

# ALGEBRA

PETER FIEBIG

Z . Dies ist das Skript zur Vorlesung Algebra im Wintersemester 2006/07. Die fünf wesentlichen Themen der Vorlesung waren Gruppen, Ringe, Körper, Galois-theorie und die Transzendenz von  $\pi$ .

## I

1. Gruppen	2
1.1. Homomorphismen von Gruppen	3
1.2. Untergruppen	4
1.3. Der Satz von Cayley	5
1.4. Der größte gemeinsame Teiler	5
1.5. Eindeutigkeit der Primfaktorzerlegung	6
1.6. Normalteiler und Faktorgruppen	6
1.7. Zyklische Gruppen	9
1.8. Der chinesische Restsatz	10
1.9. Der Hauptsatz für endlich erzeugte abelsche Gruppen	10
1.10. Freie abelsche Gruppen	11
1.11. Torsionsgruppen	12
1.12. Kompositionsreihen	15
1.13. Operationen von Gruppen	16
1.14. Konjugationsklassen	17
1.15. Sylow Untergruppen	18
1.16. Auflösbare Gruppen	19
1.17. Symmetrische und alternierende Gruppen	20
2. Ringe	21
2.1. Ideale	23
2.2. Primkörper	24
2.3. Potenzreihen und Polynomringe	25
2.4. Nullstellen von Polynomen	25
2.5. Primideale und maximale Ideale	27
2.6. Der chinesische Restsatz	27
2.7. Irreduzible und prime Elemente	28
2.8. Faktorielle Ringe	29
2.9. Hauptidealringe	29
2.10. Euklidische Ringe	30

2.11.	Der Quotientenkörper	30
2.12.	Primfaktorzerlegung in Polynomringen	32
2.13.	Das Eisensteinkriterium	33
2.14.	Kreisteilungspolynome	34
3.	Körper	35
3.1.	Körpererweiterungen	35
3.2.	Algebraische Körpererweiterungen	37
3.3.	Mit Zirkel und Lineal konstruierbare Zahlen	38
3.4.	Die Quadratur des Kreises	41
3.5.	Einschub: Endliche Untergruppen der Drehgruppe	41
3.6.	Endliche Körper	42
3.7.	Zerfällungskörper	44
3.8.	Normale Körpererweiterungen	46
3.9.	Separable Körpererweiterungen	47
4.	Galoistheorie	50
4.1.	Die Galoisgruppe	50
4.2.	Galoiserweiterungen	51
4.3.	Die Galois Korrespondenz	51
4.4.	Der Hauptsatz der Algebra	53
4.5.	$n$ -te Einheitswurzeln	53
4.6.	Galoisgruppen der Kreisteilungskörper	54
4.7.	Adjunktion $n$ -ter Wurzeln	56
4.8.	Auflösbarkeit polynomialer Gleichungen in Charakteristik Null	58
4.9.	Die allgemeine polynomiale Gleichung vom Grad $\geq 5$ ist nicht auflösbar	60
4.10.	Der algebraische Abschluß	60
5.	Die Transzendenz von $\pi$	63
5.1.	Symmetrische Polynome	63
5.2.	Der Beweis des Satzes von Lindemann	64

## 1. G

**Definition 1.1.** Eine *Halbgruppe* ist eine Menge  $M$ , auf der eine assoziative Verknüpfung  $\cdot : M \times M \rightarrow M$ ,  $(a, b) \mapsto a \cdot b$  erklärt ist (also gilt  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  für alle  $a, b, c \in M$ ). Die Halbgruppe heißt *kommutativ*, oder *abelsch*, wenn  $a \cdot b = b \cdot a$  für alle  $a, b \in M$  gilt.

*Beispiele 1.2.* (1) Sei  $X$  eine Menge. Die Menge  $\text{Abb}(X)$  aller Abbildungen von  $X$  nach  $X$  zusammen mit der Verknüpfung von Abbildungen ist eine Halbgruppe.  $\text{Abb}(X)$  ist genau dann kommutativ, wenn  $X$  nur aus einem Element besteht.

(2) Die Menge der natürlichen Zahlen  $\mathbb{N} = \{0, 1, 2, \dots\}$  mit der Addition ist eine kommutative Halbgruppe.

*Anmerkung 1.3.* Die Verknüpfung wird auch *Multiplikation* genannt oder *Addition*, wenn die Gruppe kommutativ ist. Im kommutativen Fall notiert man die Verknüpfung oft auch durch “+” statt “·”.

**Definition 1.4.** Ein Element  $e$  einer Halbgruppe  $M$  heißt *linksneutral*, wenn  $e \cdot a = a$  gilt für alle  $a \in M$ . Entsprechend heißt  $f \in M$  *rechtsneutral*, wenn  $a \cdot f = a$  gilt für alle  $a \in M$ .

**Lemma 1.5.** *Gibt es in der Halbgruppe  $M$  sowohl ein linksneutrales Element  $e$  als auch ein rechtsneutrales Element  $f$ , so gilt  $e = f$ .*

*Beweis.*  $e = e \cdot f = f$ . □

**Definition 1.6.** Ein sowohl links- als auch rechtsneutrales Element heißt das *neutrale Element*, das *Einselement*, die *Eins* oder auch, im abelschen Fall, das *Nullelement* oder die *Null* in  $M$ .

Wir schreiben auch oft  $e_M$  für das neutrale Element in der Halbgruppe  $M$ .

Sei nun  $M$  eine Halbgruppe mit Einselement  $e$ .

**Definition 1.7.** Sind  $a, b \in M$  und gilt  $a \cdot b = e$ , so heißt  $a$  ein *Links inverses* von  $b$ , und entsprechend  $b$  ein *Rechts inverses* von  $a$ .

**Lemma 1.8.** *Hat  $a$  ein Links inverses  $a'$  und ein Rechts inverses  $a''$ , so gilt  $a' = a''$ .*

*Beweis.*  $a' = a' \cdot e = a' \cdot a \cdot a'' = e \cdot a'' = a''$ . □

**Definition 1.9.** Ein zu  $a$  sowohl linksinverses als auch rechtsinverses Element  $a'$  heißt das *Inverse* zu  $a$  und wird mit  $a^{-1}$ , und im abelschen Fall mit  $-a$ , bezeichnet.

**Definition 1.10.** Eine *Gruppe* ist eine Halbgruppe, in der ein neutrales Element und zu jedem Element ein Inverses existieren.

*Beispiele 1.11.* (1)  $\mathbb{Z}$  mit “+”.

(2)  $\mathbb{Q}$  mit “+”.

(3)  $\mathbb{Q} \setminus \{0\}$  oder  $\mathbb{Q}_{>0}$  mit “·”.

(4) Ist  $X$  eine Menge, so ist  $\text{Sym}(X) = \{f \in \text{Abb}(X) \mid f \text{ ist bijektiv}\}$  mit der Verknüpfung von Abbildungen eine Gruppe, die *symmetrische Gruppe* über  $X$ . Wir definieren  $S_n := \text{Sym}(\{1, \dots, n\})$ .

(5) Ist  $V$  ein Vektorraum, so ist  $\text{GL}(V) = \{f: V \rightarrow V \mid f \text{ ist linear und invertierbar}\}$  eine Gruppe, die *lineare Gruppe* über  $V$ .

**1.1. Homomorphismen von Gruppen.** Seien  $G, H$  Gruppen.

**Definition 1.12.** Eine Abbildung  $\phi: G \rightarrow H$  heißt *Homomorphismus von Gruppen* oder kurz *Homomorphismus*, falls für alle  $a, b \in G$  gilt  $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ .

**Lemma 1.13.** *Ist  $\phi: G \rightarrow H$  ein Homomorphismus, so ist  $\phi(e_G) = e_H$  und  $\phi(a^{-1}) = \phi(a)^{-1}$  für alle  $a \in G$ .*

*Beweis.* Es ist  $\phi(e_G) \cdot \phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G)$ , und wir erhalten die Gleichung  $\phi(e_G) = e_H$  durch Linksmultiplikation mit  $\phi(e_G)^{-1}$ . Dann ist  $e_H = \phi(e_G) = \phi(a^{-1} \cdot a) = \phi(a^{-1}) \cdot \phi(a)$ , also ist  $\phi(a^{-1})$  invers zu  $\phi(a)$ . □

**Definition 1.14.** Ein Homomorphismus  $\phi: G \rightarrow H$  heißt

- *injektiv*, falls aus  $\phi(a) = \phi(b)$  folgt  $a = b$ ,
- *surjektiv*, falls für alle  $b \in H$  ein  $a \in G$  existiert mit  $\phi(a) = b$ ,
- *bijektiv* oder ein *Isomorphismus*, falls  $\phi$  injektiv und surjektiv ist.

Wir sagen, zwei Gruppen  $G$  und  $H$  sind *isomorph* und schreiben  $G \cong H$ , falls es einen Isomorphismus  $\phi: G \rightarrow H$  gibt.

*Anmerkung 1.15.* Eine Abbildung ist genau dann bijektiv, wenn sie invertierbar ist (als Abbildung zwischen Mengen).

- Übung 1.16.* (1) Sind  $\phi: G \rightarrow H$  und  $\psi: H \rightarrow I$  Homomorphismen von Gruppen, so ist auch  $\psi \circ \phi: G \rightarrow I$  ein Homomorphismus von Gruppen.  
 (2) Die inverse Abbildung eines bijektiven Homomorphismus ist ebenfalls ein Homomorphismus.

Die Notationen  $\phi: G \hookrightarrow H$ ,  $\phi: G \twoheadrightarrow H$ ,  $\phi: G \xrightarrow{\sim} H$  sollen im folgenden injektive, surjektive bzw. bijektive Abbildungen bezeichnen.

## 1.2. Untergruppen.

**Definition 1.17.** Eine Teilmenge  $U \subset G$  einer Gruppe heißt *Untergruppe*, wenn sie stabil ist unter der Verknüpfung (d.h. sind  $a, b$  in  $U$ , so auch  $a \cdot b$ ) und mittels dieser Verknüpfung selbst eine Gruppe ist.

*Anmerkung 1.18.* Notwendigerweise ist dann das neutrale Element in  $U$  auch das neutrale Element in  $G$ , und analoges gilt für das Inverse eines Elements  $a \in U$ .

- Beispiele 1.19.* (1) Jede Gruppe  $G$  enthält die *trivialen* Untergruppen  $\{e_G\}$  und  $G$ .  
 (2) Ist  $m \in \mathbb{Z}$ , so ist die Menge  $m\mathbb{Z} = \{n \cdot m \mid n \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$  eine Untergruppe von  $\mathbb{Z}$ .

**Lemma 1.20.** Jede Untergruppe von  $\mathbb{Z}$  ist von der Form  $m\mathbb{Z}$  für ein eindeutig bestimmtes  $m \in \mathbb{N}$ .

*Beweis.* Sei  $H \subset \mathbb{Z}$  eine Untergruppe. Ist  $H = \{0\}$ , so können und müssen wir  $m = 0$  wählen. Ansonsten sei  $m \in H$  die kleinste positive Zahl in  $H$  (eine solche gibt es, denn mit  $m$  ist auch  $-m \in H$ ). Wir wollen  $H = m\mathbb{Z}$  zeigen. Natürlich gilt  $m\mathbb{Z} \subset H$ . Ist  $x \in H \setminus m\mathbb{Z}$  und  $x > 0$ , so können wir  $r \in \mathbb{Z}$  maximal wählen mit  $rm < x$ . Also ist  $x - rm \in H$  und  $0 < x - rm < m$ , was der Wahl von  $m$  widerspricht.

Ist  $H = m\mathbb{Z} \neq \{0\}$ , so ist  $m$  eindeutig bestimmt als die kleinste positive Zahl in  $H$ .  
 $\square$

Sind  $H, H' \subset G$  Untergruppen, so ist auch  $H \cap H' \subset G$  eine Untergruppe. Ist  $X \subset G$  eine Teilmenge, so können wir die *von  $X$  erzeugte Untergruppe* definieren als

$$\langle X \rangle = \bigcap_{X \subset H \subset G, H \text{ Untergruppe}} H \subset G.$$

$\langle X \rangle$  ist die kleinste Untergruppe von  $G$ , die  $X$  enthält.

**Lemma und Definition 1.21.** Sei  $\phi: G \rightarrow H$  ein Gruppenhomomorphismus.

- (1) Die Menge  $\ker \phi := \{g \in G \mid \phi(g) = e\}$  ist eine Untergruppe von  $G$  und heißt der Kern von  $\phi$ .
- (2) Die Menge  $\operatorname{im} \phi := \{h \in H \mid \text{es gibt ein } g \in G \text{ mit } \phi(g) = h\}$  ist eine Untergruppe von  $H$  und heißt das Bild von  $\phi$ .

*Beweis.* Sind  $a, b \in \ker \phi$ , so  $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = e_H \cdot e_H = e_H$ , also ist  $\ker \phi$  abgeschlossen unter der Verknüpfung. Aus 1.13 folgt, daß  $e_G \in \ker \phi$  und mit  $a$  auch  $a^{-1}$  im Kern von  $\phi$  liegt.

Ist  $h = \phi(g), h' = \phi(g') \in \operatorname{im} \phi$ , so  $h \cdot h' = \phi(g) \cdot \phi(g') = \phi(g \cdot g') \in \operatorname{im} \phi$ , also ist  $\operatorname{im} \phi$  abgeschlossen unter der Verknüpfung. Aus 1.13 folgt, daß  $e_H \in \operatorname{im} \phi$  und mit  $h$  auch  $h^{-1}$  im Bild von  $\phi$  liegt.  $\square$

**Lemma 1.22.** Ein Gruppenhomomorphismus  $\phi: G \rightarrow H$  ist injektiv genau dann, wenn  $\ker \phi = \{e\}$ .

*Beweis.* Ist  $\phi$  injektiv, so folgt aus  $\phi(g) = e_H = \phi(e_G)$  schon  $g = e_G$ , also  $\ker \phi = \{e_G\}$ . Ist  $\ker \phi = \{e_G\}$  und  $\phi(a) = \phi(b)$ , so ist  $\phi(ab^{-1}) = e_H$ , also  $ab^{-1} = e_G$  oder  $a = b$ , also ist  $\phi$  injektiv.  $\square$

### 1.3. Der Satz von Cayley.

**Satz 1.23.** Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe  $\operatorname{Sym}(X)$ .

*Beweis.* Wir wählen  $X = G$  als Menge. Für  $g \in G$  ist die Abbildung  $\lambda_g: X \rightarrow X, \lambda_g(h) = gh$  eine bijektive Abbildung von  $X$  nach  $X$  (die inverse Abbildung ist offenbar  $\lambda_{g^{-1}}$ ). Dies definiert uns eine Abbildung

$$\begin{aligned} \lambda: G &\rightarrow \operatorname{Sym}(X) \\ g &\mapsto \lambda_g. \end{aligned}$$

Offenbar ist  $\lambda_{gg'} = \lambda_g \circ \lambda_{g'}$ , also ist  $\lambda$  ein Homomorphismus von Gruppen. Ist  $\lambda_g = \operatorname{id}_X$ , das neutrale Element in  $\operatorname{Sym}(X)$ , so gilt  $gx = x$  für alle  $x \in X$ , also  $g = e_G$ . Damit ist  $\lambda$  injektiv und induziert damit einen Isomorphismus  $G \cong \operatorname{im} \lambda \subset \operatorname{Sym}(X)$ .  $\square$

### 1.4. Der größte gemeinsame Teiler. Seien $a, b \in \mathbb{Z}$ .

**Definition 1.24.**  $a$  ist ein Teiler von  $b$  (oder  $a$  teilt  $b$ ), wenn es eine Zahl  $d$  gibt mit  $a \cdot d = b$ . In diesem Fall schreiben wir  $a|b$ .

Sind  $a, b \in \mathbb{Z}$  nicht beide Null, so gibt es eine größte Zahl  $d \in \mathbb{N}$  mit der Eigenschaft, daß  $d$  sowohl  $a$  als auch  $b$  teilt. Sie heißt der *größte gemeinsame Teiler* von  $a$  und  $b$  und wird mit  $d = \operatorname{ggT}(a, b)$  abgekürzt.

Die Zahlen  $a, b \in \mathbb{Z}$ , beide nicht Null, heißen *teilerfremd*, wenn  $\operatorname{ggT}(a, b) = 1$ .

**Satz 1.25.** Seien  $a, b \in \mathbb{Z}$  und nicht beide Null. So gibt es  $r, s \in \mathbb{Z}$  mit

$$\operatorname{ggT}(a, b) = ra + sb.$$

*Insbesondere: Teilt  $d$  sowohl  $a$  als auch  $b$ , so teilt  $d$  auch  $\operatorname{ggT}(a, b)$ .*

*Beweis.* Es ist

$$\langle a\mathbb{Z} \cup b\mathbb{Z} \rangle = \{ra + sb \mid r, s \in \mathbb{Z}\}$$

eine Untergruppe von  $\mathbb{Z}$ , also existiert  $c > 0$  mit  $c\mathbb{Z} = \{ra + sb \mid r, s \in \mathbb{Z}\}$ . Dann ist  $a = cd_1$  und  $b = cd_2$ ,  $c$  ist also ein gemeinsamer Teiler von  $a$  und  $b$  und es gibt  $r, s \in \mathbb{Z}$  mit  $c = ra + sb$ . Der  $\text{ggT}(a, b)$  teilt die rechte Seite dieser Gleichung, also auch  $c$ , folglich  $c = \text{ggT}(a, b)$ .  $\square$

### 1.5. Eindeutigkeit der Primfaktorzerlegung.

**Definition 1.26.** Eine *Primzahl* ist eine Zahl  $p \in \mathbb{N}$ ,  $p > 1$ , die genau zwei positive Teiler hat, nämlich 1 und  $p$ .

**Satz 1.27.** Für jede natürliche Zahl  $n \geq 2$  gibt es bis auf Reihenfolge eindeutig bestimmte Primzahlen  $p_1, \dots, p_r$  mit  $n = p_1 \cdots p_r$ .

*Beweis.* Wir zeigen die Existenz solcher Primzahlen per Induktion nach  $n$ . Für  $n = 2$  gibt es eine solche Zerlegung. Sei  $n > 2$  und  $p$  die kleinste Zahl  $> 1$ , die  $n$  teilt. Dann ist  $p$  eine Primzahl und  $n = p \cdot n'$  und eine Primzerlegung von  $n'$  (existiert nach Induktionsvoraussetzung) liefert uns eine Primzerlegung von  $n$ .

Um die Eindeutigkeit zu zeigen, benutzen wir folgendes Lemma.

