ offenbar surjektiv, und es ist $\operatorname{Kern} \varphi = aR[X]$, das von a in $R[X]$ erzeugte Hauptideal. Also ist nach dem Homomorphiesatz

$$R[X]/aR[X] \cong R/\langle a \rangle [X].$$

Nun ist a prim in R genau dann, wenn $\langle a \rangle$ ein Primideal von R ist, also genau dann, wenn $R/\langle a \rangle$ ein Integritätsring ist. Dies ist aber äquivalent damit, dass $R/\langle a \rangle [X]$ ein Integritätsring ist. Die letzte Aussage gilt genau dann, wenn $aR[X]$ ein Primideal von $R[X]$ ist, also genau dann, wenn a ein Primelement in $R[X]$ ist. □

Zu unserer obigen Frage finden wir zunächst folgende notwendige Bedingung:

Satz 10.4

Ist $R[X]$ ein faktorieller Ring, so ist auch R ein faktorieller Ring.
Beweis
Wir wollen das Kriterium in Satz 8.14 verwenden. Jede Teilerkette in R ist offenbar auch eine Teilerkette in $R[X]$, wird also stationär bis auf Einheiten. Wegen $R[X]^* = R^*$ folgt damit, dass in R der Teilerkettensatz gilt. Ist $a \in R$ irreduzibel, so ist a auch irreduzibel in $R[X]$. Also ist a prim in $R[X]$ und damit nach dem vorhergehenden Satz auch in R. Also erfüllt R das Kriterium in Satz 8.14 und ist damit faktoriell. □

Unser nächstes größeres Ziel ist es, die Umkehrung des obigen Satzes zu beweisen.

Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Ist $\mathcal{P}(R)$ ein Repräsentantensystem für die Assoziiertenklassen von Primelementen von R, dann ist diese Menge nach dem obigen Resultat Teilmenge eines geeigneten Repräsentantensystems $\mathcal{P}(R[X])$ für die Assoziiertenklassen von Primelementen von $R[X]$. Wir wissen bereits, dass $K[X]$ faktoriell ist und wollen dies benutzen, um die noch fehlenden Assoziiertenklassen von Primelementen zu finden.
Ist $g \in K[X]$, dann gibt es ein $c \in K^*$ und ein $f = \sum_{i=0}^n a_i X^i \in R[X]$, so dass $g = cf$ und $\operatorname{ggT}(a_0,\ldots,a_n) = 1$ gilt. c und f sind bis auf Einheiten in R eindeutig bestimmt. Für jedes Polynom in $K[X]$ gibt es also ein assoziiertes Polynom in $R[X]$, dessen Koeffizienten teilerfremd sind.
Wir definieren für die Polynome in $R[X]$:

Definition 10.5

Sei $f = \sum_{i=0}^n a_i X^i \in R[X]$. Dann heißt $\operatorname{cont}(f) := \operatorname{ggT}(a_0,\ldots,a_n)$ der **Inhalt** von f (bis auf Einheiten in R^* eindeutig). Oft wird auch das zugehörige Hauptideal $I(f) = (\operatorname{cont}(f))$ Inhalt von f genannt. Ist $\deg f > 0$ und $\operatorname{cont}(f) = 1$, so heißt f ein **primitives** Polynom.

Bemerkung 10.6

Zu jedem $g \in K[X] \setminus K$ gibt es ein (bis auf Assoziiertheit in $R[X]$ eindeutiges) primitives Polynom $f \in R[X]$ mit $g = cf$ für geeignetes $c \in K^*$. f ist in $K[X]$ assoziiert zu g. Ist $g \in K[X]$ ein irreduzibles Polynom in $K[X]$, dann ist das assoziierte primitive Polynom $f \in R[X]$ irreduzibel in $R[X]$:
Offenbar kann f keinen echten Teiler in R haben, da seine Koeffizienten teilerfremd sind. Andererseits kann f keine Faktorisierung in Polynome positiven Grades haben, da g sonst nicht irreduzibel wäre.

Sehr nützlich sind die folgenden beiden Sätze:

Satz 10.7

Sei R ein faktorieller Ring, $f,g \in R[X]$. Dann gilt:

$$\mathrm{cont}(fg) \sim \mathrm{cont}(f)\mathrm{cont}(g)$$

bzw.

$$I(fg) = I(f)I(g).$$

Insbesondere ist also das Produkt primitiver Polynome in $R[X]$ wieder primitiv.

Beweis

Übung. □

Satz 10.8 (Lemma von Gauß)

Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Sei $f \in R[X]$, $\deg f > 0$. Ist f irreduzibel in $R[X]$, dann ist f auch irreduzibel in $K[X]$.

Beweis

Sei $f = g_1g_2$ mit $g_i \in K[X]$, und sei $g_i = c_if_i$ mit $f_i \in R[X]$ primitiv, $c_i \in K^*$ für $i = 1,2$. Dann ist $f = cf_1f_2$, für $c = c_1c_2 \in K^*$. Sei etwa $c = \frac{a}{b}$ mit $a,b \in R$ teilerfremd. Dann ist $bf = af_1f_2$, und wir erhalten

$$b \sim b\,\mathrm{cont}(f) \sim a\,\mathrm{cont}(f_1)\mathrm{cont}(f_2) \sim a,$$

also ist $c \in R^*$, und außerdem folgt nun, dass f_1 oder f_2 eine Einheit in R sein muss. Dann ist aber auch g_1 oder g_2 eine Einheit in $K[X]$, also f irreduzibel in $K[X]$. □

Aus dem Beweis des Satzes ergibt sich auch die folgende Aussage, die oft ebenfalls als „Lemma von Gauß“ bezeichnet wird.

Folgerung 10.9

Sei R ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Sei $f \in R[X]$, $\deg f > 0$. Ist $f = g_1g_2$ eine Faktorisierung in normierte Polynome $g_1, g_2 \in K[X]$, dann liegen g_1, g_2 bereits in $R[X]$.

Bemerkung 10.10

Wir haben mit dem Lemma von Gauß gezeigt, dass die irreduziblen Polynome in $R[X]$ von positivem Grad ein Repräsentantensystem für die Assoziiertenklassen von irreduziblen Elementen (=Primelementen) in $K[X]$ sind.

Satz 10.11

Sei $f \in R[X]$ ein irreduzibles Polynom in $R[X]$ positiven Grades. Dann ist f ein Primelement in $R[X]$.

Beweis

Seien $u,v \in R[X]$ mit $f|uv$ in $R[X]$. Da f irreduzibel und damit prim in $K[X]$ ist, folgt, dass f einen der Faktoren in $K[X]$ teilt. O.E. gilt also $u = fg$ mit $g \in K[X]$. Sei $g = ch$ mit $c \in K^*$, $h \in R[X]$ primitiv. Dann ist $c = \frac{a}{b}$ mit teilerfremden $a,b \in R$, und es ergibt sich folgende Beziehung mit Faktoren in $R[X]$:

$$bu = afh.$$

Dann ist $b\,\mathrm{cont}(u) \sim a\,\mathrm{cont}(f)$, und wegen der Teilerfremdheit von a und b folgt also: $b|\mathrm{cont}(f)$. Da f irreduzibel in $R[X]$ ist, ist $\mathrm{cont}(f)$ eine Einheit in R, also ist auch b eine Einheit in R, und damit folgt: f teilt u in $R[X]$. □

Satz 10.12 (Satz von Gauß)
Ist R faktoriell, dann ist auch der Ring $R[X]$ faktoriell.
Genauer gilt: Ist $\mathcal{P}_0(R)$ ein Repräsentantensystem für die Assoziiertenklassen von Primelementen in R und $\mathcal{P}_1(R)$ ein Repräsentantensystem für die Assoziiertenklassen von irreduziblen Polynomen positiven Grades in $K[X]$, bestehend aus primitiven Polynomen in $R[X]$, dann ist $\mathcal{P}_0(R) \cup \mathcal{P}_1(R)$ ein Repräsentantensystem für die Assoziiertenklassen von Primelementen in $R[X]$.
Beweis
Sei $f \in R[X]$, $f \neq 0$. Dann ist $f = r \in R$ oder $f = rg$ mit $r \in R$, $g \in R[X]$ primitiv. Die Zerlegung von $r \in R$ in Primelemente von R, $r = \varepsilon \prod_j r_j$ mit $\varepsilon \in R^*$, $r_j \in \mathcal{P}_0(R)$, ist nach Satz 10.3 auch eine Zerlegung in Primelemente von $R[X]$.
Da $g \in K[X]$, können wir zunächst g in $K[X]$ in Primelemente zerlegen. Wir finden also eine Faktorisierung

$$g = c \prod_i f_i \text{ mit } c \in K^*,\ f_i \in \mathcal{P}_1(R) \subseteq R[X].$$

Die Polynome f_i sind primitiv und irreduzibel in $R[X]$, also Primelemente in $R[X]$. Ist $c = \frac{a}{b}$ mit teilerfremden $a,b \in R$, dann ist $bg = a \prod_i f_i$ in $R[X]$ und daher $b \sim a$, d.h. $c \in R^*$. Mit $\varepsilon' = \varepsilon \cdot c \in R^*$ ist also

$$f = \varepsilon' \prod_j r_j \prod_i f_i$$

eine Zerlegung in Primelemente von $R[X]$.
Damit ist der Ring $R[X]$ als faktoriell nachgewiesen, und die genauere Aussage ist dann ebenfalls klar. □

Folgerung 10.13
Sei R ein Integritätsring, $n \in \mathbb{N}$. Dann ist der Polynomring $R[X_1,...,X_n]$ genau dann faktoriell, wenn R faktoriell ist.

Wir wollen uns nun mit der Frage befassen, wie wir entscheiden können, ob ein gegebenes Polynom in $R[X]$ irreduzibel über R bzw. über K ist. Zunächst leiten wir aus den bisherigen Resultaten leicht das folgende Kriterium für Linearfaktoren ab:

Lemma 10.14
Sei R ein faktorieller Ring, $K = Q(R)$. Sei $f = \sum_{i=0}^{n} c_i X^i \in R[X]$ normiert. Ist $a \in K$ eine Nullstelle von f, dann ist $a \in R$, und $a | c_0$.
Beweis
Da $a \in K$ eine Nullstelle ist, können wir f in $K[X]$ faktorisieren:

$$f = (X - a)g \text{ mit } g \in K[X].$$

Da f und $X - a$ normiert sind, ist auch g normiert. Dann folgt aber: $X - a, g \in R[X]$, also gilt $a \in R$, und $c_0 = f(0) = (-a)g(0)$ zeigt, dass $a | c_0$ gilt. □

Beispiel 10.15
Betrachte $f = X^3 - 2 \in \mathbb{Z}[X]$. Wäre f reduzibel in $\mathbb{Q}[X]$, dann hätte f eine Nullstelle in $\mathbb{Q}$, also nach dem obigen Lemma eine Nullstelle in $\mathbb{Z}$, die unter den Teilern von 2 in $\mathbb{Z}$ vorkommen müsste. Da offenbar keiner dieser Teiler eine Nullstelle von f ist, ist f also irreduzibel in $\mathbb{Q}[X]$. Insbesondere folgt damit, dass $\sqrt[3]{2}$ irrational ist.

Sehr oft ist folgendes Reduktionsargument nützlich:

Satz 10.16

Sei R ein Integritätsring, und sei $\pi : R \to \overline{R}$, $a \mapsto \overline{a}$ ein Ringhomomorphismus in einen Integritätsring $\overline{R}$. Wir bezeichnen dann mit π auch den induzierten Homomorphismus $R[X] \to \overline{R}[X]$, $\sum_i a_i X^i \mapsto \sum_i \overline{a}_i X^i$ ($f \mapsto \overline{f}$).
Sei $f = \sum_{i=0}^{n} a_i X^i$ ein primitives Polynom in $R[X]$ mit $a_n \neq 0$. Ist $\overline{f}$ irreduzibel in $\overline{R}[X]$, dann ist f auch irreduzibel in $R[X]$.

Beweis

Sei f reduzibel in $R[X]$, also $f = gh$ mit $g,h \in R[X]$, $g,h \notin R^*$. Da f primitiv ist, sind beide Polynome g,h von positivem Grad. Anwenden von π liefert eine Faktorisierung $\overline{f} = \overline{g}\overline{h}$, wobei wegen $\overline{a}_n \neq 0$ die Gradgleichung

$$\deg \overline{g} + \deg \overline{h} = \deg \overline{f} = \deg f = \deg g + \deg h$$

gilt, aus der $\deg \overline{g} = \deg g$ und $\deg \overline{h} = \deg h$ folgt. Also ist $\overline{f}$ reduzibel in $\overline{R}[X]$.

Beispiel 10.17

Sei $R = \mathbb{Z}$, $\pi : \mathbb{Z} \to \mathbb{Z}_2$ der kanonische Restklassenhomomorphismus. Sei $f = 7X^3 + 4X^2 + X + 13 \in \mathbb{Z}[X]$. Dann ist f offenbar primitiv, und $\pi(7) \neq 0$. Es ist

$$\overline{f} = X^3 + X + 1 \in \mathbb{Z}_2[X].$$

Dieses Polynom hat keine Nullstelle in $\mathbb{Z}_2 = \{0,1\}$, also ist $\overline{f}$ irreduzibel in $\mathbb{Z}_2[X]$, und damit ist f irreduzibel in $\mathbb{Z}[X]$. Da $\mathbb{Z}$ ein faktorieller Ring ist, ist nach dem Lemma von Gauß dann f auch irreduzibel in $\mathbb{Q}[X]$.

Satz 10.18 (Eisenstein-Kriterium)

Sei R ein Integritätsring. Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein primitives Polynom mit folgender Eigenschaft:
Es gibt ein Primelement $p \in R$, so dass

$$p \nmid a_n \,;\; p \mid a_i \text{ für } i = 0,\ldots,n-1 \,;\; p^2 \nmid a_0 \,.$$

(Polynome dieser Form heißen **Eisenstein-Polynome**.) Dann ist f irreduzibel in $R[X]$.
Ist R ein faktorieller Ring mit $K = Q(R)$, so ist f auch irreduzibel in $K[X]$.

Beweis

Da $p \in R$ ein Primelement ist, ist $\overline{R} = R/(p)$ ein Integritätsring. Wir bezeichnen mit $\pi : R[X] \to \overline{R}[X]$, $g \mapsto \overline{g}$ wieder die induzierte Abbildung.
Angenommen, es gibt eine Faktorisierung $f = gh$ mit Polynomen $g,h \in R[X]$ positiven Grades. Dann erhalten wir nach Anwendung von π:

$$\overline{a}_n X^n = \overline{f} = \overline{g}\overline{h}\,.$$

Also sind $\overline{g}$ und $\overline{h}$ von der Form $\overline{g} = bX^k$, $\overline{h} = cX^m$ mit $k = \deg g$, $m = \deg h$ (insbesondere $k,m > 0$), $b,c \in \overline{R}$, $bc = \overline{a}_n$. Dann folgt $\overline{g}(0) = 0 = \overline{h}(0)$, d.h. $p \mid g(0)$ und $p \mid h(0)$. Also gilt $p^2 \mid g(0)h(0)$ mit $g(0)h(0) = f(0) = a_0$, im Widerspruch zur Voraussetzung. □

Folgerung 10.19

Sei $a \in \mathbb{Z} \setminus \{1,-1\}$ quadratfrei (also durch kein Primzahlquadrat teilbar), $n \in \mathbb{N}$.
Dann sind alle Polynome $X^n - a$ irreduzibel in $\mathbb{Z}[X]$ und damit auch in $\mathbb{Q}[X]$.

Folgerung 10.20

Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist das Polynom

$$X^{p-1} + X^{p-2} + ... + X + 1$$

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

Beweis

Setze $f = X^{p-1} + X^{p-2} + ... + X + 1$. Wir zeigen, dass f irreduzibel in $\mathbb{Z}[X]$ ist, dann ist es nach Lemma von Gauß auch irreduzibel in $\mathbb{Q}[X]$.

Wir führen die Substitution $X \mapsto X + 1$ durch, die einen Isomorphismus auf $\mathbb{Z}[X]$ bewirkt, also Irreduzibilität erhält. Dann wird $f(X)$ übergeführt in $g(X) = f(X+1)$. Um $g(X)$ zu berechnen, benutzen wir die Gleichung $f \cdot (X-1) = X^p - 1$. Bei unserer Substitution wird daraus $f(X+1) \cdot X = (X+1)^p - 1$. Also folgt nach Division durch X:

$$g(X) = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i .$$

Wir wollen nun zeigen, dass dieses letzte Polynom ein Eisenstein-Polynom ist, dann folgt die Irreduzibilität für g und damit für f. Es gilt $p \mid \binom{p}{j}$ für $j = 1,...,p-1$, $p \nmid \binom{p}{p} = 1$, also werden alle Koeffizienten außer dem Leitkoeffizienten durch p geteilt. Außerdem gilt $p^2 \mid \binom{p}{1} = p$, d.h. das konstante Glied von g erfüllt bezüglich p die Eisenstein-Bedingung. Also ist g ein Eisenstein-Polynom und damit irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

Bemerkung 10.21

Das Polynom $f = X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$ ist das p-te **Kreisteilungspolynom**. Es hat das Element $\zeta_p = e^{2\pi i/p}$ als Nullstelle. Wir schließen aus der Irreduzibilität von f in $\mathbb{Q}[X]$ nun:

Folgerung 10.22

Sei p eine Primzahl. Ist $p-1$ keine Potenz von 2, dann ist die Konstruktion des regulären p-Ecks mit Zirkel und Lineal nicht möglich.

Beweis

Ist das reguläre p-Eck mit Zirkel und Lineal konstruierbar, dann ist $|\mathbb{Q}(\zeta_p) : \mathbb{Q}|$ nach Folgerung 4.8 eine 2-Potenz. Nach den obigen Resultaten ist $f = X^{p-1} + X^{p-2} + ... + X + 1 = \operatorname{minpol}_{\mathbb{Q}}(\zeta_p)$, also ist $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = \deg f = p - 1$, woraus die Behauptung folgt.

Bemerkung 10.23

(i) Insbesondere ist also das reguläre n-Eck für $n = 7,11,13,14,19,...$ nicht konstruierbar. (Übung: Reguläre p^r-Ecke sind für $p \neq 2$, $r > 1$ nicht mit Zirkel und Lineal konstruierbar.)
Eine umfassende Antwort darauf, welche regulären n-Ecke konstruierbar sind, können wir erst viel später geben.

(ii) Primzahlen p mit der Eigenschaft, dass $p-1$ eine 2-Potenz ist, sind von der Form $p = F_m = 2^{2^m} + 1$ (Übung!). Sie heißen **Fermatsche Primzahlen**. Allerdings sind bisher erst wenige Fermatsche Primzahlen bekannt, für $m = 0,...,4$: $p = 3,5,17,257,65537$. F_5 ist keine Primzahl: $F_5 = 641 \cdot 6700417$.

Wir kommen nun zum Problem der Winkeldreiteilung. Ist der Winkel φ gegeben, muss in diesem Fall die Konstruierbarkeit von $e^{i\varphi/3}$ aus $\{0,1,e^{i\varphi}\}$ (nur mit Zirkel und Lineal) geklärt werden. Im Fall einer positiven Antwort muss für $K_0 = \mathbb{Q}(e^{i\varphi})$ der Grad $|K_0(e^{i\varphi/3}) : K_0|$ eine 2-Potenz sein. Da $e^{i\varphi/3}$ Nullstelle von $X^3 - e^{i\varphi} \in K_0[X]$ ist, hat die Körpererweiterung den Grad 1, 2 oder 3, und $\varphi/3$ ist genau in den ersten beiden Fällen konstruierbar.

Es ist also nun zu klären, ob $X^3 - e^{i\varphi}$ irreduzibel über $\mathbb{Q}(e^{i\varphi})$ sein kann.

Satz 10.24

Für alle $\varphi \in (0,2\pi)$, für die $e^{i\varphi}$ eine transzendente Zahl ist, ist die Dreiteilung von φ mit Zirkel und Lineal nicht möglich. Die Menge dieser φ ist dicht in $(0,2\pi)$.

Beweis

Ist $e^{i\varphi}$ transzendent über $\mathbb{Q}$, so gibt es einen Isomorphismus

$$h : \mathbb{Q}(t) \to \mathbb{Q}(e^{i\varphi}) \text{ mit } h|_{\mathbb{Q}} = id_{\mathbb{Q}},\ h(t) = e^{i\varphi},$$

wobei t eine Unbestimmte über $\mathbb{Q}$ ist. Diese Abbildung induziert einen Ringisomorphismus

$$\mathbb{Q}(t)[X] \to \mathbb{Q}(e^{i\varphi})[X],$$

der $X^3 - t$ auf $X^3 - e^{i\varphi}$ abbildet. Nach dem Eisenstein-Kriterium ist $X^3 - t$ irreduzibel in $\mathbb{Q}[t][X]$, da t in $\mathbb{Q}[t]$ prim ist. Nach dem Lemma von Gauß ist also $X^3 - t$ irreduzibel in $\mathbb{Q}(t)[X]$, und damit ist auch $X^3 - e^{i\varphi}$ irreduzibel in $\mathbb{Q}(e^{i\varphi})[X]$. Also ist $\left|\mathbb{Q}(e^{i\varphi/3}) : \mathbb{Q}(e^{i\varphi})\right| = 3$ und die Dreiteilung des Winkels φ mit Zirkel und Lineal nicht möglich.

Ist $\varphi \in (0,2\pi)$ und $z = e^{i\varphi}$ algebraisch über $\mathbb{Q}$, so sind auch der Realteil und Imaginärteil von z algebraisch über $\mathbb{Q}$. Da es nur abzählbar viele algebraische Zahlen gibt, gibt es also auch nur abzählbar viele $\varphi \in (0,2\pi)$ mit algebraischem $e^{i\varphi}$, also ist die Menge der φ mit transzendentem $e^{i\varphi}$ dicht in $(0,2\pi)$. □

Bemerkung 10.25

Auch die Menge der φ, für die die Winkeldreiteilung möglich ist, ist dicht in $(0,2\pi)$. Dies folgt daraus, dass alle Winkel der Form $\frac{\pi}{2^k}$ mit Zirkel und Lineal gedrittelt werden können.

Kapitel 11

Zerfällungskörper von Polynomen

Endliche Erweiterungen treten als zentrale Objekte beim Studium der Nullstellen eines gegebenen Polynoms bzw. der Lösungsmenge eines algebraischen Gleichungssystems auf. Sie sind zum Beispiel als Radikalerweiterungen schon begegnet. Wir benötigen zunächst ein Lemma:

Lemma 11.1 (Kronecker)

Sei K ein Körper, $f \in K[X] \setminus K$. Dann gibt es einen Erweiterungskörper L von K, in dem f eine Nullstelle besitzt.

Beweis

O.E. sei f irreduzibel, sonst betrachten wir einen irreduziblen Faktor von f. Wir setzen $L = K[X]/(f)$. Da f irreduzibel ist, ist L ein Körper, und K ist via $a \mapsto a + (f)$ kanonisch in L eingebettet. Außerdem ist $a = X + (f) \in L$ eine Nullstelle von f in L. □

Da ein gegebenes Polynom $f \in K[X]$ in jedem Erweiterungskörper von K nur endlich viele Nullstellen besitzen kann, gibt es einen endlichen Erweiterungskörper, in dem f vollständig in Linearfaktoren zerfällt. Wir definieren nun:

Definition 11.2

Sei $f \in K[X]$ ein nichtkonstantes Polynom. Dann ist ein **Zerfällungskörper von f über K** ein Erweiterungskörper L/K, für den gilt:

(i) f zerfällt in $L[X]$ in Linearfaktoren.

(ii) Sind $a_1,...,a_n$ die Nullstellen von f in L, so ist $L = K(a_1,...,a_n)$.

Bemerkung 11.3

Da die a_i offenbar algebraisch über K sind, gilt auch $L = K[a_1,...,a_n]$.

Beispiel 11.4

(i) Sei $f = X^2 + 1 \in \mathbb{Q}[X] \subset \mathbb{R}[X]$. Dann ist $\mathbb{Q}(i)$ ein Zerfällungskörper von f über $\mathbb{Q}$ und $\mathbb{C} = \mathbb{R}(i)$ ein Zerfällungskörper von f über $\mathbb{R}$.

(ii) Sei $f = X^3 - 2 \in \mathbb{Q}[X]$. Sei $a = \sqrt[3]{2}$ und $w = e^{2\pi i/3}$ eine dritte Einheitswurzel. Dann sind a, aw und aw^2 die Nullstellen von f in $\mathbb{C}$. Also ist ein Zerfällungskörper von f über $\mathbb{Q}$ gegeben durch

$$L = \mathbb{Q}(a, aw, aw^2) = \mathbb{Q}(a, w).$$

Vor dem nächsten Satz brauchen wir noch eine Definition:

Definition 11.5

Seien L_1 und L_2 Erweiterungskörper des Körpers K. Dann heißt ein Ringhomomorphismus $\varphi : L_1 \to L_2$ ein **K-Homomorphismus**, wenn $\varphi|_K = \mathrm{id}_K$ ist (entsprechend heißt ein Isomorphismus φ dann ein **K-Isomorphismus** bzw. für $L_1 = L_2$ ein **K-Automorphismus**).

Folgende Eigenschaften von Zerfällungskörpern sind grundlegend:

Satz 11.6

Sei $f \in K[X]$ ein nichtkonstantes Polynom.

(i) f besitzt einen Zerfällungskörper über K.

(ii) Ist L ein Zerfällungskörper von f über K und $\deg f = n$, so ist $|L : K| \leq n!$.

(iii) Je zwei Zerfällungskörper von f über K sind K-isomorph.

Beweis

Die Aussage (i) ergibt sich unmittelbar aus obigem Lemma mit Induktion.

Zu (ii): für die Adjunktion der ersten Nullstelle a_1 von f gilt

$$|K(a_1) : K| = \deg \operatorname{minpol}_K(a_1) \leq \deg f = n .$$

Sei nun $a_2 \notin K(a_1)$ die erste zu adjungierende Nullstelle, dann ist

$$|K(a_1, a_2) : K(a_1)| = \deg \operatorname{minpol}_{K(a_1)}(a_2) \leq \deg \frac{f}{X - a_1} = n - 1 .$$

Wir setzen dies nun induktiv fort und erhalten damit (ii).

