VORLESUNG ALGEBRA FÜR LEHRAMTSKANDIDATEN, WINTERSEMESTER 2019/20

JOHANNES EBERT

Inhaltsverzeichnis

Date: 13. Januar 2020.

1. Motivation/Einleitung

Notationen. Im folgenden werden einige Notationen ohne weitere Kommentare verwendet.

(1) $\mathbb{N}$ ist die Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$.
(2) $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
(3) $\mathbb{Z}$ ist die Menge der ganzen Zahlen.
(4) $\mathbb{Q}$, $\mathbb{R}$ sind die Mengen der rationalen bzw. reellen Zahlen.
(5) Für $n \in \mathbb{N}$ sei $\underline{n}; = \{1, \ldots, n\}$.
(6) Ist X ein endliche Menge, so ist $|X| \in \mathbb{N}_0$ die Anzahl der Elemente von X.

Die wichtigsten Sätze werden als "Theoreme" bezeichnet; es gibt keinen logischen Unterschied zwischen Sätzen, Theoremen und Lemmas.

1.1. Gruppen, Ringe, Körper.

Wir beginnen mit der Einführung einiger grundlegender Vokabeln.

Definition 1.1.1. *Eine* Gruppe *ist eine Menge G, zusammen mit einer Verknüpfung*

$$G \times G \to G; (g, h) \mapsto g \cdot h,$$

so dass folgende Axiome gelten:

(1) *Die Verknüpfung ist* assoziativ*, d.h. es gilt*

$$(g \cdot h) \cdot k = g \cdot (h \cdot k)$$

für alle $g, h, k \in G$.
(2) *Es gibt ein $e \in G$, so dass*

$$e \cdot g = g \cdot e = g$$

für alle $g \in G$. e heißt neutrales Element *von G.*
(3) *zu jedem $g \in G$ gibt es ein $h \in G$, so dass*

$$g \cdot h = h \cdot g = e.$$

h heißt das zu g inverse Element*.*

Bemerkung 1.1.2. (1) *Wir schreiben die Verknüpfung meistens kurz als $gh := g \cdot h$. Durch die Assoziativität ist der Ausdruck $ghk := (gh)k = g(hk)$ von der Klammerung unabhängig. Allgemeiner ist der Ausdruck $g_1 \cdots g_n \in G$ unzweideutig bestimmt.*
(2) *Das Element $e \in G$ ist durch die oben hingeschriebene Eigenschaft eindeutig bestimmt, das heißt, ist $e' \in G$ ein weiteres neutrales Element, so gilt*

$$e = e \cdot e' = e'.$$

Dieses Element wird meistens mit dem Symbol 1 bezeichnet.

(3) *sind h, h' zwei inverse Elemente zu $g \in G$, so gilt*

$$h' = h'1 = h'(gh) = (h'g)h = 1h = h,$$

also ist das Inverse zu g ebenfalls eindeutig bestimmt. Wir schreiben meistens g^{-1} für dieses Element. Die Formel

$$(gh)^{-1} = h^{-1}g^{-1}$$

sollte man in Erinnerung behalten.

(4) *Es gilt die* Kürzungsregel*: aus $hg = h'g$ folgt $h = h'$, und aus $gh = gh'$ folgt $h = h'$.*

(5) *Für ein Element $g \in G$ und $n \in \mathbb{N}$ definieren wir rekursiv*

$$g^1 := g;\ g^n := gg^{n-1},$$

und $g^{-n} := (g^{-1})^n = (g^n)^{-1}$. Es gilt

$$g^{m+n} = g^n g^m$$

für alle $m, n \in \mathbb{Z}$.

Definition 1.1.3. *Eine Gruppe G heißt* kommutativ *oder* abelsch*, falls*

$$g \cdot h = h \cdot g$$

für alle $g, h \in G$ gilt.

Bemerkung 1.1.4. *In abelschen Gruppen wird die Verknüpfung oft (aber keineswegs immer)* additiv *geschrieben, also als $(g, h) \mapsto g + h$. In diesem Fall wird das neutrale Element mit $0 \in G$ bezeichnet, und das Inverse zu g mit $-g$. Ferner schreiben wir für $k \in \mathbb{Z}$ $kg := g^k$.*

Beispiele 1.1.5. *Die Menge $\mathbb{Z}$, mit der Addition, ist eine abelsche Gruppe. Gleichfalls sind $\mathbb{R}$ und $\mathbb{Q}$ mit der Addition abelsche Gruppen, und $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ und $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$, jeweils mit der Multiplikation. Die Menge $\mathbb{Z} \setminus \{0\}$ mit der Multiplikation ist* keine *Gruppe, weil es keine inversen Elemente gibt. Ebensowenig ist $\mathbb{N}_0$ mit der Addition eine Gruppe.*

Beispiel 1.1.6. *Die Menge Σ_n aller bijektiven Abbildungen der Menge $\underline{n} := \{1, \ldots, n\}$ in sich, mit der Komposition von Abbildungen als Verknüpfung, ist eine Gruppe, die* symmetrische Gruppe*. Die symmetrische Gruppe ist nicht kommutativ, wenn $n \geq 3$.*

Definition 1.1.7. *Es sei G eine Gruppe. Eine* Untergruppe *ist eine Teilmenge $H \subset G$, so dass gilt:*

(1) *$1 \in H$,*
(2) *sind $g, h \in H$, so gilt auch $gh \in H$, und*
(3) *ist $g \in H$, so ist auch $g^{-1} \in H$.*

Definition 1.1.8. *Seien G und H zwei Gruppen. Eine Abbildung $\varphi : G \to H$ heißt* Gruppenhomomorphismus*, falls*

$$\varphi(g_0 g_1) = \varphi(g_0)\varphi(g_1)$$

für alle $g_0, g_1 \in G$ gilt. Falls φ bijektiv ist, so heißt φ Isomorphismus*.*

Bemerkung 1.1.9. *Es sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

(1) *$\varphi(1) = 1$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$ für jedes $g \in G$.*

(2) *Der* Kern $\ker(\varphi) := \{g \in G | \varphi(g) = 1\} \subset G$ *und das* Bild $\mathrm{im}(\varphi) := \{\varphi(g) \in H | g \in G\} \subset H$ *sind Untergruppen von* G *bzw.* H*.*
(3) *Ist* φ *bijektiv, so ist auch die Umkehrabbildung* $\varphi^{-1} : H \to G$ *ein Gruppenhomomorphismus. In diesem Fall sagt man auch, dass* φ *ein* Gruppenisomorphismus *oder einfach ein* Isomorphismus *ist. Man sagt, dass* G *und* H isomorph *sind, in Symbolen:* $G \cong H$*, wenn es einen Isomorphismus* $\varphi : G \to H$ *gibt.*

Definition 1.1.10. *Ein* Ring *ist eine Menge* R*, zusammen mit zwei Verknüpfungen, nmlich einer Addition*

$$R \times R \to R;\ (x, y) \mapsto x + y$$

und einer Multiplikation

$$R \times R \to R;\ (x, y) \mapsto xy,$$

so dass folgende Axiome gelten.

(1) $(R, +)$ *ist eine abelsche Gruppe mit neutralem Element* 0*.*
(2) *Die Multiplikation ist assoziativ.*
(3) *Es gelten die* Distributivgesetze*: für alle* $x, y, z \in R$ *ist*

$$(x + y)z = xz + yz;\ z(x + y) = zx + zy.$$

Ein Ring R *heißt* kommutativ*, falls*

$$xy = yx$$

für alle $x, y \in R$ *gilt. Ein* Einselement *in* R *ist ein* $1 \in R$*, so dass*

$$1x = x1 = x$$

für alle $x \in R$ *gilt. Wenn ein Einselement in* R *existiert, so heißt* R *auch* Ring mit Eins*.*

Bemerkung 1.1.11. *Man kann, ähnlich wie im Fall von Gruppen, zeigen, dass in einem Ring höchstens ein Einselement existieren kann.*

Bemerkung 1.1.12. *In der Literatur ist die Terminologie nicht ganz einheitlich. Viele Autoren fordern die Existenz einer Eins. Wir werden uns fast nur für Ringe mit Eins interessieren.*

Beispiele 1.1.13. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *sind kommutative Ringe mit Eins. Die Menge* $\mathrm{Mat}_{n,n}(\mathbb{R})$ *aller* $n \times n$*-Matrizen mit der üblichen Addition und der Matrizenmultiplikation ist ein Ring mit Eins, welcher für* $n \geq 2$ *jedoch nicht kommutativ ist. Die Menge* $2\mathbb{Z} \subset \mathbb{Z}$ *aller geraden Zahlen ist ein Ring, der kein Einselement besitzt.*

Definition 1.1.14. *Es seien* R, S *Ringe. Ein* Ringhomomorphismus $\varphi : R \to S$ *ist eine Abbildung, so dass für alle* $x, y \in R$ *gilt*

$$\varphi(x + y) = \varphi(x) + \varphi(y);\ \varphi(xy) = \varphi(x)\varphi(y).$$

Definition 1.1.15. *Es sei* R *ein Ring. Ein* Unterring *von* R *ist eine Teilmenge* $S \subset R$*, so dass gilt:*

(1) $0 \in S$*,*
(2) *Sind* $x, y \in S$*, dann auch* $x + y, xy, -x$*.*

Definition 1.1.16. *Ein* Körper *ist ein kommutativer Ring* K *mit Eins, so dass* $1 \neq 0$ *und so dass jedes Element* $x \in K$*,* $x \neq 0$*, ein multiplikatives Inverses* $x^{-1} = \frac{1}{x} \in K$ *besitzt.*

Ist K ein Körper, so ist

$$K^\times := \{x \in K | x \neq 0\}$$

mit der Multiplikation eine Gruppe, die *multiplikative Gruppe* von K.

Beispiele 1.1.17. *Der Ring $\mathbb{Z}$ ist kein Körper, aber $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.*

Beispiel 1.1.18. *Es sei $\mathbb{F}_2$ die Menge $\{0,1\}$, wobei wir setzen*

$$0+0=0,\ 0+1=1+0=1,\ 1+1=0,\ 0\cdot 0=0\cdot 1=1\cdot 0,\ 1\cdot 1=1.$$

Man rechnet schnell nach, dass $\mathbb{F}_2$ mit diesen beiden Verknüpfungen ein Körper ist. Wir werden im Laufe der Vorlesung lernen:

1. *Ist K ein Körper mit endlich vielen Elementen $\sharp(K) = q$, so ist $q = p^n$, p eine Primzahl, $n \geq 1$.*
2. *Zu jeder Primzahl p und jedem $n \geq 1$ gibt es einen Körper $\mathbb{F}_{p^n}$ mit genau p^n Elementen, und $\mathbb{F}_{p^n}$ ist bis auf Isomorphie eindeutig bestimmt.*

Definition 1.1.19. *Ein* Körperhomomorphismus $\varphi : K \to L$ *ist ein Ringhomomorphismus mit $\varphi(1) = 1$.*

Satz 1.1.20. *Jeder Körperhomomorphismus ist injektiv.*

Beweis. Sei $\varphi : K \to L$ ein Körperhomomorphismus und $x, y \in K$, $x \neq y$. Dann ist

$$1 = \varphi(1) = \varphi((x-y)\frac{1}{x-y}) = \varphi(x-y)\varphi(\frac{1}{x-y}) = (\varphi(x)-\varphi(y))\varphi(\frac{1}{x-y}).$$

Es folgt $\varphi(x) - \varphi(y) \neq 0$, also $\varphi(x) \neq \varphi(y)$. □

Definition 1.1.21 (Unterkörper und Körpererweiterung)**.** *Ein* Unterkörper $L \subset K$ *eines Körpers ist ein Unterring, so dass $1 \in L$, und so dass mit $x \in L$, $x \neq 0$, das Element $\frac{1}{x} \in K$ immer zu L gehört.*

Wir sagen auch, dass K ein Erweiterungskörper *von L ist.*

1.2. **Lösungen algebraischer Gleichungen.** Es sei im folgenden K ein Körper und $a_0, \ldots, a_n \in K$ seien Elemente, wobei $a_n \neq 0$ vorausgesetzt sei. Wir suchen die Lösungen der Gleichung

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0 \tag{1.2.1}$$

in K.

Bemerkung 1.2.2. *Weil $a_n \neq 0$ vorausgesetzt ist, sind die Lösungen von* (1.2.1) *dieselben wie die Lösungen von*

$$x^n + \frac{a_{n-1}}{a_n}x^{n-1} \ldots + \frac{a_0}{a_n} = 0. \tag{1.2.3}$$

Wir verlieren also nichts, wenn wir immer $a_n = 1$ voraussetzen.

Der Fall $n = 0$ ist langweilig, und für $n = 1$ ist (1.2.1) eine lineare Gleichung, die ebenfalls sehr einfach zu behandeln ist. Wir konzentrieren uns also auf den Fall $n \geq 2$. Für $n = 2$ ist (1.2.3) eine quadratische Gleichung

$$x^2 + a_1 x + a_0 = 0. \tag{1.2.4}$$

Aus der Schule ist folgender Trick bekannt, um die Lösung zu finden. Es ist nämlich

$$x^2 + a_1 x + a_0 = x^2 + a_1 x + a_0 - (x + \frac{a_1}{2})^2 + (x + \frac{a_1}{2})^2 =$$
$$x^2 + a_1 x + a_0 - (x^2 + a_1 x + \frac{a_1^2}{4}) + (x + \frac{a_1}{2})^2 =$$
$$(x + \frac{a_1}{2})^2 - (\frac{a_1^2}{4} - a_0).$$

Somit ist 1.2.4 äquivalent zu

$$(x + \frac{a_1}{2})^2 = \frac{a_1^2}{4} - a_0. \tag{1.2.5}$$

Nun substituiere $y = x + \frac{a_1}{2}$ sowie $b = \frac{a_1^2}{4} - a_0$ und erhalte

$$y^2 = b. \tag{1.2.6}$$

Wir sehen, dass x genau dann eine Lösung von (1.2.4) ist, wenn $y = x + \frac{a_1}{2}$ eine Lösung von (1.2.6) ist. Die Lösungen von (1.2.6) sind aber offenbar (?) durch

$$y = \pm\sqrt{b}$$

gegeben, und also sind die Lösungen von (1.2.4) durch

$$x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0} \tag{1.2.7}$$

gegeben. Bis hierhin sind wir sehr naiv vorgegangen.

Frage 1.2.8. *Was bedeutet das Symbol $\sqrt{b}$?*

Unter einer *Quadratwurzel* $\sqrt{b}$ versteht nichts anderes als eine Lösung y von $y^2 = b$. Mit dem Wurzelsymbol muss man vorsichtig umgehen, denn selbst wenn eine Quadratwurzel existiert, so ist der Ausdruck $\sqrt{b}$ nicht ohne weitere Erklärung unzweideutig definiert, weil im Allgemeinen mehrere Quadratwurzeln existieren können. Hat (1.2.6) Lösungen, und wenn ja, wieviele?

Lemma 1.2.9. *Es sei K ein Körper und $b \in K$. Dann hat die Gleichung $y^2 = b$ höchstens zwei Lösungen in K, und diese sind von der Form $\pm y$.*

Beweis. Falls $y^2 = b$ und $x^2 = b$, so gilt

$$0 = x^2 - y^2 = (x - y)(x + y).$$

Weil K ein Körper ist, must entweder $(x - y) = 0$ oder $(x + y) = 0$ gelten, das heißt, entweder $x = y$ oder $x = -y$. □

Der oben skizzierte Lösungsweg wirft zwei Probleme auf.

(1) Wir haben bei der Reduktion von (1.2.4) auf (1.2.5) die binomische Formel $(x + y)^2 = x^2 + y^2 + xy + yx = x^2 + y^2 + xy + xy = x^2 + y^2 + (1 + 1)xy$ benutzt, und *definieren* $2 \in K$ als $1 + 1$. Wir haben durch dieses Element 2 geteilt, und das setzt voraus, dass in K $2 \neq 0$ gilt. Im Körper $\mathbb{F}_2$ ist aber $1 + 1 = 2$, so dass wir durch Null teilen müssten, was aber keinesfalls erlaubt ist. Es folgt, dass die Formel (1.2.7) in $\mathbb{F}_2$ keinen Sinn ergibt. Für Körper wie $\mathbb{Q}$ und $\mathbb{R}$ ist dieses Problem nicht existient.

(2) Ist $a \in K$ ein Element eines Körpers, so braucht keine Quadratwurzel x, also ein $x \in K$ mit $x^2 = a$ zu existieren. In diesem Fall ist die Lösungsformel (1.2.7) ebenfalls, zumindest ohne weitere Überlegungen, ohne Bedeutung.

Wir betrachten nun zwei Beispiele.

Satz 1.2.10. *Es gibt keine rationale Zahl $x \in \mathbb{Q}$ mit $x^2 = 2$. Allgemeiner: ist p eine Primzahl und $n \geq 2$, so existiert kein $x \in \mathbb{Q}$ mit $x^n = p$.*

Bekanntlich ist eine *Primzahl* $p \in \mathbb{N}$ eine Zahl mit $p \geq 2$, so dass gilt: sind $x, y \in \mathbb{N}$ natürliche Zahlen mit $xy = p$, so gilt $x = 1$ oder $y = 1$. Im Beweis werden wir das *Lemma von Euklid* verwenden:

Lemma 1.2.11 (Lemma von Euklid)**.** *Eine natürlich Zahl $p \geq 2$ ist eine Primzahl genau dann, wenn gilt: ist p ein Teiler von ab, $a, b \in \mathbb{N}$, so ist p ein Teiler von a oder b.*

Das Thema der Teilbarkeit werden wir später (in §2) ausführlich behandeln und auch den (keineswegs trivialen) Beweis von Lemma 1.2.11 nachholen.

Beweis von Satz 1.2.10. Der Beweis wird durch Widerspruch geführt: sei also $x \in \mathbb{Q}$ ein Element mit $x^n = p$. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $x > 0$ ist (warum?). Wir können x in der Form $x = \frac{a}{b}$ schreiben, wobei $a, b \in \mathbb{N}$ teilerfremde natürliche Zahlen sind. Die Gleichung $x^n = p$ ist äquivalent zu

$$a^n = pb^n.$$

Es folgt, dass p ein Teiler von a^n ist, und nach dem Lemma von Euklid ist also p ein Teiler von a oder von a^{n-1}. Durch Wiederholung dieses Argumentes sehen wir, dass p ein Teiler von a ist. Also können wir

$$a = pa'$$

schreiben. Es folgt

$$p^n a'^n = a^n = pb^n.$$

Wir teilen diese Gleichung durch p und erhalten

$$p^{n-1} a^n = b^n.$$

Weil $n \geq 2$, teilt p die linke Seite und also auch b^n. Wie eben erhalten wir, dass p auch b teilt. Somit ist p ein gemeinsamer Teiler von a und b, im Widerspruch zur Annahme, dass a und b teilerfremd sind. □

Bemerkung 1.2.12. *Im Körper $\mathbb{R}$ existiert zu jedem $x > 0$ ein eindeutig bestimmtes $y > 0$ mit $y^n = x$; man bezeichnet dieses y mit dem Symbol $\sqrt[n]{x}$. Dies wird im Rahmen der Vorlesung Analysis I bewiesen. Es sei angemerkt, dass dieses y durch einen Grenzprozess konstruiert wird. Es folgt, dass die Gleichung $x^2 = 2$ in $\mathbb{Q}$ keine Lösung besitzt, im Erweiterungskörper $\mathbb{R}$ von $\mathbb{Q}$ aber schon. Im Laufe dieses Semesters werden wir solche* Körpererweiterungen *systematisch untersuchen.*

Satz 1.2.13. *Es gibt keine reelle Zahl x mit $x^2 = -1$.*

Beweis. Für jede reelle Zahl x gilt $x^2 \geq 0$, aber $-1 < 0$. □

Auch in diesem Fall gibt es eine Körpererweiterung von $\mathbb{R}$, in der die Gleichung $x^2 + 1 = 0$ eine Lösung hat, nämlich die komplexen Zahlen $\mathbb{C}$. Dazu später mehr.

1.3. **Polynome.**

Definition 1.3.1. *Es sei K ein Körper. Ein* Polynom *über K ist eine formale Summe*

$$f(x) = \sum_{k=0}^{\infty} a_k x^k,$$

wobei $a_k \in K$, und es gilt $a_k = 0$ für alle genügend großen k. Wir definieren die Addition und Multiplikation von Polynomen durch die Formeln

$$(\sum_{k=0}^{\infty} a_k x^k) + (\sum_{k=0}^{\infty} b_k x^k) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

und

$$(\sum_{k=0}^{\infty} a_k x^k)(\sum_{l=0}^{\infty} b_l x^l) = \sum_{n=0}^{\infty} (\sum_{m=0}^{n} a_m b_{n-m}) x^n.$$

Die Menge aller Polynome werde mit $K[x]$ bezeichnet.

Man zeigt ohne jede Idee, dass $K[x]$ mit der soeben erklärten Addition und Multiplikation ein kommutativer Ring mit Eins ist. Das Einselement ist das Polynom $1 + 0x + 0x^2 + \ldots$.

Vokabeln 1.3.2. *Sei $f(x) = \sum_k a_k x^k$ ein Polynom. Die a_k heißen* Koeffizienten *von $f(x)$. Wenn $f(x) \neq 0$, so sei $n \in \mathbb{N}_0$ die größte Zahl mit $a_n \neq 0$. Dieses n heißt* Grad *von $f(x)$ und wird mit $\deg(f(x))$ bezeichnet. In diesem Fall heißt a_n der* Leitkoeffizient*, und wenn $a_n = 1$, so heißt $f(x)$* normiert*. $f(x)$ heißt* konstant*, wenn $\deg(f(x)) = 0$. Aus formalen Gründen weisen wir dem Nullpolynom den Grad $-\infty$ zu.*

Satz 1.3.3. *Es gilt:*

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ *für alle $f, g \in K[x]$,*
2. $\deg(fg) = \deg(f) + \deg(g)$ *für alle $f, g \in K[x]$.*
3. *Der Ring $K[x]$ ist* nullteilerfrei*, d.h. wenn $fg = 0$, so ist $f = 0$ oder $g = 0$.*
4. *Ein Polynom $f \in K[x]$ besitzt ein multiplikatives Inverses genau dann, wenn f konstant und nicht das Nullpolynom ist.*

Der Beweis ist eine Übung.

Definition 1.3.4. *Es sei K ein Körper und $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$ ein Polynom. Die zugehörige* Polynomfunktion *ist die Abbildung $\Phi_f : K \to K$, welche durch*

$$\Phi_f(t) := \sum_{k=0}^{n} a_k t^k \in K$$

gegeben ist. Eine Nullstelle *von f ist ein $t \in K$, so dass $\Phi_f(t) = 0$ gilt.*

Die Definition ist so gemacht, dass

$$\Phi_{f+g} = \Phi_f + \Phi_g;\ \Phi_{fg} = \Phi_f \Phi_g$$

gilt. Wir schreiben oftmals einfach $f := \Phi_f$, was in der Regel nicht zu Verwirrungen führen wird.

Bemerkung 1.3.5. *Aus folgendem Grund muss zwischen Polynomen und Polynomfunktionen unterschieden werden. Im Körper $\mathbb{F}_2$ gilt $x^2 = x$ für jedes $x \in \mathbb{F}_2$. Aus diesem Grund definiert das nichttriviale Polynom $f(x) = x^2 - x$ die Nullfunktion. Allgemeiner gilt im endlichen Körper $\mathbb{F}_q$ stets $x^q = x$. Mit anderen Worten: in endlichen Körpern ist ein Polynom nicht eindeutig durch seine Polynomfunktion bestimmt. In unendlichen Körpern tritt dieses Problem nicht auf, als Folgerung aus dem nächsten wichtigen Satz.*

Satz 1.3.6. *Es sei $f(x) \in K[x]$ ein von Null verschiedenes Polynom vom Grad n. Dann besitzt f höchstens n Nullstellen in K.*

Ist K unendlich und $f(x) \in K[x]$ ein Polynom mit $\Phi_f = 0$, so hat f unendlich viele Nullstellen, muss also gleich dem Nullpolynom sein. Für den Beweis des Satzes ist ein fundamentales Hilfsmittel erforderlich, das im Prinzip aus der Schule vertraut sein sollte.

Satz 1.3.7 (Polynomdivision)**.** *Es sei K ein Körper und $0 \neq g(x) \in K[x]$ ein Polynom. Dann gilt: zu jedem $f(x) \in K[x]$ gibt es eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$ mit*

$$f(x) = g(x)q(x) + r(x)$$

sowie $\deg(r(x)) < \deg(g(x))$.

Beweis. Zur *Eindeutigkeit*: Sei $f(x) = q_0(x)g(x)+r_0(x) = q_1(x)g(x)+r_1(x)$, wobei $\deg(r_i(x)) < \deg(f(x))$ gelte. Wir müssen zeigen, dass $q_0(x) = q_1(x)$. Aber es ist

$$(q_0(x) - q_1(x))g(x) = r_1(x) - r_0(x).$$

Nun gilt

$$\deg(r_1(x) - r_0(x)) \leq \max\{\deg(r_0(x)), \deg(r_1(x))\} < \deg(g(x))$$

und andererseits

$$\deg(r_1(x) - r_0(x)) = \deg(g(x)) + \deg(q_0(x) - q_1(x)).$$

Beides zusammen impliziert

$$\deg(q_0(x) - q_1(x)) < 0$$

und somit $q_0(x) - q_1(x) = 0$, woraus die Eindeutigkeit folgt.

Zur *Existenz*. Sei $n := \deg(g(x))$. Wenn $\deg(f(x)) < n$, so setze $q(x) = 0$ und $r(x) = f(x)$. Für größere Grade argumentiere durch Induktion. Sei also $\deg(f(x)) = m \geq n$ und der Satz sei für alle Polynome $f(x)$ mit Grad $\leq (m-1)$ schon gezeigt. Schreibe

$$g(x) = a_n x^n + \ldots + a_0,$$
$$f(x) = b_m x^m + \ldots + b_0$$

mit $a_n, b_m \neq 0$. Das Polynom

$$h(x) := f(x) - \frac{b_m}{a_n} x^{m-n} g(x)$$

hat Grad $\leq (m-1)$ (betrachte die Leitkoeffizienten der beiden Summanden). Also gibt es nach Induktionsvoraussetzung Polynome $p(x), s(x)$ mit $\deg(s(x)) < n$, so dass

$$h(x) = p(x)g(x) + s(x).$$

Es folgt

$$f(x) = h(x) + \frac{b_m}{a_n} x^{m-n} g(x) = (p(x) + \frac{b_m}{a_n} x^{m-n}) g(x) + s(x),$$

und man setze $q(x) = p(x) + \frac{b_m}{a_n} x^{m-n}$. □

Aus dem Beweis des Satzes lässt sich ein Algorithmus ablesen, durch den $q(x)$ effektiv berechnet werden kann. Dies ist exakt das aus der Mittelstufe bekannte Verfahren.

Beweis von Satz 1.3.6. Wir beweisen den Satz durch Induktion über den Grad n. Die Fälle $n = 0$ und $n = 1$ sind trivial. Es sei nun $\deg(f(x)) = n$ und $t \in K$ sei eine Nullstelle von f. Polynomdivision mit $g(x) = x - t$ ergibt

$$f(x) = (x - t)q(x) + r(x)$$

mit $\deg(r(x)) = 0$, also muss $r(x) = a$ konstant sein. Es folgt $f(x) = (x-t)g(x)+a$, und den Wert der Konstanten a bestimmt man durch Einsetzen von t:

$$0 = f(t) = (t - t)q(t) + a = a.$$

Es gilt also $a = 0$, und daher

$$f(x) = (x - t)q(x).$$

Das Polynom $q(x)$ hat Grad $n-1$ und daher nach Induktionsvoraussetzung höchstens $n - 1$ Nullstellen in K, welche wir mit $t_2, \ldots, t_k$, $k \leq n$, bezeichnen wollen. Somit sind $t, t_2, \ldots, t_k$ genau die Nullstellen von f, und der Satz ist bewiesen. □

Aus dem Beweis des Satzes folgern wir weiterhin:

Korollar 1.3.8. *Ein Polynom $f(x) \in K[x]$ kann eindeutig in der Form*

$$f(x) = (x - t_1) \cdots (x - t_k) g(x)$$

geschrieben werden, wobei $t_1, \ldots, t_k \in K$ nicht notwendig verschiedene Nullstellen von $f(x)$ sind, $k \leq n$ und $g(x)$ keine Nullstellen in K hat. □

Die Polynome $(x - t_i)$ im Korollar bezeichnet man als *Linearfaktoren* von $f(x)$. Tritt einer der der Linearfaktoren $(x - t_i)$ mehrfach auf, so sprechen wir von einer *mehrfachen Nullstelle* von f. Wir sagen, dass f *in Linearfaktoren zerfällt*, wenn $g(x)$ ein konstantes Polynom ist, oder äquivalent, wenn f als Produkt von Polynomen vom Grad 1 geschrieben werden kann.

Korollar 1.3.9. *Es sei K ein Körper, in dem jedes nichtkonstante Polynom eine Nullstelle hat. Dann zerfällt jedes Polynom über K in Linearfaktoren.* □

Definition 1.3.10. *Ein Körper K heißt* algebraisch abgeschlossen*, wenn jedes nichtkonstante $f(x) \in K[x]$ eine Nullstelle in K besitzt.*

1.4. **Die komplexen Zahlen.**

Definition 1.4.1. *Wir definieren die Menge der* komplexen Zahlen *als $\mathbb{C} := \mathbb{R}^2$ mit der gewöhnlichen Addition und der Multiplikation*

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} := \begin{pmatrix} x_0 x_1 - y_0 y_1 \\ x_0 y_1 + x_1 y_0 \end{pmatrix}.$$

Satz 1.4.2. *$\mathbb{C}$ ist ein Körper.*

Beweis. Dies rechnet man ohne Schwierigkeiten nach. Das Einselement ist

$$1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

und wenn

$$z := \begin{pmatrix} x \\ y \end{pmatrix} \neq 0,$$

so ist

$$\frac{1}{z} = \begin{pmatrix} \frac{x}{x^2+y^2} \\ \frac{-y}{x^2+y^2} \end{pmatrix}.$$

□

Der Unterkörper

$$\{ \begin{pmatrix} x \\ 0 \end{pmatrix} | x \in \mathbb{R} \} \subset \mathbb{C}$$

ist isomorph zu $\mathbb{R}$, und wir fassen $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auf, auch wenn das nicht hundertprozentig korrekt ist.

Es gibt eine bessere Notation. Wir bezeichnen

$$i := \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

so dass sich jedes $z \in \mathbb{C}$ eindeutig als

$$z = x + iy$$

mit $x, y \in \mathbb{R}$ schreiben lässt. Die Multiplikation wird dann

$$(x_0 + iy_0)(x_1 + iy_1) = (x_0x_1 - y_0y_1) + i(x_0y_1 + x_1y_0).$$

Insbesondere ist

$$i^2 = -1,$$

und das Inverse ist durch

$$\frac{1}{x+iy} = \frac{x-iy}{x^2+y^2}$$

gegeben.

Definition 1.4.3. *Es sei $z = x + iy$, $x, y \in \mathbb{R}$, eine komplexe Zahl. Die* komplex konjugierte *Zahl ist*

$$\overline{z} := x - iy,$$

der Realteil *von z ist*

$$\Re(z) := x,$$

und der Imaginärteil *von z ist*

$$\Im(z) := y.$$

Wieder ohne irgendeine Idee rechnet man folgende Formeln nach.

Satz 1.4.4. *Für $z, z_0, z_1 \in \mathbb{C}$ gilt*

(1) $z = \Re(z) + i\Im(z)$,
(2) $\overline{z} = \Re(z) - i\Im(z)$,
(3) $\Re(z) = \frac{1}{2}(z + \overline{z})$,
(4) $\Im(z) = \frac{1}{2i}(z - \overline{z})$,
(5) $z \in \mathbb{R} \Leftrightarrow \Im(z) = 0 \Leftrightarrow z = \overline{z}$,
(6) $\overline{z_0 + z_1} = \overline{z_0} + \overline{z_1}$,

(7) $\overline{z_0 z_1} = \overline{z_0}\overline{z_1}$,
(8) $\Re(z_0 + z_1) = \Re(z_0) + \Re(z_1)$,
(9) $\Im(z_0 + z_1) = \Im(z_0) + \Im(z_1)$.

Lemma/Definition 1.4.5. *Es sei $z \in \mathbb{C}$. Dann gilt $z\overline{z} \in \mathbb{R}$, $z\overline{z} \geq 0$ und $z\overline{z} = 0$ genau dann, wenn $z = 0$. Wir definieren den* Absolutbetrag *von z als*

$$|z| := \sqrt{z\overline{z}} \in [0, \infty).$$

Beweis. Dies folgt sofort aus der Formel

$$(x + iy)(x - iy) = x^2 + y^2.$$

□

Lemma 1.4.6. *Es gilt, für $z_0, z_1, z \in \mathbb{C}$:*

(1) $|z_0 z_1| = |z_0||z_1|$,
(2) $|\overline{z}| = |z|$,
(3) $|z_0 + z_1| \leq |z_0| + |z_1|$,
(4) $|z| = 0$ *genau dann wenn* $z = 0$.

Beweis. Nichttrivial ist nur Aussage (3), also die Dreiecksungleichung. Zunächst gilt für jede komplexe Zahl z die Ungleichung

$$\Re(z)^2 \leq \Re(z)^2 + \Im(z)^2 = |z|^2,$$

welche

$$\Re(z) \leq |z|$$

nach sich zieht. Hieraus folgere

$$|z_0 + z_1|^2 = |z_0|^2 + |z_1|^2 + (z_0\overline{z_1} + \overline{z_0}z_1) = |z_0|^2 + |z_1|^2 + 2\Re(z_0\overline{z_1}) \leq$$
$$\leq |z_0|^2 + |z_1|^2 + 2|z_0\overline{z_1}| = |z_0|^2 + |z_1|^2 + 2|z_0||z_1| = (|z_0| + |z_1|)^2$$

und ziehe die Wurzel. □

Der Grund, weshalb die komplexen Zahlen im Zusammenhang dieser Vorlesung relevant sind, liegt in folgendem berühmten Satz.