**Lemma 1.28.** Sei  $p$  eine Primzahl. Ist  $p$  Teiler von  $a \cdot b$ , so ist  $p$  ein Teiler von  $a$  oder von  $b$ .

*Beweis.* Ist  $p$  kein Teiler von  $a$ , so ist  $\text{ggT}(a, p) = 1$ . Es gibt, nach Satz 1.25 Zahlen  $r, s \in \mathbb{Z}$  mit  $1 = rp + sa$ . Also gilt  $b = rpb + sab$ , und da  $p$  die beiden Summanden der rechten Seite teilt, teilt  $p$  auch die linke Seite.  $\square$

Sei nun  $n = p_1 \cdots p_r = q_1 \cdots q_s$  Produkt von Primzahlen  $p_1, \dots, p_r$  und  $q_1, \dots, q_s$ . So gibt es, nach dem Lemma, ein  $j$  mit  $p_1 | q_j$ , also  $p_1 = q_j$ . Dann ist  $p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$ , und per Induktion können wir annehmen, daß  $r - 1 = s - 1$  und  $p_2, \dots, p_r$  und  $q_1, \dots, q_{j-1} q_{j+1}, \dots, q_s$  bis auf Reihenfolge übereinstimmen. Also ist  $r = s$  und  $p_1, \dots, p_r$  und  $q_1, \dots, q_s$  stimmen bis auf Reihenfolge überein.  $\square$

**1.6. Normalteiler und Faktorgruppen.** Sei  $G$  eine Gruppe,  $H \subset G$  eine Untergruppe und  $g \in G$ . Wir definieren

$$\begin{aligned} gH &= \{gh \in G \mid h \in H\}, \text{ die Linksnebenklasse von } g \text{ unter } H, \text{ und} \\ Hg &= \{hg \in G \mid h \in H\}, \text{ die Rechtsnebenklasse von } g \text{ unter } H. \end{aligned}$$

Ist  $G$  kommutativ, so stimmen Links- und Rechtsnebenklassen natürlich überein.

**Lemma 1.29.** Zwei Linksnebenklassen sind entweder disjunkt oder gleich. Zwei Rechtsnebenklassen sind entweder disjunkt oder gleich.

*Beweis.* Nur für Linksnebenklassen: Ist  $x \in gH \cap g'H$ , so gibt es  $h, h' \in H$  mit  $x = gh = g'h'$ . Also ist  $g = g'h'h^{-1} \in g'H$  und damit  $gH \subset g'H$ . Analog erkennt man  $g'H \subset gH$ .  $\square$

Für alle  $g, g' \in G$  gilt also

$$gH \cap g'H \neq \emptyset \Leftrightarrow gH = g'H \Leftrightarrow g^{-1}g' \in H.$$

**Definition 1.30.** Wir bezeichnen mit  $G/H$  die Menge der Linksnebenklassen von  $G$  unter  $H$  und mit  $H\backslash G$  die Menge der Rechtsnebenklassen von  $G$  unter  $H$ .

*Beispiel 1.31.*  $G = \mathbb{Z}$ ,  $H = m\mathbb{Z}$  für ein  $m \geq 0$ . Dann liegen  $a, b \in \mathbb{Z}$  in derselben Linknebenklasse unter  $m\mathbb{Z}$  genau dann, wenn  $b = a + km$  für ein  $k \in \mathbb{Z}$ , wenn also  $b - a$  teilbar ist durch  $m$ , wenn also  $b$  und  $a$  bei Teilung durch  $m$  denselben Rest lassen. Wir sagen dann, daß  $a$  und  $b$  kongruent modulo  $m$  sind, und schreiben hierfür  $a \equiv b \pmod{m}$ .

Die möglichen Reste sind  $0, \dots, m-1$ . Es gibt also genau  $m$  Linksnebenklassen. Die Menge  $\mathbb{Z}/m\mathbb{Z}$  hat also  $m$  Elemente, die wir durch  $\bar{0} = 0 + m\mathbb{Z}$ ,  $\bar{1} = 1 + m\mathbb{Z}$ ,  $\dots$ ,  $\bar{m-1} = m-1 + m\mathbb{Z}$  bezeichnen.

Für eine endliche Menge  $X$  bezeichne  $|X|$  die Anzahl der Elemente in  $X$ . Ist  $G$  eine endliche Gruppe, so nennen wir  $|G|$  auch die *Gruppenordnung* von  $G$ .

**Satz 1.32** (Satz von Lagrange). *Sei  $G$  eine endliche Gruppe und  $H \subset G$  eine Untergruppe. So ist die Gruppenordnung von  $H$  ein Teiler der Gruppenordnung von  $G$ . Genauer gilt:*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

(Insbesondere ist die Anzahl der Linksnebenklassen also gleich der Anzahl der Rechtsnebenklassen.)

*Beweis.* Wir beweisen nur die Gleichung  $|G| = |H| \cdot |G/H|$ , die andere kann man analog beweisen. Natürlich liegt jedes Element  $g \in G$  in der Nebenklasse  $gH$ , andererseits sind verschiedene Nebenklassen disjunkt. Es reicht also zu zeigen, daß jede Nebenklasse genau  $|H|$  Elemente enthält. Dazu wählen wir eine Nebenklasse  $gH \in G/H$  und betrachten die Abbildung  $f: H \rightarrow gH$ ,  $f(h) = gh$ .  $f$  ist sicherlich surjektiv.  $f$  ist aber auch injektiv, denn aus  $gh = gh'$  folgt  $h = h'$ . Folglich ist  $|H| = |gH|$ .  $\square$

Ist  $|G|$  eine Primzahl, so sind folglich  $\{e\}$  und  $G$  die einzigen Untergruppen von  $G$ .

**Definition 1.33.** Die Anzahl  $|G/H| = |H\backslash G|$  der (Rechts- oder Links-)nebenklassen wird als der *Index* von  $H$  in  $G$  bezeichnet.

Wir wollen untersuchen, in welchen Fällen wir auf  $G/H$  eine Gruppenstruktur definieren können, so daß die kanonische Abbildung  $\text{can}: G \rightarrow G/H$ ,  $g \mapsto gH$  ein Homomorphismus von Gruppen wird.

Wir wollen zunächst eine notwendige Bedingung hierfür angeben. Unsere Verknüpfung auf  $G/H$  muß die Eigenschaft  $g'H \cdot gH = g'gH$  haben, damit  $\text{can}$  ein Homomorphismus von Gruppen wird. Insbesondere darf die Nebenklasse  $g'gH$  nicht von der speziellen Wahl von  $g$  in  $gH$  abhängen. Im Fall der Nebenklasse  $eH$  schließen wir, daß  $hgH = gH$  für alle  $h \in H$  gelten muß, und damit  $g^{-1}hg \in H$  für alle  $g \in G$  und  $h \in H$ . Nicht alle Untergruppen  $H \subset G$  haben notwendigerweise diese Eigenschaft.

**Definition 1.34.** Eine Untergruppe  $H \subset G$  heißt *Normalteiler* in  $G$ , falls für alle  $g \in G$  und  $h \in H$  gilt  $g^{-1}hg \in H$ .

*Anmerkungen 1.35.* (1) Unsere Bedingung an Normalteiler ist gleichbedeutend mit der Eigenschaft

$$gH = Hg$$

für alle  $g \in G$ .

- (2) Beispielsweise ist der Kern jedes Homomorphismus  $f: G \rightarrow G'$  von Gruppen ein Normalteiler.  
 (3) Ist  $G$  kommutativ, so ist jede Untergruppe ein Normalteiler.  
 (4) Die Untergruppe  $S_2 \subset S_3$  der Gruppe aller Bijektionen der Menge  $\{1, 2, 3\}$  in sich, die die 3 festhalten, ist *kein* Normalteiler.

**Satz 1.36.** Sei  $H$  ein Normalteiler in  $G$ . So definiert die Vorschrift

$$gH \cdot g'H = gg'H$$

eine Gruppenstruktur auf  $G/H$ .

*Beweis.* Wir zeigen die Wohldefiniertheit. Seien  $g_1, g_2, g \in G$  und  $g_1H = g_2H$ . Wir wollen  $g_1gH = g_2gH$  und  $gg_1H = gg_2H$  zeigen.

Es ist  $g_1gH = g_2gH$  genau dann, wenn  $(g_1g)^{-1}g_2g = g^{-1}(g_1^{-1}g_2)g \in H$ . Wegen  $g_1H = g_2H$  ist  $g_1^{-1}g_2 \in H$ , und nach Definition eines Normalteilers ist dann auch  $g^{-1}(g_1^{-1}g_2)g \in H$ . Wir haben also  $g_1gH = g_2gH$  gezeigt.

Es ist  $gg_1H = gg_2H$  genau dann, wenn  $(gg_1)^{-1}gg_2 = g_1^{-1}g_2 \in H$ , was ja nach unserer Voraussetzung  $g_1H = g_2H$  der Fall ist.

Unsere Verknüpfung ist also wohldefiniert. Es ist klar, daß  $G/H$  mit dieser Verknüpfung eine Halbgruppe ist.

Unsere Definitionen zeigen, daß  $eH = H$  das neutrale Element von  $G/H$  ist, und und daß das Inverse von  $gH$  gerade  $g^{-1}H$  ist. Damit ist  $G/H$  eine Gruppe.  $\square$

**Satz 1.37** (Die universelle Eigenschaft der Faktorgruppe). Sei  $H \subset G$  ein Normalteiler.

- (1) Die Abbildung  $\text{can}: G \rightarrow G/H$ ,  $\text{can}(g) = gH$  ist ein Homomorphismus von Gruppen mit Kern  $H$ .  
 (2) Ist  $\phi: G \rightarrow G'$  ein Homomorphismus von Gruppen mit  $H \subset \ker \phi$ , so gibt es genau einen Homomorphismus  $\tilde{\phi}: G/H \rightarrow G'$  von Gruppen, so daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ & \searrow \text{can} & \nearrow \tilde{\phi} \\ & G/H & \end{array}$$

*Bemerkung 1.38.* Für das Bild von  $g \in G$  unter der kanonischen Abbildung  $\text{can}: G \rightarrow G/H$  werden wir auch oft  $\bar{g}$  schreiben.

*Beweis.* Wir haben die Gruppenstruktur auf  $G/H$  ja gerade so definiert, daß  $\text{can}$  ein Gruppenhomomorphismus wird. Nun ist  $g \in G$  im Kern von  $\text{can}$  genau dann, wenn  $\text{can}(g) = gH = H$ , also  $g \in H$  gilt. Damit haben wir (1) bewiesen.

Ist nun  $\phi: G \rightarrow G'$  ein Homomorphismus mit  $H \subset \ker \phi$ , so definieren wir die Abbildung  $\tilde{\phi}: G/H \rightarrow G'$  durch  $\tilde{\phi}(gH) = \phi(g)$ . Das ist wohldefiniert, denn ist

$gH = g'H$ , so ist  $g^{-1}g' \in H$  und damit  $\phi(g) = \phi(g')$ . Daß  $\tilde{\phi}$  ein Homomorphismus von Gruppen ist, folgt direkt aus der Definition. Daß  $\tilde{\phi}$  die einzige Abbildung von  $G/H \rightarrow G'$  ist, die obiges Diagramm zum Kommutieren bringt, folgt aus der Surjektivität von  $\text{can}$ .  $\square$

**Satz 1.39** (Isomorphiesatz). *Jeder Gruppenhomomorphismus  $\phi: G \rightarrow G'$  induziert eine injektive Abbildung  $\tilde{\phi}: G/\ker \phi \rightarrow G'$  und einen Isomorphismus  $\hat{\phi}: G/\ker \phi \xrightarrow{\sim}$  im  $\phi$ .*

*Beweis.* Nach der universellen Eigenschaft der Faktorgruppe induziert  $\phi$  einen Homomorphismus  $\tilde{\phi}: G/\ker \phi \rightarrow G'$ .  $\tilde{\phi}$  ist aber injektiv, denn aus  $\tilde{\phi}(g \ker \phi) = e_{G'}$  folgt  $\phi(g) = e_{G'}$  mithilfe des kommutativen Diagramms aus der universellen Eigenschaft der Faktorgruppe, also  $g \in \ker \phi$  und damit  $g \ker \phi = \ker \phi = e_{G/\ker \phi}$ .

Verkleinern wir das Bild von  $\tilde{\phi}: G/\ker \phi \rightarrow G'$  zu  $\text{im } \phi$ , so erhalten wir eine bijektive Abbildung  $\hat{\phi}: G/\ker \phi \rightarrow \text{im } \phi$ , also einen Isomorphismus.  $\square$

Seien  $K \subset H \subset G$  Gruppen und  $K, H$  Normalteiler in  $G$  (dann ist  $K$  auch Normalteiler in  $H$ ). Die Verkettung  $H \hookrightarrow G \xrightarrow{\text{can}} G/K$  ist ein Homomorphismus von Gruppen mit Kern  $K$ , wir erhalten also eine injektive Abbildung  $H/K \rightarrow G/K$ . Wir können also  $H/K \subset G/K$  als Untergruppe betrachten.  $H/K$  ist sogar ein Normalteiler, denn ist  $g \in G, h \in H$ , so ist  $gK \cdot hK \cdot g^{-1}K = ghg^{-1}K \in H/K$ , denn  $ghg^{-1} \in H$ .

**Satz 1.40** (Noetherscher Isomorphiesatz). *Seien  $K \subset H \subset G$  Gruppen und  $K, H$  Normalteiler in  $G$ . So gibt es einen Isomorphismus*

$$G/H \xrightarrow{\sim} (G/K)/(H/K).$$

*Beweis.* Wir betrachten den Homomorphismus  $\phi: G \xrightarrow{\text{can}} G/K \xrightarrow{\text{can}} (G/K)/(H/K)$ . Da beide Abbildungen surjektiv sind, ist  $\phi$  surjektiv. Wir müssen, nach dem Isomorphiesatz, also nur  $\ker \phi = H$  zeigen. Es ist nun  $g \in \ker \phi$  genau dann, wenn  $gK = hK$  für ein  $h \in H$ , also  $g \in H \cdot K = H$ .  $\square$

**1.7. Zyklische Gruppen.** Sei  $G$  eine Gruppe und  $g \in G$ .

**Definition 1.41.** Wir sagen,  $g$  habe *unendliche Ordnung*, falls  $g^n \neq e$  für alle  $n \geq 1$ . Wir sagen,  $g$  habe *endliche Ordnung*, falls  $g^n = e$  für ein  $n \geq 1$ . Im zweiten Fall heißt das kleinste positive  $n$  mit  $g^n = e$  die *Ordnung von  $g$* .

Wir bezeichnen mit  $\text{ord}(g) \in \mathbb{N} \cup \infty$  die Ordnung von  $g$  in  $G$ .

Die von  $g$  erzeugte Untergruppe ist

$$\langle g \rangle = \{ \dots, g^{-1}, g^0 = e, g, g^2, \dots \} \subset G.$$

Sei  $\phi: \mathbb{Z} \rightarrow \langle g \rangle$  definiert durch  $\phi(n) = g^n$ .  $\phi$  ist ein surjektiver Gruppenhomomorphismus und wir erhalten einen Isomorphismus

$$\tilde{\phi}: \mathbb{Z}/\ker \phi \xrightarrow{\sim} \langle g \rangle.$$

Nach dem Satz über die Untergruppen von  $\mathbb{Z}$  ist entweder  $\ker \phi = 0$  oder  $\ker \phi = m\mathbb{Z}$  für ein eindeutig bestimmtes  $m > 0$ .

**Lemma 1.42.** *Es ist  $\ker \phi = 0$  genau dann, wenn  $g$  unendliche Ordnung hat. Hat  $g$  endliche Ordnung  $m$ , so ist  $\ker \phi = m\mathbb{Z}$ .*

*Beweis.*  $\ker \phi = 0$  bedeutet ja gerade  $g^n = e$  gdw.  $n = 0$ . Ist  $\ker \phi = m'\mathbb{Z}$  mit  $m' > 0$ , so ist  $m'$  die kleinste positive Zahl mit  $g^{m'} = e$ , also ist  $m' = m$ .  $\square$

Die Ordnung von  $g$  ist also gerade die Anzahl der Elemente in  $\langle g \rangle$ , und  $g$  hat genau dann endliche Ordnung  $m$ , wenn  $\mathbb{Z}/m\mathbb{Z} \cong \langle g \rangle$ . Ist  $g' \in \langle g \rangle$ , so ist  $\langle g' \rangle \subset \langle g \rangle$  eine Untergruppe, also ist die Ordnung von  $g'$  ein Teiler der Ordnung von  $g$ .

**Definition 1.43.** Eine zyklische Gruppe ist eine Gruppe  $G$ , die von einem Element erzeugt wird, also  $G = \langle g \rangle$  für ein  $g \in G$ .

**Lemma 1.44.** Sei  $G$  eine endliche Gruppe und  $g \in G$ . Dann teilt die Ordnung von  $g$  die Gruppenordnung  $|G|$ . Insbesondere ist jede Gruppe von Primzahlordnung zyklisch.

*Beweis.* Die Ordnung von  $g$  ist  $|\langle g \rangle|$  und aus  $|G| = |\langle g \rangle| \cdot |G/\langle g \rangle|$  folgt die erste Aussage. Ist  $|G|$  eine Primzahl und  $g \neq e$ , so ist  $|\langle g \rangle| \neq 1$ , also  $|G| = |\langle g \rangle|$  und damit  $G = \langle g \rangle$ .  $\square$

**1.8. Der chinesische Restsatz.** Seien  $G$  und  $H$  Gruppen. Das direkte Produkt  $G \times H$  ist dann ebenfalls eine Gruppe mit Verknüpfung  $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$ . Die Gruppe  $G \times H$  wird das *direkte Produkt* von  $G$  und  $H$  genannt. Ganz analog können wir das direkte Produkt  $G_1 \times G_2 \times \dots \times G_n$  von mehr als zwei Gruppen definieren (und sogar  $\times_{i \in I} G_i$  für eine beliebige Indexmenge  $I$ ). Für eine Gruppe  $G$  und  $r \in \mathbb{N}$  notieren wir

$$G^r := \bigtimes_{i=1}^r G = G \times \dots \times G \quad (r \text{ Kopien}).$$

**Satz 1.45** (Chinesischer Restsatz). Seien  $q_1, \dots, q_s \in \mathbb{Z}$  paarweise teilerfremde positive Zahlen (also  $\text{ggT}(q_i, q_j) = 1$  falls  $i \neq j$ ), und  $m = q_1 \cdots q_s$ . Dann gibt es einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z}.$$

*Beweis.* Sei  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z}$  definiert durch  $\phi(n) = (n+q_1\mathbb{Z}, \dots, n+q_s\mathbb{Z})$ . Es ist  $n \in \ker \phi$  genau dann, wenn jedes  $q_i$  ein Teiler von  $n$  ist. Da nun die  $q_i$  paarweise teilerfremd sind, ist dies genau dann der Fall, wenn  $m$  ein Teiler von  $n$  ist (Eindeutigkeit der Primfaktorzerlegung!). Also ist  $\ker \phi = m\mathbb{Z}$  und wir erhalten eine injektive Abbildung

$$\tilde{\phi}: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z}.$$

Nun haben beide Gruppen genau  $m = q_1 \cdots q_s$  Elemente, unsere injektive Abbildung ist also eine Bijektion.  $\square$

*Übung 1.46.* Die Gruppe  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  ist nicht zyklisch für  $n \geq 2$ .

