http://www.mathematik-netz.de

Struktur eines Körpers
- algebraische und tranzendente Körpererweiterungen

Alexander von Felbert

Köln, September 2006
München, Mai 2011

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Überblick

Das Hauptziel der klassische Algebra ist die Lösung von Gleichungen der Form

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 X^0 = 0,$$

wobei man insbesondere an konkreten Lösungsformeln für eine beliebige Gleichung n-ten Grades interessiert ist. Beide Aufgaben sind sicher recht konkret und naheliegend. Im Laufe einer jahrhundertelangen Entwicklung hat sich herausgestellt, dass die Beantwortung beider Probleme überaus schwierig und dass dazu ein gewaltiger begrifflicher und theoretischer Apparat notwendig ist. Sogenannte „Körpererweiterungen“ bilden eine Vorstufe zur Galois-Theorie, die eine Antwort auf die Existenz von allgemeinen Lösungsformlen für Gleichungen n-ten Grades gibt und daher eine Hauptrolle in der klassischen Algebra einnimmt.

Zu Beginn des zweiten Kapitels werden wir uns zunächst mit den grundlegenden „Bausteine“ eines Körpers beschäftigen, den so genannten Primkörpern. Ein Primkörper ist bezüglich der Mengeninklusion $\subset$ der kleinste Körper in einer Reihe von Körpererweiterungen. Bereits Steinitz erkannte die fundamentale Bedeutung von Primkörpern im Kontext von Körpererweiterungen.

Im dritten Kapitel werden wir – ausgehend von den möglichen Primkörpern – endliche oder unendliche Erweiterung anwenden und zumind. die Klasse der algebraischen Körper vollständig charakterisieren. Hingegen beschränken wir uns bei den sognannten transzendenten Erweiterungen auf den einfachsten Fall. Dabei werden wir feststellen, dass eine Körpererweiterungen grundsätzlich über zwei äquivalente Wege möglich ist. Zum Einen durch eine sogn. Adjunktion eines oder mehrerer Elemente oder die Konstruktion eines Erweiterungskörpers mit Hilfe des assoziierten Polynomrings $K[X]$ und eines irreduzibles Polynoms μ. Viele Beispiele werden für das notwendige Verständnis quer durch das Dokument sorgen.

Für das Verständnis dieses Dokumentes sollte der Leser elementare Begriffe der Alegebra und deren Charakteristika wie z.B. Ring, Unterring, Ideal, Faktorring, maximales Ideal oder Hauptideal kennen und beherrschen. Grundsätzlich werden wir versuchen die wichtigsten Grundlagen im nächsten Teilabschnitt prägnant bereitzustellen.

1.2 Algebraische Grundlagen

Dieser Abschnitt dient der Wiederholung und Auffrischung von Grundlegendem der Ringtheorie. Bitte beachten Sie, dass wir in diesem Abschnitt keine Beweise führen und nur ausgesuchte Themen aufführen. Ansonsten wird auf die Literatur verwiesen.

Die Menge der natürlichen Zahlen notieren wir durch $\mathbb{N} = \{1, 2, 3, \ldots\}$, die der ganzen Zahlen durch $\mathbb{Z}$, die der rationalen Zahlen durch $\mathbb{Q}$ und schließlich die reellen Zahlen

durch $\mathbb{R}$. Mit $\mathbb{C}$ sei die Menge der komplexen Zahlen bezeichnet. Ferner sei durch $\mathbb{N}_n = \{1, \ldots, n\}$ mit $n \in \mathbb{N}$, die Menge der ersten n natürlichen Zahlen bezeichnet.

1.1 Definition: Ein Tripel $(R, +, \cdot)$ bestehend aus einer nicht leeren Menge R und zwei inneren Verknüpfungen

$+$ $R \times R \to R$, mit $(a, b) \mapsto a + b$ (Addition)

$\cdot$ $R \times R \to R$, mit $(a, b) \mapsto a \cdot b$ (Multiplikation)

heißt **Ring**, wenn gilt:

(R_1) $(R, +)$ ist eine kommutative Gruppe.

(R_2) $(R, \cdot)$ ist eine Halbgruppe mit Einselement.

(R_3) Für alle $a, b, c \in R$ gelten die Distributivgesetze:

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Der Ring heißt **unitär**, falls ein Einselement $1 \in R$ bezüglich der Multiplikation existiert, d.h. $a \cdot 1 = 1 \cdot a = a$ für alle $a \in R$. Der Ring R heißt **kommutativ** oder **abelsch**, falls für die Multiplikation das Kommutativgesetz gilt.

Einer der wichtigsten Konstrukte aus der Ringtheorie ist der des *Ideals* – das sind Teilmengen eines Ringes R, die gewisse Bedingungen bezüglich ihrer Verknüpfungen erfüllen. Mit ihnen lassen sich neue Ringe konstruieren und die Strukur von Ringen charakterisieren.

1.2 Definition: Sei $(R, +, \cdot)$ ein Ring. Ein **Ideal** $\mathfrak{a}$ in R ist eine Untergruppe von $(R, +)$, so dass für alle $a \in \mathfrak{a}$ und alle $r \in R$ die Elemente ar und ra in $\mathfrak{a}$ liegen. Ist $\mathfrak{a}$ ein Ideal in R, so schreiben wir kurz $\mathfrak{a} \lhd R$. Ein **echtes Ideal** ist ein von R verschiedenes Ideal.

Ein Ideal ist also nichts anderes als eine additive Untergruppe $\mathfrak{a} \leq R$ eines Ringes R, wobei $\mathfrak{a}$ auch gegenüber der Multiplikation abgeschlossen ist. Ideale enthalten also alle „Linearkombinationen“ eines Ringelementes bezüglich der Ringaddition und -multiplikation.

1.3 Definition (Unterring): Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$, dann heißt S zusammen mit den auf S eingeschränkten Verknüpfungen des Ringes R **Unterring**, wenn $(S, +, \cdot)$ selbst ein Ring ist.

Ein Unterring S eines Ringes R kann durch die folgende Proposition charakterisiert werden.

1.4 Proposition (Unterringkriterium): Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$, dann ist S genau dann ein Unterring von R, wenn

(i) $\forall a, b \in S : a - b \in S$;

(ii) $\forall a, b \in S : ab \in S$;

(iii) $1 \in S$.

Beweis. 14.7 [10]. □

Lässt man nun die Forderung nach $1 \in S$ fallen, wie es manche Autoren bereits bei der Definition eines Ringes bzw. Unterringes tun, so wird die Verbindung zwischen Idealen und Unterringen klar. Dabei spielen die Ideale eine ähnliche Sonderrolle, wie die Nebenklassen in der Gruppentheorie.

1.5 Beispiel:

a) In jedem Ring R sind $\{0\}$ und R Ideale, diese nennt man sinnfälliger Weise auch *triviale Ideale* von R. Das $\{0\}$ ein Ideal von R ist, folgt mit der besonderen Eigenschaft des Nullelements, denn $\forall a \in R$ gilt: $a \cdot 0 = 0 \cdot a = 0 \in \{0\}$. Nach Definition eines Ringes muss auch R ein Ideal sein.

b) Sei $n \in \mathbb{N}, n > 1$. Dann ist $n\mathbb{Z} := \{nz | z \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$. Die Menge $n\mathbb{Z}$ enthält also alle ganzzahligen Vielfachen von n – die notwendigen Bedingungen für ein Ideal sind also bereits a priori gemäß Definition erfüllt.
Es seien $a, b \in \mathbb{Z}$, dann wird durch $a \sim_n b :\Leftrightarrow n \mid (a - b) \Leftrightarrow \exists x \in \mathbb{Z}$, so dass $(a - b) = nx$. Die Differenz $a - b$ muss also ein x-faches von n sein. Dadurch wird eine Äquivalenzrelation definiert und die Äquivalenzklassen $\{nz | z \in \mathbb{Z}\}$ teilen die Menge $\mathbb{Z}$ in disjunkte Klassen auf.
Wir sehen also, dass die Äquivalenzklassen gerade den Idealen des Ringes $(\mathbb{Z}, +, \cdot)$ entsprechen.

c) Für jedes $a \in R$ ist $(a) := Ra = \{ra | r \in R\}$ a priori ein Ideal: Das von einem Element $a \in R$ erzeugte Ideal (a), dessen Elemente sich in folgender Gestalt ausdrücken lassen

$$ra + na \qquad \text{mit } r \in R, n \in \mathbb{Z}$$

ist stets ein Ideal: Die Differenz zweier solcher Ausdrücke kann offenbar wieder in dieselbe Darstellung gebracht werden, und ein beliebiges ganzzahliges Vielfaches hat die Form

$$s \cdot (ra + na) = (sr + ns) \cdot a$$

also die Form $r'a$ oder $r'a + 0 \cdot a$. Damit ist das Ideal offenbar das kleinste (am wenigsten umfassende) Ideal, dass a enthält; denn jedes solche Ideal muss mindestens alle Vielfachen ra und alle Summen $\pm \sum a = na$ enthalten, also auch alle Summen $ra + na$. Deshalb kann das Ideal (a) auch als Durchschnitt aller Ideale, die a enthalten definiert werden.

Wir sehen, dass $n\mathbb{Z}$ ein Spezialfall dieser allgmeineren Definition ist.

d) Ein weiterer wichtiger Spezialfall des letzten Beispiels c) ist: Es seien $R := \mathbb{K}[X], \mathbb{K}$ ein Körper, und $f := \sum_{i=0}^{n} a_i \cdot X^i$ ein Polynom in $\mathbb{K}[X]$. Dann ist $(f) = \{fg | g \in \mathbb{K}[X]\}$ ein Ideal in $\mathbb{K}[X]$.

e) Sei $R = \mathbb{Q}$. Zwar ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, allerdings kein Ideal. Es ist beispielsweise $1 \in \mathbb{Z}, 1/2 \in \mathbb{Q}$, aber $1 \cdot 1/2 \notin \mathbb{Z}$.

Völlig analog zum Homomorphiesatz von Gruppen gilt folgender

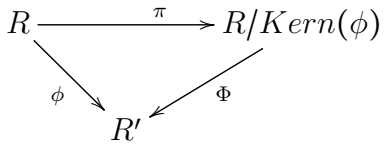
1.6 Satz (Homomorphiesatz für Ring): Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann ist $R/\text{Kern}(\phi)$ isomorph zu $\text{Bild}(\phi)$. Genauer, es ist

$$\begin{aligned} \Phi : R/\text{Kern}(\phi) &\to \text{Bild}(\phi) \\ \overline{r} &\mapsto \phi(r) \end{aligned}$$

ein Isomorphismus von Ringen.

Beweis. Satz 3.1.14, [2]. □

Der Homomorphiesatz kann durch ein kommutatives Diagramm veranschaulicht werden. Dazu sei $\phi : R \to R'$ ein Gruppen-Homomorphismus. Dann existiert nach dem Homomorphiesatz ein eindeutig bestimmter Homomorphismus $\Phi : R/Kern(\phi) \to R'$ mit $\Phi \circ \pi = \phi$, so dass das folgende Diagramm kommutiert:



1.7 Definition: Sei $(R, +, \cdot)$ ein Ring und $r \in R$ ein Ringelement.
Wir nennen r einen **Linksnullteiler** in R, wenn es ein $s \in R \setminus \{0\}$ mit $rs = 0$ gibt. Analog nennen wir r einen **Rechtsnullteiler**, wenn es ein $s \in R \setminus \{0\}$ mit $sr = 0$ gibt. Wir nennen ein Ringelement r **Nullteiler**, falls es ein Links- oder Rechtsnullteiler ist. Anderenfalls heißt r auch ein **Nichtnullteiler**.

In kommutativen Ringen fallen die drei Nullteilerbegriffe offenbar zusammen.

1.8 Definition:

1. Ein Ring $(R, +, \cdot)$ heißt **nullteilerfrei**, falls jedes von 0 verschiedene Element von R ein Nichtnullteiler ist.

2. Ein Ring R heißt ein **Bereich**, wenn er nullteilerfrei und vom Nullring verschieden ist.

3. Ein kommutativer Bereich heißt ein **Integritätsbereich** oder **Integritätsring**.

4. Sei R ein Integritätsring, und seien $r, s \in R$. Wir sagen, dass a das Element b teilt und schreiben dafür $a|b$, wenn $a' \in R$ gibt, so dass $aa' = b$ ist.

1.9 Proposition: Sei R ein Integritätsbereich. Dann gilt für alle $a, b, c \in R$:

(i) Wenn $ab = ac$ und $a \neq 0$, so folgt $b = c$;

(ii) Wenn $a|b$ und $b|c$, so folgt $a|c$;

(iii) Wenn $a|b$ und $a|c$, so folgt $a|(b+c)$;

(iv) Wenn $a|b$, so gilt $a|(bc)$ für alle $c \in R$.

Beweis. (i) Sei $ab = ac$ mit $a \neq 0$, durch Addition von $-ac$ und Ausmultiplizieren erhalten wir daraus $a(b-c) = 0$. Da R ein Integritätsring ist, folgt $(b-c) = 0$ was $b = c$ implziert.