Theorem 1.4.7 (Fundamentalsatz der Algebra)**.** *Jedes nichtkonstante Polynom $f(x) \in \mathbb{C}[x]$ besitzt eine Nullstelle in $\mathbb{C}$.*

Es gibt viele verschiedene Beweise mit unterschiedlichen Methoden; der historisch erste geht auf Gauß (1799) zurück. Ein besonders kurzer Beweis kann mit den Methoden der Funktionentheorie gegeben werden, siehe [**?**], S. 23, und es gibt einen mehr algebraischen Beweis im Buch von Bosch [**?**], §6.3, der jedoch erst gegen Ende des Semesters verständlich würde. Allen Beweise ist gemeinsam, dass Begriffsbildungen aus der Analysis verwendet werden. Wir präsentieren einen Beweis, der auf Argand (1814) zurückgeht und in [**?**], §7.6 zu finden ist. Es gibt zwei große Schritte. Wir zeigen erst

Satz 1.4.8. *Sei $n \in \mathbb{N}$ und $z \in \mathbb{C} \setminus \{0\}$. Dann hat z genau n verschiedene n-te Wurzeln in $\mathbb{C}$.*

Im zweiten Schritt folgern wir Theorem 1.4.7 aus Satz 1.4.8. In beiden Schritten benötigen wir Analysis.

Im folgenden werden einige Begründungen aus der Analysis weglassen; es handelt sich um nichts anderes, als Begriffe wie Konvergenz und Stetigkeit aus $\mathbb{R}$ auf $\mathbb{C}$ zu übertragen.

Lemma/Definition 1.4.9 (Komplexe Exponentialfunktion)**.** *Für jedes $z \in \mathbb{C}$ konvergiert die Reihe*

$$\sum_{k=0}^{\infty} \frac{1}{k!} z^k$$

absolut gegen einen Grenzwert, den wir mit $e^z = \exp(z) \in \mathbb{C}$ bezeichnen wollen. Die Funktion $\exp : \mathbb{C} \to \mathbb{C}$ ist stetig.

Für reelle Argumente $x \in \mathbb{R}$ ist $\exp(x) = e^x$ die aus der Analysis I bekannte Exponentialfunktion. Ist $t \in \mathbb{R}$, so ist

$$\exp(it) = \sum_{k=0}^{\infty} \frac{1}{k!} i^k t^k = \sum_{n=0}^{\infty} \frac{1}{(2n)!} (i^2)^n t^{2n} + \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} i (i^2)^n t^{2n+1} =$$
$$= \sum_{n=0}^{\infty} \frac{1}{(2n)!} (-1)^n t^{2n} + i \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} (-1)^n t^{2n+1} = \cos(t) + i \sin(t),$$

wie man mit den bekannten Potenzreihendarstellungen der Sinus- und Cosinusfunktion einsieht. Also gilt die *Moivre-Formel*

$$\exp(it) = \cos(t) + i \sin(t). \tag{1.4.10}$$

Satz 1.4.11. *Es gilt*

(1) $\exp(0) = 1$,
(2) $\exp(z + w) = \exp(z) \exp(w)$,
(3) $\exp(z) \neq 0$ *und* $\exp(z)^{-1} = \exp(-z)$ *für alle* $z \in \mathbb{C}$,
(4) $\overline{\exp(z)} = \exp(\overline{z})$ *für alle* $z \in \mathbb{C}$,
(5) $|\exp(z)| = e^{\Re(z)}$ *für alle* $z \in \mathbb{C}$,

Beweis. (1) ist klar. Für (2) nehme man Reihenmultiplikation:

$$\exp(z) \exp(w) = \sum_{k=0}^{\infty} \frac{1}{k!} z^k \sum_{l=0}^{\infty} \frac{1}{l!} w^l \overset{!}{=} \sum_{n=0}^{\infty} \Big(\sum_{m=0}^{n} \frac{1}{m!} \frac{1}{(n-m)!} z^m w^{n-m} \Big) \overset{!!}{=}$$
$$\sum_{n=0}^{\infty} \frac{1}{n!} \Big(\sum_{m=0}^{n} \binom{n}{m} z^m w^{n-m} \Big) \overset{!!!}{=} \sum_{n=0}^{\infty} \frac{1}{n!} (z+w)^n = \exp(z+w).$$

Die mit ! gekennzeichnete Gleichheit ist der Doppelreihensatz (und diese Umformung ist erlaubt, weil beide Reihen absolut konvergieren), !! folgt aus der Definition der Binomialkoeffizienten

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

und !!! folgt aus dem binomischen Lehrsatz. Aussage (3) folgt sofort aus (1) und (2), und (4) ist fast trivial (warum nur fast?). Für (5) rechne

$$|\exp(z)|^2 = \exp(z)\overline{\exp(z)} = \exp(z) \exp(\overline{z}) = \exp(z + \overline{z}) = \exp(2\Re(z)) = \exp(\Re(z))^2$$

und ziehe die reelle Wurzel. □

Wir sehen, dass

$$\exp : \mathbb{C} \to \mathbb{C}^\times$$

ein Gruppenhomomorphismus ist. Wir wollen zeigen, dass exp surjektiv ist und wollen den Kern bestimmen. Dafür ist ein kleiner Input aus Analysis I über die trigonometrischen Funktionen erforderlich. Zunächst folgt für $t \in \mathbb{R}$, dass

$$\sin(t)^2 + \cos(t)^2 = |\cos(t) + i \sin(t)|^2 = |\exp(it)|^2 = 1. \tag{1.4.12}$$

Lemma/Definition 1.4.13. *Es gibt eine kleinste positive Nullstelle x_0 von* cos*. Die* Kreiszahl π *ist definiert als* $2x_0$*. Auf dem Intervall* $[0, \frac{\pi}{2}]$ *ist* sin *streng monoton wachsend, und* cos *streng monoton fallend, und es gilt* $\sin(\frac{\pi}{2}) = 1$*.*

Beweis. Der Beweis kann in [**?**, S. 160] nachgelesen werden. □

Wir folgern

$$\exp(\frac{\pi}{2}i) = i$$

sowie

$$\exp(i\pi) = -1,\ \exp(2\pi i) = 1.$$

Lemma 1.4.14. *Ist $z \in \mathbb{C}$, $|z| = 1$, so gibt es eine eindeutige Zahl $t \in [0, 2\pi)$ mit* $\exp(it) = z$*.*

Beweis. Schreibe $z = x + iy$, $x, y \in \mathbb{R}$. Wenn $x > 0, y \geq 0$, so ergibt sich aus der Monotonie von sin und cos auf dem Intervall $[0, \frac{\pi}{2})$ sowie aus (1.4.12), dass genau ein $t \in [0, \frac{\pi}{2}]$ existiert mit $\exp(it) = z$.

Jedes andere z mit $|z|$ lässt sich eindeutig in der Form $z = wi^k$ schreiben, wobei $i \in \{1, 2, 3\}$ und $w = x + iy$ mit $x > 0$ und $y \geq 0$ schreiben. Weil $\exp(i\frac{\pi}{2}) = i$, ist z dann von der Form $z = \exp(it + ik\frac{\pi}{2})$, mit $t \in [0, \frac{\pi}{2}]$ und $k \in \{1, 2, 3\}$, wie behauptet. □

Satz 1.4.15. *Die Funktion* $\exp : \mathbb{C} \to \mathbb{C}^\times$ *ist ein surjektiver Gruppenhomomorphismus, und der Kern ist*

$$\ker(\exp) = 2\pi i\mathbb{Z} = \{2\pi ik | k \in \mathbb{Z}\} \subset \mathbb{C}.$$

Beweis. Wir haben schon gesehen, dass exp ein Gruppenhomomorphismus ist. Für die Surjektivität sei $z \in \mathbb{C}^\times$ gegeben, welches wir in der Form

$$z = |z|w$$

schreiben, mit $|w| = 1$. Nach Lemma 1.4.14 gibt es $t \in \mathbb{R}$ mit $\exp(it) = w$. Die reelle Exponentialfunktion $\exp : \mathbb{R} \to (0, \infty)$ ist bijektiv, wie aus Analysis I bekannt; und die Umkehrfunktion ist der natürliche Logarithmus $\log : (0, \infty) \to \mathbb{R}$. Es gilt daher

$$\exp(it + \log(|z|)) = \exp(it)|z| = z.$$

Für $k \in \mathbb{Z}$ gilt offenbar $\exp(2\pi ik) = \exp(2\pi i)^k = 1^k = 1$, also $2\pi i\mathbb{Z} \subset \ker(\exp)$. Sei nun $\exp(z) = 1$. Es gilt

$$e^{\Re(z)} = |e^z| = 1,$$

und weil $\Re(z)$ reell ist, folgt $\Re(z) = 0$, also $z = it$ für ein $t \in \mathbb{R}$. Es gibt ein eindeutiges $k \in \mathbb{Z}$ mit $2\pi k \leq t < 2\pi(k + 1)$, und weiterhin ist

$$1 = \exp(it) = \exp(2\pi ik + i(t - 2\pi k)) = \exp(2\pi ik)\exp(i(t - 2\pi k)) = \exp(i(t - 2\pi k)),$$

und aus Lemma 1.4.14 folgt $t - 2\pi k = 0$, also $t = 2\pi k$, also $z = 2\pi ik$, also $z \in 2\pi\mathbb{Z}$. □

Beweis von Satz 1.4.8. Sei $z \in \mathbb{C}$, $z \neq 0$. Es gibt nun ein $y \in \mathbb{C}$ mit $\exp(y) = z$ und wir setzen

$$w = \exp(\frac{1}{n}y).$$

Dies erfüllt $w^n = z$. Wir wollen noch zeigen, dass z genau n verschiedene Wurzeln in $\mathbb{C}$ hat, und betrachten zunächst den Fall $z = 1$. Setze

$$\zeta_n := e^{\frac{2\pi i}{n}}.$$

Es gilt dann $\zeta_n^n = 1$, und ferner

$$(\zeta_n^k)^n = 1^k = 1$$

wenn $k \in \mathbb{Z}$. Wir behaupten, dass $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ paarweise verschieden sind. Nun, wenn $\zeta_n^k = \zeta_n^m$, $0 \leq k \leq m \leq n-1$, dann gilt

$$e^{\frac{2\pi i(m-k)}{n}} = 1,$$

und weil $0 \leq \frac{2\pi(m-k)}{n} < 2\pi$, muss $m - k = 0$ sein. Ist $w \neq 0$ eine $n$te Wurzel von $z \in \mathbb{C}$, so sind

$$w, \zeta_n w, \zeta_n^2 w, \ldots, \zeta_n^{n-1} w$$

n paarweise verschiedene $n$te Wurzeln. Wegen Satz 1.3.6 kann das Polynom $x^n - z$ nicht mehr als n Nullstellen in $\mathbb{C}$ haben, und somit ist der Beweis fertig. □

Nun erbringen wir den zweiten Teil des Beweises des Fundamentalsatzes der Algebra.

Lemma 1.4.16 (Wachstumslemma)**.** *Es sei $f(x) \in \mathbb{C}[x]$ ein Polynom vom Grad n. Dann gibt es $C > 0$ und $R \geq 0$, so dass für alle $z \in \mathbb{C}$ mit $|z| \geq R$ gilt*

$$|f(z)| \geq C|z|^n.$$

Beweis. Schreibe $f(x) = a_n x^n + \ldots + a_0$, $a_n \neq 0$. Setze

$$C := \frac{1}{2}|a_n|;\ R := \max\{1, \frac{2n}{|a_n|} \max_{0 \leq k \leq n-1}\{|a_k|\}\}.$$

Es gilt dann

$$|f(z)| \geq |a_n||z|^n - \sum_{k=0}^{n-1} |a_k||z|^k \geq |a_n||z|^n - \max_{0 \leq k \leq n-1}\{|a_k|\} \sum_{k=0}^{n-1} |z|^k \overset{|z|\geq 1}{\geq}$$
$$2C|z|^n - \max_{0 \leq k \leq n-1}\{|a_k|\} n|z|^{n-1}.$$

Wenn $|z| \geq \frac{2n}{|a_n|} \max_{0 \leq k \leq n-1}\{|a_k|\}$, ist

$$\max_{0 \leq k \leq n-1}\{|a_k|\} n|z|^{n-1} \leq \frac{|a_n|}{2}|z|^n = C|z|^n,$$

und insgesamt also

$$|f(z)| \geq C|z|^n.$$ □

Lemma 1.4.17. *Eine Polynomfunktion $f : \mathbb{C} \to \mathbb{C}$ nimmt ihr Betragsminimum auf $\mathbb{C}$ an. Mit anderen Worten: es gibt $z_0 \in \mathbb{C}$ mit $|f(z_0)| \leq |f(z)|$ für alle $z \in \mathbb{C}$.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $\deg(f) \geq 1$, denn für konstante Polynome ist die Aussage trivial. Wir wählen eine Folge $z_k \in \mathbb{C}$, so dass

$$\lim_{m \to \infty} |f(z_m)| = \inf_{z \in \mathbb{C}} |f(z)|$$

gilt. Eine solche Folge gibt es nach der Konstruktion des Infimums einer Menge von reellen Zahlen! Aus Lemma 1.4.16 folgt, dass die Folge z_m beschränkt ist, denn $|z_m| \to \infty$ impliziert $|f(z_m)| \to \infty$. Mit anderen Worten, die Folgenglieder dürfen nicht nach ∞ entwischen, da sonst die Folge $|f(z_m)|$ nicht konvergieren kann.

Nach dem Satz von Bolzano und Weierstrass gibt es eine konvergente Teilfolge z_{k_l} von z_k. Der Grenzwert einer solchen Teilfolge ist das gewünschte z_0, wie man mit Hilfe der Stetigkeit von f nachweist. □

Beweis des Fundamentalsatzes der Algebra. Es sei nun $f(x)$ ein nichtkonstantes Polynom vom Grad $n \geq 1$. Nach Lemma 1.4.17 gibt es $z_0 \in \mathbb{C}$, so dass $|f(z_0)| \leq |f(z)|$ für alle z. Wir zeigen nun, dass $f(z_0) = 0$ ist, und erreichen dies durch einen Widerspruchsbeweis. Annahme: $f(z_0) \neq 0$.

Indem wir statt f das Polynom $g(x) = f(x + z_0)$ betrachten, dürfen wir $z_0 = 0$ annehmen, und indem wir $g(z)$ durch $h(z) = \frac{1}{g(0)} g(z)$ betrachten, darf des weiteren $h(0) = 1$ angenommen werden. Weil $n \geq 1$, ist h nicht konstant, und wir finden $k \geq 1$, so dass

$$h(x) = 1 + a_k x^k + a_{k+1} x^{k+1} + \ldots + a_n x^n = 1 + a_k x^k + x^{k+1} q(x)$$

gilt, für ein Polynom $q(x)$. Nach Satz 1.4.8 gibt es $w \in \mathbb{C}^\times$ mit

$$w^k = -\frac{1}{a_k},$$

und wir betrachten die Hilfsfunktion

$$\varphi : \mathbb{R} \to \mathbb{C},\ \varphi(t) := h(tw) = 1 - t^k + t^{k+1} w^{k+1} q(tw).$$

Das einzige, was wir über q wissen müssen, ist, dass q stetig ist. Dies zieht nach sich, dass $c \geq 0$ existiert, so dass

$$|w^{k+1} q(tw)| \leq c$$

wenn $t \in [0, 1]$. Nach Annahme gilt $|h(z)| \geq 1$ für alle $z \in \mathbb{C}$ und daher auch $|\varphi(t)| \geq 1$ für alle t. Ist nun aber $t \in [0, 1]$ und $0 < t < \frac{1}{c}$, so sehen wir

$$1 \leq |\varphi(t)| \leq 1 - t^k + t^{k+1} |w^{k+1} q(tw)| \leq 1 - t^k + t^{k+1} c = 1 - t^k + t^k tc < 1 - t^k < 1.$$

Das ist ein Widerspruch! □

Die n verschiedenen Wurzeln von 1 heißen *nte Einheitswurzeln* und spielen eine wichtige Rolle in der Algebra. Dies sind die Zahlen

$$e^{\frac{2\pi i}{n} k},\ k = 0, \ldots, n-1.$$

Für manche Werte von n gibt es spezielle Ausdrücke für $\zeta_n := e^{\frac{2\pi i}{n}}$.

(1) $n = 2$: $e^{\frac{2\pi i}{2}} = e^{\pi i} = -1$,
(2) $n = 3$: $e^{\frac{2\pi i}{3}} = \frac{1}{2}(1 + i\sqrt{3})$,
(3) $n = 4$: $e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = i$,
(4) $n = 5$: $e^{\frac{2\pi i}{5}} = \frac{1}{4}(-1 + \sqrt{5}) + i\sqrt{\frac{1}{8}(5 + \sqrt{5})}$,
(5) $n = 6$: $e^{\frac{2\pi i}{6}} = \frac{1}{2}(-1 + i\sqrt{3})$,
(6) $n = 8$: $e^{\frac{2\pi i}{8}} = \frac{1}{\sqrt{2}}(1 + i)$.

Die Beweise dieser Formeln sind Übungsaufgaben.

2. Teilbarkeitstheorie in Ringen

2.1. **Definitionen.** Im folgenden sei R stets ein *kommutativer Ring mit* 1.

Definition 2.1.1. (1) *Ein $x \in R$ heißt* Einheit*, falls $y \in R$ mit $xy = 1$ existiert. Die Menge aller Einheiten in R wird mit $R^\times$ bezeichnet (und ist im übrigen eine abelsche Gruppe mit der Multiplikation).*

(2) *R heißt* nullteilerfrei *oder* Integritätsring*, falls gilt: es ist $0 \neq 1$ in R und*

$$x, y \in R, xy = 0 \Rightarrow x = 0 \text{ oder } y = 0.$$

Bemerkung 2.1.2. *In einem nullteilerfreien Ring R gilt folgende* Kürzungsregel*:*

- *$x, y \in R$, $z \in R$, $z \neq 0$. Dann $xz = yz \Rightarrow x = y$.*

Denn $xz = yz$ impliziert $0 = z(x - y)$.

Beispiele 2.1.3. (1) *Körper sind stets nullteilerfrei, und es gilt $K^\times = K \setminus \{0\}$.*

(2) *$\mathbb{Z}$ ist nullteilerfrei, und $\mathbb{Z}^\times = \{\pm 1\}$.*

(3) *Der Polynomring $K[x]$ über einem Körper ist nullteilerfrei. Die Einheiten sind genau die konstanten, von Null verschiedenen Polynome. Beide Behauptungen folgen aus der Beobachtung, dass wenn $f(x) = a_n x^n + \ldots + a_0$ und $g(x) = b_m x^m + \ldots + b_0$, dann*

$$f(x)g(x) = a_n b_m x^{m+n} + p(x)$$

mit $\deg(p(x)) < m + n$. Sind also $a_n, b_m \neq 0$, so auch $a_n b_m$. Es ergibt sich, dass wenn $f(x)g(x) = 1$, notwendigerweise $\deg(f) = \deg(g) = 0$ gelten muss.

Definition 2.1.4. (1) *$x, y \in R$. Wir sagen, dass x y teilt, oder $x|y$, falls $z \in R$ existiert mit $xz = y$.*

(2) *$x, y \in R$ heißen* assoziiert*, falls eine Einheit $z \in R^\times$ existiert mit $x = zy$.*

(3) *Ein* gemeinsamer Teiler *von x und y ist ein Element $d \in R$ mit $d|x$ und $d|y$.*

(4) *Ein* größter gemeinsamer Teiler *von x und y ist ein gemeinsamer Teiler d von x und y, so dass für jeden anderen gemeinsamen Teiler e von x und y gilt: $e|d$. Wir schreiben auch $d = \mathrm{ggT}(x, y)$.*

(5) *x und y heißen* teilerfremd*, wenn jeder gemeinsame Teiler von x und y eine Einheit ist.*

(6) *Ein Element $x \in R$ heißt* irreduzibel*, wenn $x \neq 0$, x keine Einheit ist und wenn aus $x = yz$ folgt, dass y oder z eine Einheit ist.*

(7) *Ein Element x heißt* prim*, wenn $x \neq 0$, x keine Einheit ist und wenn gilt: $x|yz \Rightarrow x|y$ oder $x|z$.*

Bemerkung 2.1.5. (1) *Die Teilbarkeitsrelation hat folgende offentsichtiliche Eigenschaften:*

$$u \in R^\times, r \in R \Rightarrow u|r,$$

$$r \in R \Rightarrow r|0,$$

$$r|s,\ s|t \Rightarrow r|t,$$

$$r|s, r|t \Rightarrow r|t + s.$$

(2) *$m, n \in \mathbb{Z}$ sind assoziiert genau dann, wenn $|n| = |m|$. Insbesondere ist jedes $n \in \mathbb{Z}$ assoziiert zu genau einer nichtnegativen Zahl, nämlich $|n|$.*

(3) *Jedes Polynom* $f(x) = a_n x^n + \ldots + a_0$ *ist assoziiert zu genau einem normierten Polynom, nämlich* $\tilde{f}(x) = \frac{1}{a_n} f(x)$.
(4) *Ist* d *ein größter gemeinsamer Teiler von* x *und* y *und* $u \in R^\times$*, so ist auch* ud *ein größter gemeinsamer Teiler von* x *und* y*. Sind umgekehrt* d, d' *größte gemeinsame Teiler von* x *und* y*, so sind* d *und* d' *assoziiert. Es ist also der größte gemeinsame Teiler von* x *und* y *nicht eindeutig bestimmt. In den für uns interessanten Fällen* $R = \mathbb{Z}$ *und* $R = K[x]$ *treffen wir folgende Vereinbarung: für* $m, n \in \mathbb{Z}$ *bezeichne* $\mathrm{ggT}(m, n)$ *den eindeutigen positiven größten gemeinsamen Teiler von* x *und* y*. Für* $f, g \in K[x]$ *bezeichne* $\mathrm{ggT}(f, g)$ *den eindeutig bestimmten normierten größten gemeinsamen Teiler von* f *und* g*.*
(5) *Die irreduziblen Elemente in* $\mathbb{Z}$ *sind genau die Primzahlen.*
(6) *Die Beziehung zwischen Primelementen und irreduziblen Elementen wird später geklärt. Es stellt sich heraus, dass in den Ringen* $\mathbb{Z}$ *und* $K[x]$ *beide Begriffe zusammenfallen.*

Um uns mit den Begriffen vertraut zu machen, betrachten wir den Polynomring $K[x]$.

Lemma 2.1.6. *Es sei* K *ein Körper. Dann ist jedes Polynom* $f(x) \in K[x]$ *mit* $\deg(f(x)) = 1$ *irreduzibel. Sei umgekehrt* $f(x) \in K[x]$ *irreduzibel und normiert. Dann gilt entweder*

(1) $\deg(f(x)) = 1$*, d.h.* $f(x) = x - a$*,* $a \in K$*.*
(2) $\deg(f(x)) \geq 2$ *und* $f(x)$ *besitzt keine Nullstelle in* K*.*

Beweis. Ist $\deg(f(x)) = 1$ und $f(x) = g(x)h(x)$, so gilt wegen $\deg(f) = \deg(g) + \deg(h)$ entweder $\deg(h) = 0$ oder $\deg(g) = 0$, d.h. g oder h ist eine Einheit. Also ist jedes Polynom vom Grad 1 irreduzibel. Sei nun $\deg(f) \geq 2$. Wenn f eine Nullstelle hat, so können wir $f(x) = (x-a)g(x)$ schreiben, mit $\deg(g) = \deg(f) - 1 \geq 1$. Also sind $(x - a)$ und $g(x)$ beides keine Einheiten, und f ist nicht irreduzibel. □

Die Umkehrung ("ein Polynom ohne Nullstelle ist irreduzibel") ist nicht richtig, wie man an

$$f(x) = (x^2 + 1)(x^2 + 2) \in \mathbb{R}[x]$$

ablesen kann. Immerhin gilt aber

Lemma 2.1.7. *Es sei* $f(x) \in K[x]$ *mit* $2 \leq \deg(f(x)) \leq 3$*, und* $f(x)$ *habe keine Nullstelle in* K*. Dann ist* $f(x)$ *irreduzibel.*

Beweis. Es sei $\deg(f) = 2$ oder 3 und f sei nicht irreduzibel. Dann schreibe $f(x) = g(x)h(x)$, wobei g und h beide keine Einheit seien. Es folgt $\deg(g) \geq 1$ und $\deg(h) \geq 1$, also

$$2 \leq \deg(g) + \deg(h) = \deg(gh) = \deg(f) \leq 3.$$

Das geht nur dann, wenn $\deg(g) = 1$ oder $\deg(h) = 1$. Also ist einer der beiden Faktoren linear, und lineare Polynome haben Nullstellen. Somit hat auch f eine Nullstelle. □

Lemma 2.1.8. *Jedes lineare Polynom ist irreduzibel.*

Der Beweis ist eine Übung.

Satz 2.1.9. *Ein Körper* K *ist algebraisch abgeschlossen genau dann, wenn jedes irreduzible Polynom den Grad* 1 *hat.*

Der Beweis ist eine Übung.

Satz 2.1.10. *Ein normiertes Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{R}[x]$ ist irreduzibel genau dann, wenn eine der folgenden Alternativen gilt:*

(1) $n = 1$ *oder*
(2) $n = 2$ *und* $\frac{a_1^2}{4} - a_0 < 0$.

Der Beweis ist eine Übung.

Lemma 2.1.11. *Es sei R ein nulteilerfreier kommutativer Ring und $x \in R$ prim. Dann ist x irreduzibel.*

Beweis. Es ist zu zeigen: $x = yz$ impliziert, dass y oder z eine Einheit ist. Jedenfalls folgt aus $x = yz$, dass $x|yz$, und weil x prim ist, teilt x eins der beiden Elemente y und z, sagen wir $x|z$. Mit anderen Worten: es gibt $u \in R$ mit $z = ux$. Es folgt

$$x = yz = yux$$

also

$$(1 - yu)x = 0.$$

Weil R nullteilerfrei und $x \neq 0$ nach Annahme, muss $1 - yu = 0$ gelten, also $uy = 1$, womit y als Einheit erkannt ist. □

Die Umkehrung gilt nur unter einer zusätzlichen Voraussetzung.

2.2. **Euklidische Ringe.** Wir wollen nun beweisen, dass in Polynomringen ein Analogon zur bekannten Primfaktorzerlegung in $\mathbb{Z}$ existiert. Auf dem Weg dahin werden wir auch die Primfaktorzerlegung ganzer Zahlen systematisch behandeln, und die Beziehung zwischen Primelementen und irreduziblen Elementen klären.

Definition 2.2.1. *Ein* euklidischer Ring *ist ein nullteilerfreier kommutativer Ring R mit* 1*, so dass eine* Normfunkton $\nu : R \setminus \{0\} \to \mathbb{N}$ *existiert mit folgenden Eigenschaften:*

(1) *Für alle $x, z \in R$ mit $z \neq 0$ gibt es $y, u \in R$ mit $x = yz + u$ und $\nu(u) < \nu(z)$ oder $u = 0$.*
(2) *$\nu(xy) \geq \nu(x)$, wenn $x, y \neq 0$,*
(3) *$\nu(1) = 1$.*

Beispiele 2.2.2. (1) *Der Ring $\mathbb{Z}$ ist euklidisch; man setzt $\nu(x) := |x|$. Das erste Axiom ist erfüllt, weil es Division mit Rest gibt. Genauer, für $x \in \mathbb{Z}$ und $y \in \mathbb{Z}$, $y > 0$, gibt es genau ein $k \in \mathbb{Z}$, so dass $ky \leq x \leq (k+1)y - 1$, und man setzt einfach $y = k$ und $u = x - ky$. Ist $y < 0$, so argumentiert man sehr ähnlich.*
(2) *Der Ring $K[x]$ ist euklidisch. Man setzt $\nu(f(x)) = \deg(f) + 1$ und zitiert Satz 1.3.7.*

Lemma 2.2.3. *Sei R ein euklidischer Ring mit Normfunktion ν. Dann gilt:*

(1) *$x \in R \setminus \{0\}$ ist eine Einheit genau dann, wenn $\nu(x) = 1$.*
(2) *$x, y \neq 0$, dann gilt $\nu(xy) = \nu(x)$ genau dann, wenn y eine Einheit ist.*

Beweis. (1) Sei x eine Einheit und $xy = 1$. Dann folgt $1 = \nu(1) \geq \nu(x) > 0$, also $\nu(x) = 1$. Sei umgekehrt $\nu(x) = 1$. Schreibe $1 = yx + u$ mit $\nu(u) < \nu(x)$ oder $u = 0$. Es kann nur $u = 0$ gelten; also ist x eine Einheit.

(2) Ist y eine Einheit, $yu = 1$, so gilt $\nu(x) = \nu(xyu) \geq \nu(xy) \geq \nu(x)$, und die beiden Ungleichungen sind Gleichungen. Also $\nu(x) = \nu(xy)$. Sei umgekehrt $\nu(xy) = \nu(x)$, und wir behaupten, dass y eine Einheit sein muss. Schreibe $x = z(xy) + u$, mit $\nu(u) < \nu(xy)$ oder $u = 0$. Wir behaupten, dass $u = 0$ gelten muss. Wäre $u \neq 0$, so ist $\nu(u) < \nu(xy) = \nu(x)$, und wegen

$$x(1 - zy) = u$$

folgt $\nu(u) \geq \nu(x) = \nu(xy)$, was nicht sein kann. Folglich ist $u = 0$, und daher $x = xzy$. Weil R nullteilerfrei ist, folgt $zy = 1$, also ist y eine Einheit. □

Wir kommen nun zu dem Schlüsselresultat.

Theorem 2.2.4. *Es sei R ein euklidischer Ring und $x, y \in R$. Dann existiert ein größter gemeinsamer Teiler d von x und y, welcher darüber hinaus eine Darstellung der Form*

$$d = rx + sy$$

mit $r, s \in R$ erlaubt.

Der Beweis erfolgt in zwei Schritten, von denen der erste so wichtig ist, dass er eine neue Begriffsbildung motiviert. Sind $x, y \in R$, so betrachte die Teilmenge

$$I := \{rx + sy | r, s \in R\} \subset R. \tag{2.2.5}$$

Diese Menge erfüllt offensichtlich die Eigenschaften

(1) $0 \in I$,
(2) mit $z_0, z_1 \in I$ ist auch $z_0 + z_1 \in I$,
(3) mit $z \in I$ und $r \in R$ ist auch $rz \in I$.

Wir werden zeigen:

Satz 2.2.6. *Es sei R ein euklidischer Ring und $I \subset R$ eine Teilmenge, welche die beiden obigen Eigenschaften erfüllt. Dann gibt es ein $d \in R$, so dass*

$$I = \{rd | r \in R\}.$$

Beweis von Theorem 2.2.4 aus Satz 2.2.6. Es sei I wie in (2.2.5) definiert, und es sei $d \in R$ mit der in Satz 2.2.6 behaupteten Eigenschaft. Offenbar gilt $y, x \in I$, und nach Satz 2.2.6 können wir

$$x = ad, y = bd,\ a, b \in R,$$

schreiben. Es folgt, dass d ein gemeinsamer Teiler von x und y ist. Andererseits ist $d \in I$ und kann somit nach Definition als $d = rx + sy$ geschrieben werden. Um den Beweis zu beenden, müssen wir uns davon überzeugen, dass jeder gemeinsame Teiler e von x und y ein Teiler von d ist.

Ist aber e ein gemeinsamer Teiler von x und y, so schreiben wir $x = fe$, $y = ge$, und es folgt

$$d = rx + sy = (rf + sg)e;$$

□

Beweis von Satz 2.2.6. Im Fall $I = 0$, den wir nicht ausgeschlossen haben, hat das Element $d = 0$ offensichtlich die gewünschte Eigenschaft. Wenn $I \neq 0$, so wählen wir $d \in I$, $d \neq 0$, so dass $\nu(d) \leq \nu(z)$ für alle $z \in I$, $z \neq 0$, gilt. Ist nun $z \in I$ ein beliebiges Element, so schreibe

$$z = ad + u$$

wobei $u = 0$ oder $\nu(u) < \nu(d)$ gelten muss. Weil $z, d \in I$, ist auch $u \in I$. Nach der Wahl von d ist der Fall $u \neq 0$ unmöglich. Somit muss $u = 0$ sein, also $z = ad$, wie behauptet. □

Wir werden das Argument aus dem Beweis von 2.2.6 später axiomatisieren, kommen aber zunächst zu einigen Konsequenzen. Die Darstellung des größten gemeinsamen Teilers in der Form

$$\mathrm{ggT}(x, y) = rx + sy,$$

welche in jedem euklidischen Ring, also inbesondere sowohl in $\mathbb{Z}$ als auch im Polynomring $K[x]$, existiert, ist sehr wichtig und hat vielerlei Anwendungen. Als erste tragen wir die Charakterisierung irreduzibler Elemente in euklidischen Ringen nach.

Satz 2.2.7 (Lemma von Euklid)**.** *Sei R ein euklidischer Ring und $x \in R$ keine Einheit und $x \neq 0$. Dann ist x prim genau dann, wenn x irreduzibel ist.*

Beweis. Wir haben in Lemma 2.1.11 bereits gezeigt, dass Primelemente irreduzibel sind. Sei nun umgekehrt $x \in R$ irreduzibel, und $x|yz$. Wir müssen zeigen, dass $x|y$ oder $x|z$ gilt. Es sei d ein größter gemeinsamer Teiler von x und y, der in der Form

$$d = rx + sy \tag{2.2.8}$$

geschrieben sei. Weil d ein Teiler von x ist, gibt es $a \in R$ mit

$$x = ad.$$

Es sind jetzt zwei Fälle zu unterscheiden.

(1): d ist keine Einheit. Weil x nach Annahme irreduzibel ist, muss dann a eine Einheit sein, so dass wir $d = a^{-1}x$ schreiben können, woraus $x|d$ folgt. Weil auch $d|y$, gilt dann $x|y$.

(2) d ist eine Einheit. Durch Multiplikation von (2.2.8) mit d^{-1} erhalten wir eine Darstellung der Form

$$1 = r'x + s'y.$$

Weil $x|yz$, gibt es $c \in R$ mit

$$yz = cx.$$

Es folgt

$$z = r'xz + s'yz = r'xz + s'cx = x(r'z + s'c),$$

und also $x|z$. □

Es gibt ein konkretes Verfahren, um den größten gemeinsamen Teiler von x und y zu berechnen.