**1.9. Der Hauptsatz für endlich erzeugte abelsche Gruppen.**

**Definition 1.47.** Eine Gruppe  $G$  heißt *endlich erzeugt*, falls es  $g_1, \dots, g_m \in G$  gibt mit  $G = \langle g_1, \dots, g_m \rangle$ .

Die Gruppe  $\mathbb{Q}$  (mit der Addition als Verknüpfung) ist *nicht* endlich erzeugt.

Notation: In diesem Abschnitt behandeln wir nur abelsche Gruppen und schreiben die Verknüpfung deswegen durchweg additiv. Das wesentliche Resultat dieses Abschnitts ist der folgende Satz.

**Satz 1.48** (Hauptsatz über endlich erzeugte abelsche Gruppen). *Sei  $G$  eine endlich erzeugte abelsche Gruppe. So gibt es Primzahlpotenzen  $q_1, \dots, q_s \in \mathbb{N}$  und eine natürliche Zahl  $r$ , so daß*

$$G \cong \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z} \times \mathbb{Z}^r.$$

*Die Zahl  $r$  ist eindeutig bestimmt und heißt der Rang von  $G$ . Die Zahlen  $q_1, \dots, q_s$  sind eindeutig bestimmt bis auf Reihenfolge.*

Anmerkung: Eine *Primzahlpotenz* ist eine Zahl  $q \in \mathbb{N}$  der Form  $q = p^n$ , wobei  $p \in \mathbb{N}$  eine Primzahl ist und  $n \in \mathbb{N}$ .

### 1.10. Freie abelsche Gruppen.

**Definition 1.49.** Eine Gruppe  $G$  heißt *freie abelsche Gruppe* (von endlichem Rang), falls

$$G \cong \mathbb{Z}^r = \mathbb{Z} \times \dots \times \mathbb{Z} \quad (r \text{ Kopien}).$$

Die Zahl  $r$  heißt der *Rang* von  $G$  (wir sagen auch:  $G$  ist eine freie abelsche Gruppe vom Rang  $r$ ). Der Rang einer Gruppe ist eindeutig bestimmt. Ein Isomorphismus  $\mathbb{Z}^r \xrightarrow{\sim} \mathbb{Z}^s$  induziert nämlich eine Bijektion  $(\mathbb{Z}/n\mathbb{Z})^r \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^s$  für jede Zahl  $n \in \mathbb{N}$ . Die Gruppe links hat  $n^r$  Elemente und die Gruppe rechts hat  $n^s$  Elemente, also ist  $r = s$ . ( $\mathbb{Z}^r \rightarrow (\mathbb{Z}/n\mathbb{Z})^r$  ist surjektiv und hat Kern  $n\mathbb{Z}^r = \{x \in \mathbb{Z}^r \mid \text{es gibt } y \in \mathbb{Z}^r \text{ mit } x = ny\}$ ).

Wir vereinbaren die Notation  $e_1 = (1, 0, \dots, 0)$ ,  $e_2 = (0, 1, 0, \dots, 0)$ ,  $\dots$ ,  $e_r = (0, \dots, 0, 1)$  für die Standard"basis" der Gruppe  $\mathbb{Z}^r$ .

Seien  $G$  und  $H$  Gruppen und

$$\text{Hom}_{Gr}(G, H) = \{\phi: G \rightarrow H \mid \phi \text{ ist ein Homomorphismus von Gruppen}\}.$$

**Lemma 1.50.** *Sei  $H$  eine abelsche Gruppe und  $r \in \mathbb{N}$ . Dann ist die Abbildung*

$$\begin{aligned} \text{Hom}_{Gr}(\mathbb{Z}^r, H) &\rightarrow H^r \\ \phi &\mapsto (\phi(e_1), \dots, \phi(e_r)) \end{aligned}$$

*eine Bijektion.*

*Beweis.* Die inverse Abbildung ist gegeben durch  $(h_1, \dots, h_r) \mapsto ((n_1, \dots, n_r) \mapsto n_1 h_1 + \dots + n_r h_r)$  (das Bild ist ein Homomorphismus von Gruppen, da  $H$  abelsch ist!).  $\square$

**Lemma 1.51.** *Seien  $A, B$  abelsche Gruppen und  $\phi: A \rightarrow B$ ,  $\psi: B \rightarrow A$  Homomorphismen mit  $\phi \circ \psi = \text{id}_B$ . Dann ist die natürliche Abbildung*

$$\begin{aligned} \chi: \ker \phi \times \text{im } \psi &\rightarrow A \\ (a, b) &\mapsto a + b \end{aligned}$$

*ein Isomorphismus. ( $\text{im } \psi \cong B$ !)*

*Beweis.*  $\chi$  ist ein Homomorphismus, da  $A$  abelsch ist.  $\chi$  ist injektiv, denn aus  $a+b=0$  folgt  $\phi(a+b)=\phi(b)=0$  und damit  $b=0$ , denn es ist  $b=\psi(b')$  für ein  $b' \in B$  und  $b'=\phi \circ \psi(b')=\phi(b)=0$ . Dann folgt auch  $a=0$ .

$\chi$  ist aber auch surjektiv, denn ist  $a \in A$ , so ist mit  $b=\psi \circ \phi(a)$ ,  $a-b \in \ker \phi$ ,  $b \in \text{im } \psi$  und  $\chi(a-b, b)=a$ , was zu zeigen war.  $\square$

**Proposition 1.52.** *Sei  $\phi: A \rightarrow B$  ein surjektiver Homomorphismus von abelschen Gruppen und sei  $B$  frei. So existiert ein Homomorphismus  $\psi: B \rightarrow A$  mit  $\phi \circ \psi = \text{id}_B$ . Insbesondere ist*

$$A = \ker \phi \times \text{im } \psi \cong \ker \phi \times B.$$

*Beweis.* Wir können  $B = \mathbb{Z}^r$  annehmen für ein  $r \in \mathbb{N}$ . Seien  $a_1, \dots, a_r \in A$  Urbilder unter  $\phi$  von  $e_1, \dots, e_r \in \mathbb{Z}^r$ . Nach Lemma 1.50 gibt es einen Homomorphismus  $\psi: \mathbb{Z}^r \rightarrow A$  mit  $\psi(e_i) = a_i$  für  $i = 1, \dots, r$ . Dann gilt, nach Konstruktion,  $\phi \circ \psi(e_i) = e_i$ , also  $\phi \circ \psi = \text{id}_{\mathbb{Z}^r}$ , erneut nach Lemma 1.50.

Die zweite Aussage folgt sofort aus Lemma 1.51.  $\square$

Man sagt, ein surjektiver Homomorphismus  $\psi: A \rightarrow B$  von Gruppen *spaltet*, wenn es einen rechtssinversen Homomorphismus  $\psi': B \rightarrow A$  gibt. Surjektive Homomorphismen in freie Gruppen spalten also immer.

**Satz 1.53.** *Jede Untergruppe einer freien Gruppe ist frei von kleinerem Rang.*

*Beweis.* Sei  $H \subset \mathbb{Z}^r$  eine Untergruppe. Wir zeigen, daß es ein  $s \leq r$  gibt mit  $H \cong \mathbb{Z}^s$  mittels Induktion nach  $r$ . Für  $r = 1$  ist  $H = \{0\}$  oder  $H = m\mathbb{Z} \subset \mathbb{Z}$  für ein  $m \geq 0$ . Im ersten Fall ist  $H = \mathbb{Z}^0$  und im zweiten Fall  $H \cong \mathbb{Z}$ .

Sei also nun  $r > 1$ . Sei

$$\begin{aligned} \phi: \mathbb{Z}^r &\rightarrow \mathbb{Z} \\ (n_1, \dots, n_r) &\mapsto n_1 \end{aligned}$$

die Projektion auf die erste Komponente. Dann ist  $\phi(H) \subset \mathbb{Z}$  frei vom Rang  $s \leq 1$ . Die surjektive Abbildung  $\phi|_H: H \rightarrow \phi(H)$  spaltet, es ist also  $H \cong \ker \phi|_H \times \phi(H)$ . Nun ist  $\ker \phi|_H = \ker \phi \cap H$  enthalten  $\ker \phi \cong \mathbb{Z}^{r-1}$  (die Untergruppe von  $\mathbb{Z}^r$  aller Elemente mit Eintrag Null an erster Stelle). Nach Induktionsvoraussetzung ist  $\ker \phi|_H$  damit frei vom Rang  $t \leq r-1$ . Also ist  $H = \ker \phi \times \text{im } \phi$  frei vom Rang  $s+t \leq r$ .  $\square$

**Korollar 1.54.** *Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt.*

*Beweis.* Sei  $G$  eine endlich erzeugte abelsche Gruppe und  $H \subset G$  eine Untergruppe. So gibt es eine freie Gruppe  $F$  von endlichem Rang und eine Surjektion  $\phi: F \rightarrow G$  nach Lemma 1.50. Dann ist  $\phi^{-1}(H) \subset F$  eine Untergruppe, und nach Satz 1.53 endlich erzeugt. Dann ist aber auch das Bild  $H = \phi(\phi^{-1}(H))$  endlich erzeugt.  $\square$

**1.11. Torsionsgruppen.** Sei  $G$  eine abelsche Gruppe und  $G_{\text{tor}} \subset G$  die Teilmenge aller Elemente mit endlicher Ordnung. Dann ist  $G_{\text{tor}}$  eine Untergruppe, denn haben  $a, b \in G$  die Ordnungen  $m$  und  $n$ , so ist  $mn \cdot (a \pm b) = mn \cdot a \pm mn \cdot b = 0$ , also haben auch  $a+b$  und  $a-b$  endliche Ordnung. Also ist  $G_{\text{tor}}$  abgeschlossen unter der

Verknüpfung und enthält mit jedem Element auch sein inverses. Wir nennen  $G$  eine (abelsche) Torsionsgruppe, wenn jedes Element endliche Ordnung hat, in Formeln:  $G = G_{\text{tor}}$ .

Das obige Argument zeigt auch, daß die Ordnung von  $a + b$  ein Teiler von  $mn$  ist. Ist  $p \in \mathbb{N}$  eine Primzahl, so ist insbesondere  $G(p) \subset G_{\text{tor}}$ , die Teilmenge aller Elemente, deren Ordnung eine Potenz von  $p$  ist, eine Untergruppe.

*Übung 1.55.* Jede endlich erzeugte abelsche Torsionsgruppe ist endlich.

**Proposition 1.56.** Sei  $G$  eine endlich erzeugte abelsche Torsionsgruppe. Dann ist  $G(p) = \{0\}$  für fast alle Primzahlen, und

$$G \cong \bigtimes_{p \text{ prim}} G(p).$$

*Beweis.* Da  $G$  eine endliche Gruppe ist und  $G(p) \cap G(p') = \{0\}$  für  $p \neq p'$ , gilt  $G(p) = \{0\}$  für fast alle Primzahlen  $p$ . Seien  $p_1, \dots, p_n$  die Primzahlen mit  $G(p_i) \neq \{0\}$ . Wir betrachten die Abbildung

$$\begin{aligned} \phi: G(p_1) \times \cdots \times G(p_n) &\rightarrow G \\ (x_1, \dots, x_n) &\mapsto x_1 + \cdots + x_n. \end{aligned}$$

Sei  $(x_1, \dots, x_n)$  im Kern von  $\phi$ . Wäre  $x_i \neq 0$  für ein  $i$ , so  $x_i = \sum_{j \neq i} (-x_j)$ . Nun steht rechts ein Element, dessen Ordnung ein Produkt der Primzahlen  $p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_n$  ist, dessen Ordnung also teilerfremd ist zu  $p_i$ . Das steht im Widerspruch dazu, daß die Ordnung von  $x_i$  eine Potenz von  $p_i$  ist. Somit ist  $(x_1, \dots, x_n) = 0$ , unsere Abbildung  $\phi$  ist also injektiv.

Wir zeigen nun die Surjektivität. Sei  $a \in G$  und sei  $m$  die Ordnung von  $a$ . Wir schreiben  $m = q_1 \cdots q_r$  mit paarweise teilerfremden Primpotenzen  $q_1, \dots, q_r$ . Nun ist  $\langle a \rangle \cong \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_r\mathbb{Z}$  nach dem chinesischen Restsatz 1.45. Insbesondere läßt sich  $a$  schreiben als Summe  $a = x_1 + \cdots + x_r$ , wobei die Ordnung von  $x_i$  eine Potenz des Primteilers  $p_i$  von  $q_i$  ist (sogar ein Teiler von  $q_i$ ), also  $x_i \in G(p_i)$ . Also liegt  $a$  im Bild von  $G(p_1) \times \cdots \times G(p_n)$ .  $\square$

**Proposition 1.57.** Sei  $G$  eine endlich erzeugte abelsche Torsionsgruppe mit  $G = G(p)$  für eine Primzahl  $p$ . Dann gibt es bis auf Reihenfolge eindeutig bestimmte Zahlen  $r_1, \dots, r_s$  mit

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z}.$$

*Beweis.* Wir zeigen die Existenz einer solchen Zerlegung mittels Induktion nach  $|G|$ . Ist  $|G| = 1$  (oder eine Primzahl), ist alles klar.

Sei das Theorem bewiesen für alle Gruppen  $G'$  mit  $G' = G'(p)$  und  $|G'| < |G|$ . Sei  $a \in G$  ein Element mit maximaler Ordnung  $p^r$ . Dann ist  $G/\langle a \rangle \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z}$  nach Induktionsvoraussetzung. Wir betrachten die Abbildung

$$G \xrightarrow{\text{can}} G/\langle a \rangle \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z}$$

und wollen zeigen, daß can spaltet, daß also eine Abbildung  $\phi: \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z} \rightarrow G$  existiert mit  $\text{can} \circ \phi = \text{id}$ . Daraus folgt dann nämlich  $G \cong \langle a \rangle \times \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_s}\mathbb{Z}$ , und da  $\langle a \rangle \cong \mathbb{Z}/p^r\mathbb{Z}$ , folgt die Existenz einer Zerlegung der gewünschten Art.

**Lemma 1.58.** *Sei  $b \in G/\langle a \rangle$  ein Element der Ordnung  $p^k$ . Dann gibt es ein Urbild  $x \in G$  von  $b$  der Ordnung  $p^k$ .*

*Beweis des Lemmas.* Sei  $x' \in G$  irgendein Urbild von  $b$ . Ist die Ordnung von  $x'$  gleich  $p^k$ , so sind wir fertig. Ansonsten ist sie größer als  $p^k$ . Es ist  $p^k x' \in \langle a \rangle$ , also  $p^k x' = na$  für ein  $n \in \mathbb{Z}$ . Wir schreiben  $n = p^l m$  mit maximalem  $l \leq r$ , also  $\text{ggT}(p, m) = 1$ . Wir haben also  $p^k x' = p^l ma$ . Nun ist die Ordnung von  $ma$  gleich der Ordnung von  $a$ , also  $p^r$ . Somit ist die Ordnung von  $x'$  gerade  $p^{r-l+k}$ . Wir erhalten, wegen der Maximalität von  $r$ ,  $r + k - l \leq r$  oder  $k \leq l$ . Somit ist  $p^k x' = p^k(p^{l-k} ma)$ . Wir setzen nun  $x = x' - p^{l-k} ma$ . Dann ist  $\text{can } x = \text{can } x' = b$  und  $p^k x = 0$ , die Ordnung von  $x$  ist also  $p^k$  (kleiner kann sie ja nicht sein, da  $p^k$  die Ordnung von  $b$  ist!).  $\square$

Wir kommen zurück zur Abbildung  $G \rightarrow G/\langle a \rangle \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_s}\mathbb{Z}$ . Nach dem eben Bewiesenen existieren Urbilder  $a_1, \dots, a_s \in G$  der Erzeuger der Faktoren rechts mit Ordnung  $p^{r_1}, \dots, p^{r_s}$ , und wir können den Homomorphismus

$$\begin{aligned} \phi: \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_s}\mathbb{Z} &\rightarrow G \\ (\bar{n}_1, \dots, \bar{n}_s) &\mapsto n_1 a_1 + \dots + n_s a_s \end{aligned}$$

konstruieren (Anmerkung: Hier ist  $\bar{n} \in \mathbb{Z}/m\mathbb{Z}$  das Bild von  $n \in \mathbb{Z}$ , obige Abbildung ist wohldefiniert, da  $a_i$  die Ordnung  $p^{r_i}$  hat). Es ist  $\text{can} \circ \phi = \text{id}$ , also spaltet  $\text{can}$ .

Zur Eindeutigkeit: Wie nehmen an, es gäbe zwei Darstellungen

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_s}\mathbb{Z} \cong \mathbb{Z}/p^{t_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{t_u}\mathbb{Z}.$$

Wir können  $r_1 \geq r_2 \geq \dots \geq r_s$  und  $t_1 \geq t_2 \geq \dots \geq t_u$  annehmen, und müssen dann  $s = u$  und  $r_i = t_i$  für alle  $i = 1, \dots, s$  zeigen.

Wir betrachten nun die Untergruppe  $pG \subset G$ . Es ist  $p(\mathbb{Z}/p^k\mathbb{Z}) \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$  für  $k > 1$  und  $p(\mathbb{Z}/p\mathbb{Z}) = \{0\}$  (also  $k \geq 1$ ). Wir erhalten also

$$pG \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_s-1}\mathbb{Z} \cong \mathbb{Z}/p^{t_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{t_u-1}\mathbb{Z}.$$

Per Induktion erhalten wir  $r_i = t_i$ , falls  $r_i \neq 1$  oder  $t_i \neq 1$ . Somit können sich die Tupel  $(r_1, \dots, r_s)$  und  $(t_1, \dots, t_u)$  nur unterscheiden in der Anzahl der Einsen am rechten Rand. Die Anzahl der Elemente von  $G$  ist aber sowohl  $p^{r_1+\dots+r_s}$  als auch  $p^{t_1+\dots+t_s}$ , also gilt  $r_1 + \dots + r_s = t_1 + \dots + t_u$  und daher muß auch die Anzahl der Einsen am rechten Rand unserer Tupel übereinstimmen.  $\square$

Wir fassen unsere letzten beiden Sätze zusammen. ( $G_{\text{tor}}$  ist endlich erzeugt nach Korollar 1.54)

**Proposition 1.59.** *Sei  $G$  eine endlich erzeugte abelsche Gruppe. Dann gibt es bis auf Reihenfolge eindeutig bestimmte Primpotenzen  $q_1, \dots, q_s$  mit*

$$G_{\text{tor}} \cong \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_s\mathbb{Z}.$$

Der Hauptsatz über endlich erzeugte abelsche Gruppen ist nun eine Konsequenz der nächsten Proposition.