(ii) Aus $a|b$ und $b|c$ folgt die Existenz von $a', b' \in R$ mit $aa' = b$ sowie $bb' = c$. Fasst man dies zusammen, so erhalten wir $(aa')b' = a(a'b') = c$, d.h. $a|c$.

(iii) Seien $aa' = b$ und $aa* = c$, dann ist $b + c = aa' + aa* = a(a' + a*)$, d.h. $a|(b+c)$.

(iv) Sei $aa' = b$, so folgt $a(a'c) = bc \Leftrightarrow a|bc$ für alle $c \in R$.

□

Je nachdem welche Eigenschaften Ringe besitzen, erhalten diese ausgezeichneten Ringe eigene Namen.

1.10 Definition: 1. Ein kommutativer Ring $(R, +, \cdot)$ heißt **Schiefkörper**, wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.

2. Ein kommutativer Schiefkörper wird ein **Körper** genannt.

Natürlich ist jeder Schiefkörper $(R, +, \cdot)$ ein Integritätsbereich.

1.11 Proposition: In jedem Schiefkörper R folgt aus $ab = 0$, dass $a = 0$ oder $b = 0$ gilt. Jeder Schiefkörper ist somit ein Integritätsring.

Beweis. Wir zeigen zunächst, dass $r \cdot 0 = 0$ ist, für alle $r \in R$. Es gilt $r \cdot 0 = r \cdot (0+0) = r \cdot 0 + r \cdot 0$. Durch Subtraktion auf beiden Seiten der Gleichung folgt die Behauptung. Seien nun $a, b \in R$ mit $ab = 0$. Wenn $a = 0$, so sind wir fertig. Sei also $a \neq 0$, dann müssen wir zeigen, dass $b = 0$ ist. Dazu multiplzieren wir $ab = 0$ auf beiden Seiten von links mit a^{-1}, dadurch ergibt sich $a^{-1}ab = b = 0$. Damit ist R nullteilerfrei und es gilt gemäß Definition $1 \neq 0$, woraus folgt, dass R ein Integritätsring ist. □

1.12 Proposition: Jeder Integritätsring, der nur endlich viele Elemente enthält, ist ein Körper.

Beweis. Seien R ein Integritätsring bestehend aus den verschiedenen Elementen $\{a_1, \ldots, a_n\}$ und $a \in R \setminus \{0\}$. Sodann bilden wir die Produkte

$$aa_1, \ldots, aa_n,$$

die allesamt verschiedene Elemente aus R repräsentieren. Angenommen dem wäre nicht so, d.h. $aa_i = aa_j$ mit $i \neq j$ und $i, j \in \mathbb{N}_n$. Durch Subtraktion von aa_j und Ausmultiplizieren erhalten wir $a \cdot (a_i - a_j) = 0$. Da R ein Integritätsring ist, muss entweder $a = 0$ oder $(a_i - a_j) = 0$ sein. Gemäß Voraussetzung ist demnach $a_i - a_j = 0 \Leftrightarrow a_i = a_j$, was gemäß Voraussetzung nicht sein kann. Die Elemente $aa_1, \ldots, aa_n$ sind also allesamt verschieden. Eines der Produkte daraus stellt das Einselement des Ringes dar, d.h. es gilt $aa_i = 1$. Da R kommutativ ist, folgt auch $a_i a = 1$. Somit hat jedes Element in $R \setminus \{0\}$ ein inverses Element. Mit anderen Worten $(R \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe und damit $(R, +, \cdot)$ ein Körper. □

1.3 Der Quotientenkörper

Seien $R \neq \{0\}$ ein Integritätsbereich und $R^\times := R \setminus \{0\}$, dann ist auf der Menge der Paare $(a, b) \in R \times R^\times$ die Beziehung

$$(a, b) \sim (c, d) \;:\Leftrightarrow\; ad = bc \;\Leftrightarrow\; \frac{a}{b} = \frac{c}{d} \quad \text{mit } b, d \neq 0$$

eine Äquivalenzrelation.

Beweis. Es ist $(a, b) \sim (a, b)$, da R als Integritätsring kommutativ ist und somit $ab = ba$, die Reflexivität von $\sim$, gilt. Ist $(a, b) \sim (c, d) \Leftrightarrow ad = bc$, dann folgt mit der Kommutativität $cb = da$ und damit $(c, d) \sim (a, b)$. Es ist $\sim$ demnach symmetrisch. Bleibt nur noch die Transitivität nachzuweisen: Dazu sei $(a, b) \sim (c, d)$ sowie $(c, d) \sim (e, f)$, dann ist $ac = bd$ sowie $cf = de$. Multiplizieren wir letztere Gleichung mit b von links und die andere mit f von rechts, so erhalten wir $adf = bcf = bde$. Da $d \neq 0$ und da R ein Integritätsring ist, folgt mit Proposition 1.9 (i), dass $af = be$. Demnach ist $(a, b) \sim (e, f)$, was noch zu zeigen war. □

1.13 Definition: Die Äquivalenzklasse, die das Paar (a, b) bezüglich $\sim$ enthält, wird Quotient von a durch b genannt und durch $\frac{a}{b}$ notiert.

1.14 Beispiel: Sei $R = K[X]$ der Polynomring über dem Körper K. Da $K[X]$ ein Integritätsbereich ist, können wir die eben eingeführte Relation darauf anwenden. Dazu seien $f, g \in K[X]$ mit $g \neq 0$. Sei d ein größter gemeinsamer Teiler von f und g, und seien $f = df'$ und $g = dg'$. Dann gilt

$$\frac{f}{g} = \frac{f'}{g'} = \frac{hf'}{hg'} \qquad \forall h \in K[X] \setminus \{0\}.$$

Beweis. Da $g \neq 0$ ist $g' \neq 0$, d.h. die Notation $\frac{f'}{g'}$ ist legitim. Durch Multiplikation der Gleichungen $f = df'$ und $g = dg'$ mit f' bzw. g' erhalten wir

$$fg' = f'dg' = f'g = gf',$$

d.h. es ist $(f, g) \sim (f', g')$. Dann liegt (f, g) in der Äquivalenzklasse, die (f', g') enthält. Da Äquivalenzklassen gleich oder disjunkt sind, folgt $\frac{f}{g} = \frac{f'}{g'}$. Sei nun $h \in K[X]$, $h \neq 0$. Dann ist $hg' \neq 0$ und es gilt $f'hg' = g'hf'$, d.h. $(f', g') \sim (hf', hg')$. Die Vielfachen von (hf', hg') liegen demnach in derselben Äquivalenzklasse wie (f', g'), d.h. es ist $\frac{f'}{g'} = \frac{hf'}{hg'}$. □

Als nächstes definieren wir zwei Abbildungen auf der Menge der Äquivalenzklassen. Dazu seien $\frac{a}{b}$ und $\frac{c}{d}$ in Q, sodann erklären wir

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \in Q \qquad \text{sowie} \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \in Q.$$

Dass es sich bei diesen Definitionen tatsächlich um Verkünpfungen handelt, müssten man noch die Wohldefiniertheit nachweisen. Wir überspringen dies und verweisen stattdessen auf [9]. Für alle $\frac{a}{b} \in Q$ gilt

$$\frac{a}{b} + \frac{0}{1} = \frac{0}{1} + \frac{a}{b} = \frac{a}{b}$$
$$\frac{a}{b} + \frac{-a}{b} = \frac{ab-ab}{b^2} = \frac{0}{b^2} = \frac{0}{1}$$

und

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b}.$$

Für alle $\frac{a}{b} \neq \frac{0}{1}$ gilt

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$$

und ein Standardbeweis zeigt, dass $(Q, +, \cdot)$ die weiteren Körperaxiome erfüllt.

1.15 Definition (Quotientenkörper): Der Körper $(Q, +, \cdot)$ heißt **Quotientenkörper** zum Integritätsring R.

Identifizieren wir die Elemente r des Integritätsrings R mit den Elementen $\frac{r}{1} \in Q$, so betten wir auf diese Weise R in die Menge Q ein und können R als dazu isomorphen Unterring von Q auffassen.

1.16 Proposition: Zu jedem Integritätsring $R \neq \{0\}$ gibt es einen Körper Q, den Quotientenkörper von R, so dass R ein Unterring von Q ist.

1.17 Beispiel: Betrachten wir z.B. den Integritätsring $\mathbb{Z}$, so erhalten wir aus obiger Konstruktion den Körper $\mathbb{Q}$ der rationalen Zahlen. Gehen wir vom Polynomring $K[X]$ aus, so erhalten wir den **Körper der rationalen Funktionen**

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

Im Beispiel oben haben wir gesehen, dass $\frac{f}{g} = \frac{f'}{g'}$, wobei $f = df'$ und $g = dg'$ und d ein größter gemeinsamer Teiler von f und g ist. Daher sind die Polynome f' und g' teilerfremd, weshalb

$$\begin{aligned} K(X) &= \left\{ \frac{f}{g} \mid f, g \in K[X];\ g \neq 0 \right\} \\ &= \left\{ \frac{p}{q} \mid p, q \in K[X];\ q \neq 0;\ p, q \text{ teilerfremd} \right\} \end{aligned}$$

gilt.

2 Primringe und Primkörper

Ein Körper $(K, +, \cdot)$ kann als ein kommutativer Ring mit Null- und Einselement interpretiert werden. Es ist also K genau dann ein (nicht trivialer) Körper, wenn $(K, +)$ eine abelsche Gruppe mit neutralem Element 0 und die Einheitengruppe $(K^\times, \cdot)$ eine abelsche Gruppe mit dem neutralen Element 1 ist. Zudem ist das Zusammenspiel beider Gruppen durch ein Distributivgesetz geregelt.

Wir vereinbaren, dass wir unter einem Ring in diesem Dokument stets einen unitären Ring (also einem Ring mit Einselement) verstehen.

2.1 Primringe und Ringhomomorphismen

Seien $(\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen und $(R, \hat{+}, \hat{\cdot})$ ein beliebiger Ring mit e als Einselement, dann heißt $\phi : \mathbb{Z} \to R$ definiert durch

$$n \mapsto \phi(n) := n * e := \underbrace{e \hat{+} \ldots \hat{+} e}_{n \text{ Summanden}}$$

kanonischer Ringhomomorphismus. Aus dem Unterringkriterium 1.4 und den Rechenregeln für Ringe folgt unmittelbar, dass

$$\text{Bild}(\phi) := \mathbb{Z} * e = \{\phi(n) | \quad n \in \mathbb{Z}\}$$

ein Unterring von R ist. Vergleichen Sie bitte $\mathbb{Z} * e$ mit Beispiel 1.5 b). Dass ϕ tatsächlich ein Homomorphismus ist, weisen wir als nächstes nach. Dabei soll die bereits eingeführte Notation übernommen werden.

2.1 Proposition: Die Abbildung $\phi : \mathbb{Z} \to R$ ist ein Ringhomomorphismus bei dem $\text{Bild}(\phi)$ der bezüglich der Inklusion kleinste Unterring von R ist.

Beweis. Seien $m, n \in \mathbb{Z}$ beliebig gewählt, dann gilt

$$\phi(m+n) = (m+n) * e = \underbrace{e \hat{+} \ldots \hat{+} e}_{(m+n) \text{ Summanden}} = (m * e) \hat{+} (n * e) = \phi(m) \hat{+} \phi(n).$$

Analog folgt für $m, n \in \mathbb{Z}$ die Gleichung

$$\phi(mn) = (mn) * e = (mn) * e^2 = (m * e) \hat{\cdot} (n * e) = \phi(m) \hat{\cdot} \phi(n).$$

Unmittelbar aus der Definition folgt $\phi(1) = 1 * e = e$. Wir haben bereits nachgewiesen, dass $\text{Bild}(\phi) = \mathbb{Z} * e$ ein Unterring von R ist, bleibt noch zu zeigen, dass $\mathbb{Z} * e$ der kleinste Unterring von R ist. Nehmen wir dazu an, dass S ein Unterring von R ist, d.h. $S \leq R$. Das Einselement e ist in S enthalten, ferner muss

$$n * e = \underbrace{e \hat{+} \ldots \hat{+} e}_{n \text{ Summanden}} \in S \qquad \forall n \in \mathbb{Z}$$

gelten, was $\mathbb{Z} * e \subseteq S \subseteq \text{Bild}(\phi) = \mathbb{Z} * e$ impliziert. Daraus folgt $S = \text{Bild}(\phi) = \mathbb{Z} * e$. □

Diesen bezüglich der Inklusion kleinsten Ring zeichnen wir durch einen Namen aus.

2.2 Definition: Seien R ein Ring und e das neutrale Element der Multiplikation in R. Der Unterring $\mathbb{Z} * e$ von R wird **Primring** genannt und mit $P(R)$ bezeichnet.

Wendet man nun den Homomorphiessatz für Ringe 1.6 auf ϕ an, so induziert dieser die Existenz eines Monomorphismus $\Phi : \mathbb{Z}/Kern(\phi) \to R$ und die Isomorphie

$$\mathbb{Z}/\text{Kern}(\phi) \cong \mathbb{Z} * e,$$

wobei Kern(ϕ) ein Ideal von $\mathbb{Z}$ ist. Wir können also den Primring eines jeden Ringes R isomorph mit Hilfe von $\mathbb{Z}/\text{Kern}(\phi)$ beschreiben.