Die Aussage (iii) ist eine Folgerung aus dem nachfolgenden Ergebnis, das auf ein zentrales Thema der Galoistheorie deutet, wir müssen dazu nur $K = \widetilde{K}$ und $\varphi = \mathrm{id}_K$ setzen.

Satz 11.7

Seien K und $\widetilde{K}$ Körper, sei $\varphi : K \to \widetilde{K}$ ein Isomorphismus, und sei $\Phi : K[X] \to \widetilde{K}[X]$ der induzierte Isomorphismus der Polynomringe. Sei $f \in K[X] \setminus K$. Ist L/K ein Zerfällungskörper von f und $\widetilde{L}/\widetilde{K}$ ein Zerfällungskörper von $\tilde{f} = \Phi(f) \in \widetilde{K}[X]$, dann gibt es einen Isomorphismus $\psi : L \to \widetilde{L}$ mit folgenden Eigenschaften:

(i) $\psi|_K = \varphi$.

(ii) ψ bildet die Menge der Nullstellen von f in L auf die Menge der Nullstellen von $\tilde{f}$ in $\widetilde{L}$ ab.

(Die Abbildung ψ heißt dann eine **Fortsetzung** von φ.)

Beweis

Wir wollen die Behauptung per Induktion über den Grad $n = |L : K|$ beweisen. Ist $n = 1$, so zerfällt f über K in Linearfaktoren, also zerfällt auch $\tilde{f}$ über $\widetilde{K}$ in Linearfaktoren, und die Aussage des Satzes gilt mit $\psi = \varphi$.

Sei nun $n > 1$, also ist $\deg f > 1$ und f besitzt einen normierten irreduziblen Faktor g vom Grad > 1. Dann hat auch $\tilde{f} = \Phi(f)$ einen normierten irreduziblen Faktor $\tilde{g} = \Phi(g)$ vom Grad > 1.

Wir zeigen nun für den Induktionsschritt folgendes Hilfsresultat:

Lemma 11.8

Sei die Situation wie in obigem Satz, $g \in K[X]$ ein irreduzibles Polynom, das in $L[X]$ in Linearfaktoren zerfällt. Sei $a \in L$ eine Nullstelle von g und $\tilde{a} \in \widetilde{L}$ eine Nullstelle von $\tilde{g} = \Phi(g)$.

Dann gibt es einen eindeutig bestimmten Isomorphismus

$$\psi : K\langle a \rangle \to \widetilde{K}\langle \tilde{a} \rangle \text{ mit } \psi|_K = \varphi \text{ und } \psi\langle a \rangle = \tilde{a}$$

Beweis

Jeder Homomorphismus mit $\psi|_K = \varphi$ und $\psi\langle a \rangle = \tilde{a}$ bildet $\sum_i c_i a^i$ auf $\sum_i \varphi(c_i)\tilde{a}^i$ ab. Da $K\langle a \rangle = K[a]$ ist, folgt daraus die Eindeutigkeit. Wir müssen noch zeigen, dass es tatsächlich einen solchen Isomorphismus gibt, d.h. dass durch diese Setzung eine **wohl definierte~** Abbildung Abbildung gegeben ist.

Aufgrund der universellen Eigenschaft des Polynomrings gibt es einen Ringhomomorphismus $\sigma : K[X] \to \widetilde{K}[\tilde{a}] = \widetilde{K}(\tilde{a})$ mit $\sigma|_K = \varphi$ und $\sigma(X) = \tilde{a}$. Offenbar ist σ surjektiv. Wir berechnen nun den Kern von σ. Sei $0 \neq h = \sum_i c_i X^i \in \operatorname{Kern}\sigma$. Dann ist

$$0 = \sigma(h) = \sum_i \varphi(c_i)\tilde{a}^i\,,$$

also ist $\tilde{a}$ eine Nullstelle von $\Phi(h) = \sum_i \varphi(c_i)X^i$. Da $\tilde{g} = \Phi(g)$ das Minimalpolynom von $\tilde{a}$ ist, folgt:

$$\Phi(h) \in \Phi(g)\widetilde{K}[X]\,.$$

Anwenden von Φ^{-1} liefert:

$$h \in gK[X]\,.$$

Umgekehrt ist offenbar $gK[X]$ im Kern von σ enthalten, also ist $\operatorname{Kern}\sigma = gK[X]$.
Nach dem Homomorphiesatz erhalten wir damit einen Isomorphismus

$$\overline{\sigma} : K[X]/(g) \to \widetilde{K}[\tilde{a}]\,,$$

der $\sum_i c_i X^i + (g)$ auf $\sum_i \varphi(c_i)\tilde{a}^i$ abbildet. Andererseits haben wir aber auch einen Isomorphismus

$$K[a] \to K[X]/(g)\,,$$

der $\sum_i r_i a^i$ auf $\sum_i r_i X^i + (g)$ abbildet. Hintereinanderausführung dieser beiden Isomorphismen liefert den gesuchten Isomorphismus. □

Beweis (Fortsetzung, Satz 11.7)
Sei $a \in L$ eine Nullstelle von g und $\tilde{a} \in \widetilde{L}$ eine Nullstelle von $\tilde{g} = \Phi(g)$.
Dann haben wir nach dem Lemma also einen Isomorphismus

$$\varphi' : K(a) \to \widetilde{K}(\tilde{a})\,,$$

der φ fortsetzt und die Nullstelle a von f auf die Nullstelle $\tilde{a}$ von $\tilde{f}$ abbildet. Da $\deg g = |K(a) : K| > 1$ ist, folgt

$$|L : K(a)| = \frac{|L : K|}{|K(a) : K|} < n\,,$$

und wir können nun die Induktionsvoraussetzung anwenden, da L auch Zerfällungskörper von f über $\widetilde{K}(\tilde{a})$ ist. Also gibt es einen Isomorphismus

$$\psi : L \to \widetilde{L}\,,$$

der φ' (und damit erst recht φ) fortsetzt und die Nullstellen von f in L auf die Nullstellen von $\tilde{f}$ in $\widetilde{L}$ abbildet. □

Wir können nun genauere Aussagen über die Zahl der Fortsetzungen von φ machen. Zunächst definieren wir:

Definition 11.9

Ist $f \in K[X]$ ein irreduzibles Polynom, das in seinem Zerfällungskörper lauter verschiedene Nullstellen hat, so heißt f **separabel**. Ein beliebiges nichtkonstantes Polynom heißt **separabel**, wenn alle seine irreduziblen Faktoren separabel sind, sonst heißt es **inseparabel**.

Beispiel 11.10

(i) Das Polynom $(X^2+1)(X^3-2)^2$ ist separabel in $\mathbb{Q}[X]$.
(ii) Ist t eine Unbestimmte über $\mathbb{Z}_2$, dann ist $X^2 + t \in \mathbb{Z}_2(t)[X]$ inseparabel.

Mit denselben Voraussetzungen und Bezeichnungen wie in obigem Satz gilt:

Folgerung 11.11

Es gibt höchstens $|L:K|$ Fortsetzungen von φ. Ist f separabel, so gibt es genau $|L:K|$ Fortsetzungen von φ.

Beweis

Wir beweisen die Behauptung wieder durch Induktion nach $n = |L:K|$. Ist $n = 1$, so ist $L = K$, und es ist nichts zu zeigen. Ist $n > 1$, so hat f einen normierten irreduziblen Faktor g vom Grad > 1. Sei a eine Nullstelle von g und $\psi : L \to \tilde{L}$ eine Fortsetzung von φ. Durch Einschränkung auf $K(a)$ erhalten wir einen Isomorphismus

$$\varphi' : K(a) \to \widetilde{K}(\psi(a)).$$

Nach Induktionsvoraussetzung gibt es höchstens $|L:K(a)|$ Fortsetzungen von φ'. Da $\psi(a)$ eine Nullstelle von $\Phi(g)$ sein muss, gibt es aber auch höchstens $\deg\Phi(g) = \deg g = |K(a):K|$ viele Einbettungen von $K(a)$ nach $\tilde{L}$. Also ist die Anzahl der Fortsetzungen von φ höchstens

$$|L:K(a)|\cdot|K(a):K| = |L:K|.$$

Hat f lauter verschiedene Nullstellen, so zeigen analoge Argumente die Gleichheit. □

Insbesondere folgt nun die Anzahl der K-Automorphismen von L:

Folgerung 11.12

Ist L Zerfällungskörper eines nichtkonstanten Polynoms $f \in K[X]$, so gibt es höchstens $|L:K|$ K-Automorphismen von L. Ist f separabel, so gibt es genau $|L:K|$ verschiedene K-Automorphismen.

Definition 11.13

Sei L/K eine Körpererweiterung. Dann bezeichnen wir mit $G\left(L/K\right)$ die Gruppe der K-Automorphismen von L (mit der Komposition von Abbildungen als Verknüpfung).

Ist L Zerfällungskörper über K eines nichtkonstanten separablen Polynoms $f \in K[X]$, dann heißt $G(f) := G\left(L/K\right)$ die **Galoisgruppe** des Polynoms f.

Folgerung 11.14

Ist L Zerfällungskörper eines nichtkonstanten separablen Polynoms $f \in K[X]$, dann ist:

$$|G(f)| = \left|G\left(L/K\right)\right| = |L:K|.$$

Bemerkung 11.15

Im Satz 11.7 spielte bereits das Verhalten auf der Nullstellenmenge eines gegebenen Polynoms f eine wichtige Rolle. Wir betrachten dies etwas genauer in der Situation eines nichtkonstanten irreduziblen separablen Polynoms $f \in K[X]$ mit Zerfällungskörper L über K. Sei $n = \deg f$.

Ist $a \in L$ eine Nullstelle von f, dann ist für jedes Element $\sigma \in G(f)$ auch $\sigma(a)$ eine Nullstelle von f. Die Galoisgruppe permutiert also die Nullstellenmenge von f. Andererseits ist jedes $\sigma \in G(f)$ durch seine Operation auf den n Nullstellen $a_1,...,a_n$ von f eindeutig bestimmt, da $L = K(a_1,...,a_n)$. Aber nicht jede Permutation der Nullstellen liefert einen K-Automorphismus von L, da es i.A. zwischen den Nullstellen Abhängigkeiten gibt. Das bedeutet, dass der Homomorphismus(!)

$$G(f) \to S_n,\ \sigma \mapsto (i \mapsto j,\ \text{falls } \sigma(a_i) = a_j)$$

injektiv, aber i.A. nicht surjektiv ist. Es ist also $G(f)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Wir werden diese Gruppe und das Wechselspiel ihrer Eigenschaften mit denen der Körpererweiterung L/K noch genauer untersuchen.

Ist ein konkretes Polynom $f \in K[X]$ gegeben, dessen Zerfällungskörper konstruiert werden soll, so wird i.A. nicht die obige „abstrakte“ Konstruktion durchgezogen, sondern meist ist bereits ein Erweiterungskörper L von K bekannt, in dem f in Linearfaktoren zerfällt. Dann müssen „nur“ die Nullstellen von f in L ausgerechnet und an K adjungiert werden, um – nach Definition – einen Zerfällungskörper zu erhalten.

Beispiel 11.16

Sei wieder $f = X^3 - 2 \in \mathbb{Q}[X]$. Wir haben auf die oben beschriebene Weise bereits zu Beginn des Paragraphen einen (und damit den) Zerfällungskörper von f in $\mathbb{C}$ konstruiert:

$$L = \mathbb{Q}(a, aw, aw^2) = \mathbb{Q}(a, w)$$

mit $a = \sqrt[3]{2}$ und $w = e^{2\pi i/3}$ eine dritte Einheitswurzel. Es ist

$$|L : \mathbb{Q}| = |L : \mathbb{Q}(a)| \cdot |\mathbb{Q}(a) : \mathbb{Q}| = 2 \cdot 3 = 6\,,$$

denn $|L : \mathbb{Q}(a)| = 2$, weil w Nullstelle von $X^2 + X + 1$ ist, aber $w \notin \mathbb{Q}(a) \subseteq \mathbb{R}$.

Die $\mathbb{Q}$-Automorphismen von L müssen a auf eine der drei Nullstellen a, aw, aw^2 von f und w auf eine der beiden Nullstellen w, w^2 des Minimalpolynoms $X^2 + X + 1$ von w über $\mathbb{Q}$ abbilden. Wegen $L = \mathbb{Q}(a, w)$ ist jeder $\mathbb{Q}$-Automorphismus von L durch die Bilder von a und w bereits eindeutig bestimmt. Da wir bereits wissen, dass $|G(f)| = \left|G\left(L/K\right)\right| = 6$ ist, definiert tatsächlich jede der beschriebenen sechs Wahlen einen $\mathbb{Q}$-Automorphismus von L, also ein $\psi \in G\left(L/K\right) = G(f)$. Es ist hier also $G(f) \cong S_3$.

Wie sehen die Permutationen auf den Nullstellen explizit aus? Sei etwa $\tau \in G(f)$ bestimmt durch $\tau(a) = aw$, $\tau(w) = w^2$. Dann operiert τ auf den drei Nullstellen $a_1 = a$, $a_2 = aw$, $a_3 = aw^2$ von f wie folgt: $\tau(a_1) = a_2$, $\tau(a_2) = \tau(aw) = \tau(a)\tau(w) = aw \cdot w^2 = a = a_1$, $\tau(a_3) = \tau(aw^2) = \tau(a)\tau(w)^2 = aw \cdot (w^2)^2 = aw^2 = a_3$ (die letzte Rechnung diente nur zur Überprüfung!). Die zu τ gehörende Permutation in S_3 ist also die Transposition $(1\ 2)$.

Kapitel 12

Separabilität

In den vorhergehenden Abschnitten haben wir gesehen, dass die Nullstellen eines irreduziblen Polynoms in $K[X]$ durch K-Automorphismen des Zerfällungskörpers permutiert werden. Wir wollen uns nun mit dem Problem befassen, wie wir entscheiden können, ob ein gegebenes Polynom separabel ist. Zunächst brauchen wir einige Vorbereitungen.
Sei R ein Ring mit 1, dann ist durch die folgende Definition ein Ringhomomorphismus $\varphi : \mathbb{Z} \to R$ gegeben: für $n \in \mathbb{N}_0$ sei $\varphi(n) = \underbrace{1_R + \ldots + 1_R}_{n\text{-mal}} = n \cdot 1_R$, und für $n \in \mathbb{Z}$, $n < 0$ sei $\varphi(n) = -\varphi(-n) = -((-n) \cdot 1_R)$.
Dann ist $\varphi(\mathbb{Z}) \subseteq R$ ein Unterring von R und $\operatorname{Kern}\varphi$ ein Ideal von $\mathbb{Z}$.

Definition 12.1

Der Unterring $\varphi(\mathbb{Z}) \subseteq R$ heißt der **Primring** von R. Die (eindeutig bestimmte) Zahl $n \in \mathbb{N}_0$ mit $\operatorname{Kern}\varphi = n\mathbb{Z}$ heißt die **Charakteristik** des Rings R, kurz: $n = \operatorname{Char} R$.

Bemerkung 12.2

(i) Ist φ injektiv, so ist $n = 0$ und der Primring ist isomorph zu $\mathbb{Z}$. Ist φ nicht injektiv, so ist n die kleinste positive Zahl mit $n \cdot 1_R = 0$, und der Primring ist isomorph zu $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Insbesondere hat der Ring $\mathbb{Z}_n$ die Charakteristik n.

(ii) Die Charakteristik eines Integritätsrings mit 1 (also insbesondere eines Körpers) ist 0 oder eine Primzahl.

In Ringen der Charakteristik p, p eine Primzahl, gibt es einen besonderen Ringhomomorphismus:

Lemma 12.3

Sei R ein kommutativer Ring mit 1, $\operatorname{Char} R = p$ eine Primzahl. Dann ist die Abbildung

$$F : R \to R,\ a \mapsto a^p$$

ein Ringhomomorphismus. Sie heißt **Frobenius-Abbildung**.
Die Menge $R^p := F(R)$ der p-ten Potenzen von Elementen aus R ist ein Unterring von R. Ist R ein Integritätsring, so ist R^p ein zu R isomorpher Ring. Ist R ein endlicher Körper, so ist $R = R^p$.

Beweis

Seien $a, b \in R$, dann ist

$$F(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$

Für $i = 1, \ldots, p-1$ sind die Binomialkoeffizienten $\binom{p}{i}$ durch p teilbare ganze Zahlen, also folgt

$$F(a+b) = a^p + b^p.$$

Es ist klar, dass $F(ab) = F(a)F(b)$ gilt. Also ist F ein Ringhomomorphismus, und $F(R) = R^p$ ist ein Unterring von R.

Ist R ein Integritätsring, so ist $F(a) = a^p \neq 0$ für alle $0 \neq a \in R$, also ist F injektiv und damit R isomorph zu R^p.
Ist R ein endlicher Körper, so sind nach dem Vorhergehenden R und R^p gleichmächtig, also ist $R = R^p$.

Wir kommen nun zum Problem der Charakterisierung irreduzibler separabler Polynome. Dies geschieht wie in der Analysis durch Bilden der Ableitung. Für Polynome definieren wir dazu ein formales algebraisches Analogon, für das dieselben Rechenregeln (Linearität, Produktregel) wie in der Analysis gelten.

Definition 12.4

Sei R ein kommutativer Ring mit 1, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Dann heißt

$$D(f) = f' = \sum_{i=1}^{n} i a_i X^{i-1}$$

die **(formale) Ableitung** von f.
Für $m \in \mathbb{N}$ ist die m-te Ableitung $f^{(m)}$ die m-fache Iteration der Ableitung von f.

Es besteht folgende Beziehung zwischen f und f' (Beweis: Übung):

Lemma 12.5

Sei $f = (X-a)^m \cdot g$ mit $a \in R$, $m \in \mathbb{N}$, $g \in R[X]$. Dann ist

$$f' = (X-a)^{m-1}\big(m \cdot g + (X-a)g'\big).$$

Für die Bestimmung der Vielfachheit einer Nullstelle können wir daraus folgendes ableiten. Ist a eine (genau) m-fache Nullstelle, also $f = (X-a)^m \cdot g$ mit $g \in R[X]$, $g(a) \neq 0$, so ist

$$f(a) = f'(a) = \ldots = f^{(m-1)}(a) = 0 \text{ und } f^{(m)}(a) = m! \cdot g(a)$$

Ist $m!$ eine Einheit in R, so gilt also $f^{(m)}(a) \neq 0$, und die Vielfachheit einer Nullstelle kann durch Bilden der höheren Ableitungen erkannt werden. In Abhängigkeit von der Charakteristik des Rings können dabei allerdings Probleme auftreten:

Beispiel 12.6

Sei p eine Primzahl und $K = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Das Polynom $f = (X-1)^p \in K[X]$ hat offenbar 1 als p-fache Nullstelle. Es ist aber $f = X^p - 1 \in K[X]$ und damit $f' = p \cdot X^{p-1} = 0$ in $K[X]$ und somit $f^{(i)} = 0$ für alle $i \in \mathbb{N}$.

Satz 12.7

Sei $f \in K[X]$ ein irreduzibles Polynom. Dann sind äquivalent:

(i) f ist inseparabel.

(ii) $f' = 0$.

(iii) $\operatorname{Char} K = p$ ist eine Primzahl, und f ist von der Form $f(X) = g(X^{p^e})$, wobei $g \in K[X]$ ein irreduzibles separables Polynom und $e \in \mathbb{N}$ ist.

Beweis

(i) $\Rightarrow$ (ii): Ist a eine mehrfache Nullstelle von f in seinem Zerfällungskörper, so ist $f'(a) = 0$ nach Lemma 12.5. Da f irreduzibel ist, ist f ein Polynom in $K[X] \setminus \{0\}$ kleinsten Grades mit Nullstelle a. Aber $\deg f' < \deg f$, also muss $f' = 0$ gelten.
(ii) $\Rightarrow$ (iii): Ist $f = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in K$, $a_n \neq 0$, $n > 0$, so ist $f' = \sum_{i=1}^{n} i a_i X^{i-1}$ und $f' = 0$ impliziert $i a_i = 0$ für $i = 1,\ldots,n$. Insbesondere folgt aus $n a_n = 0$, dass $n \cdot 1_K = 0$ ist, also ist $\operatorname{Char} K = p$ eine Primzahl, $n = mp$.

Aus $ia_i = 0$ folgt $a_i = 0$ oder $i \equiv 0 \bmod p$, also:

$$f = \sum_{j=0}^{m} a_{jp} (X^p)^j = f_1(X^p)$$

mit $f_1 = \sum_{j=0}^{m} a_{jp} X^j$. Da die Abbildung

$$K[X] \to K[X^p],\ h(X) \mapsto h(X^p)$$

offenbar ein Ringisomorphismus ist, folgt aus der Irreduzibilität von f auch die Irreduzibilität von f_1.
Ist f_1 separabel, so haben wir das gesuchte Polynom g gefunden. Andernfalls ist $f_1' = 0$, und wir können das Verfahren wiederholen, finden also ein irreduzibles Polynom $f_2 \in K[X]$ mit

$$f(X) = f_1(X^p) = f_2(X^{p^2}).$$

Dabei ist offenbar $\deg f_2 < \deg f_1$. Daher muss das Verfahren nach endlich vielen Schritten bei einem irreduziblen separablen Polynom enden.
(iii) $\Rightarrow$ (i): Sei $\operatorname{Char} K = p$, und sei f von der Form $f = \sum_{j=0}^{m} a_j (X^{p^e})^j$ für ein $e \in \mathbb{N}$. Sei a eine Nullstelle von f in seinem Zerfällungskörper über K. Dann gilt:

$$f = f - f(a) = \sum_{j=1}^{m} a_j \left((X^{p^e})^j - (a^{p^e})^j \right) = \sum_{j=1}^{m} a_j (X^j - a^j)^{p^e}.$$

Also ist a eine mindestens p^e-fache Nullstelle von f. □

Definition 12.8

Ein Körper K heißt **vollkommen**, wenn jedes nichtkonstante Polynom aus $K[X]$ separabel ist.

Bemerkung 12.9

Jeder Körper der Charakteristik 0 ist vollkommen.

Satz 12.10

Sei K ein Körper der Charakteristik $p > 0$. Dann ist K genau dann vollkommen, wenn $K = K^p$ gilt.

Beweis

Sei $K \neq K^p$, und sei $a \in K \setminus K^p$, $f = X^p - a \in K[X]$. Sei z eine Nullstelle von f in seinem Zerfällungskörper, dann ist $a = z^p$ und $f = (X - z)^p$. Da $a \notin K^p$, ist $z \notin K$, also ist $|K(z) : K| \geq 2$. Das Minimalpolynom von z über K teilt f, und ist daher ein inseparables irreduzibles Polynom in $K[X]$. Also ist K nicht vollkommen.
Sei $K = K^p$. Falls K nicht vollkommen ist, gibt es ein irreduzibles inseparables Polynom $f \in K[X]$. Nach Satz 12.7 ist dann

$$f = \sum_j a_j (X^{p^e})^j, \text{ wobei } a_j \in K,\ e \geq 1.$$

Da $K = K^p = K^{p^2} = \ldots = K^{p^e}$, gibt es $b_j \in K$ mit $a_j = b_j^{p^e}$. Also ist

$$f = \sum_j b_j^{p^e} (X^{p^e})^j = \left(\sum_j b_j X^j \right)^{p^e}.$$

Dies widerspricht der Irreduzibilät von f. Also muss K vollkommen sein. □

Wir können unserer Liste vollkommener Körper nun noch eine wichtige Familie hinzufügen:

Folgerung 12.11

Alle endlichen Körper sind vollkommen.

Beweis

Ein endlicher Körper K ist von Primzahlcharakteristik $p > 0$ und erfüllt nach Lemma 12.3 $K = K^p$. □

Beispiel 12.12

Ein unendlicher Körper von Charakteristik $p > 0$ ist z.B. der rationale Funktionenkörper $K(t)$ über einem Körper K von Charakteristik p. Dann ist $K(t)^p = K^p(t^p) \neq K(t)$, denn das Polynom $X^p - t \in K(t)[X]$ ist irreduzibel und inseparabel, also ist $K(t)$ nicht vollkommen.

Definition 12.13

Sei L/K eine Körpererweiterung.

(i) Ein Element $a \in L$ heißt **separabel algebraisch** über K, wenn a algebraisch und sein Minimalpolynom über K separabel ist.

(ii) Sind alle $a \in L$ separabel algebraisch über K, so heißt die Erweiterung L/K **separabel algebraisch**, andernfalls heißt sie **inseparabel**.

Beispiel 12.14

Jede algebraische Erweiterung $L/\mathbb{Q}$ ist separabel algebraisch, da $\mathbb{Q}$ vollkommen ist.

Es gilt wieder eine Übertragung auf Zwischenkörper:

Satz 12.15

Sei Z ein Zwischenkörper einer Erweiterung L/K. Ist L/K separabel algebraisch, so sind auch L/Z und Z/K separabel algebraische Körpererweiterungen.

Beweis

Aus der Definition folgt unmittelbar, dass Z/K separabel algebraisch ist. Ist $a \in L$, so ist $g = \mathrm{minpol}_Z a$ ein Teiler von $f = \mathrm{minpol}_K a$ in $Z[X]$. Da f keine mehrfachen Nullstellen in seinem Zerfällungskörper hat, kann daher auch g keine mehrfachen Nullstellen in seinem Zerfällungskörper haben. Also ist L/Z separabel algebraisch. □

Wie wir später sehen werden, gilt auch die Umkehrung des obigen Satzes.

Kapitel 13

Algebraischer Abschluss

Zu einem gegebenen nichtkonstanten Polynom $f \in K[X]$ haben wir bereits einen Erweiterungskörper konstruiert, in dem f in Linearfaktoren zerfällt.
Wir wollen nun in diesem Abschnitt einen Erweiterungskörper von K konstruieren, über dem **alle** nichtkonstanten Polynome in Linearfaktoren zerfallen bzw. in dem jedes nichtkonstante Polynom eine Nullstelle hat.