**Proposition 1.60.** *Sei  $G$  eine endlich erzeugte abelsche Gruppe. Dann ist  $G/G_{\text{tor}}$  eine freie Gruppe von endlichem Rang. Die Surjektion  $G \xrightarrow{\text{can}} G/G_{\text{tor}}$  spaltet, es gibt also einen Isomorphismus*

$$G \cong G_{\text{tor}} \times \mathbb{Z}^r$$

für ein eindeutig bestimmtes  $r$ .

*Beweis.* Zur Vereinfachung sei  $A = G/G_{tor}$ . Dann ist  $A$  eine *torsionsfreie* Gruppe, also  $A_{tor} = \{0\}$ , denn hat  $a \in A$  endliche Ordnung, so hat jedes Urbild endliche Ordnung, liegt also in  $G_{tor}$ , also  $a = 0$ .

Wir zeigen nun, daß jede torsionsfreie endliche erzeugte abelsche Gruppe  $A$  frei ist. Sei dazu  $S \subset A$  eine endliche Menge von Erzeugern, und  $\{x_1, \dots, x_n\} \subset S$  eine maximale Teilmenge mit der Eigenschaft, daß  $m_1x_1 + \dots + m_nx_n = 0$  impliziert, daß  $m_1 = \dots = m_n = 0$ . Dann ist die von  $\{x_1, \dots, x_n\}$  erzeugte Untergruppe  $B$  von  $A$  frei. Sei nun  $y \in S$ . So gibt es, nach der Maximalität von  $\{x_1, \dots, x_n\}$ , Zahlen  $m, m_1, \dots, m_n$ , nicht alle  $= 0$ , mit  $my + m_1x_1 + \dots + m_nx_n = 0$ . Insbesondere ist  $m \neq 0$ . Also liegt  $my$  in  $B$ . Da  $S$  endlich ist, gibt es ein  $m$  mit  $mS \subset B$ . Der Homomorphismus  $\phi: A \rightarrow A$ ,  $\phi(a) = ma$  ist injektiv und identifiziert  $A$  mit einer Untergruppe der freien Gruppe  $B$ . Nach Satz 1.53 ist also auch  $A$  frei.

Also ist  $G/G_{tor}$  eine freie Gruppe, und nach Proposition 1.52 ist  $G \cong G_{tor} \times G/G_{tor}$ . Die Zahl  $r$  ist eindeutig bestimmt als der Rang von  $G/G_{tor}$ .  $\square$

### 1.12. Kompositionsreihen.

**Definition 1.61.** Eine Gruppe  $G$  heißt *einfach*, wenn  $G \neq \{e\}$  und es außer den trivialen Normalteilern  $\{e\}$  und  $G$  keine weiteren gibt.

*Beispiel 1.62.* Die Gruppe  $\mathbb{Z}/m\mathbb{Z}$  ist genau dann einfach, wenn  $m$  eine Primzahl ist.

**Definition 1.63.** Sei  $G$  eine Gruppe. Eine *Kompositionsreihe* von  $G$  ist eine Folge von Untergruppen

$$\{1\} = G_0 \subset G_1 \subset \dots \subset G_r = G,$$

wobei  $G_{i-1}$  ein Normalteiler in  $G_i$  und  $G_i/G_{i-1}$  einfach ist für alle  $i = 1, \dots, r$ . Die Gruppen  $G_i/G_{i-1}$  heißen die *Subquotienten* der Kompositionsreihe.

*Anmerkungen 1.64.* (1) Die Gruppe  $\mathbb{Z}$  hat keine Kompositionsreihe.

(2) Für endliche Gruppen  $G \neq \{e\}$  existiert immer eine Kompositionsreihe. Ist nämlich  $G$  nicht einfach, so können wir einen maximalen echten Normalteiler  $G' \subset G$ ,  $G' \neq G$  wählen. Dann ist  $G/G'$  eine einfache Gruppe, denn gäbe es einen nichttrivialen Normalteiler  $N \subset G/G'$ , so wäre sein Urbild in  $G$  ein echter Normalteiler, der  $G'$  enthielte. Per Induktion können wir annehmen, daß für  $G'$  eine Kompositionsreihe existiert.

**Satz 1.65** (Satz von Jordan–Hölder). *Je zwei Kompositionsreihen haben bis auf Umordnung isomorphe Subquotienten. Genauer: Sind  $\{1\} = M_0 \subset M_1 \subset \dots \subset M_r = G$  und  $\{1\} = N_0 \subset N_1 \subset \dots \subset N_s = G$  zwei Kompositionsreihen, so gilt  $r = s$  und es gibt  $\sigma \in S_r$  mit  $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$  für  $i = 1, \dots, r$ .*

*Beweis.* Per Induktion über  $r$ . Ist  $r = 1$ , so ist  $G$  einfach, also stimmen unsere Kompositionsreihe sogar überein. Sei also  $r \geq 2$ . Ist  $M_{r-1} = N_{s-1}$ , so folgt der Satz per Induktion. Ist  $M_{r-1} \neq N_{s-1}$ , so kürzen wir zunächst  $M := M_{r-1}$  und  $N := N_{s-1}$  ab und betrachten dann die Verkettung  $M \rightarrow G \rightarrow G/N$ . Das Bild von  $M$  ist ein Normalteiler  $\neq \{e\}$  in  $G/N$ . Da  $G/N$  einfach ist, muß die Abbildung  $M \rightarrow G \rightarrow G/N$  surjektiv sein und wir erhalten nach dem Isomorphiesatz 1.39 einen Isomorphismus  $M/(M \cap N) \xrightarrow{\sim} G/N$ . Analog erhalten wir einen natürlichen Isomorphismus  $N/(M \cap N) \xrightarrow{\sim} G/M$ .

Wir wählen nun eine Kompositionsreihe für  $M \cap N$ . Eine Kompositionsreihe von  $M \cap N$  existiert sicherlich. Es gilt sogar allgemeiner: Ist  $H \subset G$  ein Normalteiler,  $\{1\} = G_0 \subset G_1 \subset \dots \subset G_n = G$  eine Kompositionsreihe, so ist  $\{1\} = G_0 \cap H \subset G_1 \cap H \subset \dots \subset G_n \cap H = H$ , wobei wir die nicht-echten Inklusionen weglassen, eine Kompositionsreihe von  $H$ . Denn zunächst ist  $G_i \cap H \subset G_{i+1} \cap H$  ein Normalteiler, weil  $G_i \subset G_{i+1}$  ein Normalteiler ist. Ist  $G_i \cap H \neq G_{i+1} \cap H$ , so ist  $G_{i+1} \cap H / (G_i \cap H) \cong G_{i+1} / G_i$ , denn das Bild der natürlichen Abbildung  $G_{i+1} \cap H / (G_i \cap H) \hookrightarrow G_{i+1} / G_i$  ist ein Normalteiler.

Wir haben nun vier Kompositionsreihen:

$$\begin{array}{l} 1) \quad \dots \quad M_{r-2} \subset M \subset G \\ 2) \quad \dots \subset M \cap N \subset M \subset G \\ 3) \quad \dots \subset M \cap N \subset N \subset G \\ 4) \quad \dots \quad N_{s-2} \subset N \subset G \end{array}$$

Die Subquotienten von 1) und 2) stimmen per Induktionsannahme, angewandt auf die Gruppe  $M$ , bis auf Reihenfolge überein. Analoges gilt für die Subquotienten von 3) und 4). Die Subquotienten von 2) und 3) stimmen natürlich bis  $M \cap N$  überein, und die letzten beiden sind bis auf Vertauschung isomorph, wie wir gerade bewiesen hatten.  $\square$

**1.13. Operationen von Gruppen.** Sei  $X$  eine Menge und  $G$  eine Gruppe.

**Definition 1.66.** Eine *Operation* der Gruppe  $G$  auf der Menge  $X$  ist ein Homomorphismus

$$\phi: G \rightarrow \text{Sym}(X).$$

Notation: Wir schreiben auch  $g.x$  für  $\phi(g)(x)$ .

Ist  $\phi: G \rightarrow \text{Sym}(X)$  ein Homomorphismus, so können wir die Abbildung  $\chi: G \times X \rightarrow X$  definieren durch  $\chi(g, x) = \phi(g)(x)$ . Wir schreiben auch  $g.x$  für  $\chi(g, x)$ . Da  $\phi$  ein Homomorphismus ist, gilt für alle  $g, g' \in G$

$$(*) \quad \chi(gg', x) = \chi(g, \chi(g', x)),$$

oder, intuitiver,

$$(gg').x = g.(g'.x).$$

Ist umgekehrt  $\chi: G \times X \rightarrow X$  gegeben mit der Eigenschaft (\*), so definiert  $\phi: G \rightarrow \text{Sym}(X)$ ,  $\phi(g)(x) = \chi(g, x)$  einen Gruppenhomomorphismus.

**Beispiele 1.67.** (1)  $G$  operiert auf sich selbst durch Multiplikation von links:

$$\chi: G \times G \rightarrow G \text{ ist gegeben durch } \chi(g, g') = gg'.$$

(2) Die Abbildung  $\chi: G \times G \rightarrow G$ ,  $(g, h) \mapsto hg$ , definiert im allgemeinen *keine* Operation von  $G$  auf sich.

(3) Die Abbildung  $\chi: G \times G \rightarrow G$ ,  $(g, h) \mapsto hg^{-1}$ , definiert eine Operation von  $G$  auf sich.

(4) Die *Konjugation* von  $G$  auf  $G$  ist definiert durch  $(g, h) \mapsto ghg^{-1}$ . Dies definiert eine Operation der Gruppe  $G$  auf der Menge  $G$ .

(5) Ist  $V$  ein Vektorraum, so operiert  $\text{GL}(V)$  auf  $V$  mittels der Abbildung  $\chi: \text{GL}(V) \times V \rightarrow V$ ,  $\chi(A, v) = Av$ .

**Definition 1.68.** Die Gruppe  $G$  operiere auf der Menge  $X$  mittels  $\phi: G \rightarrow \text{Sym}(X)$ .

- (1) Der *Stabilisator* oder die *Isotropiegruppe* von  $x \in X$  ist die Untergruppe  $G_x = \{g \in G \mid g.x = x\}$  von  $G$ .
- (2) Sei  $x \in X$ . Die Menge  $G.x = \{g.x \mid g \in G\}$  heißt die *Bahn* oder der *Orbit* von  $x$ .
- (3) Die Operation heißt *transitiv*, falls  $G.x = X$  für ein  $x \in X$ .

Gilt  $G.x \cap G.y \neq \emptyset$ , so folgt schon  $G.x = G.y$ , denn gibt es  $g, g' \in G$  mit  $g.x = g'.y$ , so folgt  $x = g^{-1}g'.y \in Gy$  und daraus  $G.x \subset G.y$  und, analog,  $G.y \subset G.x$ . Die Bahnen bilden also eine *disjunkte Zerlegung* von  $X$ .

**Lemma 1.69.** Sei  $x \in X$ . So definiert die Operation von  $G$  eine Bijektion  $G/G_x \rightarrow G.x$ .

*Beweis.* Wir definieren eine Abbildung  $f: G/G_x \rightarrow G.x$  durch  $f(gG_x) = g.x$ .  $f$  ist wohldefiniert, denn gilt  $gG_x = g'G_x$ , so ist  $g^{-1}g' \in G_x$ , also  $g^{-1}g'.x = x$  oder  $g.x = g'.x$ . Es ist klar, daß  $f$  surjektiv ist. Ist aber  $g.x = g'.x$ , so ist  $g^{-1}g' \in G_x$ , also  $gG_x = g'G_x$ , also ist  $f$  auch injektiv.  $\square$

Mithilfe des Satzes von Lagrange erhalten wir die *Bahnformel*

$$|G| = |G_x| \cdot |G.x|.$$

1.14. **Konjugationsklassen.** Sei  $\phi: G \rightarrow \text{Sym}(G)$  die *Konjugationsoperation*, also  $\phi(g)(h) = ghg^{-1}$ . Die Bahnen von  $\phi$  heißen die *Konjugationsklassen* von  $G$ . Die Elemente  $h$  und  $h'$  liegen also genau dann in derselben Konjugationsklasse, wenn es ein  $g \in G$  gibt mit  $h' = ghg^{-1}$ . In einer abelschen Gruppe besteht jede Konjugationsklasse aus nur einem Element.

*Beispiel 1.70.* Ist  $G = GL(V)$  die Gruppe der invertierbaren Endomorphismen eines Vektorraums  $V$ , so sind die Konjugationsklassen gerade die Ähnlichkeitsklassen invertierbarer Endomorphismen. Ist  $V$  ein Vektorraum über einem algebraisch abgeschlossenen Körper, so werden die Konjugationsklassen also beschrieben durch Matrizen in Jordanscher Normalform (man beachte jedoch, daß zwei Matrizen in Jordanscher Normalform ähnlich sind, wenn sie sich nur in der Anordnung der Jordanblöcke unterscheiden).

Der Stabilisator von  $h \in G$  unter der Konjugation wird auch der *Zentralisator*  $Z_G(h)$  von  $h$  genannt. Es ist also

$$Z_G(h) = \{g \in G \mid ghg^{-1} = h\}.$$

Der Durchschnitt der Zentralisatoren aller Elemente von  $G$  heißt das *Zentrum*  $Z(G)$  von  $G$ . Es besteht also aus allen  $g \in G$  mit der Eigenschaft  $gh = hg$  für alle  $h \in G$ :

$$Z(G) = \{g \in G \mid gh = hg \text{ für alle } h \in G\}.$$

Ist  $H \subset G$  eine Untergruppe und  $g \in G$ , so ist  $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subset G$  wieder eine Untergruppe. Man nennt  $H$  und  $gHg^{-1}$  *zueinander konjugierte* Untergruppen.

**Satz 1.71** (Klassengleichung). Sei  $G$  eine endliche Gruppe und  $(g_i)_{i \in I}$  ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element (also der nicht-zentralen Konjugationsklassen). So gilt

$$|G| = |Z(G)| + \sum_{i \in I} |G/Z_G(g_i)|.$$

*Beweis.* Natürlich ist

$$|G| = \sum_{K \text{ Konj.klasse}} |K|.$$

Die einelementigen Konjugationsklassen werden gerade durch die Elemente von  $Z(G)$  gebildet, und die Konjugationsklasse von  $g_i$  hat genau  $|G/Z_G(g_i)|$  Elemente.  $\square$

**1.15. Sylow Untergruppen.** Sei  $G$  eine endliche Gruppe und  $p$  eine Primzahl. Sei  $r \in \mathbb{N}$ ,  $r \geq 0$  die größte Zahl, so daß  $p^r$  die Gruppenordnung  $|G|$  teilt.

**Definition 1.72.** Eine Untergruppe  $H \subset G$  der Ordnung  $p^r$  heißt *p-Sylowuntergruppe* von  $G$  (oder *p-Sylow* von  $G$ ).

**Satz 1.73.** (1) Die Anzahl der *p-Sylows* in  $G$  ist ein Teiler von  $|G|/p^r$  und kongruent zu 1 modulo  $p$ . Insbesondere gibt es mindestens eine *p-Sylow* in  $G$ .  
 (2) Je zwei *p-Sylows* sind zueinander konjugiert.  
 (3) Jede Untergruppe, deren Ordnung eine *p-Potenz* ist, liegt in einer *p-Sylow*.

*Beweis.* Wir zeigen zunächst die Existenz einer *p-Sylow* in  $G$  per Induktion nach  $|G|$ . Ist  $p$  kein Teiler von  $|G|$ , so ist  $\{e\}$  eine (und die einzige) *p-Sylow*. Wir nehmen nun an,  $p$  sei ein Teiler von  $|G|$ . Gibt es eine echte Untergruppe  $H \subset G$ , so daß  $p^r$  ein Teiler von  $|H|$  ist, so können wir die Induktionsvoraussetzung auf  $H$  anwenden und erhalten eine *p-Sylow* von  $H$  und von  $G$ . Andernfalls ist  $p$  ein Teiler des Index  $|G/H|$  jeder Untergruppe  $H$ .

Nach der Klassenformel ist  $p$  dann auch ein Teiler von  $|Z(G)|$  und nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es ein  $g \in Z(G)$  der Ordnung  $p$ . Nach Induktionsvoraussetzung gibt es eine *p-Sylow*  $H'$  in  $G/\langle g \rangle$ . Ihr Urbild  $H \subset G$  ist offenbar eine *p-Sylow* in  $G$ .

Sei  $S$  die Menge aller *p-Sylows* von  $G$ . Ist  $P \in S$ , so ist  $gPg^{-1} \in S$ . Also operiert  $G$  auf der Menge  $S$  durch Konjugation. Wir fixieren nun ein  $P \in S$  und betrachten die Bahn  $G.P \subset S$ . Die Gruppe  $P$  ist enthalten im Stabilisator  $G_P$ , also ist  $|G.P|$  teilerfremd zu  $p$ .

Sei  $H \subset G$  eine Untergruppe mit *p-Potenz*ordnung. Wir betrachten nun die Operation von  $H$  auf  $G.P$ . Die Anzahl der Elemente einer Bahn ist entweder eins oder eine Potenz von  $p$ . Da  $|G.P|$  teilerfremd ist zu  $p$ , muß es also einen Fixpunkt  $Q = g.P = gPg^{-1}$  unter  $H$  geben, also  $hQh^{-1} = Q$  für alle  $h \in H$ . Die Menge  $HQ = QH \subset G$  ist eine Untergruppe von  $G$  der Ordnung  $|HQ| = |HQ/H| \cdot |H| = |Q/Q \cap H| \cdot |H|$ . Also ist  $|HQ|$  eine *p-Potenz*, folglich  $HQ = Q$ , also  $H \subset Q$ .