2.2 Die Charakteristik eines Ringes

Wir übernehmen die im letzten Teilabschnitt eingeführte Notation. Die Struktur des Primrings ist also insbesondere durch das Ideal Kern(ϕ) determiniert, daher untersuchen wir zunächst die Struktur der Ideale in $\mathbb{Z}$. Die trivialen Ideale von $\mathbb{Z}$ sind $\{0\}$ und $\mathbb{Z}$ selbst. Wir wissen, dass $\mathbb{Z}$ zyklisch ist, das bedeutet auch, dass alle Untergruppen (also insbesondere auch die Ideale) zyklisch sind. Für die Ideale bedeutet das aber gerade, dass es sich um Hauptideale handelt! Zu einem beliebigen Ideal I von $\mathbb{Z}$ existiert demnach ein Element $m \in \mathbb{Z}$, so dass $I = (m) := \{nm |\ n \in \mathbb{Z}\}$.

Die Zahl m, welche ein beliebiges Ideal aus $\mathbb{Z}$ erzeugt, werden wir im Folgenden konstruieren. Dazu sei $k \in I$, dann ist $-k \in I$, da ein Ideal eine abelsche additive Gruppe ist. In jedem Fall existiert eine positive Zahl in I, welche wir mit $m \in I$ bezeichnen. Die durch m erzeugte Menge

$$(m) = \{mn |\ n \in \mathbb{Z}\} \subseteq I$$

ist somit in I enthalten. Sei nun $a \in I$ ein beliebiges Element aus $I \setminus \{0\}$, welches wir durch m mit Rest teilen. Wir erhalten

$$a = mq + r \text{ mit } r, q \in \mathbb{Z}, 0 \leq r < m.$$

Ist $r \neq 0$, so gilt $0 < a - mq = r < m$ und $r \in I$, was nicht sein kann, da m die kleinste positive Zahl in I ist. Es muss daher $r = 0$ gelten, woraus $a = qm \in I$ folgt. Daher ist $I \subseteq (m)$ woraus mit dem bereits Gezeigtem die Identität $I = (m)$ folgt.

Bemerkung: Ideale in $\mathbb{Z}$ sind also von der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}_0$.

Handelt es sich beim Ring R im kanonischen Ringhomomorphismus $\phi : \mathbb{Z} \to R$ um einen Integritätsbereich (etwa einem Körper), so der Faktorring $\mathbb{Z}/\text{Kern}(\phi)$ ein Integritätsbereich und somit Kern(ϕ) ein Primideal. Dann ist Kern(ϕ) entweder das Nullideal oder aber ein Ideal, welches von einer Primzahl p erzeugt wird.

Wir können also grundsätzlich zwei Fälle unterscheiden:

Fall 1: Sei $\mathrm{Kern}(\phi) = \{0\}$, dann folgt mit dem Homomorphiesatz, dass $\mathbb{Z}/\{0\} \cong \mathbb{Z}$. Es ist also $\phi(n) \neq 0$ für alle $n \in \mathbb{Z} \setminus \{0\}$, d.h. ϕ ist injektiv.

Fall 2: Sei $\mathrm{Kern}(\phi) = m\mathbb{Z}$ für ein gewisses $m \in \mathbb{N}$. Ist m eine Primzahl, dann ist $\mathbb{Z}/m\mathbb{Z}$ ein endlicher Körper $\mathbb{F}_p$ mit p Elementen, da dann $\mathrm{Kern}(\phi)$ ein maximales Ideal ist. Ist m dagegen keine Primzahl, so ist $\mathbb{Z}/m\mathbb{Z}$ kein Körper und auch kein Integritätsbereich, da dann $\mathrm{Kern}(\phi)$ nicht einmal ein Primideal ist. Für alle $m \in \mathbb{N}_0$, $\overline{m} \in \mathbb{Z}/\mathrm{Kern}(\phi)$ und für die aus dem Homomorphiesatz induzierte Funktion $\Phi(\overline{x}) := \phi(x)$ gilt

$$\Phi(\overline{m}) = \Phi(\overline{0}) = m * e = \underbrace{e \hat{+} \ldots \hat{+} e}_{n \text{ Summanden}} = 0,$$
$$\underbrace{\Phi(\overline{1})}_{\neq 0} = e, \ldots, \underbrace{\Phi(\overline{m-1})}_{\neq 0} = (m-1) * e.$$

Somit ist m die *kleinste positive Zahl* mit $m * e = 0$.

Diese kleinste natürliche Zahl mit $m * e = 0$ wird in der nächsten Definition der sogn. *Charakteristik* eines Ringes R münden. Zuvor konstatieren wir noch die

2.3 Folgerung: Sei R ein Ring mit Primring $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$. Dann gilt $n * a = 0$ für alle $a \in R$, falls n ein ganzes Vielfaches von m ist.

Beweis. Sei $n = qm$ für ein $q \in \mathbb{Z}$. Da $m * e = 0$ folgt

$$\phi(qm) = (qm * e) = n * e = \underbrace{e \hat{+} \ldots \hat{+} e}_{qm \text{ Summanden}} = q * (\underbrace{e \hat{+} \ldots \hat{+} e}_{m \text{ Summanden}}) = q * 0_R = 0_R,$$

wobei 0_R das Nullelement von R sei. Insgesamt folgt $n*a = q*(m*e)a = (q*0_R)a = 0_R$. □

Nun schließlich die zentrale Definition dieses Abschnittes.

2.4 Definition: Sei R ein Ring mit Primring $P(R)$.

(i) Wenn $P(R) \cong \mathbb{Z}$ ist, dann sagen wir, dass R die **Charakteristik** 0 hat und schreiben $char(R) = 0$.

(ii) Wenn $P(R) \cong \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$ ist, dann sagen wir, dass R die Charakteristik m hat, bzw., dass R **positive Charakteristik** hat, und schreiben $char(R) = m$.

2.3 Der Primkörper

Der folgende Satz zeigt einen sehr schönen Zusammenhang zwischen Integritätsringen und Primzahlen auf. Vergleichen Sie bitte auch mit dem in letzten Abschnitt aufgeführten Fall 2.

2.5 Proposition: Sei $(R, \hat{+}, \hat{\cdot})$ ein Integritätsring mit $char(R) = m > 0$. Dann ist m eine Primzahl.

Beweis. Ein Integritätsring ist ein Bereich, d.h. es ist $1 \neq 0$, weshalb $m \geq 2$ gilt. Angenommen, m ist keine Primzahl, dann gibt es $1 < s,t \in \mathbb{N}$ mit $m = st$ (die –bis auf die Reihenfolge– eindeutige Primfaktorzerlegung) und $s < m$, $t < m$. Sei e das neutrale Element der Multiplikation in R. Dann gilt

$$0 = m * e = (st) * (e \hat{\cdot} e) = (s * e) \hat{\cdot} (t * e).$$

Da R ein Integritätsring ist, folgt $s * e = 0$ oder $t * e = 0$, wobei $s,t < m$. Das steht jedoch im Widerspruch dazu, dass m nach Voraussetzung die kleinste positive Zahl mit $m * e = 0$ ist. Es kann m also keine zusammengesetzte Zahl sein oder anders formuliert m ist eine Primzahl. □

2.6 Beispiel: Die Körper $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ haben alle die Charakteristik 0. Das ist einsichtig, da jeder Körperhomomorphismus ϕ injektiv ist, d.h. $\text{Kern}(\phi) = \{0\}$ (vgl. Proposition 3.3). Die endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit positiver Charakteristik besitzen gemäß Proposition 2.5 die Primzahl p als Charakteristik.

Durch die letzten beiden Erkenntnisse ist die nächste Definition naheliegend.

2.7 Definition: Ein Körper K, der keine Unterkörper enthält, die eine echte Teilmenge von K sind, wird **Primkörper** genannt.

Wie Eingangs erläutert sind Primkörper die elementaren Bausteine für alle weiteren Körper. Der Durchschnitt über alle Unterkörper eines Körpers K *entspricht* dem zugehörigen Primkörper. Diese Aussage folgt - im Vorgriff - aus den Propositionen 3.3 und 3.6. Wir stellen nun die wichtigsten (da bis auf Isomorphie einzigen) Vertreter der Familie der Primkörper vor.

2.8 Proposition: Die Körper $\mathbb{Q}$ und $\mathbb{F}_p$, wobei p eine Primzahl ist, sind Primkörper.

Beweis. Sei $K \subseteq \mathbb{Q}$ ein Unterkörper. Dann folgt $0, 1 \in K$ und da K abgeschlossen bezüglich der Addition ist, folgt $\mathbb{Z} \subseteq K$. Da K genauso abgeschlossen ist bezüglich der Multiplikation, folgt $\mathbb{Q} \subseteq K$. Also ist $\mathbb{Q} = K$.

Sei nun p eine Primzahl und $K \subseteq \mathbb{F}_p$ ein Unterkörper. Dann folgt, wie für jeden Körper, dass $0, 1 \in K$, und da auch K abgeschlossen ist unter der Addition, folgt bereits $\mathbb{F}_p \subseteq K$, also $K = \mathbb{F}_p$. □

2.9 Proposition: Ein Ring R entspricht genau dann seinem Primring $P(R)$, wenn seine additive Gruppe zyklisch ist.

Beweis. „⇒“: Sei $R = P(R)$ ein Primring, dann wird die additive Gruppe $(R, +)$ von 1_R als Bild des kanonischen Ringhomomorphismus ϕ erzeugt.
„⇐“: Sei umgekehrt R ein Ring, dessen additive Gruppe $(R, +)$ von einem Element $a \in R$ erzeugt wird. Sodann gibt es $r, s \in \mathbb{Z}$ mit $1_R = ra$ und $a^2 = sa$, so dass $a = 1_R a = ra^2 = rsa = sra = s1_R$. Somit ist $a \in \mathbb{Z} * 1_R$ und folglich $R = \mathbb{Z} * 1_R = P(R)$. □

2.10 Satz: Für einen Primring R mit positiver Charakteristik $m > 0$ sind die folgenden Aussagen äquivalent:

(i) R ist ein endlicher Körper;

(ii) R ist ein Intergritätsring;

(iii) m ist eine Primzahl.

Beweis. Die Äquivalenz von (i) und (ii) folgt aus der Argumentation aus Fall 2 des letzten Abschnittes. Die Implikation (ii) $\Rightarrow$ (iii) ergibt sich mit Hilfe von Proposition 2.5. Wir zeigen schließlich noch $(iii) \Rightarrow (i)$. Dazu halten wir fest, dass jedes Element $r \in R \setminus \{0\}$ durch $n * e$ mit $0 < n < m$ erzeugt werden kann. Diese Elemente sind allesamt Einheiten, da $ggT(m, n) = 1$ ist. Dabei beachte man, dass m eine Primzahl ist. Vgl. auch [10] 17.3. □

3 Grundlegendes über Körpererweiterungen

3.1 Körperhomomorphismen

Analog zu den Gruppen- und Ringhomomorphismen definiert man Körperhomomorphismen. Diese entsprechen, je nach Definition eines Ringes (ob mit Einselement oder nicht), den Ringhomomorphismen.

3.1 Definition: Seien K und L Körper. Eine Abbildung $\phi : K \to L$ heißt **Körperhomomorphismus**, wenn gilt

a) $\phi(k + k') = \phi(k) + \phi(k')$ für alle $k, k' \in K$;

b) $\phi(kk') = \phi(k)\phi(k')$ für alle $k, k' \in K$;

c) $\phi(1) \neq 0$.

Mit dem Punkt c) der Definition will man insbesondere die Nullabbbildung als Homomorphismus bzw. den Nullring als Körper ausschließen.

3.2 Proposition: Seien K und L Körper, $\phi : K \to L$ ein Körperhomomorphismus und $a \in K$, dann gelten:

(i) $\phi(0) = 0$;

(ii) $\phi(1) = 1$;

(iii) $\phi(a^{-1}) = \phi(a)^{-1}$, wenn $a \neq 0$;

(iv) $\phi(-a) = -\phi(a)$.

Beweis. (i) Wir müssen zeigen, dass das neutrale Element der Addition der Gruppe $(K, +)$ auf das neutrale Element der Addition der Gruppe $(L, +)$ abgebildet wird. Aus den Eigenschaften des Homomorphismus und des Nullelements folgt durch

Subtraktion von $\phi(0)$ angewendet auf die Gleichung $\phi(0) = \phi(0+0) = \phi(0)+\phi(0) \Rightarrow 0 = \phi(0)$ die Behauptung.

(ii) Gemäß Definition ist $\phi(1) \neq 0$, d.h. es existiert das multiplikative Inverse $\phi(1)^{-1}$. Aufgrund der Definition des Einselements und da ϕ ein Homomorphismus ist, gilt $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$. Multipliziert man $\phi(1)^{-1}$ zu dieser Gleichung so folgt gerade die Behauptung.