Satz 2.2.9 (Euklidischer Algorithmus)**.** *Es sei R ein euklidischer Ring mit Normfunktion ν. Seien $x_0, x_1 \in R \setminus \{0\}$. Man schreibe*

$$\begin{aligned} x_0 &= q_0 x_1 + x_2 \\ x_1 &= q_1 x_2 + x_3 \\ x_2 &= q_2 x_3 + x_4 \\ &\cdots\cdots \end{aligned}$$

jeweils mit $\nu(x_j) < \nu(x_{j-1})$. Dann gibt es ein r mit $x_r \neq 0$ und $x_{r+1} = 0$. Es gilt dann

$$x_r = \mathrm{ggT}(x_0, x_1).$$

Beweis. Weil stets $\nu(x_j) < \nu(x_{j-1})$ ist, und weil die Normfunktion Werte in den natürlichen Zahlen annimmt, muss ein r wie im Satz behauptet existieren. Nach Konstruktion gilt dann

$$x_{r-2} = q_{r-1}x_{r-1} + x_r$$

und

$$x_{r-1} = q_r x_r.$$

Die letzte Gleichung besagt, dass $x_r | x_{r-1}$. Zusammen mit der vorletzten folgt $x_r | x_{r-2}$, und so fortfahrend sieht man

$$x_r | x_1,\ x_r | x_0,$$

also ist x_r ein gemeinsamer Teiler von x_0 und x_1. Sei nun d ein gemeinsamer Teiler von x_0 und x_1. Die erste Gleichung impliziert $d|x_2$, zusammen mit der zweiten $d|x_3$. So fortfahrend sieht man

$$d|x_r.$$

Also ist jeder gemeinsame Teiler von x_0 und x_1 ein Teiler von x_r, und zusammen folgt, dass x_r ein größter gemeinsamer Teiler von x_0 und x_1 ist. □

Durch Ineinandersetzen der obigen Gleichungen finden man des weiteren eine Darstellung $\mathrm{ggT}(x_0, x_1) = rx_0 + sx_1$. Wir verzichten darauf, den konkreten Algorithmus hier anzugeben, aber das Verfahren ist sehr effizient.

2.3. **Primfaktorzerlegung in euklidischen Ringen.**

Theorem 2.3.1 (Primfaktorzerlegung in euklidischen Ringen)**.** *Es sei R ein euklidischer Ring und $0 \neq r \in R$.*

(1) *Dann gibt es irreduzible Elemente $x_1, \ldots, x_n \in R$ und eine Einheit $u \in R$, so dass*

$$r = ux_1 \cdots x_n. \tag{2.3.2}$$

(2) *Die obige Darstellung von r als Produkt irreduzibler Faktoren ist eindeutig bis auf Umordnung der Faktoren und Multiplikation mit Einheiten. Genauer: sind $y_1, \ldots, y_m$ irreduzible Elemente mit*

$$r = vy_1 \cdots y_m, \tag{2.3.3}$$

so gilt $m = n$, und es gibt eine Bijektion $\sigma : \underline{n} \to \underline{n}$, so dass x_i und $y_{\sigma(i)}$ assoziiert sind.

Beweis von Theorem 2.3.1 (1). Es sei $\nu : R \setminus \{0\} \to \mathbb{N}$ eine Normfunktion. Wir argumentieren durch Induktion über $\nu(r)$. Der Fall $\nu(r) = 1$ ist klar: in diesem Falle ist r nach Lemma 2.2.3 eine Einheit. Setze $n = 0$, und $u = r$.

Für den Induktionsschritt sei $\nu(r) = k$, und (1) sei für alle $r' \in R \setminus \{0\}$ mit $\nu(r') < k$ schon gezeigt. Falls r irreduzibel ist, ist nichts zu zeigen: setze $u = 1$, $n = 1$ und $x_1 = r$. Wenn r nicht irreduzibel ist, können wir $r = r_1 r_2$ schreiben, wobei r_1 und r_2 beides keine Einheiten sind. Wegen Lemma 2.2.3 gilt $\nu(r_1), \nu(r_2) < \nu(r) = k$. Nach Induktionsannahme könne wir

$$r_1 = ux_1 \cdots x_n$$

und

$$r_2 = u' x_{n+1} \cdots x_{n+m}$$

schreiben, mit Einheiten u, u' und irreduziblen x_i. Insgesamt ist dann

$$r = r_1 r_2 (uu') x_1 \cdots x_{n+m}.$$ □

Für den Beweis von Teil (2) des Satzes benutzen wir Satz 2.2.7 und folgende einfache Feststellung

Lemma 2.3.4. *Es seien $x_1, \ldots, x_n \in R$ Elemente, so dass $x_1 \cdots x_n$ eine Einheit ist. Dann ist jedes x_i eine Einheit.*

Beweis. Nach Annahme können wir $(ux_1 \cdots x_{n-1})x_n = 1$ schreiben, mit einer Einheit u. Es folgt, dass x_n eine Einheit ist, und dass $x_1 \cdots x_{n-1}$ eine Einheit ist. Daraus folgt die Behauptung durch Induktion über n. □

Beweis von Theorem 2.3.1 (2). Wir führen den Beweis durch Induktion über $\nu(r)$. Ist $\nu(r) = 1$, so ist r eine Einheit. Es ist zu zeigen, dass wenn

$$r = vy_1 \cdots y_m$$

für eine Einheit und irreduzible Elemente y_i, dann $m = 0$ gelten muss. Aber aus Lemma 2.3.4 folgt, dass jedes y_i eine Einheit ist, und weil irreduzible Elemente nach Definition keine Einheiten sind, kann nichts anderes als $m = 0$ gelten.

Für den Induktionsschritt sei $\nu(r) = k$, und der Satz sei für jedes Element $r' \in R \setminus \{0\}$ mit $\nu(r') \leq k - 1$ schon geführt. Es gelte die Gleichung

$$r = ux_1 \cdots x_n = vy_1 \cdots y_m,$$

Nun ist x_n irreduzibel und daher nach Satz 2.2.7 auch prim. Es muss also $x_n | v$ oder $x_n | y_1 \cdots y_m$ gelten, und weil x_n die Einheit v nicht teilen kann, muss $x_n | y_1 \cdots y_m$ gelten. Durch Wiederholung dieses Argumentes sieht man ein, dass x_n einen der Faktoren y_i teilen muss. Ohne Beschränkung der Allgemeinheit (nämlich gegebenenfalls durch Umordnung der Faktoren) dürfen wir $x_n | y_m$ annehmen. Weil y_m irreduzible ist, müssen x_n und y_m assoziiert sein, also $y_m = ax_n$ mit $a \in R^\times$. Es folgt dann

$$ux_1 \cdots x_{n-1}x_n = (av)y_1 \cdots y_{m-1}x_n.$$

Weil R nullteilerfrei ist, folgert man

$$r' := ux_1 \cdots x_{n-1} = (av)y_1 \cdots y_{m-1},$$

und es gilt $\nu(r') < \nu(r)$. Wegen der Induktionssannahme folgt daher $n - 1 = m - 1$ und dass nach Umordnen die Faktoren x_i und y_i assoziiert sind, wodurch der Beweis erbracht ist. □

2.4. **Ideale in Ringen.** Wir kommen nun zu der versprochenen Axiomatisierung des Beweises von Satz 2.2.6.

Definition 2.4.1. *Es sei R ein kommutativer Ring. Ein* Ideal *in R ist eine Teilmenge $I \subset R$, so dass gilt*

(1) $0 \in I$,
(2) *mit $x, y \in I$ ist auch $x + y \in I$,*
(3) *mit $x \in I$ und $r \in R$ ist auch $rx \in I$.*

Seien $x_1, \ldots, x_n \in I$. Dann ist das von $x_1, \ldots, x_n$ erzeugte Ideal *das Ideal*

$$(x_1, \ldots, x_n) := \{r_1x_1 + \ldots + r_nx_n | r_i \in R\} \subset R.$$

Das Ideal (x) wird auch das von x erzeugte Hauptideal *genannt. Ein kommutativer Ring mit 1 heißt* Hauptidealring*, wenn jedes Ideal in R ein Hauptideal ist.*

Beispiele 2.4.2. (1) *Sei $R = \mathbb{Z}$ und $d \in \mathbb{Z}$, $d \neq 0$. Dann ist $(d) \subset \mathbb{Z}$ das Ideal der durch d teilbaren ganzen Zahlen.*

(2) *In jedem Ring sind das* Nullideal $(0) \subset R$ *und das* Einsideal $(1) = R$ *Ideale.*
(3) *Ein Körper* K *hat nur die beiden Ideale* (0) *und* K*.*
(4) *Ist* $\varphi : R \to S$ *ein Ringhomomorphismus, so ist der* Kern von φ

$$\ker(\varphi) := \{r \in R | \varphi(r) = 0\}$$

ein Ideal, denn ist $z_0, z_1 \in \ker(\varphi)$*, so folgt* $\varphi(-z_0) = \varphi(z_0 + z_1) = 0$*, und ist* $r \in R$ *beliebig, so gilt darüber hinaus* $\varphi(rz_0) = \varphi(r)\varphi(z_0) = 0$*. Das Bild* $\mathrm{im}(\varphi)$ *hingegen ist üblicherweise kein Ideal.*

Mit diesen Begriffbildungen können wir Satz 2.2.6 auch so formulieren:

Theorem 2.4.3. *Jedes Ideal in einem euklidischen Ring ist ein Hauptideal. Ein euklidischer Ring ist ein Hauptidealring.*

Beweis. Den Beweis haben wir im wesentlichen schon gesehen: sei $I \subset R$ ein Ideal. Falls $I = \{0\}$, so ist $I = (0)$, und es ist nichts mehr zu zeigen. Sei $I \neq \{0\}$. Wähle unter allen von Null verschiedenen Elementen von I ein $d \in I$, dass die Normfunktion minimiert, d.h. $\nu(d) = \min_{x \in I, x \neq 0} \nu(x)$. Wir behaupten, dass $I = (d)$. Sei dafür $x \in I$ und schreibe

$$x = ad + r$$

mit $\nu(r) < \nu(d)$ oder $r = 0$. Es gilt

$$r = x - ad \in I,$$

weil I ein Ideal ist. Somit folgt, wegen der Wahl von d, dass $r = 0$, also $x = ad$, also $x = (d)$. Weil x beliebig war, ist $I \subset (d)$. Die andere Inklusion $(d) \subset I$ ist klar, weil $d \in I$. □

3. Quotientenkonstruktionen

In diesem Abschnitt werden wir zwei wichtige allgemeine Konstruktionen kennenlernen, die einen Ring in einen anderen Ring überführen. Die erste dieser beiden Konstruktionen ist der *Quotientenkörper* eines nullteilerfreien Ringes, welcher eine Abstraktion der Konstruktion der rationalen Zahlen aus den ganzen Zahlen ist.

3.1. **Der Quotientenkörper eines Ringes.** Wir stellen uns für den Moment auf den Standpunkt, dass uns die rationalen Zahlen unbekannt seien, und dass wir nur die ganzen Zahlen kennen. Wie kann man den Körper $\mathbb{Q}$ sauber konstruieren? Bekanntlich sind rationale Zahlen Brüche der Form

$$x = \frac{r}{s},\ r, s \in \mathbb{Z}, s \neq 0.$$

Es liegt nahe, rationale Zahlen als Paare von ganzen Zahlen (r, s) mit $s \neq 0$ zu verstehen. Die Regeln für die Addition und Multiplikation von Brüchen übersetzt sich in die Formeln

$$\frac{r}{s} + \frac{u}{t} = \frac{rt + us}{st} : (r, s) + (u, t) = (tr + us, st)$$

und

$$\frac{r}{s}\frac{u}{t} = \frac{ru}{st} : (r, s)(u, t) = (ru, st).$$

Das Problem bei dieser Sache ist, dass eine rationale Zahl auf viele verschiedene Arten durch Brüche dargestellt werden kann. Z.B. ist

$$\frac{2}{3} = \frac{6}{9} = \frac{4}{6},$$

und es ist nicht sofort klar, dass die Formeln für Addition und Multiplikation nicht von der Art abhängen, wie eine rationale Zahl als Bruch geschrieben wird.

Um mit der Vieldeutigkeit der Darstellung einer rationalen Zahl als Bruch (und analog in vielen ähnlichen Situationen) sauber umgehen zu können, müssen wir an den Begriff einer *Äquivalenzrelation* erinnern. Zunächst notiere:

$$\frac{r}{s} = \frac{u}{t} \Leftrightarrow rt = su, \tag{3.1.1}$$

und beachte, dass der Ausdruck auf der rechten Seite nicht auf die rationalen Zahlen, sondern nur auf $\mathbb{Z}$ Bezug nimmt. Wir wollen also die rationalen Zahlen als Paare $(r, s) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ansehen, wobei wir zwei Paare (r, s) und (u, t) als gleich ansehen, wenn $rt = su$ gilt.

Definition 3.1.2. *Eine* Äquivalenzrelation *auf einer Menge X ist eine Teilmenge $\Gamma \subset X \times X$, welche die folgenden Axiome erfüllt:*

1. $(x, x) \in \Gamma$ *für alle $x \in X$ (Reflexivität),*
2. $(x, y) \in \Gamma \Rightarrow (y, x) \in \Gamma$ *(Symmetrie),*
3. $(x, y) \in \Gamma, (y, z) \in \Gamma \Rightarrow (x, z) \in \Gamma$ *(Transitivität).*

Ist Γ eine Äquivalenzrelation auf X, so schreiben wir

$$x \sim y :\Leftrightarrow (x, y) \in \Gamma.$$

Mit dieser Notation besagen die drei Axiome

1. $x \sim x$ für alle $x \in X$,
2. $x \sim y \Rightarrow y \sim x$,
3. $x \sim y, y \sim z \Rightarrow x \sim z$.

Wir wollen in Zukunft die Äquivalenzrelation einfach durch das Zeichen $\sim$ bezeichnen, und nicht durch die Teilmenge $\{(x,y) \in X \times X | x \sim y\}$.

Lemma 3.1.3. *Auf der Menge $\mathbb{Z} \times (\mathbb{Z} \setminus 0)$ sei folgende Relation erklärt*

$$(r,s) \sim (u,t) :\Leftrightarrow rt = su.$$

Diese Relation ist eine Äquivalenzrelation.

Beweis. Reflexivität: $(r,s) \sim (r,s)$ folgt sofort aus der kommutativität: $rs = sr$. Symmetrie: wenn $(r,s) \sim (u,t)$, dann ist $rt = su$, also $us = tr$, also $(u,t) \sim (r,s)$. Transitivität: sei $(r,s) \sim (u,t)$ und $(u,t) \sim (v,w)$. Dann ist $rt = su$ und $uw = tv$, also auch

$$rtw = suw = stv,$$

das heißt $t(rw - sv) = 0$. Weil $\mathbb{Z}$ nullteilerfrei und $t \neq 0$, folgt hieraus $rw = sv$ und daher $(r,s) \sim (v,w)$, wie behauptet. □

Wie oben angedeutet, soll für ganze Zahlen die Beziehung $(r,s) \sim (u,t)$ als Gleichheit $\frac{r}{s} = \frac{u}{t}$ interpretiert werden. Etwas anders ausgedrückt: sei

$$q : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$$

die Abbildung

$$q(r,s) := \frac{r}{s}.$$

Dann ist q offenbar surjektiv, und es gilt

$$q(r,t) = q(u,s) \Leftrightarrow (r,t) \sim (u,s).$$

Diese Beobachtung basiert natürlich darauf, dass wir die Menge $\mathbb{Q}$ bereits kennen. Hier geht es aber darum, die Menge $\mathbb{Q}$ zu erschaffen. Das geschieht mittels einer ganz allgemeinen Konstruktion, welche wir jetzt diskutieren wollen. Zunächst ein kleines Lemma.

Lemma 3.1.4. *Es sei X eine Menge und $\sim$ eine Äquivalenzrelation auf X. Für $x \in X$ setzen wir*

$$[x] := \{y \in X | x \sim y\} \subset X,$$

die Äquivalenzklasse *von x. Dann gilt: sind $x, y \in X$, so sind die folgenden Aussagen äquivalent:*

(1) $[x] \cap [y] \neq \emptyset$,
(2) $[x] = [y]$,
(3) $x \sim y$.

Beweis. $1 \Rightarrow 3$: ist $[x] \cap [y] \neq \emptyset$, so wähle $z \in [x] \cap [y]$. Nach Definition gilt dann $x \sim z$ und $y \sim z$, also auch $z \sim y$ (Symmetrie) und $x \sim y$ (Transitivität).

$3 \Rightarrow 2$: sei $x \sim y$. Es gilt dann $[x] \subset [y]$: denn ist $z \in [x]$, so ist $x \sim z$, und wegen der Symmetrie und Transitivität auch $y \sim z$, also $z \in [y]$. Das zeigt $[x] \subset [y]$, und die Inklusion $[y] \subset [x]$ folgt mit demselben Argument.

$2 \Rightarrow 1$: wegen der Reflexivität gilt stets $x \in [x]$, und es folgt $[x] \neq \emptyset$. Also, wenn $[x] = [y]$, dann ist $[x] \cap [y] = [x] \neq \emptyset$. □

Korollar 3.1.5. *Es sei $\sim$ eine Äquivalenzrelation auf der Menge X. Dann ist X die disjunkte Vereinigung der Äquivalenzklassen.*

Beweis. Klar. □

Ist nun $Y \subset X$ eine Äquivalenzklasse, so heißt ein Element $x \in Y$ ein *Repräsentant* der Äquivalenzklasse Y. Natürlich gibt es y mit $[y] = Y$, aber jedes andere Element $x \in [y]$ ist auch ein Repräsentant.

Definition 3.1.6. *Sei X eine Menge und es sei $\sim$ eine Äquivalenzrelation. Es sei $X/\sim$ die Menge der Äquivalenzklassen, und es sei $\pi : X \to X/\sim$ die Abbildung, welche durch*

$$\pi(x) := [x]$$

definiert ist.

Die Abbildung π ist surjektiv, und es gilt $x \sim y \Leftrightarrow [x] = [y]$. Ferner ist[1]

$$\pi^{-1}([x]) = [x] \subset X.$$

Definition 3.1.7. *Die rationalen Zahlen sind definiert als*

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim,$$

wobei $\sim$ die in 3.1.3 erklärte Äquivalenzrelation ist.

Natürlich ist das noch kein Körper, weil wir ja dafür zwei Verknüpfungen brauchen. Weil wir

$$\frac{r}{s} + \frac{u}{t} = \frac{rt + us}{st}$$

und

$$\frac{r}{s}\frac{u}{t} = \frac{ru}{st}$$

haben wollen, liegt es nahe, die Addition durch

$$[r, s] + [u, t] := [rt + us, st]$$

und die Multiplikation durch

$$[r, s][u, t] = [ru, st]$$

zu definieren. Das Problem bei dieser Sache ist es, dass man das Element $[r, s] \in \mathbb{Q}$ auf verschiedene Arten als Äquivalenzklasse schreiben kann. Wir müssen also zeigen, dass

$$(r, s) \sim (r', s'), (u, t) \sim (u', t') \Rightarrow (rt + us, st) \sim (r't' + u's', s't')$$

und

$$(r, s) \sim (r', s'), (u, t) \sim (u', t') \Rightarrow (ru, st) \sim (r'u', s't')$$

gilt. Das rechnen wir wie folgt nach:

$$\begin{aligned}(r, s) \sim (r', s'), (u, t) \sim (u', t') \Rightarrow rs' = r's, ut' = u't \Rightarrow \\ (rt + us)s't' - (r't' + u's')st = (rs' - r's)tt' + (ut' - u't)ss' = 0 \Rightarrow \\ (rt + us, st) \sim (r't' + u's', s't')\end{aligned}$$

und

$$\begin{aligned}(r, s) \sim (r', s'), (u, t) \sim (u', t') \Rightarrow rs' = r's, ut' = u't \Rightarrow \\ rus't' = r'su't \Rightarrow (ru, st) \sim (r'u', s't').\end{aligned}$$

Wir sagen, dass die beiden Verknüpfungen auf $\mathbb{Q}$ *wohldefiniert* sind. Natürlich gilt jetzt:

[1]Ist $f : Y \to Z$ eine Abbildung von Mengen und $z \in Z$, so bezeichnet man $f^{-1}(z) := \{y \in Y | f8xy) = z\}$.

Satz 3.1.8. *Die Menge $\mathbb{Q}$, zusammen mit den beiden oben erklärten Verknüpfungen, ist ein Körper. Die Abbildung $\mathbb{Z} \to \mathbb{Q}$, $r \mapsto [r,1]$, ist ein injektiver Ringhomomorphismus.*

Beweis. Es ist eine reine Fleißarbeit, nachzurechnen, dass $\mathbb{Q}$ ein kommutativer Ring mit 1 ist. Das neutrale Element der Addition ist $[0,1]$, und das neutrale Element der Multiplikation ist $[1,1]$. Es ist ebenfalls durch Rechnung einzusehen, dass $r \mapsto [r,1]$ ein Ringhomomorphismus ist, der $1 \in \mathbb{Z}$ auf das Einselement in $\mathbb{Q}$ schickt.

Nicht ganz so einfach ist es, zu sehen, dass j injektiv ist und das $\mathbb{Q}$ ein Körper ist. Zunächst überlege man sich, dass

$$[r,s] = [0,1] \Leftrightarrow r = 0.$$

Hieraus folgt die Injektivität von j, denn ist $j(r) = 0$ für ein $r \in \mathbb{Z}$, so folgt $[r,1] = [0,1]$, also $r = 0$. Außerdem impliziert obige Rechnung, dass $[1,1] \neq [0,1] \in \mathbb{Q}$. Ist nun $[r,s] \neq [0,1]$, so ist $r \neq 0$ und also ist $[s,r] \in \mathbb{Q}$, und offenbar ist

$$[r,s][s,r] = [rs,rs] = [1,1],$$

also ist $[s,r]$ ein multiplikatives Inverses von $[r,s]$. □

Natürlich werden wir in Zukunft die Notation $\frac{r}{s} := [r,s] \in \mathbb{Q}$ benutzen. Eine Analyse der Beweise von Satz 3.1.8 und Lemma 3.1.3 zeigt, dass die einzige Eigenschaft von $\mathbb{Z}$, die benutzt wurde, war, dass $\mathbb{Z}$ ein nullteilerfreier kommutativer Ring mit 1 ist, und wir können in allen Argumenten in diesem Abschnitt das Symbol $\mathbb{Z}$ durch einen solchen Ring R ersetzen. Dies zeigt folgenden Satz.

Satz 3.1.9. *Es sei R ein nullteilerfreier kommutativer Ring mit 1. Die folgende Relation auf der Menge $R \times (R \setminus \{0\})$:*

$$(r,s) \sim (u,t) :\Leftrightarrow rt = su,$$

ist eine Äquivalenzrelation. Wir bezeichnen

$$\mathrm{Quot}(R) := (R \times (R \setminus \{0\}))/\sim .$$

Auf der Menge $\mathrm{Quot}(R)$ erklären wir die beiden Verknüpfungen

$$[r,s] + [u,t] := [rt + us, st]$$

und

$$[r,s][u,t] = [ru, st].$$

Diese sind wohldefiniert, und machen $\mathrm{Quot}(R)$ zu einem Körper, dem Quotientenkörper *von R. Die Abbildung $j : R \to \mathrm{Quot}(R)$, $r \mapsto [r,1]$, ist ein injektiver Ringhomomorphismus.* □

Satz 3.1.10. *Es sei R ein nullteilerfreier kommutativer Ring mit $1 \neq 0$, K ein Körper und $f : R \to K$ ein injektiver Ringhomomorphismus mit $f(1) = 1$. Dann gibt es genau einen Körperhomomorphismus $\tilde{f} : \mathrm{Quot}(R) \to K$ mit $\tilde{f} \circ \iota = f$.*

Beweis. Natürlich setzen wir $\tilde{f}([r,s]) = \frac{f(r)}{f(s)}$, und man rechnet nach, dass dies alle Eigenschaften erfüllt. □

3.2. **Der Restklassenring.**

Definition 3.2.1. *Es sei R ein kommutativer Ring mit Eins und $I \subset R$ ein Ideal. Zwei Elemente $r, r' \in R$ heißen* kongruent modulo I*, in Symbolen*

$$r \equiv r' \pmod{I},$$

falls

$$r - r' \in I.$$

Es ist trivial, nachzurechnen, dass Kongruenz modulo I eine Äquivalenzrelation ist. Ist $I = (d)$ ein Hauptideal, so sagen wir auch, etwas ungenau, dass r und r' "kongruent modulo d" sind und schreiben

$$r \equiv r' \pmod{d}.$$

Die Äquivalenzklasse von r wird als

$$[r] := r + I := \{r' \in R | r \equiv r' \pmod{I}\} \subset R$$

bezeichnet, was dadurch gerechtfertigt ist, dass

$$\{r' \in R | r \equiv r' \pmod{I}\} = \{r + x | x \in I\}$$

gilt. Eine andere Vokabel hierfür ist die *Restklasse* von r modulo I. Wir benutzen beide Notationen, $[r]$ und $r + I$. Die erste hat den Vorteil, kürzer zu sein, und die zweite den Vorteil, dass das Ideal I explizit mitnotiert ist. Wir schreiben

$$R/I := R/\sim$$

und $\pi : R \to R/I$, $\pi(x) := [x]$ für die Quotientenabbildung.

Beispiel 3.2.2. *Sei $R = \mathbb{Z}$, $I = (2)$. Es gilt dann*

$$m \equiv n \pmod{2} \Leftrightarrow 2|(m - n).$$

Mit anderen Worten, zwei ganze Zahlen sind kongruent modulo 2, wenn die Differenz $m - n$ gerade ist. Die Äquivalenzklasse von 0 ist

$$0 + (2) = \{2n | n \in \mathbb{Z}\},$$

also die Menge der geraden Zahlen, und die Äquivalenzklasse von 1 ist

$$1 + (2) = \{2n + 1 | n \in \mathbb{Z}\},$$

also die Menge der ungeraden Zahlen.

Beispiel 3.2.3. *In Verallgemeinerung des vorigen Beispiels betrachten wir $R = \mathbb{Z}$, $I = (d)$ mit $d \geq 1$. Wir behaupten, dass $\mathbb{Z}/(d)$ genau d Elemente hat, nämlich*

$$\{[0], [1], \ldots, [d-1]\}. \tag{3.2.4}$$

Für den Beweis betrachte $k \in \mathbb{Z}$ und schreibe (Division mit Rest)

$$k = qd + r,\ 0 \leq r < d.$$

Dann ist

$$k - r = qd \Rightarrow k \equiv r \pmod{d}$$

und somit $[k] = [r]$. Daraus folgt, dass jedes Element von $\mathbb{Z}/(d)$ eines der in (3.2.4) aufgelisteten Elemente ist. Wir müssen noch zeigen, dass diese paarweise verschieden sind, d.h., falls $0 \leq l \leq k < d$ und $[k] = [l]$, dann gilt $k = l$. Aber $[k] = [l]$ bedeutet nichts anderes als $k \equiv l \pmod{d}$, also $(k - l) = qd$ für ein $q \in \mathbb{Z}$. Weil auch $0 \leq k - l < d$, geht das nur, wenn $q = 0$.

Wir wollen nun auf $R/\sim$ die Struktur eines kommutativen Ringes mit 1 erklären, so dass die Quotientenabbildung $\pi : R \to R/I$, $r \mapsto [r] = r + I$ ein Ringhomomorphismus ist.

Satz 3.2.5. *Es sei R ein kommutativer Ring mit 1 und es sei $I \subset R$ ein Ideal. Dann gibt es eindeutig bestimmte Verknüpfungen $+ : R/I \times R/I \to R/I$ und $\cdot : R/I \times R/I \to R/I$, so dass R/I ein kommutativer Ring mit 1 ist und π ein Ringhomomorphismus. Im Übrigen gilt $\ker(\pi) = I$. Der Ring R/I heißt der* Restklassenring *von R modulo I, und π auch der* Restklassenhomomorphismus*.*

Beweis. Wir beginnen mit der Eindeutigkeit: sind auf R/I Addition und Multiplikation erklärt, so dass π ein Ringhomomorpismus ist, so *muss* gelten:

$$[r] + [s] = \pi(r) + \pi(s) = \pi(r + s) = [r + s]$$

und

$$[rs] = \pi(rs) = \pi(r)\pi(s) = [r][s].$$

Wir befinden uns im Zugzwang: es gibt keine andere Möglichkeit, als

$$[r] + [s] := [r + s] \tag{3.2.6}$$

und

$$[r][s] := [rs] \tag{3.2.7}$$

zu setzen. Die Eindeutigkeit der Verknüpfungen folgt hieraus. Für die *Existenz* muss gezeigt werden, dass die Formeln (3.2.6) und (3.2.7) wohldefinierte Verknüpfungen sind, und dass diese die Axiome für einen kommutativen Ring mit Eins erfüllen. Die Addition (3.2.6) ist wohldefiniert, denn

$$[r] = [r'], [s] = [s'] \Rightarrow r - r', s - s' \in I \Rightarrow (r + s) - (r' + s') \in I \Rightarrow [r + s] = [r' + s'].$$

Die Multiplikation (3.2.7) ist wohldefiniert, denn

$$[r] = [r'], [s] = [s'] \Rightarrow r-r', s-s' \in I \Rightarrow rs-r's' = r(s-s')+(r-r')s' \in I \Rightarrow [rs] = [r's']$$

(hier haben wir die Eigenschaft, dass I ein Ideal ist, ausgenutzt). Die Ringaxiome sind ohne Idee nachzurechnen. Es sei nur festgehalten, dass [0] das neutrale Element der Addition ist und [1] das neutrale Element der Multiplikation. Es ist klar, dass π ein Ringhomomorphismus ist, und $r \in \ker(\pi)$ gilt genau dann, wenn $r \in I$. □

Beispiel 3.2.8. *$R = \mathbb{Z}$, $I = (2)$. In diesem Fall gibt es genau zwei Restklassen, nämlich* [0] *und* [1]*, d.h. die Mengen der geraden und der ungeraden Zahlen. Man kann sich leicht davon überzeugen, dass $\mathbb{Z}/(2)$ isomorph zum Körper $\mathbb{F}_2$ ist.*

Die Konstruktion des Restklassenringes hat eine wichtige formale Eigenschaft.

Satz 3.2.9. *Es sei R ein kommutativer Ring mit 1 und $I \subset R$ ein Ideal. Ferner sei S ein anderer Ring und $\psi : R \to S$ ein Ringhomomorphismus mit $I \subset \ker(\psi)$. Dann existiert ein eindeutig bestimmter Ringhomomorphismus $\psi' : R/I \to S$ mit $\psi' \circ \pi = \psi$.*

Beweis. Wieder ist die Eindeutigkeit leichter und weist den Pfad für den Beweis der Existenz. Ist $r \in R$, so muss

$$\psi'([r]) = \psi(\pi(r)) = \psi(r)$$

gelten, und weil jedes Element von R/I in der Form $[r]$ mit $r \in R$ geschrieben werden kann, ist die Eindeutigkeit erwiesen.

Für die Existenz von ψ' wollen wir natürlich

$$\psi'([r]) := \psi(r)$$

setzen, und müssen zeigen, dass ψ' wohldefiniert ist. Sei also $[r] = [r']$, d.h. $r' = r+x$ mit $x \in I$. Es gilt dann

$$\psi(r') = \psi(r) + \psi(x) = \psi(r),$$

denn $\psi(x) = 0$ weil $I \subset \ker(\psi)$. Somit ist ψ' wohldefiniert. Es ist trivial nachzurechnen, dass ψ' ein Ringhomomorphismus ist. □

Satz 3.2.10. *Es sei R ein euklidischer Ring und $r \in R$ von Null verschieden und keine Einheit. Dann gilt*

1. *Sei $s \in R$. Dann besitzt $[s] \in R/(r)$ genau dann ein multiplikatives Inverses, wenn s und r teilerfremd sind.*
2. *$R/(r)$ ist genau dann ein Körper, wenn r ein irreduzibles Element ist.*

Beweis. Ad (1): wenn s und t teilerfremd sind, so ist 1 ein größter gemeinsamer Teiler von r und s, und es gibt eine Darstellung der Form

$$1 = ar + bs \in R.$$

Es folgt, weil $\pi : R \to R/(r)$ ein Ringhomomorphismus ist,

$$1 = [1] = [a][r] + [b][s] = [b][s],$$

denn es gilt $[r] = 0 \in R/(r)$. Somit besitzt $[s]$ ein multiplikatives Inverses.

Wenn umgekehrt $[s]$ ein multiplikatives Inverses besitzt, so existiert $b \in R$ mit

$$[s][b] = 1 \in R/(r).$$

Das heißt, dass $bs - 1 \in (r)$, also dass $a \in R$ existiert mit $bs - 1 = ar$, also

$$1 = ar + bs.$$

Jeder gemeinsame Teiler e von r und s muss den Ausdruck $ar + bs$ teilen. Also ist jeder gemeinsame Teiler e von r und s eine Einheit, wodurch 1 als größter gemeinsame Teiler von r und s erkannt ist.

Ad (2): Sei r irreduzibel und $s \in R$ mit $0 \neq [s] \in R/(r)$ gegeben. Wir müssen zeigen, dass $[s]$ ein multiplikatives Inverses in $R/(r)$ besitzt. Weil (r) genau aus den durch r teilbaren Elementen besteht, ist r kein Teiler von s. Es folgt, dass 1 ein größter gemeinsamer Teiler von r und s ist. Also sind r und s teilerfremd, und nach (1) hat $[s]$ dann ein multiplikatives Inverses. Somit ist $R/(r)$ ein Körper.

Sei umgekehrt r nicht irreduzibel, keine Einheit und auch nicht 0. Wir können daher $r = st$ schreiben, wobei weder s noch t Einheiten sind. Dann sind weder s noch t durch r teilbar, und daraus folgt

$$[s], [t] \neq 0 \in R/(r).$$

Weil

$$[s][t] = [st] = [r] = 0 \in R/(r),$$

ist $R/(r)$ nicht nullteilerfrei, und daher erst recht kein Körper. □

Beispiel 3.2.11. *Es sei $p \geq 2$ eine Primzahl. Dann ist der Ring $\mathbb{Z}/(p)$ ein Körper, welchen wir mit*

$$\mathbb{F}_p := \mathbb{Z}/(p)$$

bezeichnen wollen.

3.3. **Anwendung: der Satz von Kronecker.** Wir behandeln nun ausführlich ein weiteres wichtiges Beispiel, das für die spätere Entwicklung der Theorie fundamental sein wird. Man betrachte einen Körper K und ein normiertes Polynom

$$f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in K[x]$$

vom Grad $n \geq 2$. Wir nehmen an, dass $f(x)$ *irreduzibel* ist. Dann ist

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

ein Körper.

Lemma 3.3.1. *Jedes Element von $K[x]/(f)$ kann eindeutig in der Form*

$$\sum_{k=0}^{n-1} [b_k x^k]$$

geschrieben werden ($b_k \in K$).