Wir haben also (3) gezeigt, und sogar, daß jede Untergruppe mit *p-Potenz*ordnung in einer zu  $P$  konjugierten Sylow liegt. Daraus folgt (2). Schließlich betrachten wir die Operation von  $P$  auf  $S$ . Ist  $Q \in S$  und  $P.Q = \{Q\}$ , so zeigt obiges Argument  $P \subset Q$ , also  $P = Q$ . Damit gibt es genau eine einelementige Bahn in  $S$  unter  $P$ . Die Anzahl jeder andere Bahn ist eine *p-Potenz*, woraus wir  $|S| \equiv 1 \pmod{p}$  folgern. Die Isotropiegruppe  $G_P$  von  $P$  enthält  $P$ , also ist  $|S| = |G|/|G_P|$  ein Teiler von  $|G|/|P| = |G|/p^r$ .  $\square$

**Korollar 1.74.** Sei  $G$  eine endliche Gruppe und  $p$  eine Primzahl, die  $|G|$  teilt. So gibt es in  $G$  ein Element der Ordnung  $p$ .

*Beweis.* Sei  $S$  eine  $p$ -Sylowgruppe von  $G$ . Dann ist  $S$  nicht trivial und die Ordnung von  $S$  ist eine Potenz von  $p$ . Sei  $x \in S$  nicht das neutrale Element. Dann hat  $x$  Ordnung  $p^r$  für ein  $r > 0$ ,  $x^{p^{r-1}}$  hat also Ordnung  $p$ .  $\square$

**Satz 1.75.** *Seien  $p > q$  Primzahlen und  $q$  kein Teiler von  $p - 1$ . So ist jede Gruppe der Ordnung  $pq$  zyklisch.*

*Beweis.* Sei  $G$  eine Gruppe der Ordnung  $pq$ . Sei  $m_q$  die Anzahl der  $q$ -Sylows. Dann ist  $m_q$  ein Teiler von  $p$ , also  $m_q = 1$  oder  $m_q = p$ . Wäre  $m_q = p$ , so wäre wegen  $m_q \equiv 1 \pmod{q}$  die Zahl  $q$  ein Teiler von  $p - 1$ , was unserer Voraussetzung widerspricht. Also ist  $m_q = 1$ . Auf ähnliche Weise erkennt man  $m_p = 1$  unter Zuhilfenahme der Voraussetzung  $p > q$ .

Es gibt also jeweils nur eine  $p$ -Sylow und nur eine  $q$ -Sylow in  $G$ . Jedes Element der Ordnung  $p$  ist in dieser  $p$ -Sylow enthalten. Damit gibt es genau  $p - 1$  Elemente der Ordnung  $p$  in  $G$ . Analog gibt es  $q - 1$  Elemente der Ordnung  $q$  in  $G$ . Mit dem neutralen Element haben wir alle  $p + q - 1$  Elemente der Ordnungen  $1$ ,  $p$  oder  $q$  gefunden. Wegen  $p + q - 1 < pq$  gibt es in  $G$  ein Element der Ordnung  $pq$ , also ist  $G$  zyklisch.  $\square$

### 1.16. Auflösbare Gruppen.

**Definition 1.76.** Eine Gruppe  $G$  heißt *auflösbar*, wenn es eine Folge von Untergruppen

$$\{e\} = G_0 \subset G_1 \subset \dots \subset G_r = G$$

gibt, so daß  $G_{i-1} \subset G_i$  Normalteiler und  $G_i/G_{i-1}$  eine abelsche Gruppe ist für alle  $i = 1, \dots, r$ .

**Definition 1.77.** Die *Kommutatorgruppe*  $G'$  von  $G$  ist die von allen Elementen der Form  $aba^{-1}b^{-1}$  erzeugte Untergruppe.

Ist  $g \in G$ , so ist  $g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$ , also ist  $G'$  ein Normalteiler in  $G$ , und  $G/G'$  ist eine abelsche Gruppe. Ist  $N \subset G$  ein Normalteiler, so daß  $G/N$  abelsch ist, so muß  $G' \subset N$  gelten. Also ist  $G'$  der kleinste Normalteiler mit abelscher Faktorgruppe.

Wir schreiben  $G^{(1)}$  für die Kommutatorgruppe  $G'$  von  $G$  und definieren, induktiv,  $G^{(n)}$  als die Kommutatorgruppe von  $G^{(n-1)}$  für  $n \geq 2$ .

**Satz 1.78.**  *$G$  ist genau dann auflösbar, wenn  $G^{(n)} = \{e\}$  gilt für genügend großes  $n$ .*

*Beweis.* Ist  $G^{(n)} = \{e\}$  für ein  $n$ , so ist

$$\{e\} = G^{(n)} \subset G^{(n-1)} \subset \dots \subset G^{(1)} \subset G$$

eine Normalreihe mit abelschen Quotienten, also ist  $G$  auflösbar. Ist umgekehrt  $\{e\} = N_0 \subset N_1 \subset \dots \subset N_r = G$  eine Reihe mit abelschen Quotienten, so folgt induktiv  $G^{(i)} \subset N_{r-i}$ :

$$G^{(i+1)} = (G^{(i)})' \subset (N_{r-i})' \subset N_{r-i-1}.$$

$\square$

**Definition 1.79.** Sei  $p$  eine Primzahl. Eine  $p$ -Gruppe ist eine endliche Gruppe, deren Ordnung eine Potenz von  $p$  ist.

**Proposition 1.80.** Ist  $G$  eine nicht-triviale  $p$ -Gruppe, so hat  $G$  nicht-triviales Zentrum.

*Beweis.* Die Anzahl der Elemente jeder Konjugationsklasse mit mehr als einem Element ist durch  $p$  teilbar, nach der Bahnformel. Die Klassengleichung 1.71 zeigt, daß  $|Z(G)|$  durch  $p$  teilbar ist.  $\square$

**Satz 1.81** (Struktur von  $p$ -Gruppen). Sei  $G$  eine  $p$ -Gruppe. Dann gibt es eine Reihe  $\{e\} = G_0 \subset G_1 \subset \dots \subset G_r = G$  von Normalteilern von  $G$ , so daß  $G_i/G_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$  für  $i = 1, \dots, r$ . Insbesondere ist  $G$  also auflösbar.

*Beweis.*  $G$  hat nach Proposition 1.80 nicht-triviales Zentrum, und im Zentrum finden wir ein Element  $x$  der Ordnung  $p$ .  $G_1 := \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$  ist ein Normalteiler. Induktiv können wir annehmen, daß es eine Reihe  $\{e\} = G'_0 \subset G'_1 \subset \dots \subset G'_r = G/G_1$  der gewünschten Art in der  $p$ -Gruppe  $G/G_1$  gibt. Sei  $G_{i+1} \subset G$  das Urbild von  $G'_i \subset G/G_1$ . Wir erhalten eine Reihe von Untergruppen

$$\{e\} \subset G_1 \subset G_2 \subset \dots \subset G_{r+1} = G.$$

Dann ist jedes  $G_i$  ein Normalteiler in  $G$  und nach dem Noetherschen Isomorphiesatz ist

$$G_{i+1}/G_i \cong (G_{i+1}/G_1)/(G_i/G_1) = G'_i/G'_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$$

für  $i \geq 1$ . Außerdem ist  $G_1/G_0 \cong \mathbb{Z}/p\mathbb{Z}$  nach Konstruktion.  $\square$

**1.17. Symmetrische und alternierende Gruppen.** Wir hatten schon die *symmetrische Gruppe*  $S_n = \text{Sym}(\{1, \dots, n\})$  definiert. Elemente von  $S_n$  heißen auch Permutationen. Per Definitionem operiert  $S_n$  auf der Menge  $\{1, \dots, n\}$ . Sei  $m > 1$ . Ein  $\sigma \in S_n$  heißt  $m$ -Zykel, wenn es genau einen  $m$ -elementigen Orbit der Gruppe  $\langle \sigma \rangle$  auf  $\{1, \dots, n\}$  und sonst nur einelementige Orbiten gibt. Ein 2-Zykel heißt auch Transposition.

Schreibweise: Für einen Zykel, der  $a$  nach  $b$ ,  $b$  nach  $c$ ,  $\dots$ ,  $r$  nach  $a$  abbildet, schreiben wir  $(ab \dots r)$ . Speziellerweise sind also  $(ab)$  Transpositionen.

Jedes  $\sigma \in S_n$  läßt sich schreiben als Produkt von Transpositionen, und die Parität der Anzahl der Transpositionen ist unabhängig von allen Wahlen. Wir erhalten einen Gruppenhomomorphismus, das *Signum*

$$\text{Sgn}: S_n \rightarrow \{-1, 1\},$$

wobei  $\text{Sgn}(\tau_1 \dots \tau_r) = (-1)^r$  für Transpositionen  $\tau_1, \dots, \tau_r \in S_n$ . Permutationen mit Signum 1 bzw. -1 nennt man *gerade* bzw. *ungerade* Permutationen. Wir nennen die Gruppe  $A_n := \ker \text{Sgn}$  der geraden Permutationen die *alternierende Gruppe* über  $\{1, \dots, n\}$ .

**Satz 1.82.** Für  $n \geq 5$  ist  $A_n$  einfach.

Zum Beweis benötigen wir zwei Lemmata.

**Lemma 1.83.** Die alternierende Gruppe  $A_n$  wird erzeugt von allen 3-Zykeln.

*Beweis.* Sei  $\tau\tau' \neq e$  das Produkt zweier Transpositionen. Wir wollen zeigen, daß sich  $\tau\tau'$  als Produkt von 3-Zykeln schreiben läßt. Kommutieren  $\tau$  und  $\tau'$  nicht, so ist  $\tau\tau'$  schon ein 3-Zykel. Ansonsten läßt sich  $\tau''$  finden, so daß weder  $\tau$  und  $\tau''$  noch  $\tau'$  und  $\tau''$  kommutieren, also ist  $\tau\tau' = \tau\tau''\tau''\tau'$  Produkt zweier 3-Zykel.  $\square$

**Lemma 1.84.** Für  $n \geq 5$  sind je zwei 3-Zykel konjugiert in  $A_n$ .

*Beweis.* Sind  $(abc)$  und  $(a'b'c')$  zwei 3-Zykel, so finden wir eine Permutation  $\sigma$  in  $S_n$ , die  $a$  mit  $a'$ ,  $b$  mit  $b'$  und  $c$  mit  $c'$  vertauscht. Ist  $\sigma$  eine gerade Permutation, so sind wir fertig. Ansonsten finden wir  $d, e$ , verschieden von  $a, b, c$ . Nun können wir  $(abc)$  mit  $(de)\sigma$  konjugieren und erhalten die Behauptung (denn  $(de)(abc)(de) = (abc)$ ).  $\square$

*Beweis des Satzes 1.82.* Sei  $N \subset A_n$ ,  $N \neq \{e\}$  ein Normalteiler und  $\sigma \in N$ ,  $\sigma \neq e$ , eine Permutation mit maximal vielen Fixpunkten. Nach den Lemmata reicht es zu zeigen, daß  $\sigma$  ein 3-Zykel ist.

Wir betrachten die Bahnen von  $\sigma$  (der von  $\sigma$  erzeugten Untergruppe) auf  $\{1, \dots, n\}$ . Zunächst nehmen wir an, jede Bahn habe höchstens zwei Elemente. Dann gibt es mindestens zwei Bahnen,  $\{a, b\}$  und  $\{c, d\}$  mit zwei Elementen, da  $\sigma$  gerade ist. Sei  $e \neq a, b, c, d$ , und  $\tau = (cde)$ . So ist  $\tau\sigma\tau^{-1}\sigma^{-1}$  ein Element in  $N$  mit mehr Fixpunkten als  $\sigma$  (denn die Fixpunkte außerhalb von  $a, b, c, d, e, \sigma(e)$  sind dieselben, und  $a$  und  $b$  sind zusätzlich fix, und nur der eventuelle Fixpunkt  $e$  geht verloren), aber nicht das neutrale Element ( $c$  wird auf  $e$  abgebildet). Das ist ein Widerspruch zur Wahl von  $\sigma$ .

Also hat  $\sigma$  eine Bahn mit mindestens drei Elementen  $a, b, c$ . Wir nehmen  $\sigma(a) = b$  und  $\sigma(b) = c$  an. Ist  $\sigma$  kein 3-Zykel, so gibt es von  $a, b, c$  verschiedene  $d, e$ , die ebenfalls keine Fixpunkte von  $\sigma$  sind (sonst wäre  $\sigma$  ein Vierzykel und damit nicht gerade!). Sei  $\tau = (cde)$ . So hat  $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$  weniger Fixpunkte als  $\sigma$  (denn jeder Fixpunkt von  $\sigma$  ist auch Fixpunkt von  $\sigma'$  und  $\sigma'(b) = b$ ) und ist nicht das neutrale Element (denn  $\sigma'(c) = d$ ).  $\square$

**Satz 1.85.** Für  $n \geq 5$  ist die Gruppe  $S_n$  nicht auflösbar.

*Beweis.* Die alternierende Gruppe  $A_n \subset S_n$  ist ein Normalteiler als Kern des Gruppenhomomorphismus 'Sgn'. Wäre  $S_n$  auflösbar, so auch  $A_n$  (der Schnitt eines Normalteilers mit einer Untergruppe ist ein Normalteiler der Untergruppe, Quotienten bleiben abelsch).  $A_n$  ist aber einfach für  $n \geq 5$  und nicht abelsch, also nicht auflösbar.  $\square$

## 2. R

**Definition 2.1.** Ein Ring  $R$  ist eine Menge mit zwei assoziativen Verknüpfungen,  $+$  und  $\cdot$ , mit den folgenden Eigenschaften:

- (1)  $R$  ist eine kommutative Gruppe mit der Verknüpfung  $+$ . Das neutrale Element bzgl.  $+$  bezeichnen wir mit  $0$ .
- (2) Es gelten die Distributivgesetze, also

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

für alle  $a, b, c \in R$ .

(3) Es gibt ein neutrales Element  $1 = 1_R \in R$  bzgl. der Verknüpfung  $\cdot$ .

Man nennt  $+$  die *Addition* in  $R$  und  $\cdot$  die *Multiplikation* in  $R$ . Man nennt einen Ring  $R$  *kommutativ*, falls auch  $\cdot$  eine kommutative Verknüpfung ist, also  $a \cdot b = b \cdot a$  für alle  $a, b \in R$  gilt.

Der Ring, der nur aus dem Nullelement besteht, heißt der *Nullring*. Dies ist der einzige Ring mit der Eigenschaft  $0 = 1$ .

*Beispiele 2.2.* (1) Die ganzen Zahlen  $\mathbb{Z}$  bilden mit der Addition  $+$  und der Multiplikation  $\cdot$  einen Ring.

**Definition 2.3.** Ein Element  $a \in R$  heißt *invertierbar* oder eine *Einheit*, wenn es ein Element  $b \in R$  gibt mit  $a \cdot b = b \cdot a = 1$ . Wir haben in 1.8 schon gezeigt, daß  $b$  mit dieser Eigenschaft eindeutig bestimmt ist. Wir schreiben  $a^{-1} := b$ . Wir bezeichnen mit  $R^\times \subset R$  die Menge der Einheiten in  $R$ .

$R^\times$  ist stabil unter der Verknüpfung  $\cdot$  und bildet dann sogar eine Gruppe. Aber  $R^\times$  ist nicht stabil unter der Verknüpfung  $+$  (außer im Fall des Nullrings!).

In jedem Ring  $R$  gilt  $0 \cdot a = a \cdot 0 = 0$  für alle  $a \in R$ , denn es ist  $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$  (nach dem Distributivgesetz), und es folgt  $0 = 0 \cdot a$ , wenn wir auf beiden Seiten  $-(0 \cdot a)$  addieren.

**Definition 2.4.** Seien  $R$  und  $S$  Ringe. Eine Abbildung  $\phi: R \rightarrow S$  heißt *Ringhomomorphismus*, falls  $\phi(1_R) = 1_S$  gilt und  $\phi$  verträglich ist mit den Verknüpfungen auf  $R$  und  $S$ , wenn also

$$\begin{aligned}\phi(a + b) &= \phi(a) + \phi(b) \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b)\end{aligned}$$

gilt für alle  $a, b \in R$ .

Der *Kern* eines Ringhomomorphismus  $\phi: R \rightarrow S$  ist die Untergruppe

$$\ker \phi := \{a \in R \mid \phi(a) = 0\},$$

also gleich dem Kern, wenn wir  $\phi$  nur als Gruppenhomomorphismus von additiven Gruppen auffassen.

**Definition 2.5.** Ein Ring  $R$  ist ein *Schiefkörper*, wenn  $1 \neq 0$  gilt und alle von Null verschiedenen Elemente Einheiten sind (wenn also  $R^\times = R \setminus \{0\}$  gilt). Ein kommutativer Schiefkörper ist ein *Körper*.

**Definition 2.6.** Sei  $R$  ein Ring.

- (1) Ist  $R$  kommutativ und  $a, b \in R$ , so heißt  $a$  ein *Teiler* von  $b$  (man sagt auch  $a$  *teilt*  $b$ ), falls es ein  $d \in R$  gibt mit  $ad = b$ . (Jedes Element teilt die Null!). Wir schreiben  $a \mid b$ , falls  $a$  ein Teiler ist von  $b$ .
- (2) Ein Element  $a \in R$  heißt *Nullteiler*, falls es ein  $b \in R$  gibt mit  $b \neq 0$ , aber  $ab = 0$  oder  $ba = 0$ .
- (3)  $R$  heißt *nullteilerfrei*, falls 0 der einzige Nullteiler ist.
- (4)  $R$  heißt *Integritätsbereich*, wenn  $R$  kommutativ und nullteilerfrei und nicht der Nullring ist.

*Beispiel 2.7.* Sei  $X$  eine nicht-leere Menge und  $R$  ein Ring. Dann ist  $R^X = \{f: X \rightarrow R\}$ , die Menge aller Abbildungen von  $X$  nach  $R$ , mit der komponentenweisen Addition und Multiplikation wieder ein Ring. Er ist nullteilerfrei genau dann, wenn  $X$  nur aus einem Element besteht.

In Integritätsbereichen kann man “Kürzen”: Ist  $ab = ac$  und  $a \neq 0$ , so folgt  $b = c$ , denn aus  $a(b - c) = 0$  folgt  $b - c = 0$ .

**2.1. Ideale.** Sei  $R$  ein Ring und  $I \subset R$  eine Untergruppe bzgl. der additiven Gruppenstruktur von  $R$ . Dann ist  $I$  ein Normalteiler von  $R$ , da  $R$  ja kommutativ ist, und wir können also die Faktorgruppe  $R/I$  und den kanonischen Gruppenhomomorphismus

$$\text{can}: R \rightarrow R/I$$

betrachten. Wir wollen aber auf  $R/I$  noch eine Multiplikation definieren, so daß  $R/I$  ein Ring und  $\text{can}$  ein Homomorphismus von Ringen wird.