(iii) Sei $a \in K^\times := K \setminus \{0\}$ ein Element der Einheitengruppe, dann existiert wie in (ii) festgehalten ein multiplikative Inverses $\phi(1)^{-1}$. Wegen (ii) und da ϕ ein Homomorphismus ist, gilt

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

Durch Multiplikation mit $\phi(a)^{-1}$ gegen diese Gleichung folgt die Behauptung.

(iv) Sei $a \in K$, dann ist $\phi(a) + \phi(-a) = \phi(a - a) = \phi(-a + a) = \phi(-a) + \phi(a) = \phi(0) = 0$. Somit ist $\phi(-a)$ das zur Addition inverse Element von $\phi(a)$.

□

Die eben bewiesenen Eigenschaften werden wir im Beweis der nächsten Proposition benötigen.

3.3 Proposition: Ist $\phi : K \to L$ ein Körperhomomorphismus, dann ist ϕ injektiv. Insbesondere ist jeder Körperhomomorphismus ein Isomorphismus auf sein Bild.

Beweis. Wir konstatieren, dass $K \neq \{0\}$ oder äquivalent $0 \neq 1$. Angenommen es wäre $\phi(k) = \phi(k')$ für $k, k' \in K$, dann folgt $\phi(k) - \phi(k') = 0$ und somit $\phi(k - k') = 0$. Damit ist $(k - k')$ ein Element von Kern(ϕ). Wir müssen also nur noch nachweisen, dass $k - k' = 0$, da dies Kern$(\phi) = \{0\}$ impliziert. Dazu nehmen wir an, dass $(k - k') \neq 0$. Aufgrund der Annahme existiert ein multiplikatives Inverses $(k - k')^{-1} \neq 0$. Daraus folgt

$$\begin{aligned} & 1 = \phi((k - k')(k - k')^{-1}) = \phi(k - k')\phi((k - k'))^{-1} \\ \Rightarrow\ & 1 = 0 \cdot \phi((k - k'))^{-1} = 0 \\ \Rightarrow\ & 1 = 0, \end{aligned}$$

was der Annahme $1 \neq 0$ widerspricht. Natürlich ist ϕ bezüglich seines Bildes surjektiv, also insgesamt bijektiv, d.h. ϕ ist bezüglich seines Bildes ein Isomorphismus. □

Mit Hilfe der Idealtheorie ist die letzte Proposition sehr einfach nachzuweisen. Es ist Kern(ϕ) ein Ideal und jeder Körper besitzt nur die trivialen Ideale $\{0\}$ und K. Im ersten Fall ist ϕ gerade injektiv, im anderen Fall ist $\phi(a) = 0$ für alle $a \in K$, d.h. $\phi = 0$.

3.2 Erweiterungskörper und Zwischenkörper

Wir stellen direkt den Hauptakteur dieses Abschnittes in der nächsten Definition vor.

3.4 Definition: Ist K ein Unterkörper des Körpers L, dann heißt L eine **Körpererweiterung** über K (oder Erweiterungskörper von K). Wir schreiben hierfür $L : K$. Ein Körper M heißt **Zwischenkörper** der Erweiterung $L : K$, wenn M Unterkörper von L ist mit $K \subseteq M \subseteq L$.

Natürlich ist eine Teilmenge $K \subseteq L$ zusammen mit den Verknüpfungen des Körpers L genau dann ein *Teilkörper*, wenn $(K, +, \cdot)$ ein Körper ist.

Hin und wieder nennt man dann auch L den *Oberkörper* von K, entsprechend K den *Teilkörper* (Unterkörper) von L. Wir fassen Körpererweiterungen auch *als Paar* von Körpern $K \subseteq L$ auf, wobei K ein Teilkörper von L ist.

Bitte beachten Sie im nächsten Beispiel d), dass der Faktorring $\mathbb{K}[X]/(f)$ aus den Nebenklassen

$$[g] = g + (f) = \{g + hf |\ h \in \mathbb{K}[X]\}$$

besteht. Die Verknüpfungen im Faktorring sind durch

$$[g] + [g'] := [g + g']$$
$$[g] \cdot [g'] := [g \cdot g']$$

definiert. Zwei Nebenklassen sind identisch, falls $g - g' \in (f) = \{hf |\ h \in \mathbb{K}[X]\}$, d.h. wenn $g - g'$ durch f ohne Rest teilbar ist. Jedes Element des Faktorrings enthält genau ein Polynom r mit $\mathrm{Grad}(r) < \mathrm{Grad}(f)$. Das Polynom r ist gerade der Rest der bei Division von g durch f überbleibt.

Zusammengefasst besteht $\mathbb{K}[X]/(f)$ aus allen Nebenklassen $[r] = r + (f)$, wobei r alle Polynome in $\mathbb{K}[X]$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(f) = n$ durchläuft. Ist $\mathbb{K} = \mathbb{F}_p$, p eine Primzahl und somit $\mathbb{F}_p$ ein endlicher Körper mit p Elementen, dann gibt es p^n Polynome der Form

$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1},$$

vom Grad $< n$. Das ist klar, denn jeder der n Koeffizienten a_i kann den Wert eines beliebigen Elementes aus $\mathbb{F}_p$ annehmen.

3.5 Beispiel:

a) Die wohlbekannten Körper $\mathbb{R}$ und $\mathbb{C}$ bilden eine Körpererweiterung $\mathbb{C} : \mathbb{R}$. Dabei ist $\mathbb{C}$ der Oberkörper und $\mathbb{R}$ der Teilkörper. Stellt man die Elemente des Körper $\mathbb{C}$ in der Form $(a + ib)$ mit $a, b \in \mathbb{R}$ dar, dann verwenden beide Körper dieselben Verknüpfungen.

b) Ebenfalls wohlbekannt ist der Körper der rationalen Zahlen $\mathbb{Q}$, dieser ist Teilkörper von $\mathbb{R}$, d.h. $\mathbb{R} : \mathbb{Q}$ ist eine Körpererweiterung. Sodann können wir schließen, dass $\mathbb{R}$ Zwischenkörper der Körpererweiterung $\mathbb{C} : \mathbb{Q}$ sein muss, da $\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$ gilt.

c) Es sei $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, wobei p eine Primzahl sei. Dann ist $\mathbb{F}_p$ zusammen mit den üblichen Verknüpfungen auf Restklassenringen ein Körper. Es sei f ein irreduzibles Polynom über dem Polynomring $\mathbb{F}_p[X]$, sodann ist $\mathbb{F}_p[X]/(f)$ ein Körper, es gilt sogar $\mathbb{F}_p[X]/(f) : \mathbb{F}_p$.

d) Konkretisieren wir das Beispiel c) und setzen dazu $p := 2$ und $f := X$. Die Elemente von $L := \mathbb{F}_2[X]/(f)$ sind die Polynome $[0]$ und $[1]$. Es gibt also zwei Polynome

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

vom Grad kleiner eins in L, das sind die konstanten Polynome [0] und [1]. Die Verknüpfungen in L entsprechen denen in $\mathbb{F}_2$, wie aus den beiden Tabellen einfach abzulesen ist.
Offenbar ist L somit ein Körper der isomorph zu $\mathbb{F}_2$ ist.

Folgende Proposition benötigen wir im Beweis des Satzes 3.7.

3.6 Proposition: Sei L ein Körper, sei I eine nicht leere Indexmenge und sei $(K_i)_{i\in I}$ ein System von Unterkörpern von L. Dann ist

$$\bigcap_{i\in I} K_i$$

ein Körper.

Beweis. Es sei $M := \bigcap_{i\in I} K_i$ der Durchschnitt des Systems aus Unterkörpern von L. Seien $a, b \in M$, dann gilt $a, b \in K_i$ für alle $i \in I$, also $a + b \in K_i$ und $ab \in K_i$ für alle $i \in I$. D.h. ab bzw. $a + b \in M$. Dies zeigt, dass + und · Verknüpfungen auf M sind.
Da die neutralen Elemente der Addition bzw. Multiplikation in jedem Körper liegen müssen, sind diese auch in M vorhanden. Entsprechend kann man folgern, dass auch alle Inversen in M enthalten sein müssen. Da M eine Teilmenge von L ist gilt auch für M das Assoziativgesetz für die Addition und Multiplikation und die Distributivgesetze. Außerdem sind Addition und Multiplikation kommutativ. □

Offenbar ist der sich aus letzter Proposition 3.6 ergebende Körper innerhalb der Menge $\{K_i |\ i \in I\}$ der kleinste Körper bezüglich der Inklusion.

3.3 Körpererweiterungen und die Charakteristik

Nun kehren wir noch einmal zu den Primkörper bzw. Primringen zurück und verknüpfen diese mit den bereits gewonnenen Erkenntnissen aus der Körpertheorie.
Mit Hilfe von Primkörpern kann man Körper an Hand ihrer Charakterisierung klassifizieren, denn jeder Körper enthält einen kleinsten Unterkörper.

3.7 Satz: Sei K ein Körper. Dann besitzt K einen Unterkörper P, der ein Primkörper ist. Dabei gilt entweder

- $P \cong \mathbb{Q}$, wenn $char(K) = 0$ gilt, oder
- $P \cong \mathbb{F}_p$ für eine Primzahl p, wenn $char(K) = p$ gilt.

Beweis. Zunächst nehmen wir an, dass $char(K) = 0$ gilt, es sich also um einen nicht-endlichen Körper handelt. Sei

$$P := \bigcap_{K \text{ ist ein Unterkörper von } L} K.$$

Dann ist P mit Proposition 3.6 ein Körper. Jeder Körper K enthält (gemäß Definition) die neutralen Elemente $0, 1 \in K$, zudem ist die additive Verknüpfung per Definition abgeschlossen. Daher enthält jeder Unterkörper $M \leq K$ die Menge $\{n * 1 |\ n \in \mathbb{Z}\}$, was dem Primring von K entspricht. Da $char(K) = 0$ gilt, ist der Primring von K isomorph zu $\mathbb{Z}$. Da $(M^\times, \cdot)$ für alle Unterkörper $M \leq K$ eine abelsche Gruppe ist, enthält jeder Unterkörper M auch einen Unterkörper der Isomorph ist zu $\mathbb{Q}$. Dabei beachte man, dass die Inversen aus $\mathbb{Z}$ überwiegend in $\mathbb{Q}$ enthalten sind. Dieser Unterkörper ist dann gerade P, und es gilt $P \cong \mathbb{Q}$.

Gilt $char(K) = p$, dann ist der Primring $P(K) \cong \mathbb{F}_p$ und $\mathbb{F}_p$ ist ein Körper. D.h. Primring und Primkörper stimmen überein. □

Folgede Proposition ist klar, da Primkörper bzw. Primringe gemäß Definition die kleinsten Körper bzw. Ringe sind, die in einer Menge enthalten sein können.

3.8 Proposition: Sei $L : K$ eine Körpererweiterung. Dann gilt:

(i) $char(K) = char(L)$

(ii) Seien $P(K)$ und $P(L)$ die zu K bzw. L gehörigen Primkörper. Dann gilt $P(K) = P(L)$

Beweis. (i): Da die Addition und die Multiplikation in K und L die gleichen sind, sind auch $\{n * 1_K | n \in \mathbb{Z}\}$ und $\{n * 1_L | n \in \mathbb{Z}\}$ gleich, also haben K und L denselben Primring.

(ii): Da der Primkörper $P(K)$ von K der kleinste Unterkörper von K ist, gilt $P(K) \subseteq K \subseteq L$ dasselbe für L. Also $P(K) = P(L)$. □

Alle Erweiterungskörper L eines Körper K haben also dieselbe Charakterisitk bzw. enthalten denselben kleinsten (Prim-)Körper.

3.4 Körpererweiterungen als Vektorräume

Im Folgenden sei $L : K$ eine Körpererweiterung, d.h. L Körper, $K \leq L$ Unterkörper. Folgende einfache Überlegung ist *grundlegend* für die gesamte Körpertheorie.

Bemerkung: Der Oberkörper (Erweiterungskörper) L ist in natürlicher Weise ein **Vektorraum** über K. Denn $(L, +)$ ist eine abelsche Gruppe und es ist eine Multiplikation von Elementen aus L mit Skalaren aus K erklärt, nämlich die gegebene Multiplikation aus L. Aus den Körperaxiomen sieht man sofort, dass die Axiome für einen Vektorraum erfüllt sind.

Ein Vektorraum besitzt eine Dimension, diese können wir uns von Nutzen machen, um ein zweites Chrakteristikum für Körpererweiterungen bzw. Körper zu gewinnen.

3.9 Definition: Es sei $L : K$ eine Körpererweiterung. Dann bezeichnet man die Vektorraumdimension $[L : K] := dim_K(L)$ als den **Grad von L über K**. Die Körpererweiterung heißt **endlich** oder **unendlich**, je nachdem ob $[L : K]$ endlich oder unendlich ist.

Offenbar ist $L \cong K$ äquivalent zu $[L : K] = 1$. Körpererweiterungen vom Grad 1 nennen wir **unecht**.