Beweis. Das Lemma besagt, dass jedes Element von $K[x]/(f)$ eindeutig als Restklasse eines Polynoms vom Grad $\leq n-1$ geschrieben werden kann. Eindeutigkeit: sind $h(x), g(x) \in K[x]$ zwei Polynome mit $\deg(g(x)), \deg(h(x)) < n$ und gilt $[g(x) = [h(x)] \in K[x]/(f)$, so gilt $g(x) = h(x)$. Denn $\deg(g(x) - h(x)) < n$ und $g8x) - h(x) \equiv 0 \pmod{f)(x)}$ impliziert offenbar $g(x) = h(x)$.

Existenz: sei $h(x) \in K[x]$ beliebig. Schreibe

$$h(x) = q(x)f(x) + r(x),\ \deg(r(x)) < n,$$

so gilt

$$[h(x)] = [q(x)][f(x)] + [r(x)] = [r(x)] \in K[x]/(f),$$

und wir haben eine Darstellung der Restklasse $[h(x)]$ inder gewünschten Form aufgefunden. □

Die Menge

$$\{[a] \in K[x]/(f) | a \in K\} \subset K[x]/(f)$$

ist ein zu K isomorpher Unterkörper von $K[x]/(f)$, den wir von nun an mit K identifizieren wollen. Wir haben also eine Körpererweiterung

$$K \subset K[x]/(f)$$

konstruiert. Sei nun

$$z := [x] \in K[x]/(f)$$

die Restklasse des Polynoms x. Bemerkung: ist $n = 1$ und $f(x) = x - a$, so ist $z \in K$ und $z = a$. Falls $n \geq 2$, so gehört z nicht zu K, wie man anhand von Lemma 3.3.1 leicht einsieht. Das Körperelement z definiert einen Einsetzungshomomorphismus

$$\phi_z : K[x] \to K[x]/(f);\ h(x) \mapsto h(z).$$

Dieser schickt ein Element $h(x) = \sum_{k=0}^m b_k x^k$ auf

$$h(z) = \sum_{k=0}^m b_k z^k = \sum_{k=0}^m b_k [x]^k = [\sum_{k=0}^m b_k x^k] = [h(x)]. \tag{3.3.2}$$

Hieraus ergibt sich folgende interessante Feststellung:

- Das Element $z = [x] \in K[x]/(f)$ ist eine Nullstelle des Polynoms $f(x)$!

Insgesamt haben wir folgenden Satz bewiesen:

Satz 3.3.3 (Satz von Kronecker)**.** *Es sei K ein Körper und $h(x) \in K[x]$ ein nichtkonstantes Polynom. Dann gibt es einen Erweiterungskörper $K \subset L$, in dem $h(x)$ eine Nullstelle besitzt.*

Beweis. Schreibe

$$g(x) = f(x)h(x)$$

mit $f(x)$ irreduzibel und normiert. Betrachte die Körpererweiterung $L = K[x]/(f)$. □

3.4. **Anwendung: Eisenstein's Irreduzibilitätskriterium.** Für die spätere Behandlung von Beispielen ist es essentiell, Kriterien für die Irreduzibilität eines Polynoms $f(x) \in K[x]$ zur Hand zu haben. Wir konzentrieren uns auf den Fall $K = \mathbb{Q}$. Das Ergebnis soll demonstrieren, wie mächtig die vorher eingeführten abstrakten Begriffsbildungen sind, um konkrete algebraische Probleme zu behandeln.

Definition 3.4.1. *Wir bezeichnen mit $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ die Menge aller ganzzahligen Polynome, also aller $f(x) = \sum_{k=0}^{n} a_k x^k$ mit $a_k \in \mathbb{Z}$. Dies ist ein Unterring von $\mathbb{Q}[x]$.*

Man könnte von vorneherein den Ring $R[x]$ aller Polynome mit Koeffizienten in einem beliebigen Ring definieren, aber das benötigen wir nicht. Es sei angemerkt, dass der Ring $\mathbb{Z}[x]$ zwar nullteilerfrei ist, aber nicht euklidisch, und auch kein Hauptidealring. Es sei nun p eine Primzahl und $\pi : \mathbb{Z} \to \mathbb{F}_p$ der Restklassenhomomorphismus. Wir definieren einen Ringhomomorphismus

$$\pi_* : \mathbb{Z}[x] \to \mathbb{F}_p[x], \sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} [a_k] x^k$$

(es ist klar, dass π_* ein Ringhomomorphismus ist). Der Vorteil dieser Konstruktion ist, dass $\mathbb{F}_p$ ein Körper ist, und daher $\mathbb{F}_p[x]$ ein euklidischer Ring, so dass wir die gesamte Teilbarkeitstheorie zur Verfügung haben.

Satz 3.4.2 (Lemma von Gauß)**.** *Es sei $f(x) \in \mathbb{Z}[x]$, und es gebe nichtkonstante Polynome $g(x), h(x) \in \mathbb{Q}[x]$ mit $f(x) = g(x)h(x)$. Dann gibt es nichtkonstante Polynome $g'(x), h'(x) \in \mathbb{Z}[x]$ mit $f(x) = g'(x)h'(x)$, und man kann g' und h' so wählen, dass $g'(x) = ag(x)$ und $h'(x) = \frac{1}{a}h(x)$, wobei $a \in \mathbb{Q}^\times$.*

Es ist nicht richtig, dass die Polynome $g(x)$ und $h(x)$ ganzzahlige Koeffizienten haben, wie man am Beispiel $g(x) = 2(x-1)$, $h(x) = \frac{1}{2}(x-1)$, $g(x)h(x) = x^2 - 2x + 1$ erkennt.

Beweis. Sei $f(x) = g(x)h(x)$, $g, h \in \mathbb{Q}[x]$ nichtkonstant. Es gibt dann $m \in \mathbb{N}$ mit $g_1(x) := mg(x) \in \mathbb{Z}[x]$: man wähle z.B. m als Produkt aller Nenner der Koeffizienten von $g(x)$. Analog findet man $n \in \mathbb{N}$ mit $h_1(x) := nh(x) \in \mathbb{Z}[x]$. Es ist dann

$$mnf(x) = g_1(x)h_1(x) \tag{3.4.3}$$

eine nichttriviale Produktzerlegung in $\mathbb{Z}[x]$. Wenn $mn = 1$, so ist $m = n = 1$ und wir sind fertig. Wir argumentieren jetzt, dass wenn p eine Primzahl ist, welche mn teilt, eine nichttriviale Produktzerlegung

$$\frac{mn}{p} f(x) = g_2(x)h_2(x)$$

in $\mathbb{Z}[x]$ gefunden werden kann. Auf diese Art können alle Primfaktoren von mn herausgekürzt werden, und nach endlich vielen Schritten finden wir eine nichttriviale Produktzerlegung

$$f(x) = g_r(x)h_r(x) \in \mathbb{Z}[x],$$

wie gewünscht.

Sei nun p eine Primzahl, welche mn teilt. Anwendung des Homomorphismus π_* auf (3.4.3) zeigt

$$\pi_*(g_1(x))\pi_*(h_1(x)) = \pi_*(mnf(x)) = [mn]\pi_*(f(x)) = 0$$

(denn $[mn] = 0 \in \mathbb{F}_p$). Weil der Ring $\mathbb{F}_p[x]$ nullteilerfrei ist, muss einer der beiden Faktoren $\pi_*(g_1(x))$ oder $\pi_*(h_1(x))$ gleich Null sein. Ohne Beschränkung der Allgemeinheit sei $\pi_*(g_1(x)) = 0$. Daraus folgt, dass p alle Koeffizienten von $g_1(x)$ teilt, und wir können $g_1(x) = pg_2(x)$ mit $g_2(x) \in \mathbb{Z}[x]$ schreiben. Man setze $h_2(x) := h_1(x)$ und sieht sofort, dass

$$\frac{mn}{p} f(x) = g_2(x)h_2(x)$$

gilt, wie erwünscht. □

Satz 3.4.4 (Eisenstein-Kriterium)**.** *Es sei $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$, $n \geq 2$, und es gebe eine Primzahl p, so dass*

(1) *p teilt $a_0, \ldots, a_{n-1}$,*
(2) *p teilt a_n nicht, und*
(3) *p^2 teilt a_0 nicht.*

Dann ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$.

Beweis. Wir nehmen an, dass $f(x)$ nicht irreduzibel ist, und die Bedingungen (1) sowie (2) gelten, und leiten daraus her, dass die Bedingung (3) verletzt ist.

Wenn $f(x)$ nicht irreduzibel ist, dann können wir nach Satz 3.4.2 $f(x) = g(x)h(x)$ schreiben, mit $g(x) = \sum_{j=0}^m b_j x^j \in \mathbb{Z}[x]$ und $h(x) = \sum_{j=0}^k c_j x^j \in \mathbb{Z}[x]$ und $m, k < n$.

Sei $\pi_* : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ der Restklassenhomomorphismus. Die Annahmen (1) und (2) zeigen, dass

$$\pi_*(f(x)) = [a_n]x^n \neq 0,$$

und dass

$$\pi_*(f(x)) = [a_n]x \cdots x$$

eine Zerlegung in irreduzible Faktoren ist. Die Faktoren $\pi_*(g(x))$ und $\pi_*(h(x))$ von $\pi_*(f(x))$ sind von Null verschieden. Weil $\mathbb{F}_p[x]$ euklidisch ist, gibt es Zerlegungen von $\pi_*(g(x))$ und $\pi_*(h(x))$ in irreduzible Faktoren. Wegen der Eindeutigkeit der Primfaktorzerlegung im euklidischen Ring $\mathbb{F}_p[x]$ muss daher

$$\pi_*(g(x)) = [b_m]x^m,\ \pi_*(h(x)) = [c_k]x^k$$

gelten (weil p kein Teiler von $a_n = b_m c_k$ ist, sind $[b_m], [c_k] \neq 0 \in \mathbb{F}_p$). Daraus folgt, dass $p|b_j$ für $j < m$ und $p|c_j$ für $j < k$. Insbesondere gilt $p|b_0$ und $p|c_0$. Weil $a_0 = b_0 c_0$, folgt

$$p^2|a_0.$$

□

Beispiel 3.4.5. *Sei p eine Primzahl und $n \geq 2$. Dann ist das Polynom*

$$x^n - p \in \mathbb{Q}[x]$$

irreduzibel (das stimmt auch für $n = 1$, ist aber langweilig).

Beispiel 3.4.6. *Sei p eine Primzahl, und betrachte*

$$\phi_p(x) = \sum_{k=0}^{p-1} x^k = \frac{x^p - 1}{x - 1} \in \mathbb{Q}[x].$$

Dies ist das sogenannte pte Kreisteilungspolynom*; die Nullstellen von $\phi_p(x)$ in $\mathbb{C}$ sind genau die von 1 verschiedenen p-ten Einheitswurzeln in $\mathbb{C}$. Das Eisenstein-Kriterium zeigt, dass $\phi_p(x)$ irreduzibel ist, wobei wir den folgenden Trick anwenden. Die Irreduzibilität von $\phi_p(x)$ ist äquivalent zur Irreduzibilität von $f(x) = \phi_p(x+1)$. Es gilt aber nach dem binomischen Lehrsatz*

$$f(x) = \frac{(x+1)^p - 1}{x} = \frac{1}{x} \sum_{k=1}^{p} \binom{p}{k} x^k \overset{k=l+1}{=} \sum_{l=0}^{p-1} \binom{p}{l+1} x^l =: \sum_{l=0}^{p-1} a_l x^l,$$

wobei $a_l = \binom{p}{l+1}$. Es gilt $a_{p-1} = \binom{p}{p} = 1$ und $a_0 = \binom{p}{1} = p$; daher sind die Voraussetzungen (1) und (3) des Eisenstein-Kriteriums erfüllt. Die Voraussetzung (2) folgt aus dem nächsten Lemma, das wir explizit notieren, um späteren Nutzen daraus ziehen zu können.

Lemma 3.4.7. *Sei p eine Primzahl. Dann teilt p die Binomialkoeffizienten $\binom{p}{k}$, wenn $0 < k < p$.*

Beweis. Es gilt

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}.$$

Schreibe $a = (p-1)!$, $b = k!(p-k)!$ und $c := \binom{p}{k}$, so dass

$$c = \frac{ap}{b} \in \mathbb{Z}.$$

(die Zahlen ap und b sind i.A. nicht teilerfremd). Wir müssen argumentieren, dass $\frac{a}{b} \in \mathbb{Z}$ gilt. Jedenfalls ist

$$cb = ap,$$

so dass $p|cb$. Nach dem Lemma von Euklid muss dann $p|c$ oder $p|b$ gelten. Allerdings ist p kein Teiler von $b = k!(p-k)!$, wenn $0 < k < p$! Grund:

$$b = 2 \cdot 2 \cdot \ldots \cdot k \cdot 2 \cdot 3 \cdot \ldots (p-k)$$

ist ein Produkt von Zahlen, welche alle kleiner als p sind und daher nicht durch p teilbar sein können. Nach dem Lemma von Euklid folgt, dass p kein Teiler von b ist. Somit ist p ein Teiler von $c = \binom{p}{k}$, wie behauptet. □

Aus Satz 3.4.2 lässt sich noch ein weiteres Irreduzibilitätskriterium herleiten.

Lemma 3.4.8. *Es sei $f(x) \in \mathbb{Z}[x]$ ein* normiertes Polynom*, und es gebe normierte Polynome $g(x), h(x) \in \mathbb{Q}[x]$ mit*

$$f(x) = g(x)h(x).$$

Dann gilt: $g(x), h(x) \in \mathbb{Z}[x]$. Insbesondere folgt: ist $z \in \mathbb{Q}$ und $f(z) = 0$, so ist bereits $z \in \mathbb{Z}$.

Beweis. Aus Satz 3.4.2 folgt, dass $a \in \mathbb{Q}^\times$ existiert, so dass $ag(x)$ und $\frac{1}{a}h(x)$ ganzzahlig sind. Weil die Leitkoeffizienten von $g(x)$ und $h(x)$ gleich 1 sind, muss sowohl a als auch $\frac{1}{a}$ ganzzahlig sein, und das geht nur, wenn $a = \pm 1$. Somit sind

$g(x)$ und $h(x)$ bereits ganzzahlig. Die Aussage über die Nullstellen folgt sofort, denn ist $z \in \mathbb{Q}$ eine Nullstelle von f, so schreibe

$$f(x) = (x - z)g(x),$$

mit $g(x) \in \mathbb{Q}[x]$. Nun ist, weil $f(x)$ normiert ist, $g(x)$ ebenfalls normiert, und daher sind sowohl $(x-z)$ als auch $g(x)$ ganzzahlig, aber das heißt insbesondere $z \in \mathbb{Z}$. □

Wir entwickeln aus Lemma 3.4.8 nun eine weitere Methode, um Irreduzibilität nachzuweisen, nämlich *Reduktion modulo p*.

Satz 3.4.9. *Es sei $f(x) \in \mathbb{Z}[x]$ ein normiertes Polynom und es sei p eine Primzahl, so dass $\pi_* f(x) \in \mathbb{F}_p[x]$ irreduzibel ist. Dann ist $f(x) \in \mathbb{Q}[x]$ irreduzibel.*

Beweis. Wäre $f(x)$ reduzibel, so erhielten wir aus Lemma 3.4.8 eine Zerlegung $f(x) = g(x)h(x)$ in normierte Polynome von positivem Grad. Es folgt $\pi_*(f(x)) = \pi_*(g(x))\pi_*(h(x))$, und weil $g(x)$ sowie $h(x)$ normiert sind, sind es auch $\pi_*(g(x))$ und $\pi_*(h(x))$, so dass wir eine Zerlegung von $\pi_*(f(x))$ in Polynome von positivem Grad erhalten, im Widerspruch zur Annahme. □

Weil es nur endlich viele Polynome vom Grad $\leq n$ in $\mathbb{F}_p[x]$ gibt, kann die Irreduzibilität durch eine endliche Rechnung nachgewiesen werden.

4. Körpererweiterungen

Wir werden jetzt das systematische Studium von Körpererweiterungen in Angriff nehmen.

4.1. **Der Primkörper und die Charakteristik.** Sei R ein Ring mit 1. Es gibt einen eindeutig bestimmten Ringhomomorphismus

$$j = j_R : \mathbb{Z} \to R$$

mit $j(1) = 1_R$ (für den Moment sind wir in der Notation sehr präzise). Dieser ist gegeben durch die Vorschrift $j(n) := n \cdot 1_R$. Hierbei ist $1_R \in R$, $n \in \mathbb{Z}$, und das Symbol $n \cdot 1_R \in R$ ist wie in Bemerkungen 1.1.2 und 1.1.4 eingeführt. Wie in diesen Bemerkungen gesagt, ist j ein Homomorphismus von Gruppen, d.h. es gilt

$$j(n + m) = j(n) + j(m).$$

Um zu zeigen, dass $j(mn) = j(m)j(n)$, muss man das Distributivgesetz verwenden. Die genaue Rechtfertigung ist etwas länglich und unterbleibt hier; mit solchen Formalitäten wollen wir uns nicht länger aufhalten.

Sei nun K ein Körper, und betrachte den eben diskutierten Ringhomomorphismus

$$j = j_K : \mathbb{Z} \to K.$$

Wir unterscheiden jetzt zwei Fälle: entweder j ist injektiv, oder j ist nicht injektiv.

Satz 4.1.1. *Sei K ein Körper und j_K sei injektiv. Dann kann j zu einem Körperhomomorphismus $\tilde{j} : \mathbb{Q} \to K$ fortgesetzt werden, welcher automatisch injektiv ist (nach Satz 1.1.20). Der Unterkörper $\tilde{j}(\mathbb{Q}) \subset K$ ist isomorph zu $\mathbb{Q}$. Der Unterkörper $\tilde{j}(\mathbb{Q})$ ist der kleinste Unterkörper von K und heißt* Primkörper *von K. Wir sagen auch, dass K die* Charakteristik 0 *hat;* $\mathrm{char}(K) = 0$.

Beispiele für Körper der Charakteristik 0 sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ und jeder Zwischenkörper $\mathbb{Q} \subset K \subset \mathbb{C}$. Körper der Charakteristik 0 sind immer unendlich.

Beweis. Wir setzen

$$\tilde{j}(\frac{m}{n}) := \frac{j(m)}{j(n)}.$$

Dies geht, weil der Nenner $j(n)$ nur für $n = 0$ verschwindet: j injektiv. Ist $\frac{m}{n} = \frac{m'}{n'}$, so ist $mn' = m'n$, und daher

$$\frac{j(m)}{j(n)} = \frac{j(m')}{j(n')}$$

nach einem mitlerweile vertrauten Argument, so dass $\tilde{j}$ wohldefiniert ist. Es ist klar, dass $\tilde{j}(\mathbb{Q})$ ein Unterkörper ist, welcher isomorph zu $\mathbb{Q}$ ist. Jeder andere Unterkörper $L \subset K$ muss $\tilde{j}$ enthalten, weil L automatisch das Bild von j enthält, und alle Inversen der Elemente $j(n)$. □

Satz 4.1.2. *Sei K ein Körper, so dass j_K nicht injektiv ist. Dann gibt es genau eine Primzahl $p \in \mathbb{N}$, so dass $j(p) = 0$, und j induziert einen Körperhomomorphismus $\tilde{j} : \mathbb{F}_p \to K$. Das Bild $\tilde{j}(\mathbb{F}_p)$ ist der kleinste Unterkörper von K, und heißt wieder Primkörper. Wir sagen, dass K die* Charakteristik p *hat,* $\mathrm{char}(K) = p$.

Beweis. Der Kern $\ker(j) = \{n | j(n) = 0\} \subset \mathbb{Z}$ ist ein Ideal, und also von der Form $\ker(j) = (p)$ für ein $p > 0$ (weil j nicht injektiv, ist $\ker(j) \neq (0)$). j induziert dann einen injektiven Ringhomomorphismus

$$\tilde{j} : \mathbb{Z}/p \to K.$$

Weil K nullteilerfrei ist, muss auch $\mathbb{Z}/p$ nullteilerfrei sein und daher muss p eine Primzahl sein. Genauso wie im Fall, dass j injektiv ist, sieht man, dass $\tilde{j}(\mathbb{F}_p)$ ein zu $\mathbb{F}_p$ isomorpher Unterkörper von K ist, und der kleinste Unterkörper von K. □

Es gibt durchaus unendliche Körper der Charakteristik p.

4.2. **Der Grad einer Körpererweiterung.**

Beobachtung 4.2.1. *Es sei $K \subset L$ eine Körpererweiterung. Dann ist durch die Addition und die Einschränkung*

$$K \times L \to L, (x, y) \mapsto xy$$

der Multiplikation die Struktur eines K-Vektorraumes auf L erklärt.

Diese einfache Beobachtung erschließt die Methoden der linearen Algebra für das Studium von Körpererweiterungen!

Definition 4.2.2. *Es sei $K \subset L$ eine Körpererweiterung. Der* Grad *von L über K ist die Dimension von L als K-Vektorraum;*

$$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}.$$

Die Körpererweiterung $K \subset L$ heißt endlich, *wenn $[L : K] < \infty$.*

Beispiele 4.2.3.

(1) *Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist endlich, und es gilt $[\mathbb{C} : \mathbb{R}] = 2$.*

(2) *Die Körpererweiterung $\mathbb{Q} \subset \mathbb{R}$ ist nicht endlich. Das lässt sich auf viele verschiedene Arten einsehen. Zum Beispiel ist jede endliche Körpererweiterung von $\mathbb{Q}$ automatisch abzählbar, und bekanntlich ist $\mathbb{R}$ überabzählbar. Oder man kann argumentieren, dass die Elemente $\sqrt{p}$, p Primzahl, linear unabhängig über $\mathbb{Q}$ sind. Wir geben später ein alternatives einfaches Argument an.*

(3) *Ist K ein endlicher Körper, so gibt es eine Primzahl p mit $\mathrm{char}(K) = p$, und K kann als Erweiterungskörper von $\mathbb{F}_p$ angesehen werden. Der Grad $[K : \mathbb{F}_p]$ ist endlich, weil eine $\mathbb{F}_p$-Basis von K nur endlich viele Elemente haben kann. Ist $n := [K : \mathbb{F}_p]$, so ist K als $\mathbb{F}_p$-Vektorraum isomorph zu $\mathbb{F}_p^n$, und $\mathbb{F}_p^n$ hat genau p^n Elemente. Wir schließen, dass ein endlicher Körper K die Mächtigkeit p^n haben muss, für eine Primzahl p und ein $n \in \mathbb{N}$.*

(4) *In §3.3 haben wir für ein irreduzibles Polynom $f(x) \in K[x]$ vom Grad n die Körpererweiterung $K \subset K[x]/(f)$ studiert. Lemma 3.3.1 lässt sich auch so ausdrücken, dass die Elemente $1, [x], \ldots, [x^{n-1}]$ eine Basis von $K[x]/(f)$ über K bilden. Somit gilt*

$$[K[x]/(f) : K] = \deg(f(x)). \tag{4.2.4}$$

Theorem 4.2.5 (Gradformel)**.** *Es seien $K \subset L \subset F$ Körpererweiterungen. Dann gilt*

$$[F : K] = [F : L][L : K].$$

(Dies ist mit der Vereinbarung zu lesen, dass $\infty \cdot \infty = \infty$ und $\infty \cdot n = \infty$ für jedes $n \in \mathbb{N}$.)

Beweis. Wir zeigen den Satz nur unter der Voraussetzung $[F : L], [L : K] < \infty$. Es sei $[F : L] = m$ und $\mathcal{A} = \{y_1, \ldots, y_m\}$ eine Basis von F als L-Vektorraum. Ferner sei $[L : K] = n$ und $\mathcal{B} = \{x_1, \ldots, x_n\}$ eine Basis von L als K-Vektorraum. Wir behaupten, dass

$$\mathcal{C} = \{x_i y_j | i \in \underline{n}, j \in \underline{m}\}$$

eine Basis von F als K-Vektorraum ist, womit der Beweis erbracht wäre.

Zunächst zeigen wir, dass $\mathcal{C}$ linear unabhängig über K ist. Sei also

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} x_i y_j = 0,$$

wobei $a_{ij} \in K$. Zu zeigen ist, dass alle $a_{ij} = 0$.

Nun ist $c_j := \sum_{i=1}^{n} a_{ij} x_i \in L$ und $\sum_{j=1}^{m} c_j y_j = 0$. Weil die y_j's linear unabhängig über L sind, folgt

$$0 = c_j = \sum_{i=1}^{n} a_{ij} x_i$$

für jedes j. Weil die x_i's linear unabhängig über K sind, und weil $a_{ij} \in K$, folgt ferner $a_{ij} = 0$ für alle i und j. Somit ist $\mathcal{C}$ linear unabhängig.

Des weiteren müssen wir zeigen, dass $\mathcal{C}$ den K-Vektorraum F aufspannt. Sei also $z \in F$. Wir können z als Linearkombination

$$z = \sum_{j=1}^{m} b_j y_j, \ b_j \in L$$

mit Koeffizienten in L schreiben. Des weiteren kann b_j als Linearkombination

$$b_j = \sum_{i=1}^{n} c_{ij} x_i, \ c_{ij} \in K$$

geschrieben werden. Insgesamt ist

$$z = \sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij} x_i y_j.$$

Weil z beliebig war, ist $\mathcal{C}$ als Erzeugendensystem des K-Vektorraumes F erkannt. □

4.3. **Einfache Körpererweiterungen, Algebraizität und das Minimalpolynom.**

Lemma 4.3.1. *Es sei L ein Körper und $S \subset L$ eine Teilmenge. Es gibt dann einen (eindeutig bestimmten) kleinsten Unterkörper K von L, welcher die Menge S enthält.*

Beweis. Das ist eine reine Formalität. Man beobachtet, dass der Schnitt zweier Unterkörper $K_0, K_1 \subset L$ wieder ein Unterkörper $K_0 \cap K_1$ von L ist. Es sei I die Menge aller Unterkörper von L, welche S enthalten. Dann ist

$$K := \cap_{F \in I} F$$

der gesuchte Unterkörper. □

Ist zum Beispiel $S = \emptyset$, so ist der Primkörper aus dem letzten Abschnitt der kleinste Unterkörper, der S enthält. Wichtiger ist der Fall, dass $K \subset L$ eine Körpererweiterung ist und $T \subset L$ eine Teilmenge. Der kleinste Unterkörper von L, welcher $K \cup T$ enthält, wird auch mit $K(T) \subset L$ bezeichnet. Es handelt sich um einen *Zwischenkörper*, also $K \subset K(T) \subset L$. Für endliches $T = \{z_1, \ldots, z_n\}$ schreiben wir auch kürzer

$$K(z_1, \ldots, z_n) := K(\{z_1, \ldots, z_n\}).$$

Definition 4.3.2. *Eine Körpererweiterung $K \subset L$ heißt* endlich erzeugt*, wenn eine endliche Menge $\{z_1, \ldots, z_n\} \subset L$ existiert mit*

$$L = K(z_1, \ldots, z_n).$$

Eine Körpererweiterung heißt einfach*, wenn ein $z \in L$ existiert mit*

$$L = K(z).$$

Beispiele 4.3.3.
(1) *Sei $K \subset F$ eine Körpererweiterung und $z \in F$. Dann ist $K \subset K(z)$ nach Definition eine einfache Erweiterung.*
(2) *$\mathbb{R} \subset \mathbb{C}$ ist einfach, denn $\mathbb{C} = \mathbb{R}(i)$.*
(3) *Ist $K \subset F$ eine Körpererweiterung und $a \in F$, $a \notin K$ ein Element mit $a^2 \in K$, so ist $K \subset K(a)$ eine einfache Körpererweiterung (und hat den Grad 2).*
(4) *Die Körpererweiterung $K \subset K[x]/(f)$ für ein irreduzibles $f(x) \in K[x]$ ist einfach, und es gilt $K([x]) = K[x]/(f)$. Denn ist $g(x) \in K[x]$ ein beliebiges Polynom, so ist*
$$[g(x)] \overset{3.3.2}{=} g([x]),$$
und offenbar ist $g([x]) \in K([x])$. Somit ist eingesehen, dass $K([x]) = K[x]/(f)$.

Definition 4.3.4. *Es sei $K \subset L$ eine Körpererweiterung und $z \in L$. Wir sagen, dass z* algebraisch über K *ist, wenn ein Polynom $0 \neq f(x) \in K[x]$ existiert mit $f(z) = 0$. Wenn z nicht algebraisch über K ist, so heißt z* transzendent über K*.*

Satz 4.3.5. *Es sei $K \subset L$ eine Körpererweiterung und $z \in L$. Dann sind äquivalent:*
(1) *die Körpererweiterung $K \subset K(z)$ ist endlich,*
(2) *z ist algebraisch über K.* □

Erster Teil des Beweises. Wir zeigen zunächst $1 \Rightarrow 2$. Es sei $K \subset K(z)$ endlich. Wie im letzten Abschnitt gesehen ist $K(z)$ ein K-Vektorraum, und wir betrachten die Folge

$$1, z, z^2, \ldots \in K(z).$$

Weil $\dim_K(K(z)) < \infty$, sind diese Elemente von $K(z)$ linear abhängig über K. Das bedeutet, dass Elemente $a_0, a_1, \ldots, a_n \in K$ gefunden werden können, die nicht alle verschwinden und so dass die lineare Gleichung

$$a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n = 0$$

gilt. Setze $f(x) := \sum_{k=0}^n a_k x^k$, dies ist ein von Null verschiedenes Element von $K[x]$, und obige Gleichung besagt schlicht und einfach $f(z) = 0$. □

Um die Umkehrung zu beweisen, ist etwas mehr erforderlich; außerdem wird der Beweis mehr Information liefern.

Lemma 4.3.6. *Es sei $K \subset L$ eine (beliebige) Körpererweiterung und $z \in L$ sei algebraisch über K. Dann gibt es ein eindeutig bestimmtes normiertes irreduzibles Polynom $\mu_{z,K}(x) = \mu_z(x) \in K[x]$ mit $\mu_z(z) = 0$. Dieses Polynom heißt* Minimalpolynom *von z über K. Das Minimalpolynom kann alternativ als das normierte Polynom vom kleinsten Grad, das z als Nullstelle hat, charakteristiert werden.*

Ferner gilt: ist $g(x) \in K[x]$ mit $g(z) = 0$, so ist $f(x)$ ein Teiler von $g(x)$.

Beweis. Sei $I \subset K[x]$ die Menge aller f mit $f(z) = 0$. Es handelt sich dabei offensichtlich um ein Ideal, und die Voraussetzung besagt, dass $I \neq (0)$. Weil $K[x]$ euklidisch ist, gibt es ein f mit $(f) = I$. Wir dürfen f als normiert annehmen, und offenbar ist $f(z) = 0$, und f ist das normierte Polynom vom kleinsten Grad in I, wie aus dem Beweis von Theorem 2.4.3 folgt.

Außerdem ist f irreduzibel, denn $f(x) = g(x)h(x)$ impliziert $0 = f(z) = g(z)h(z)$, also $g(z) = 0$ oder $h(z) = 0$. Weil der Grad von f minimal unter allen Polynomen, die z als Nullstelle haben, ist, muss g oder h konstant und also eine Einheit sein.

Nun sei g ein anderes irreduzibles normiertes Polynom mit $g(z) = 0$. Es ist dann $g(x) \in I$, also $g(x) = a(x)f(x)$, d.h. $f(x)$ ist ein Teiler von $g(x)$.

Wenn $g(x)$ überdies irreduzibel ist, muss a eine Einheit sein, also konstant, und weil g normiert ist, muss $a = 1$ sein, also $g = f$. □

Satz 4.3.7. *Es sei $K \subset L$ eine Körpererweiterung und es sei $z \in L$ algebraisch über K, mit Minimalpolynom*

$$f(x) = \mu_{K,z}(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in K[x].$$

Dann gilt

1. *die Körpererweiterung $K \subset K(z)$ ist endlich,*
2. *$K(z)$ ist isomorph zum Körper $K[x]/(f)$,*
3. *$\{1, z, z^2, \ldots, z^{n-1}\}$ ist eine K-Basis von $K(z)$. Insbesondere ist*

$$[K(z) : K] = \deg(\mu_{K,z}(x)).$$

Zweiter Teil des Beweises von Satz 4.3.5. Es ist die Implikation $2 \Rightarrow 1$ zu beweisen. Sei also $z \in L$ algebraisch über K und sei $f(x)$ das Minimalpolynom von z über K. Aus Satz 4.3.7 folgt, dass $[K(z) : K] = [K[x]/(f) : K] = \deg(f(x)) < \infty$. □

Beweis von Satz 4.3.7. Wir betrachten den Ringhomomorphismus

$$\phi : K[x] \to L,\ g \mapsto g(z).$$

Der Kern ϕ besteht aus allen Polynomen, welche z als Nullstelle haben, und ist ein Ideal von $K[x]$. Im Beweis von Lemma 4.3.6 haben wir gesehen, dass $\ker(\phi) = (f)$, wobei f das Minimalpolynom von z und irreduzibel ist.