Definition 13.1

Ein Körper K heißt **algebraisch abgeschlossen**, wenn jedes nichtkonstante Polynom $f \in K[X]$ eine Nullstelle in K besitzt.

Beispiel 13.2

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$ (p Primzahl) sind nicht algebraisch abgeschlossen. Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.
Wir hatten früher bereits einen **relativen** algebraischen Abschluss definiert, nämlich in einer Körpererweiterung L/K den Körper $\overline{K}$ der über K algebraischen Elemente in L. Ist L algebraisch abgeschlossen, so ist auch $\overline{K}$ algebraisch abgeschlossen:

Lemma 13.3

Sei L/K eine Körpererweiterung, L algebraisch abgeschlossen. Dann ist der algebraische Abschluss $\overline{K}$ von K in L algebraisch abgeschlossen.

Beweis

Ist $f \in \overline{K}[X]$ ein nichtkonstantes Polynom, so hat f eine Nullstelle a in L. Dann ist a ein über $\overline{K}$ algebraisches Element von L, liegt also bereits in $\overline{K}$. □

Bemerkung 13.4

Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist auch der Körper $\overline{\mathbb{Q}}$ der algebraischen Zahlen algebraisch abgeschlossen.

Satz 13.5

Ist K ein Körper, so sind folgende Aussagen äquivalent:

(i) K ist algebraisch abgeschlossen.

(ii) Jedes $f \in K[X]$ hat eine Darstellung der Form

$$f = b(X - a_1) \cdot (X - a_2) \cdot \ldots \cdot (X - a_n)$$

mit $b, a_1, \ldots, a_n \in K$.

(iii) Die irreduziblen Polynome in $K[X]$ sind genau die Polynome vom Grad 1.

(iv) Ist L/K eine algebraische Erweiterung, so ist $L = K$.

Beweis
(i) $\Rightarrow$ (ii): Ist $f \in K$, dann ist nichts zu zeigen. Sei $f \in K[X]$ ein nichtkonstantes Polynom, also hat f eine Nullstelle $a \in K$ und wir können f faktorisieren: $f = (X-a)g$ mit $g \in K[X]$. Ist $g \in K$, so sind wir fertig, sonst wende (i) auf g an. Nach $\deg f$ vielen Schritten haben wir die gesuchte Zerlegung erreicht.
(ii) $\Rightarrow$ (iii) ist klar.
(iii) $\Rightarrow$ (iv): Ist $a \in L$, so ist a algebraisch über K, ist also Nullstelle eines irreduziblen normierten Polynoms $f \in K[X]$. Nach (iii) ist f vom Grad 1, also liegt a bereits in K.
(iv) $\Rightarrow$ (i): Sei $f \in K[X]$ nichtkonstant. Der Zerfällungskörper von f ist eine algebraische Erweiterung von K, also bereits gleich K, und damit hat f eine Nullstelle in K. □

Definition 13.6
Ein Erweiterungskörper $\overline{K}$ von K heißt **algebraischer Abschluss** von K, wenn $\overline{K}$ algebraisch abgeschlossen und die Erweiterung $\overline{K}/K$ algebraisch ist.

Wir haben oben bereits gesehen, dass ein algebraisch abgeschlossener Erweiterungskörper L/K stets einen algebraischen Abschluss von K enthält. Wir wollen nun zeigen, dass ein algebraischer Abschluss von K bereits alle algebraischen Erweiterungskörper von K bis auf Isomorphie enthält. Daraus wird die Eindeutigkeit des algebraischen Abschlusses folgen. Anschließend werden wir die Existenz eines algebraischen Abschlusses beweisen.

Satz 13.7
Sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K. Sei L/K eine algebraische Körpererweiterung und Z ein Zwischenkörper der Erweiterung.
Dann lässt sich jeder K-Homomorphismus $\varphi : Z \to \overline{K}$ zu einem K-Homomorphismus $\Phi : L \to \overline{K}$ fortsetzen.
Beweis
Sei A die Menge aller Paare (M,ψ), wobei M ein Zwischenkörper von L/Z und $\psi : M \to \overline{K}$ eine Fortsetzung von φ ist. Da (Z,φ) zu A gehört, ist A nicht leer.
Wir definieren nun eine Halbordnung(!) auf A durch:

$$(M,\psi) \leq (M',\psi') \text{ genau dann, wenn } M \subseteq M' \text{ und } \psi'|_M = \psi .$$

Sei C eine Kette in A. Dann ist $\{M \mid (M,\psi) \in C \text{ für ein geeignetes } \psi\}$ ein Körperturm in L, also ist die Vereinigung L' dieses Körperturms ein Teilkörper von L. Wir wollen nun eine Fortsetzung $\varphi' : L' \to \overline{K}$ definieren. Ist $x \in L'$, so gibt es ein $(M,\psi) \in C$ mit $x \in M$. Wir setzen nun: $\varphi'(x) = \psi(x)$, müssen uns aber noch überlegen, dass dies wohl definiert ist, d.h. nicht von der Wahl von $(M,\psi) \in C$ abhängt. Ist $(M',\psi') \in C$ ein anderes Paar mit $x \in M'$, so sind die beiden Paare vergleichbar, da C eine Kette ist, also $(M,\psi) \leq (M',\psi')$ oder $(M',\psi') \leq (M,\psi)$. Dann folgt $\psi(x) = \psi'(x)$.
Also ist $(L',\varphi') \in A$ eine obere Schranke von C. Damit haben wir nun die Voraussetzungen für die Anwendung des Zornschen Lemmas nachgewiesen und können schließen, dass die Menge A ein maximales Element (M,ψ) besitzt. Wir wollen nun zeigen: $M = L$.
Angenommen, $M \subset L$, dann gibt es also ein $a \in L \setminus M$. Wir konstruieren nun eine Fortsetzung $\psi' : M(a) \to \overline{K}$ von ψ und gehen dabei wie bei der Konstruktion des Zerfällungskörpers vor.
Es sei also $\Psi : M[X] \to \overline{K}[X]$ die durch ψ induzierte Abbildung der Polynomringe. Sei nun $f = \operatorname{minpol}_M a$ und $g = \Psi(f) \in \overline{K}[X]$. Da $\overline{K}$ algebraisch abgeschlossen ist, besitzt g eine Nullstelle $b \in \overline{K}$. Dann ist die Abbildung

$$\sigma : M[X] \to \overline{K}, \ \sum_i c_i X^i \mapsto \sum_i \psi(c_i) b^i$$

ein K-Homomorphismus mit $\sigma(f)=0$. Also ist $(f)\subseteq \operatorname{Kern}\sigma$, und es gibt nach dem Homomorphiesatz einen K-Homomorphismus

$$\sigma' : M[X]/(f) \to \overline{K},\ \sum_i c_i X^i + (f) \mapsto \sum_i \psi(c_i) b^i .$$

Insbesondere ist also $\sigma'|_M = \psi$. Nun ist aber $M[a] \cong M[X]/(f)$ mit $a \mapsto X+(f)$, also erhalten wir durch Hintereinanderausführung einen K-Homomorphismus

$$\psi' : M(a) = M[a] \to \overline{K},\ \psi'|_M = \psi$$

und haben damit ein Element $(M(a),\psi') > (M,\psi)$ in A konstruiert, im Widerspruch zur Maximalität von (M,ψ). Also muss $M=L$ gelten, und die Behauptung ist bewiesen. □

Folgerung 13.8

Ist $\overline{K}$ ein algebraischer Abschluss eines Körpers K, so gibt es für jede algebraische Erweiterung L/K einen K-Monomorphismus $L \to \overline{K}$.

Folgerung 13.9

Sind $\overline{K}$ und L algebraische Abschlüsse eines Körpers K, so gibt es einen K-Isomorphismus $L \to \overline{K}$.

Beweis

Nach der vorhergehenden Folgerung gibt es einen K-Monomorphismus $\psi : L \to \overline{K}$. Mit L ist auch der isomorphe Körper $\psi(L)$ algebraisch abgeschlossen, und $\overline{K}/\psi(L)$ ist eine algebraische Erweiterung. Also muss bereits $\overline{K} = \psi(L)$ sein. □

Nachdem wir die Eindeutigkeit des algebraischen Abschlusses eines Körpers K gezeigt haben, weisen wir nun die Existenz nach:

Satz 13.10 (Steinitz)

Jeder Körper K besitzt einen algebraischen Abschluss.

Beweis

Zunächst produzieren wir einen Erweiterungskörper von K, in dem jedes nichtkonstante Polynom aus $K[X]$ eine Nullstelle hat. Setze $\Lambda = K[X]\setminus K$. Wir wählen nun für jedes Polynom $f\in\Lambda$ eine Unbestimmte X_f und bilden den Polynomring $R = K[\{X_f\}_{f\in\Lambda}]$. Sei I das von den Elementen $f(X_f)\in R$ erzeugte Ideal von R.

Falls $I = R$, dann gibt es eine Darstellung

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

mit $g_1,\dots,g_n \in R$, $f_1,\dots,f_n \in \Lambda$.

Sei nun L ein Erweiterungskörper von K, in dem jedes f_i eine Nullstelle a_i besitzt ($i=1,\dots,n$). Wir betrachten den Einsetzungshomomorphismus $\varphi : R \to L$ mit $\varphi(X_{f_i}) = a_i$ für $i=1,\dots,n$ und $\varphi(X_f)=0$ für $f \notin \{f_1,\dots,f_n\}$. Wenden wir φ auf $\circledast$ an, so erhalten wir

$$1 = \varphi(1) = \sum_{i=1}^{n} \varphi(g_i)\varphi(f_i(X_{f_i})) = \sum_{i=1}^{n} \varphi(g_i) f_i(a_i) = 0 .$$

– Widerspruch!

Also ist $I \subset R$, und daher gibt es ein maximales Ideal $\mathcal{M}$ von R, das I enthält. Dann ist $K_1 = R/\mathcal{M}$ ein Körper. K_1 enthält K (bis auf Isomorphie), denn wegen $1\notin\mathcal{M}$ ist die Abbildung $K \to K_1$, $a \mapsto a+\mathcal{M}$ ein Monomorphismus. Wir identifizieren $a\in K$ mit $a+\mathcal{M}\in K_1$. Für $f\in\Lambda$ gilt nun:

$$f(X_f+\mathcal{M}) = f(X_f)+\mathcal{M} = \mathcal{M},$$

d.h. f hat in K_1 die Nullstelle $X_f + \mathcal{M}$. Insbesondere lernen wir daraus auch, dass K_1/K eine algebraische Körpererweiterung ist.
Wir iterieren dieses Verfahren nun. Dann erhalten wir eine Kette

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq ...$$

von algebraischen Körpererweiterungen, so dass jedes nichtkonstante Polynom aus $K_i[X]$ eine Nullstelle in K_{i+1} besitzt.
Wir setzen nun $\overline{K} = \bigcup_{i=0}^{\infty} K_i$ und stellen fest, dass $\overline{K}$ als Vereinigung eines Körperturms wieder eine Körperstruktur besitzt.
Da die Erweiterungen K_i/K_{i-1} algebraisch sind, sind auch die Erweiterungen K_i/K algebraisch, und damit ist auch $\overline{K}/K$ algebraisch.
Ist $f \in \overline{K}[X]$ ein nichtkonstantes Polynom, so liegt f bereits in einem $K_i[X]$, da f nur endlich viele von Null verschiedene Koeffizienten hat.
Also hat f eine Nullstelle in $K_{i+1} \subseteq \overline{K}$, d.h. $\overline{K}$ ist algebraisch abgeschlossen. □

Kapitel 14

Normale und galoissche Erweiterungen

In dem vorhergehenden Paragraphen haben wir bereits Zusammenhänge zwischen einem Polynom f in $K[X]$ und den K-Automorphismen des Zerfällungskörpers, d.h. der Gruppe $G\left(L/K\right)$, untersucht. Dies wird im Rahmen der Galoistheorie weiter vertieft.

Eine leichte Variation des Beweises von Satz 11.7 bzw. Lemma 11.8 zeigt:

Lemma 14.1
Seien L_1 , L_2 Körper, $\sigma : L_1 \to L_2$ ein Ringmonomorphismus mit induziertem Homomorphismus $\Sigma : L_1[X] \to L_2[X]$. Sei $L_1\langle a\rangle$ eine einfache algebraische Erweiterung von L_1, $f = \operatorname{minpol}_{L_1} a$, $\tilde{f} = \Sigma(f)$. Hat $\tilde{f}$ genau m verschiedene Nullstellen in L_2, dann hat σ genau m verschiedene Fortsetzungen zu einem Homomorphismus $\overline{\sigma} : L_1\langle a\rangle \to L_2$ (die jeweils a auf eine Nullstelle von $\tilde{f}$ abbilden).

Mit $L_1 = K$, $L_2 = L = K\langle a\rangle$, σ die Einbettung $K \subseteq L$, folgt daraus:

Folgerung 14.2
Ist $L = K\langle a\rangle$ eine einfache algebraische Erweiterung des Körpers K, $f = \operatorname{minpol}_K a$, dann ist $\left|G\left(L/K\right)\right|$ gleich der Zahl der verschiedenen Nullstellen von f in L.

Beispiel 14.3

(i) Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ quadratfrei, $d \notin \{0,1\}$. Dann hat $f = \operatorname{minpol}_{\mathbb{Q}} \sqrt{d} = X^2 - d$ in L genau die beiden Nullstellen $\sqrt{d}$ und $-\sqrt{d}$, also hat die Körpererweiterung L/K genau zwei $\mathbb{Q}$-Automorphismen, nämlich die durch
$$\sqrt{d} \mapsto \sqrt{d} \text{ (Identität), bzw. } \sqrt{d} \mapsto -\sqrt{d} \text{ (Konjugation)}$$
gegebenen Automorphismen. Die Konjugationsabbildung bildet ein allgemeines Element $a_0 + a_1\sqrt{d} \in L$ auf $a_0 - a_1\sqrt{d}$ ab.

(ii) Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, $a = \sqrt[3]{2}$. Dann ist $f = \operatorname{minpol}_{\mathbb{Q}} a = X^3 - 2$. Mit $\rho = e^{2\pi i/3}$ hat f die Nullstellen a, $a\rho$ und $a\rho^2$ in seinem Zerfällungskörper über $\mathbb{Q}$, aber nur die Nullstelle a liegt in L. Also ist hier $G\left(L/K\right) = \{\mathrm{id}\}$.

Satz 14.4
Sei L/K eine endliche Körpererweiterung. Dann gilt:

(i) $\left|G\left(L/K\right)\right| \leq |L : K|$.

(ii) L/K ist genau dann eine separable Erweiterung, wenn es $|L : K|$ verschiedene K-Einbettungen von L in den algebraischen Abschluss $\overline{K}$ gibt.

Beweis

(i) Es ist $L = K(a_1,...,a_n)$ für geeignete $a_1,...,a_n \in L$. Wende nun Lemma 14.1 iterativ auf die Erweiterungen $K(a_1,...,a_n)/K(a_1,...,a_i)$ und ihre Einbettungen nach L an.

(ii) Ist L/K separabel, so sind es auch alle Erweiterungen von Zwischenkörpern von L/K, also haben alle in (i) auftretenden Minimalpolynome lauter verschiedene Nullstellen, und es gibt stets so viele Fortsetzungen wie der Grad angibt, also gibt es $|L:K|$ verschiedene K-Einbettungen von L nach $\overline{K}$.
Sei nun L/K inseparabel. Wähle $a \in L$ inseparabel über K. Dann hat sein Minimalpolynom f weniger als $\deg f$ verschiedene Nullstellen in seinem Zerfällungskörper, also auch in $\overline{K}$. Daher gibt es weniger als $d = \deg f$ Einbettungen von $K(a)$ in $\overline{K}$, und damit insgesamt weniger als $d \cdot \frac{|L:K|}{d} = |L:K|$ Einbettungen von L in $\overline{K}$. □

Aus dem Beweis des vorherigen Satzes folgt auch:

Folgerung 14.5

Sei $L = K(a_1,...,a_t)$, wobei jeweils a_i separabel über $K(a_1,...,a_{i-1})$ ist, für $i = 1,...,t$. Dann ist L/K separabel.

Damit folgt allgemein die Transitivität der Separabilität:

Folgerung 14.6

Sind M/L und L/K separabel algebraische Erweiterungen, so ist auch M/K separabel algebraisch.

Beweis

Sei $a \in M$, $X^n + a_{n-1}X^{n-1} + ... + a_0$ das Minimalpolynom von a über L. Dann ist a auch separabel über $L' = K(a_0,...,a_{n-1})$ und L' ist über K separabel. Nach der vorhergehenden Folgerung ist also $L'(a)$ separabel über K, und damit ist a separabel über K. □

Für die Galoistheorie spielen besonders die Körpererweiterungen eine Rolle, in denen mit einer Nullstelle eines irreduziblen Polynoms auch die anderen Nullstellen zu finden sind:

Definition 14.7

Eine Körpererweiterung L/K heißt **normal**, wenn sie algebraisch ist, und wenn außerdem jedes irreduzible Polynom $f \in K[X]$, das eine Nullstelle in L hat, bereits über L vollständig in Linearfaktoren zerfällt.

Beispiel 14.8

(i) $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ ist eine normale Erweiterung.

(ii) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist offenbar nicht normal.

(iii) $\mathbb{C}/\mathbb{R}$ ist eine normale Erweiterung, da jedes Polynom aus $\mathbb{R}[X]$ über $\mathbb{C}$ vollständig in Linearfaktoren zerfällt.

Normale Körpererweiterungen lassen sich als Zwischenkörper von Polynommengen charakterisieren:

Satz 14.9

Sei L/K eine algebraische Körpererweiterung, $\overline{L}$ der algebraische Abschluss von L (und damit auch von K). Dann sind äquivalent:

(i) L/K ist normal.

(ii) Es gibt eine Menge $M \subseteq K[X]$ von Polynomen, so dass L aus K durch Adjunktion der Nullstellen in $\overline{L}$ der Polynome in M entsteht.

(iii) Für jeden K-Homomorphismus $\sigma : L \to \overline{L}$ gilt $\sigma(L) = L$.

Beweis

(i) $\Rightarrow$ (ii): Sei $M = \{\operatorname{minpol}_K a \mid a \in L\} \subseteq K[X]$. Da L/K normal ist, sind bereits alle Nullstellen in $\overline{L}$ der Polynome in M in L enthalten, und offenbar tritt sogar jedes Element aus L als Nullstelle eines $f \in M$ auf.

(ii) $\Rightarrow$ (iii): Sei N die Menge der Nullstellen der Polynome in M. Jeder K-Homomorphismus $\sigma : L \to \overline{L}$ muss die Menge N in sich abbilden, da die von σ induzierte Abbildung auf $L[X]$ den Polynomring $K[X]$ in sich abbildet. Da σ injektiv ist, bildet σ für ein gegebenes Polynom $f \in M$ die Nullstellenmenge von f auf sich ab, d.h. es gilt sogar $\sigma(N) = N$. Da $L = K(N)$ ist, folgt somit $\sigma(L) = L$.

(iii) $\Rightarrow$ (i): Sei $f \in K[X]$ irreduzibel und a eine Nullstelle von f in L. Ist $b \in \overline{L}$ eine weitere Nullstelle von f, dann gibt es einen K-Homomorphismus $\sigma' : K(a) \to \overline{L}$ mit $\sigma'(a) = b$. Nach Satz 13.7 lässt sich σ' zu einem K-Homomorphismus $\sigma : L \to \overline{L}$ fortsetzen. Nach (iii) gilt $\sigma(L) = L$, also ist $b \in L$. □

Aus den Beschreibungen in (ii) oder (iii) können wir nun für den Fall endlicher Erweiterungen folgende schöne Charakterisierung der Normalität ableiten:

Satz 14.10

Sei L/K eine endliche Körpererweiterung. Dann ist L/K genau dann normal, wenn L der Zerfällungskörper eines Polynoms $f \in K[X]$ ist.

Aus Satz 14.9 folgt auch:

Folgerung 14.11

Ist L/K normal und Z ein Zwischenkörper von L/K, so ist auch L/Z normal.

Bemerkung 14.12

Normalität ist keine transitive Eigenschaft, d.h. sind L/Z und Z/K normale Körpererweiterungen, so ist L/K i.A. nicht normal!

Wir betrachten dazu folgendes Beispiel. Sei $K = \mathbb{Q}$, dann ist $Z = \mathbb{Q}(\sqrt{2})$ als Zerfällungskörper des in $\mathbb{Q}[X]$ irreduziblen Polynoms $X^2 - 2$ eine normale Erweiterung von $\mathbb{Q}$. Über Z ist das Polynom $X^2 - \sqrt{2}$ irreduzibel. Sein Zerfällungskörper über Z ist $L = \mathbb{Q}(\sqrt[4]{2})$, also ist L/Z normal. L/K ist dagegen nicht normal, denn das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $f = X^4 - 2$, und f zerfällt über L nicht in Linearfaktoren. Der Zerfällungskörper von f ist $\mathbb{Q}(\sqrt[4]{2}, i)$, denn f hat die Nullstellen $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$.

Wir führen nun einen zentralen Begriff der Körpertheorie ein, der auf Galois zurückgeht (für $K = \mathbb{Q}$). Er konnte damit einige schwierige Probleme in der Theorie der algebraischen Gleichungen lösen.

Definition 14.13

Eine Körpererweiterung L/K heißt **galoissch**, wenn sie endlich, normal und separabel ist. Die Gruppe $G(L/K)$ heißt dann die **Galoisgruppe** von L/K.

Satz 14.14

Ist $f \in K[X]$ ein separables Polynom, dann ist sein Zerfällungskörper L über K separabel (14.5), also ist L/K galoissch. Die Galoisgruppe $G(f) = G\left(L/K\right)$ von f ist dann also die Galoisgruppe der galoisschen Erweiterung L/K.

Beweis

Da f separabel ist, ist nach Folgerung 11.11 $\left|G\left(L/K\right)\right| = |L : K|$. Nach Definition eines Zerfällungskörpers ist für L die Bedingung in Satz 14.4 (ii) erfüllt, also ist L/K separabel. □

Auch für Galoiserweiterungen gibt es gute Charakterisierungen:

Satz 14.15

Für eine Körpererweiterung L/K sind folgende Aussagen äquivalent:

(i) L/K ist galoissch.

(ii) L ist der Zerfällungskörper eines separablen Polynoms aus $K[X]$.

(iii) L/K ist endlich und $\left|G\left(L/K\right)\right| = |L : K|$.

Beweis

(i) $\Rightarrow$ (ii): Ist L/K galoissch, dann ist L/K normal, also ist L nach Satz 14.10 Zerfällungskörper eines Polynoms $f \in K[X]$. Da L/K auch separabel ist, ist f außerdem separabel.

(ii) $\Rightarrow$ (iii): Ist L der Zerfällungskörper eines separablen Polynoms, so gibt es nach Folgerung 11.11 genau $|L : K|$ verschiedene K-Automorphismen von L, also ist dann $\left|G\left(L/K\right)\right| = |L : K|$.

(iii) $\Rightarrow$ (i): Jeder K-Automorphismus von L liefert eine Einbettung von L nach $\overline{L} = \overline{K}$. Da es $\left|G\left(L/K\right)\right| = |L : K|$ solche Einbettungen gibt, ist L/K nach Satz 14.4 (ii) separabel. Außerdem folgt aus diesem Satz, dass alle Einbettungen von L in $\overline{K}$ auf diese Weise aus K-Automorphismen von L entstehen. Dann ist aber die Bedingung (iii) in Satz 14.9 erfüllt, also ist L/K normal. Damit ist insgesamt L/K als galoissch nachgewiesen. □

Da für Körper der Charakteristik 0 alle Polynome separabel sind, folgt auch:

Folgerung 14.16

Die Galoiserweiterungen eines Körpers K der Charakteristik 0 sind genau die Zerfällungskörper der Polynome aus $K[X]$.

Aus der Charakterisierung in (ii) oben folgt sofort:

Folgerung 14.17

Ist Z ein Zwischenkörper einer Galoiserweiterung L/K, dann ist auch L/Z galoissch.

Sei f ein separables Polynom über einem Körper K, L der Zerfällungskörper von f über K. Dann können wir nach den bisherigen Ergebnissen Folgendes über die Galoisgruppe $G(f)$ sagen:

Jedes Element $\alpha \in G(f)$ permutiert die Nullstellen von f und ist durch diese Permutation eindeutig bestimmt. Hat f n verschiedene Nullstellen, so ist also $G(f)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n vom Grad n. Wir werden $G(f)$ stets mit der entsprechenden Untergruppe von S_n identi-

fizieren. Insbesondere ist nicht nur $|G(f)| = |L:K| \leq n!$, wie wir bereits früher gesehen haben, sondern es gilt sogar die Teilbarkeitsbeziehung

$$|G(f)| = |L:K| | n!,$$

da die Ordnung einer Untergruppe in einer endlichen Gruppe nach dem Satz von Lagrange (siehe Lineare Algebra I) stets die Ordnung der Gruppe teilt.
Genauer wissen wir, dass $\sigma \in G(f)$ die Nullstellen der irreduziblen Faktoren von f jeweils unter sich permutiert.
Für ein irreduzibles Polynom gilt darüber hinaus:

Satz 14.18

Ist $f \in K[X]$ irreduzibel und separabel, dann operiert $G(f)$ transitiv auf den Nullstellen von f, d.h. dass es zu beliebigen Nullstellen a,b von f stets ein $\sigma \in G(f)$ mit $\sigma(a) = b$ gibt.

Beweis

Sind a,b zwei Nullstellen von f, dann gibt es einen K-Isomorphismus $K(a) \to K(b)$, der a auf b abbildet (Lemma 11.8). Ist L der Zerfällungskörper von f über K, dann lässt sich dieser Isomorphismus nach Satz 11.7 zu einem K-Isomorphismus $\sigma : L \to L$ fortsetzen. Also ist $\sigma \in G(f)$ ein Element der Galoisgruppe mit $\sigma(a) = b$. □

Bemerkung 14.19

(i) Die Separabilität von f wird für die transitive Operation von $G\left(L/K\right)$ nicht benötigt. Wir hatten dies aber in der Definition der Galoisgruppe $G(f)$ vorausgesetzt.