3.10 Beispiel:

a) Die Körpererweiterung $\mathbb{C} : \mathbb{R}$ hat den Grad 2, da zwei (Basis-)Vektoren notwendig sind, um den Vektorraum $\mathbb{C}$ über $\mathbb{R}$ eindeutig zu erzeugen, bspw. $\{1, i\}$. Dagegen ist $[\mathbb{C} : \mathbb{C}] = 1$ eine unechte Erweiterung. Hier ist nur ein (Basis-)Vektor notwendig, um $\mathbb{C}$ eindeutig aufzuspannen.

b) $[\mathbb{R} : \mathbb{Q}] = \infty$, d.h. mit endlich vielen (Basis-)Vektoren lässt sich $\mathbb{R}$ nicht über $\mathbb{Q}$ erzeugen.

c) $[\mathbb{F}_2[X]/(X^2 + X + 1) : \mathbb{F}_2] = 2$ mit Basis $\{[1], [X]\}$.

Erweiterungen vom Grad 2 werden häufig als **quadratische Erweiterungen** bezeichent. Wenn wir über lineare Unabhängigkeit, Basen, etc. im Kontext von Erweiterungen $L : K$ sprechen, so beziehen wir uns selbstverständlich auf den Vektorraum L über K.

3.11 Proposition: Sei K ein Körper und $f(X)$ ein Polynom über K vom Grad $n \geq 0$. Dann ist $K[X]/(f(X))$ ein K-Vektorraum der Dimension n mit Basis $1, \xi, \ldots, \xi^{n-1}$, wobei $\xi := \pi(X)$ das Bild der kanonschen Projektion ist.

Beweis. Offensichtlich ist $K[X]$ ein K-Vektorraum und das Ideal $(f) = I$ ein K-Untervektorraum von $K[X]$, also ist auch der Faktorraum $K[X]/I$ ein K-Vektorraum. Es sei $\pi : K[X] \to K[X]/(f(X))$ die kanonsche Projektion und $\xi := \pi(X)$. Dann bilden $1, \xi, \xi^2, \ldots, \xi^{n-1}$ mit $n = \text{Grad}(f)$ eine K-Basis von $K[X]/(f(X))$. Ist $\pi(g(X))$ ein beliebiges Element von $K[X]/(f(X))$, so dividieren wir $g(X)$ durch $f(X)$ mit Rest:

$$g(X) = q(X)f(X) + r(X), \qquad \text{Grad}(r) < n.$$

Es folgt $\pi(g(X)) = \pi(r(X))$, da (f) der Kern von π ist. Ist $r(X) = b_0 + b_1\xi + \ldots + b_m X^m$ mit $m < n$, so gilt

$$\begin{aligned} \pi(g(X)) = \pi(r(X)) &= \pi(b_0 + b_1 X + \ldots + b_m X^m) \\ &= b_0\pi(1) + b_1\pi(X) + \ldots + b_m\pi(X^m) \\ &= b_0 + b_1\xi + \ldots + b_m\xi^m \end{aligned}$$

Also bilden $\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ ein Erzeugendensystem des K-Vektorraumes $K[X]/(f(X))$. Sie sind auch linear unabhängig, denn aus

$$a_0 + a_1\xi + \ldots + a_{n-1}\xi^{n-1} = 0$$

mit $a_0, \ldots, a_{n-1} \in K$ folgt

$$\pi(a_0 + a_1X + \ldots + a_{n-1}X^{n-1}) = 0,$$

also $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in \mathrm{Kern}(\pi) = (f(X))$. Weil f den Grad n und damit jedes Vielfache $\neq 0$ einen Grad größer oder gleich n hat, ist die letzte Gleichung nur für die Trivialkombination, d.h. $a_0, \ldots, a_{n-1} = 0$ möglich.

□

Jeder Körper K ist ein Vektorraum über seinem Primkörper $P(K)$ und für Körper mit endliche vielen Elementen gilt weiter der folgende

3.12 Satz: Jeder endliche Körper K mit Charakteristik $p := char(K)$ ist eine endliche Erweiterung $K : P(K)$ über seinem Primkörper $P(K)$. Der Vektorraum K über $P(K)$ ist damit endlich, d.h. $[K : P(K)] := n < \infty$ und hat $(char(K))^n$ Elemente.

Beweis. Da der Vektorraum K endlich ist, kann K nur endlich viele über $P(K)$ linear unabhängige Elemente enthalten. Wir setzen daher $[K : P(K)] =: n < \infty$. Seien $b_1, \ldots, b_n$ Basisvektoren von K über $P(K)$, dann besitzt jeder Vektor $v \in K$ eine eindeutige Darstellung $v = \sum_{i=1}^{n} \lambda_i b_i$ mit Skalaren $\lambda_i \in P(K)$. Da die Darstellung eines Körperelements mit Hilfe von Linearkombinationen durch Basisvektoren eindeutig ist, existieren genau soviele Elemente im Körper K, wie es verschiedene n-Tupel $(\lambda_1, \ldots, \lambda_n)$ mit $\lambda_i \in P(K)$ gibt. Wegen $P(K) \cong \mathbb{Z}_p$ gibt es offenbar p^n solcher n-Tupel. □

3.5 Der Gradsatz

Der folgende Gradsatz ist von Bedeutung für die gesamte Körpertheorie, er drückt aus, dass die Grade Erweiterungen bzw. der dadurch entstehenden Vektorräume multiplikativ zusammenhängen.

3.13 Satz: (Gradsatz)
Ist L Zwischenkörper der Körpererweiterung $M : K$, dann gilt

$$[M : K] = [M : L][L : K]. \tag{GS}$$

Die Gleichung (GS) ist symbolisch zu verstehen, wenn einer der Grade unendlich ist. Der interessante Fall ist der, dass beide Grade endlich sind:

Beweis. Seien $[M : L] = m$ und $[L : K] = n$. Weiter seien $(w_1, \ldots, w_m)$ eine Basis von M über L und $(v_1, \ldots, v_n)$ eine Basis von L über K.
Sei $x \in M$ ein beliebiges Element aus M. Dann gibt es $\alpha_1, \ldots, \alpha_m \in L$, so dass eine eindeutige Darstellung von $x = \sum_{j=1}^{m} \alpha_j w_j$ möglich ist. Zu jedem α_j mit $1 \leq j \leq m$ gibt es wiederum $\beta_{1_j}, \ldots, \beta_{n_j} \in K$ mit $\alpha_j = \sum_{i=1}^{n} \beta_{i_j} v_i$. Zusammengesetzt ergibt das

$$x = \sum_{j=1}^{m} \alpha_j w_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \beta_{i_j} v_i \right) w_j = \sum_{j=1}^{m} \sum_{i=1}^{n} \beta_{i_j} v_i w_j$$

Dies ist eine Linearkombination der nm Elemente $v_i w_j$, $1 \leq i \leq n, 1 \leq j \leq m$, mit Koeffizienten aus dem bzgl. der Inklusion kleinsten Körper K. Damit ist gezeigt, dass diese Elemente ein Erzeugendensystem von M über K bilden. Es ist nun noch zu zeigen, dass sie linear unabhängig sind, dazu müssen wir im Prinzip nur den „umgekehrten“ Weg gehen.

Für $1 \leq i \leq n, 1 \leq j \leq m$ seien also $\gamma_{i_j} \in K$ mit

$$\sum_{i=1}^{m} \sum_{i=1}^{n} \gamma_{i_j} v_i w_j = 0.$$

Dann folgt

$$\sum_{i=1}^{m} \left(\sum_{i=1}^{n} \gamma_{i_j} v_i \right) w_j = 0,$$

wobei für $1 \leq j \leq m$ dann $\sum_{i=1}^{n} \gamma_{i_j} v_i \in L$ gilt. Da $(w_1, \ldots, w_m)$ eine Basis von M über L, folgt $\sum_{i=1}^{n} \gamma_{i_j} v_i = 0$ für $j = 1, \ldots, m$. Nun ist aber auch $(v_1, \ldots, v_n)$ eine Basis von L über K, also folgt $\gamma_{i_j} = 0$ für $1 \leq j \leq n$. D.h. $[M : K] = mn$.

□

Allein der Gradsatz bzw. das folgende Korollar liefern bereits wichtige Erkenntnisse über endliche Körpererweiterungen, wie die nächsten Folgerungen zeigen.

3.14 Folgerung: Ist L ein Zwischenkörper einer endlichen Erweiterung $M : K$, dann sind $[M : L]$ und $[L : K]$ Teiler von $[M : K]$.

Der Beweis ist mit Hilfe der Gradformel (GS) evident. Das letzte Korollar schränkt bereits die Möglichkeit für die Zwischenkörper stark ein. Danach besitzt z.B. eine Erweiterung $L : K$, bei der $[L : K]$ eine *Primzahl* ist, keine echten Zwischenkörper. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ hat damit $\mathbb{C} : \mathbb{R}$ keine echten Zwischenkörper, d.h. es existiert kein Zwischenkörper $M \neq \mathbb{R}$ bzw. $M \neq \mathbb{C}$.

3.15 Folgerung: Für einen Zwischenkörper L einer endlichen Erweiterung $M : K$ ist $[M : K] = [L : K]$ nur für $L \cong M$ möglich.

Beweis. Der Gradsatz und die Voraussetzungen ergeben $[M : L] = 1$, also $M \cong L$. □

Im Korollar kann dabei auf die Voraussetzung „endliche Erweiterung“ nicht verzichtet werden, denn für die *nicht* endliche Erweiterung $\mathbb{C} : \mathbb{Q}$ gilt $[\mathbb{C} : \mathbb{Q}] = [\mathbb{R} : \mathbb{Q}]$.

3.16 Folgerung: Für einen „Körperturm“ $K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ gilt

$$[K_n : K_1] = \prod_{i=1}^{n-1} [K_{i+1} : K_i].$$

3.6 Die Adjunktion

Will man Aussagen über eine Teilmenge $A \subseteq M$ im Kontext einer Körpererweiterung $M : K$ treffen, so ist es zweckmäßig, sich zunächst auf die Untersuchung des kleinesten Zwischenkörpers von $M : K$ der A enthält zu beschränken.

3.17 Definition: Sei $M : K$ eine Körpererweiterung und $A \subseteq M$ eine Teilmenge von M. Dann ist $K(A)$ definiert als der Schnitt über alle Unterkörper von M, die sowohl K als auch alle Elemente von A enthalten. Es ist also

$$K(A) := \{L |\ L \text{ ist ein Zwischenkörper von } M : K \text{ mit } A \subseteq L\} \tag{Adj}$$

der durch **Adjunktion** von A an K erhaltene Zwischenkörper der Erweiterung $M : K$. Ist $A := \{a_1, \ldots, a_n\}$ endlich, so schreibt man auch $K(a_1, \ldots, a_n)$ und sagt, dass dieser Körper aus K durch Adjungieren von $a_1, \ldots, a_n$ entstanden ist.

Für den Körper $K(A)$ gilt:

(I) Ist L ein Zwischenkörper von $M : K$, der A enthält, dann gilt $K(A) \subseteq L$. In diesem Sinne ist $K(A)$ bezüglich $\subset$ der kleinste Unterkörper von M, der $K \cup A$ enthält. $K(A)$ ist der von $K \cup A$ erzeugte Unterkörper von M.

(II) Die Adjunktion von $A \subseteq K$ an K ist K selbst.

(III) $K(A_1 \cup A_2) = K(A_1)(A_2) = K(A_2)(A_1)$, denn nach (I) ist jeder dieser Körper der kleinste Unterkörper von M, der $K \cup A_1 \cup A_2$ enthält.

(IV) Seien $K \subseteq L \subseteq M$ und $A \subseteq M$, dann ist $K(A) \subseteq L(A) \subseteq M(A) = M$. Ist insbesondere $M = K(A)$, dann auch $M = L(A)$ für jeden Zwischenkörper L von $M : K$.

Wir betrachten zunächst den einfachsten Fall mit $A := \{a\}$.

3.18 Definition: Eine Körpererweiterung $L : K$ heißt **einfach**, wenn es ein $a \in L$ gibt mit $L = K(a)$. In diesem Fall heißt a **primitives Element** von $L : K$.

3.19 Beispiel:

a) Sei $K = \mathbb{Q}$ und $a = \sqrt{2}$, dann ist

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}.$$

Jeder Körper L, der $\mathbb{Q}$ und $\sqrt{2}$ enthält, muss aufgrund der Körperaxiome auch die Menge $M := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ enthalten, d.h. $M \subseteq L$. Wir müssen also nur noch zeigen, dass M ein Körper ist. Offenbar kann man die Summe zweier Elemte aus M wieder ein Element in M, d.h. + ist eine Verknüpfung auf M. Seien nun $(a + b\sqrt{2}), (c + d\sqrt{2}) \in M$ mit $a, b, c, d \in \mathbb{Q}$. Dann ist $(a + b\sqrt{2})(c + d\sqrt{2}) = [(ac + 2bd) + (ad + bc)\sqrt{2}] \in M$, also ist auch $\cdot$ eine Verknüpfung auf M.