Der Homomorphismus ϕ induziert nach Satz 3.2.9 einen Ringhomomorphismus

$$\varphi : K[x]/(f) \to L;\ [g] \mapsto g(z).$$

Weil f irreduzibel ist, ist $K[x]/(f)$ nach Satz 3.2.10 ein Körper. Es folgt, dass $\varphi : K[x]/(f) \to L$ ein (automatisch injektiver) Körperhomomorphismus ist. Ferner ist das Bild $\mathrm{im}(\varphi) \subset L$ ein Körper, und φ liefert einen Körperisomorphismus

$$\varphi : K[x]/(f) \cong \mathrm{im}(\varphi).$$

Es gilt

$$\varphi([x]) = \phi(x) = z,$$

das heißt, es ist $z \in \mathrm{im}(\varphi)$. Weil außerdem offenbar $K \subset \mathrm{im}(\varphi)$, ist $\mathrm{im}(\varphi)$ ein Unterkörper, der sowohl z als auch K enthält, und daher muss auch der kleinste Körper mit diesen Eigenschaften (das ist gerade $K(z)$) in $\mathrm{im}(\varphi)$ enthalten sein. Es gilt daher

$$K(z) \subset \mathrm{im}(\varphi).$$

Auf der anderen Seite ist

$$\mathrm{im}(\varphi) \subset K(z),$$

denn jedes Element von $\mathrm{im}(\varphi)$ von der Form $g(z)$ für ein $g(x) \in K[x]$, und daher eine K-Linearkombination von Potenzen von z. Allerdings in $K(z)$ ein Unterkörper, der sowohl K als auch z enthält, und muss daher alle solchen Linearkombinationen enthalten. Insgesamt ergibt sich

$$\mathrm{im}(\varphi) = K(z).$$

Es folgt sofort Behauptung (2), und Lemma 3.3.1 impliziert dann sofort die Behauptungen (1) und (3). □

Beispiel 4.3.8. *Das Minimalpolynom eines Elementes $z \in L$ hängt ganz entscheidend davon ab, welcher Grundkörper K zugrunde gelegt wurde. Wir diskutieren das anhand der Körpererweiterungen*

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Betrachte das Element $z := i\sqrt[4]{2}$. Dies ist natürlich Nullstelle des normierten irreduziblen Polynoms

$$(x - i\sqrt[4]{2}) \in \mathbb{C}[x]$$

mit komplexen Koeffizienten. Also gilt

$$\mu_{\mathbb{C},z}(x) = (x - z).$$

Ein Polynom mit reellen Koeffizienten*, welches z als Nullstelle hat, ist*

$$(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) = x^2 + \sqrt{2} \in \mathbb{R}[x].$$

Dies ist irreduzibel, weil vom Grad 2 und ohne Nullstelle in $\mathbb{R}$. Folglich ist

$$\mu_{\mathbb{R},z}(x) = x^2 + \sqrt{2}.$$

Natürlich ist $\sqrt{2} \notin \mathbb{Q}$. Ein Polynom mit rationalen Koeffizienten*, welches z als Nullstelle hat, ist*

$$(x^2 + \sqrt{2})(x^2 - \sqrt{2}) = x^4 - 2 \in \mathbb{Q}[x].$$

Dies ist irreduzibel nach dem Eisenstein-Kriterium, und es folgt

$$\mu_{\mathbb{R},z}(x) = x^4 - 2.$$

Es gilt aber immerhin folgendes.

Lemma 4.3.9. *Es seien $K \subset L \subset F$ Körpererweiterungen und $z \in F$ sei algebraisch über K. Dann ist z algebraisch über L, es gilt*

$$\mu_{z,L}(x) | \mu_{z,K}$$

und daher auch

$$\deg(\mu_{z,L}) \leq \deg(\mu_{z,K}).$$

Beweis. Weil $K[x] \subset L[x]$, ist $\mu_{z,L}(x) \in L[x]$ ein Polynom mit $\mu_{z,L}(z) = 0$. Folglich gilt $\mu_{z,L}(x) | \mu_{z,K}$ und die Aussage über die Grade folgt sofort. □

Beispiel 4.3.10. *Es sei $z \in \mathbb{C}$, $z \notin \mathbb{R}$. Dann ist*

$$(x-z)(x-\overline{z}) = x^2 - 2\Re(z)x + |z|^2 \in \mathbb{R}[x]$$

irreduzibel (weil keine Nullstelle reell ist) und muss daher mit dem Minimalpolynom übereinstimmen.

Beispiel 4.3.11. *Sei $z := e^{\frac{2\pi i}{p}} \in \mathbb{C}$, p Primzahl. z ist eine Nullstelle des Kreisteilungspolynoms*

$$\phi_p(x) = x^{p-1} + \ldots + x + 1,$$

welches wir in 3.4.6 als irreduzibel erkannt haben. Folglich $\mu_{\mathbb{Q},z}(x) = \phi_p(x)$.

Beispiel 4.3.12. *$z := \sqrt[3]{2}$. Dann ist $\mu_{\mathbb{Q},z}(x) = x^3 - 2$, denn dieses Polynom ist irreduzibel nach dem Eisensteinkriterium.*

Wir diskutieren nun einige Beispiele mehrfacher Körpererweiterungen.

Beispiel 4.3.13. *Betrachte $f(x) = x^3 - 2$; dieses Polynom ist irreduzibel. Es sei $z := \sqrt[3]{2}$ und $\zeta := e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Die Nullstellen von $f(x)$ sind gerade*

$$z, \zeta z, \zeta^2 z.$$

Das Minimalpolynom von ζ ist $x^2 + x + 1$, und dasjenige von z ist $x^3 - 2$, beides über $\mathbb{Q}$. Man betrachte den Körper $\mathbb{Q}(z,\zeta) \subset \mathbb{C}$. Was ist der Grad $[\mathbb{Q}(z,\zeta) : \mathbb{Q}]$? Wir betrachten zunächst

$$[\mathbb{Q}(z,\zeta) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}][\mathbb{Q}(z,\zeta) : \mathbb{Q}(z)] = 3[\mathbb{Q}(z,\zeta) : \mathbb{Q}(z)].$$

Andererseits ist nach Lemma 4.3.9 $[\mathbb{Q}(z,\zeta) : \mathbb{Q}(z)] \leq 2$.

Betrachte ferner

$$[\mathbb{Q}(z,\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}][\mathbb{Q}(z,\zeta) : \mathbb{Q}(\zeta)] = 2[\mathbb{Q}(z,\zeta) : \mathbb{Q}(\zeta)],$$

and wieder wegen Lemma 4.3.9 ist $[\mathbb{Q}(z,\zeta) : \mathbb{Q}(\zeta)] \leq 3$. Es folgt

$$[\mathbb{Q}(z,\zeta) : \mathbb{Q}] \leq 6,\ 2|[\mathbb{Q}(z,\zeta) : \mathbb{Q}],\ 3|[\mathbb{Q}(z,\zeta) : \mathbb{Q}],$$

und alle drei Bedingungen zusammen zeigen

$$[\mathbb{Q}(z,\zeta) : \mathbb{Q}] = 6.$$

Beispiel 4.3.14. *Betrachte $\mathbb{Q}(\sqrt{3},\sqrt{2}) \subset \mathbb{R}$. Es gilt $2|[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] \leq 4$, also it der Grad entweder 2 oder 4. Die Anwort lautet, dass der Grad gleich 4 ist. Eine Möglichkeit, dies zu sehen, ist es, zu zeigen, dass das Polynom x^2-3 keine Nullstelle in $\mathbb{Q}(\sqrt{2})$ besitzt. Wir argumentieren etwas anders und indirekter. Betrachte $z = \sqrt{2} + \sqrt{3}$. Es gilt dann*

$$z^2 = 5 + 2\sqrt{6}$$

beziehungsweise

$$z^2 - 5 = 2\sqrt{6}$$

und daher

$$(z^2 - 5)^2 - 24 = 0$$

oder

$$f(z) = z^4 - 10z^2 + 1 = 0$$

Man kann zeigen, dass dieses Polynom irreduzibel über $\mathbb{Q}$ ist. Wenn $f(x)$ reduzibel wäre, so würden nach Satz 3.4.2 eine Zerlegung

$$f(x) = g(x)h(x)$$

mit ganzzahligen g, h existieren. Man kann sich leicht davon überzeugen, dass $f(x)$ keine Nullstelle in $\mathbb{Z}$ hat, also müssten beide Faktoren g und h quadratisch sein. Weil f normiert ist, sind notwendigerweise g und h normiert, und obige Zerlegung läuft auf

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

hinaus, mit ganzzahligen a, b, c, d. Durch Ausmultiplizieren erkennt man schnell, dass keine solchen Zahlen existieren können. Somit ist $f8x)$ irreduzibel und damit gleich dem Minimalpolynom von $\sqrt{3} + \sqrt{2}$. Ferner folgt, dass $[\mathbb{Q}(z) : \mathbb{Q}] = 4$ und daraus auch, dass

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(z).$$

4.4. **Einige Bemerkungen über transzendente Zahlen.** Man kann relativ leicht zeigen, dass viele komplexe Zahlen z existieren, die transzendent über $\mathbb{C}$ sind. Das geht so: $\mathbb{Q}$ ist abzählbar, und ebenso hat der Polynomring $\mathbb{Q}[x]$ nur abzählbar viele Elemente. Jedes Element $0 \neq f(x) \in \mathbb{Q}[x]$ hat nur endlich viele Nullstellen. Es folgt, dass die Menge aller Nullstellen in $\mathbb{C}$ aller von Null verschiedenen rationalen Polynome abzählbar ist. Mit anderen Worten: es gibt nur abzählbar viele Elemente von $\mathbb{C}$, die algebraisch über $\mathbb{Q}$ sind. Andererseits in $\mathbb{C}$ überabzählbar, und es folgt, dass die Menge der transzendenten Zahlen überabzählbar ist.

Eine ganz andere und viel tiefere Frage ist es, nachzuweisen, dass eine konkrete komplexe Zahl transzendent über $\mathbb{Q}$ ist. Ohne Beweis sei erwähnen wir jedoch:

Satz 4.4.1 (Satz von Lindemann–Hermite)**.** *Es sei $0 \neq z \in \mathbb{C}$ algebraisch (über $\mathbb{Q}$). Dann ist e^z transzendent über $\mathbb{Q}$.*

Für den Beweis sei auf [**?**, §17] verwiesen. Es folgt:

(1) $e = e^1$ ist transzendent.
(2) Ist $x > 0$, $x \neq 1$, $x \in \mathbb{Q}$, so ist $\log(x)$ transzendent.
(3) Weil $e^{\pi i} = -1$, ist $e^{\pi i}$ algebraisch und folglich πi transzendent. Mit Korollar 4.5.4 unten folgt, dass π transzendent ist. Diese Tatsache löste das 2000 Jahre alte Problem der *Quadratur des Kreises*.

Dies ist alles, was wir an Worten über transzendente Zahlen verlieren wollen.

4.5. **Algebraische Körpererweiterungen.**

Definition 4.5.1. *Eine Körpererweiterung $K \subset L$ heißt* algebraisch*, wenn jedes $z \in L$ algebraisch über K ist.*

Satz 4.5.2. *Eine endliche Erweiterung $K \subset L$ ist algebraisch.*

Beweis. Sei $z \in L$. Dann ist $K \subset K(z) \subset L$, und es folgt $[K(z) : K] \leq [L : K] < \infty$, und aus Satz 4.3.5 folgt, dass z algebraisch über K ist. □

Satz 4.5.3. *Es sei $K \subset L$ eine Körpererweiterung, und es seien $z_1, \ldots, z_r \in L$ algebraisch über K. Dann ist die Erweiterung $K \subset K(z_1, \ldots, z_r)$ endlich, und es gilt*

$$[K(z_1, \ldots, z_r) : K] \leq \prod_{j=1}^{r} [K(z_j) : K].$$

Beweis. Wir setzen $K_0 := K$ und $K_j := K(z_1, \ldots, z_j)$, so dass eine Folge

$$K_0 \subset K_1 \subset \ldots \subset K_r = K(z_1, \ldots, z_r)$$

von Körpererweiterungen gegeben ist, mit $K_j = K_{j-1}(z_j)$. Nach Lemma 4.3.9 ist z_j algebraisch über K_{j-1}, und es gilt

$$\deg(\mu_{K_{j-1},z_j}) \leq \deg(\mu_{K,z_j}),$$

und es ist außerdem (Satz 4.3.7)

$$\deg(\mu_{K,z_j}) = [K(z_j) : K]$$

und

$$\deg(\mu_{K_{j-1},z_j}) = [K_j : K_{j-1}].$$

Aus der Gradformel folgt ferner

$$[K_r : K] = \prod_{j=1}^{r} [K_j : K_{j-1}],$$

so dass insgesamt gilt:

$$[K_r : K] = \prod_{j=1}^{r} [K_j : K_{j-1}] \leq \prod_{j=1}^{r} [K_j : K],$$

wie behauptet. □

Korollar 4.5.4. *Es sei $K \subset L$ eine Körpererweiterung und es seien $0 \neq z, w \in L$ algebraisch über K. Dann sind auch*

$$z + w, zw, \frac{1}{z}$$

algebraisch über K.

Zunächst mache man sich klar, dass die Aussage überhaupt nicht trivial ist: denn sind f, g Polynome mit $f(z) = 0$ und $g(w) = 0$, wie findet man ein Polynom h mit $h(z+w) = 0$ und ein Polynom k mit $k(zw) = 0$? Der folgende Beweis ist denn auch nichtkonstruktiv.

Beweis. Die Körpererweiterung $K \subset K(z, w)$ ist nach Satz 4.5.3 endlich, und nach Satz 4.5.2 auch algebraisch. Ferner sind die Elemente $z+w$, $\frac{1}{z}$ und zw alle in $K(z, w)$ enthalten. Es folgt, dass diese drei Elemente algebraisch über K sind. □

4.6. **Zerfällungskörper.**

Definition 4.6.1. *Es sei K ein Körper und $f(x) \in K[x]$ ein nichtkonstantes Polynom. Ein* Zerfällungskörper *von f ist eine Körpererweiterung $K \subset L$, so dass $f(x)$ über L in Linearfaktoren zerfällt, und so dass $f(x)$ über keinem echten Zwischenkörper $K \subset N \subsetneq L$ in Linearfaktoren zerfällt.*

Satz 4.6.2. *Zu jedem Polynom $f(x)$ gibt es einen Zerfällungskörper L, und dieser kann so gewählt werden, dass, mit $n := \deg(f)$, gilt*

$$[L : K] \leq n!$$

Bemerkung 4.6.3. *Wir werden bald sehen, dass Zerfällungskörper bis auf Isomorphismus eindeutig sind, so dass $[L : K] \leq n!$ für jeden Zerfällungskörper gilt.*

Beweis. Wir beweisen den Satz durch Induktion über $\deg(f(x))$. Im Fall $\deg(f(x)) = 1$ ist nichts zu zeigen, denn $L = K$ ist ein Zerfällungskörper von $f(x)$. Sei nun $\deg(f(x)) \geq 2$. Nach dem Satz von Kronecker 3.3.3 gibt es eine (einfache) Körpererweiterung $K \subset L_1$, in der $f(x)$ mindestens eine Nullstelle hat. Wir können daher $f(x) = (x-z)g(x)$ schreiben, wobei $g(x) \in L_1[x]$ kleineren Grad als $f(x)$ hat. Nach Induktionssannahme gibt es einen Zerfällungskörper $L_1 \subset L_2$ von $g(x)$. Das Polynom $f(x)$ zerfällt über L_2 in Linearfaktoren, und es seien $z_1, \ldots, z_r$ die Nullstellen von $f(x)$ in L_2. Wir setzen

$$L := K(z_1, \ldots, z_r) \subset L_2.$$

Dies enthält alle Nullstellen von $f(x)$; insbesondere zerfällt $f(x)$ über L in Linearfaktoren, aber $f(x)$ zerfällt über keinem echten Unterkörper von L in Nullstellen, denn jeder echte Unterkörper von L enthält eine der Nullstellen $z_1, \ldots, z_r$ nicht.

Die Aussage über die Grade folgt ebenfalls induktiv, und ist im Fall $n = 1$ klar. Induktionsschritt:

$$[L : K] \leq [L_2 : K] = [L_2 : L_1][L_1 : K] \leq (n-1)! \cdot n = n!$$

□

Bemerkung 4.6.4. *Der Satz macht keine Aussage darüber, wieviele der Nullstellen von f wirklich nötig sind, um L zu erzeugen. Das hängt stark vom Polynom ab, wie wir gleich sehen werden. Wir werden bald sehen, dass je zwei Zerfällungskörper von f isomorph sind.*

Beispiel 4.6.5. *Es sei $f(x) = x^2 + ax + b \in K[x]$ ein quadratisches Polynom ohne Nullstelle in $K[x]$ (und daher irreduzibel). In der Körpererweiterung $K[x]/(f)$ (vom Grad 2) hat f eine Nullstelle, und muss daher auch eine zweite besitzen. Für irreduzible quadratische Polynome ist ein Zerfällungskörper daher stets eine einfache Erweiterung vom Grad 2.*

Beispiel 4.6.6. *Betrachte $f(x) = x^n - 1 \in \mathbb{Q}[x]$, und es sei $\zeta_n := \exp(\frac{2\pi i}{n}) \in \mathbb{C}$. Dann ist $\mathbb{Q}(\zeta_n)$ ein Zerfällungskörper von $f(x)$. Es gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq n-1$, denn das Polynom $g_n(x) = x^{n-1} + \ldots + x + 1$ hat ζ_n als Nullstelle; daher ist das Minimalpolynom von ζ_n ein Teiler von $g(x)$. Ist $n = p$ eine Primzahl, so wissen wir, dass $g_p(x)$ irreduzibel ist, und daher $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Im Allgemeinen ist es schwerer, den Grad auszurechnen. Antwort: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, die Anzahl der Zahlen d mit $1 \leq d \leq n-1$, welche teilerfremd zu n sind. Beweis am Ende des Semesters.*

Beispiel 4.6.7. *Es sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Wir behaupten, dass $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) =: L$ ein Zerfällungskörper von $f(x)$ ist. Weil $f(x)$ in L die drei Nullstellen $z_1 := \sqrt[3]{2}, z_2 := \zeta_3\sqrt[3]{2}$ und $z_3 := \zeta_3^2\sqrt[3]{2}$ hat, zerfällt f über L in Linearfaktoren. Andererseits enthält jeder Körper $\mathbb{Q} \subset N \subset L$, über dem $f(x)$ zerfällt, die Elemente z_1 und $\frac{z_2}{z_1} = \zeta_3$. Somit zerfällt $f(x)$ über keinem echten Unterkörper von L. In Beispiel 4.3.13 haben wir gesehen, dass $[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}] = 6 = 3!$.*

Unser nächstes Ziel ist es, zu beweisen, dass je zwei Zerfällungskörper eines Polynoms isomorph sind. Allerdings gibt es im Allgemeinen mehr als einen solchen Isomorphismus, und das systematische Studium aller verschiedenen Isomorphismen wird im letzten Kapitel der Vorlesung im Zentrum stehen.

Eine große Rolle werden im folgenden Homomorphismen von Körpern spielen, und dafür führen wir einige Vokabeln ein.

Vokabeln 4.6.8. *Es sei K ein Körper und es seien $K \subset L$ und $K \subset F$ Körpererweiterungen. Ein K-*Homomorphismus *ist ein Körperhomomorphismus $\varphi : L \to F$, so dass $\varphi|_K = \mathrm{id}$. Wir erinnern daran, dass Körperhomomorphismen stets injektiv sind, siehe Satz 1.1.20.*

*Etwas allgemeiner sei $K \subset L$ eine Körpererweiterung und $\varphi_0 : K \to F$ ein Körperhomomorphismus. Ein φ_0-*Homomorphismus *$\varphi : L \to F$ ist ein Körperhomomorphismus, so dass $\varphi|_K = \varphi_0$.*

Ein Körperhomomorphismus $\varphi : L \to F$ induziert einen Ringhomomorphismus

$$\varphi_* : L[x] \to F[x]; \sum_k a_k x^k \mapsto \sum_k \varphi(a_k) x^k.$$

Satz 4.6.9. *Es sei $\varphi_0 : K \to L$ ein Körperhomomorphismus, und $K \subset K(y)$ sei eine einfache algebraische Erweiterung, und $f(x) \in K[x]$ sei das Minimalpolynom von y über K. Dann gilt*

1. *Ist $\varphi : K(y) \to L$ ein φ_0-Homomorphismus, so ist $\varphi(y)$ eine Nullstelle des Polynoms $(\varphi_0)_* f(x)$.*
2. *Die Abbildung*

$$\Lambda : \{\varphi : K(z) \to L | \varphi_0\text{-Homomorphismus}\} \to \{y | (\varphi_0)_* f(y) = 0\},$$

welche durch

$$\varphi \mapsto \varphi(z)$$

gegeben ist, ist bijektiv.

Beweis. (1): ist $f(x) = \sum_k a_k x^k$, so gilt

$$(\varphi_0)_* f(\varphi(y)) = \sum_k \varphi_0(a_k)\varphi(y)^k = \varphi(\sum_k a_k y^k) = \varphi(0) = 0.$$

(2), Injektivität von Λ: seien $\varphi, \varphi' : K(y) \to L$ zwei φ_0-Homomorphismen mit $\Lambda(\varphi) = \Lambda(\varphi')$, also $\varphi(y) = \varphi'(y)$. Weil jedes Element von $K(y)$ als $\sum_k b_k y^k$ mit $b_k \in K$ geschrieben werden kann, folgt

$$\varphi(\sum_k b_k y^k) = \sum_k \varphi(b_k y^k) = \sum_k \varphi(b_k)\varphi(y^k) = \sum_k \varphi_0(b_k)\varphi(y)^k.$$

und mit derselben Rechnung

$$\varphi'(\sum_k b_k y^k) = \sum_k \varphi_0(b_k)\varphi(y)^k,$$

also $\varphi = \varphi'$.

(2), Surjektivität von Λ: Aus Satz 4.3.7 folgt, dass es einen Isomorphismus $K(y) \cong K[x]/(f)$ gibt, unter dem y auf die Restklasse $[x]$ geht. Wir dürfen daher ohne Beschränkung der Allgemeinheit annehmen, dass $K(y) = K[x]/(f)$ und $y = [x]$.

Es sei nun $z \in L$ eine Nullstelle von $(\varphi_0)_* f$, und betrachte den Einsetzungshomomorphismus

$$\phi : K[x] \to L; g(x) \mapsto (\varphi_0)_* g(z).$$

Dies ist ein Ringhomomorphismus, dessen Kern von einem normierten Polynom $h \in K[x]$ erzeugt wird. Nach dem ersten Teil des Satzes ist $(\varphi_0)_* f(z) = 0$, also $f \in (h)$. Es folgt $h | f$. Nun ist aber h keine Einheit, denn sonst wäre ϕ_z die Nullabbildung, was sie offensichtlich nicht ist. Weil darüber hinaus f irreduzibel ist, folgt $h = f$.

Wegen Satz 3.2.9 gibt es daher einen Homomorphismus

$$\varphi : K[x]/(f) \to L$$

mit $\varphi([g]) = (\varphi_0)_* g(z)$ für alle $g \in K[x]$. Offenbar ist $\varphi([x]) = z$. □

Wir wollen nun Satz 4.6.9 auf den Fall mehrfacher Körpererweiterungen verallgemeinern. Hierfür eine Sprechweise. Es sei $f(x) \in K[x]$ ein normiertes Polynom, und wir schreiben

$$f(x) = \left(\prod_{j=1}^{n} (x - z_j) \right) g(x),$$

wobei $g(x)$ entweder gleich 1 oder vom Grad ≥ 2 ist und keine Nullstellen in K besitzt (das geht nach Korollar 1.3.8). Wir sagen, dass $f(x)$ *keine mehrfachen Nullstellen in K hat*, wenn die z_j's paarweise verschieden sind.

Theorem 4.6.10. *Es sei $\varphi_0 : K \to L$ ein Körperhomomorphismus und es sei $K \subset K(y_1, \ldots, y_r)$ eine algebraische (insbesondere endliche) Körpererweiterung. Es sei $f(x) \in K[x]$ ein normiertes Polynom, so dass $y_1, \ldots, y_r$ Nullstellen von f sind, und es sei angenommen, dass $(\varphi_0)_* f$ in $L[x]$ in Linearfaktoren zerfalle. Dann gilt*

1. *es gibt einen φ_0-Homomorphismus $\varphi : K(y_1, \ldots, y_r) \to L$,*
2. *die Anzahl der φ_0-Homomorphismen $K(y_1, \ldots, y_r) \to L$ ist höchstens $[K(y_1, \ldots, y_r) : K]$,*
3. *es gibt genau $[K(y_1, \ldots, y_r) : K]$ viele φ_0-Homomorphismen, wenn $(\varphi_0)_* f(x)$ keine mehrfachen Nullstellen in L hat.*

Für den Beweis benötigen wir ein Lemma. Für einen Körper K und $g(x), f(x) \in K[x]$ sei der (normierte) größte gemeinsame Teiler in $K[x]$ mit

$$\mathrm{ggT}_K(f, g) \in K[x]$$

bezeichnet.

Lemma 4.6.11. *Es sei $K \subset L$ eine Körpererweiterung und $f(x), g(x) \in K[x]$. Dann gilt*

$$\mathrm{ggT}_L(f, g) = \mathrm{ggT}_K(f, g).$$

Beweis. Übung. □

Beweis von Theorem 4.6.10. Dies ist im wesentlichen ein Induktionsbeweis, und es sei zunächst der mathematische Kern des Induktionsschrittes diskutiert. Am Ende werden wir sehen, wie die einzelnen Teilaussagen zu einem Induktionsbeweis zusammengeflickt werden.

Es sei $N := K(y_1, \ldots, y_{j-1})$ und es sei $\varphi_1 : N \to L$ ein φ_0-Homomorphismus, der zunächst festgehalten werde. Ferner schreibe $y := y_j$ und beachte, dass

$$K(y_1, \ldots, y_j) = N(y).$$

Sei des weiteren $g(x) \in N[x]$ das Minimalpolynom von y über N. Der erste Schritt ist es, zu zeigen, dass

1. $(\varphi_1)_* g$ eine Nullstelle in L hat,
2. dass $(\varphi_1)_* g$ über L in Linearfaktoren zerfällt, und
3. dass die Linearfaktoren von $(\varphi_1)_* g$ in L paarweise verschieden sind, wenn $(\varphi_0)_* f$ einfache Nullstellen in L hat.

Weil $g(x)$ sowie $f(x)$ eine gemeinsame Nullstelle in $N(y)$ haben (nämlich y), sind $g, f \in N(y)[x]$ nicht teilerfremd. Aus Lemma 4.6.11 ergibt sich, dass $g(x)$ und $f(x)$ in $N[x]$ ncht teilerfremd sind. Aber $g(x)$ ist in $N[x]$ irreduzibel, und daher folgt

$$g(x)|f(x).$$

Also gilt auch

$$(\varphi_1)_* g(x)|(\varphi_1)_* f(x) = (\varphi_0)_* f(x);$$

die Gleichung stimmt, denn die Koeffizienten von $f(x)$ sind aus K, und φ_1 ist ein φ_0-Homomorphismus. Aus der Eindeutigkeit der Primfaktorzerlegung in $L[x]$ folgt, dass $(\varphi_1)_* g$ in Linearfaktoren zerfällt, und dass diese verschieden sind, wenn die von f es sind. Damit sind die obigen drei Behauptungen bewiesen. Nun argumentieren wir wie folgt:

(1) Es gibt mindestens einen φ_1-Homomorphismus $N(y) \to L$. Dies folgt aus Satz 4.6.9, zusammen mit der Tatsache, dass $(\varphi_1)_* g$ eine Nullstelle in L hat.
(2) Die Anzahl dieser φ_1-Homomorphismen ist höchstens $[N(y) : N]$: Nach Satz 4.6.9 ist die Anzahl dieser φ_1-Homomorphismen gleich der Anzahl der Nullstellen von $(\varphi_1)_* g$ in L, und daher höchstens $\deg(g)$, und weil g das Minimalpolynom von y über N ist, ist $[N(y) : N] = \deg(g)$.
(3) Die Anzahl dieser φ_1-Homomorphismen ist genau $[N(y) : N]$, wenn $(\varphi_0)_* f$ keine mehrfachen Nullstellen in L hat. Denn dann hat $(\varphi_* g)$ ebenfalls keine mehrfachen Nullstellen, und also genau $\deg(g) = [N(y) : N]$ viele Nullstellen in L, und die Behauptung folgt aus Satz 4.6.9.

Um diese Aussagen zu einem Induktionsbeweis zusammenzuflicken, führen wir folgende Notation ein: $K_0 := K$ und $K_j := K(y_1, \ldots, y_j) = K_{j-1}(y_j)$. Es sei

$$M_j := \{\varphi : K_j \to L | \varphi_0 - \text{Homomorphismus}\}.$$

Ferner sei

$$\Lambda_j : M_j \to M_{j-1};\ \Lambda_j(\varphi) := \varphi|_{K_{j-1}}.$$

Die Ergebnisse des ersten Beweisteils können wie folgt umformuliert werden.

(1) Λ_j ist surjektiv für alle j. Mit der Notation aus dem ersten Teil des Beweises bedeutet dies nichts anderes, als dass jeder φ_0-Homomorphismus $\varphi_1 : N \to L$ zu einem φ_0-Homomorpismus $N(y) \to L$ fortgesetzt werden kann, was wir gerade gesehen haben.
(2) Ist $\varphi_1 \in M_{j-1}$, so ist $|\Lambda_j^{-1}(\varphi_1)| \leq [K_j : K_{j-1}]$. Das heißt, dass die Anzahl der φ_1-Homomorphismen $N(y) \to L$ höchstens gleich $[N(y) : N]$ ist (s.o.).
(3) Wenn $(\varphi_0)_* f$ keine mehrfachen Nullstellen in L hat, so gilt $|\Lambda_j^{-1}(\varphi_1)| = [K_j : K_{j-1}]$ für alle $\varphi_1 \in M_{j-1}$. Das ist die Aussage, dass die Zahl der φ_1-Homomorpismen $N(y) \to L$ gleich $[N(y) : N]$ ist, wenn $(\varphi_0)_* f$ keine mehrfachen Nullstellen hat.

Nun zum Induktionsbeweis. Wir zeigen, dass für $j = 0, \ldots, r$ folgendes gilt:

(1) $M_j \neq \emptyset$
(2) $|M_j| \leq [K_j : K_0]$,
(3) $|M_j| = [K_j : K_0]$, wenn $(\varphi_0)_* f$ keine mehrfachen Nullstellen hat.

Für $j = r$ ergibt sich der Satz. Der Fall $j = 0$ ist klar, denn $M_0 = \{\varphi_0\}$. Induktionsschritt $j - 1 \to j$: M_j ist nicht leer, weil $\Lambda_j : M_j \to M_{j-1}$ surjektiv ist und weil

$M_{j-1} \neq \emptyset$. Ferner ist

$$|M_j| = \sum_{\varphi_1 \in M_{j-1}} |\Lambda_j^{-1}(\varphi_1)| \leq \sum_{\varphi_1 \in M_{j-1}} [K_j : K_{j-1}] = |M_{j-1}|[K_j : K_{j-1}] \leq$$

$$\leq [K_{j-1} : K_0][K_j : K_{j-1}] = [K_j : K_0],$$

und Gleichheit gilt, wenn $(\varphi_0)_* f$ keine mehrfachen Nullstellen in L hat. □

Korollar 4.6.12. *Je zwei Zerfällungskörper eines Polynoms $f(x) \in K[x]$ sind isomorph.*

Für den Beweis nutzen wir das folgende Prinzip aus der linearen Algebra.

Lemma 4.6.13. *Es sei V ein endlich-dimensionaler K-Vektorraum und $F : V \to V$ sei linear. Dann ist F genau dann surjektiv, wenn F injektiv ist.*

Beweis. Dimensionsformel:

$$\dim(V) = \dim(\ker(F)) + \dim(\mathrm{im}(F)).$$ □

Beweis von Korollar 4.6.12. Es seien $K \subset L$ und $K \subset N$ zwei Zerfällungskörper von $f(x)$. Aus Theorem 4.6.10 folgt die Existenz von K-Homomorphismen

$$\varphi : L \to N,\ \psi : N \to L.$$

Wir behaupten, dass φ und ψ Isomorphismen sind. Weil Körperhomomorphismen stets injektiv sind, sind

$$\psi \circ \varphi : L \to L,\ \varphi \circ \psi : N \to N$$

injektiv. Nun ist L ein endlich-dimensionaler K-Vektorraum, und der K-Homomorphismus $\psi \circ \varphi$ ist injektiv. Ferner ist $\psi \circ \varphi$ K-linear, denn für $a \in K$ und $b \in L$ gilt

$$\psi \circ \varphi(ab) = \psi \circ \varphi(a)\psi \circ \varphi(b) = a\psi \circ \varphi(b).$$

Daher ist $\psi \circ \varphi$ nach Lemma 4.6.13 auch surjektiv. Es folgt, dass ψ auch surjektiv ist, also ist ψ ein Isomorphismus. Mit demselben Argument folgt, dass φ ein Isomorphismus ist. □

Korollar 4.6.14. *Es sei $K \subset L$ eine endliche algebraische Erweiterung. Dann gibt es höchstens $[L : K]$ viele K-Homomorphismen $L \to L$. Ist L ein Zerfällungskörper eines Polynoms, das in L keine mehrfachen Nullstellen hat, so gibt es genau $[L : K]$ solche Körperhomomorphismen.*

Beweis. Schreibe $L = K(y_1, \ldots, y_r)$. Es sei $g_i(x) \in K[x]$ das Minimalpolynom von y_i und $f(x) = \prod_{i=1}^r g_i(x) \in K[x]$. Das Polynom $f(x)$ muss auch in $L[x]$ nicht in Linearfaktoren zerfallen, aber wir können einen Zerfällungskörper $L \subset N$ von f wählen.

Jeder K-Homomorphismus $L \to L$ kann insbesondere als K-Homomorphismus $L \to N$ angesehen werden, und nach Theorem 4.6.10 gibt es höchstens $[L : K]$ viele solche Homomorphismen.

Ist L ein Zerfällungskörper eines Polynoms, dass keine mehrfachen Nullstellen hat, so besagt Theorem 4.6.10, dass es genau $[L : K]$ solcher Homomorphismen gibt. □

4.7. **Mehrfache Nullstellen und Separabilität.** In Theorem 4.6.10 tauchte das Kriterium auf, dass ein Polynom $f(x)$ in seinem Zerfällungskörper keine mehrfachen Nullstellen hat. Es ist zunächst nicht klar, wie man einem $f(x)$ ansehen kann, dass es diese Eigenschaft hat, ohne die Zerlegung in Linearfaktoren über dem Zerfällungskörper explizit zu berechnen.

Definition 4.7.1. *Sei K ein Körper und $f(x) \in K[x]$ ein Polynom. Dann heißt $f(x)$* separabel*, wenn f über einem (und dann jedem) Zerfällungskörper in paarweise verschiedene Linearfaktoren zerfällt.*

Mit dieser Begriffsbildung können wir Korollar 4.6.14 griffiger formulieren.

Satz 4.7.2. *Es sei K ein Körper und $f(x) \in K[x]$ ein separables Polynom und es sei $K \subset L$ ein Zerfällungskörper. Dann gibt es genau $[L : K]$ viele K-Isomorphismen $L \to L$.* □

Wie überprüft man, ob ein Polynom separabel ist, ohne den Zerfällungskörper und eine Zerlegung in Linearfaktoren zu berechnen? Es gibt ein bequemes Kriterium, das nur auf den Grundkörper K Bezug nimmt. Hierfür führen wir die *formale Ableitung* eines Polynoms ein.