Falls solch eine Multiplikation auf  $R/I$  existiert, muß  $\text{can}(a) \cdot \text{can}(b) = \text{can}(ab)$  gelten, und da  $\text{can}$  surjektiv ist, ist die Multiplikation eindeutig bestimmt. Wegen  $\text{can}(0_R) = 0_{R/I}$  muß darüberhinaus  $\text{can}(0) \cdot \text{can}(a) = \text{can}(a) \cdot \text{can}(0) = 0_{R/I}$  gelten für alle  $a \in R$ . Wegen  $\text{can}(0) = \text{can}(i)$  für alle  $i \in I$  muß also  $\text{can}(ai) = \text{can}(ia) = 0_{R/I}$  sein für alle  $a \in R$  und  $i \in I$ . Eine Ringstruktur auf  $R/I$  mit der Eigenschaft, daß  $\text{can}: R \rightarrow R/I$  ein Ringhomomorphismus ist, kann es also nur geben, wenn  $ai, ia \in I$  für alle  $a \in R$  und  $i \in I$ . Proposition 2.10 zeigt, daß diese Bedingung sogar hinreichend ist.

**Definition 2.8.** Eine Teilmenge  $I \subset R$  heißt *Ideal in  $R$* , falls  $I$  eine Untergruppe von  $R$  mit der Addition als Verknüpfung ist und  $R \cdot I \subset I$  und  $I \cdot R \subset I$  gilt. (Hier soll  $R \cdot I$  die Menge aller Elemente der Form  $r \cdot i$  mit  $i \in I$  und  $r \in R$  bezeichnen, und analog sei  $I \cdot R$  definiert.)

*Beispiele 2.9.* (1) Der Kern  $\phi^{-1}(0)$  jedes Homomorphismus von Ringen ist ein Ideal.

(2) Jede Untergruppe in  $\mathbb{Z}$  ist ein Ideal in  $\mathbb{Z}$ .

Der Schnitt über eine beliebige Menge von Idealen in einem Ring  $R$  ist wieder ein Ideal. Für eine Teilmenge  $T \subset R$  definieren wir  $(T)$  als den Schnitt über alle Ideale  $I \subset R$ , die  $T$  enthalten. Also ist  $(T)$  das *kleinste* Ideal, daß  $T$  enthält. Man sagt, ein Teilmenge  $T$  *erzeugt das Ideal  $I$* , falls  $I = (T)$ .

Für endliche Mengen schreiben wir auch  $(a_1, \dots, a_n)$  statt  $(\{a_1, \dots, a_n\})$ . Ideale, die von einem Element erzeugt werden, heißen *Hauptideale*.

**Proposition 2.10.** Sei  $I \subset R$  ein Ideal.

- (1) Die Verknüpfung  $(a + I) \cdot (b + I) = a \cdot b + I$  definiert auf  $R/I$  die Struktur eines Rings.
- (2) Die kanonische Abbildung  $\text{can}: R \rightarrow R/I$  ist ein Homomorphismus von Ringen mit  $\text{can}^{-1}(0) = I$ .
- (3) Ist  $\phi: R \rightarrow R'$  ein Ringhomomorphismus mit  $I \subset \ker \phi$ , so ist der induzierte Gruppenhomomorphismus  $\tilde{\phi}: R/I \rightarrow R'$  (vgl. 1.37) ein Ringhomomorphismus.

*Beweis.* Zunächst ist  $R/I$  mit der induzierten Addition natürlich eine abelsche Gruppe. Die oben angegebene Verknüpfung ist wohldefiniert, denn ist  $a + I = a' + I$ , so

ist  $a - a' \in I$ , und es gilt  $ab - a'b = (a - a') \cdot b \in I$  für alle  $b \in R$ , also  $ab + I = a'b + I$ . Analog zeigt man  $ab + I = ab' + I$ , falls  $b$  und  $b'$  in derselben Restklasse bzgl.  $I$  liegen. Daß die Distributivgesetze gelten, folgt unmittelbar aus den Definitionen, und die Restklasse  $1 + I$  ist natürlich ein neutrales Element bzgl. der Multiplikation. Also ist  $R/I$  mit der Addition der Restklassengruppe und der oben definierten Multiplikation ein Ring. Wir haben also (1) gezeigt.

Die kanonische Abbildung  $\text{can}: R \rightarrow R/I$  ist ein Homomorphismus von Gruppen nach der Definition der Restklassengruppe. Die Multiplikation auf  $R/I$  ist gerade so definiert, daß  $\text{can}(ab) = \text{can}(a)\text{can}(b)$  und  $\text{can}(1_R) = 1_{R/I}$  gilt. Nach Definition der Restklassengruppe ist  $\text{can}^{-1}(0) = I$ . Also haben wir (2) gezeigt.

Sei schließlich  $\phi: R \rightarrow R'$  wie in (3) und  $\tilde{\phi}: R/I \rightarrow R'$  der nach 1.37 induzierte Homomorphismus von Gruppen. Dann ist  $\tilde{\phi}(a + I) = \phi(a)$  und deshalb  $\tilde{\phi}(1 + I) = \phi(1) = 1$  und  $\tilde{\phi}((a + I) \cdot (b + I)) = \tilde{\phi}(ab + I) = \phi(ab) = \phi(a) \cdot \phi(b) = \tilde{\phi}(a + I) \cdot \tilde{\phi}(b + I)$ . Also ist  $\tilde{\phi}$  ein Ringhomomorphismus.  $\square$

*Beispiel 2.11.*  $\mathbb{Z}/m\mathbb{Z}$  ist ein Ring für jedes  $m \in \mathbb{N}$ .

## 2.2. Primkörper.

**Lemma 2.12.**  $I = \{0\}$  und  $I = K$  sind die einzigen Ideale in einem Körper  $K$ .

*Beweis.* Ist  $a \in I$ ,  $a \neq 0$ , so ist  $a$  invertierbar in  $K$  und somit  $a^{-1} \cdot a = 1 \in I$ , also  $I = K$ .  $\square$

*Übung 2.13.* Ein kommutativer Ring  $R$ , der nicht der Nullring ist, ist genau dann ein Körper, wenn er nur die Ideale  $\{0\}$  und  $R$  hat.

Insbesondere ist jeder Ringhomomorphismus  $\phi: K \rightarrow R$  von einem Körper in einen von Null verschiedenen Ring injektiv ( $\phi$  ist nicht die Nullabbildung, da  $\phi(1) = 1 \neq 0$ , und  $\ker \phi \subset K$  ist ein Ideal).

**Proposition 2.14.** Sei  $m \in \mathbb{N}$ ,  $m > 0$ . Genau dann ist  $\mathbb{Z}/m\mathbb{Z}$  ein Körper, wenn  $m$  eine Primzahl ist.

*Beweis.* Ist  $m = a \cdot b$  mit  $0 < a, b < m$ , so ist  $\bar{a} \neq 0$ ,  $\bar{b} \neq 0$ , aber  $\bar{a} \cdot \bar{b} = 0$ , folglich kann  $\mathbb{Z}/m\mathbb{Z}$  kein Körper sein.

Wir zeigen nun, daß für eine Primzahl  $p$  jedes Element  $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ ,  $\bar{x} \neq 0$ , invertierbar ist. Ist  $x \in \mathbb{Z}$  ein Repräsentant von  $\bar{x}$ , so ist  $x$  teilerfremd zu  $p$ . Es gibt also, nach 1.25,  $m, n \in \mathbb{Z}$  mit  $1 = m \cdot x + n \cdot p$ . In  $\mathbb{Z}/m\mathbb{Z}$  liest sich diese Gleichung

$$\bar{1} = \bar{m} \cdot \bar{x}.$$

$\square$

Üblicherweise schreibt man  $\mathbb{F}_p$  für den Körper  $\mathbb{Z}/p\mathbb{Z}$ .

**Korollar 2.15** (Kleiner Fermat). Ist  $p$  eine Primzahl und  $a \in \mathbb{Z}$ , so gilt

$$a^p \equiv a \pmod{p}.$$

*Beweis.* Ist  $a$  durch  $p$  teilbar, so gilt die Gleichung offensichtlich. Andernfalls ist  $\bar{a} \neq 0$  in  $\mathbb{Z}/p\mathbb{Z}$  invertierbar. Die multiplikative Gruppe der Einheiten in  $\mathbb{Z}/p\mathbb{Z}$  hat

$p-1$  Elemente. Nach dem Satz von Lagrange teilt die Ordnung von  $\bar{a}$  die Zahl  $p-1$ , also ist  $\bar{a}^{p-1} = \bar{1}$  in  $\mathbb{Z}/p\mathbb{Z}$ , mit anderen Worten  $a^{p-1} \equiv 1 \pmod{p}$ . Daraus folgt die Behauptung.  $\square$

**2.3. Potenzreihen und Polynomringe.** Ist  $R$  ein Ring, so konstruieren wir den Ring  $R[[X]]$  der *Potenzreihen mit Koeffizienten in  $R$*  wie folgt.  $R[[X]]$  ist zunächst die Menge aller Abbildungen von  $\mathbb{N}$  nach  $R$ . Sind  $a$  und  $b$  Elemente dieser Menge, so definieren wir  $a+b: \mathbb{N} \rightarrow R$  durch die Vorschrift  $(a+b)(n) = a(n) + b(n)$ . Mittels dieser Addition wird  $R[[X]]$  eine kommutative Gruppe. Als Produkt von  $a$  und  $b$  definieren wir die Abbildung  $a \cdot b: \mathbb{N} \rightarrow R$  durch  $(a \cdot b)(n) = \sum_{i,j \in \mathbb{N}, i+j=n} a(i) \cdot b(j)$ .  $R[[X]]$  ist mit dieser Addition und Multiplikation ein Ring.

Die Definition der Multiplikation in  $R[[X]]$  wird verständlicher, wenn man sich eine Abbildung  $a: \mathbb{N} \rightarrow R$  zunächst vorstellt als Folge  $(a_0, a_1, \dots)$  von Elementen aus  $R$  ( $a_i = a(i)$ ) und dann als *Potenzreihe*  $a_0 + a_1X + a_2X^2 + \dots$ . Die Multiplikation zweier solcher Reihen ist dann gegeben durch

$$\begin{aligned} & (a_0 + a_1X + a_2X^2 + \dots)(b_0 + b_1X + b_2X^2 + \dots) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \dots \end{aligned}$$

*Übung 2.16.* Man zeige, daß  $a_0 + a_1X + a_2X^2 + \dots \in R[[X]]$  eine Einheit ist genau dann, wenn  $a_0 \in R$  eine Einheit ist.

Wir definieren den Ring  $R[X] \subset R[[X]]$  der *Polynome in einer Variablen  $X$  über  $R$*  als die Teilmenge aller Abbildungen  $a: \mathbb{N} \rightarrow R$  mit  $a(n) = 0$  für fast alle  $n$ . Man macht sich leicht klar, daß  $R[X]$  stabil unter der Addition und Multiplikation in  $R[[X]]$  ist und dadurch selbst zu einem Ring wird. Wir schreiben von nun an  $P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$  für ein solches Polynom. Ein Polynom der Form  $P(X) = a_0$  nennt man *konstant*. Die konstanten Polynome bilden einen zu  $R$  isomorphen Unterring in  $R[X]$ .

Ist  $\phi: R \rightarrow R'$  ein Ringhomomorphismus und  $x \in R'$  ein Element, das mit jedem Element aus  $\phi(R)$  kommutiert, so definiert

$$\begin{aligned} \text{ev}_x: R[X] &\rightarrow R' \\ P(X) = a_0 + a_1X + \dots + a_nX^n &\mapsto P(x) := \phi(a_0) + \phi(a_1)x + \dots + \phi(a_n)x^n \end{aligned}$$

einen Homomorphismus von Ringen (man rechnet das leicht nach!).

Ein Wort der Warnung: Ist  $R$  kommutativ, so können wir insbesondere (für  $\phi = \text{id}: R \rightarrow R$ ) einem Polynom  $P(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$  die Abbildung  $R \rightarrow R$ ,  $r \mapsto P(r) = a_0 + a_1r + \dots + a_nr^n$  zuordnen. Dabei muß jedoch beachtet werden, daß dabei einem nichttrivialen Polynom durchaus die Nullabbildung zugeordnet werden kann. Ist  $p$  eine Primzahl und  $P(X) = X - X^p \in \mathbb{Z}/p\mathbb{Z}[X]$ , so gilt  $P(r) = 0$  für alle  $r \in \mathbb{Z}/p\mathbb{Z}$ , wie wir in Korollar 2.15 gesehen haben.

Ist  $R$  ein Ring, so können wir den Polynomring in *mehreren* Variablen induktiv definieren als

$$R[X_1, \dots, X_n] = R[X_1][X_2] \dots [X_n].$$

**2.4. Nullstellen von Polynomen.** Sei  $R$  ein kommutativer Ring. Dann können wir für jedes Polynom  $P(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$  und jedes  $r \in R$  das Element  $P(r) = a_0 + a_1r + \dots + a_nr^n$  bilden.

**Definition 2.17.** Das Element  $r \in R$  ist eine *Nullstelle* von  $P$ , falls  $P(r) = 0$ .

Sei von nun an  $R = K$  ein Körper.

**Definition 2.18.** Ist  $K$  ein Körper mit der Eigenschaft, daß jedes nicht konstante Polynom  $P \in K[X]$  eine Nullstelle hat, so heißt  $k$  *algebraisch abgeschlossen*.

Wir werden sehen, daß der Körper  $\mathbb{C}$  der komplexen Zahlen algebraisch abgeschlossen ist. Im allgemeinen kann man zu einem beliebigen Körper  $k$  einen Körper  $\bar{k}$  finden, der  $k$  enthält und algebraisch abgeschlossen ist. Jedoch braucht man hierzu das Zornsche Lemma.

Der wichtigste Satz dieses Abschnitts ist der folgende.

**Satz 2.19** (Zerlegung in Linearfaktoren). *Ist  $K$  ein algebraisch abgeschlossener Körper und  $P \in K[X]$  nicht das Nullpolynom, so gibt es ein eindeutig bestimmtes  $c \in K$  und eindeutig bis auf Reihenfolge bestimmte  $a_1, \dots, a_n \in K$  mit*

$$P(X) = c \cdot (X - a_1) \cdots (X - a_n).$$

Sei zunächst  $R$  ein nullteilerfreier Ring. Ist  $P(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$  und ist  $a_n \neq 0$ , so definieren wir  $\text{grad } P := n$ , den *Grad* von  $P$ , und nennen  $a_n$  den *Leitkoeffizienten* von  $P$ . Den Grad des Nullpolynoms definieren wir als  $-\infty$ . Polynome vom Grad Null sind gerade die Konstanten aus  $R$ .

**Lemma 2.20.**  *$R[X]$  ist ein nullteilerfreier Ring und es gilt  $\text{grad } P \cdot Q = \text{grad } P + \text{grad } Q$ , für  $P, Q \in R[X]$ , beide  $\neq 0$ .*

*Beweis.* Ist  $P = a_0 + a_1X + \cdots + a_nX^n$  mit  $a_n \neq 0$  und  $Q = b_0 + b_1X + \cdots + b_mX^m$  mit  $b_m \neq 0$ , so ist  $P \cdot Q = a_0b_0 + \cdots + a_nb_mX^{m+n}$  mit  $a_nb_m \neq 0$ .  $\square$

Sei nun  $K$  ein Körper.

**Proposition 2.21.** *Sind  $P, Q \in K[X]$  und  $Q \neq 0$ , so gibt es Polynome  $D, S \in K[X]$  mit  $\text{grad } S < \text{grad } Q$ , so daß  $P = D \cdot Q + S$ .*

*Beweis.* Wir wählen ein Polynom  $D$ , so daß  $S := P - DQ$  kleinstmöglichen Grad hat. Wäre der Grad von  $S$  größer oder gleich  $Q$ , so hätte  $P - (D + cX^{\text{grad } S - \text{grad } Q})Q$ , mit passend gewähltem  $c \in K$ , echt kleineren Grad als  $S$ , was der Wahl von  $S$  widerspricht. Wir haben also die Existenz von  $D, S$  gezeigt. Ist  $D', S'$  ein weiteres Paar mit den geforderten Eigenschaften, so ist  $(D - D') \cdot Q = S - S'$ . Der Grad des Polynoms rechts ist aber echt kleiner als der Grad von  $Q$  und hieraus folgt  $D - D' = 0$  und dann  $S - S' = 0$ .  $\square$

**Korollar 2.22.** *Ist  $r \in K$  eine Nullstelle von  $P \in K[X]$ , so gibt es ein Polynom  $D \in K[X]$  mit  $P = D \cdot (X - r)$ .*

*Beweis.* Nach obiger Proposition gibt es  $D, S$  mit  $P = D \cdot (X - r) + S$  mit  $\text{grad } S = 0$ .  $S$  ist also eine Konstante und muß sogar Null sein, wie wir durch Einsetzen von  $r$  erkennen.  $\square$

*Beweis von Satz 2.19.* Wir wählen eine Zerlegung

$$P(X) = Q(X) \cdot (X - a_1) \cdots (X - a_k)$$

mit maximalem  $k$  und einem Polynom  $Q$ . Dann kann nach Korollar 2.22  $Q$  keine Nullstelle mehr haben. Da  $K$  algebraisch abgeschlossen ist, muß  $Q$  ein konstantes Polynom sein,  $Q(X) = c$  für eine Einheit  $c \in K$ . Also gibt es eine Zerlegung der gewünschten Art. Daß diese eindeutig ist, folgt induktiv nach dem Grad von  $P$ , denn aus  $(X - a)\tilde{P}(X) = (X - a)\tilde{Q}(X)$  folgt schon  $\tilde{P}(X) = \tilde{Q}(X)$ .  $\square$

**Satz 2.23.** *Ist  $P \in K[X]$ ,  $P \neq 0$ , so ist die Zahl der Nullstellen von  $P$  kleiner oder gleich dem Grad von  $P$ .*

*Beweis.* Wir zeigen den Satz mittels Induktion über den Grad von  $P$ . Hat  $P$  den Grad Null, so gibt es gar keine Nullstelle. Sei nun  $P \in K[X]$ ,  $P \neq 0$  und sei die Aussage bewiesen für alle Polynome vom Grad  $< \text{grad } P$ . Hat  $P$  gar keine Nullstelle, so müssen wir auch nichts beweisen. Ansonsten sei  $r \in K$  eine Nullstelle von  $P$ . Dann gibt es  $D \in K[X]$  mit  $P = D \cdot (X - r)$  und  $\text{grad } D = \text{grad } P - 1$ . Jede weitere Nullstelle von  $P$  ist, da  $K$  nullteilerfrei ist, auch eine Nullstelle von  $D$ . Nach Induktionsvoraussetzung gibt es davon höchstens  $\text{grad } P - 1$ .  $\square$

**2.5. Primideale und maximale Ideale.** Sei  $R$  ein kommutativer Ring und  $I \subset R$  ein echtes Ideal (also  $I \neq R$ ).