(ii) Für ein irreduzibles separables Polynom f können wir auch die numerische Aussage über die Ordnung von $G(f)$ ergänzen. Ist f vom Grad n, a eine Nullstelle, so ist $K(a) \subseteq L$, also teilt $n = |K(a):K|$ die Ordnung $|G(f)| = |L:K|$.

Beispiel 14.20

(i) Das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und hat die Nullstellen $a = \sqrt[3]{2}$, aw, aw^2, mit $w = e^{2\pi i/3}$. Wir haben bereits gesehen, dass $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht normal, also damit nicht galoissch ist. Der Zerfällungskörper L von f über $\mathbb{Q}$ ist $L = \mathbb{Q}(a,w)$. Die Erweiterung $L/\mathbb{Q}$ ist nach den Ergebnissen dieses Paragraphen galoissch mit Galoisgruppe $G(f) = G\left(L/\mathbb{Q}\right)$. Wir haben uns bereits überlegt, dass gilt: $|L:\mathbb{Q}| = 6 = |G(f)|$. Außerdem haben wir bereits erkannt: $G(f) \cong S_3$, d.h. jede Permutation der Nullstellen von f definiert einen $\mathbb{Q}$-Automorphismus von L.

(ii) Das Polynom $f = X^4 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und hat die Nullstellen $a = \sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ und $-i\sqrt[4]{2}$. Der Zerfällungskörper L von f über $\mathbb{Q}$ ist $L = \mathbb{Q}(a,i)$. Die Erweiterung $L/\mathbb{Q}$ ist galoissch mit Galoisgruppe $G(f) = G\left(L/\mathbb{Q}\right)$ von der Ordnung $|G(f)| = |L:\mathbb{Q}| = 8$. Andererseits ist $G(f)$ eine Untergruppe von S_4. In diesem Fall definiert also nicht jede Permutation der 4 Nullstellen von f einen $\mathbb{Q}$-Automorphismus von L. Der Grund liegt darin, dass es algebraische Relationen zwischen den Nullstellen gibt, in diesem Fall besonders einfache. Ist $\sigma \in G\left(L/\mathbb{Q}\right)$, dann gilt $\sigma(-a) = -\sigma(a)$, also ist das Bild der Nullstelle $-a$ bereits durch das Bild von a festgelegt, und daher ist nicht jede Permutation der Nullstellen mit Galoisautomorphismen möglich.

Für Polynome größeren Grades ist die Struktur der Galoisgruppe i.A. wesentlich komplizierter, und es ist nützlich, tiefere Kenntnisse aus der Galoistheorie zur Verfügung zu haben. Der im nächsten Paragraphen zu behandelnde Hauptsatz der Galoistheorie zeigt, dass zwischen einer galoisschen Körpererweiterung und der

zugehörigen Galoisgruppe eine enge Verbindung besteht. Die Kenntnis der Struktur der Galoisgruppe wird dann eingesetzt, um Fragen aus der Körpertheorie bzw. über die Auflösung algebraischer Gleichungen zu beantworten.

Im Fall einer algebraischen Körpererweiterung, die nicht normal ist, hilft häufig ein geeigneter Abschlussoperator weiter:

Satz 14.21

Sei L/K eine algebraische Körpererweiterung. Dann gibt es eine Körpererweiterung N/L mit folgenden Eigenschaften:

(i) Die Erweiterung N/K ist normal.

(ii) Ist Z ein Zwischenkörper von N/L, für den Z/K normal ist, so gilt $Z = N$.

Der Körper N ist bis auf L-Isomorphie durch die Eigenschaften (i) und (ii) eindeutig bestimmt.

Beweis

Für $a \in L$ sei $f_a \in K[X]$ das Minimalpolynom von a über K. Sei N der durch Adjunktion der Nullstellen aller f_a in $\overline{L}$ an L entstehende Körper. Nach Satz 14.9 hat N die Eigenschaften (i) und (ii).

Ist N' ein weiterer Körper mit diesen Eigenschaften, dann gibt es eine Einbettung $\sigma : N' \to \overline{L}$, und es muss $\sigma(N') = N$ sein. □

Definition 14.22

Ein Körper N mit den Eigenschaften (i) und (ii) in der obigen Situation heißt eine **normale Hülle** von L/K.

Nicht nur die normalen Hüllen, auch ihre K-Automorphismengruppen sind eindeutig bestimmt (bis auf Isomorphie). Seien N und N' normale Hüllen von L/K und $\sigma : N \to N'$ ein L-Isomorphismus. Dann induziert σ einen Gruppenisomorphismus

$$G\left(N/K\right) \to G\left(N'/K\right),\ \alpha \mapsto \sigma\alpha\sigma^{-1}.$$

Also ist auch $G\left(N/K\right)$ unabhängig von der speziellen Wahl der normalen Hülle.

Kapitel 15

Der Hauptsatz der Galoistheorie (Teil 1)

Wir haben bereits gesehen, dass für die Lösung von Konstruktionsproblemen und für die Auflösung algebraischer Gleichungen durch Radikale die Kenntnis von Zwischenkörpern in einer gegebenen Körpererweiterung entscheidend ist. Der Hauptsatz der Galoistheorie besagt, dass in Galoiserweiterungen die Struktur des Zwischenkörperverbandes an der Untergruppenstruktur der Galoisgruppe abgelesen werden kann. Der Vorteil ist, dass damit das Rechnen in unendlichen Körpern durch die Handhabung einer endlichen Gruppe ersetzt werden kann. Mit der Theorie endlicher Gruppen, die auch für viele andere Anwendungen nützlich ist, werden wir uns dann noch befassen.
Im Folgenden sei stets G eine (multiplikative) Gruppe, K ein Körper und $K^* = K \setminus \{0\}$ die multiplikative Gruppe von K. In dieser Situation definieren wir:

Definition 15.1
Ein (linearer) **Charakter** von G in K ist ein Gruppenhomomorphismus $\sigma : G \to K^*$.

Bemerkung 15.2
In der Charaktertheorie sind Charaktere von Gruppen allgemeiner definiert. Die obigen Charaktere sind dann speziell die Charaktere vom Grad 1.

Beispiel 15.3
(i) Ist $\sigma : L \to K$ ein Ringhomomorphismus zwischen zwei Körpern K und L, $\sigma \neq 0$, so liefert die Einschränkung auf L^* einen Charakter $\sigma^* : L^* \to K^*$. Insbesondere liefert jeder Automorphismus von L einen Charakter der Gruppe L^*.

(ii) Ist G eine Gruppe der invertierbaren $n \times n$-Matrizen über einem Körper K (mit der üblichen Matrizenmultiplikation als Verknüpfung), dann ist die Determinantenabbildung
$$\det : G \to K^*,\ A \mapsto \det A$$
ein Gruppenhomomorphismus, also ein Charakter von G.

(iii) $\mathrm{sgn} : S_n \to \mathbb{Q}^*$ ist der Signumcharakter der symmetrischen Gruppe S_n.

Satz 15.4 (Lineare Unabhängigkeit von Charakteren)
Seien $\sigma_1,...,\sigma_n$ verschiedene Charaktere von G in K. Dann sind $\sigma_1,...,\sigma_n$ linear unabhängig über K, d.h. sind $a_1,...,a_n \in K$ mit $\sum_{i=1}^n a_i\sigma_i = 0$, also
$$\sum_{i=1}^n a_i\sigma_i(x) = 0 \text{ für alle } x \in G, \qquad \circledast$$
dann muss bereits $a_1 = ... = a_n = 0$ gelten.

Beweis
Wir beweisen die Aussage durch Induktion nach n. Für $n = 1$ ist sie offenbar richtig, da $\sigma_1(x) \in K^*$ für $x \in G$.

Sei also $n > 1$ und die Behauptung bis $n-1$ bereits gezeigt. Da $\sigma_1 \neq \sigma_n$, gibt es ein $y \in G$ mit $\sigma_1(y) \neq \sigma_n(y)$. Multiplikation von $\circledast$ mit $\sigma_n(y)$ liefert

$$\sum_{i=1}^{n} a_i \sigma_n(y)\sigma_i(x) = 0 \text{ für alle } x \in G .$$

Andererseits gilt $\circledast$ aber auch für alle $yx \in G$, also ist

$$\sum_{i=1}^{n} a_i \sigma_i(y)\sigma_i(x) = 0 \text{ für alle } x \in G .$$

Subtraktion liefert nun

$$\sum_{i=1}^{n-1} a_i(\sigma_n(y) - \sigma_i(y))\sigma_i(x) = 0 \text{ für alle } x \in G .$$

Nach Induktionsvoraussetzung müssen hierin alle Koeffizienten 0 sein, also folgt (wegen $\sigma_1(y) \neq \sigma_n(y)$) $a_1 = 0$. Dann ist die Gleichung $\circledast$ aber eine Gleichung in der höchstens $n-1$ Charaktere involviert sind, also müssen nach Induktionsvoraussetzung auch alle anderen a_i gleich 0 sein. □

Für den Beweis des nächsten Satzes brauchen wir noch weitere wichtige Begriffe:

Definition 15.5

Sei K ein Körper und G eine endliche Untergruppe der Automorphismengruppe $\mathrm{Aut}(K)$ von K. Dann heißt die Abbildung

$$\mathrm{tr}_G : K \to K,\ a \mapsto \sum_{\sigma \in G} \sigma(a)$$

die **G-Spur in K**.

Ist L/K eine Galoiserweiterung und $G = G(L/K)$, dann heißen für $a \in L$ die Elemente $\sigma(a)$, $\sigma \in G$, die **Konjugierten** von a.

Bemerkung 15.6

(i) Ist P der Primkörper von K, dann ist $\mathrm{Aut}(K) = G(K/P)$.

(ii) Ist L/K eine Galoiserweiterung und $G = G(L/K)$, dann sind die Konjugierten von $a \in L$ genau die Nullstellen des Minimalpolynoms $f = \mathrm{minpol}_K a$ (das über L vollständig in Linearfaktoren zerfällt!). Es ist daher $\mathrm{tr}_G(a) \in K$.

(iii) Die komplexe Konjugation ist ein Automorphismus auf $\mathbb{C}$. Sei G die von der Konjugation erzeugte Untergruppe der Ordnung 2 von $\mathrm{Aut}(\mathbb{C})$. Dann ist $\mathrm{tr}_G(z) = z + \overline{z}$ für $z \in \mathbb{C}$.

Lemma 15.7

Sei K ein Körper, G eine endliche Untergruppe von $\mathrm{Aut}(K)$. Dann gilt $\mathrm{tr}_G(K) \neq 0$, und somit $\tau(\mathrm{tr}_G(a)) = \mathrm{tr}_G(a)$ für alle $\tau \in G$, $a \in K$.

Beweis

Wäre $\mathrm{tr}_G(K) = 0$, dann wäre $\sum_{\sigma \in G} \sigma$ die Nullabbildung, im Widerspruch zum vorhergehenden Satz 15.4. Sei $\tau \in G$, $a \in K$, dann ist

$$\tau\Big(\sum_{\sigma \in G} \sigma(a)\Big) = \sum_{\sigma \in G} \tau(\sigma(a)) = \sum_{\sigma \in G} \sigma(a),$$

da mit σ auch $\tau\sigma$ über die ganze Gruppe G läuft. □

Wir wollen diese Ergebnisse im Beweis des folgenden Satzes verwenden, der für den Hauptsatz der Galoistheorie grundlegend ist und wichtige Konzepte einführt.

Satz 15.8 (E. Artin)

Sei G eine endliche Untergruppe der Automorphismengruppe eines Körpers L. Sei $K = \{ x \in L \mid \sigma(x) = x \text{ f.alle } \sigma \in G \}$. Dann gilt:

(i) K ist ein Teilkörper von L mit $|L : K| = |G|$.

(ii) Die Erweiterung L/K ist galoissch und $G\big(L/K\big) = G$.

Beweis

Sei $|G| = n$, $G = \{\sigma_1,...,\sigma_n\}$. Da $G \subseteq \mathrm{Aut}(L)$, ist K ein Teilkörper von L. Nach Definition von K lassen die Elemente von G außerdem K elementweise fest, also gilt $G \subseteq G\big(L/K\big)$.

Wir zeigen zunächst, dass $|L : K| \geq n$ ist. Setze $r = |L : K|$, und sei $\{w_1,...,w_r\}$ eine K-Basis von L. Ist $r < n$, dann hat das lineare Gleichungssystem

$$\sum_{i=1}^{n} \sigma_i(w_k) X_i = 0\,,\ k = 1,...,r$$

eine nichttriviale Lösung $(a_1,...,a_n) \in L^n$, also

$$\sum_{i=1}^{n} \sigma_i(w_k) a_i = 0\,,\ k = 1,...,r\,.$$

Ist $x \in L$, dann gibt es $l_1,...,l_r \in K$ mit $x = \sum_{k=1}^{r} l_k w_k$. Also ist

$$0 = \sum_{k=1}^{r} l_k \sum_{i=1}^{n} \sigma_i(w_k) a_i = \sum_{i=1}^{n} a_i \sigma_i\Big(\sum\nolimits_{k=1}^{r} l_k w_k\Big) = \sum_{i=1}^{n} a_i \sigma_i(x)$$

für alle $x \in L$. Da die Elemente aus G als Charaktere von L^* aufgefasst werden können, widerspricht die Gleichung $\sum_{i=1}^{n} a_i \sigma_i = 0$ aber der linearen Unabhängigkeit der Charaktere $\sigma_1,...,\sigma_n$. Also ist $|L : K| \geq n$.

Wir zeigen nun, dass für $m > n$ je m Elemente von L über K linear unabhängig sind, was dann $|L : K| = n$ beweist.

Seien also $y_1,...,y_m \in L$, $m > n$. Wir betrachten das lineare Gleichungssystem

$$\sum_{k=1}^{m} \sigma_i^{-1}(y_k) X_k = 0\,,\ i = 1,...,n\,.$$

Wegen $m > n$ gibt es eine nichttriviale Lösung $(a_1,...,a_m) \in L^m$. Durch Umnummerierung können wir erreichen, dass $a_1 \neq 0$ ist. Nach Lemma 15.7 gibt es ein $a \in L$ mit $\mathrm{tr}_G(a) \neq 0$. Da für jedes $z \in L$ auch $z \cdot (a_1,...,a_m)$ eine Lösung obigen Gleichungssystems ist, können wir also auch annehmen, dass $\mathrm{tr}_G(a_1) \neq 0$ gilt.

Wir setzen nun unsere Lösung in das obige System ein, wenden auf die i-te Gleichung den Automorphismus σ_i an und addieren dann alle Gleichungen:

$$0 = \sum_{i=1}^{n} \sigma_i\Big(\sum\nolimits_{k=1}^{m} \sigma_i^{-1}(y_k) a_k\Big) = \sum_{k=1}^{m} y_k \sum_{i=1}^{n} \sigma_i(a_k) = \sum_{k=1}^{m} \mathrm{tr}_G(a_k)\, y_k\,.$$

Da die Elemente $\mathrm{tr}_G(a_k)$ alle in K liegen, folgt daraus die lineare Abhängigkeit von $y_1,...,y_m$ über K. Damit ist nun $|G| = |L : K|$ bewiesen.

Nach Satz 14.3 ist stets $\big|G\big(L/K\big)\big| \leq |L : K|$. Da $G \subseteq G\big(L/K\big)$, muss also nun $G = G\big(L/K\big)$ sein. Aus Satz 14.15 folgt, dass L/K galoissch ist. □

Vor der Formulierung des Hauptsatzes der Galoistheorie halten wir einige Bezeichnungen fest und führen noch einige Notationen ein.

Es sei L/K eine Galoiserweiterung und $G = G\big(L/K\big)$. Wir setzen

$$\mathcal{Z} = \big\{ Z \mid Z \text{ Zwischenkörper der Erweiterung } L/K \big\},$$
$$\mathcal{U} = \{ U \mid U \text{ Untergruppe von } G \}.$$

Für $U \in \mathcal{U}$ heißt $L_U = \{ a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in U \}$ der **Fixkörper** von U. Offenbar ist dann $L_U \in \mathcal{Z}$. Wir definieren $\Phi : \mathcal{U} \to \mathcal{Z}$ durch $U \mapsto L_U$.

Für einen Zwischenkörper $Z \in \mathcal{Z}$ heißt $G_Z = \{\sigma \in G \mid \sigma(a) = a \text{ für alle } a \in Z\}$ der **Stabilisator** oder auch die **Isotropiegruppe** von Z. Es sei $\Psi : \mathcal{Z} \to \mathcal{U}$ definiert durch $Z \mapsto G_Z$.

Satz 15.9 (Hauptsatz der Galoistheorie, Teil 1)

In der obigen Situation gilt:

(i) Φ und Ψ sind zueinander inverse Bijektionen. Die Zwischenkörper von L/K entsprechen also eindeutig den Untergruppen der Galoisgruppe $G = G\left(L/K\right)$.

(ii) Die Abbildungen Φ und Ψ sind inklusionsumkehrend, d.h. für $Z_1 \subseteq Z_2$ in $\mathcal{Z}$ ist $G_{Z_1} \supseteq G_{Z_2}$, und für $U_1 \subseteq U_2$ in $\mathcal{U}$ ist $L_{U_1} \supseteq L_{U_2}$.

(iii) Für $Z \in \mathcal{Z}$ ist $|G_Z| = |L : Z|$ und $G_Z = G\left(L/Z\right)$ ist die Galoisgruppe von L/Z. Insbesondere ist $G_K = G$.

(iv) Für $U \in \mathcal{U}$ ist $|L : L_U| = |U|$. Insbesondere ist $L_G = K$.

Beweis

Für $Z \in \mathcal{Z}$ ist $G_Z = G\left(L/Z\right)$ nach Definition von G_Z. Es ist klar, dass $Z \subseteq L_{G_Z} = Z'$ gilt. Nach Satz 15.8 ist $|G_Z| = |L : Z'|$. Andererseits ist nach Folgerung 14.17 L/Z galoissch, und daher ist nach Satz 14.15 $\left|G\left(L/Z\right)\right| = |L : Z|$. Damit folgt insgesamt $|L : Z| = |L : Z'|$, und daher ist $Z = Z'$. Das zeigt $\Phi \cdot \Psi = \mathrm{id}_{\mathcal{Z}}$.

Für $U \in \mathcal{U}$ ist nach Satz 15.8 $|U| = |L : L_U|$ und $U = G\left(L/L_U\right) = G_{L_U}$. Also ist auch $\Psi \cdot \Phi = \mathrm{id}_{\mathcal{U}}$.

Die Aussagen (i), (iii) und (iv) sind damit bewiesen, (ii) ist offensichtlich. □

Folgerung 15.10

Jede endliche separable Körpererweiterung L/K besitzt nur endlich viele Zwischenkörper.

Beweis

Sei $L = K(a_1,\ldots,a_n)$, f das Produkt der Minimalpolynome der a_i über K, und sei N der Zerfällungskörper von f über K. Nach Voraussetzung ist f separabel, also ist N/K galoissch. Da nach dem Hauptsatz N/K nur endlich viele Zwischenkörper besitzt, gilt dies erst recht für L/K. □

Bemerkung 15.11

Die obige Folgerung ist im inseparablen Fall i.A. nicht richtig.

Aus der obigen Folgerung und dem nachfolgenden Satz ergibt sich ein wichtiger Struktursatz für endliche separable Erweiterungen: solche Erweiterungen sind einfach (Satz vom primitiven Element). Wir wollen zunächst die algebraischen Erweiterungen für den Fall eines unendlichen Grundkörpers untersuchen. Später werden wir sehen, dass für endliche Grundkörper die Aussage auch richtig ist.

Satz 15.12

Sei K ein unendlicher Körper, und sei L/K eine algebraische Körpererweiterung. Dann ist L/K genau dann einfach, wenn L/K nur endlich viele Zwischenkörper besitzt.

Beweis

Sei zunächst $L = K(a)$ einfach.

Wir ordnen jedem Zwischenkörper Z von L/K das Minimalpolynom f_Z von a über Z zu. Dies ist ein normiertes Polynom, das f_K teilt, also gibt es nur endlich viele verschiedene Polynome f_Z. Wir zeigen nun, dass f_Z den Zwischenkörper Z eindeutig bestimmt, woraus dann die Behauptung folgt.

Sei $f_Z = \sum_{i=0}^{d} c_i X^i$, $c_0,...,c_d \in Z$. Setze $Z' = K(c_0,...,c_d)$. Dann ist $Z' \subseteq Z$, und f_Z ist auch irreduzibel über Z' . Weiter ist $L = K\langle a\rangle = Z'\langle a\rangle = Z\langle a\rangle$, also ist $|L:Z| = |L:Z'|$ und damit $Z = Z' = K(c_0,...,c_d)$, d.h. Z ist durch die Koeffizienten von f_Z bestimmt.
Sei nun umgekehrt die Menge der Zwischenkörper als endlich vorausgesetzt. Dann gibt es endlich viele Elemente $a_1,...,a_n$ mit $L = K(a_1,...,a_n)$. Wir beweisen die Behauptung für $n = 2$, woraus der allgemeine Fall mit Induktion folgt. Sei also $L = K(a,b)$. Da K unendlich ist, finden wir Elemente $c_1 \neq c_2 \in K$ mit

$$K(c_1a + b) = K(c_2a + b) =: E\,.$$

Also liegt $(c_1 - c_2)a = (c_1a + b) - (c_2a + b)$ in E , und damit liegt auch a und dann $b = (c_1a + b) - c_1a$ in E . Damit folgt $L = K(a,b) = E = K(c_1a + b)$, also ist L/K einfach. □

Folgerung 15.13 (Satz vom primitiven Element)
Sei K ein unendlicher Körper. Dann ist jede endliche separable Erweiterung L/K einfach.
Insbesondere ist für Körper K der Charakteristik 0 jede endliche Erweiterung L/K einfach.

Bemerkung 15.14
Wie schon oben erwähnt, ist die Aussage auch ohne die Voraussetzung „unendlich“ richtig!

Beispiel 15.15
Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(i,\sqrt{5})$. Sei mit den Bezeichnungen aus dem Beweis des Satzes $a = \sqrt{5}$, $b = i$. Da $(i + \sqrt{5})(i - \sqrt{5}) = -6 \in \mathbb{Q}$, gilt für $c_1 = 1$, $c_2 = -1$: $K(c_1a + b) = K(c_2a + b)$, also ist nach dem Beweis oben $L = \mathbb{Q}(i + \sqrt{5})$.

Zuletzt wollen wir in diesem Abschnitt als Anwendung der Galoistheorie den Fundamentalsatz der Algebra beweisen, den wir bereits früher formuliert hatten:

Satz 15.16
Der Körper $\mathbb{C}$ der komplexen Zahlen ist **algebraisch abgeschlossen**, d.h. jedes nichtkonstante Polynom in $\mathbb{C}[X]$ hat eine Nullstelle in $\mathbb{C}$.

Es gibt inzwischen eine ganze Reihe von Beweisen für diesen Satz. Wir wollen einen Beweis führen, der nur die folgenden vergleichsweise schwachen Hilfsmittel aus der Analysis benutzt.

Lemma 15.17
Ist $f \in \mathbb{R}[X]$ ein Polynom ungeraden Grades, so hat f eine reelle Nullstelle.
Beweis
Dies folgt leicht aus dem Zwischenwertsatz. □

Da jede komplexe Zahl eine komplexe Quadratwurzel besitzt, folgt aus der Nullstellenformel für quadratische Polynome sofort:

Lemma 15.18
Ist $f \in \mathbb{C}[X]$ vom Grad 2, so zerfällt f in Linearfaktoren.

Beweis (Fundamentalsatz der Algebra, nach Lagrange)
Wir haben zu zeigen, dass jedes nichtkonstante Polynom $f \in \mathbb{C}[X]$ eine komplexe Nullstelle besitzt. Ist $\overline{f} \in \mathbb{C}[X]$ das Polynom mit den komplex konjugierten Koeffizienten, so ist $f \cdot \overline{f} \in \mathbb{R}[X]$. Ist $a \in \mathbb{C}$ eine Nullstelle von $f \cdot \overline{f}$, so ist a eine Nullstelle von f oder von $\overline{f}$. Ist a eine Nullstelle von $\overline{f}$, so ist $\overline{a}$ eine Nullstelle von f. Wir brauchen also nur zu zeigen, dass jedes nichtkonstante Polynom $f \in \mathbb{R}[X]$ eine Nullstelle in $\mathbb{C}$ besitzt. O.E. können wir dabei f als normiert voraussetzen.
Es sei nun $\deg f = n = 2^l m$ mit $l \in \mathbb{N}_0$ und ungeradem $m \in \mathbb{N}$, und wir führen Induktion nach l. Ist $l = 0$, so hat f ungeraden Grad, und die Behauptung folgt aus Lemma 15.13. Sei also jetzt $l > 0$. Sei K der Zerfällungskörper von f über $\mathbb{C}$, und seien $a_1,...,a_n \in K$ mit

$$f = (X - a_1) \cdot ... \cdot (X - a_n).$$

Es sei nun $\lambda \in \mathbb{R}$ fest gewählt, und wir definieren dazu $b_{rs} = a_r + a_s + \lambda a_r a_s$ für $r,s \in \{1,...,n\}$. Dann setzen wir

$$g_\lambda = \prod_{1 \le r < s \le n} (X - b_{rs}) \in K[X].$$

Da $f \in \mathbb{R}[X]$, gilt für jedes $\varphi \in G\left(K/\mathbb{R}\right)$:

$$\varphi(\{a_1,...,a_n\}) = \{a_1,...,a_n\},$$

und damit bleibt auch g_λ unter φ fest. Nun ist K auch eine Galoiserweiterung von $\mathbb{R}$, etwa als Zerfällungskörper des Polynoms $(X^2+1) \cdot f$. Da g_λ unter allen Galoisautomorphismen in $G\left(K/\mathbb{R}\right)$ fest bleibt, ist daher $g_\lambda \in \mathbb{R}[X]$. Nun ist $\deg g_\lambda = \binom{n}{2} = \frac{1}{2} n(n-1) = 2^{l-1} m(n-1)$, und wegen $l > 0$ ist $n-1$ ungerade, also hat g_λ nach Induktionsvoraussetzung eine komplexe Nullstelle. Also gibt es zu unserem gewählten $\lambda \in \mathbb{R}$ Indizes $r < s$ mit $b_{rs} = a_r + a_s + \lambda a_r a_s \in \mathbb{C}$. Da es nur endlich viele solche Indizes, aber unendlich viele reelle Zahlen gibt, finden wir zwei verschiedene reelle Zahlen λ und μ mit $a_r + a_s + \lambda a_r a_s \in \mathbb{C}$ und $a_r + a_s + \mu a_r a_s \in \mathbb{C}$. Dann folgt $a_r a_s \in \mathbb{C}$ und $a_r + a_s \in \mathbb{C}$, und daher liegt das Polynom $(X - a_r)(X - a_s)$ in $\mathbb{C}[X]$. Nach Lemma 15.14 folgt dann $a_r, a_s \in \mathbb{C}$, also hat f eine komplexe Nullstelle. □

Kapitel 16

Operationen von Gruppen und der Hauptsatz der Galoistheorie (Teil 2)

Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = G(L/K)$. Wir verwenden die Notationen aus dem vorhergehenden Paragraphen weiter.