Definition 4.7.3. *Es sei $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$ ein Polynom. Die* formale Ableitung *von f ist das Polynom*

$$f'(x) := \sum_{k=0}^{n} k a_k x^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k \in K[x].$$

Der Name rührt natürlich daher, dass im Fall $K = \mathbb{R}$ die formale Ableitung mit der aus der Analysis bekannten Ableitung übereinstimmt.

Lemma 4.7.4. *Die formale Ableitung hat folgende Eigenschaften (für $f(x), g(x) \in K[x]$ und $a \in K$)*

(1) $(f+g)'(x) = f'(x) + g'(x)$,
(2) $(af)'(x) = af'(x)$,
(3) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

Beweis. Die ersten beiden Eigenschaften sind trivial, und die dritte lässt sich mittels der ersten beiden auf den Fall $f(x) = x^n$ und $g(x) = x^m$ reduzieren, in welchem man die Formel einfach nachrechnet. □

Lemma 4.7.5. *Sei $f(x) \in K[x]$ ein Polynom. Dann hat $f(x)$ keine mehrfachen Nullstellen in K genau dann, wenn $f(x), f'(x)$ keine gemeinsame Nullstelle in K haben.*

Beweis. Wenn $f(x)$ eine mehrfache Nullstelle $z \in K$ hat, so können wir $f(x) = (x-z)^2 g(x)$ schreiben, berechnen

$$f'(x) = 2(x-z)g(x) + (x-z)^2 g'(x)$$

und folgern, dass $f'(z) = 0$, so dass $f(x)$ und $f'(x)$ in K eine gemeinsame Nullstelle haben. Ist umgekehrt $f(z) = f'(z) = 0$, so schreibe $f(x) = (x-z)h(x)$ und berechne

$$f'(x) = h(x) + (x-z)h'(x).$$

Wegen $f'(z) = 0$ folgt

$$h(z) = 0,$$

also können wir $h(x) = (x-z)k(x)$ schreiben, und folglich

$$f(x) = (x-z)^2 k(x). \qquad \square$$

Satz 4.7.6. *Es sei $f(x) \in K[x]$ ein Polynom. Die folgenden Aussagen sind äquivalent.*

1. *Ist $K \subset N$ eine Körpererweiterung, so hat f keine mehrfachen Nullstellen in N.*
2. *$f(x), f'(x) \in K[x]$ sind teilerfremd.*
3. *$f(x)$ ist separabel.*

Beweis. Es sei $K \subset L$ ein Zerfällungskörper von f. $1 \Rightarrow 3$ ist trivial (wende (1) auf $N = L$ an). $3 \Rightarrow 2$: Nach Lemma 4.7.5 sind $f'(x), f(x) \in L[x]$ teilerfremd, und aus Lemma 4.6.11 folgt, dass $f(x)$ und $f'(x)$ in $K[x]$ teilerfremd sind.

$2 \Rightarrow 1$: Sei $K \subset N$ irgendeine Körpererweiterung. Wieder aus Lemma 4.6.11 folgt, dass $f(x)$, $f'(x)$ in $N[x]$ teilerfremd sind; diese beiden Polynome haben daher in N keine gemeinsame Nullstelle. Aus Lemma 4.7.5 folgt, dass $f(x)$ in N keine mehrfachen Nullstellen hat. $\square$

Satz 4.7.7. *Es sei K ein Körper der Charakteristik 0 und es sei $f(x) \in K[x]$ normiert. Dann ist f separabel.*

Beweis. Sei $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$. Dann ist der Leitkoeffizient von $f'(x)$ gleich $n \neq 0$ (letzteres, weil K die Charakteristik 0 hat). Weil $\deg(f') = n-1$ und weil f irreduzibel ist, müssen f und f' teilerfremd sein. Daher ist $f(x)$ nach Satz 4.7.6 separabel. $\square$

Satz 4.7.7 lässt sich auf nicht irreduzible Polynome verallgemeinern.

Lemma 4.7.8. *Es sei K ein Körper und $f(x)$ und $g(x) \in K[x]$. Dann gilt:*

1. *Wenn f und g separabel und teilerfremd sind, dann ist fg separabel.*
2. *Wenn fg separabel ist, dann sind f und g separabel.*

Beweis. (1) Wir zeigen: ist fg nicht separabel, so ist f oder g nicht separabel, oder f und g sind nicht teilerfremd. Wenn fg nicht separabel ist, so ist $\mathrm{ggT}(fg, (fg)') \neq 1$, es gibt also ein irreduzibles Polynom p mit $p|fg$ und $p|(fg)'$. Weil p prim ist, so gilt $p|f$ oder $p|g$.

Sei $p|f$. Wegen $(fg)' = f'g + fg'$ und $p|(fg)'$ folgt

$$p|((fg)' - fg') = f'g,$$

also $p|f'$ oder $p|g$. Im ersten Fall ist f nicht separabel, im zweiten Fall sind f und g nicht teilerfremd.

Sei $p|g$. Es folgt (analog zur obigen Argumentation)

$$p|((fg)' - f'g) = fg',$$

also $p|f$ oder $p|g'$. Im ersten Fall sind f und g nicht teilerfremd, im zweiten Fall ist g nicht separabel.

(2) Wir zeigen: ist f oder g nicht separabel, so ist fg nicht separabel. Sei also p irreduzibel und $p|f$, $p|f'$. Dann gilt $p|fg$, und wegen $(fg)' = f'g + fg'$ ist p auch ein Teiler von $(fg)'$. $\square$

Satz 4.7.9. *Es sei K ein Körper der Charakteristik 0 und $f(x) \in K[x]$. Es sind äquivalent:*

1. *f ist separabel,*

(2) *f ist Produkt paarweise verschiedener irreduzibler Faktoren.*

Beweis. $1 \Rightarrow 2$: wir zeigen $\neg 2 \Rightarrow \neg 1$, indem wir nachweisen, dass ein Polynom der Form $f(x) = g(x)^2 h(x)$ mit nichtkonstanten $g(x)$ nicht separabel ist. Es gilt

$$f'(x) = g(x)(2g'(x)h(x) + g(x)h'(x)),$$

also ist $g(x)$ ein gemeinsamer Teiler von $f(x)$ und $f'(x)$, also $f(x)$ nicht separabel.

$2 \Rightarrow 1$: dies folgt induktiv aus Satz 4.7.7 und Lemma 4.7.8. □

Bemerkung 4.7.10. *In Charakteristik p kann es durchaus passieren, dass ein Polynom von positivem Grad verschwindende formale Ableitung hat. Ist etwa $f(x) = x^p$, so ist $f'(x) = px^{p-1} = 0$. Nun ist $x^p \in \mathbb{F}_p[x]$ natürlich nicht irreduzibel. Auf der anderen Seite kann zeigen, mit etwas größerem Aufwand, dass der Satz für endliche Körper trotzdem stimmt. In gewissen unendlichen Körpern endlicher Charakteristik gibt es ein Problem, das im Kontext dieser Vorlesung ignoriert werden kann.*

5. Konstruktionen mit Zirkel und Lineal

Wir verlassen nun für eine Weile die Sphäre der abstrakten Körpererweiterungen, und wenden uns konkreten geometrischen Problemen zu. Wir erinnern uns daran, dass die komplexen Zahlen $\mathbb{C}$ als $\mathbb{R}^2$ mit einer speziellen Multiplikation definiert worden sind. Aus der elementaren analytischen Geometrie ist das *Skalarprodukt* in $\mathbb{R}^2$ bekannt; es ist definiert durch

$$\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle := x_1 y_1 + x_2 y_2.$$

Unter dem Isomorphismus $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto x_1 + ix_2 \in \mathbb{C}$ kann das Skalarprodukt alternativ als

$$\langle z_1, z_2 \rangle = \Re(\overline{z_1} z_2)$$

definiert werden. Wir sagen, dass $z, w \in \mathbb{C}$ *orthogonal* oder *senkrecht* zueinander sind, wenn $\langle z, w \rangle = 0$ gilt.

5.1. **Konstruktionen mit Zirkel und Lineal.** Zunächst wollen wir klären, was Konstruierbarkeit mit Zirkel und Lineal heißen soll.

Definition 5.1.1. *Seien $z_0 \neq z_1 \in \mathbb{C}$. Die* Gerade $\mathrm{Ge}(z_0, z_1)$ *durch z_0 und z_1 ist die Menge*

$$\mathrm{Ge}(z_0, z_1) := \{tz_0 + (1-t)z_1, |t \in \mathbb{R}\} \subset \mathbb{C}.$$

Der Kreis $\mathrm{Kr}(z, r)$ *um z mit Radius r ist die Menge*

$$\mathrm{Kr}(z, r) := \{w \in \mathbb{C} || w - z| = r\} = \{z + re^{it}, |t \in \mathbb{R}\} \subset \mathbb{C}.$$

Für $S \subset \mathbb{C}$ sei $\mathrm{GK}(S)$ *die Menge aller Geraden* $\mathrm{Ge}(z_0, z_1)$ *und aller Kreise* $\mathrm{Kr}(z, |z_1 - z_0|)$*, wobei $z, z_0, z_1 \in S$.*

Definition 5.1.2. *Es sei $S \subset \mathbb{C}$. Ein Punkt $z \in \mathbb{C}$ ist* mit Zirkel und Lineal aus S konstruierbar*, wenn es eine Folge von Punkten*

$$z_1, z_2, \ldots, z_n = z$$

in $\mathbb{C}$ gibt, so dass gilt: Für jedes $i = 1, \ldots, n$ ist z_i ein Schnittpunkt zweier verschiedener Elemente aus $\mathrm{GK}(S \cup \{z_1, \ldots, z_n\})$*. (Dies ist so zu verstehen, dass z_1 ein Schnittpunkt zweier verschiedener Elemente aus* $\mathrm{GK}(S)$ *ist.)*

Wir bezeichnen mit

$$\mathbb{K} \subset \mathbb{C}$$

die Menge aller komplexen Zahlen, die aus $S = \{0, 1\}$ *mit Zirkel und Lineal konstruierbar sind, oder kurz die Menge aller konstruierbaren Zahlen.*

Wir wollen jetzt die Frage untersuchen, wie entschieden werden kann, ob eine gegebene komplexe Zahl $z \in \mathbb{C}$ zur Menge $\mathbb{K}$ gehört. Konkrete Beispiele dafür sind folgende, jede mit einem klassischen geometrischen Problem verbunden:

Fragen 5.1.3. (1) *Sind, für eine gegebene Zahl* $n \in \mathbb{N}$*, die* n*ten Einheitswurzeln* $\exp(2\pi i/n)^k$*, in* $\mathbb{K}$*? Dies entspricht der Frage, welches reguläre* n*-Eck mit Zirkel und Lineal konstruierbar ist.*

(2) *Ist* $\sqrt[3]{2} \in \mathbb{K}$*? Das ist die Frage, ob die* Verdoppelung des Würfels *mit Zirkel und Lineal durchführbar ist.*

(3) *Ist* $\pi \in \mathbb{K}$*? Bekanntlich ist dies der Flächeninhalt des Einheitskreises. Dieses Problem ist auch als die* Quadratur des Kreises *bekannt.*

(4) Dreiteilung eines Winkels*: falls* $z = e^{it} \in \mathbb{K}$*,* $t \in \mathbb{R}$*, ist dann* $e^{\frac{1}{3}it} \in \mathbb{K}$*?*

Um diese Fragen angehen zu können, werden wir sie mit der Theorie der Körpererweiterungen in Verbindung bringen. Wir beginnen mit einigen Grundkonstruktionen.

(1) $\mathbb{N} \subset \mathbb{K}$, d.h. jede natürliche Zahl n ist konstruierbar. Der Induktionsanfang $n = 1$ ist klar. Die reelle Achse ist $\mathrm{Ge}(0, 1)$, und $n + 1$ und $n - 1$ sind die Schnittpunkte von $\mathrm{Ge}(0, 1)$ und $\mathrm{Kr}(n, 1)$. Also $n \in \mathbb{K} \Rightarrow n + 1 \in \mathbb{K}$.

(2) $z \in \mathbb{K} \Rightarrow -z \in \mathbb{K}$. Denn $\mathrm{Ge}(0, z)$ und $\mathrm{Kr}(0, |z|)$ gehören beide zu $\mathrm{GK}(0, z)$, und die Schnittpunkte sind z sowie $-z$.

(3) Mit $z, w \in \mathbb{K}$ ist auch der Mittelpunkt $\frac{1}{2}(z+w)$ in $\mathbb{K}$, denn die beiden Kreise $\mathrm{Kr}(z, |z - w|)$ und $\mathrm{Kr}(w, |z - w|)$ schneiden sich in zwei Punkten p und q, und die Gerade $\mathrm{Ge}(p, q)$ schneidet die Gerade $\mathrm{Ge}(z, w)$ genau in $\frac{1}{2}(z + w)$.

(4) Mit $z, w \in \mathbb{K}$ liegt auch $z+w \in \mathbb{K}$. Hierfür betrachte die Gerade $\mathrm{Ge}(0, \frac{1}{2}(z+w))$; sie schneidet den Kreis $\mathrm{Kr}(\frac{1}{2}(z+w), |\frac{1}{2}(z+w)|)$ genau in 0 und $z+w$.

(5) Sei $y, z, w \in \mathbb{K}$. Die zur Gerade $\mathrm{Ge}(y, z)$ senkrechte Gerade durch den Punkt w kann wie konstruiert werden. Wähle $n \in \mathbb{N}$ groß genug, dass sich $\mathrm{Ge}(y, z)$ und $\mathrm{Kr}(w, n)$ in genau zwei Punkten $p, q \in \mathbb{K}$ schneiden. Die Kreise $\mathrm{Kr}(p, |p-q|)$ und $\mathrm{Kr}(q, |p-q|)$ schneiden sich in genau zwei Punkten $r, s \in \mathbb{K}$, und $\mathrm{Ge}(r, s)$ ist die gesuchte Gerade.

(6) Für $y, z, w \in \mathbb{K}$ kann die zu $\mathrm{Ge}(y, z)$ parallel Gerade durch w wie folgt konstruiert werden. Man nimmt die zu $\mathrm{Ge}(y, z)$ senkrechte Gerade durch w, die Parallele ist die zur zweiteren senkrechte Gerade durch w.

Satz 5.1.4. $\mathbb{K}$ *ist ein Unterkörper von* $\mathbb{C}$*. Es gilt* $\overline{\mathbb{K}} = \mathbb{K}$*, d.h.* $z \in \mathbb{K} \Rightarrow \overline{\Delta z} \in \mathbb{K}$*. Ferner ist* $\mathbb{K}$ quadratisch abgeschlossen*, d.h. zu* $z \in \mathbb{K}$ *sind die beiden Wurzeln* $\pm\sqrt{z} \in \mathbb{C}$ *Elemente von* $\mathbb{K}$*.*

Beweis. Wir haben in die Definition eingebaut, dass $0, 1 \in \mathbb{K}$. Wir haben oben gesehen, dass mit $z, w \in \mathbb{K}$ auch $z+w$ und $-z$ in $\mathbb{K}$ liegen. Seien nun $z, w \in \mathbb{K}$. Wir zeigen jetzt:

(1) $|z| \in \mathbb{K}$; es ist einer der Schnittpunkte von $\mathrm{Ge}(0, 1)$ und $\mathrm{Kr}(0, |z|)$.

(2) $\Re(z), \overline{z}, \Im(z) \in \mathbb{K}$. Sei G die zur Gerade $\mathrm{Ge}(0, 1)$ senkrechte Gerade durch z. Dann schneiden sich G und $\mathrm{Ge}(0, 1)$ genau in $\Re(z)$. Hieraus folgt $\Re(z) \in \mathbb{K}$. Ferner schneidet G den Kreis $\mathrm{Kr}(0, |z|)$ genau in z und $\overline{z}$. Daher ist $\overline{z} \in \mathbb{K}$.

Des weiteren ist $i\Im(z) = z - \Re(z) \in \mathbb{K}$, und $\Im(z) = \pm|i\Im(z)|$ liegt ebenfalls in $\mathbb{K}$.

(3) $x \in \mathbb{K} \cap \mathbb{R} \Rightarrow ix \in \mathbb{K}$, denn ix ist einer der beiden Schnittpunkte von $\mathrm{Ge}(0, i)$, der zu $\mathrm{Ge}(0, 1)$ senkrechten Gerade durch i, mit dem Kreis $\mathrm{Kr}(0, |x|)$.

(4) $zw \in \mathbb{K}$. Wir nehmen zuerst an, dass $x, y \in \mathbb{R} \cap \mathbb{K}$ und $x, y > 0$ gilt, und zeigen, dass $xy \in \mathbb{K}$. Betrachte dazu die Gerade $\mathrm{Ge}(iy, 1)$ und die dazu parallele Gerade G durch den Punkt $x + 1$. Der Schnittpunkt von G mit der imaginären Achse ist $i(y + xy)$. Also $y + xy \in \mathbb{K}$, somit $xy \in \mathbb{K}$. Der allgemeine Fall folgt mit der letzten Aussage und Trennung von Realteil und Imaginärteil.

(5) $\frac{1}{z} \in \mathbb{K}$. Wegen $\frac{1}{z} = \frac{x-iy}{x^2+y^2}$ reicht es, zu zeigen, dass $x \in \mathbb{K} \cap \mathbb{R}$, $x > 0 \Rightarrow \frac{1}{x} \in \mathbb{K}$. Betrachte hierfür $\mathrm{Ge}(0, 1 + ix)$ und die zur imaginären Achse senkrechte Gerade G durch i. Der Schnittpunkt von G und $\mathrm{Ge}(0, 1 + ix)$ ist $\frac{1}{x} + i$, also $\frac{1}{x} \in \mathbb{K}$.

Daraus folgen alle Behauptungen des Satzes, bis auf die quadratische Abgeschlossenheit. Sei also $z \in \mathbb{K}$ und wir müssen zeigen, dass $\sqrt{z} \in \mathbb{K}$. Für $z = 0, 1, -1$ ist nichts zu zeigen, denn wir wissen schon, dass $0, \pm i, \pm 1 \in \mathbb{K}$. Sei zunächst $|z| = 1$, $z \neq \pm 1$. Dann ist $\frac{1+z}{|1+z|}$ eine Quadratwurzel von z, wie man aus

$$\left(\frac{1+z}{|1+z|}\right)^2 = \frac{(1+z)(1+z)}{(1+z)(1+\overline{z})} = \frac{(1+z)(1+z)}{(1+z)(1+\frac{1}{z})} = \frac{1+2z+z^2}{2+z+\frac{1}{z}} = z\frac{1+2z+z^2}{2z+z^2+1} = z$$

sieht (beachte, dass $\overline{z} = z^{-1}$ gilt, wenn $|z| = 1$). Aber nach dem bis hierhin gezeigten ist $\frac{1+z}{|1+|z|} \in \mathbb{K}$, wenn $z \in \mathbb{K}$ und $|z| = 1$.

Nun sei $x \in \mathbb{K} \cap \mathbb{R}$, $x > 0$. Wenn wir zeigen können, dass $\sqrt{x} \in \mathbb{K}$, ist der Beweis des Satzes nach folgendem Argument fertig. Eine beliebige Zahl $z \in \mathbb{K}$ werde in der Form $|z|\frac{[z}{|z|}$ geschrieben. Beide Faktoren liegen in $\mathbb{K}$, und weil jeder Faktor eine Quadratwurzel in $\mathbb{K}$ besitzt, dann auch z.

Sei nun $x > 0$, und wir wollen zeigen, dass $\sqrt{x} \in \mathbb{K}$. Weil $\frac{1}{x}$ in $\mathbb{K}$ liegt, dürfen wir ohne Beschränkung der Allgemeinheit annehmen, dass $x < 1$ gilt. Der Kreis $K = \mathrm{Kr}(1+x, \frac{1}{2}(1+x))$ und die zu $\mathrm{Ge}(0, 1)$ senkrechte Gerade G durch 1 schneiden sich in zwei Punkten p und q, und $|p - 1| = \sqrt{z}$. Dies folgt aus den Sätzen von Thales und Pythagoras. □

Wir wollen nun den Körper $\mathbb{K}$ genauer untersuchen, und eine körpertheoretische Charakterisierung der konstruierbaren Zahlen erarbeiten, welche es dann ermöglicht, die Fragen 5.1.3 zu beantworten.

Satz 5.1.5 (Körpertheoretische Charakterisierung der konstruierbaren Zahlen)**.** *Sei $z \in \mathbb{C}$. Es sind äquivalent*

(1) $z \in \mathbb{K}$,

(2) *es existiert eine Folge*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{C}$$

von Körpererweiterungen, so dass $z \in K_n$ und so dass $[K_i : K_{i-1}] = 2$, für $i = 1, \ldots, n$.

Beweis. $2 \Rightarrow 1$: Induktion über n. Der Fall $n = 0$ ist klar, weil $K_0 = \mathbb{Q} \subset \mathbb{K}$. Für den Induktionschritt dürfen wir annehmen, dass $z \notin K_{n-1}$, $z \in K_n$. Der Zwischenkörper $K_{n-1} \subset K_{n-1}(z) \subset K_n$ muss aus Gradgründen mit K_n übereinstimmt. Es folgt,

dass das Minimalpolynom $f(x)$ von z über K_{n-1} den Grad 2 hat. Schreibe $f(x) = x^2 + a_1 x + a_0$. Dann ist

$$z = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^4}{4} - a_0}.$$

Weil $a_0, a_1 \in K_{n-1} \subset \mathbb{K}$ und weil $\mathbb{K}$ quadratisch abgeschlossen ist, folgt $z \in \mathbb{K}$.

Für die Richtung $1 \Rightarrow 2$ ist ein weiteres Lemma nötig.

Lemma 5.1.6. *Es sei $\mathbb{Q} \subset L \subset \mathbb{C}$ ein Zwischenkörper, und es gelte*

$$\overline{L} := \{\overline{z} | z \in L\} = L$$

(mit anderen Worten, falls $z \in L$, so ist auch $\overline{z} \in L$). Es sei ferner $y \in \mathbb{C}$ ein Schnittpunkt zweier verschiedener Elemente aus $\mathrm{GK}(L)$. Dann gilt entweder $y \in L$, oder y ist algebraisch über L, mit Grad $[L(y) : L] = 2$, und es gilt $\overline{L(y)} = L(y)$.

Der Beweis sei für den Moment aufgeschoben, und wir wollen zuerst einsehen, wie die Implikation $1 \Rightarrow 2$ des Satzes aus dem Lemma folgt. Sei also $z \in \mathbb{K}$. Nach Definition gibt es eine Folge von Punkten

$$z_1, z_2, \ldots, z_m = z,$$

so dass gilt: Für jedes $i = 1, \ldots, m$ ist z_i ein Schnittpunkt zweier verschiedener Elemente aus $\mathrm{GK}(\{0,1\} \cup \{z_1, \ldots, z_{i-1}\})$. Wir setzen nun provisorisch

$$L_0 = \mathbb{Q};\ L_k := \mathbb{Q}(z_1, \ldots, z_k),$$

so dass

$$\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_m \tag{5.1.7}$$

und $z \in L_m$. Wir wissen, dass z_k ein Schnittpunkt zweier verschiedener Elemente aus $\mathrm{GK}(L_{k-1})$ ist. Nach Lemma 5.1.6 gilt entweder $z_k \in L_{k-1}$ und daher $L_k = L_{k-1}$, oder $[L_k : L_{k-1}]$. Induktiv sehen wir ebenfalls $\overline{L_k} = L_k$, so dass das Lemma wiedderholt angewandt werden kann.

Wir streichen nun aus der Folge (5.1.7) alle L_i mit $L_i = L_{i-1}$ heraus und haben eine Folge wie im Satz behauptet gefunden. □

Beweis von Lemma 5.1.6. Wir beginnen mit einer Vorbemerkung. Ist $\overline{L} = L$, so gilt für $z \in L$, dass

$$\begin{aligned} \Re(z) &= \frac{1}{2}(z + \overline{z}) \in L, \\ i\Im(z) &= z - \Re(z) \in L, \\ |z|^2 &= z\overline{z} \in L. \end{aligned}$$

Wir haben nun drei Fälle zu unterscheiden.

(1) y ist der Schnittpunkt zweier Geraden. Wir behaupten, dass dann $y \in L$ gilt. Sei zunächst y der Schnittpunkt der Geraden $\mathrm{Ge}(0,1) = \mathbb{R}$ und $\mathrm{Ge}(z_0, z_1)$, wobei $z_0, z_1 \in L$. Diese beiden Geraden sind verschieden und nicht parallel, gdw. $z_0 - z_1 \notin \mathbb{R}$. Den Schnittpunkt y findet man mit dem Ansatz

$$y = z_0 + t(z_1 - z_0) \in \mathbb{R}$$

mit $t \in \mathbb{R}$. Wir haben zu zeigen, dass $t \in L$ gilt. Die obige Gleichung ist äquivalent zu

$$i\Im(z_0) + ti\Im(z_1 - z_0) = 0$$

und hat die Lösung

$$t = -\frac{i\Im(z_0)}{i\Im(z_1 - z_0)},$$

welche nach der Vorbemerkung in L liegt. Dies zeigt die Behauptung für den Schnitt der Geraden $\mathrm{Ge}(0,1)$ und $\mathrm{Ge}(z_0, z_1)$. Im allgemeinen Fall seien $\mathrm{Ge}(z_0, z_1)$ und $\mathrm{Ge}(w_0, w_1)$ zwei verschiedene, nicht parallele Geraden mit Schnittpunkt y. Der Schnittpunkt y' der Geraden $\mathrm{Ge}(0,1)$ und $\mathrm{Ge}(\frac{z_0-w_0}{w_1-w_0}, \frac{z_1-w_0}{w_1-w_0})$ ist nach dem eben bewiesenen in L enthalten, und man überzeugt sich durch eine kurze Rechnung davon, dass

$$y = w_0 + (w_1 - w_0)y',$$

also in L.

(2) y ist der Schnittpunkt einer Gerade $\mathrm{Ge}(z_0, z_1)$ und eines Kreises $\mathrm{Kr}(z_2, r)$. Hierbei ist r von der Form $|z - z'|$ für gewisse $z, z' \in L$, und wir folgern

$$r^2 \in L.$$

Es reicht, den Fall $z_2 = 0$ zu betrachten, denn ist y' der Schnittpunkt von $\mathrm{Ge}(z_0 - z_2, z_1 - z_2)$ und $\mathrm{Kr}(0, r)$, so gilt $y = y' + z_2$; und y gehört zu L genau dann, wenn y' zu L gehört. *Es sei nun OBdA* $z_2 = 0$. Ein Punkt auf $\mathrm{Ge}(z_0, z_1)$ ist von der Form $z_0 + t(z_1 - z_0)$, $t \in \mathbb{R}$, und das liegt in $\mathrm{Kr}(0, r)$ genau dann, wenn

$$|z_0 + t(z_1 - z_0)|^2 = r^2.$$

Die Zahlen t sind die Nullstellen des Polynoms

$$|z_1 - z_0|^2 x^2 + 2\Re(\overline{z_0}(z_1 - z_0))x + |z_0|^2 - r^2 \in (L \cap \mathbb{R})[x].$$

Also liegt t (und daher auch $y = z_0 + t(z_1 - z_0)$ in einem Körper der Form $L(\sqrt{a})$, wobei $a \in L$ reell und positiv ist. Offenbar gilt $\overline{L(\sqrt{a})} = L(\sqrt{a}) = L(y)$.

(3) y ist der Schnittpunkt zweier Kreise. Wie in den vorigen Schritten können wir ohne Beschränkung der Allgemeinheit annehmen, dass die beiden Kreise $\mathrm{Kr}(0, r)$ und $\mathrm{Kr}(1, s)$ sind, wobei wieder $r, s \in L \cap \mathbb{R}$. Die Schnittpunkte y dieser beiden Kreise sind durch die Gleichungen

$$|y|^2 = r^2;\ |y - 1|^2 = s^2$$

gegeben. Ist y einer der beiden Schnittpunkte, so ist $\overline{y}$ der andere. Nun sind $y, \overline{y}$ die Nullstellen des Polynoms

$$p(x) = (x - y)(x - \overline{y}) = x^2 - 2\Re(y)x + |y|^2 = x^2 - 2\Re(y)x + r^2 \in \mathbb{R}[x].$$

Andererseits ist

$$s^2 = |y - 1|^2 = |y|^2 + 1 - 2\Re(y) = r^2 + 1 - 2\Re(y) \Rightarrow 2\Re(y) = r^2 + 1 - s^2,$$

und somit

$$p(x) = x^2 - (r^2 + 1 - s^2)x + r^2 \in (L \cap \mathbb{R})[x].$$

Die Nullstellen liegen von $p(x)$ liegen in der Körpererweiterung $L(w)$ mit

$$w = \sqrt{\frac{(r^2 + 1 - s^2)^2}{4} - r^2}.$$

Man beachte, das der Ausdruck in der Wurzel negativ ist, so dass $\overline{w} = -w$. Wie eben folgern wir $\overline{L(w)} = L(w) = L(y)$.

□

Wir können nun die in 5.1.3 gestellten Fragen zumindest teilweise beantworten. Zunächst eine Schlussfolgerung aus Satz 5.1.5.

Korollar 5.1.8. *Sei $z \in \mathbb{K}$. Dann ist z algebraisch über $\mathbb{Q}$, und der Grad des Minimalpolynoms $\mu_{\mathbb{Q},z}(x) \in \mathbb{Q}[x]$ ist eine Potenz von 2.*

Beweis. Nach Satz 5.1.5 gibt es eine Kette von Körpererweiterungen

$$\mathbb{Q} \subset K_1 \subset \ldots \subset K_n,$$

so dass $z \in K_n$ und so, dass $[K_i : K_{i-1}] = 2$ gilt. Es ist klar, dass z algebraisch über $\mathbb{Q}$ ist. Aus der Gradformel folgt dann

$$[K_n : \mathbb{Q}] = 2^n.$$

Betrachte nun den Unterkörper $\mathbb{Q}(z) \subset K_n$. Wieder mit der Gradformel ergibt sich

$$2^n = [\mathbb{Q}(z) : \mathbb{Q}][K_n : \mathbb{Q}(z)].$$

Weil

$$[\mathbb{Q}(z) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},z}(x)),$$

gilt also

$$2^n = \deg(\mu_{\mathbb{Q},z}(x))[K_n : \mathbb{Q}(z)].$$ □

Satz 5.1.9. *Die Verdopplung des Würfels ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Das Minimalpolynom ist

$$\mu_{\mathbb{Q},\sqrt[3]{2}}(x) = x^3 - 2$$

und hat Grad 3. Aus Korollar 5.1.8 folgt $\sqrt[3]{2} \notin \mathbb{K}$. □

Satz 5.1.10. *Die Kreiszahl π ist nicht in $\mathbb{K}$, also ist die Quadratur des Kreises mit Zirkel und Lineal nicht ausführbar.*

Das folgt sofort aus dem tiefen Satz von Hermite-Lindemann.

Satz 5.1.11. *Die Dreiteilung des Winkels mit Zirkel und Lineal ist im Allgemeinen nicht möglich.*

Beweis. Es genügt, einen konkreten Winkel α anzugeben, so dass $e^{i\alpha} \notin \mathbb{K}$, aber $e^{3i\alpha} \in \mathbb{K}$. Der Winkel $\alpha = \frac{2\pi}{9}$ tut es. Es ist nämlich $e^{i\frac{2\pi}{9}} = \zeta_9$ die neunte Einheitswurzel und $e^{3i\frac{2\pi}{9}} = \zeta_3$. Es gilt $\zeta_3 \in \mathbb{K}$, denn das Minimalpolynom von ζ_3 ist

$$x^2 + x + 1 \in \mathbb{Q}[x],$$

so dass $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ gilt.

Um zu zeigen, dass $\zeta_9 \notin \mathbb{K}$, müssen wir das Minimalpolynom berechnen. Es hilft uns die Information, dass $\zeta_9^3 = \zeta_3$ und dass $\zeta_3^2 + \zeta_3 + 1 = 0$. Es folgt

$$\zeta_9^6 + \zeta_9^3 + 1 = 0,$$

und daher ist ζ_9 eine Nullstelle von $x^6 + x^3 + 1$. Behauptung: $f(x) = x^6 + x^3 + 1$ ist irreduzibel. Es folgt, dass $f(x)$ das Minimalpolynom von ζ_9 ist, und weil 6 keine Potenz von 2 ist, folgt der Satz.

Die Irreduzibilität von $f(x)$ ist äquivalent zur Irreduzibilität von

$$(x+1)^6 + (x+1)^3 + 1,$$

und der binomische Lehrsatz und das Nachschlagen der Binomialkoeffizienten zeigt

$$(x+1)^6+(x+1)^3+1 = x^6+6x^5+15x^4+21x^3+18x^2+9x+3.$$

Das Eisensteinkriterium mit $p=3$ gibt die Antwort. □

Satz 5.1.12. *Es sei p eine Primzahl und es sei $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{K}$. Dann ist $p-1$ eine Potenz von 2.*

Beweis. Das Minimalpolynom von ζ_p ist $x^{p-1}+\ldots+x+1$. □

Die ersten Primzahlen, die von dieser Form sind, sind

$$3 = 2^1+1,\ 5 = 2^2+1,\ 17 = 2^4+1,\ 257 = 2^8+1,\ 2^{16}+1 = 65537.$$

Es handelt sich um die sogenannten Fermatschen Primzahlen; sie sind alle von der Form $2^{2^k}+1$. Man vermutet, dass die obigen fünf Beispiele die einzigen Fermatschen Primzahlen sind.

Um die Umkehrung des Satzes zu beweisen, müssen wir mehr Theorie entwickeln. Wesentlich schwerer, aber durchaus in Reichweite dieser Vorlesung, ist es, den Fall von nicht primen n zu behandeln.

Satz 5.1.13. *Die Zahl ζ_n gehört genau dann zu $\mathbb{K}$, wenn n von der Form*

$$n = 2^k p_1 \cdots p_r$$

ist, wobei die p_i paarweise verschiedene Fermat-Primzahlen sind.