Die neutralen Elemente $0 = 0 + 0 \cdot \sqrt{2}$ und $1 = 1 + 0 \cdot \sqrt{2}$ liegen in M, und die Assoziativ- und Distributivgesetze gelten in M, denn M ist eine Teilmenge von $\mathbb{R}$. Zu zeigen ist deshalb nur noch, dass die Inversen bezüglich der Addition und der Multipliaktion in M liegen. Zu $a+b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ ist $(-a)+(-b)\sqrt{2}$ bezüglich der Addition invers, und das Inverse zu $a + b\sqrt{2} \neq 0$ bezüglich der Multiplikation ist

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

mit Nenner ungleich 0. Damit folgt, dass M ein Körper ist und somit $M = \mathbb{Q}(\sqrt{2})$ gilt.

b) Es ist $\mathbb{C} : \mathbb{R}$ eine einfache Körpererweiterung mit der imaginären Einheit als primitives Element i.

c) Der Funktionenkörper $\mathbb{R}(X)$ ist einfach über $\mathbb{R}$, wobei X das primitive Element ist.

d) Ist $L := K(a) : K$ einfach, so ist auch ka primitives Element von $L : K$ für jedes $k \in K \setminus \{0\}$.

e) Beachten Sie, dass zwar $\mathbb{Q}(\sqrt[3]{2})$ eine einfache Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ ist, der Vektorraum $\mathbb{Q}(\sqrt[3]{2})$ über $\mathbb{Q}$ aber die Dimension 3 besitzt. D.h. insbesondere, dass $\mathbb{Q}(\sqrt[3]{2}) \neq \{a + b\sqrt[3]{2} | a, b \in \mathbb{Q}\}$.

3.20 Satz: Jede endliche Erweiterung $L : K$ eines endlichen Körpers K ist einfach.

Beweis. Der Grundkörper K ist endlich und L besitzt endliche Dimension $n \in \mathbb{N}$ über K. Seien $b_1, \ldots, b_n$ Basisvektoren, dann existieren genau $|K|^n$ verschiedene n-Tupel bestehend aus Skalaren aus K. Dies entspricht gerade der Anzahl der Elemente aus L, da Darstellung der Vektoren aus L über Linearkombinationen mit Basisvektoren eindeutig ist. Es ist L demnach ein endlicher Körper. Zudem ist $L^\times$ zyklisch, da jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Es existiert daher ein einziges Element $a \in L$ mit $L = \{0, a, a^2, \ldots, a^m\}$, weshalb $L = K(a)$ folgt. □

3.7 Algebraische & transzendente Elemente

Bei einer einfachen Körpererweiterung $K(a) : K$ unterscheiden wir die beiden folgenden Fälle:

1. Es gibt ein von Null verschiedenes Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$;
2. Für alle $f \in K[X] \setminus \{0\}$ gilt $f(a) \neq 0$.

3.21 Definition:

1. Sei $L : K$ eine Körpererweiterung und sei $a \in L$. Ist a Nullstelle eines Polynoms $f \in K[X] \setminus \{0\}$, dann heißt a **algebraisch** über K.

2. Ein Element $a \in L$ heißt **transzendent** über K, wenn es nicht algebraisch ist; d.h. für $f \in K[X]$ gilt $f(a) = 0$ *nur* für $f = 0$.

3.22 Beispiel:

a) Das Element $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn es ist Nullstelle von $X^2 - 2 \in \mathbb{Q}[X]$.

b) Jedes Element $a \in K$ ist algebraisch über K, denn es ist Nullstelle von $X - a \in K[X]$.

c) Das Element $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn es ist Nullstelle von $X^2 + 1 \in \mathbb{R}[X]$

d) Das Element $\sqrt[3]{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, da offenbar $f := X^3 - 2 \in \mathbb{Q}[X]$ die Nullstelle $\sqrt[3]{2}$ besitzt.

e) Die Elemente $\pi, e \in \mathbb{R}$ sind transzendent über $\mathbb{Q}$, denn es gibt kein Polynom $f \in \mathbb{Q}[X] \setminus \{0\}$ mit $f(\pi) = 0$ oder $f(e) = 0$. Einen Nachweis unterdrücken wird, da wir hauptsächlich an den algebraischen Körpererweiterungen interessiert sind.

3.8 Das Minimalpolynom

Bevor wir mit dem eigentlichen Thema beginnen führen wir eine bedeutende Abbildung ein. Dazu sei $L : K$ eine Körpererweiterung und $a \in L$.

Man sagt, $f(a)$ entsteht durch „**Einsetzen von** a“ in das Polynom $f \in K[X]$. Mit Hilfe der Definition der Funktionen-Addition bzw. -Multiplikation können wir leicht nachweisen, dass

$$\psi_a : K[X] \to L \quad \text{bestimmt durch} \quad f \mapsto \psi_a(f) := f(a).$$

ein Körperhomomorphismus ist. Dazu seien $f, g \in K[X]$ und $a \in L$, dann gilt

$$\begin{aligned} \psi_a(f+g) &= (f+g)(a) = f(a) + g(a) = \psi_a(f) + \psi_a(g), \\ \psi_a(fg) &= (fg)(a) = f(a)g(a) = \psi_a(f)\psi_a(g). \end{aligned}$$

Da diese Abbildung für Körpererweiterungen und darüber hinaus von Bedeutung ist zeichnen wir diesen in der folgenden Definition aus.

3.23 Definition: Es sei L ein Körper. Die Abbildung ψ_a nennen wir für *festes* $a \in L$ den **Substitutionshomomorphismus** (oder auch **Einsetzungshomomorphismus**) von a.

Der Substitutionshomomorphismus kann auch für Ringe erklärt werden, entsprechend handelt es sich dann um einen Ringhomomorphismus.

Sei $L : K$ eine Körpererweiterung und $a \in L$ algebraisch über K, d.h. es gibt ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = \sum_{i=1}^{n} \lambda_i a^i = 0$ und $\lambda_i \in K$ für alle $i \in \mathbb{N}_n$. Mindestens ein Skalar $\lambda_1, \ldots, \lambda_n$ ist ungleich 0, da gemäß Voraussetzung $f \neq 0$. Dies impliziert, dass der Kern des Substitutionshomomorphismus neben der Nullabbildung 0 zumindest noch

f enthalten muss, d.h. $\mathrm{Kern}(\psi_a) \neq \{0\}$. In der nächsten Proposition werden wir den Kern des Substitutionshomomorphismus näher untersuchen.

3.24 Proposition: Sei $L : K$ eine Körpererweiterung und sei $a \in L$ algebraisch über K. Dann ist die Menge

$$I := \mathrm{Kern}(\psi_a) = \{f \in K[X] \mid f(a) = 0\}$$

ein Ideal in $K[X]$.

Beweis. Zunächst müssen wir zeigen, dass $(I, +)$ eine abelsche Untergruppe von $(K, +)$ ist. Es gilt $0 \in I$ und für $f, g \in I$ ist $(f-g)(a) = f(a)+(-g)(a) = 0+0 = 0$, also $(f-g) \in f$. Mit dem Untergruppenkriterium ist also I eine Untergruppe von $K[X]$. Sei $f \in I$ und $g \in K[X]$, dann gilt $(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$, also $fg \in I$. Insgesamt folgt, dass I ein Ideal von $K[X]$ ist. □

Wir wissen, dass jeder Polynomring über einem Körper ein Hauptidealring ist. Es ist I aus obiger Bemerkung ein Hauptidealring, d.h. es existiert ein *eindeutig bestimmtes* und *normiertes* Polynom $\mu \in K[X]$ mit $(\mu) = I$. Dies veranlasst uns zur

3.25 Definition: Ist $L : K$ eine Körpererweiterung und $a \in L$ algebraisch über K, so existiert ein eindeutig bestimmtes normiertes Polynom kleinsten Grades $\mu_a \in K[X]$ mit $\mu_a(a) = 0$. Wir bezeichnen μ_a als **Minimalpolynom** von a. Der Grad von μ_a wird auch als **Grad** von a über K bezeichnet.

Wenn keine Verwechslungen zu befürchten sind werden wir schlicht μ anstatt μ_a schreiben.

3.26 Beispiel: Das Minimalpolynom von $i \in \mathbb{C}$ über $\mathbb{R}$ ist $\mu = X^2 + 1 \in \mathbb{R}[X]$, es ist normiert und es gilt $\mu(i) = 0$. Angenommen, es gibt ein normiertes Polynom $f \in \mathbb{R}[X]$ mit $f(i) = 0$ und $\mathrm{Grad}(f) < \mathrm{Grad}(\mu) = 2$, dann muss $\mathrm{Grad}(f) = 1$ gelten, also $f = X - \lambda$ für ein $\lambda \in \mathbb{R}$. Das kann aber nicht sein, da $i \notin \mathbb{R}$ nicht Nullstelle eines Polynoms der Form $X - \lambda$ ist. Also ist μ das Minimalpolynom und der Grad von i über $\mathbb{R}$ ist 2.

Natürlich ist der Grundkörper über dem wir für ein Element a das Minimalpolynoms μ bestimmen von Bedeutung. So ist z.B. das Minimalpolynom $(X^2 + 1)$ von $i \in \mathbb{C}$ über $\mathbb{R}$ vom Grad 2. Im Gegensatz dazu ist $i \in \mathbb{C}$ über $\mathbb{C}$ vom Grad 1 mit $(X - i)$ als Minimalpolynom.

Die Abbildung ψ_a ist in erstaunlicher Weise mit dem Minimalpolynom verknüpft. Offensichtlich ist $\mathrm{Bild}(\psi_a) = K[a]$. Sei nun a algebraisch mit Minimalpolynom $\mu(X)$ über K, so ist der $\mathrm{Kern}(\psi_a) = \{f(X) \in K[X] \mid f(X) = 0\}$ gerade das Hauptideal I aus Proposition 3.24 und es gilt

$$(\mu) = \{\mu p \mid p \in K[X]\} = I = \mathrm{Kern}(\psi_a).$$

Das Minimalpolynom erzeugt also den $\mathrm{Kern}(\psi_a)$ des Substitutionshomomorphismus. Die wichtigsten Eigenschaften von Minimalpolynomen halten wir in folgender Proposition fest.

3.27 Proposition: Sei $L : K$ eine Körpererweiterung und $a \in L$ algebraisch über K mit Minimalpolynom μ. Sei $f \in K[X]$ ein Polynom und ψ_a der Einsetzungshomomorphismus. Dann gilt:

(i) Das Minimalpolynom μ ist irreduzibel in $K[X]$;

(ii) $f \in \text{Kern}(\psi_a)$, d.h. $f(a) = 0 \Leftrightarrow \mu | f$;

(iii) Ist $f \in K[X]$ normiert und irreduzibel mit $f(a) = 0$, dann gilt bereits $f = \mu$;

(iv) $[K(a) : K] = \text{Grad}(a) = \text{Grad}(\mu_a)$.

Beweis.

(i) Wir zeigen die Behauptung durch Widerspruch. Dazu nehmen wir $\mu = h_1 h_2$ mit $h_1, h_2 \in K[X]$ und $1 \leq \text{Grad}(h_1), \text{Grad}(h_2) \leq \text{Grad}(\mu)$. Da $K[X]$ ein Integritätsring ist, gilt $0 = \mu(a) = h_1(a)h_2(a) \Rightarrow h_1(a) = 0$ oder $h_2(a) = 0$. Entweder ist also $h_1 \in \text{Kern}(\psi_a)$ oder $h_2 \in \text{Kern}(\psi_a)$. In beiden Fällen führt dies zu einem Widerspruch, da μ gemäß Definition das (Minimal-)Polynom $\neq 0$ kleinsten Grades aus $\text{Kern}(\psi_a)$ ist.

(ii) „$\Rightarrow$“: Sei zunächst $f \in K[X]$ mit $f(a) = 0$. Dann folgt offenbar $f \in I = (\mu) = \text{Kern}(\psi_a)$, also gibt es $h \in K[X]$ mit $f = \mu h$, und μ teilt f.
„$\Leftarrow$“: Nun gelte umgekehrt $\mu | f \Rightarrow \exists h \in K[X]$, so dass $f = h\mu$. Dann ist $f(a) = h(a)\mu(a) = h(a) \cdot 0 = 0$.

(iii) Nach Voraussetzung gilt $f(a) = 0$, d.h. $\mu | f$. Gemäß Definition ist μ das normierte Polynom kleinsten Grades in $\text{Kern}(\psi_a)$ mit $(\mu) = \text{Kern}(\psi_a)$. Da f irreduzibel und in $\text{Kern}(\psi_a)$ enthalten ist folgt $f = \mu$.