Die Gruppe G operiert in natürlicher Weise auf den Zwischenkörpern der Galoiserweiterung: ist $Z \in \mathcal{Z}$, so ist für jedes $\sigma \in G$ auch $\sigma(Z) \in \mathcal{Z}$, und da σ ein K-Automorphismus von L ist, ist außerdem $|Z : K| = |\sigma(Z) : K|$ und $|L : Z| = |L : \sigma(Z)|$. Die Zwischenkörper der Form $\sigma(Z)$, $\sigma \in G$, heißen zu Z **konjugierte** Zwischenkörper. Sie haben offenbar einige Eigenschaften mit Z gemeinsam.
Was entspricht dieser Operation auf der Seite der Untergruppen der Galoisgruppe G?

Satz 16.1

In der obigen Situation gilt für alle $Z \in \mathcal{Z}$ und $\sigma \in G$:

$$G_{\sigma(Z)} = \sigma G_Z \sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in G_Z\}.$$

Beweis
Die Inklusion $\sigma G_Z \sigma^{-1} \subseteq G_{\sigma(Z)}$ folgt sofort durch einfaches Nachrechnen. Dann gilt aber dieselbe Inklusion auch für $\sigma(Z)$ statt Z und σ^{-1} statt σ, d.h. $\sigma^{-1} G_{\sigma(Z)} \sigma \subseteq G_Z$ und damit $G_{\sigma(Z)} \subseteq \sigma G_Z \sigma^{-1}$, woraus die Gleichheit folgt. □

Bemerkung 16.2

Sei G eine Gruppe, $x \in G$. Dann ist die **Konjugation mit** x

$$c_x : G \to G,\ g \mapsto xgx^{-1}$$

ein Automorphismus der Gruppe G. Die Elemente g und xgx^{-1} heißen zueinander **konjugierte Elemente** von G. Ist U eine Untergruppe von G, dann ist $c_x(U) = xUx^{-1}$ eine **zu** U **konjugierte Untergruppe** von G. Die Gruppe G bewirkt also via Konjugation sowohl Permutationen auf ihren Elementen als auch auf ihren Untergruppen.

Nach Satz 16.1 entsprechen also konjugierte Zwischenkörper der Galoiserweiterung L/K genau konjugierten Untergruppen der Galoisgruppe $G(L/K)$. Wir sehen uns ein Beispiel an.
Sei L der Zerfällungskörper von $f = X^3 - 2$ über $\mathbb{Q}$, also $L = \mathbb{Q}(a, w)$ mit $a = \sqrt[3]{2}$, $w = e^{2\pi i/3}$. Wir wissen bereits, dass die Galoisgruppe $G = G(L/K)$ isomorph zur symmetrischen Gruppe S_3 ist. Die Galoisautomorphismen werden von den 6 Permutationen der 3 Nullstellen von f induziert. Die drei Untergruppen $\{\mathrm{id}, (1\ 2)\}$, $\{\mathrm{id}, (1\ 3)\}$, $\{\mathrm{id}, (2\ 3)\}$ der Ordnung 2 in S_3 sind alle zueinander konjugiert, also sind es auch die Zwischenkörper vom Grad 3 über $\mathbb{Q}$. Wir erhalten also alle diese Zwischenkörper durch Anwendung der Galoisgruppe auf den Zwischenkörper $Z = \mathbb{Q}(a)$. Die anderen beiden Zwischenkörper sind also $\mathbb{Q}(aw)$ und $\mathbb{Q}(aw^2)$.

Wir haben oben bereits den Begriff der Operation benutzt, ohne ihn genau zu definieren. Wir wollen dies hier nun ganz allgemein tun:

Definition 16.3

Sei M eine nichtleere Menge und G eine Gruppe. Eine **Operation von G auf der Menge M** ist ein Gruppenhomomorphismus $\varphi : G \to S(M)$ von G in die Gruppe der Permutationen von M. Wir sagen auch: die Gruppe G **operiert auf** M, und wir schreiben kurz: $g \cdot m := \varphi(g)(m)$ (bzw. auch nur gm). Die Menge M wird in dieser Situation auch eine **G-Menge** genannt.

Bemerkung 16.4

Eine Operation von G auf M definiert eine Abbildung

$$G \times M \to M\,,\ (g,m) \mapsto gm$$

mit $em = m$ (e das neutrale Element von G), $(gh)m = g(hm)$ für alle $m \in M$, $g,h \in G$.
Es ist leicht nachzuprüfen, dass umgekehrt jede solche Abbildung eine Operation von G auf M definiert.

Beispiel 16.5

(i) Sei L/K eine Galoiserweiterung. Wie schon oben angedeutet, operiert die Galoisgruppe $G = G\left(L/K\right)$ auf den Zwischenkörpern von L/K und auf den Untergruppen von G, und die Galoiskorrespondenz ist verträglich mit diesen beiden Operationen nach Satz 16.1. Natürlich operiert G nach Definition auch auf dem Körper L.

(ii) Ist $f \in K[X]$ ein separables Polynom, dann operiert $G(f)$ auf den Nullstellen von f.

(iii) Ist V ein K-Vektorraum, dann operiert die Gruppe $\mathrm{GL}(V)$ der K-Vektorraumautomorphismen auf V:

$$\mathrm{GL}(V) \times V \to V\,,\ (\varphi,v) \mapsto \varphi(v)\,.$$

(iv) Die Gruppe S_n operiert auf der Menge $\{1,\ldots,n\}$.

(v) Jede Gruppe G operiert auf sich selbst via Linkstranslation:

$$G \to S(G)\,,\ x \mapsto (\ell_x : g \mapsto xg)\,.$$

(vi) Jede Gruppe G operiert auf sich selbst und auf ihrer Untergruppenmenge $\mathcal{U}$ via Konjugation:

$$G \to S(G)\,,\ x \mapsto \left(c_x : g \mapsto xgx^{-1}\right),$$
$$G \to S(\mathcal{U})\,,\ x \mapsto \left(c_x : U \mapsto xUx^{-1}\right).$$

(vii) Die Gruppe der Drehungen von $\mathbb{R}^2$ um den Ursprung operiert auf $\mathbb{R}^2$.

Aus dem Beispiel (v) erhalten wir sofort:

Satz 16.6 (Satz von Cayley)

Jede Gruppe der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Beweis

Der oben angegebene Homomorphismus

$$G \to S(G)\,,\ x \mapsto (\ell_x : g \mapsto xg)$$

ist injektiv, denn $\ell_x = \mathrm{id}_G$ impliziert sofort $e = \ell_x(e) = xe = x$. □

Wir hatten bereits oben gesehen, dass es nützlich ist, Elemente zu betrachten, die über eine Gruppenoperation miteinander verknüpft sind, da sie ähnliche Eigenschaften haben. Allgemein definieren wir:

Definition 16.7

Die Gruppe G operiere auf der Menge $M \neq \emptyset$. Dann heißt die Menge

$$Gx = \{ gx \mid g \in G \}$$

die (G-)**Bahn** von x (oder auch: **Orbit** von x). Die Mächtigkeit $|Gx|$ heißt die **Länge der Bahn**. Die Operation heißt **transitiv**, wenn $M = Gx$ für ein (und damit jedes) $x \in M$ gilt.

Bemerkung 16.8

Die Bahnen der Gruppenoperation von G auf M sind genau die Äquivalenzkassen der folgenden Äquivalenzrelation(!) auf M:

$$a \sim b \iff \exists g \in G : \ ga = b .$$

Die Menge M ist also die disjunkte Vereinigung der G-Bahnen auf M, und insbesondere ist daher für eine endliche Menge M:

$$|M| = \sum_{B \in \mathcal{B}} |B| ,$$

wobei $\mathcal{B}$ die Menge der G-Bahnen auf M ist.

Wir sehen uns in den obigen Beispielen die jeweiligen G-Bahnen an (die Nummerierung entspricht der aus 16.5):

Beispiel 16.9

(i) Die Bahnen der Galoisgruppe $G = G\left(L/K\right)$ auf $\mathcal{Z}$ bzw. $\mathcal{U}$ sind nach Definition genau die Mengen konjugierter Zwischenkörper bzw. konjugierter Untergruppen.
Die G-Bahnen auf L sind genau die Nullstellenmengen in L der irreduziblen Polynome in $K[X]$.

(ii) Die Bahnen von $G(f)$ auf der Nullstellenmenge des separablen Polynoms $f \in K[X]$ sind genau die Nullstellenmengen der irreduziblen Faktoren von f in $K[X]$.

(iii) Die Gruppe $\mathrm{GL}(V)$ hat auf V genau zwei Bahnen: $\{0\}$ und $V \setminus \{0\}$.

(iv) Die Operation von S_n auf $\{1,...,n\}$ ist transitiv.

(v) Die Operation von G auf sich selbst via Linkstranslation ist transitiv.

(vi) Die Bahnen der Konjugationsoperation von G auf sich selbst bzw. ihrer Untergruppenmenge $\mathcal{U}$ heißen **Konjugationsklassen** (von Elementen) von G bzw. **Konjugationsklassen von Untergruppen** von G.

(vii) Ist G die Gruppe der Drehungen von $\mathbb{R}^2$ um den Ursprung, dann sind die G-Bahnen genau die Kreise mit Mittelpunkt im Ursprung.

Wir sehen uns die Operation einer Gruppe auf sich selbst durch Linkstranslation genauer an (die Operation durch Rechtstranslation verhält sich entsprechend). Die Einschränkung dieser Operation auf eine Untergruppe $H \leq G$ liefert eine Operation von H auf G. Die H-Bahnen auf G bezüglich der Linkstranslation nur mit Elementen aus H haben die Form

$$Hx = \{ hx \mid h \in H \}, \ x \in G .$$

Dies sind die **Rechtsnebenklassen** von H in G. Die Bahn Hx heißt die **Rechtsnebenklasse** von x bezüglich H. Die Menge dieser Nebenklassen wird mit $H \setminus G$ bezeichnet. Ihre Mächtigkeit heißt der **Index** von H in G, er wird mit $|G : H|$ bezeichnet. Da die Linksmultiplikation mit einem Gruppenelement eine Bijektion ist, sind alle Bahnen Hx, $x \in G$, gleichmächtig mit H. Daraus folgt sofort:

Satz 16.10 (Satz von Lagrange)

Ist G eine endliche Gruppe, H eine Untergruppe von G, dann gilt:

$$|G| = |G : H| \cdot |H| .$$

Insbesondere ist die Ordnung von H ein Teiler der Gruppenordnung $|G|$.

Bemerkung 16.11

Analog zu den Rechtsnebenklassen von H in G sind die **Linksnebenklassen von H in G** die H-Bahnen xH, $x \in G$ der Rechtstranslation von H auf G. Da G auch disjunkte Vereinigung der Linksnebenklassen von H ist, die ebenfalls alle gleichmächtig mit H sind, ist die Menge G/H der Linksnebenklassen gleichmächtig mit der Menge $H \backslash G$ der Rechtsnebenklassen (deswegen benötigt der Index von H in G keine Vorsilbe „Rechts“ oder „Links“). Ist G endlich, so ist nach dem Satz von Lagrange

$$|H \backslash G| = \left|G/H\right| = |G : H| = \frac{|G|}{|H|}.$$

Wie in der Analysis spielen auch bei Gruppenoperationen Fixpunkte eine besondere Rolle. Wir haben dies bereits bei der Galoiskorrespondenz gesehen.

Definition 16.12

Die Gruppe G operiere auf der Menge M. Dann heißt $x \in M$ ein **Fixpunkt von $g \in G$**, wenn $gx = x$ gilt. x heißt **Fixpunkt von G**, wenn $gx = x$ für alle $g \in G$ gilt. Für $g \in G$ ist

$$M_g = \{ x \in M \mid gx = x \}$$

die Menge der Fixpunkte von g. Wir bezeichnen die gemeinsame Fixpunktmenge der gesamten Gruppe G auf M mit $\mathrm{Fix}_G(M)$ (oder auch: M_G).
Die Menge

$$G_x = \{ g \in G \mid gx = g \}$$

ist eine Untergruppe von G, genannt der **Stabilisator von x in G** (oder auch: **Fixpunktgruppe** oder **Standuntergruppe von x**).

Es gilt folgende wichtige Beziehung zwischen Bahnen und Stabilisatoren:

Satz 16.13

Die Gruppe G operiere auf der Menge M. Sei $x \in M$. Dann induziert die Abbildung $G \to Gx$, $g \mapsto gx$ eine Bijektion zwischen der Linksnebenklassenmenge G/G_x und der Bahn Gx.
Ist G endlich, so ist also

$$|Gx| = |G : G_x| = \frac{|G|}{|G_x|}.$$

Insbesondere sind die Bahnenlängen dann also Teiler der Gruppenordnung $|G|$.

Beweis

Für $g \in G$, $h \in G_x$ ist $(gh)x = g(hx) = gx$, d.h. alle Elemente der Linksnebenklasse gG_x werden auf dasselbe Element $gx \in Gx$ abgebildet. Es wird also tatsächlich eine Abbildung $G/G_x \to Gx$ induziert, die offenbar surjektiv ist. Ist $gx = g'x$ für $g, g' \in G$, dann ist $g^{-1}g'x = x$, d.h. $g^{-1}g' \in G_x$ und damit $gG_x = g'G_x$. Also ist die Abbildung auch injektiv und damit eine Bijektion. □

Aus diesem Ergebnis folgt sofort:

Folgerung 16.14 (Bahnengleichung)

Die Gruppe G operiere auf der endlichen Menge M. Sei $\mathcal{V}$ ein Vertretersystem für die G-Bahnen auf M, d.h. $|B \cap \mathcal{V}| = 1$ für jede G-Bahn B. Dann gilt

$$|M| = \sum_{v \in \mathcal{V}} |G : G_v|.$$

Satz 16.15 (Cauchy-Frobenius-Lemma)
Die endliche Gruppe G operiere auf der Menge M. Dann ist die Anzahl der G-Bahnen auf M genau

$$\frac{1}{|G|}\sum_{g\in G}|M_g|,$$

d.h. gleich der durchschnittlichen Anzahl von Fixpunkten.

Beweis
Sei $S=\{(g,x)\in G\times M \mid gx=x\}$, und sei $\mathcal{V}$ ein Vertretersystem für die G-Bahnen auf M. Dann gilt:

$$\begin{aligned}|S| &= \sum_{g\in G}|M_g| \\ &= \sum_{x\in M}|G_x| = \sum_{x\in M}\frac{|G|}{|Gx|} \\ &= \sum_{x\in\mathcal{V}}|Gx|\frac{|G|}{|Gx|} = |\mathcal{V}|\cdot|G|.\end{aligned}$$

Also ist die Anzahl der Bahnen $|\mathcal{V}| = \frac{1}{|G|}\sum_{g\in G}|M_g|$. □

Wir sehen uns die obigen Begriffe und Resultate am Beispiel der Konjugationsoperation einer Gruppe G an. Zunächst betrachten wir die Konjugationsoperation von G auf sich selbst.
In diesem Fall heißt die Fixpunktmenge

$$\mathrm{Fix}_G(G)=\{x\in G \mid gxg^{-1}=x \text{ für alle } g\in G\}$$

das **Zentrum** von G, kurz mit $Z(G)$ bezeichnet. Da

$$Z(G)=\{x\in G \mid gx=xg \text{ für alle } g\in G\}$$

ist, ist das Zentrum ein Maß dafür, wie weit die Gruppe G davon entfernt ist, abelsch zu sein: $G=Z(G)$ gilt genau dann, wenn G abelsch ist. Der Stabilisator

$$G_x=\{g\in G \mid gxg^{-1}=x\}$$

eines Elementes x heißt der **Zentralisator von x in G**, kurz mit $C_G(x)$ bezeichnet.

Aus der Bahnengleichung erhalten wir unmittelbar (beachte, dass $Z(G)$ in jedem Vertretersystem für die Konjugationsklassen von G enthalten sein muss):

Folgerung 16.16 (Klassengleichung)
Sei G eine endliche Gruppe, $\mathcal{V}$ ein Vertretersystem für die Konjugationsklassen von G, und sei $\mathcal{V}'=\mathcal{V}\setminus Z(G)$. Dann gilt:

$$|G| = |Z(G)| + \sum_{x\in\mathcal{V}'}|G:C_G(x)|.$$

Eine Anwendung der Klassengleichung ist das folgende nützliche Ergebnis (Übung!):

Satz 16.17
Sei p eine Primzahl und G eine endliche Gruppe mit $|G|=p^r$ für ein $r\in\mathbb{N}$ (eine solche Gruppe heißt eine **p-Gruppe**). Dann ist $|Z(G)|>1$.

Nun zur Konjugationsoperation der Gruppe G auf ihren Untergruppen (diese Operation ist insbesondere im Hinblick auf unsere Untersuchung von Galoiserweiterungen interessant!).
Fixpunkte dieser Operation sind Untergruppen U von G mit

$$gUg^{-1}=U \text{ für alle } g\in G.$$

Diese Untergruppen sind gerade die **Normalteiler** von G (andere Sprechweisen: U ist **normal** oder **invariant** in G). Wir schreiben dann: $U\trianglelefteq G$.
Der Stabilisator von U in G, also

$$G_U = \{ g \in G \mid gUg^{-1} = U \}$$

heißt der **Normalisator** von U in G und wird mit $N_G(U)$ bezeichnet.

Wir können nun unsere Untersuchung von Galoiserweiterungen fortsetzen. Wir verwenden wieder die früheren Bezeichnungen:

Satz 16.18

Für $Z \in \mathcal{Z}$ ist Z/K genau dann eine normale (und damit eine galoissche) Erweiterung, wenn G_Z ein Normalteiler von G ist.

Beweis

Als Zwischenkörper der galoisschen Erweiterung L/K ist Z/K genau dann galoissch, wenn Z/K normal ist. Sei $Z = K(a_1,...,a_n)$, f das Produkt der Minimalpolynome f_i der a_i über K. Dann ist Z/K genau dann normal, wenn f über Z in Linearfaktoren zerfällt. Da L/K normal ist, zerfällt f auf jeden Fall über L in Linearfaktoren, d.h. der Zerfällungskörper Z' von f über K ist ein Zwischenkörper von L/Z. Nach dem Fortsetzungssatz operiert $G(L/K)$ jeweils transitiv auf den Nullstellen der f_i in Z'. Also ist $Z = Z'$ genau dann, wenn $\sigma(Z) = Z$ für alle $\sigma \in G(L/K)$ gilt. Dies ist nach Satz 16.1 äquivalent zu $\sigma G_Z \sigma^{-1} = G_Z$ für alle $\sigma \in G$, d.h. aber gerade, dass G_Z ein Normalteiler von G ist. □

Wie hängt in der Situation einer galoisschen Zwischenerweiterung Z/K die Galoisgruppe $G(Z/K)$ mit der Galoisgruppe $G(L/K)$ zusammen?

Bevor wir die Antwort auf diese Frage formulieren, erinnern wir an eine Konstruktion für Gruppen, mit der wir im Fall von Ringen bisher schon häufiger gearbeitet haben: die Faktorkonstruktion. Analog zu Faktorringen nach Idealen werden Faktorgruppen nach Normalteilern gebildet.

Satz 16.19

Sei G eine Gruppe, N ein Normalteiler in G. Dann wird auf der Menge G/N der Linksnebenklassen durch

$$xN \cdot yN = xyN \text{ für alle } x,y \in G$$

eine Verknüpfung $\cdot$ definiert, so dass $(G/N, \cdot)$ eine Gruppe ist, die **Faktorgruppe** (oder: **Restklassengruppe**) von G nach N (oder: modulo N).

Die Abbildung $\pi : G \to G/N$, $x \mapsto xN$, ist ein surjektiver Gruppenhomomorphismus mit $\operatorname{Kern} \pi = N$. π ist der kanonische Epimorphismus.

Beweis

Wir zeigen zunächst, dass die Setzung $xN \cdot yN = xyN$ für $x,y \in G$ wohl definiert ist, d.h. unabhängig von der Repräsentantenwahl. Seien $x',y' \in G$ mit $xN = x'N$, $yN = y'N$. Dann gibt es $a,b \in N$ mit $x' = xa$, $y' = yb$, also ist $x'y' = xayb$. Da N ein Normalteiler ist, ist $N = yNy^{-1}$, also $Ny = yN$. Also gibt es $c \in N$ mit $ay = yc$, und es folgt dann

$$x'y'N = xycbN = xyN .$$

Die Gruppeneigenschaften von $(G/N, \cdot)$ sind leicht zu kontrollieren. Das neutrale Element in G/N ist die Nebenklasse $eN = N$, das zu xN inverse Element ist $x^{-1}N$.

Die Eigenschaften der Abbildung π sind offensichtlich. □

Bemerkung 16.20

(i) Es ist nicht schwer zu zeigen, dass die Bildung der Faktorgruppe nur genau für Normalteiler möglich ist.

(ii) Die Normalteiler von G sind genau die Kerne von Gruppenhomomorphismen $G \to H$, wobei H eine beliebige Gruppe ist.

(iii) Genauso wie im Fall von Faktorringen induziert der kanonische Epimorphismus $\pi : G \to G/N$ eine Bijektion zwischen den Untergruppen bzw. Normalteilern von G, die N enthalten und allen Untergruppen bzw. Normalteilern von G/N.

Wir erinnern auch daran, dass – wie im Fall von Faktorringen – für Gruppen ein Homomorphiesatz gilt, der eine universelle Eigenschaft der Faktorgruppe beinhaltet:

Satz 16.21

Sei $\varphi : G \to H$ ein Homomorphismus zwischen Gruppen G und H. Sei N ein Normalteiler von G mit $N \subseteq \operatorname{Kern}\varphi$, und sei $\pi : G \to G/N$ der kanonische Epimorphismus. Dann gibt es einen eindeutig bestimmten Homomorphismus $\psi : G/N \to H$ mit $\psi \circ \pi = \varphi$ (d.h.: $\psi(xN) = \varphi(x)$).
Es ist $\operatorname{Kern}\psi = \operatorname{Kern}\varphi/N \leq G/N$ und $\operatorname{Bild}\psi = \operatorname{Bild}\varphi$. Der Homomorphismus ψ heißt auch der **von φ induzierte Homomorphismus**.
Ist insbesondere φ ein Epimorphismus mit $\operatorname{Kern}\varphi = N$, dann induziert φ einen Isomorphismus $\psi : G/N \to H$.

Definition 16.22

Ist G eine Gruppe, $x \in G$, dann ist $\langle x \rangle := \{x^m \mid m \in \mathbb{Z}\}$ **die von x erzeugte (zyklische) Untergruppe von G**. Die Gruppe G heißt **zyklisch**, wenn sie von der Form $G = \langle x \rangle$ für ein geeignetes $x \in G$ ist.

Die Struktur solcher Gruppen ist gut verstanden. Wir benutzen dazu den Homomorphiesatz, um zyklische Gruppen mit $\mathbb{Z}$ zu vergleichen.

Folgerung 16.23

Sei G eine Gruppe, $x \in G$.

(i) Ist $\langle x \rangle$ eine unendliche Gruppe, so ist $\langle x \rangle \cong \mathbb{Z}$.

(ii) Ist $\langle x \rangle$ eine endliche Gruppe, dann existiert $n := \min\{k \in \mathbb{N} \mid x^k = 1\}$, und
$$\langle x \rangle = \{1, x, \ldots, x^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$$
ist eine Untergruppe der Ordnung n in G.
Ist $k \in \mathbb{Z}$, dann gilt $x^k = 1$ genau dann, wenn $n|k$ gilt.
Die Zahl n heißt die Ordnung des Elementes x, kurz: $n = \operatorname{ord} x$.

(iii) Ist G eine endliche Gruppe, so gilt für alle $x \in G$:
$$x^{|G|} = 1 .$$

Beweis
Die Abbildung
$$\varphi : \mathbb{Z} \to G , \; k \mapsto x^k$$
ist ein Gruppenhomomorphismus mit $\operatorname{Bild}\varphi = \langle x \rangle$ und $\operatorname{Kern}\varphi = m\mathbb{Z}$, für ein $m \in \mathbb{N}_0$, denn in $\mathbb{Z}$ ist jede Untergruppe bereits ein Ideal(!). Nach dem Homomorphiesatz ist dann $\mathbb{Z}/m\mathbb{Z} \cong \langle x \rangle$.
Ist $\langle x \rangle$ unendlich, dann ist also $m = 0$ und $\mathbb{Z} \cong \langle x \rangle$.
Ist $\langle x \rangle$ endlich, dann ist $m \in \mathbb{N}$. Da jedes Ideal $I \neq 0$ in $\mathbb{Z}$ von der kleinsten positiven Zahl in I erzeugt wird, ist $m = n$ und (ii) folgt.
(iii) Da $|\langle x \rangle| | |G|$, folgt die letzte Aussage sofort aus (ii). □

Wir halten explizit die Klassifikation der zyklischen Gruppen fest:

Folgerung 16.24

Jede zyklische Gruppe der Ordnung $n \in \mathbb{N}$ ist isomorph zur Gruppe $\mathbb{Z}/n\mathbb{Z}$.
Jede unendliche zyklische Gruppe ist isomorph zur Gruppe $\mathbb{Z}$.