6. Galoistheorie

6.1. **Motivation.** In Satz 5.1.12 haben wir gesehen, dass (für eine Primzahl p) die Einheitswurzel ζ_p nur dann im Körper $\mathbb{K}$ liegen kann, wenn $p-1$ eine Potenz von 2 ist. Wir wenden uns nun dem umgekehrten Problem zu; eines der Ziele wird der Beweis des folgenden Satzes sein:

Satz 6.1.1. *Es sei p eine Primzahl der Form $p = 2^k + 1$. Dann ist $\zeta_p \in \mathbb{K}$, d.h. das regelmäßige n-Eck ist mit Zirkel und Lineal konstruierbar.*

Wir wissen, dass das Polynom $\phi_p(x) = x^{p-1} + \ldots + 1$ das Minimalpolynom von ζ_p ist, und dass $\mathbb{Q}(\zeta_p)$ ein Zerfällungskörper von $\phi_p(x)$ ist, und dass der Grad gleich

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = 2^k$$

ist. Wenn wir es schaffen könnten, eine Folge

$$\mathbb{Q} = K_0 \subset \ldots \subset K_k = \mathbb{Q}(\zeta_p)$$

von Körpererweiterungen zu konstruieren mit $[K_i : \mathbb{Q}] = 2^i$, so wären wir fertig, nach Satz 5.1.5. Für manche p ist es offensichtlich, wie eine solche Folge zu konstruieren ist. Beispielsweise ist

$$\zeta_5 = \frac{\sqrt{5}-1}{4} + i\sqrt{\frac{\sqrt{5}+5}{8}},$$

und wenn wir etwa $K_1 := \mathbb{Q}(\sqrt{5})$ setzen, so sind

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$$

eine solche Folge von Körpererweiterungen.

Eine durchschlagende Methode hierfür bietet die *Galoistheorie*, die das Problem auf ein gruppentheoretisches Problem reduziert. Dieses gruppentheoretische Problem ist im vorliegenden Fall sehr einfach, so dass wir mit einem Minimum an Gruppentheorie auskommen werden.

Das Einfallstor für Gruppentheorie in die Theorie der Körpererweiterungen ist folgende Beobachtung.

Definition 6.1.2. *Es sei L ein Körper. Ein* Automorphismus *von L ist ein Körperisomorphismus $\sigma : L \to L$. Die Menge der Automorphismen wird mit dem Symbol* $\mathrm{Aut}(L)$ *bezeichnet. Wir definieren eine Verknüpfung*

$$\mathrm{Aut}(L) \times \mathrm{Aut}(L) \to \mathrm{Aut}(L);\ (\sigma, \tau) \mapsto \sigma \circ \tau.$$

Diese ist assoziativ, weil Verknüpfung von Abbildungen immer assoziativ ist. Ein neutrales Element ist die Identität id_L*, und nach Definition besitzt jedes $\sigma \in \mathrm{Aut}(L)$ ein Inverses σ^{-1}, welches leicht als ein Automorphismus zu erkennen ist. Daher ist* $\mathrm{Aut}(L)$ *eine Gruppe.*

Ist $K \subset L$ ein Unterkörper, so bezeichne

$$\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) | \forall z \in K : \sigma(z) = z\} \subset \mathrm{Aut}(L).$$

Dies ist eine Untergruppe von $\mathrm{Aut}(L)$.

Die entscheidende Idee der Galoistheorie besteht darin, eine Beziehung von Zwischenkörpern von $K \subset L$ und Untergruppen $G \subset \mathrm{Aut}(L/K)$ herzustellen. Die grundlegende Konstruktion ist folgende.

Definition 6.1.3. *Es sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine Untergruppe. Dann sei*

$$L^G := \{z \in L | \forall \sigma \in G : \sigma(z) = z\} \subset L$$

der Fixkörper *von G. Es ist klar, dass L^G ein Unterkörper von L ist.*

Definition 6.1.4. *Es sei $K \subset L$ eine Körpererweiterung. Mit $\mathrm{ZwK}(L/K)$ bezeichnen wir die Menge aller Zwischenkörper $K \subset N \subset L$. Ist G eine Gruppe, so ist $\mathrm{Ugr}(G)$ die Menge aller Untergruppen von G.*

Es sei nun $K \subset L$ eine Körpererweiterung und $G := \mathrm{Aut}(L/K)$. Wir erhalten Abbildungen

$$\Psi : \mathrm{ZwK}(L/K) \to \mathrm{Ugr}(G);\ N \mapsto \mathrm{Aut}(L/N)$$

sowie

$$\Phi : \mathrm{Ugr}(G) \to \mathrm{ZwK}(L/K);\ H \mapsto L^H.$$

Um nun eine perfekte Korrespondenz zwischen Untergruppen und Zwischenkörpern zu erlangen, ist es wünschenswert, dass die beiden Konstruktionen zueinander invers sind, also dass

$$\Psi \circ \Phi = \mathrm{id};\ \mathrm{Aut}(L/L^G) = G$$

und

$$\Phi \circ \Psi = \mathrm{id};\ L^{\mathrm{Aut}(K/N)} = N$$

für alle Untergruppen $G \subset \mathrm{Aut}(L/K)$ und alle Zwischenkörper $K \subset N \subset L$ gilt. Das ist nicht der Fall, aber es wird sich herausstellen, dass dies immer stimmt, wenn $K \subset L$ Zerfällungskörper eines separablen Polynoms ist. Zunächst eine einfache Beobachtung.

Lemma 6.1.5. *Es sei L ein Körper.*

1. *Für jede Untergruppe $G \subset \mathrm{Aut}(L)$ gilt $G \subset \mathrm{Aut}(L/L^G)$.*
2. *Für jeden Unterkörper $K \subset L$ gilt $K \subset L^{\mathrm{Aut}(L/K)}$.*
3. *Sind $K \subset N \subset L$ Unterkörper, so gilt $\mathrm{Aut}(L/N) \subset \mathrm{Aut}(L/K)$.*
4. *Sind $H \subset G \subset \mathrm{Aut}(L)$ Untergruppen, so gilt $L^G \subset L^H$.* □

Lemma 6.1.6. *Ist $K \subset L$ eine endliche Körpererweiterung, so ist $\mathrm{Aut}(K/L)$ eine endliche Gruppe, und es ist*

$$|\mathrm{Aut}(K/L)| \leq [L : K].$$

Ist L ein Zerfällungskörper eines separablen Polynoms, so gilt sogar

$$|\mathrm{Aut}(K/L)| = [L : K].$$

Beweis. Korollar 4.6.14 und Satz 4.7.2. □

Wir können nun den Hauptsatz der Galoistheorie formulieren.

Theorem 6.1.7 (Hauptsatz der Galoistheorie)**.** *Es sei $K \subset L$ ein Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$. Dann sind die Abbildungen*

$$\Psi : \mathrm{ZwK}(L/K) \to \mathrm{Ugr}(\mathrm{Aut}(L/K));\ N \mapsto \mathrm{Aut}(L/N)$$

sowie

$$\Phi : \mathrm{Ugr}(\mathrm{Aut}(L/K)) \to \mathrm{ZwK}(L/K);\ H \mapsto L^H$$

zueinander inverse Bijektionen. Mit anderen Worten, es gilt:

1. *Ist $K \subset N \subset L$ ein Zwischenkörper, so ist $N = L^{\mathrm{Aut}(L/N)}$.*
2. *Ist $H \subset \mathrm{Aut}(L/K)$ eine Untergruppe, so ist $H = \mathrm{Aut}(L/L^H)$.*

Des weiteren gilt:

(1) *Für jede Untergruppe* $H \in \mathrm{Aut}(L/K)$ *ist*

$$|H| = [L : L^H].$$

(2) *Für jeden Zwischenkörper* $K \subset N \subset L$ *ist*

$$[L : N] = |\mathrm{Aut}(L/N)|.$$

6.2. **Beispiele für die Galois-Korrespondenz.** Bevor wir in den Beweis des Hauptsatzes einsteigen, wollen wir die Aussage anhand von Beispielen erklären.

Beispiel 6.2.1. $\mathbb{R} \subset \mathbb{C}$ *ist ein Zerfällungskörper des Polynoms* $f(x) = x^2 + 1$*, welches irreduzibel und daher separabel ist. Offenbar gilt* $[\mathbb{C} : \mathbb{R}] = 2$*. Die Automorphismengruppe* $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ *besteht daher aus zwei Elementen. Eines davon ist die Identität, und das andere ist die komplexe Konjugation* $\kappa(z) := \overline{z}$*. Demnach gilt*

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \kappa\}.$$

Jede Gruppe mit zwei Elementen ist isomorph zu $\mathbb{Z}/2$*, der additiven Gruppe des Ringes* $\mathbb{Z}/2$*. Dieser Isomorphismus ist gegeben durch*

$$[0] \mapsto \mathrm{id},\ [1] \mapsto \kappa.$$

Die Gruppe $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ *hat genau zwei Untergruppen, nämlich* $\{\mathrm{id}\}$ *und* $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ *selbst. Die dazugehörigen Zwischenkörper sind*

$$\mathbb{C}^{\mathrm{id}} = \mathbb{C};\ \mathbb{C}^{\mathrm{Aut}(\mathbb{C}/\mathbb{R})} = \mathbb{R}.$$

Andererseits gibt es nur zwei Zwischenkörper: aus Gradgründen sind $\mathbb{R}$ *und* $\mathbb{C}$ *die einzigen Zwischenkörper. Offenbar ist*

$$\mathrm{Aut}(\mathbb{C}/\mathbb{C}) = \{\mathrm{id}\};\ \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathrm{Aut}(\mathbb{C}/\mathbb{R}).$$

Für dieses einfache Beispiel haben wir Theorem 6.1.7 verifiziert.

Beispiel 6.2.2. *Es sei* $\mathrm{char}(K) = 0$*, und wir betrachten* $a \in K$*, so dass* a *keine Wurzel in* K *hat. Die Erweiterung* $K \subset K(\sqrt{a})$ *ist ein Zerfällungskörper des irreduziblen (und separablen) Polynoms* $x^2 - a$*. Weil* $[K(\sqrt{a}) : K] = 2$*, gilt* $|\mathrm{Aut}(K(\sqrt{a})/K)| = 2$*, wegen Lemma 6.1.6. Also können wir* $\mathrm{Aut}(K(\sqrt{a})/K) = \{\mathrm{id}, \sigma\}$ *schreiben, wobei* $\sigma \neq \mathrm{id}$*. Der Automorphismus* σ *ist nicht die Identität, und weil*

$$(\sigma(\sqrt{a}))^2 = \sigma(\sqrt{a}^2) = \sigma(a) = a,$$

muss $\sigma(\sqrt{a}) = -\sqrt{a}$ *gelten, denn* $\sigma(\sqrt{a}) = \sqrt{a}$ *würde* $\sigma = \mathrm{id}$ *nach sich ziehen. Der Rest geht so wie in Beispiel 6.2.1.*

Nun sei $z = s + t\sqrt{a}$*,* $s, t \in K$ *ein beliebiges Element von* $K(\sqrt{a})$*. Wir betrachten das Polynom*

$$f(x) := (x - z)(x - \sigma(z)) = (x - s - t\sqrt{a})(x - s + t\sqrt{a}) = x^2 - 2sx + (s^2 - t^2 a).$$

Dies ist offenbar ein Polynom aus $K[x]$*, und wenn* $t \neq 0$*, so ist* $f(x)$ *irreduzibel (weil es keine Nullstelle in* K *hat). Ist* $t = 0$*, so ist* $f(x) = (x - s)^2$ *reduzibel. Die obige Vorschrift erlaubt also die Berechnung der Minimalpolynome aller Elemente von* $K(\sqrt{a})$*.*

Beispiel 6.2.2 beschreibt die einfachste mögliche Situation. Für die Diskussion komplizierterer Beispiele machen wir zwei nützliche Beobachtungen.

Lemma 6.2.3. *Es sei $K \subset L$ eine Körpererweiterung, $f(x) \in K[x]$ ein Polynom und $g \in \mathrm{Aut}(L/K)$, und $z \in L$ eine Nullstelle von $f(x)$. Dann ist $g(z)$ eine Nullstelle von $f(x)$.* □

Satz 6.2.4. *Es sei $f(x) \in K[x]$ separabel und normiert, und $n = \deg(f)$. Es sei $K \subset L$ ein Zerfällungskörper von f. Dann ist die Gruppe $\mathrm{Aut}(L/K)$ isomorph zu einer Untergruppe der symmetrischen Gruppe Σ_n.*

Beweis. Wir wollen einen injektiven Gruppenhomomorphismus

$$\rho : \mathrm{Aut}(L/K) \to \Sigma_n$$

konstruieren. Dafür seien $z_1, \ldots, z_n$ die Nullstellen von f in L. Ist $\sigma \in \mathrm{Aut}(L/K)$, so ist $\sigma(z_i)$ wieder eine Nullstelle von f (wegen Lemma 6.2.3). Es gibt also ein $j \in \underline{n}$, so dass $\sigma(z_i) = z_j$, und dieses j bezeichnen wir mit

$$\rho(\sigma)(i) := j.$$

Es ist nun zu zeigen, dass die so definierte Abbildung

$$\rho(\sigma) : \underline{n} \to \underline{n}$$

bijektiv ist, also ein Element von Σ_n. Allerdings ist σ bijektiv, und daher ist $\rho(\sigma)$ injektiv. Als Abbildung der endlichen Menge $\underline{n}$ in sich muss $\rho(\sigma)$ dann auch surjektiv sein. Bis hierhin haben wir eine Abbildung

$$\rho : \mathrm{Aut}(L/K) \to \Sigma_n$$

konstruiert. Als nächstes rechnet man nach, dass ρ ein Gruppenhomomorphismus ist. Das aber sieht man mit folgender Rechnung: für $\sigma, \tau \in \mathrm{Aut}(L/K)$ und $i \in \underline{n}$ ist nämlich

$$z_{\rho(\sigma\circ\tau)(i)} = (\sigma \circ \tau)(z_i) = \sigma(\tau(z_i)) = \sigma(z_{\rho(\tau)(i)}) = z_{\rho(\sigma)(\rho(\tau)(i))}$$

und daher

$$\rho(\sigma \circ \tau)(i) = \rho(\sigma)(\rho(\tau)(i)).$$

Weil i beliebig war, folgt

$$\rho(\sigma \circ \tau) = \rho(\sigma) \circ \rho(\tau).$$

Zu guter Letzt ist zu zeigen, dass ρ injektiv ist. Hierfür ist zu zeigen, dass $\rho(\sigma) = \mathrm{id}_{\underline{n}}$ impliziert, dass $\sigma = \mathrm{id}_L$. Nach der Definition von $\rho(\sigma)$ heißt $\rho(\sigma) = \mathrm{id}$ nichts anderes, als dass $\sigma(z_i) = z_i$ für jedes $i \in \underline{n}$. Weil die Elemente $z_1, \ldots, z_n$ die Körpererweiterung L erzeugen, muss automatisch $\sigma = \mathrm{id}$ gelten, wie behauptet. □

Definition 6.2.5. *Es sei G eine endliche Gruppe. Die Anzahl $|G|$ der Elemente von G heißt* Ordung *von G.*

Beispiel 6.2.6. *$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Wir wissen, dass L ein Zerfällungskörper von $f(x) = x^3 - 2$ ist, und daraus folgt*

$$|\mathrm{Aut}(L/K) = [L : K] = 6.$$

Die Nullstellen von $f(x)$ sind $z_1 = \sqrt[3]{2}$, $z_2 = \zeta_3 z_1$, $z_3 = \zeta_3^2 z_1$. Aus Lemma 6.2.4 erhalten wir einen injektiven Gruppenhomomorphismus

$$\rho : \mathrm{Aut}(L/K) \to \Sigma_3.$$

Weil beide Gruppen Ordnung 6 haben, ist ρ ein Isomorphismus.

Welche Untergruppen hat Σ_3? Um uns einen Überblick darüber zu verschaffen, führen wir Notation für Elemente in Σ_n ein. Wenn $i_1, \dots, i_r \in \underline{n}$ paarweise verschiedene Elemente sind, so bezeichne $(i_1\, i_2\, \dots\, i_r)$ die Permutation, welche durch

$$i_j \mapsto i_{j+1},\ j = 1, \dots, r,$$
$$i_r \mapsto i_1$$

und $i \mapsto i$ für alle $i \in \underline{n} \setminus \{i_1, \dots, i_r\}$ gegeben ist. Man überlegt sich, dass die Elemente von Σ_3 gerade die Elemente

$$\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)$$

sind. Man sieht ferner, dass

$$\{\mathrm{id}\}, H_1 = \{\mathrm{id}, (1\,2)\}, H_2 = \{\mathrm{id}, (1\,3)\}, H_3 = \{\mathrm{id}, (2\,3)\},$$
$$A = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$$

und Σ_3 eine vollständige Liste aller Untergruppen von Σ_3 ist.

Ferner hat $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ die Zwischenkörper

$$M = \mathbb{Q}(\zeta_3), N_3 = \mathbb{Q}(\sqrt[3]{2}), N_2 = \mathbb{Q}(\zeta_3\sqrt[3]{2}), N_1 = \mathbb{Q}(\zeta_3\sqrt[3]{2}).$$

Die Nummerierung ist so gewählt, dass

$$N_i = L^{H_i}, M = L^A$$

gilt.

Beispiel 6.2.7. *Es sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In Beispiel 4.3.14 haben wir das Minimalpolynom $f(x)$ von $\sqrt{2} + \sqrt{3}$ berechnet, es ist*

$$f(x) = x^4 - 10x^2 + 1$$

mit den Nullstellen

$$z_1 = \sqrt{2} + \sqrt{3},\ z_2 = \sqrt{2} - \sqrt{3},\ z_3 = -\sqrt{2} + \sqrt{3},\ z_4 = -\sqrt{2} - \sqrt{3}.$$

Wir folgern, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, und folglich ist

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Q}[x]/(f)$$

sowie

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4,$$

und daher

$$|\mathrm{Aut}(L/\mathbb{Q})| = 4.$$

Wir wollen nun die Struktur dieser Gruppe bestimmen. Satz 6.2.4 erklärt einen injektiven Homomorphismus nach Σ_4; bequemer ist es, die Methode des Beweises des Satzes zu kopieren.

Dafür betrachtet man das Polynom $f(x) = x^2 - 2$ mit den beiden Nullstellen $\pm\sqrt{2}$ in L. Wegen Lemma 6.2.3 gibt es zu jedem $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ ein $\epsilon(\sigma) \in \{\pm 1\}$, so dass

$$\sigma(\sqrt{2}) = \epsilon(\sigma)\sqrt{2}.$$

Die Zuordnung $\sigma \mapsto \epsilon(\sigma)$ ist ein Gruppenhomomorphismus $\epsilon : \mathrm{Aut}(L/\mathbb{Q}) \to \{\pm 1\}$ (letztes ist die Gruppe der Einheiten in $\mathbb{Z}$), denn

$$\tau(\sigma(\sqrt{2})) = \tau(\epsilon(\sigma)\sqrt{2}) = \epsilon(\sigma)\tau(\sqrt{2}) = \epsilon(\sigma)\epsilon(\tau)\sqrt{2}.$$

Analog definieren wir einen Homomorphismus

$$\eta : \mathrm{Aut}(L/\mathbb{Q}) \to \{\pm 1\}$$

durch

$$\sigma(\sqrt{3}) = \eta(\sigma)\sqrt{3}.$$

Die Gruppe ± 1 *hat zwei Elemente, ist also isomorph zu* $\mathbb{Z}/2$*, und beide Abbildungen zusammen definieren einen Homomorphismus*

$$\rho : \mathrm{Aut}(L/\mathbb{Q}) \to \pm 1 \times \pm 1 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

(Definition folgt unten). Die Abbildung ρ *ist injektiv, denn* $\rho(\sigma) = (1,1)$ *bedeutet* $\sigma(\sqrt{2}) = \sqrt{2}$ *und* $\sigma(\sqrt{3}) = \sqrt{3}$*, und daher* $\sigma = \mathrm{id}$*. Weil beide Gruppen die Ordnung* 4 *haben, ist* ρ *ein Isomorphismus.*

Um nun die Zwischenkörper zu berechnen, reicht es, nach dem Hauptsatz, die Untergruppen von $\mathrm{Aut}(L/\mathbb{Q})$ *zu berechnen. Die obige Rechnung zeigt, dass es ein eindeutig bestimmtes* $\sigma_1 \in \mathrm{Aut}(L/\mathbb{Q})$ *gibt mit* $\sigma_1(\sqrt{2}) = -\sqrt{2}$ *und* $\sigma_1(\sqrt{3}) = \sqrt{3}$*, und ein eindeutig bestimmtes* σ_2 *mit* $\sigma_2(\sqrt{2}) = \sqrt{2}$ *und* $\sigma_2(\sqrt{3}) = \sqrt{3}$*. Es gilt*

$$\sigma_2^2 = \mathrm{id} = \sigma_3^2$$

und

$$\sigma_2\sigma_3 = \sigma_3\sigma_2;\ (\sigma_2\sigma_3)^2 = \mathrm{id}.$$

Die Untergruppen von $\mathrm{Aut}(L/\mathbb{Q})$ *sind, außer* $\{\mathrm{id}\}$ *und* $\mathrm{Aut}(L/\mathbb{Q})$*, die Gruppen*

$$H_2 = \{\mathrm{id}, \sigma_2\};\ H_3 = \{\mathrm{id}, \sigma_3\};\ H_4 = \{\mathrm{id}, \sigma_2\sigma_3\}.$$

Die Fixkörper sind

$$L^{H_2} = \mathbb{Q}(\sqrt{3}),\ L^{H_3} = \mathbb{Q}(\sqrt{2}).$$

Das Element $\sqrt{6} = \sqrt{2}\sqrt{3}$ *wird von* $\sigma_2\sigma_3$ *festgelassen, und daher ist*

$$L^{H_4} = \mathbb{Q}(\sqrt{6}).$$

In diesem Beispiel haben wir die Definition des *direkten Produktes* $G \times H$ zweier Gruppen verwendet. Auf der Menge $G \times H$ definieren wir die Verknüpfung $(g,h)(g',h') := (gg', hh')$, und man sieht leicht, dass dies eine Gruppe ist.

6.3. **Kreisteilungskörper.** $K = \mathbb{Q} \subset L = \mathbb{Q}(\zeta_n)$. Dies ist ein Zerfällungskörper des Polynoms

$$F_n(x) := x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1) \in \mathbb{Q}[x].$$

Weil $F_n(x)$ genau die n paarweise verschiedenen Nullstellen

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$$

hat, ist $F_n(x)$ separabel. Wir wissen außerdem

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\zeta_n}) \leq n-1,$$

denn ζ_n ist eine Nullstelle des Polynoms $x^{n-1} + \ldots + x + 1$ vom Grad $n-1$. Ferner gilt

$$|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Ist p eine Primzahl, so ist $x^{p-1} + \ldots + x + 1$ irreduzibel, und in diesem Fall folgt

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\zeta_p}) = p - 1.$$

Es sei nun

$$C_n := \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \subset \mathbb{Q}(\zeta_n)^\times.$$

Dies ist die Nullstellenmenge von $F_n(x)$, und die besondere Eigenschaft des Polynoms $F_n(x)$ ist, dass C_n eine Untergruppe von $\mathbb{Q}(\zeta_n)^\times$ ist.

Lemma 6.3.1. (1) *Für $w \in C_n$ und $k \in \mathbb{Z}$ hängt die Zahl $w^k \in C_n$ nur von der Restklasse $[k] \in \mathbb{Z}/n$ ab. Insbesondere ist der Ausdruck w^l für $w \in C_n$ und $l \in \mathbb{Z}/n$ wohldefiniert.*

(2) *Für jedes $w \in C_n$ gibt es ein eindeutig bestimmtes $l \in \mathbb{Z}/n$ mit $w = \zeta_n^l$.*

Beweis. Wenn $k \equiv k' \pmod{n}$, so gilt $k' = k + an$ für ein $a \in \mathbb{Z}$, und es gilt

$$w^{k'} = w^k w^{an} = w^k (w^n)^a = w^k,$$

was die erste Aussage beweist. Weil jedes $w \in C_n$ in der Form ζ_n^k geschrieben werden kann, gibt es ein $l \in \mathbb{Z}/n$ mit $w = \zeta_n^l$. Dieses l ist eindeutig bestimmt, denn aus $\zeta_n^k = \zeta_n^{k'}$, $k, k' \in \mathbb{Z}$, folgt $\zeta_n^{k-k'} = 1$, also $k \equiv k' \pmod{n}$. □

Für einen beliebigen Automorphismus $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ und $w \in C_n$ ist

$$\sigma(w)^n = \sigma(w^n) = \sigma(1) = 1$$

und daher

$$\sigma(w) \in C_n.$$

Definition 6.3.2. *Für $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sei $\kappa(\sigma) \in \mathbb{Z}/n$ das durch Lemma 6.3.1 eindeutig bestimmte Element mit*

$$\sigma(\zeta_n) = \zeta_n^{\kappa(\sigma)}.$$

Lemma 6.3.3. *Es seien $\sigma, \tau \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.*

(1) *Für jedes $w \in C_n$ ist $\sigma(w) = w^{\kappa(\sigma)}$.*

(2) *Es gilt $\kappa(\sigma \circ \tau) = \kappa(\sigma)\kappa(\tau)$, $\kappa(\mathrm{id}) = 1$, und $\kappa(\sigma)$ ist eine Einheit im Ring $\mathbb{Z}/n$.*

(3) *$\kappa : \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}/n^\times$ ist ein injektiver Gruppenhomomorphismus.*

Beweis. (1): Schreibe $w = \zeta_n^k$, $k \in \mathbb{Z}$. Dann ist

$$\sigma(w) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = \zeta_n^{\kappa(\sigma)k} = w^{\kappa(\sigma)}.$$

(2) Es gilt

$$\zeta_n^{\kappa(\sigma\circ\tau)} = \sigma \circ \tau(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\kappa(\tau)}) = \sigma(\zeta_n)^{\kappa(\tau)} = \zeta_n^{\kappa(\sigma)\kappa(\tau)}.$$

Aus Lemma 6.3.1 (2) folgt $\kappa(\sigma \circ \tau) = \kappa(\sigma)\kappa(\tau)$. Die Gleichung $\kappa(\mathrm{id}) = 1$ ist trivial. Wegen $1 = \kappa(\mathrm{id}) = \kappa(\sigma \circ \sigma^{-1}) = \kappa(\sigma)\kappa(\sigma^{-1})$ folgt außerdem, dass $\kappa(\sigma)$ eine Einheit in $\mathbb{Z}/n$ ist. (3): Aus den beiden vorherigen Punkten folgt, dass $\kappa : \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}/n^\times$ ein Gruppenhomomorphismus ist. Injektivität ergibt sich aus

$$\kappa(\sigma) = 1 \Rightarrow \sigma(\zeta_n) = \zeta_n \Rightarrow \sigma = \mathrm{id}.$$

□

Satz 6.3.4. *Ist p eine Primzahl, so ist*

$$\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$$

ein Isomorphismus.

Beweis. Weil $\mathbb{F}_p = \mathbb{Z}/p$ ein Körper ist, ist jedes von Null verschiedene Element eine Einheit und daher gilt

$$|\mathbb{F}_p^\times| = p - 1.$$

Weil $|\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, ist der (nach Lemma 6.3.3 injektive) Gruppenhomomorphismus

$$\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$$

ein Isomorphismus. □

6.4. **Beweis des Hauptsatzes der Galois-Theorie.**

Definition 6.4.1. *Eine endliche Körpererweiterung $K \subset L$ ist eine* Galois-Erweiterung*, wenn $K = L^{\mathrm{Aut}(L/K)}$ gilt. Die Gruppe* $\mathrm{Aut}(L/K)$ *heißt auch* Galois-Gruppe *der Erweiterung.*

Nach Lemma 6.1.5 gilt für jede Körpererweiterung $K \subset L^{\mathrm{Aut}(L/K)}$; es ist die umgekehrte Inklusion, auf die es ankommt. Konkreter gesagt lautet die Bedingung: zu jedem $z \in L$ mit $z \notin K$ gibt es einen K-Automorphismus σ von L mit $\sigma(z) \neq z$.

Theorem 6.4.2 (Charakterisierung von Galois-Erweiterungen)**.** *Es sei $K \subset L$ eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent.*

1. *L ist Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$.*
2. *$K \subset L$ ist eine Galois-Erweiterung.*
3. *Es gibt eine endliche Untergruppe $G \subset \mathrm{Aut}(L)$, so dass $K = L^G$.*
4. *Das Minimalpolynom (über K) eines jeden Elementes von L ist separabel und zerfällt über L in Linearfaktoren.*

Beweis. $1 \Rightarrow 2$: Aus Satz 4.7.2 folgt

$$|\mathrm{Aut}(L/K)| = [L : K]. \tag{6.4.3}$$

Wegen Lemma 6.1.5 (ii) ist

$$K \subset L^{\mathrm{Aut}(L/K)} =: N \subset L.$$

Wenn wir zeigen könne, dass $N = K$ gilt, so ist $K \subset L$ als Galois-Erweiterung erwiesen. Wir können $f(x)$ als Polynom in $N[x]$ auffassen. Weil $\mathrm{ggT}_N(f, f') = \mathrm{ggT}_K(f, f') = 1$ (Lemma 4.6.11) ist $f(x)$ auch dann separabel, wenn es als Polynom mit Koeffizienten in N angesehen ist, und $N \subset L$ ist ein Zerfällungskörper von $f(x)$.

Weil $K \subset N$, gilt $\mathrm{Aut}(L/N) \subset \mathrm{Aut}(L/K)$, und weil jedes Element von $\mathrm{Aut}(L/K)$ nach Konstruktion N festhält, gilt auch $\mathrm{Aut}(L/K) \subset \mathrm{Aut}(L/N)$, also zusammen

$$\mathrm{Aut}(L/N) = \mathrm{Aut}(L/K).$$

Satz 4.7.2 impliziert daher

$$|\mathrm{Aut}(L/K)| = [L : N]. \tag{6.4.4}$$

Aus den Gleichungen (6.4.3) und (6.4.4) folgt

$$[L : K] = [L : N],$$

und mit der Gradformel ist

$$[L : K] = [L : N][N : K],$$

also $[N : K] = 1$, also $N = K$. Das heißt aber $K = L^{\mathrm{Aut}(K/L)}$, also ist $K \subset L$ eine Galois-Erweiterung.

$2 \Rightarrow 3$ ist trivial: nimm $G = \mathrm{Aut}(L/K)$.

$3 \Rightarrow 4$: Es sei $z \in L$ und $f(x) \in K[x]$ sei das Minimalpolynom von z über K. Es sei $Z := \{z_1, \ldots, z_r\} \subset L$ die Menge der Elemente der Form $\sigma(z)$, mit $\sigma \in G$, wobei alle z_i's paarweise verschieden seien. Man beachte, dass $z \in Z$. Setze

$$g(x) := (x - z_1) \cdots (x - z_r) \in L[x].$$

A priori ist das ein Polynom mit Koeffizienten in L. Für $\sigma \in G$ ist aber $\sigma(Z) = Z$, und die Einschränkung $\sigma|_Z : Z \to Z$ ist bijektiv. Daher ist

$$\sigma_* g(x) = (x - \sigma(z_1)) \cdots (x - \sigma(z_r)) = (x - z_1) \cdots (x - z_r) = g(x).$$

Also werden alle Koeffizienten von $g(x)$ von allen Elementen aus G festgehalten und liegen somit in $L^G = K$. Somit ist $g(x) \in K[x]$, ein separables Polynom, das in $L[x]$ in Linearfaktoren zerfällt. Ferner ist z eine Nullstelle von $g(x)$.

Weil $g(x)$ und $f(x)$ eine gemeinsame Nullstelle in L haben (nämlich z), sind $f(x)$ und $g(x)$ nicht teilerfremd. Weil $f(x)$ in $K[x]$ irreduzibel ist, muss $f(x)$ ein Teiler von $g(x)$ sein.

Nun zerfällt $g(x)$ nach Konstruktion über L in paarweise verschiedene Linearfaktoren, und wegen der Eindeutigkeit der Primfaktorzerlegung ist dies auch für $f(x)$ richtig. Somit ist $f(x)$ separabel und zerfällt über L in Linearfaktoren, wie behauptet.

$4 \Rightarrow 1$: Weil $K \subset L$ endlich ist, gibt es $z_1, \ldots, z_s \in L$ mit $L = K(z_1, \ldots, z_s)$. Alle z_i's sind algebraisch über K, und es sei $f_i(x) \in K[x]$ das Minimalpolynom von z_i. Diese müssen nicht notwendig voneinander verschieden sein. Wir betrachten das Produkt $f(x)$ der verschiedenen $f_i(x)$.

Nach Annahme ist jedes $f_i(x)$ separabel und zerfällt über L in Linearfaktoren. Weil wir das Produkt über verschiedene $f_i(x)$ genommen haben, ist $f(x)$ separabel und zerfällt über L in Linearfaktoren. Weil jedes z_i eine Nullstelle von $f(x)$ ist, ist $L = K(z_1, \ldots, z_s)$ ein Zerfällungskörper von $f(x)$, wie behauptet. □

An dieser Stelle können wir die erste Hälfte des Hauptsatzes der Galoistheorie beweisen.

Satz 6.4.5 (Erste Hälfte des Hauptsatzes)**.** *Es sei $K \subset L$ eine Galois-Erweiterung und es sei $K \subset N \subset L$ ein Zwischenkörper. Dann ist $N \subset L$ eine Galois-Erweiterung. Insbesondere gilt*

$$N = L^{\mathrm{Aut}(L/N)},$$

und die Komposition $\Phi \circ \Psi : \mathrm{ZwK}(L/K) \to \mathrm{ZwK}(L/K)$ ist die Identität. Ferner gilt $[L : N] = \mathrm{Aut}(L/N)$.

Beweis. Wir benutzen das Kriterium (4) aus Theorem 6.4.2. Sei also $\mu_{N,z}(x) \in N[x]$ das Minimalpolynom von $z \in L$ über N. Es ist zu zeigen, dass $\mu_{z,N}(x)$ separabel ist und über L in Linearfaktoren zerfällt. Es gilt aber $\mu_{z,N}(x) | \mu_{z,K}(x) \in N[x]$, und weil $\mu_{z,K}(x)$ über L in paarweise verschiedene Linearfaktoren zerfällt, muss dies auch für $\mu_{z,N}(x)$ gelten. Aus Theorem 6.4.2 folgt, dass $N \subset L$ eine Galois-Erweiterung ist. Nach Definition der Vokabel "Galois-Erweiterung" bedeutet dies $N = L^{\mathrm{Aut}(L/N)}$, und die Definition der Abbildungen Ψ und Φ impliziert, dass $\Phi \circ \Psi$ die Identität ist. Die Gleichung $[L : N] = \mathrm{Aut}(L/N)$ folgt sofort aus Lemma 6.1.6. □

Für den Beweis der zweiten Hälfte ist eine weitere Zutat erforderlich.