(iv) Sei $n := \text{Grad}(a) = \text{Grad}(\mu_a)$ der Grad des Minimalpolynoms und somit auch des Körperelementes $a \in L$. Wir möchten nachweisen, dass die Menge

$$B := \{1, a, a^2, \ldots, a^{n-1}\}$$

eine Basis des K-Vektorraumes $K(a)$ ist. Dazu nehmen wir an, dass $\sum_{i=0}^{n-1} \lambda_i a^i = 0$ mit $\lambda_i \in K$ für alle $i \in \mathbb{N}_{n-1}$. Dabei ist wenigstens einer dieser Koeffizienten $\lambda_j \neq 0$. Sodann wäre $f := \sum_{i=0}^{n-1} \lambda_i X^i$ ein von Null verschiedenes Polynom mit $\text{Grad}(f) < \text{Grad}(\mu)$, was gemäß Definition nicht sein kann. Es folgt die lineare Unabhängigkeit der Vektoren aus B. Sei nun $h(a)$ ein beliebiges Element aus $K(a)$ und teilen wir dies durch die Zahl $\mu(a)$ mit Rest, so erhalten wir wegen (ii) die Gleichung $h(a) = q(a)\mu(a) + r(a)$. Damit ist $h(a)$ bereits eine Linearkombination von den Elementen aus B. Insgesamt folgt, dass B eine Basis von $K(a)$ ist.

□

4 Algebraische Körpererweiterungen

Gegeben sei wieder die Körpererweiterung $L : K$ und $a \in L$.

4.1 Definition: 1. Es sei $L : K$ eine Körpererweiterung und $a \in L$. Sei

$$K[a] := \{f(a) | f \in K[X]\}$$

die **Menge aller Einsetzungen** von a in Polynome aus $K[X]$. Also gilt $K \subset K[a] \subset L$. Es ist $K[a]$ ein Ring und ein K-Vektorraum. Offenbar ist $K[a]$ der kleinste Unterring von L, der K und a enthält. Dies ist klar, denn der Polynomring entsteht durch Adjunktion.

2. Es sei $\varphi : L \to L'$ ein Isomorphismus von zwei Erweiterungskörpern L, L' von K. Dann heißt φ ein **K-Isomorphismus**, falls $\varphi(a) = a$ für alle $a \in K$ gilt, also $\varphi_{|K} = id_K$.

Im Folgenden werden wir die Zusammenhänge mit dem Einsetzungshomomorphismus näher studieren.

Sei $L : K$ eine Körpererweiterung mit $a \in L$ und Minimalpolynom $\mu \in K[X]$. Genau dann ist $a \in K$, wenn $\text{Grad}(\mu) = 1$ gilt: Ist $a \in K$, so ist $(X - a)$ das Minimalpolynom μ von a. Es besitzt den Grad 1, ist irreduzibel und normiert. Sei nun μ das Minimalpolynom von a mit Grad 1, dann muss $\mu(X)$ die Form $\mu = (X - a)$ mit $a \in K$ besitzen.

4.2 Definition: Eine **Körpererweiterung** $L : K$ heißt **algebraisch**, wenn jedes Element aus L algebraisch über K ist. Die Erweiterung heißt **transzendent**, wenn sie nicht algebraisch ist.

Im transzendenten Fall genügt ein über K transzendentes Element, damit $L : K$ transzendent ist!

4.3 Proposition: Sei K ein Körper. Jede endliche Erweiterung von K ist algebraisch.

Beweis. Sei $L : K$ eine endliche Körpererweiterung von K mit $[L : K] =: n \in \mathbb{N}$. Sei $a \in L$, dann sind die $n + 1$ Elemente

$$1, a, a^2, \ldots, a^n$$

linear abhängig über K (vgl. (iv) aus Proposition 3.27). Das heißt, es gibt Skalare $\alpha_0, \ldots, \alpha_n \in K$, wovon mind. einer ungleich 0 ist, so dass $\alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n = 0$ gilt. Also ist a Nullstelle des Polynoms $f(X) := \sum_{i=0}^{n} \alpha_i X^i \in K[X] \setminus \{0\}$ und damit a gemäß Definition algebraisch. Da $a \in L$ beliebig gewählt wurde folgt insgesamt, dass $L : K$ algebraisch ist. □

Die Umkehrung der Aussage aus der Proposition ist nicht richtig, d.h. es gibt algebraische Körpererweiterungen, die nicht endlich sind.

4.4 Beispiel: Es sei $R := \{\sum_{i=0}^{n} a_i 2^{b_i} |$ mit $a_i, b_i \in \mathbb{Q}$ und $n \in \mathbb{N}\}$ die Menge aller endlichen rationalen Summenprodukten. Diese Menge ist ein Unterring von $\mathbb{R}$, jedoch kein Körper. Deshalb betrachten wir den Quotientenkörper K von R. Auch im Quotientenkörper ist jedes Element eine endliche rationale Linearkombination von Wurzeln. Deshalb existieren Polynome f_a, so dass jedes Element $k \in K$ eingsetzt in f_a verschwindet, also ist $K : \mathbb{Q}$ algebraisch.
Allerdings ist diese Erweiterung nicht endlich, da für jedes $n \in \mathbb{N}$ die Körper $\mathbb{Q}(2^{1/n})$ Teilkörper von K sind, d.h. der Vektorraum $K : R$ kann damit nur unendlich-dimensional sein.

Das letzte Beispiel hat gezeigt, dass es einen algebraischen (Erweiterungs-) Körper L von K gibt, der nicht endlich erzeugt werden kann bzw. das der K-Vektorraum L unendlich-dimensional über K ist.

4.5 Satz: Es sei $L : K$ eine Körpererweiterung und $a \in L$. Dann sind folgende Aussagen äquivalent:

(i) a ist algebraisch über K;

(ii) $K[a]$ ist endlich-dimensional als K-Vektorraum;

(iii) $K[a]$ ist ein Körper.

Ist eine (und damit alle) dieser Bedingungen erfüllt und ist $\mu \in K[X]$ das Minimalpolynom von a über K mit $n := \mathrm{Grad}(\mu)$, so existiert ein K-Isomorphismus

$$\mathbf{K(a)=K[a]} \cong K[X]/(\mu).$$

Dabei sind $[K[a] : K] = n$ und $\{1, a, a^2, \ldots, a^{n-1}\}$ eine K-Basis von $K[a]$.

Beweis. Zu $K(A)$ gehören alle Elemente von K und A und somit auch alle Elemente, die durch Addition, Subtraktion, Multiplikation und Division aus den Elementen von $K \cup A$ hervorgehen. Insbesondere ist die Menge aller Einsetzungen in Polynomen

$$K[a] = \{f(a) = \sum_{i=1}^{n} \lambda_i a^i |\ f \in K[X]\}$$

Teil der Adjunktion $K(a)$, d.h. es gilt $K[a] \subseteq K(a)$. Zudem ist aufgrund der Definition $K[a] = \mathrm{Bild}(\psi_a)$. Ist $a \in L$ algebraisch mit Minimalpolynom μ_a über K, so ist $\mathrm{Kern}(\psi_a)$ das Hauptideal $I := \mathrm{Kern}(\psi_a) = (\mu_a)$. Wenden wir nun den Homomorphiesatz an, dann gilt

$$K[X]/\mathrm{Kern}(\psi_a) \cong \mathrm{Bild}(\psi_a) = K[a]. \qquad (*)$$

Ist das Element a hingegen transzendent, dann ist $I = \mathrm{Kern}(\psi_a) = \{0\}$ weshalb mit (*) $K[a] \cong K[X]$ folgt. Wegen $(\psi_a)_{|K} = \mathrm{id}_K$ ist dies ein K-Isomorphismus, also auch ein Isomorphismus der K-Vektorräume.

(i) $\Leftrightarrow$ (ii):

„⇒“: Sei zunächst a algebraisch mit μ als Minimalpolynom von a. In Proposition 3.27 (iv) haben wir nachgewiesen, dass die Menge

$$B := \{1, a, \ldots, a^{n-1}\}$$

eine Basis des K-Vektorraumes $K(a) \cong K[a]$ ist.

„⇐“: Diese Aussage wurde bereits in Proposition 4.3 gezeigt.

(i)⇔ (iii):

„⇒“: Das Minimalpolynom μ ist gemäß Proposition 3.27 (i) irreduzibel und daher ist (μ) ein maximales Ideal. Daraus folgt wiederum, dass $K[X]/(\mu)$ ein Körper ist. Aufgrund des Isomorphismus $K[X]/(\mu) \cong K[a]$ ist auch $K[a]$ ein Körper.

„⇐“: Ist a nicht algebraisch, so ist $\mathrm{Kern}(\psi_a) = \{0\}$, also

$$K[a] = Bild(\psi_a) \cong K[X].$$

Somit ist $K[a]$ kein Körper und nicht endlich-dimensional über K. Verneinen wir diese Implikation, so erhalten wir gerade die gewünschte Aussage. □

Das Argument zu Beginn des Beweises ist von zentraler Bedeutung und sollte unbedingt verstanden worden sein!

Die Kernaussage des letzten Satzes ist demnach, dass die algebraische Körpererweiterung $K(a) : K$ mit $K[a]$ isomorph ist und demnach beide Körpererweiterungen im wesentlichen dasselbe sind.

4.6 Beispiel: Sei $a := \sqrt[3]{2} \in \mathbb{R}$. Wir untersuchen die Körpererweiterung $\mathbb{Q}(a) : \mathbb{Q}$. Es ist $\mu_a(X) = X^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Gemäß (*) aus Satz 4.5 ist $\mathbb{Q}[X]/(\mu_a(X)) \cong \mathbb{Q}(a)$. In natürlicher Weise bildet $\mathbb{Q}(a)$ einen Vektorraum über $\mathbb{Q}$. Der Vektorraum $\mathbb{Q}(a)$ besitzt Dimension 3, da das Minimalpolynoms μ_a den Grad 3 besitzt. Die Vektoren

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$$

bilden eine Basis von $\mathbb{Q}(a)$. Demnach können wir jeden Vektor aus $\mathbb{Q}(a)$ als Linearkombination mit einer dieser drei Vektoren erzeugen, d.h. es gilt

$$\mathbb{Q}(a) = \{\lambda_0 + \lambda_1 \sqrt[3]{2} + \lambda_2 (\sqrt[3]{2})^2 |\ \lambda_0, \lambda_1, \lambda_2 \in \mathbb{Q}\}.$$

Ganz analog folgt aus Satz 4.5 bzw. (*), dass $\mathbb{R}(i) \cong \mathbb{R}[X]/(X^2 + 1)$, da $(X^2 + 1)$ das Minimalpolynom von i über $\mathbb{R}$ ist.

4.7 Folgerung: Es seien $L : K$ und $L' : K$ Körpererweiterungen, $a \in L$ und $a' \in L$ seien algebraisch über K mit gleichem Minimalpolynom. Dann existiert ein K-Isomorphismus $K[a] \xrightarrow{\sim} K[a']$.

Beweis. Da beide Erweiterungen dasselbe Minimalpolynom μ besitzen folgt die Behauptung mit $K[a] \cong K[X]/(\mu(X)) \cong K[a']$. □

4.8 Proposition: Sei $L : K$ eine Körpererweiterung. Es existieren algebraische Elemente $a_1, \ldots, a_n \in L$ mit $n \in \mathbb{N}$ über K, so dass $L \cong K(a_1, \ldots, a_n)$ genau dann, wenn $[L : K]$ endlich ist.

Beweis. „⇒“: Seien $a_1, \ldots, a_n$ algebraische Elemente über K, dann sind diese Elemente ebenfalls algebraisch über jeden Zwischenkörper mit demselben Minimalpolynomen. Wegen $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_{n-1})(a_n)$ ist nach Proposition 4.3 der Grad $[K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]$ endlich. Die Behauptung folgt nun durch Anwendung von Folgerung 3.16 auf den „Körperturm“ $K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \ldots \subseteq K(a_1, \ldots, a_n) = L$.

„⇐“: Sei $[L : K]$ endlich, d.h. der K-Vektorraumes L besitzt endliche Dimension. Mit Proposition 4.3 folgt bereits die Behauptung. □

Um die bald folgende Charakterisierung von einfachen algebraischen Erweiterungen beweisen zu können, benötigen wir die folgende

4.9 Proposition: Seien $K(a)$ eine einfache algebraische Erweiterung von K und M ein Zwischenkörper von $K(a) : K$ sowie $\mu_a = \sum_{i=0}^{r} \lambda_i X^i \in M[X]$ das Minimalpolynom von a über M. Dann ist

$$M = K(\lambda_0, \lambda_1, \ldots, \lambda_r).$$

Beweis. Sei $M' := K(\lambda_0, \ldots, \lambda_r)$ der kleinste Zwischenkörper von $L : K$ der $(K \cup m_0 \cup \ldots \cup m_r)$ enthält. Dann ist $M' \subseteq M$, weil die λ_i $i \in \mathbb{N}_r$ aus dem Körper M stammen. Das über M normierte irreduzible Polynom $\mu_a \in M[X]$ ist auch in $M'[X]$ enthalten, da deren Skalare sämtlich in M' enthalten sind. Zudem ist μ_a in $M'[X]$ normiert und irreduzibel und nach Proposition 3.27 (iii) ist μ_a das Minimalpolynom von a über M'. D.h. M' und M haben dasselbe Minimalpolynom, damit gilt $[M : K] = [M' : K]$ und mit Folgerung 4.7 ergibt sich das Gewünschte. □

Die letzte Proposition zeigt auf, dass sich ein beliebiger Zwischenkörper M einer einfachen algebraischen Körpererweiterung $K(a) : K$ mit Hilfe der Koeffizienten des zugehörigen Minimalpolynoms μ_a darstellen lässt.