Ein sehr oft genutztes Resultat über Körper ist der folgende Satz:

Satz 16.25

Sei K ein Körper. Dann ist jede endliche Untergruppe der multiplikativen Gruppe K^* zyklisch.
Insbesondere ist für jeden endlichen Körper K seine multiplikative Gruppe K^* zyklisch.

Beweis

Sei U eine endliche Untergruppe von K^*, $n = |U|$. Dann gilt nach Folgerung 16.23 für jedes $x \in U$:

$$x^n = 1 \text{ und } \operatorname{ord} x | n .$$

Sei $a \in U$ ein Element maximaler Ordnung in U. Ist $\operatorname{ord} a = n$, dann ist $U = \langle a \rangle$ zyklisch, und die Aussage ist gezeigt. Sei also $\operatorname{ord} a = k < n$ angenommen. Sei $b \in U$ mit $\operatorname{ord} b = l \nmid k$. Es komme etwa die Primzahl p in höherer Potenz in l als in k vor. Ist $l = p^j l'$ mit $p \nmid l'$, dann ist $c = b^{l/p^j} \in U$ von der Ordnung p^j. Es gilt dann für $m = \operatorname{kgV}(k, p^j)$:

$$\langle ac \rangle^m = a^m c^m = 1 .$$

Andererseits gilt aber:

$$\langle ac \rangle^{m/p} = a^{m/p} c^{m/p} = c^{m/p} \neq 1 .$$

Ebenso gilt für alle Primteiler $q \neq p$ von k:

$$\langle ac \rangle^{m/q} = a^{m/q} c^{m/q} = a^{m/q} \neq 1 .$$

Also ist die Ordnung von $ac \in U$ genau m. Wegen $m > k$ ist dies ein Widerspruch zur Maximalität von k.
Wir haben damit gezeigt: für jedes $b \in U$ ist $\operatorname{ord} b$ ein Teiler von k. Daher gilt für jedes $b \in U$:

$$b^k = 1 .$$

Da das Polynom $X^k - 1 \in K[X]$ aber höchstens k verschiedene Nullstellen hat, folgt nun $n \leq k$, im Widerspruch zu unserer Annahme. Damit ist der Satz bewiesen. □

Wir können daraus unmittelbar schließen, dass auch für endliche Körper der Satz 15.12 und die Folgerung 15.13 richtig ist. Wir formulieren zumindest den Satz vom primitiven Element für diese Situation:

Folgerung 16.26

Sei K ein endlicher Körper. Dann ist jede endliche Erweiterung L/K einfach.

Bevor wir zu Galoiserweiterungen zurückkehren, halten wir noch folgende wichtige Struktursätze fest, die sich als Anwendung des Homomorphiesatzes ergeben:

Satz 16.27

Sei G eine Gruppe.

(i) (1. Noetherscher Isomorphiesatz) Seien $U \leq G$, $N \trianglelefteq G$. Dann ist

$$UN = \{ uh \mid u \in U, h \in N \} \leq G , \; U \cap N \trianglelefteq U ,$$

und der Homomorphismus $U \to G/N$, $u \mapsto uN$, induziert einen Isomorphismus

$$U/(U \cap N) \xrightarrow{\cong} UN/N , \; u(U \cap N) \mapsto uN .$$

(ii) (2. Noetherscher Isomorphiesatz) Seien $N_1, N_2 \trianglelefteq G$ mit $N_2 \subseteq N_1$.

Dann induziert die Komposition der kanonischen Epimorphismen

$$G \to G/N_2 \to \Big(G/N_2\Big)\Big/\Big(N_1/N_2\Big)$$

einen Isomorphismus

$$G/N_1 \xrightarrow{\cong} \Big(G/N_2\Big)\Big/\Big(N_1/N_2\Big),\ xN_1 \mapsto (xN_2)N_1/N_2\,.$$

Beispiel 16.28

(i) Für $G = S_4$ ist $N = V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq G$. Für N und $U = S_3$ gilt dann $G = UN$ und $U \cap N = \{\mathrm{id}\}$. Also folgt nach dem 1. Isomorphiesatz: $S_3 \cong S_4/V_4$.

(ii) Sei $G = S_4$ und $N_2 = V_4$ wie oben, $N_1 = A_4$. Es sind V_4 und A_4 Normalteiler von S_4 mit $V_4 \leq A_4$. Dann folgt nach dem 2. Isomorphiesatz: $\big(S_4/V_4\big)\big/\big(A_4/V_4\big) \cong S_4/V_4$.

Satz 16.29

Für $Z \in \mathcal{Z}$ sei Z/K galoissch. Dann definiert die Einschränkung der K-Automorphismen von L auf Z einen Gruppenisomorphismus

$$G/G_Z \xrightarrow{\cong} G\big(Z/K\big),\ \sigma G_Z \mapsto \sigma|_Z\,.$$

Beweis

Ist Z/K galoissch, so gilt $\sigma(Z) = Z$ für alle $\sigma \in G$. Wir können daher durch Einschränkung einen Gruppenhomomorphismus definieren:

$$\rho : G \to G\big(Z/K\big),\ \sigma \mapsto \sigma|_Z\,.$$

Offenbar ist $\operatorname{Kern}\rho = G_Z$, also induziert ρ einen injektiven Homomorphismus

$$\overline{\rho} : G/G_Z \to G\big(Z/K\big).$$

Da nach Satz 15.9 (c) $|G_Z| = |L : Z|$ ist, folgt

$$\big|G/G_Z\big| = \frac{|G|}{|G_Z|} = \frac{|L : K|}{|L : Z|} = |Z : K| = \big|G\big(Z/K\big)\big|.$$

Also ist $\overline{\rho}$ sogar ein Gruppenisomorphismus. □

Galoissche Körpererweiterungen werden nach der Struktur der zugehörigen Galoisgruppe klassifiziert. Wir betrachten zunächst den abelschen Fall:

Definition 16.30

Eine Körpererweiterung L/K heißt **abelsch** (bzw. **zyklisch**), wenn L/K galoissch ist und die Galoisgruppe $G\big(L/K\big)$ abelsch (bzw. zyklisch) ist. Ein separables Polynom $f \in K[X]$ heißt **abelsch** (bzw. **zyklisch**), wenn $G(f)$ die entsprechende Eigenschaft hat.

Beispiel 16.31

(i) Das Polynom $f = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ ist ein abelsches Polynom, da $G(f)$ eine abelsche Gruppe (der Ordnung 4) ist.

(ii) Das Polynom $f = X^5 - 1 \in \mathbb{Q}[X]$ hat eine zyklische Galoisgruppe $G(f)$, erzeugt von dem durch $\zeta \mapsto \zeta^2$ bestimmten Automorphismus seines Zerfällungskörpers $\mathbb{Q}(\zeta)$, wobei $\zeta = e^{2\pi i/5}$ ist.

Folgerung 16.32

Ist L/K eine abelsche (bzw. zyklische) Erweiterung, so ist für jeden Zwischenkörper Z von L/K auch Z/K abelsch (bzw. zyklisch).

Beweis

Aus Satz 16.18 folgt, dass Z/K galoissch ist, da in einer abelschen Gruppe alle Untergruppen Normalteiler sind. Da Faktorgruppen abelscher Gruppen ebenfalls abelsch sind, folgt mit Satz 16.29, dass Z/K abelsch ist. Im zyklischen Fall ist zu zeigen, dass alle Faktorgruppen einer zyklischen Gruppe ebenfalls zyklisch sind. Ist $G = \langle x \rangle$ eine zyklische Gruppe, so ist jede Faktorgruppe G/N zyklisch, da sie von dem kanonischen Bildelement xN erzeugt wird. □

Kapitel 17

Konstruktion mit Zirkel und Lineal (Teil 2)

Eine positive Antwort auf die Frage nach der Konstruktion regulärer n-Ecke mit Zirkel und Lineal steht noch aus. Wir wollen die Galoiskorrespondenz verwenden, um unser früheres Konstruktionskriterium in eine gruppentheoretische Frage zu übersetzen.
Dazu müssen wir die körpertheoretische Aussage der „sukzessiven Adjunktion von Quadratwurzeln" gruppentheoretisch fassen. Wir behandeln hier gleich eine allgemeinere Situation und zeigen, dass p-Gruppen in Schritten der Ordnung p aufgebaut werden können.

Satz 17.1

Sei p eine Primzahl und G eine p-Gruppe, $|G| = p^m$. Dann gibt es Normalteiler $N_1,...,N_m$ in G mit

$$\{1\} = N_m \subset N_{m-1} \subset ... \subset N_2 \subset N_1 \subset N_0 = G$$

und $|N_{i-1} : N_i| = p$ für $i = 1,...,m$.

Beweis

Wir führen Induktion nach m durch. Für $m = 0$ ist nichts zu zeigen. Sei also nun $m > 0$. Nach Satz 16.17 ist $Z(G)$ nichttrivial. Sei etwa $1 \neq x \in Z(G)$ von der Ordnung p, also ist $N = \langle y \rangle \subseteq Z(G)$ ein Normalteiler der Ordnung p in G. Die Faktorgruppe $\overline{G} = G/N$ hat die Ordnung p^{m-1}, also gibt es nach Induktion in $\overline{G}$ eine Kette von Normalteilern

$$\{\overline{1}\} = H_{m-1} \subset H_{m-2} \subset ... \subset H_2 \subset H_1 \subset H_0 = \overline{G}$$

mit $|H_{i-1} : H_i| = p$ für $i = 1,...,m-1$.
Ist $\pi : G \to G/N$ der kanonische Epimorphismus, dann bilden die Urbilder der H_i unter π eine Kette von Normalteilern in G:

$$N = N_{m-1} \subset ... \subset N_2 \subset N_1 \subset N_0 = G$$

mit $|N_{i-1} : N_i| = p$ für $i = 1,...,m-1$ (benutze Satz 16.27). Insgesamt hat die Kette

$$\{1\} = N_m \subset N_{m-1} \subset ... \subset N_2 \subset N_1 \subset N_0 = G$$

dann die gewünschten Eigenschaften. □

Wir können nun zeigen:

Satz 17.2

Sei $M \subseteq \mathbb{C}$, $0,1 \in M$, $K = \mathbb{Q}(M \cup \overline{M})$. Dann sind für $z \in \mathbb{C}$ folgende Aussagen äquivalent:

(i) Die Zahl z ist aus M mit Zirkel und Lineal konstruierbar.

(ii) Die Zahl z ist algebraisch über K, und für den Zerfällungskörper L seines Minimalpolynoms f über K gilt: $|L : K|$ ist eine 2-Potenz.

(iii) Die Zahl z ist algebraisch über K, und für sein Minimalpolynom f über K ist $G(f)$ eine 2-Gruppe.

Beweis

(ii) $\Longleftrightarrow$ (iii): Ist klar.

(i) $\Rightarrow$ (ii): Sei E/K eine Erweiterung, die durch sukzessive Adjunktion von Quadratwurzeln entsteht, und sei $z \in E$. Da E endlich und separabel ist, ist E Zwischenkörper einer Galoiserweiterung F/K . Ist $G = G\left(F/K\right)$, dann ist die normale Hülle von E/K gerade das Körperkompositum $N = \prod_{\sigma \in G} \sigma(E)$, und N ist galoissch über K (die so genannte **galoissche Hülle** von E). Beachte, dass N den Zerfällungskörper L von f enthält. Auch N entsteht durch sukzessive Adjunktion von Quadratwurzeln aus K , also ist $|N : K|$ eine 2-Potenz. Da $L \subseteq N$, ist damit auch $|L : K|$ eine 2-Potenz.
(iii) $\Rightarrow$ (i): Da $G(f)$ eine 2-Gruppe ist, finden wir eine Normalteilerkette in $G(f)$ wie in Satz 17.1. Vermöge Galoiskorrespondenz liefert dies eine Kette von Zwischenkörpern von L/K , bei denen die einzelnen Gradschritte jeweils 2 sind. Da jede Erweiterung vom Grad 2 in Charakteristik 0 durch sukzessive Adjunktion einer Quadratwurzel entsteht, liegt z also in einem Körper, der durch sukzessive Adjunktion von Quadratwurzeln entsteht, und wir wenden nun unser Konstruierbarkeitskriterium 1.15 an. □

Für die Konstruktion des regulären n -Ecks ist zu entscheiden, ob $\zeta = e^{2\pi i/n}$ aus $\mathbb{Q}$ mit Zirkel und Lineal konstruierbar ist.

Definition 17.3

Der Körper $\mathbb{Q}(\zeta)$ heißt der n -te **Kreisteilungskörper über** $\mathbb{Q}$. Die Nullstellen von $X^n - 1$ in $\mathbb{Q}(\zeta)$ heißen n -te **Einheitswurzeln über** $\mathbb{Q}$.

Bemerkung 17.4

(i) Die Menge $W_n = \{a \in \mathbb{C} \mid a^n = 1\}$ der n -ten Einheitswurzeln in $\mathbb{C}$ ist eine zyklische Untergruppe von $\mathbb{C}^*$ nach Satz 16.25. Sie ist von der Ordnung n und von ζ erzeugt. Ist $z \in W_n$ von der Ordnung n , dann heißt z eine **primitive** n -te Einheitswurzel.

(ii) Da $\mathbb{Q}(\zeta)$ der Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist, ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoissch. Nach dem obigen Satz haben wir also für die Konstruierbarkeitsfrage zu untersuchen, wann $|\mathbb{Q}(\zeta) : \mathbb{Q}|$ eine 2-Potenz ist.

Satz 17.5

Die Galoisgruppe $G\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ ist kanonisch isomorph zur Gruppe $\mathbb{Z}_n^*$ der multiplikativen Einheiten von $\mathbb{Z}_n$ ($\mathbb{Z}_n^*$ ist die **prime Restklassengruppe modulo** n).

Beweis

Für $\sigma \in G = G\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ ist $\sigma(\zeta) = \zeta^k$ für ein (eindeutig bestimmtes) $k \in \{1,...,n\}$. Da ζ^k ebenfalls die Ordnung n haben muss, ist außerdem $\mathrm{ggT}(k,n) = 1$ (ist $d = \mathrm{ggT}(n,k)$, dann ist bereits $\left(\zeta^k\right)^{n/d} = \left(\zeta^{k/d}\right)^n = 1$). Damit erhalten wir also eine Abbildung

$$\psi : G \to \mathbb{Z}_n^*\,,\ \sigma \mapsto \overline{k} = k + n\mathbb{Z}\,.$$

(Die Zahl k hängt nicht von der Wahl der primitiven n -ten Einheitswurzel ab, in diesem Sinne ist die Abbildung kanonisch.) Die Abbildung ψ ist ein Gruppenhomomorphismus (leicht zu überprüfen), der injektiv ist, da $\psi(\sigma) = \overline{1}$ sofort $\sigma(\zeta) = \zeta$ und damit $\sigma = \mathrm{id}$ impliziert. Wir haben noch die Surjektivität zu zeigen, d.h. es ist nachzuweisen, dass es für jede Zahl $k \in \{1,...,n\}$ mit $\mathrm{ggT}(k,n) = 1$ ein $\sigma \in G$ mit $\sigma(\zeta) = \zeta^k$ gibt. Dies ist äquivalent dazu, dass für jede solche Zahl k auch ζ^k eine Nullstelle von $f = \mathrm{minpol}_{\mathbb{Q}}\,\zeta$ ist. Es reicht, den Fall $k = p$ prim zu betrachten, dann folgt die Behauptung per Induktion über die Anzahl der Primfaktoren von k . In $\mathbb{Q}[X]$ gilt

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

für ein geeignetes Polynom $g(X) \in \mathbb{Q}[X]$. Da f normiert ist, folgt dann nach Satz ?? sogar: $f(X), g(X) \in \mathbb{Z}[X]$. Ist $f(\zeta^p) \neq 0$, dann muss $g(\zeta^p) = 0$ sein, d.h. ζ ist Nullstelle von $g(X^p)$. Dann folgt

$$g(X^p) = f(X)\cdot h(X)$$

für ein geeignetes Polynom $h(X)\in\mathbb{Z}[X]$. Wir reduzieren nun die Koeffizienten modulo p und erhalten eine Polynomgleichung in $\mathbb{Z}_p[X]$:

$$\overline{g}(X^p) = \overline{f}(X)\cdot\overline{h}(X)\,.$$

Für $\overline{g}(X) = \sum_i a_i X^i$ gilt aber:

$$\overline{g}(X)^p = \left(\sum_i a_i X^i\right)^p = \sum_i a_i^p X^{ip} = \sum_i a_i X^{ip} = \overline{g}(X^p)\,.$$

Im Zerfällungskörper von $\overline{g}(X)$ über $\mathbb{Z}_p$ haben also $\overline{g}$ und $\overline{f}$ eine gemeinsame Nullstelle. Dann hat also

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

eine mehrfache Nullstelle, aber dies steht im Widerspruch dazu, dass die Ableitung nX^{n-1} keine n-te Einheitswurzel als Nullstelle hat (beachte, dass wir in der Situation $p\nmid n$ sind).

Also war die Annahme $f(\zeta^p)\neq 0$ falsch, und damit folgt die Behauptung. □

Die Ordnung der Galoisgruppe $G\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$ ist also

$$\varphi(n) = \left|\mathbb{Z}_n^*\right| = \left|\{k\in\{1,\ldots,n\}\mid \mathrm{ggT}(k,n)=1\}\right|,$$

wobei φ die **Eulersche Phi-Funktion** ist. Wenn die Primfaktorisierung von n bekannt ist, kann die Ordnung explizit so berechnet werden:

Satz 17.6

Sei $n=\prod_{i=1}^k p_i^{r_i}$ mit paarweise verschiedenen Primzahlen p_i und Exponenten $r_i\in\mathbb{N}$ die Primfaktorisierung von n. Dann ist

$$\varphi(n) = \prod_{i=1}^k p_i^{r_i-1}(p_i-1)\,.$$

Beweis

In der Übung wurde bereits die Ringisomorphie $\mathbb{Z}_n\cong\mathbb{Z}_{p_1^{r_1}}\times\ldots\times\mathbb{Z}_{p_k^{r_k}}$ gezeigt (Chinesischer Restsatz). Daraus folgt unmittelbar die Isomorphie der Einheitengruppen

$$\mathbb{Z}_n^*\cong\mathbb{Z}_{p_1^{r_1}}^*\times\ldots\times\mathbb{Z}_{p_k^{r_k}}^*\,.$$

Also ist $\varphi(n)=\prod_{i=1}^k\varphi(p_i^{r_i})$. Da für eine Primzahlpotenz p^r offenbar $\varphi(p^r)=p^r-p^{r-1}$ gilt (genau jede p-te Zahl ist durch p teilbar!), folgt die Behauptung. □

Satz 17.7 (Gauß)

Für $n\in\mathbb{N}$, $n\geq 3$, ist das reguläre n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form

$$n = 2^m\cdot p_1\cdot\ldots\cdot p_k$$

mit $m\in\mathbb{N}_0$ und paarweise verschiedenen Fermatschen Primzahlen $p_1,\ldots,p_k$, $k\in\mathbb{N}_0$, ist.

Beweis

Nach Satz 17.2 und Satz 17.5 ist das reguläre n-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)=\left|\mathbb{Q}(e^{2\pi i/n}):\mathbb{Q}\right|$ eine 2-Potenz ist. Ist $n=2^m\cdot p_1^{r_1}\cdot\ldots\cdot p_k^{r_k}$ mit verschiedenen ungeraden Primzahlen $p_1,\ldots,p_k$, dann ist

$$\varphi(n) = 2^{m'}\cdot p_1^{r_1-1}(p_1-1)\cdot\ldots\cdot p_k^{r_k-1}(p_k-1)\,,$$

wobei $m'=\max\{m-1,0\}$. Dies ist genau dann eine 2-Potenz, wenn alle $r_i=1$ und die p_i Fermatsche Primzahlen sind. □

Kapitel 18

Die Sätze von Sylow

Mit Hilfe der Galoiskorrespondenz kommen wir von Zwischenkörpern einer galoisschen Erweiterung zu Untergruppen der zugehörigen Galoisgruppe. Wir brauchen dann also Resultate über Untergruppen einer Gruppe. Im Fall endlicher zyklischer Gruppen gibt es zu jedem Teiler der Gruppenordnung (genau) eine Untergruppe dieser Ordnung. Für beliebige endliche Gruppen ist dies nicht richtig, z.B. hat die alternierende Gruppe A_4 der Ordnung 12 keine Untergruppe der Ordnung 6. Ziel dieses Paragraphen ist es, für beliebige endliche Gruppen Existenzsätze für Untergruppen von Primzahlpotenzordnung zu beweisen.
Wir hatten bereits früher verschiedene Operationen von Gruppen auf Mengen untersucht. Wir knüpfen dort nun wieder an.

Sei G eine Gruppe, H eine Untergruppe von G. Dann operiert G auf der Menge $G/H = \{ xH \mid x \in G \}$ der Linksnebenklassen von G nach H durch:

$$G \times G/H \to G/H \,,\ (g, xH) \mapsto gxH \,.$$

Diese Operation hat folgende Eigenschaften:

(i) Die Gruppe G operiert transitiv auf G/H.

(ii) Der Stabilisator der Linksnebenklasse xH in G ist $G_{xH} = xHx^{-1}$.

Wir betrachten nun eine weitere Untergruppe $U \leq G$ und schränken die obige Operation auf U ein, d.h. wir betrachten die Operation

$$U \times G/H \to G/H \,,\ (u, xH) \mapsto uxH \,.$$

Diese Operation hat folgende Eigenschaften:

(i) Die U-Bahn einer Linksnebenklasse xH ist $\{ uxH \mid u \in U \}$.

(ii) Der Stabilisator der Linksnebenklasse xH in U ist $U_{xH} = U \cap xHx^{-1}$.

Die Vereinigung der Linksnebenklassen in der U-Bahn von xH ist die Menge

$$UxH = \bigcup_{u \in U} uxH = \{ uxh \mid h \in H \} \,,$$

die **Doppelnebenklasse von** x **nach** U **und** H.

Da die Gruppe G die disjunkte Vereinigung der Linksnebenklassen von H ist, folgt dann unmittelbar, dass G auch die disjunkte Vereinigung der verschiedenen Doppelnebenklassen von H und U ist.

Für endliche Gruppen können wir einige nützliche Anzahlaussagen in Bezug auf Doppelnebenklassen treffen:

Satz 18.1

Sei G eine endliche Gruppe. Seien $U, H \leq G$, dann gilt:

(i) Für $x \in G$ hat die Doppelnebenklasse UxH die Mächtigkeit

$$|UxH| = \frac{|U|\,|H|}{|U \cap xHx^{-1}|} \,.$$

(ii) Sei $\mathcal{T} \subseteq \mathcal{G}$ ein Vertretersystem für die verschiedenen Doppelnebenklassen nach U und H. Dann ist

$$|G| = \sum_{g \in \mathcal{T}} \frac{|U||H|}{|U \cap gHg^{-1}|} = \sum_{g \in \mathcal{T}} \frac{|U||H|}{|H \cap g^{-1}Ug|}.$$

Beweis

(i) Sei l die Länge der U-Bahn von xH. Dann ist l der Index des zugehörigen Stabilisators in U, also ist UxH eine disjunkte Vereinigung von

$$l = |U : (U \cap xHx^{-1})|$$

Linksnebenklassen von H in G. Da jede dieser Nebenklassen genau $|H|$ Elemente enthält, folgt

$$|UxH| = |H| \cdot |U : (U \cap xHx^{-1})| = \frac{|U||H|}{|U \cap xHx^{-1}|}.$$

(ii) Da $|U \cap xHx^{-1}| = |x^{-1}Ux \cap H|$ ist, folgt (ii) unmittelbar aus (i). □

Wir hatten früher bereits endliche p-Gruppen betrachtet und einige nützliche Eigenschaften gezeigt. Wir wollen nun Untergruppen diesen Typs in beliebigen endlichen Gruppen untersuchen.

Definition 18.2

Sei G eine endliche Gruppe, p eine Primzahl. Ist $H \leq G$ mit $|H| = p^r$ für ein $r \in \mathbb{N}_0$, dann heißt H eine **p-Untergruppe von G**.

Ist p^r die maximale p-Potenz in $|G|$, also $|G| = p^r m$ mit $\mathrm{ggT}(p, m) = 1$, dann heißt H eine **p-Sylow(unter)gruppe von G** (oder auch **Sylow p-Untergruppe**). Eine Untergruppe $H \leq G$ heißt **Sylow(unter)gruppe von G**, wenn sie p-Sylowgruppe von G für die Primzahl p ist.

Die Menge der p-Sylowuntergruppen von G bezeichnen wir mit $\mathrm{Syl}_p(G)$.

Bemerkung 18.3

(i) p-Sylowuntergruppen werden auch als maximale p-Untergruppen von G bezüglich Inklusion definiert. Wir werden unten sehen, dass diese beiden Definitionen äquivalent sind.

(ii) Alle zu einer p-Sylowgruppe von G konjugierten Untergruppen von G sind ebenfalls p-Sylowgruppen von G.

Das folgende Beispiel wird im Beweis der Sätze von Sylow eine wesentliche Rolle spielen:

Beispiel 18.4

Sei $G = \mathrm{GL}_n(p) = \mathrm{GL}_n(\mathbb{Z}_p)$ die Gruppe der invertierbaren $n \times n$-Matrizen über dem Körper $\mathbb{Z}_p$. Dann ist die Ordnung von G:

$$|G| = (p^n - 1)(p^{n-1} - p) \cdot \ldots \cdot (p^n - p^{n-1}).$$

Die maximale in $|G|$ auftretende p-Potenz ist also

$$p^{1+2+\ldots+n-1} = p^{\frac{n(n-1)}{2}}.$$

Die Menge

$$P = \{A = (a_{ij}) \in \mathrm{GL}_n(p) \mid a_{ii} = 1 \text{ für alle } i, a_{ij} = 0 \text{ für alle } i > j\}$$

der oberen Dreiecksmatrizen mit Einsen auf der Diagonale ist eine Untergruppe von G, und es ist

$$|P| = p^{\frac{n(n-1)}{2}},$$

also ist P eine p-Sylowgruppe von G.