Satz 6.4.6. *Es sei K ein Körper und $G \subset \mathrm{Aut}(K)$ endlich. Dann ist $K^G \subset K$ eine endliche Erweiterung, und es gilt*

$$[K : K^G] \leq |G|.$$

Beweis. Es sei $|G| = n$, und schreibe $G = \{\sigma_1, \ldots, \sigma_n\}$, mit $\sigma_1 = \mathrm{id}$. Es ist zu zeigen, dass $\dim_{K^G}(K) \leq n$, oder dass jede Teilmenge $\{y_1, \ldots, y_m\} \subset K$ mit $m > n$ linear abhängig über K^G ist.

Man betrachte das lineare Gleichungssystem

$$\begin{aligned} y_1x_1 + y_2x_2 + \ldots + y_mx_m &= 0 \\ \sigma_2(y_1)x_1 + \sigma_2(y_2)x_2 + \ldots + \sigma_2(y_m)x_m &= 0 \\ \ldots\ldots &= 0 \\ \sigma_n(y_1)x_1 + \sigma_n(y_2)x_2 \ldots + \sigma_n(y_m)x_m &= 0 \end{aligned} \tag{6.4.7}$$

über dem Körper K. Weil $m > n$ vorausgesetzt ist, gibt es eine nichttriviale Lösung $(x_1, \ldots, x_m) \in K^m$. Wenn wir eine nichttriviale Lösung mit $x_1, \ldots, x_m \in K^G$ finden können, ist der Beweis fertig, denn die Gleichung in der ersten Reihe ist dann eine nichttriviale lineare Relation zwischen den y_i's, und daher ist $\{y_1, \ldots, y_m\}$ linear abhängig.

Wir wählen eine nichttriviale Lösung $(x_1, \ldots, x_m)$ des Gleichungssystems (6.4.7), mit minimaler Anzahl an von Null verschiedenen Einträgen. Nach Umsortieren dürfen wir annehmen, dass $x_1 \neq 0$, und nach Division durch x_1 darf des weiteren $x_1 = 1$ angenommen werden. Wir behaupten, dass mit diesen Normierungen $(x_1, \ldots, x_m) \in (K^G)^m$ gilt, mit anderen Worten, dass $\sigma_j(x_i) = x_i$ für alle i, j gilt.

Dies zeigen wir durch Widerspruch. Wenn nicht, so gibt es $2 \leq j \leq m$ und $2 \leq k \leq n$, so dass $\sigma_k(x_j) \neq x_j$. Wir wenden den Automorphismus σ_k auf alle Gleichungen aus (6.4.7) an, und erhalten ein neues Gleichungssystem

$$\begin{aligned} \sigma_k(y_1)x_1 + \sigma_k(y_2)\sigma_k(x_2) + \ldots + \sigma_k(y_m)\sigma_k(x_m) &= 0 \\ \sigma_k\sigma_2(y_1)x_1 + \sigma_k\sigma_2(y_2)\sigma_k(x_2) + \ldots + \sigma_k\sigma_2(y_m)\sigma_k(x_m) &= 0 \\ \ldots\ldots &= 0 \\ \sigma_k\sigma_n(y_1)x_1 + \sigma_k\sigma_n(y_2)\sigma_k(x_2) + \ldots + \sigma_k\sigma_n(y_m)\sigma_k(x_m) &= 0. \end{aligned} \tag{6.4.8}$$

Hier wurde benutzt, dass $x_1 \in K^G$, das heißt $\sigma_i(x_1) = x_1$ für alle $i = 1, \ldots, n$, und dass σ_i ein Körperhomomorphismus ist. Des weiteren ist G eine Gruppe. Die Gruppenaxiome implizieren, dass die Abbildung $G \to G$, $g \mapsto \sigma_k \circ g$, bijektiv ist. Aus diesem Grund können wir die Zeilen von (6.4.8) umsortieren, und erhalten

$$\begin{aligned} y_1x_1 + y_2\sigma_k(x_2) + \ldots + y_m\sigma_k(x_m) &= 0 \\ \sigma_2(y_1)x_1 + \sigma_2(y_2)\sigma_k(x_2) + \ldots + \sigma_2(y_m)\sigma_k(x_m) &= 0 \\ \ldots\ldots &= 0 \\ \sigma_n(y_1)x_1 + \sigma_n(y_2)\sigma_k(x_2) + \ldots + \sigma_n(y_m)\sigma_k(x_m) &= 0. \end{aligned} \tag{6.4.9}$$

wo wieder eingegangen ist, dass stets $\sigma_i(x_1) = x_1$ gilt. Also ist

$$(x_1, \sigma_k(x_2), \ldots, \sigma_k(x_m)) \tag{6.4.10}$$

ebenfalls eine Lösung von (6.4.7). Es folgt, dass

$$(x_1 - x_1, x_2 - \sigma_k(x_2), \ldots, x_m - \sigma_k(x_m))$$

ebenfalls eine Lösung ist. Diese ist nichttrivial, denn der $i$te Eintrag ist $x_i - \sigma_k(x_i) \neq 0$. Der erste Eintrag ist $x_1 - x_1 = 0$, und wenn $x_j = 0$, so auch $x_j - \sigma_k(x_j) = 0$. Somit ist (6.4.10) eine Lösung von (6.4.7) mit weniger von Null verschiedenen Einträgen. Widerspruch. □

Satz 6.4.11 (Zweite Hälfte des Hauptsatzes)**.** *Es sei $K \subset L$ eine Galois-Erweiterung und es sei $G \subset \mathrm{Aut}(L/K)$ eine Untergruppe. Dann gilt $G = \mathrm{Aut}(L/L^G)$. Insbesondere ist die Komposition $\Psi \circ \Phi : \mathrm{Ugr}(\mathrm{Aut}(L/K)) \to \mathrm{Ugr}(\mathrm{Aut}(L/K))$ die Identität. Ferner gilt $|G| = [L : L^G]$.*

Beweis. Aus Lemma 6.1.5 folgt $G \subset \mathrm{Aut}(L/L^G)$. Aus Satz 6.4.6 folgt $|G| \geq [L : L^G]$ und damit die Gleichheit $G = \mathrm{Aut}(L/L^G)$. Daher ist $\Psi \circ \Phi$ die Identität. Aus Theorem 6.4.2 ergibt sich, dass $L^G \subset L$ eine Galois-Erweiterung ist. Somit gilt $[L : L^G] = |\mathrm{Aut}(L/L^G)|$ wegen Lemma 6.1.6. Hiermit ist alles gezeigt. □

7. Abschluss: Konstruierbarkeit des regelmässigen n-Ecks

7.1. **Überblick.** Wir sind nun am Ende dieser Vorlesung angelangt. Ziel des letzten Abschnittes ist der Beweis des folgenden Satzes, der den Satz 5.1.13 präzisiert.

Satz 7.1.1. *Es sei $n \in \mathbb{N}$. Die folgenden Aussagen sind äquivalent.*

(1) *Die Zahl $\zeta_n \in \mathbb{C}$ gehört zu $\mathbb{K}$.*
(2) *Der Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ ist eine Potenz von 2.*
(3) *n ist von der Form*
$$n = 2^k p_1 \cdots p_r,$$
wobei die p_i paarweise verschiedene Fermat-Primzahlen sind.

Ein Teil davon ist mit der bisher entwickelten Theorie einfach.

Beweis von $1 \Rightarrow 2$. Durch Satz 5.1.5 wissen wir, dass eine Körpererweiterung $\mathbb{Q} \subset K$ existiert mit $\zeta_n \in K$ und $[K : \mathbb{Q}] = 2^k$. Es folgt $\mathbb{Q}(\zeta_n) \subset K$ und daher ist wegen der Gradformel $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ ein Teiler von $[K : \mathbb{Q}]$, also selber eine Potenz von 2. □

Der entscheidende Punkt für den Beweis der Implikation $2 \Rightarrow 1$ und die Äquivalenz $2 \Leftrightarrow 3$ ist die Berechnung der Galois-Gruppe von $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$. In Lemma 6.3.3 haben wir einen injektiven Gruppenhomomorphismus

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}/n^\times \tag{7.1.2}$$

konstruiert, und wenn n eine Primzahl ist, so ist (7.1.2) ein Isomorphismus. Wir werden beweisen:

Satz 7.1.3. *Der Homorphismus* (7.1.2) *ist ein Isomorphismus, für jedes n. Insbesondere gilt*
$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n)^\times|.$$

Für den Beweis der Äquivalenz $2 \Leftrightarrow 3$ in Satz **??** fehlt die Berechnung von $|(\mathbb{Z}/n)^\times|$.

Satz 7.1.4. *Ist $n = 2^k p_1^{m_1} \cdots p_r^{m_r}$ die Primfaktorzerlegung von n mit ungeraden Primzahlen p_j, so ist*
$$|(\mathbb{Z}/n)^\times| = 2^{k-1} \prod_{j=1}^{r} (p_j - 1) p_j^{m_j - 1}.$$

Diese Zahl ist eine Potenz von 2 genau dann, wenn n von der Form $2^k p_1 \cdots p_r$ mit paarweise verschiedenen Fermat-Primzahlen ist. Dies zeigt die Äquivalenz $2 \Leftrightarrow 3$.

Für die Implikation $2 \Rightarrow 1$ beweisen wir einen gruppentheoretischen Satz:

Satz 7.1.5. *Es sei p eine Primzahl und G eine kommutative Gruppe mit $|G| = p^k$. Dann gibt es eine Folge von Untergruppen*
$$G_1 \subset \ldots \subset G_k = G$$
mit $|G_j| = p^j$.

Der Satz stimmt auch für nichtkommutative Gruppen, mit einem schwierigeren Beweis.

Beweis der Implikation $2 \Rightarrow 1$. Die Galoisgruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ ist kommutativ und ihre Ordnung ist eine Potenz von 2. Wir können daher eine Kette von Untergruppen wie in Satz 7.1.5 wählen. Dann ist

$$\mathbb{Q} = \mathbb{Q}(\zeta_n)^{G_k} \subset \ldots \subset \mathbb{Q}(\zeta_n)^{G_1} \subset \mathbb{Q}(\zeta_n)$$

eine Kette von Körpererweiterungen, und der Grad jeder einzelnen Erweiterung ist, nach dem Hauptsatz der Galois-Theorie, gleich 2. Somit ist $\zeta_n \in \mathbb{K}$, nach Satz 5.1.5. □

7.2. **Die Einheiten im Restklassenring modulo n.** Unser erstes Ziel ist der Beweis von Satz (7.1.4), welcher die Ordnung der Gruppe $(\mathbb{Z}/n)^\times$ der multiplikativen Einheiten in $\mathbb{Z}/n$ berechnet. Das folgende Lemma ist ein Spezialfall von Satz 3.2.10.

Lemma 7.2.1. *Sei $a \in \mathbb{Z}$. Dann ist die Restklasse $[a] \in \mathbb{Z}/n$ genau dann eine Einheit, wenn $\mathrm{ggT}(a, n) = 1$ ist.*

Korollar 7.2.2. *Es gilt*

$$|\mathbb{Z}/n^\times| = \varphi(n),$$

wobei die Eulersche φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ *durch*

$$\varphi(n) := |\{k \in \{1, \ldots, n-1\} | \mathrm{ggT}(k, n) = 1\}|$$

definiert ist. □

Der folgende Satz erlaubt die Berechnung von $\varphi(n)$, wenn die Primfaktorzerlegung von n bekannt ist.

Satz 7.2.3. *Es gilt:*

(1) *ist p eine Primzahl, so gilt $\varphi(p) = p - 1$,*
(2) *$\varphi(p^n) = p^{n-1}(p-1)$,*
(3) *wenn $\mathrm{ggT}(m, n) = 1$, so ist $\varphi(mn) = \varphi(m)\varphi(n)$.*

Beweis. Die erste Aussage ist klar, denn jedes $1 \leq k \leq p-1$ ist teilerfremd zu p. Für die zweite Aussage bemerke, dass $\mathrm{ggT}(k, p^n) = 1$ genau dann, wenn $\mathrm{ggT}(k, p) = 1$. Somit sind die zu p^n nicht teilerfremden Zahlen $1 \leq k \leq p^n - 1$ genau die Zahlen

$$p, 2p, 3p, \ldots, (p^{n-1} - 1)p,$$

und das sind genau $(p^{n-1} - 1)$ Stück. Also ist

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

Die dritte Aussage ist am besten mit einem Stück abstrakter Algebra zu beweisen. □

Für zwei Ringe R und S (kommutativ und mit Eins) ist das direkte Produkt $R \times S$ die Menge $R \times S$, ausgestattet mit den Verknüpfungen $(r, s) + (r', s') := (r + r', s + s')$ und $(r, s)(r', s') := (rr', ss')$. Es ist klar, dass $R \times S$ ein kommutativer Ring mit Eins ist. Des weiteren gilt

$$(R \times S)^\times = R^\times \times S^\times.$$

Satz 7.2.4 (Chinesischer Restsatz)**.** *Es sei* $\mathrm{ggT}(n,m)=1$*. Dann ist der Ringhomomorphismus*

$$\pi : \mathbb{Z} \to \mathbb{Z}/n \times \mathbb{Z}/m;\ \pi(k) := ([k]_n, [k]_m)$$

surjektiv, und der Kern von π *ist das Ideal* (mn)*. Es ist*

$$\mathbb{Z}/mn \cong \mathbb{Z}/n \times \mathbb{Z}/m$$

und

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

Beweis. Wähle $a, b \in \mathbb{Z}$ mit $an + bm = 1$. Für $k, l \in \mathbb{Z}$ ist dann

$$\pi(aln+bkm) = ([aln+bkm]_n, [aln+bkm]_m) = ([bkm]_n, [aln]_m) = ([k-ank]_n, [l-bml]_m) = ([k]_n, [l]_m),$$

also ist π surjektiv. Weil der Ring $\mathbb{Z}/n \times \mathbb{Z}/m$ genau mn Elemente hat, muss der Kern von π gerade das Ideal (mn) sein. Es folgt

$$\mathbb{Z}/mn \cong \mathbb{Z}/n \times \mathbb{Z}/m$$

und somit

$$(\mathbb{Z}/mn)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$$

und durch Abzählen $\varphi(mn) = \varphi(n)\varphi(m)$. □

Korollar 7.2.5. *Es gilt:* $|(\mathbb{Z}/n)^\times| = \varphi(n)$ *ist eine Potenz von* 2 *genau dann, wenn* $n = 2^k p_1 \cdots p_r$ *ein Produkt aus einer* 2*er-Potenz und paarweise verschiedenen Fermat-Primzahlen ist.*

Beweis von Satz 7.1.4. Es sei

$$n = 2^k p_1^{m_1} \cdots p_r^{m_r}$$

die Primfaktorzerlegung von n, mit ungeraden, paarweise verschiedenen Primzahlen p_j. Aus Satz 7.2.3 folgt

$$\varphi(n) = \varphi(2^k) \prod_{j=1}^{r} \varphi(p_j^{m_j}) = 2^{k-1} \prod_{j=1}^{r} p_j^{m_j-1}(p_j - 1).$$

□

7.3. **Der Grad des Kreisteilungskörpers.** Wir wollen uns nun dem Beweis von Satz 7.1.3 zuwenden, welcher besagt, dass der Homomorphismus

$$\kappa : \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}/n^\times$$

bijektiv ist. Injektivität folgt aus Lemma 6.3.3, und es bleibt, die Surjektivität zu zeigen. Dafür genügt es, zu zeigen, dass

$$|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |\mathbb{Z}/n^\times|$$

gilt. Andererseits ist

$$|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \overset{\text{Satz 4.3.7}}{=} \deg(\mu_{\mathbb{Q},\zeta_n}(x)),$$

und

$$|\mathbb{Z}/n^\times| = \varphi(n).$$

Also müssen wir nur noch

$$\deg(\mu_{\mathbb{Q},\zeta_n}(x)) = \varphi(n) \tag{7.3.1}$$

zeigen. Dies ist, was wir beweisen werden, um den Beweis von Satz 7.1.1 und diese Vorlesung zu beenden.

Wir erinnern daran, dass

$$C_n = \{z \in \mathbb{C} | z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\} \subset \mathbb{C}^\times.$$

Definition 7.3.2. *Es sei $z \in \mathbb{C}^\times$ und es gelte $z^n = 1$ für ein $n \in \mathbb{N}$. Die* Ordnung $\mathrm{ord}(z)$ *von z ist die kleinste Zahl $k \in \mathbb{N}$, so dass $z^k = 1$.*

Lemma 7.3.3. *Die Ordnung $\mathrm{ord}(z) \in \mathbb{N}$ eines Elements $z \in C_n$ ist ein Teiler von n.*

Beweis. Sei $k = \mathrm{ord}(z)$, $d := \mathrm{ggT}(k, n)$ und wähle $a, b \in \mathbb{Z}$ mit $ak + bn = d$. Es gilt dann

$$z^d = z^{ak+bn} = (z^k)^a (z^n)^b = 1$$

und nach der Definition der Ordnung ist $d \geq k$. Es gilt aber auch $\mathrm{ggT}(k, n) \leq k$, also $k = d$, also ist k ein Teiler von n. □

Definition 7.3.4. *Eine* primitive n-te Einheitswurzel *ist eine Zahl $w \in \mathbb{C}^\times$, so dass $\mathrm{ord}(w) = n$ ist. Mit anderen Worten, es gilt $w^n = 1$, und n ist die kleinste Zahl mit dieser Eigenschaft. Mit*

$$A_n := \{w \in \mathbb{C}^\times | \mathrm{ord}(w) = n\} \subset C_n \subset \mathbb{C}^\times$$

bezeichnen wir die Menge der primitiven n-ten Einheitswurzeln.

Die Menge A_d ist *keine* Untergruppe. Beispielsweise ist

$$A_1 = \{1\},$$
$$A_2 = \{-1\},$$
$$A_3 = \{\zeta_3, \zeta_3^2\},$$
$$A_4 = \{\pm i\}.$$

Lemma 7.3.5. *Für ein Element $w \in C_n$ sind äquivalent:*

1. *$w \in A_n$,*
2. *$w = \zeta_n^m$, mit $\mathrm{ggT}(m, n) = 1$,*
3. *es gibt l mit $\zeta_n = w^l$.*

Beweis. $1 \Rightarrow 3$: falls $\mathrm{ord}(w) = n$, so sind die n Elemente

$$w, w^2, \dots, w^{n-1}, w^n = 1 \in C_n$$

paarweise verschieden (sonst würde $w^a = 1$ für ein $0 < a < n$ gelten). Weil C_n genau n Elemente hat, muss eines der Elemente aus der obigen Liste gleich ζ_n sein.

$3 \Rightarrow 2$: Es gibt m mit $w = \zeta_n^m$. Es folgt

$$\zeta_n = w^l = \zeta_n^{ml},$$

und daher

$$ml \equiv 1 \pmod{n}.$$

Daraus folgt, dass m und n teilerfremd sind.

$2 \Rightarrow 1$: ist $w^k = 1$, so ist $\zeta_n^{mk} = 1$, also $mk \equiv 0 \pmod{n}$. Weil aber m und n teilerfremd sind, folgt $n | k$, also $\mathrm{ord}(w) = n$. □

Lemma 7.3.6. (1) *Die Mengen A_d sind paarweise disjunkt.*

(2) *Für jedes $n \in \mathbb{N}$ gilt*

$$C_n = \coprod_{d|n} A_d. \tag{7.3.7}$$

(3) *Es gilt* $|A_n| = \varphi(n)$.

Beweis. (1) ist klar: die Ordnung eines Elementes in $\mathbb{C}^\times$ ist eine wohldefinierte Zahl. (2): ist d ein Teiler von n und $w \in A_d$, so gilt $w^d = 1$ und erst recht $w^n = 1$, also $w \in C_n$. Somit ist die rechte Seite in der linken Seite enthalten. Ist umgekehrt $w \in C_n$, so ist $\mathrm{ord}(w)$ ein Teiler von n, und $w \in A_{\mathrm{ord}(w)}$. Aus Lemma **??** folgt

$$A_n = \{\zeta_n^a | \mathrm{ggT}(a,n) = 1\},$$

und daher

$$|A_n| = |\{a \in \underline{n-1} | \mathrm{ggT}(a,n) = 1\}| = \varphi(n)$$

nach der Definition der Eulerschen φ-Funktion. □

Nun setzen wir

$$F_n(x) := x^n - 1 = \prod_{w \in C_n} (x - w) \in \mathbb{Z}[x]$$

und

$$\phi_n(x) := \prod_{w \in A_n} (x - w) \in \mathbb{C}[x].$$

Das Polynom $\phi_n(x)$ ist normiert, und weil $\zeta_n \in A_n$, gilt

$$\phi_n(\zeta_n) = 0.$$

Ferner ist (wegen Lemma 7.3.8 (5))

$$\deg(\phi_n(x)) = \varphi(n).$$

A priori ist $\phi_n(x)$ ein Polynom mit komplexen Koeffizienten. Wenn wir zeigen können, dass $\phi_n(x)$ in Wahrheit rationale Koeffizienten hat und dass $\phi_n(x)$ irreduzibel in $\mathbb{Q}[x]$ ist, so ist $\phi_n(x)$ das Minimalpolynom von ζ_n über $\mathbb{Q}$, und es folgt die Gleichung (7.3.1), womit der Beweis von Satz 7.1.3 erbracht wäre.

Lemma 7.3.8. *Für jedes $n \in \mathbb{N}$ ist $\phi_n(x) \in \mathbb{Z}[x]$.*

Beweis. Induktion über n. Der Fall $n = 1$ ist klar, denn $\phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Die Zerlegung (7.3.9) übersetzt sich in die Formel

$$F_n(x) = \prod_{d|n} \phi_d(x). \tag{7.3.9}$$

Nun ist

$$x^n - 1 = F_n(x) = \prod_{d|n} \phi_d(x) = \phi_n(x) \prod_{d|n, d<n} \phi_d(x).$$

Das Produkt und der zweite Faktor sind offensichtlich beziehungsweise nach Induktionsannahme ganzzahlig und normiert, und das Lemma von Gauss (oder genauer gesagt Lemma 3.4.8) impliziert, dass $\phi_n(x)$ ganze Koeffizienten hat. □

Satz 7.3.10. *Das Polynom $\phi_n(x) \in \mathbb{Z}[x]$ ist irreduzibel in $\mathbb{Q}[x]$.*

Für den Beweis benötigen wir ein Lemma.

Lemma 7.3.11. *Es sei $w \in A_n$ eine primitive $n$te Einheitswurzel, und p sei eine Primzahl mit $\mathrm{ggT}(p,n) = 1$. Sei ferner $f(x) \in \mathbb{Q}[x]$ ein irreduzibles normiertes Polynom mit $f(w) = 0$. Dann gilt $f(w^p) = 0$.*

Beweis. Weil $f(x)$ und x^n-1 in $\mathbb{C}$ die gemeinsame Nullstelle w haben, ist $\mathrm{ggT}_{\mathbb{C}}(f, x^n-1) \neq 1$ und daher $\mathrm{ggT}_{\mathbb{Q}}(f, x^n-1) \neq 1$. Weil f irreduzibel ist, folgt $f|x^n-1$, und wir können

$$F_n(x) = x^n - 1 = f(x)g(x)$$

schreiben, wobei $g(x) \in \mathbb{Q}[x]$. Aus dem Lemma von Gauss (oder genauer gesagt Lemma 3.4.8) folgt, dass sowohl f als auch g ganzzahlige Koeffizienten haben.

Wir wollen $f(w^p) = 0$ zeigen und argumentieren durch Widerspruch. Es sei also angenommen, dass $f(w^p) \neq 0$, und weil $F_n(w^p) = 0$, folgt $g(w^p) = 0$.

Mit anderen Worten, w ist eine Nullstelle des Polynoms $g(x^p) \in \mathbb{Z}[x]$. Damit sind $f(x)$ und $g(x^p)$ in $\mathbb{C}[x]$ nicht teilerfremd (sie haben die gemeinsame Nullstelle $w \in \mathbb{C}$), und somit folgt $\mathrm{ggT}_{\mathbb{Q}}(f(x), g(x^p)) \neq 1$. Wieder weil f irreduzibel ist, folgt die Existenz eines Polynoms $h(x) \in \mathbb{Q}[x]$ mit

$$g(x^p) = f(x)h(x).$$

Eine weitere Anwendung von Lemma 3.4.8 zeigt, dass $h(x) \in \mathbb{Z}[x]$.

Nun reduzieren wir modulo p: sei $\pi_* : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ durch Reduktion der Koeffizienten modulo p gegeben. Es folgt

$$\pi_*(F_n(x)) = \pi_*(f(x))\pi_*(g(x)) \in \mathbb{F}_p[x]$$

und

$$\pi_*(g(x^p)) = \pi_*(f(x))\pi_*(h(x)) \in \mathbb{F}_p[x].$$

Nun erscheint ein *deus ex machina* auf der Bühne, und wir unterbrechen den Beweis für ein weiteres Lemma. □

Lemma 7.3.12. *Es sei $g(x) \in \mathbb{F}_p[x]$ ein Polynom. Dann gilt $g(x^p) = g(x)^p$.*

Beweis. Beweis durch Induktion über den Grad von g. Zunächst zeigen wir, dass für jedes $a \in \mathbb{F}_p$ die Gleichung $a^p = a$ gilt. Dies ist klar für $a = 0$. Andernfalls ist $a \in \mathbb{F}_p$ eine Einheit, und weil $|\mathbb{F}_p^\times| = p-1$, folgt $a^{p-1} = 1$ für jedes $a \in \mathbb{F}_p$. Nun sei $g(x) = h(x) + bx^n$, $\deg(h) \leq n-1$. Aus dem binomischen Lehrsatz folgt

$$g(x)^p = \sum_{k=0}^{p} \binom{p}{k} h(x)^k b^{p-k} x^{n(p-k)},$$

und weil alle Binomialkoeffizienten (außer für $k = 0, p$) durch p teilbar sind, ist dies gleich

$$\binom{p}{0} h(x)^0 b^p x^p + \binom{p}{p} h(x)^p = b^p x^p + h(x)^p =$$

($b^p = b$ und Induktionsannahme)

$$= bx^p + h(x^p) = g(x^p).$$ □

Beweis von Lemma 7.3.13, Fortsetzung. Aus Lemma 7.3.14 und dem ersten Teil des Beweises folgt

$$\pi_* F_n(x) = \pi_*(f(x))\pi_*(g(x)) \in \mathbb{F}_p[x]$$

und

$$\pi_*(g(x))^p = \pi_*(f(x))\pi_*(h(x)) \in \mathbb{F}_p[x].$$

Ist $q(x) \in \mathbb{F}_p[x]$ irreduzibel mit $q(x)|\pi_*(f(x))$, so ist damit

$$q(x)|\pi_*(g(x))^p \Rightarrow q(x)|\pi_*(g(x)),$$

und es folgt

$$q(x)^2 | \pi_*(F_n(x)) = x^n - 1.$$

Damit ist $x^n - 1 \in \mathbb{F}_p[x]$ nicht separabel. Aber die formale Ableitung ist

$$(x^n - 1)' = nx^{n-1} \neq 0$$

(hier haben wir zu guter Letzt die Vorassetzung $\mathrm{ggT}(p, n) = 1$ verwendet!). Das ist ein Widerspruch zur Annahme, dass $f(w^p) \neq 0$. □

Beweis von Satz 7.3.12. Es sei $w \in C_n$ eine primitive Einheitswurzel und es sei $f(x) \in \mathbb{Q}[x]$ das Minimalpolynom von w über $\mathbb{Q}$. Wir zeigen, dass jede andere primitive Einheitswurzel eine Nullstelle von $f(x)$ ist. Daraus folgt, dass $\phi_n(x)|f(x)$, und weil $f(x)$ irreduzibel ist, dass $\phi_n(x)$ irreduzibel ist.

Nun ist jedes $v \in C_n$ von der Form w^a für ein $a \in \mathbb{Z}$, und v ist primitiv genau dann, wenn $\mathrm{ggT}(a, n) = 1$. Wir schreiben

$$a = p_1 \cdots p_r$$

mit nicht notwendig verschiedenen Primzahlen p_i, die allesamt n nicht teilen. Aus dem Lemma 7.3.13 folgt, dass

$$w^{p_1}$$

eine Nullstelle von f ist. Aber w^{p_1} ist primitiv, und daher ist auch

$$w^{p_1 p_2}$$

eine Nullstelle von f, durch Wiederholung des Argumentes. r-fache Iteration der Schlussweise zeigt, dass $f(w^a) = 0$, wie gewünscht. □

7.4. **Etwas Gruppentheorie.** Schlussendlich wollen wir Satz 7.1.5 zeigen, wofür ein kurzer Ausflug in die Gruppentheorie erforderlich ist. Wir beginnen mit Definitionen.

Definition 7.4.1. *Es sei G eine Gruppe und $H \subset G$ eine Untergruppe. Die* Linksnebenklasse *gH von g ist die Menge*

$$gH := \{gh | h \in H\} \subset G.$$

Die Menge der Linksnebenklassen wird mit G/H bezeichnet, und $\pi : G \to G/H$, $\pi(g) := gH$ sei die Quotientenabbildung.

Analog zum Fall von Ringen wollen wir eine Verknüpfung auf G/H erklären, welche G/H zu einer Gruppe macht und π zu einem Gruppenhomomorphismus. Das geht nicht immer, und eine zusätzliche Bedingung ist notwendig.

Definition 7.4.2. *Es sei G eine Gruppe. Eine* normale Untergruppe *$H \subset G$ ist eine Untergruppe, so dass gilt: für $h \in H$ und $g \in G$ ist $ghg^{-1} \in H$.*

Satz 7.4.3. *Es sei G eine Gruppe und $H \subset G$ eine normale Untergruppe. Dann gibt es genau eine Verknüpfung $G/H \times G/H \to G/H$, welche G/H zu einer Gruppe macht, und π zu einem Gruppenhomomorphismus.*

Beweis. Die Eindeutigkeit ist schnell zu zeigen: ist π ein Gruppenhomomorphismus, so muss

$$g_0 H \cdot g_1 H = \pi(g_0)\pi(g_1) = \pi(g_0 g_1) = g_0 g_1 H$$

gelten. Wir haben also keine Wahl, als

$$(g_0 H)(g_1 H) := (g_0 g_1) H$$

zu setzen, und müssen uns überlegen, wann dies wohldefiniert ist. Offenbar gilt

$$gH = g'H \Leftrightarrow g^{-1}g' \in H.$$

Wenn $g_0H = g_0'H$ und $g_1H = g_1'H$, so ist also $g_1^{-1}g_1', g_0^{-1}g_0' \in H$. Es folgt

$$(g_0g_1)^{-1}g_0'g_1' = g_1^{-1}g_0^{-1}g_0'g_1' = g_1^{-1}(g_0^{-1}g_0')g_1(g_1^{-1}g_1').$$

Dies ist ein Element von H, weil H eine normale Untergruppe ist. Also gilt:

$$(g_0H = g_0'H \wedge g_1H = g_1'H) \Rightarrow g_0g_1H = g_0'g_1'H,$$

und die Verknüpfung ist wohldefiniert. Der Nachweis, dass die Verknüpfung assoziativ ist, ein neutrales Element und inverse Elemente besitzt, ist Fleißarbeit, und es ist klar, dass π ein Gruppenhomomorphismus ist. □

Definition 7.4.4. *Es sei G eine endliche Gruppe. Die* Ordnung *von G ist die Mächtigkeit der Menge G.*

Satz 7.4.5 (Satz von Lagrange)**.** *Es sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$. Die Zahl $[G : H] := \frac{|G|}{|H|}$ heißt der* Index von H in G.

Beweis. Wir betrachten die Restklassenabbildung $\pi : G \to G/H$. Das Urbild $\pi^{-1}(gH) \subset G$ ist gerade die Linksnebenklasse gH von g. Die Abbildung

$$H \to gH,\ h \mapsto gh$$

ist bijektiv, und daher hat jede Linksnebenklasse genau $|H|$ viele Elemente. Es folgt

$$|G| = |G/H||H|.$$

□

Korollar 7.4.6. *Es sei G eine endliche Gruppe und $g \in G$. Die kleinste positive Zahl n mit $g^n = 1$ wird als Ordnung* $\mathrm{ord}(g)$ *von g bezeichnet, und ist ein Teiler von $|G|$.*

Beweis. Die Menge $\langle g\rangle := \{g^n | n \in \mathbb{Z}\} \subset G$ ist eine Untergruppe, deren Ordnung daher die Ordnung von G teilt. □

Beweis von Satz 7.1.5. Der Beweis wird durch Induktion über k geführt. Im Fall $k = 1$ ist nichts zu zeigen, denn $\{1\} \subset G$ ist bereits die gewünschte Kette von Untergruppen. Sei nun $|G| = p^k$, und der Satz sei für Gruppen der Ordnung p^{k-1} bereits bewiesen. Wähle ein Element $g \in G$, das vom neutralen Element 1 verschieden ist. Die Ordnung $\mathrm{ord}(g)$ ist ein Teiler von p^k, sagen wir p^r, wobei $r \geq 1$, weil $g \neq 1$. Das Element

$$h := g^{p^{r-1}} \in G$$

ist nicht das neutrale Element, und es gilt $h^p = 1$ nach Definition. Weil p eine Primzahl ist, ist dann $\mathrm{ord}(h) = p$, und die Untergruppe $H := \langle h\rangle \subset G$ hat Ordnung p.

Nun haben wir G als kommutativ vorausgesetzt. Das impliziert, dass H eine normale Untergruppe ist, denn für $g \in G$ und $k \in H$ gilt

$$gkg^{-1} = gg^{-1}k = k \in H.$$

Die Quotientengruppe G/H hat die Ordnung $|G|/|H| = p^{k-1}$. Die Induktionsannahme zeigt, dass eine Folge

$$\{1H\} \subset K_1 \subset \ldots K_{k-1} = G/H$$

von Untergruppen existiert, mit $|K_j| = p^j$. Setze nun $G_1 := H$ und $G_j := \pi^{-1}(K_{j-1})$ für $j \geq 2$. Es ist dann

$$G_1 \subset G_2 \subset G_k = G$$

eine Folge von Untergruppen. Man kann durch eine ähnliche Überlegung wie im Satz von Lagrange zeigen, dass

$$|\pi^{-1}(K_{j-1})| = p|K_{j-1}| = pp^{j-1} = p^j$$

gilt. Somit ist gezeigt, dass $|G_j| = p^j$, und der Beweis ist fertig. □

Wie bereits gesagt, stimmt der Satz auch für nichtkommutative G. Der Beweis geht im wesentlichen genau so, nur dass der entscheidende Schritt, eine normale Untergruppe der Ordnung p zu finden, schwieriger ist.

Literatur