Nun folgt der bereits angekündigte Satz.

4.10 Satz: Die Körpererweiterung $L : K$ ist genau dann einfach algebraisch, wenn $L : K$ nur endlich viele Zwischenkörper besitzt.

Beweis. „⇒“: Es sei $L : K$ eine einfache algebraische Körpererweiterung, d.h. es existiert ein über K algebraisches Element $a \in L$ mit $L = K(a)$. Sei M ein Zwischenkörper von $K(a) : K$ und $\mu_a = \sum_{i=0}^{r} \lambda_i X^i \in M[X]$ das Minimalpolynom von a über M. Gemäß Proposition 4.9 ist $M = K(\lambda_0, \lambda_1, \ldots, \lambda_r)$ durch die Koeffizienten des Minimalpolynoms μ_a

eindeutig bestimmt. Weiter sei μ'_a das Minimalpolynom von a über L. Aufgrund Proposition 3.27 ist μ_a ein normierter Teiler von μ'_a über $L[X]$. Davon kann es aber nur endlich viele geben, da $L[X]$ ein faktorieller Ring ist. Wegen der Isomorphie (*) kann es demnach nur endlich viele Zwischenkörper geben.

„⇐“: Hat umgekehrt $L : K$ genau $n \in \mathbb{N}$ viele Zwischenkörper, dann existieren gemäß Proposition 4.8 algebraische Elemente $a_1, \ldots, a_n$ mit $L = K(a_1, \ldots, a_n)$. Beginnend mit $a_1 \notin K, a_2 \notin K(a_1), \ldots, a_i \notin K(a_1, \ldots, a_{i-1})$, etc. konstruieren wir einen Körperturm $K \subseteq K(a_1) \subseteq \ldots \subseteq K(a_1, \ldots, a_i) \subseteq \ldots$, der nach endlich vielen Schritten in L endet. Dies zeigt, dass $[L : K]$ endlich ist. Ist K ein endlicher Körper, dann ist die endliche Erweiterung $L : K$ einfach.
Sei K ein unendlicher Körper. Für alle $\lambda \in K$ betrachten wir die Zwischenkörper

$$K_\lambda := K(a_1 + \lambda a_2).$$

Offensichtlich gilt $K \subseteq K_z \subseteq K(a_1, a_2) \subseteq L$. Da für die unendlich vielen Zwischenkörpern K_λ mit $\lambda \in K$ – gemäß Voraussetzung – nur endlich viele verschiedene sein können, gibt es $\lambda_1, \lambda_2 \in K$, $\lambda_1 \neq \lambda_2$ mit $K_{\lambda_1} = K_{\lambda_2}$. Daher ist $a_1 + \lambda_1 a_2$ ein Element aus K_{λ_2} und somit gilt auch

$$(a_1 + \lambda_2 a_2) - (a_1 + \lambda_1 a_2) = (\lambda_2 - \lambda_1) a_2 \in K_{\lambda_2}.$$

Da $\lambda_1 \neq \lambda_2$ ist $\lambda_2 - \lambda_1 \neq 0$ in K, weshalb $a_2 \in K_{\lambda_2}$ gilt. Sodann ist $a_1 = (a_1 + \lambda_2 a_2) - (\lambda_2 a_2)$ in K_{λ_2} enthalten und es folgt $K(a_1, a_2) \subseteq K_{\lambda_2}$, bzw.

$$K(a_1, a_2) = K(a_1 + z a_2).$$

Iterieren wir dieses Verfahrens so finden wir $\lambda_2, \ldots, \lambda_n \in K$ mit $L = K(a_1, \ldots, a_n) = K(a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n)$. □

4.11 Folgerung: Jeder Zwischenkörper einer einfach algebraischen Erweiterung von K ist einfach algebraisch über K.

Beweis. Wenn die Erweiterung nur endlich viele Zwischenkörper hat, dann liegen zwischen K und dem betrachteten Zwischenkörper erst recht nur endlich viele andere Zwischenkörper. □

4.12 Proposition: Es sei M ein Zwischenkörper der Erweiterung $L : K$, dann gilt:
$L : K$ ist genau dann algebraisch, wenn $L : M$ und $M : K$ es sind.

Beweis.
„⇒“: Nach Voraussetzungen existiert für jedes $a \in L$ ein Minimalpolynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$. Diese Polynome können auch für die Erweiterungen $L : M$ bzw. $M : K$ dienen.

„⇐“: Seien nun $L : M$ und $M : K$ algebraische Erweiterungen. Zu $a \in L$ sei $\mu_a(X) = \sum_{i=0}^{r} \lambda_i X^i$ das Minimalpolynom von a über M. Die Koeffizienten $\lambda_i \in M$ sind algebraisch über K, weshalb $M' := K(\lambda_0, \ldots, \lambda_r)$ über K eine endliche Erweiterung von K ist,

d.h. $[M' : K] \in \mathbb{N}$. Es ist auch a algebraisch über M', da $\mu_a \in M'[X]$ ist. Zudem ist $[M'(a) : M']$ endlich. Der Gradsatz liefert

$$[M'(a) : K] = [M'(a) : M'][M' : K]$$

Beide Faktoren der rechten Seite haben wir als endlich nachgewiesen, damit ist auch $[M'(a) : K]$ endlich, woraus wir mit Proposition 4.3 ableiten, dass a algebraisch über K ist. Dies geht für jedes $a \in L$, folglich ist $L : K$ algebraisch. □

Ein sehr schönes Ergebnis ist der folgende

4.13 Satz: In jeder Körpererweiterung $L : K$ ist die Menge

$$A(L) := \{a \in L |\ a \text{ ist algebraisch über } K\}$$

ein algebraischer Erweiterungskörper von K.

Beweis. Es gilt $K \subseteq A(L)$ und alle Elemente aus $A(L)$ sind algebraisch über K. Es bleibt zu zeigen, dass $A(L)$ ein Körper ist. Dazu betrachten wir zu $a, b \in A(L)$ den Körper $K(a, b)$, der nach Proposition 4.8 über K algebraisch ist. Insbesondere sind dann die in $K(a, b)$ liegenden Elemente $a \pm b, ab, ab^{-1}$ (sofern $b \neq 0$) algebraisch über K, also auch in $A(L)$. □

Wie wir nun wissen bildet die Menge aller algebraischen Zahlen eines Körpers K selbst einen abzählbaren Körper $A(K)$. Der Körper $A(K)$ ist algebraisch abgeschlossen, d.h. jedes Polynom $f \in A(K)[X]$ mit algebraischen Koeffizienten besitzt nur algebraische Nullstellen. $A(K)$ ist ein mimimaler algebraisch abgeschlossener Oberkörper von K. D.h. auch, wie wir im Beweis bereits festgestellt haben, dass für $a, b \in A(K)$ gilt, dass bspw. $a + b \in A(K)$ liegt. Hat man also das Minimalpolynom von a und b, so kann man explizit (mit Hilfe eines Gleichungssystems) das Minimalpolynom von $a + b$ berechnen.

4.14 Beispiel: Es sei $\mathbb{C} : \mathbb{Q}$ eine Körpererweiterung, dann ist

$$A(\mathbb{Q}) = \{a \in \mathbb{C} |\ a \text{ ist algebraisch über } \mathbb{Q}\}$$

ein minimaler algebraisch abgeschlossener Oberkörper von $\mathbb{Q}$. Wie wir wissen ist der maximale algebraisch abgeschlossene Oberkörper von $\mathbb{Q}$ gerade $\mathbb{C}$, denn über $\mathbb{C}$ zerfällt jedes Polynom in Linearfaktoren.

5 Tranzendente Körpererweiterungen

In diesem Kapitel untersuchen wir die einfachen tranzendenten Körpererweiterungen.

Vergegenwärtigen wir uns nocheinmal die Bedeutung einer algebraischen Zahl a über einem Körper K: Ist a algebraisch, so existiert ein vom Nullpolynom verschiedenes $f \in K[X]$, so dass $f(a) = 0$ gilt. Die Eigenschaft „a ist algebraisch“ bedeutet also im Bezug auf den Einsetzungshomomorphismus ψ_a, dass der $\text{Kern}(\psi_a) \neq \{0\}$ ist.

Ist a hingegen nicht algebraisch, also tranzendent, so existiert kein Polynom in $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$. Daher ist $\text{Kern}(\psi_a) = \{0\}$ und aufgrund des Homomorphiesatzes folgt

$$K[X]/(0) = K[X] \cong K[a] = \text{Bild}(\psi_a).$$

Das Bild des Substitutionshomomorphismus ist demnach isomorph zum Polynomring und damit kein Körper. Insbesondere ist $K[a] \nsubseteq K(a)$, da $K(a)$ der kleinste Körper ist, der K und a enthält.

5.1 Satz: Es sei $K(a) : K$ eine Körpererweiterung und a transzendent über K, dann gilt:

(i) $K(a) \cong K[X]$;

(ii) $[K(a) : K] = \infty$;

(iii) a^2 ist transzendent über K und es gilt $K(a^2) \subsetneq K(a)$.

Beweis. (i) Ein Beweis wurde im Text unmittelbar vor diesem Satz erbracht.

(ii) Es gilt $K[X] \cong K(a)$ und der Polynomring $K[X]$ ist als Vektorraum unendlichdimensional.

(iii) Sei $f = \sum_{i \in \mathbb{N}} \lambda_i X^i \in K[X]$ mit $f(a^2) = \sum_{i \in \mathbb{N}} \lambda_i a^{2i} = 0$. Da gemäß (ii) die Dimension des K-Vektorraumes $K[X]$ unendlich ist, folgt, dass die Potenzen $\{a^i | \ i \in \mathbb{N}\}$ von a linear unabhängige Vektoren sind, d.h. $\lambda_i = 0$ für alle $i \in \mathbb{N}$. Es ist also $f = 0$ und a^2 somit transzendent. Unmittelbar aus der Definition folgt $K(a^2) \subseteq K(a)$. Wir zeigen durch einen Widerspruch, dass die Inklusion echt ist, das also $K(a^2) \subsetneq K(a)$. Dazu nehmen wir das Gegenteil an, was zur Folge hat, dass a in $K(a^2)$ enthalten ist. Nach (i) dieses Satzes folgt für das Element a^2, dass $K(a^2) \cong K[X]$ gilt. Es gibt also Polynome $f, g \in K[X]$ mit

$$a \cong f(a^2)g(a^2)^{-1},$$

woraus $g(a^2)a \cong f(a^2)$ folgt. Auf der linken Seite der letzten Gleichung steht eine Linearkombination ungerader Potenzen von a und auf der rechten Seite eine Linearkombination gerader Potenzen. Wegen der linearen Unabhängigkeit von $\{a^i | \ i \in \mathbb{N}\}$ folgt $f(a^2) = 0$ und $g(a^2)a = 0$, was wiederum $f = g = 0$ impliziert. Das kann aber nicht sein, da $a \neq 0$ - Widerspruch. Somit ist

□

5.2 Folgerung: Eine einfache transzendente Körpererweiterung hat unendlich viele Zwischenkörper.

Beweis. Wiederholte Anwendung von (iii) des letzten Satzes ergibt einen unendlichen echt absteigenden „Körperturm“

$$K \subsetneq \ldots \subsetneq K(a^{2n}) \subsetneq \ldots K(a^4) \subsetneq K(a^2) \subsetneq K(a).$$

□

Hinweis:

Haben Sie einen Fehler oder eine Unstimmigkeit in diesem Dokument entdeckt?
Falls dem so ist, dann senden Sie mir bitte eine E-Mail an Alexander@mathematik-netz.de.

Vielen Dank!

Weiterhin viel Spaß mit der Mathematik!

http://www.mathematik-netz.de
http://www.mathering.de

Literaturverzeichnis

[1] Bosch, S.; Algebra; 2003, fünfte Auflage; Springer Verlag.

[2] Meyberg, K.; Algebra, Teil 1; 1979, 2. Auflage; Hanser Verlag.

[3] Meyberg, K.; Algebra, Teil 2; 1979, 2 Auflage; Hanser Verlag.

[4] Lang, S.; Algebra; 2004, 3. Auflage; Springer Verlag.

[5] van der Waerden, B.L.; Algebra – Erster Teil; 1967, 5. Auflage; Springer Verlag.

[6] van der Waerden, B.L.; Algebra – Zweiter Teil; 1966, 7. Auflage; Springer Verlag.

[7] Unger, L.; Lineare Algebra I (1102); 2003; Skript der FernUniversität in Hagen.

[8] Scharlau, W.; Algebra I, Kurs 1312; 2004; FernUniversität in Hagen.

[9] Hartlieb, S. und Unger, L.; Mathematische Grundlagen der Kryptografie, Kurs 1321; 2005; FernUniversität in Hagen.

[10] Scheja, G. und Storch, U.; Lehrbuch der Algebra, Teil 1; 1993; B.G. Teubner Verlag.