Entsprechend ist auch die Menge der unteren Dreiecksmatrizen mit Einsen auf der Diagonale eine p-Sylowgruppe von G.

Wir wollen eine beliebige endliche Gruppe G mit der Gruppe $\mathrm{GL}_n(p)$ vergleichen, um eine p-Sylowgruppe in G zu finden. Dazu brauchen wir zunächst:

Satz 18.5

Sei G eine endliche Gruppe, $H \leq G$. Sei P eine p-Sylowgruppe von G. Dann gibt es ein $g \in G$, so dass $H \cap P^g$ eine p-Sylowgruppe von H ist.

Beweis

Wir wollen Satz 18.1 auf die Untergruppen H und P anwenden. Ist $\mathcal{T}$ ein Vertretersystem für die Doppelnebenklassen von G nach P und H, dann ist also

$$|G| = \sum_{g \in \mathcal{T}} \frac{|P||H|}{|H \cap P^g|}. \qquad \circledast$$

Dividieren wir diese Gleichung durch $|P|$, so erhalten wir

$$\sum_{g \in \mathcal{T}} |H : H \cap P^g| = |G : P| \not\equiv 0 (\mathrm{mod}\ p).$$

Also gibt es ein $g \in G$ mit

$$|H : H \cap P^g| \not\equiv 0 (\mathrm{mod}\ p).$$

Da $H \cap P^g$ eine p-Gruppe ist, folgt dann, dass $H \cap P^g$ eine p-Sylowgruppe von H ist. □

Die Aussagen (i) bis (iii) in folgendem Satz werden oft auch als 1. bis 3. Sylowsatz zitiert.

Satz 18.6 (Sylowsätze)

Sei G eine endliche Gruppe, p eine Primzahl. Sei $|G| = p^r m$ mit $\mathrm{ggT}(p, m) = 1$. Dann gilt:

(i) Für jedes $s \in \{0, ..., r\}$ besitzt G eine Untergruppe der Ordnung p^s. Insbesondere hat G stets eine p-Sylowgruppe. Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

(ii) Je zwei p-Sylowgruppen von G sind zueinander konjugiert.

(iii) Sei s_p die Anzahl der p-Sylowgruppen von G. Dann hat s_p die folgenden beiden arithmetischen Eigenschaften:

$$s_p = |G : N_G(P)|, \text{ insbesondere ist } s_p \text{ ein Teiler von } |G : P|.$$
$$s_p \equiv 1 (\mathrm{mod}\ p).$$

Beweis

(i) Sei $|G| = n$, und $G = \{g_1, ..., g_n\}$. Da die Linksmultiplikation mit $g \in G$ eine Bijektion auf G ist, ist die durch $gg_j = g_{k(j)}$ definierte Abbildung $j \mapsto k(j)$ eine Bijektion und die zugehörige Matrix $A_g = (a_{ij})$ mit $a_{ij} = \delta_{i,k(j)}$ eine Permutationsmatrix in $\mathrm{GL}_n(p)$. Vermöge des Monomorphismus(!) $g \mapsto A_g$ ist G also isomorph zu einer Untergruppe H von $\mathrm{GL}_n(p)$. Für $\mathrm{GL}_n(p)$ hatten wir bereits wir bereits eine p-Sylowgruppe angegeben, also hat nach dem vorhergehenden Resultat H dann auch eine p-Sylowgruppe und damit auch G. Nach Satz 17.1 gibt es in einer p-Gruppe der Ordnung p^r zu jeder p-Potenz p^s, $s \in \{0, ..., r\}$, eine Untergruppe der Ordnung p^s, also hat auch G solche Untergruppen.

Wir müssen noch zeigen, dass jede p-Untergruppe von G Untergruppe einer geeigneten p-Sylowgruppe von G ist. Sei dazu H eine beliebige p-Untergruppe von G und P eine p-Sylowgruppe von G. Nach Satz 18.5 gibt es dann ein $g \in G$, so dass $H \cap P^g$ eine p-Sylowgruppe von H ist. Dann muss bereits $H = H \cap P^g$ und damit $H \subseteq P^g$ gelten. Da auch P^g eine p-Sylowgruppe von G ist, folgt die Behauptung.

(ii) Mit dem vorhergehenden Argument haben wir insbesondere gezeigt: sind H, P zwei p-Sylowgruppen von G, dann ist $H = P^g$ für ein geeignetes $g \in G$, d.h. H und P sind zueinander konjugiert.

(iii) Nach (ii) operiert die Gruppe G durch Konjugation transitiv auf ihren p-Sylowgruppen. Ist P eine p-Sylowgruppe von G, dann ist also $\mathrm{Syl}_p(G) = \{P^g \mid g \in G\}$, und die Länge dieser einen G-Bahn ist

$$s_p = |G : G_P| = |G : N_G(P)|.$$

Dies zeigt die erste Aussage in (iii).

Für den zweiten Teil betrachten wir Doppelnebenklassen von G nach P und $H = N_G(P)$, d.h. PgH mit $g \in G$. Sei $\mathcal{T}$ ein Vertretersystem für diese Doppelnebenklassen, o.E. sei $1 \in \mathcal{T}$, und damit $g \notin H$ für $1 \neq g \in \mathcal{T}$. Da P die einzige p-Sylowgruppe in seinem Normalisator H ist (wegen (ii)), ist für $g \in G$ der Durchschnitt $P^g \cap H \subseteq P^g \cap P$ nach Satz 18.5. Also ist dann $P^g \cap H = P^g \cap P$. Für $1 \neq g \in \mathcal{T}$ ist dies eine echte Untergruppe von P. Aus der Gleichung $\circledast$ im Beweis von Satz 18.5 ergibt sich nun nach Division durch $|H|$:

$$|G : H| = \sum_{g \in \mathcal{T}} \frac{|P|}{|H \cap P^g|} = 1 + \sum_{1 \neq g \in \mathcal{T}} |P : P \cap P^g| \equiv 1 (\mathrm{mod}\ p). \qquad \square$$

Bemerkung 18.7

(i) G hat nur eine einzige p-Sylowgruppe P genau dann, wenn eine (und damit die) p-Sylowgruppe P ein Normalteiler von G ist.

(ii) Der Beweis von (iii) zeigt, dass die Kongruenz $s_p \equiv 1$ sogar richtig ist modulo jeder Potenz p^d mit der Eigenschaft $p^d || P : P \cap Q|$ für je zwei verschiedene p-Sylowgruppen P, Q von G.

(iii) Die Anzahlaussage $s_p \equiv 1 (\mathrm{mod}\ p)$ gilt nicht nur für die p-Sylowgruppen, sondern allgemeiner für Untergruppen von p-Potenzordnung, d.h. für jede feste p-Potenz p^s mit $p^s || G|$ gilt:

$$|\{U \leq G \mid |U| = p^s\}| \equiv 1 (\mathrm{mod}\ p)$$

(iv) Sei G eine endliche Gruppe mit $p||G|$, p prim. Dann enthält G Elemente der Ordnung p (Satz von Cauchy).

(v) Via Galoiskorrespondenz liefern die Sylowsätze Aussagen über die Existenz und Anzahl von gewissen Zwischenkörpern in galoisschen Erweiterungen!

Folgerung 18.8

Sei G eine endliche Gruppe, p eine Primzahl mit $p||G|$. Dann gilt für die Anzahl t_p der Elemente der Ordnung p in G:

$$t_p \equiv -1 (\mathrm{mod}\ p)$$

Beweis

Übung! $\square$

Die Sylowsätze garantieren also die Existenz von Untergruppen von Primzahlpotenzgrad, und sie liefern außerdem ein Kriterium für die Normalität von Sylowgruppen. Wir wollen ihre Anwendung illustrieren.

Beispiel 18.9

(i) Sei G eine Gruppe der Ordnung $p \cdot q$ mit Primzahlen $p < q$.
Dann hat G also q-Sylowgruppe Q der Ordnung q. Außerdem gilt für die Anzahl s_q der q-Sylowgruppen von G:

$$s_q || G : Q| = p \text{ und } s_q \equiv 1 (\mathrm{mod}\ p).$$

Wegen $p < q$ ist dann $s_q = 1$, und die q-Sylowgruppe Q ist ein Normalteiler in G.

(ii) Sei G eine Gruppe der Ordnung $105 = 3 \cdot 5 \cdot 7$.
Für $p = 7$ gibt es eine 7-Sylowgruppe P der Ordnung 7 in G. Außerdem gilt:

$$s_7 || G : P| = 15 \text{ und } s_7 \equiv 1 (\mathrm{mod}\ 7).$$

In dieser Situation haben wir also zwei Möglichkeiten: $s_7 = 1$ oder $s_7 = 15$.
Ist $s_7 = 1$, dann ist P ein Normalteiler von G.
Wir nehmen nun an, dass es 15 7-Sylowgruppen in G gibt. Da der Durchschnitt je zweier verschiedener 7-Sylowgruppen trivial ist, enthalten die 7-Sylowgruppen also insgesamt $15 \cdot 6 = 90$ Elemente der Ordnung 7 und das neutrale Element.

Sei Q eine 5-Sylowgruppe von G. Für die Anzahl der 5-Sylowgruppen erhalten wir

$$s_5 | |G:Q| = 21 \text{ und } s_5 \equiv 1 (\mathrm{mod}\ 5)$$

also ist $s_5 = 1$ oder $s_5 = 21$. Ist $s_5 = 21$, dann enthält G in den 21 5-Sylowgruppen $21 \cdot 4 = 84$ Elemente der Ordnung 5. Aber dann erhalten wir den Widerspruch

$$105 = |G| \geq 91 + 84 = 175 .$$

Also ist in diesem Fall $s_5 = 1$, und damit ist die 5-Sylowgruppe Q von G ein Normalteiler.
Wir haben also in jedem Fall einen nichttrivialen Normalteiler in G gefunden.

Wir wollen die Sylowsätze benutzen, um die Struktur von endlichen Gruppen genauer zu bestimmen.

Satz 18.10

Sei G eine Gruppe der Ordnung $p \cdot q$ mit Primzahlen $p < q$, $q \not\equiv 1 (\mathrm{mod}\ p)$. Dann gilt: G ist zyklisch, also $G \cong \mathbb{Z}_{pq}$.

Beweis

Sei G eine Gruppe der Ordnung pq. In Beispiel 18.9 (i) haben wir bereits gezeigt, dass G einen Normalteiler Q der Ordnung q hat. Für die Anzahl s_p der p-Sylowgruppen von G gilt:

$$s_p | q \text{ und } s_p \equiv 1 (\mathrm{mod}\ p) .$$

Also ist auch $s_p = 1$, d.h. G hat auch einen Normalteiler der Ordnung p, etwa P. Nun ist PQ eine Untergruppe von G, die wegen $\mathrm{ggT}(p,q) = 1$ von der Ordnung $pq = |G|$ ist. Sind $a \in P$, $b \in Q$, so ist $aba^{-1}b^{-1} \in P \cap Q = \{1\}$, also kommutieren die Elemente von P und Q miteinander. Dann ist $P \times Q \to G$, $(a,b) \mapsto ab$ ein Gruppenhomomorphismus(!), also folgt mit dem Chinesischen Restsatz

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} . \qquad \square$$

Für die Ordnung $6 = 2 \cdot 3$ ist die Bedingung in obigem Satz nicht erfüllt, und wir kennen in diesem Fall ja auch die nichtzyklische Gruppe S_3. Allgemeiner klassifizieren wir die Gruppen der Ordnung $2p$:

Satz 18.11

Sei $p > 2$ eine Primzahl. Dann gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung $2p$, nämlich die zyklische Gruppe $\mathbb{Z}_{2p}$ und die Diedergruppe D_{2p}.

Beweis

Sei G eine Gruppe der Ordnung $2p$. Nach Beispiel 18.9 (i) wissen wir bereits, dass G einen Normalteiler P der Ordnung p hat. Außerdem erhalten wir für die Anzahl s_2 der 2-Sylowgruppen mit den Sylowsätzen sofort: $s_2 \in \{1, p\}$.

Ist $s_2 = 1$, dann folgt wie im vorhergehenden Beweis sofort $G \cong \mathbb{Z}_{2p}$.

Sei also $s_2 = p$. Dann hat G genau p Elemente der Ordnung 2, die die Menge $G \setminus P$ bilden. Ist $P = \langle a \rangle$, $b \in G \setminus P$, dann gilt: $a^p = b^2 = e = (ab)^2$, also $a^{-1} = bab$. Ist d eine Drehung der Ordnung p in der Diedergruppe D_{2p} und s eine Spiegelung, so ist nun leicht zu zeigen, dass $a \mapsto d$, $b \mapsto s$ einen Isomorphismus $G \to D_{2p}$ liefert. $\square$

Wir wollen nun noch einen allgemeinen Struktursatz für endliche abelsche Gruppen herleiten, den wir später im Rahmen der Ring- und Modultheorie noch verallgemeinern werden. Zunächst halten wir fest, dass wir für abelsche Gruppen ihre Sylowgruppen explizit angeben können:

Lemma 18.12

Sei G eine endliche abelsche Gruppe, p eine Primzahl. Dann ist

$$G_p = \{ x \in G \mid \operatorname{ord} x \text{ ist eine } p\text{-Potenz} \}$$

die p-Sylowgruppe von G.

Satz 18.13

Sei G eine endliche abelsche Gruppe. Dann ist G direktes Produkt zyklischer Untergruppen.
Insbesondere ist also $G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$ für geeignete Zahlen $n_1,...,n_r$.

Beweis

Sei $|G| = \prod_{i=1}^{t} p_i^{r_i}$ die Primfaktorzerlegung von $|G|$, und sei P_i die p_i-Sylowgruppe von G, $i = 1,...,t$. Wegen $\prod_{i=1}^{t} |P_i| = |G|$ ist $G = P_1 \cdot ... \cdot P_t$, und

$$P_1 \times ... \times P_t \to P_1 \cdot ... \cdot P_t = G \,,\ (x_1,...,x_t) \mapsto x_1 \cdot ... \cdot x_t$$

ist ein Isomorphismus. Wir dürfen daher nun annehmen, dass G eine p-Gruppe ist. Sei etwa $|G| = p^n$ für eine Primzahl p.
Wir zeigen zunächst mit Induktion nach n: ist $x \in G$ von maximaler Ordnung, dann ist $G = \langle x \rangle \cdot U \cong \langle x \rangle \times U$ für eine geeignete Untergruppe $U \leq G$.
Für $n = 0$ ist die Aussage klar. Sei also jetzt $n > 0$.
Sei $a \in G$ von maximaler Ordnung. Ist $\operatorname{ord} a = p^n$, dann ist $G = \langle a \rangle$ zyklisch, und wir sind fertig.
Sei also nun $\operatorname{ord} a < p^n$, d.h. $A = \langle a \rangle < G$. Dann gibt es $b \in G \setminus A$ mit $b^p \in A$. Da $\operatorname{ord} b \leq \operatorname{ord} a$, ist $b^p = a'^p$ für ein $a' \in A$. Also ist $b' := ba'^{-1} \in G \setminus A$ von der Ordnung p, und daher gilt für $U = \langle b' \rangle$: $U \cap A = \{1\}$. Da aU auch maximale Ordnung in G/U hat, ist $G/U = \langle aU \rangle \cdot C/U \cong \langle aU \rangle \times C/U$ für eine Untergruppe C von G mit $U \leq C$. Dann ist $A \cap C = \{1\}$ und $G = A \cdot C \cong A \times C$. Da $C < G$, können wir nun die Induktionsvoraussetzung anwenden und erhalten so die gewünschte Zerlegung von G. □

Bemerkung 18.14

Sei G eine endliche abelsche Gruppe. Die Zahlen $n_1,...,n_r$ in einer Zerlegung $G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$ sind nicht eindeutig bestimmt, z.B. ist ja $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Wegen des Chinesischen Restsatzes können wir aber stets eine Zerlegung $G \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_s}$ angeben, so dass alle m_i Primpotenzen sind. Diese Zahlen sind dann (bis auf die Reihenfolge) eindeutig (zähle dazu nacheinander die Elemente „großer“ Ordnung!). Wir können daher die endlichen abelschen Gruppen bis auf Isomorphie klassifizieren:

Satz 18.15

Seien G, H endliche abelsche Gruppen. Sei $G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$ und $H \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_s}$, wobei $n_1,...,n_r$, $m_1,...,m_s$ Primpotenzen sind.
Dann ist G genau dann isomorph zu H, wenn $r = s$ ist und die Zahlen $n_1,...,n_r$ und $m_1,...,m_r$ bis auf die Reihenfolge übereinstimmen.

Kapitel 19

Kreisteilungskörper

Wir wollen nun das Polynom $X^n - 1$ über beliebigen Körpern K untersuchen. Dies ist der einfachste Spezialfall eines Polynoms vom Typ $X^n - a$ (dessen Nullstellen Radikale sind). Für die Frage nach der Auflösbarkeit algebraischer Gleichungen durch Radikale spielen diese Polynome eine wichtige Rolle.

Satz 19.1

Sei K ein Körper, $n \in \mathbb{N}$. Dann ist die Menge

$$W_n(K) = \{a \in K \mid a^n = 1\}$$

der n-ten Einheitswurzeln in K eine zyklische Gruppe, deren Ordnung n teilt.

Beweis

Da $X^n - 1 \in K[X]$ höchstens n verschiedene Nullstellen in K hat, ist $W_n(K)$ offenbar endlich. Außerdem ist klar, dass $W_n(K)$ eine multiplikative Gruppe ist. Nach Satz 16.25 ist $W_n(K)$ daher zyklisch. Da die Ordnung jedes Elementes von $W_n(K)$ nach Folgerung 16.23 ein Teiler von n ist, also dies insbesondere für die Ordnung eines erzeugenden Elementes von $W_n(K)$ gilt, folgt die zweite Aussage. □

Bemerkung 19.2

Ist $\operatorname{Char} K = p > 0$, dann ist

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

d.h. es ist $W_{np}(K) = W_n(K)$. Insbesondere ist $W_p(K) = \{1\}$.

Zerfällt $X^n - 1$ über K, und ist $\operatorname{Char} K$ kein Teiler von n, dann ist $|W_n(K)| = n$.

Definition 19.3

Für einen Körper K heißt der Zerfällungskörper L von $X^n - 1$ über K der **Körper der n-ten Einheitswurzeln über K** oder auch der **n-te Kreisteilungskörper über K**.

Ist z eine Einheitswurzel in K von der Ordnung n, dann heißt z eine primitive n-te Einheitswurzel in K.

Bemerkung 19.4

Ist L der n-te Kreisteilungskörper über K, dann ist ein erzeugendes Element von $W_n(L)$ gleichzeitig ein primitives Element der einfachen Körpererweiterung L/K (aber nicht umgekehrt!). Wir schreiben auch $L = K(\sqrt[n]{1})$.

Wir haben bereits die Kreisteilungskörper über $\mathbb{Q}$ untersucht. Welche Aussagen können wir für die Kreisteilungskörper über beliebigen Körpern K machen?

Satz 19.5

Sei $n \in \mathbb{N}$ nicht durch $p = \operatorname{Char} K$ teilbar. Dann ist der n-te Kreisteilungskörper L über K galoissch über K.

Beweis
Nach Definition zerfällt $f = X^n - 1$ über L in Linearfaktoren. Da $f' = nX^{n-1}$ keine der n-ten Einheitswurzeln als Nullstellen hat, ist jede n-te Einheitswurzel eine einfache Nullstelle von f, also ist f separabel. Als Zerfällungskörper von f über K ist damit L galoissch über K. □

Wir setzen im Folgenden stets voraus:

Die Charakteristik von K teilt die Zahl $n \in \mathbb{N}$ nicht.

Es gibt dann also genau n verschiedene n-te Einheitswurzeln im Kreisteilungskörper L über K. Da eine zyklische Gruppe der Ordnung n genau $\varphi(n)$ erzeugende Elemente besitzt, gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln in L. Wir bezeichnen sie mit $\xi_1,...,\xi_{\varphi(n)}$ und setzen

$$\Phi_n = (X - \xi_1) \cdot ... \cdot (X - \xi_{\varphi(n)}) \in L[X].$$

Φ_n heißt n-tes **Kreisteilungspolynom**. Wir werden gleich zeigen, dass stets $\Phi_n \in K[X]$ gilt.

Lemma 19.6

Seien K und n wie oben. Dann gilt:
(i) $X^n - 1 = \prod_{d|n} \Phi_d$.
(ii) Sei R der Primring von K. Dann liegt Φ_n in $R[X]$.

Beweis
(i) Ist ξ eine n-te Einheitswurzel, $d = \operatorname{ord}\xi$, dann ist ξ eine primitive d-te Einheitswurzel und $d|n$.
(ii) Wir beweisen die Behauptung durch Induktion nach n. Für $n = 1$ ist offenbar $\Phi_1 = X - 1 \in R[X]$. Sei nun $n > 1$ und die Behauptung bis $n-1$ bereits gezeigt. Nach (i) ist $X^n - 1 = \Phi_n \cdot g$, wobei $g \in R[X]$ ein normiertes Polynom ist. Division von $X^n - 1$ durch g in $R[X]$ liefert also Φ_n, und damit ist auch $\Phi_n \in R[X]$. □

Wir können nun zeigen, dass die Galoiserweiterung L/K abelsch ist, genauer:

Satz 19.7

Sei K ein Körper der Charakteristik $p > 0$, $n \in \mathbb{N}$ mit $n > 1$ und $p \nmid n$. Sei L der n-te Kreisteilungskörper über K. Dann ist $G(L/K)$ isomorph zu einer Untergruppe von $\mathbb{Z}_n^*$. Insbesondere ist also $G(L/K)$ abelsch.

Beweis
Die Beweisidee kennen wir bereits aus dem vorherigen Paragraphen.
Da $\Phi_n \in K[X]$, permutiert jedes $\sigma \in G(L/K)$ die primitiven n-ten Einheitswurzeln. Sei ξ eine primitive n-te Einheitswurzel, dann ist $\sigma(\xi) = \xi^r$ für ein $r \in \{1,...,n-1\}$ mit $\operatorname{ggT}(r,n) = 1$. Die Abbildung

$$\varepsilon : G(L/K) \to \mathbb{Z}_n^*,\ \sigma \mapsto r + n\mathbb{Z}, \text{ wenn } \sigma(\xi) = \xi^r$$

ist wohl definiert, injektiv und ein Gruppenhomomorphismus. Also ist $G(L/K)$ isomorph zu einer Untergruppe von $\mathbb{Z}_n^*$. □

Wir haben bereits einige Eigenschaften von endlichen Körpern kennen gelernt. Zu jeder Primzahl p und zu jedem $n \in \mathbb{N}$ wurde ein Körper der Ordnung p^n als Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{Z}_p$ konstruiert. Wir wollen nun alle endlichen Körper angeben und dann die Galoisgruppen ihrer endlichen Erweiterungen bestimmen.

Satz 19.8

Sei K ein endlicher Körper der Charakteristik $p > 0$, P sein Primkörper, und sei $|K : P| = m$. Dann ist K der Zerfällungskörper von $X^{p^m} - X$ über P. Insbesondere hat K genau p^m Elemente, und die Erweiterung K/P ist galoissch.

Beweis

Als Vektorraum der Dimension m über dem Körper $P \cong \mathbb{Z}_p$ mit p Elementen hat K genau p^m Elemente. Dann ist K^* eine zyklische Gruppe der Ordnung $p^m - 1$, also gilt für alle $a \in K^*$: $a^{p^m-1} = 1$. Daher ist jedes Element aus K Nullstelle des Polynoms $X(X^{p^m-1} - 1) = X^{p^m} - X \in P[X]$, und daher ist K der Zerfällungskörper des (separablen) Polynoms $X^{p^m} - X \in P[X]$, insbesondere ist K also galoissch über P. □

Bemerkung 19.9

Jeder endliche Körper ist also ein Kreisteilungskörper über seinem Primkörper!

Folgerung 19.10

Für jede Primzahl p und jedes $m \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen Körper mit p^m Elementen. (Dieser Körper wird als **Galoisfeld der Ordnung** $q = p^m$ bezeichnet. Wir schreiben dafür kurz: $\mathrm{GF}(q)$.)

Satz 19.11

Die Galoisgruppe von $\mathrm{GF}(p^m)/\mathrm{GF}(p)$ ist zyklisch von der Ordnung m, mit dem Frobeniusautomorphismus $F : a \mapsto a^p$ als erzeugendem Element.

Beweis

Wir wissen bereits, dass die Frobeniusabbildung

$$F : \mathrm{GF}(p^m) \to \mathrm{GF}(p^m),\ a \mapsto a^p$$

ein Automorphismus von $L = \mathrm{GF}(p^m)$ ist, der $K = \mathrm{GF}(p)$ elementweise festhält, also ist $F \in G(L/K)$.

Sei a ein primitives Element von L^*. Es ist $F^j(a) = a^{p^j}$ für $j \in \mathbb{N}$, und da die Elemente a^{p^j} für $j = 1, \ldots, m$ paarweise verschieden. Wegen $\left|G(L/K)\right| = |L : K| = m$ folgt daraus die Behauptung. □

Folgerung 19.12

Sei K ein endlicher Körper, L/K eine endliche Körpererweiterung. Dann ist L/K eine zyklische Erweiterung. Die Zwischenkörper von L/K entsprechen eindeutig den Teilern von $|L : K|$.