**Definition 2.24.** (1)  $I$  heißt *Primideal*, falls aus  $a, b \in R$  mit  $ab \in I$  folgt, daß  $a \in I$  oder  $b \in I$ .

(2)  $I$  heißt *maximales Ideal*, falls es kein echtes Ideal  $J \subset R$  gibt mit  $I \subset J \subset R$  und  $I \neq J$ .

**Lemma 2.25.** *Ein echtes Ideal  $I \subset R$  ist genau dann maximal, wenn  $R/I$  ein Körper ist. Es ist genau dann ein Primideal, wenn  $R/I$  ein Integritätsbereich ist.*

*Beweis.* Die kanonische Abbildung  $R \rightarrow R/I$  ist surjektiv und definiert deshalb eine Bijektion zwischen den Idealen von  $R/I$  und den Idealen in  $R$ , die  $I$  enthalten. Ist  $R/I$  ein Körper, so ist folglich  $I$  maximal. Ist andererseits  $I$  maximal und  $a \notin I$ , so ist  $(I \cup \{a\}) = R$ , es gibt folglich  $x \in I$  und  $b \in R$  mit  $1 = x + ab$ , also gilt  $\bar{a} \cdot \bar{b} = \bar{1}$  in  $R/I$  und  $\bar{a}$  ist also invertierbar. Also ist  $R/I$  ein Körper. ( $\bar{x}$  = Bild von  $x$  unter der kanonischen Abbildung  $R \rightarrow R/I$ ).

Ist  $I$  nun ein Primideal und  $a, b \in R$  mit  $\bar{a}\bar{b} = 0$ , so  $ab \in I$  und deshalb  $a \in I$  oder  $b \in I$ , also  $\bar{a} = 0$  oder  $\bar{b} = 0$  und  $R/I$  ist ein Integritätsbereich. Die Umkehrung erhält man, indem man die Satzteile des vorigen Satzes geeignet umordnet.  $\square$

**2.6. Der chinesische Restsatz.** Sind  $R_1, \dots, R_n$  Ringe, so wird das kartesische Produkt  $R_1 \times \dots \times R_n$  mittels komponentenweiser Addition und Multiplikation wieder zu einem Ring:

$$\begin{aligned}(a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 + b_1, \dots, a_n + b_n) \\ (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) &= (a_1 \cdot b_1, \dots, a_n \cdot b_n)\end{aligned}$$

Ist  $R$  ein Ring und sind  $I, J \subset R$  Ideale in  $R$ , so ist die Menge  $I + J = \{i + j \mid i \in I, j \in J\}$  wieder ein Ideal. Die Menge  $\{i \cdot j \mid i \in I, j \in J\}$  ist im allgemeinen kein Ideal, sogar nicht einmal eine Untergruppe von  $R$ . Deshalb bezeichnen wir mit  $I \cdot J = (\{i \cdot j \mid i \in I, j \in J\})$  das von allen Produkten  $i \cdot j$  erzeugte Ideal. Analog definieren wir das Produkt  $I_1 \cdots I_n$  endlich vieler Ideale.

*Übung 2.26.* Ist  $R$  kommutativ, sind  $I, J$  Ideale in  $R$  mit  $I+J = R$ , so gilt  $I \cdot J = I \cap J$ .

Sind  $I_1, \dots, I_n \subset R$  Ideale, so ist die kanonische Abbildung

$$\begin{aligned} \phi: R &\rightarrow R/I_1 \times \dots \times R/I_n \\ r &\mapsto (\bar{r}, \dots, \bar{r}) \end{aligned}$$

natürlich ein Homomorphismus von Ringen.

**Satz 2.27** (Der chinesische Restsatz). *Sei  $R$  ein kommutativer Ring,  $I_1, \dots, I_n \subset R$  Ideale in  $R$  mit der Eigenschaft  $I_r + I_s = R$  für alle Paare  $(r, s)$  mit  $r \neq s$ . So induziert die eben definierte Abbildung  $\phi$  einen Isomorphismus*

$$\tilde{\phi}: R/(I_1 \cap \dots \cap I_n) \xrightarrow{\sim} R/I_1 \times \dots \times R/I_n.$$

*Beweis.* Wir zeigen zunächst, daß  $\tilde{\phi}$ , oder, gleichbedeutend,  $\phi$  surjektiv ist. Sei  $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in R/I_1 \times \dots \times R/I_n$  das Element mit der 1 an der  $i$ -ten Stelle. Dann ist  $(\bar{r}_1, \dots, \bar{r}_n) = \phi(r_1)e_1 + \dots + \phi(r_n)e_n$ , wobei  $r_1, \dots, r_n \in R$  und  $\bar{r}_i \in R/I_i$  die Restklasse von  $r_i$  ist. Es genügt,  $f_i \in R$  zu finden mit  $\phi(f_i) = e_i$ , denn dann ist  $\phi(r_1 f_1 + \dots + r_n f_n) = (\bar{r}_1, \dots, \bar{r}_n)$ .

Wir fixieren also  $i$ . Sei  $j \neq i$ . Nach unserer Voraussetzung  $I_i + I_j = R$  gibt es Elemente  $a_j \in I_i$  und  $b_j \in I_j$  mit  $1 = a_j + b_j$ . Wir setzen  $f_i = \prod_{j \neq i} b_j$ . Ist  $\phi(f_i) = (c_1, \dots, c_n)$ , so ist, für  $j \neq i$ ,  $c_j = 0$ , da  $b_j \in I_j$ , und  $c_i = 1$ , da  $f_i = \prod_{j \neq i} (1 - a_j)$  und  $a_j \in I_i$  für alle  $j \neq i$ . Also ist  $\phi(f_i) = e_i$ .

Offensichtlich ist der Kern von  $\phi$  der Durchschnitt über die Ideale  $I_1, \dots, I_n$ , also ist  $\tilde{\phi}$  injektiv.  $\square$

Eine Anwendung:

**Satz 2.28** (Interpolation durch Polynome, einfache Form). *Ist  $K$  ein Körper,  $a_1, \dots, a_n \in K$  paarweise verschieden und  $b_1, \dots, b_n \in K$ , so gibt es ein Polynom  $P \in K[X]$  mit  $P(a_i) = b_i$ .*

*Beweis.* Nach dem chinesischen Restsatz gibt es  $P \in K[X]$  mit  $\bar{P} = \bar{b}_i$  in  $K[X]/(X - a_i)$  für  $i = 1, \dots, n$ , denn es ist  $(X - a_i) + (X - a_j) = K[X]$  für  $i \neq j$ . Dies bedeutet aber  $P(a_i) = b_i$ .  $\square$

**2.7. Irreduzible und prime Elemente.** Sei  $R$  ein kommutativer Ring.

**Definition 2.29.** Ein Element  $a \in R$  heißt *irreduzibel*, wenn es nicht invertierbar ist, und wenn aus einer Darstellung  $a = bc$  mit  $b, c \in R$  folgt, daß entweder  $b$  oder  $c$  invertierbar sind.

*Beispiele 2.30.* (1) Ein Element  $a \in \mathbb{Z}$  ist genau dann irreduzibel, wenn  $a$  oder  $-a$  eine Primzahl ist.

(2) Das Polynom  $X^2 + 1$  ist irreduzibel in  $\mathbb{R}[X]$ , aber reduzibel in  $\mathbb{C}[X]$  und  $\mathbb{F}_2[X]$ .

**Definition 2.31.** Sei  $R$  ein Integritätsbereich. Ein Element  $p \in R$  heißt *prim*, falls es nicht Null ist und keine Einheit, und wenn aus  $p \mid ab$  mit  $a, b \in R$  folgt  $p \mid a$  oder  $p \mid b$ .

*Beispiel 2.32.* Ein Element  $a \in \mathbb{Z}$  ist genau dann prim, wenn  $a$  oder  $-a$  eine Primzahl ist, also genau dann, wenn  $a$  irreduzibel ist. (Hier rächt sich, daß wir gefordert haben, eine Primzahl in  $\mathbb{Z}$  sei positiv.)

Ist  $p$  prim, so ist  $p$  irreduzibel, denn wäre  $p = ab$ , so folgt entweder  $p \mid a$ , also  $a = cp$  und damit  $p = p(cb)$  und  $b$  wäre eine Einheit, oder  $p \mid b$  und  $a$  wäre eine Einheit. Aber irreduzible Elemente müssen nicht prim sein.

*Beispiel 2.33.* In  $\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$  ist das Element 2 irreduzibel, aber nicht prim, denn  $2 \mid 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ , aber  $2 \nmid 1 \pm i\sqrt{5}$ .

## 2.8. Faktorielle Ringe.

**Definition 2.34.** Ein Ring  $R$  heißt *faktoriell*, wenn  $R$  ein Integritätsbereich ist und jedes  $a \in R$ ,  $a \neq 0$  sich als Produkt  $a = up_1 \cdots p_n$  von irreduziblen Elementen  $p_1, \dots, p_n \in R$  und einer Einheit  $u \in R^\times$  schreiben läßt und diese Darstellung eindeutig bis auf Reihenfolge und Einheiten ist.

“Eindeutigkeit bis auf Reihenfolge und Einheiten” soll folgendes bedeuten: Sind  $a = up_1 \cdots p_n = vq_1 \cdots q_m$  zwei Darstellungen mit irreduziblen Elementen  $p_1, \dots, p_n, q_1, \dots, q_m \in R$  und Einheiten  $u, v \in R^\times$ , so gilt  $m = n$  und es gibt eine Permutation  $\sigma \in S_n$  und Einheiten  $u_1, \dots, u_n$  mit  $p_i = u_i q_{\sigma(i)}$ .

*Beispiel 2.35.*  $\mathbb{Z}$  ist ein faktorieller Ring: Die irreduziblen Elemente in  $\mathbb{Z}$  sind gerade die Primzahlen und negativen Primzahlen. Ist  $n \in \mathbb{Z}$ ,  $n \neq 0$ , so läßt sich  $n$  schreiben in der Form  $n = (\pm 1)p_1 \cdots p_n$  mit Primzahlen  $p_1, \dots, p_n \in P$  nach 1.27. Diese Darstellung ist eindeutig bis auf Reihenfolge der  $p_i$  und wir erhalten offenbar jede weitere Darstellung als Produkt irreduzibler Elemente, indem wir eine gerade Anzahl von  $-$ -Zeichen auf die  $p_i$  verteilen.

**Lemma 2.36.** *Ist  $R$  faktoriell, so ist jedes irreduzible Element prim.*

*Beweis.* Das folgt direkt aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren.  $\square$

## 2.9. Hauptidealringe.

**Definition 2.37.** Ein Integritätsbereich  $R$  heißt *Hauptidealring*, falls jedes Ideal in  $R$  ein Hauptideal ist, also von einem Element erzeugt ist. In Formeln: Ist  $I \subset R$  ein Ideal, so gibt es  $a \in I$  mit  $I = (a)$ .

**Lemma 2.38.** *In einem Hauptidealring ist jedes irreduzible Element prim.*

*Beweis.* Sei  $R$  ein Hauptidealring und  $p \in R$  irreduzibel. Seien  $a, b \in R$  mit  $p \mid ab$ . Wir müssen zeigen, daß  $p$  entweder  $a$  oder  $b$  teilt. Falls  $p$  kein Teiler von  $a$  ist, liegt  $a$  nicht in  $(p)$ . Sei  $(d) = (a, p)$  das von  $a$  und  $p$  erzeugte Ideal. Dann gibt es  $r \in R$  mit  $dr = p$ . Da  $p$  irreduzibel ist, ist entweder  $d$  oder  $r$  eine Einheit, d.h. es gilt entweder  $(d) = R$  oder  $(d) = (p)$ . Der zweite Fall würde  $a \notin (p)$  widersprechen, also gilt  $(d) = R$ . Es gibt also  $r, s \in R$  mit  $1 = ra + sp$ , also  $b = bra + bsp$ . Nun teilt  $p$  sowohl  $rba$  als auch  $bsp$ , also auch deren Summe  $b$ .  $\square$

## 2.10. Euklidische Ringe.

**Definition 2.39.** Ein *euklidischer Ring* ist ein Integritätsbereich  $R$ , für den eine Abbildung  $d: R \setminus \{0\} \rightarrow \mathbb{N}$  existiert mit der folgenden Eigenschaft: Für alle  $a, b \in R$  mit  $a \neq 0$  gibt es  $c, r \in R$  mit  $b = ca + r$  und  $r = 0$  oder  $d(r) < d(a)$ .

*Beispiele 2.40.* (1)  $\mathbb{Z}$  mit dem Absolutbetrag  $|\cdot|$ .

(2) Der Polynomring  $K[x]$  über einem Körper  $K$  mit der Gradabbildung  $\text{grad}$ .

(3) Der Ring der *Gaußschen Zahlen*  $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$  mit der Abbildung  $d(a + ib) = a^2 + b^2$ .

**Satz 2.41.** (1) *Jeder euklidische Ring ist ein Hauptidealring.*

(2) *Jeder Hauptidealring ist faktoriell.*

*Beweis.* Sei  $R$  ein euklidischer Ring,  $I \subset R$  ein Ideal. Wir wollen zeigen, daß es ein  $a \in R$  gibt mit  $I = (a)$ . Ist  $I = \{0\}$ , dann ist  $I = (0)$ . Ansonsten sei  $a \in I$ ,  $a \neq 0$  ein Element mit  $d(a)$  minimal. Dann gilt sicherlich  $(a) \subset I$ . Ist  $b \in I$ , so gibt es  $c, r \in R$  mit  $b = ca + r$ . Dann ist auch  $r \in I$  und wegen der Minimalität von  $d(a)$  muß  $r = 0$  gelten, also  $b = ca$  und damit  $I = (a)$ . Damit ist (1) gezeigt.

Sei nun  $R$  ein Hauptidealring, und  $a \in R$ ,  $a \neq 0$ . Angenommen, es gäbe keine Zerlegung von  $a$  in ein Produkt aus einer Einheit und Irreduziblen (im Folgenden kurz "Zerlegung" genannt). Dann ist  $a$  nicht irreduzibel, läßt sich also schreiben  $a = a_1 b_1$ , wobei  $a_1$  und  $b_1$  keine Einheiten sind. Zerlegungen von  $a_1$  und  $b_1$  würden eine Zerlegung von  $a$  ergeben, wir können also annehmen,  $a_1$  habe ebenfalls keine Zerlegung. Wir fahren fort und erhalten Elemente  $a_2, a_3, a_4, \dots$  mit  $a_{i+1} \mid a_i$ , die alle keine Zerlegung besitzen. Dies ergibt eine Kette

$$(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset$$

von Idealen in  $R$ , deren Vereinigung wieder ein Ideal in  $R$  ist, also von der Form  $(h)$  für ein  $h \in R$ .  $h$  muß aber in irgendeinem  $(a_i)$  enthalten sein, und es folgt  $(a_i) = (a_{i+1}) = (a_{i+2}) = \dots$ . Insbesondere unterscheiden sich  $a_{i+1}$  und  $a_i$  nur um eine Einheit, was unserer Konstruktion widerspricht. Es gibt also eine Zerlegung von  $a$  in eine Einheit und Irreduzible.

Zur Eindeutigkeit der Zerlegung: Seien  $a = up_1 \cdots p_n = vq_1 \cdots q_m$  zwei Zerlegungen. Nach ... ist jedes irreduzible Element in  $R$  prim. Da  $p_1$  das Produkt  $vq_1 \cdots q_m$  und damit auch  $q_1 \cdots q_m$  teilt, muß  $p_1$  einen der Faktoren teilen, und nach Umsortieren können wir annehmen  $p_1$  teile  $q_1$ . Da  $q_1$  irreduzibel ist, gilt  $q_1 = p_1 u_1$  mit einer Einheit  $u_1 \in R^\times$ . Durch Kürzen ( $R$  ist ein Integritätsbereich!) erhalten wir die Gleichung  $up_2 p_3 \cdots p_n = v' q_2 \cdots q_m$ . Jetzt können wir die Argumentation wiederholen und erhalten induktiv die Eindeutigkeit der Zerlegung.  $\square$

**Proposition 2.42.** *Der Polynomring  $K[X]$  ist ein euklidischer Ring, also ein Hauptidealring und faktoriell.*

*Beweis.* Die Gradabbildung  $\text{grad}: K[X] \setminus \{0\} \rightarrow \mathbb{N}$  erfüllt die Voraussetzungen in der Definition eines euklidischen Rings nach 2.21.  $\square$

**2.11. Der Quotientenkörper.** Sei  $R$  ein Integritätsbereich. Wir betrachten die Menge  $X = \{(a, b) \mid a, b \in R, b \neq 0\}$  und auf  $X$  die Äquivalenzrelation  $(a, b) \sim (a', b')$

genau dann, wenn  $ab' = ba'$  (dies ist eine Äquivalenzrelation, wenn  $R$  ein Integritätsbereich ist!). Wenn wir uns  $(a, b)$  als Bruch  $\frac{a}{b}$  geschrieben vorstellen, ist dies genau die Äquivalenzrelation von Brüchen:

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b.$$

Insbesondere darf man Kürzen: Es ist  $(ad, bd) \sim (a, b)$  für alle  $d \neq 0!$  Von nun an bezeichnen wir intuitiv die Ähnlichkeitsklasse von  $(a, b)$  mit Symbol  $\frac{a}{b}$ .

Wir wollen auf der Menge der Klassen  $\text{Quot}(R) := X/\sim$  eine Ringstruktur definieren und lassen uns von der Vorstellung an Brüche leiten. Wir definieren also

$$\begin{aligned} \frac{a}{b} + \frac{a'}{b'} &= \frac{ab' + a'b}{bb'} \\ \frac{a}{b} \cdot \frac{a'}{b'} &= \frac{aa'}{bb'}. \end{aligned}$$

Die Addition wird verständlich, wenn man die Brüche “auf Hauptnenner bringt”. Unsere Definition lautet dann nämlich  $\frac{ab'}{bb'} + \frac{a'b}{bb'} = \frac{ab'+a'b}{bb'}$ .