Beweis

Sei P der Primkörper von K, dann ist L/P galoissch, also ist auch L/K galoissch, mit einer Untergruppe der zyklischen Gruppe $G(L/P)$ als Galoisgruppe, also ist auch $G(L/K)$ zyklisch (und von der Ordnung $m = |L : K|$). Die zweite Aussage folgt dann unmittelbar aus dem Hauptsatz der Galoistheorie, da es für eine zyklische Gruppe der Ordnung m zu jedem Teiler d von m genau eine Untergruppe der Ordnung d gibt. □

Folgerung 19.13

Sei K ein endlicher Körper, $f \in K[X]$ ein irreduzibles Polynom. Dann ist f separabel und $G(f)$ zyklisch von der Ordnung $\deg f$.

Beweis

Sei a eine Nullstelle von f in seinem Zerfällungskörper L über K. Dann ist $K(a)$ eine zyklische Erweiterung von K vom Grad $\deg f$. Als Galoiserweiterung von K, muss $K(a)$ dann bereits der Zerfällungskörper L von f über K sein, also ist $G(f) = G(K(a)/K)$, und die Aussage bewiesen. □

Kapitel 20

Auflösbarkeit durch Radikale und auflösbare Gruppen

Sei K ein Körper. Wir sehen uns die Radikalerweiterungen an und versuchen, via Galoiskorrespondenz zu gruppentheoretischen Bedingungen zu kommen.
Zunächst betrachten wir algebraische Gleichungen der einfachsten Bauart, die offenbar durch Radikale lösbar sind, nämlich zu Polynomen der Form $X^n - a \in K[X]$, $a \in K^*$. Da wir für die Galoiskorrespondenz außerdem von einem separablen Polynom ausgehen müssen, setzen wir voraus, dass $\operatorname{Char} K = p \in \mathbb{N}_0$ die Zahl n nicht teilt. Dann ist $X^n - a$ ein separables Polynom.
Eine Gleichung der Form $X^n - a = 0$, $a \in K^*$, wird eine **reine Gleichung** genannt. Sei L der Zerfällungskörper von $f = X^n - a$ über K, $b \in L$ mit $b^n = a$, und sei w eine primitive n-te Einheitswurzel. Dann sind die Lösungen von $X^n - a = 0$ von der Form $w^i b$, $i = 0,...,n-1$. Also enthält L die n-ten Einheitswurzeln. Da wir die Erweiterung $K(w)/K$ bereits betrachtet haben, wenden wir uns jetzt der Erweiterung $L/K(w)$ zu, d.h. dass wir im folgenden Satz voraussetzen können, dass der Grundkörper bereits die n-ten Einheitswurzeln enthält.

Satz 20.1

Sei $n \in \mathbb{N}$, $\operatorname{Char} K \nmid n$, und es seien die n-ten Einheitswurzeln in K enthalten. Dann gilt:

(i) Für $f = X^n - a$, $a \in K^*$, ist $G(f)$ zyklisch. Ist f irreduzibel, so ist $|G(f)| = n$.

(ii) Zu jeder zyklischen Erweiterung L/K mit $|L:K| = n$ gibt es ein $b \in L$ mit $L = K(b)$ und $b^n \in K$.

Beweis

(i) Sei L der Zerfällungskörper von f über K, und sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Ist b eine Nullstelle von f in L, dann sind $b, \zeta b, ..., \zeta^{n-1} b$ genau die n Nullstellen von f. Also ist $L = K(b)$, und jedes $\sigma \in G(f) = G\left(L/K\right)$ ist durch seinen Wert $\sigma(b) = \zeta^j b$, $j = 0,...,n-1$, eindeutig bestimmt, also durch die Restklasse $j + n\mathbb{Z} \in \mathbb{Z}_n$. Wir haben daher eine injektive Abbildung

$$\varphi : G(f) \to \mathbb{Z}_n,\ \sigma \mapsto j + n\mathbb{Z}, \text{ wobei } \sigma(b) = \zeta^j b.$$

Wir zeigen, dass φ ein Gruppenhomomorphismus von $G(f)$ in die additive Gruppe $\mathbb{Z}_n$ ist. Seien $\sigma, \tau \in G(f)$ mit $\sigma(b) = \zeta^j b$, $\tau(b) = \zeta^k b$, dann ist

$$\tau\sigma(b) = \tau\left(\zeta^j b\right) = \zeta^j \tau(b) = \zeta^j \zeta^k b = \zeta^{j+k} b,$$

also ist

$$\varphi(\tau\sigma) = j + k + n\mathbb{Z} = (j + n\mathbb{Z}) + (k + n\mathbb{Z}) = \varphi(\tau) + \varphi(\sigma).$$

Daher ist $G(f)$ isomorph zu einer Untergruppe der zyklischen Gruppe $\mathbb{Z}_n$, und damit ist $G(f)$ ebenfalls zyklisch.

(ii) Sei σ ein erzeugendes Element von $G\left(L/K\right)$, und sei wieder $\zeta \in K$ eine primitive n-te Einheitswurzel. Da $n = |L:K| = \left|G\left(L/K\right)\right|$, sind nach Satz 15.4 die Automorphismen $1, \sigma, ..., \sigma^{n-1}$ linear unabhängig über K, also ist $\sum_{i=0}^{n-1} \zeta^i \sigma^i \neq 0$ und daher gibt es ein $x \in L$ mit

$$b := (\zeta, x) := x + \zeta\sigma(x) + \zeta^2\sigma^2(x) + ... + \zeta^{n-1}\sigma^{n-1}(x) \neq 0\,.$$

Das Element (ζ, x) heißt **Lagrangesche Resolvente**. Es ist

$$\sigma(b) = \sigma(x) + \zeta\sigma^2(x) + \zeta^2\sigma^3(x) + ... + \zeta^{n-2}\sigma^{n-1}(x) + \zeta^{n-1}x = \zeta^{-1} \cdot b\,,$$

und daher $\sigma(b^n) = \sigma(b)^n = \zeta^{-n}b^n = b^n$ für alle $\sigma \in G\left(L/K\right)$. Da L/K galoissch ist, folgt also $b^n \in K$. Da $\sigma^r(b) = \zeta^{-r} \cdot b$ für $r = 0,...,n-1$ ist, sind die σ^r, $r \in \{0,...,n-1\}$, n verschiedene K-Automorphismen von $K(b)$. Da $|L : K| = n$ ist, folgt daraus $L = K(b)$, und die Behauptung ist gezeigt. □

Bevor wir zum Auflösbarkeitskriterium für algebraische Gleichungen durch Radikale kommen können, benötigen wir nun eine Reihe neuer Begriffe, vor allem gruppentheoretische Definitionen, um die Bedingung an die Galoisgruppe formulieren zu können.
Zur Verallgemeinerung der Körpererweiterungen, die durch sukzessive Adjunktion von Quadratwurzeln entstehen (wie sie bei den geometrischen Konstruktionsproblemen vorgekommen waren), führen wir folgende Definition ein:

Definition 20.2

Eine Körpererweiterung L/K heißt **metazyklisch** (bzw. p**-metazyklisch** für eine Primzahl $p \in \mathbb{N}$), wenn es eine Kette

$$K = Z_0 \subseteq Z_1 \subseteq ... \subseteq Z_r = L$$

von Zwischenkörpern Z_i von L/K gibt, so dass die Körpererweiterungen Z_{i+1}/Z_i für $i = 0,...,r-1$ zyklisch (bzw. zyklisch vom Grad p) sind.

Für Gruppen definieren wir:

Definition 20.3

Sei G eine Gruppe. Eine Kette von Untergruppen $N_i \leq G$

$$\{1\} = N_m \subset N_{m-1} \subset ... \subset N_2 \subset N_1 \subset N_0 = G$$

für die N_i Normalteiler in N_{i-1} ist, für $i = 1,...,m$, heißt eine **Normalreihe** (der **Länge** n) von G. Die Faktorgruppen N_{i-1}/N_i, $i = 1,...,m$, heißen **Faktoren** der Normalreihe. Gibt es eine Normalreihe von G, für die alle Faktoren abelsch sind, so heißt die Gruppe G **auflösbar**.

Bemerkung 20.4

(i) Offenbar sind alle abelschen Gruppen auflösbar.
(ii) Alle endlichen p-Gruppen sind auflösbar nach Satz 17.1.
(iii) Die symmetrische Gruppe S_n ist für $n \in \{1,2,3,4\}$ auflösbar.

Alle endlichen abelschen Gruppen haben sogar Normalreihen mit zyklischen Faktoren. Dies führt leicht auf folgenden Satz:

Satz 20.5

Ist G eine endliche auflösbare Gruppe, dann hat G eine Normalreihe, deren Faktoren alle zyklisch und von Primzahlordnung sind.

Ein nützliches Hilfsmittel für den Nachweis der Auflösbarkeit ist ...

Satz 20.6

Ist G eine Gruppe, $N \trianglelefteq G$, dann gilt: G ist auflösbar genau dann, wenn N und G/N auflösbar sind.

Beweis

Übung! (Verwende Noethersche Isomorphiesätze.) □

Beispiel 20.7

In den Beispielen 18.8 hatten wir bereits die passenden Informationen gesammelt, um jetzt zu sehen:

(i) Ist G eine Gruppe der Ordnung pq mit Primzahlen p,q, dann ist G auflösbar.

(ii) Ist G eine Gruppe der Ordnung 105, dann ist G auflösbar.

Eine Reihe gruppentheoretischer Auflösbarkeitssätze zu Gruppen spezieller Ordnung wie in den obigen Beispielen haben Burnside auf den folgenden Satz geführt:

Satz 20.8 (p^aq^b-Satz von Burnside, 1904)

Seien p,q Primzahlen, $a,b \in \mathbb{N}_0$. Dann ist jede Gruppe der Ordnung p^aq^b auflösbar.

Einer der wichtigsten Bausteine für die Klassifikation der endlichen einfachen Gruppen war der berühmte Satz:

Satz 20.9 (Feit und Thompson, 1963)

Jede Gruppe ungerader Ordnung ist auflösbar.

Die Beweise dieser Sätze liegen außerhalb des Rahmens der Vorlesung. Beide benutzen Methoden der Darstellungstheorie endlicher Gruppen. Der Beweis des Burnsideschen Satzes ist damit recht kurz und elegant, während der Satz von Feit und Thompson wesentlich mehr Arbeit erfordert.
Wir werden auflösbare Gruppen und den Nachweis der Auflösbarkeit für weitere Gruppen später noch genauer untersuchen.

Bemerkung 20.10

Ist L/K eine metazyklische Körpererweiterung, dann folgt daraus, dass alle Erweiterungen Z_{i+1}/Z_i insbesondere separabel sind, dass auch L/K separabel ist (14.6). Ist L/K galoissch, so folgt mit dem Hauptsatz der Galoistheorie, dass L/K genau dann metazyklisch ist, wenn $G\left(L/K\right)$ auflösbar ist. Außerdem folgt mit Satz 17.1, dass L/K genau dann p-metazyklisch ist, wenn $G\left(L/K\right)$ eine p-Gruppe ist. Ist $\operatorname{Char} K \neq 2$, dann ist L/K genau dann 2-metazyklisch, wenn L aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht, da jede Körpererweiterung vom Grad 2 galoissch ist und durch Adjunktion einer Quadratwurzel entsteht.

Wir brauchen noch den folgenden **Verschiebungssatz**:

Satz 20.11

Sei L/K eine Körpererweiterung, und seien $Z_1 \subseteq Z_2$ und Z Zwischenkörper von L/K. Ist Z_2/Z_1 galoissch, so ist auch $Z \cdot Z_2/Z \cdot Z_1$ galoissch, und die Galoisgruppe dieser Erweiterung ist isomorph zu einer Untergruppe von $G\left(Z_2/Z_1\right)$.

Beweis
Nach Satz 14.15 ist Z_2 der Zerfällungskörper eines separablen Polynoms $f \in Z_1[X]$. Dann entsteht $Z \cdot Z_2$ durch Adjunktion der Nullstellen von f an $Z \cdot Z_1$, ist also endlich und normal über $Z \cdot Z_1$. Da f auch als Polynom in $Z \cdot Z_1[X]$ separabel ist, ist die Erweiterung $Z \cdot Z_2 / Z \cdot Z_1$ auch separabel, also insgesamt galoissch.
Den gesuchten Monomorphismus erhalten wir, wenn wir die Einschränkung der Automorphismen von $Z \cdot Z_2$ auf Z_2 betrachten (diese Abbildung ist offenbar injektiv!):

$$G\left(Z \cdot Z_2 / Z \cdot Z_1\right) \to G\left(Z_2 / Z_1\right),\ \sigma \mapsto \sigma|_{Z_2}$$ □

Satz 20.12

Sei $p \in \mathbb{N}$ eine Primzahl und L/K eine Körpererweiterung. Sind Z_1, Z_2 Zwischenkörper von L/K, für die Z_i/K metazyklisch (bzw. p-metazyklisch) ist ($i = 1,2$), so ist auch $Z_1 \cdot Z_2/K$ metazyklisch (bzw. p-metazyklisch).
Beweis
Sind

$$K = K_0^i \subseteq K_1^i \subseteq ... \subseteq K_{r_i}^i = Z_i$$

für $i = 1$ und $i = 2$ Körperketten entsprechend der obigen Definition, so ist

$$K = K_0^1 \subseteq K_1^1 \subseteq ... \subseteq K_{r_1}^1 = Z_1 \subseteq Z_1K_1^2 \subseteq ... \subseteq Z_1K_{r_2}^2 = Z_1Z_2$$

eine Körperkette, für die die Erweiterungen $Z_1K_{i+1}^2 / Z_1K_i^2$ nach dem vorhergehenden Satz zyklisch (bzw. vom Grad p oder 1) sind. Dies zeigt, dass $Z_1 \cdot Z_2/K$ metazyklisch (bzw. p-metazyklisch). □

Satz 20.13

Sei $p \in \mathbb{N}$ eine Primzahl, L/K eine metazyklisch (bzw. p-metazyklische) Körpererweiterung und N die galoissche Hülle von L/K. Dann ist N/K auflösbar (bzw. die Galoisgruppe von N/K ist eine p-Gruppe).
Beweis
Die zu L konjugierten Körper in N sind ebenfalls metazyklisch (bzw. p-metazyklisch) über K. Da N das Kompositum dieser endlich vielen Zwischenkörper ist, ist nach Satz 20.11 auch N/K metazyklisch (bzw. p-metazyklisch). Da N/K galoissch ist, folgt daraus mit dem Hauptsatz der Galoistheorie die Behauptung. □

Wir können nun das folgende hinreichende Kriterium für Auflösbarkeit beweisen:

Satz 20.14

Sei K ein Körper, $\operatorname{Char} K = p \in \mathbb{N}_0$, und sei $f \in K[X]$ ein irreduzibles, separables Polynom. Die Galoisgruppe $G(f)$ sei auflösbar, und es gelte $p \nmid |G(f)|$. Dann ist die Gleichung $f = 0$ durch Radikale auflösbar, und alle Lösungen sind Radikale.
Beweis
Sei L der Zerfällungskörper von f über K. Da $G(f)$ auflösbar ist, gibt es eine Kette von Untergruppen

$$G(f) = N_t \supset N_{t-1} \supset ... \supset N_1 \supset N_0 = \{\mathrm{id}\},$$

wobei jeweils N_{i-1} normal in N_i und N_i/N_{i-1} zyklisch von Primzahlordnung p_i ist. Nach dem Hauptsatz der Galoistheorie erhalten wir durch Bildung der entsprechenden Fixkörper dazu eine Kette von Zwischenkörpern von L/K:

$$K = Z_t \subset Z_{t-1} \subset ... \subset Z_1 \subset Z_0 = L,$$

wobei Z_{i-1}/Z_i eine zyklische Erweiterung vom Grad p_i ist. Sei $n = |L:K|$ und K' der n-te Kreisteilungskörper über K. Sei $L' = K'L$ das Kompositum von K' und L im algebraischen Abschluss $\overline{K}$. Da $n = p_1 \cdot ... \cdot p_t$, und $p \nmid n$, ist $p_i \neq p$ für $i = 1,...,t$. Da K' alle n-ten Einheitswurzeln enthält, enthält K' auch die p_i-ten Einheitswurzeln für $i = 1,...,t$. Wir erweitern nun in der obigen Körperkette alle Körper mit K':

$$K' = K'Z_t \subset K'Z_{t-1} \subset ... \subset K'Z_1 \subset K'Z_0 = L'.$$

Nach Satz 20.11 sind dann auch die Erweiterungen $K'Z_{i-1}/K'Z_i$ zyklisch für alle i. Nach Satz 20.1 existiert dann für jedes i ein $b_i \in K'Z_{i-1}$ und ein $m_i \in \mathbb{N}$, so dass $K'Z_i(b_i) = K'Z_{i-1}$ und $b_i^{m_i} \in K'Z_i$ gilt. Nach Definition ist also L'/K' eine Radikalerweiterung. Da auch K'/K eine Radikalerweiterung ist, ist also auch L'/K eine Radikalerweiterung. Da alle Nullstellen von f in L' liegen, folgt daraus der Satz. □

Folgerung 20.15

Sei K ein Körper, $f \in K[X]$ separabel und vom Grad ≤ 4, und es gelte $\mathrm{Char}\, K \nmid |G(f)|$. Dann ist f durch Radikale auflösbar, und alle Lösungen sind Radikale.

Satz 20.16

Sei K ein Körper der Charakteristik 0, und sei $f \in K[X]$ ein irreduzibles Polynom. Dann ist $f = 0$ genau dann durch Radikale auflösbar, wenn $G(f)$ auflösbar ist.

Beweis

Ist $G(f)$ auflösbar, dann ist $f = 0$ durch Radikale auflösbar nach Satz 20.14. Wir zeigen nun die Umkehrung und setzen daher jetzt voraus, dass f eine Nullstelle in einer Radikalerweiterung L von K besitzt. Es gibt also $b_1,...,b_t \in L$, $r_1,...,r_t \in \mathbb{N}$, so dass $L = K(b_1,...,b_t)$, $b_1^{r_1} \in K$, $b_i^{r_i} \in K(b_1,...,b_{i-1})$ für $i = 2,...,t$, gilt. Setze $Z_i = K(b_1,...,b_i)$ für $i = 0,...,t$. Weiter sei $n = r_1 \cdot ... \cdot r_t$ und K' der n-te Kreisteilungskörper über K. Dann enthält K' insbesondere auch alle r_i-ten Einheitswurzeln, für $i = 1,...,t$. Wir betrachten nun die Zwischenkörperkette

$$K \subset K' \subset K'Z_1 \subset ... \subset K'Z_t = L'.$$

Die Erweiterungen $K'Z_i/K'Z_{i-1}$ sind nach Satz 20.1 für $i = 1,...,t$ zyklisch, und die Erweiterung K'/K ist abelsch nach Satz 19.7. Dann ist insgesamt L'/K metazyklisch. Also ist die galoissche Hülle N von L'/K auflösbar nach Satz 20.13, d.h. $G\left(N/K\right)$ ist auflösbar. Da f eine Nullstelle in $L \subset N$ besitzt, ist der Zerfällungskörper Z von f ein Zwischenkörper von N/K. Außerdem ist Z/K galoissch. Nach dem Hauptsatz der Galoistheorie ist $G(f)$ eine Faktorgruppe von $G\left(N/K\right)$, und damit ist $G(f)$ ebenfalls auflösbar. □

Unsere Frage, ob algebraische Gleichungen stets durch Radikale auflösbar sind, gliedert sich also nun in zwei Teile:

- Gibt es Gruppen, die nicht auflösbar sind?
- Gibt es Polynome, deren Galoisgruppe eine solche nicht auflösbare Gruppe ist?

Wir wollen zunächst ein äquivalentes Kriterium für Auflösbarkeit angeben.

Definition 20.17

Sei G eine Gruppe. Sind $a,b \in G$, dann heißt das Element

$$[a,b] := aba^{-1}b^{-1}$$

der **Kommutator** von a und b. Die von den Kommutatoren erzeugte Untergruppe

$$G' := [G,G] := \langle [a,b] \mid a,b \in G \rangle$$

heißt die **Kommutatorgruppe** von G.

Wir setzen $G^{(0)} = G$, $G^{(1)} = G'$, und definieren induktiv für $i \in \mathbb{N}$:

$$G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right].$$

Die Untergruppe $G^{(i)}$ heißt die **i-te Kommutatorgruppe** von G.

Die Kette

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(j-1)} \supseteq G^{(j)} \supseteq \ldots$$

heißt die **Kommutatorreihe** von G.

Folgende nützliche Eigenschaften von Kommutatorgruppen sind leicht zu überprüfen:

Satz 20.18

Sei G eine Gruppe. Dann gilt:

(i) $G^{(i)}$ ist ein Normalteiler von G für alle $i \in \mathbb{N}$.

(ii) Die Faktorgruppe G/G' ist abelsch.

(iii) Ist $N \trianglelefteq G$ mit abelscher Faktorgruppe G/N, dann gilt $G' \subseteq N$.

(iv) Ist $U \leq G$, dann ist $U' \subseteq G'$. Ist $N \trianglelefteq G$, dann ist $\left(G/N\right)' = G'N/N$.

Bemerkung 20.19

(i) Eine Gruppe G ist genau dann abelsch, wenn $G' = \{1\}$ ist.

(ii) $S_n' \leq A_n$ für alle $n \in \mathbb{N}$, $S_n' = A_n$ für $n = 1,2,3$ ist leicht zu sehen.

(iii) $\mathrm{GL}_n(K)' \leq \mathrm{SL}_n(K)$ für alle Körper K und $n \in \mathbb{N}$.

(iv) $G^{(i)}$ ist sogar eine **charakteristische** Untergruppe von G, d.h. sie ist invariant unter allen Automorphismen von G.

Satz 20.20

Sei G eine Gruppe. Dann ist G auflösbar genau dann, wenn $G^{(j)} = 1$ für ein $j \in \mathbb{N}$.

Beweis

Ist $G^{(j)} = 1$, dann ist

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(j-1)} \supseteq G^{(j)} = 1$$

eine (endliche) Normalreihe mit abelschen Faktoren, also ist G auflösbar.

Ist umgekehrt G auflösbar und

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_{n-1} \supseteq G_n = 1$$

eine Normalreihe mit abelschen Faktoren, dann zeigen wir mit Induktion nach n: $G^{(n)} = 1$. Ist $n = 0$, dann ist $G = G_0 = 1$ und die Behauptung klar.

Da mit G auch G_1 auflösbar ist und G_1 die Normalreihe

$$G_1 \supseteq \ldots \supseteq G_{n-1} \supseteq G_n = 1$$

der Länge $n-1$ hat, folgt nach Induktionsvoraussetzung $G_1^{(n-1)} = 1$. Außerdem ist $G' \subseteq G_1$ nach Satz 20.18. Also folgt

$$G^{(n)} = G'^{(n-1)} \subseteq G_1^{(n-1)} = 1. \qquad \square$$

Beispiel 20.21

Sei $G = S_4$. Dann ist die Kommutatorreihe von S_4

$$S_4 \supset A_4 \supset V_4 \supset 1,$$

insbesondere zeigt dies die Auflösbarkeit von S_4.

Satz 20.22

(i) $S_n' = A_n$ für $n \in \mathbb{N}$.

(ii) $A_n' = 1$ für $n \leq 3$, $A_4' = V_4$, $A_n' = A_n$ für $n \geq 5$.

Beweis

Die Aussagen in (i), (ii) für $n \leq 4$ haben wir bereits gezeigt.

Wir zeigen zunächst, dass für $n \geq 3$ die alternierende Gruppe A_n von den 3-Zyklen erzeugt wird. Dazu müssen wir nur zeigen, dass das Produkt von je zwei Transpositionen ein Produkt von 3-Zyklen ist. Seien also a,b,c drei verschiedene bzw. a,b,c,d vier verschiedene Zahlen in $\{1,...,n\}$. Es gilt dann:

$$(a\ b)(a\ c) = (a\ c\ b)$$
$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d).$$

Sei nun $n \geq 5$, und seien a,b,c drei verschiedene Zahlen, d,e zwei weitere Zahlen in $\{1,...,n\}$ mit $|\{a,b,c,d,e\}| = 5$. Dann ist

$$(a\ b\ c) = [(a\ b\ d),(c\ e\ a)]$$

ein Kommutator von Elementen aus A_n. Da A_n von den 3-Zyklen erzeugt wird, ist dann $A_n \leq A_n' \leq S_n'$. Da S_n/A_n abelsch ist, folgt $A_n = S_n' = A_n'$. □

Es folgt daraus mit Satz 20.20 insbesondere:

Folgerung 20.23

Für $n \geq 5$ sind die symmetrische Gruppe S_n und die alternierende Gruppe A_n nicht auflösbar.

Wir wollen nun klären, ob es Polynome in $\mathbb{Q}[X]$ gibt, deren Galoisgruppe nicht auflösbar ist, und die daher nicht durch Radikale auflösbar sind.

Satz 20.24

Sei p eine Primzahl, $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p, das in $\mathbb{C}$ genau zwei nichtreelle Nullstellen hat. Dann ist die Galoisgruppe $G(f)$ isomorph zu S_p.

Beweis

Da $\mathbb{C}$ den Zerfällungskörper von f über $\mathbb{Q}$ enthält, hat f in $\mathbb{C}$ genau p Nullstellen, von denen $p-2$ reell sind. Die beiden nichtreellen Nullstellen müssen konjugiert komplex zueinander sein. Also enthält $G(f)$ als Permutationsgruppe auf den Nullstellen betrachtet eine Transposition, nämlich den von der komplexen Konjugation induzierten Automorphismus auf dem Zerfällungskörper von f über $\mathbb{Q}$. Andererseits enthält $G(f)$ ein Element der Ordnung p, da f irreduzibel und vom Grad p ist. Eine Untergruppe der S_p, die eine Transposition und ein Element der Ordnung p enthält, ist aber bereits gleich der ganzen Gruppe S_p (Übung!). Also ist $G(f) \cong S_p$. □

Beispiel 20.25

Das Polynom $X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist irreduzibel und hat genau 3 reelle Nullstellen (Kurvendiskussion!), also hat dieses Polynom die Galoisgruppe S_5.

Folgerung 20.26 (Galois)

Es gibt irreduzible Polynome 5. Grades in $\mathbb{Q}[X]$, die nicht durch Radikale auflösbar sind.

Index