Unsere Verknüpfungen sind wohldefiniert auf Äquivalenzklassen, denn ist beispielsweise  $\frac{a'}{b'} = \frac{a''}{b''}$ , also  $a'b'' = b'a''$ , so ist

$$\begin{aligned} (ab'' + a''b)bb' &= abb'b'' + a''b'b^2 \\ &= abb'b'' + a'b''b^2 \\ &= (ab' + a'b)bb'', \end{aligned}$$

also  $\frac{ab''+a''b}{bb''} = \frac{ab'+a'b}{bb'}$ . Man rechnet auch leicht nach, daß beide Verknüpfungen assoziativ sind. Außerdem ist die Multiplikation offensichtlich kommutativ.

$\text{Quot}(R)$  ist mit dieser Addition eine abelsche Gruppe, mit neutralem Element  $\frac{0}{1}$  und zu  $\frac{a}{b}$  Inversem  $\frac{-a}{b}$ . Das bzgl. der Multiplikation neutrale Element ist  $\frac{1}{1}$ , und schließlich gelten auch die Distributivgesetze, denn

$$\begin{aligned} \left(\frac{a}{b} + \frac{a'}{b'}\right) \cdot \frac{c}{d} &= \frac{ab' + a'b}{bb'} \cdot \frac{c}{d} \\ &= \frac{ab'c + a'bc}{bb'd} \\ &= \frac{ab'cd + a'bcd}{bb'd^2} \\ &= \frac{ac}{bd} \cdot \frac{a'c}{b'd} \\ &= \frac{ac}{d} \cdot \frac{1}{d} + \frac{a'c}{b'} \cdot \frac{1}{d}. \end{aligned}$$

Damit wird  $\text{Quot}(R)$  ein kommutativer Ring. Aber  $\text{Quot}(R)$  ist sogar ein Körper, denn ist  $\frac{a}{b}$ ,  $a, b \neq 0$ , so ist  $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$ .

**Definition 2.43.** Wir nennen den so aus dem Integritätsbereich  $R$  konstruierten Körper  $\text{Quot}(R)$  den *Quotientenkörper* von  $R$ .

Die Abbildung  $\text{can}: R \rightarrow \text{Quot}(R)$ ,  $r \mapsto \frac{r}{1}$ , ist ein Homomorphismus von Ringen.

**Satz 2.44** (Die universelle Eigenschaft des Quotientenkörpers). *Sei  $\phi: R \rightarrow R'$  ein Ringhomomorphismus mit der Eigenschaft, daß  $\phi(r) \in R'$  eine Einheit ist für alle*

$r \neq 0$  (also  $\phi(R \setminus 0) \subset (R')^\times$ ). Dann gibt es einen eindeutig bestimmten Homomorphismus  $\tilde{\phi}: \text{Quot}(R) \rightarrow R'$  von Ringen, so daß das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R' \\ & \searrow \text{can} & \nearrow \tilde{\phi} \\ & \text{Quot}(R) & \end{array}$$

kommutiert.

*Beweis.* Sind  $a, b \in R$  mit  $b \neq 0$  so definieren wir  $\hat{\phi}\left(\frac{a}{b}\right) = \phi(a) \cdot \phi^{-1}(b)$ . Diese Abbildung ist konstant auf den Ähnlichkeitsklassen, induziert also eine Abbildung  $\tilde{\phi}: \text{Quot}(R) \rightarrow R'$ . Man rechnet leicht nach, daß  $\tilde{\phi}$  ein Homomorphismus von Ringen ist, und man macht sich schnell klar, daß  $\tilde{\phi}$  der einzige Homomorphismus ist, der obiges Diagramm zum Kommutieren bringt.  $\square$

Ist  $K$  ein Körper, so bezeichnen wir den Quotientenkörper von  $K[X]$  mit  $K(X)$ .

*Übung 2.45.* Bestimmen Sie den Quotientenkörper  $K((X))$  von  $K[[X]]$ .

## 2.12. Primfaktorzerlegung in Polynomringen.

**Definition 2.46.** Sei  $R$  ein faktorieller Ring. Dann heißt ein Polynom  $P(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$  *primitiv*, wenn es kein irreduzibles Element  $b \in R$  gibt, das alle  $a_i$  teilt, wenn es also kein  $b \in R$  gibt mit  $b \mid P(X)$  (wir fassen hier  $R \subset R[X]$  als den Unterring der konstanten Polynome auf!).

**Lemma von Gauß 2.47.** Ist  $R$  faktoriell und  $P, Q \in R[X]$  primitiv, so ist auch  $P \cdot Q \in R[X]$  primitiv.

*Beweis.* Wir benötigen ein Lemma.

**Lemma 2.48.** In einem Integritätsbereich  $R$  ist ein Element  $p$  genau dann prim, wenn  $R/(p)$  ebenfalls ein Integritätsbereich ist.

*Beweis.*  $R/(p)$  ist ein Integritätsbereich wenn für alle  $a, b \in R$  aus  $\bar{a} \cdot \bar{b} = 0$  entweder  $\bar{a} = 0$  oder  $\bar{b} = 0$  folgt. Dies ist genau dann der Fall, wenn aus  $p \mid ab$  folgt  $p \mid a$  oder  $p \mid b$ . Dies ist die Definition eines primen Elements  $p$ .  $\square$

Wir beweisen nun das Lemma von Gauß. Sind  $P, Q \in R[X]$  Polynome und  $P \cdot Q$  nicht primitiv, so gibt es ein irreduzibles (=prim) Element  $p \in R$  mit  $p \mid P \cdot Q$ , also  $\overline{P \cdot Q} = 0$  in  $R/(p)$ . Nun ist nach obigem Lemma  $R/(p)$  ein Integritätsbereich und nach Lemma 2.20 ist auch  $R/(p)[X]$  nullteilerfrei. Also ist  $\bar{P} = 0$  oder  $\bar{Q} = 0$ , also  $p \mid P$  oder  $p \mid Q$  und damit  $P$  oder  $Q$  nicht primitiv.  $\square$

Wir haben schon gesehen, daß der Ring  $K[X]$  der Polynome über einem Körper  $K$  euklidisch, also insbesondere faktoriell ist. Der nächste Satz verallgemeinert diese Aussage.

**Satz 2.49.** Der Polynomring  $R[X]$  über einem faktoriellen Ring  $R$  ist wieder faktoriell.

Insbesondere sind also die Ringe  $\mathbb{Z}[X_1, \dots, X_n]$  und  $K[X_1, \dots, X_n]$  faktoriell.

*Beweis.* Sei  $P \in R[X]$ . Dann können wir  $P$  auch auffassen als Polynom in  $\text{Quot}(R)[X]$ . Da  $\text{Quot}(R)[X]$  ein faktorieller Ring ist, gibt es eine Zerlegung  $P(X) = \tilde{Q}_1(X) \cdots \tilde{Q}_n(X)$  mit irreduziblen Polynomen  $\tilde{Q}_1(X), \dots, \tilde{Q}_n(X)$ . “Multiplikation mit dem Hauptnenner” und anschließendem “Teilen durch den größten gemeinsamen Faktor” liefert uns eine Zerlegung  $P(X) = cQ_1(X) \cdots Q_n(X)$  mit primitiven Polynomen  $Q_1(X), \dots, Q_n(X)$  und einem Element  $c \in \text{Quot}(R)$ . Nach dem Lemma von Gauß ist  $Q_1(X) \cdots Q_n(X)$  primitiv und wir schließen  $c \in R$ . Da  $R$  faktoriell ist, gibt es eine Einheit  $u \in R^\times$  und irreduzible Elemente  $p_1, \dots, p_m \in R$  mit  $c = up_1 \cdots p_m$ . Wir erhalten

$$P(X) = up_1 \cdots p_m Q_1(X) \cdots Q_n(X).$$

Man macht sich leicht klar, daß  $p_1, \dots, p_m, Q_1(X), \dots, Q_n(X) \in R[X]$  irreduzibel sind. Es gibt also eine Zerlegung von  $P$  in Einheit und Irreduzible. Wir haben übrigens auch gezeigt, daß ein nicht-konstantes Polynom  $Q(X) \in R[X]$  irreduzibel ist genau dann, wenn es primitiv und in  $\text{Quot}(R)[X]$  irreduzibel ist.

Wir müssen noch zeigen, daß diese Zerlegung bis auf Reihenfolge und Einheiten eindeutig ist. Ist

$$P(X) = u'p'_1 \cdots p'_m Q'_1(X) \cdots Q'_n(X)$$

eine weitere Zerlegung der gewünschten Art mit nicht konstanten Polynomen  $Q'_i(X)$ , so sind die  $Q'_i(X)$  irreduzibel in  $\text{Quot}(R)[X]$ . Da  $\text{Quot}(R)[X]$  faktoriell ist, gilt also  $n = n'$  und es gibt  $\sigma \in S_n$  und Einheiten  $q_i \in \text{Quot}(R)$  mit  $Q_i(X) = q_i Q'_{\sigma(i)}(X)$ . Da nun  $Q_i$  und  $Q'_i$  primitiv sind, folgt  $q_i \in R^\times$ . Schließlich müssen  $up_1 \cdots p_m$  und  $u'p'_1 \cdots p'_m$  bis auf eine Einheit in  $R^\times$  übereinstimmen und wir schließen den Beweis mit der Bemerkung, daß  $R$  faktoriell ist. □

Wir haben eben auch folgendes bewiesen:

**Satz 2.50.** *Ist  $R$  ein faktorieller Ring, so ist  $P \in R[X]$  genau dann irreduzibel, wenn entweder*

- (1)  $P$  ein konstantes Polynom und irreduzibel als Element in  $R$  ist, oder
- (2)  $P$  ein primitives Polynom und irreduzibel in  $\text{Quot}(R)[X]$  ist.

### 2.13. Das Eisensteinkriterium.

**Satz 2.51** (Eisensteinkriterium). *Ist  $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$  und ist  $p$  ein Primzahl mit  $p \nmid a_n$ ,  $p \mid a_{n-1}, \dots, p \mid a_0$  und  $p^2 \nmid a_0$ , dann ist  $P$  irreduzibel in  $\mathbb{Q}[X]$ .*

*Beweis.* Wir nehmen unter den Voraussetzungen des Satzes das Gegenteil an, nämlich daß  $P(X)$  reduzibel ist in  $\mathbb{Q}[X]$ . Wir können sogar annehmen,  $P \in \mathbb{Z}[X]$  sei primitiv. Dann ist nach Satz 2.50  $P$  sogar reduzibel in  $\mathbb{Z}[X]$ , also  $P = Q \cdot R$  mit  $Q, R \in \mathbb{Z}[X]$  von positivem Grad. Die natürliche Abbildung  $\mathbb{Z} \rightarrow \mathbb{F}_p$  induziert eine Abbildung  $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ ,  $F \mapsto \bar{F}$ , die man das *Reduzieren modulo  $p$*  nennt. Dies ist ein Ringhomomorphismus und wir erhalten  $\bar{P} = \bar{Q} \cdot \bar{R}$ . Nach unseren Voraussetzungen ist  $\bar{P} = \bar{a}_n X^n$ , also  $\bar{Q} = cX^q$  und  $\bar{R} = dX^r$  mit  $c, d \in \mathbb{F}_p$ ,  $c, d \neq 0$  und  $q, r \geq 0$ . Es gilt sogar  $q, r > 0$ , denn aus  $r = 0$  würde  $q = n$  folgen, also wäre  $R$  ein konstantes Polynom, was ja nicht der Fall ist. Es ist also  $q, r > 0$ , also sind die konstanten Terme von  $Q, R$  durch  $p$  teilbar, also ist der konstante Term von  $P$  durch  $p^2$  teilbar, was unserer Voraussetzung widerspricht. □

### 2.14. Kreisteilungspolynome.

**Definition 2.52.** Sei  $n \in \mathbb{N}$ . Ein  $\zeta \in \mathbb{C}$  mit  $\zeta^n = 1$  heißt (*komplexe*) *n-te Einheitswurzel*.

Eine *n-te Einheitswurzel* ist also nichts anderes als eine Nullstelle des Polynoms  $X^n - 1 \in \mathbb{C}[X]$ .

Das Produkt zweier *n-ten Einheitswurzeln*, sowie das multiplikativ inverse einer *n-ten Einheitswurzel* ist wieder eine *n-te Einheitswurzel*, also bilden die *n-ten Einheitswurzeln* eine Untergruppe der multiplikativen Gruppe  $\mathbb{C}^\times$ . Aus der Analysis sollte bekannt sein, daß die Menge der *n-ten Einheitswurzeln* gerade  $\{e^{2\pi i k/n} \mid k = 0, \dots, n-1\}$  ist. Es gibt also genau *n n-te Einheitswurzeln* und die Gruppe der *n-ten Einheitswurzeln* ist zyklisch, also isomorph zu  $\mathbb{Z}/n\mathbb{Z}$ .

Wir erhalten die Identität

$$X^n - 1 = \prod_{\zeta^n=1} (X - \zeta) = \prod_{k=1}^n (X - e^{2\pi i k/n}).$$

Wir können die *n-ten Einheitswurzeln* nun nach ihrer Ordnung in Klassen einteilen und definieren für  $d \geq 1$

$$\Phi_d(X) = \prod_{\text{ord } \zeta=d} (X - \zeta).$$

(Anmerkung: Hier bezeichnet  $\text{ord } \zeta$  die Ordnung von  $\zeta$ ). Dann gilt also

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

*Beispiele 2.53.* Es ist  $\Phi_1(X) = X-1$ ,  $\Phi_2(X) = X+1$ ,  $\Phi_3(X) = (X-e^{2\pi i/3})(X-e^{2\pi i \cdot 2/3}) = X^2 - (e^{2\pi i/3} + e^{2\pi i \cdot 2/3})X + 1$ . Aus  $X^3 - 1 = \Phi_1(X)\Phi_3(X) = (X-1)(X^2 - (e^{2\pi i/3} + e^{2\pi i \cdot 2/3})X + 1)$  erhalten wir  $e^{2\pi i/3} + e^{2\pi i \cdot 2/3} = 1$ , also  $\Phi_3(X) = X^2 + X + 1$ .

Ist  $n = 4$ , so sind  $\zeta = i$  und  $\zeta = -i$  die einzigen Einheitswurzeln der Ordnung 4 und  $\zeta = -1$  die einzige Einheitswurzel der Ordnung 2. Es ist also  $\Phi_4(X) = (X+i)(X-1) = X^2 + 1$  und  $\Phi_2(X) = X + 1$ . Tatsächlich ist

$$X^4 - 1 = \Phi_4\Phi_2\Phi_1 = (X^2 + 1)(X + 1)(X - 1).$$

*Übung 2.54.* Man zeige  $\Phi_9(X) = X^6 + X^3 + 1$ .

Ganz allgemein gilt  $X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \dots + 1)$ , und damit  $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + 1$  für eine Primzahl  $p$ . Insbesondere  $\Phi_p \in \mathbb{Z}[X]$ .

**Lemma 2.55.** Für alle  $d \geq 1$  hat  $\Phi_d$  ganze Koeffizienten:  $\Phi_d \in \mathbb{Z}[X]$ .

*Beweis.* Per Induktion nach  $d$ . Für  $d = 1$  haben wir das schon gesehen. Sei das Lemma also bewiesen für alle  $d'$  mit  $d' < d$ . Dann ist  $X^d - 1 = P(X)\Phi_d(X)$  mit einem Polynom  $P(X) = a_0 + \dots + a_{s-1}X^{s-1} + X^s \in \mathbb{Z}[X]$  mit Leitkoeffizient 1, und per absteigender Induktion über den Exponenten erkennen wir, daß jeder Koeffizient in  $\Phi_d(X)$  eine ganze Zahl ist.  $\square$

**Lemma 2.56.** Sei  $p$  eine Primzahl. Dann ist das *p-te Kreisteilungspolynom*  $\Phi_p \in \mathbb{Q}[X]$  irreduzibel.

*Beweis.* Die Gleichung  $X^p - 1 = (X - 1)\Phi_p(X)$  liest sich nach Reduktion modulo  $p$

$$(X - \bar{1})^p = X^p - \bar{1} = (X - \bar{1})\bar{\Phi}_p(X).$$

Also ist  $\bar{\Phi}_p(X) = (X - \bar{1})^{p-1}$ . Substituieren wir  $X = Y + 1$ , so ist  $\bar{\Phi}_p(Y + 1) = Y^{p-1}$ . Der konstante Koeffizient von  $\Phi_p(Y + 1) = (Y + 1)^{p-1} + \dots + (Y + 1) + 1$  ist  $= p$ , während alle anderen bis auf den Leitkoeffizienten durch  $p$  teilbar sind, wie wir eben hergeleitet haben. Nach dem Eisensteinkriterium ist  $\Phi_p$  irreduzibel in  $\mathbb{Q}[X]$ .  $\square$

### 3. K $\bar{\bar{}}$

Sei  $L$  ein Körper. Ein Teilring  $K \subset L$ , der selbst ein Körper ist, heißt *Unterkörper* von  $L$ . Natürlich ist der Durchschnitt zweier Unterkörper wieder ein Unterkörper. Es gibt also einen kleinsten Unterkörper  $\mathbb{P} \subset L$ , der der *Primkörper* von  $L$  genannt wird.

**Satz 3.1.** *Der Primkörper  $\mathbb{P}$  von  $L$  ist entweder isomorph zu  $\mathbb{Q}$  oder zu  $\mathbb{F}_p$  für eine Primzahl  $p$ .*

*Anmerkung 3.2.* Da  $\mathbb{Q}$  unendlich viele und  $\mathbb{F}_p$  genau  $p$  Elemente hat, sind die Körper  $\mathbb{Q}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \dots$  paarweise nicht isomorph.

*Beweis.* Sei  $\phi: \mathbb{Z} \rightarrow L$  der Homomorphismus von Ringen mit  $\phi(n) = n \cdot 1$ . Wir unterscheiden zwei Fälle.

Erstens:  $\phi$  ist injektiv. Dann gibt es nach der universellen Eigenschaft des Quotientenkörpers einen injektiven Ringhomomorphismus  $\tilde{\phi}: \mathbb{Q} = \text{Quot}(\mathbb{Z}) \rightarrow L$ . Da jeder Unterkörper von  $L$  das Bild von  $\phi$  enthalten muß, muß jeder Unterkörper auch das Bild von  $\tilde{\phi}$  enthalten, also haben wir den Primkörper  $\mathbb{P}$  von  $L$  mit  $\mathbb{Q}$  identifiziert.

Zweitens:  $\phi$  ist nicht injektiv. Dann ist  $\ker \phi = m\mathbb{Z}$  für ein  $m \in \mathbb{Z}$  und wir erhalten wegen der universellen Eigenschaft des Faktorrings einen injektiven Ringhomomorphismus  $\tilde{\phi}: \mathbb{Z}/m\mathbb{Z} \rightarrow L$ . Da  $L$  nullteilerfrei ist, muß, nach Proposition 2.14,  $m$  eine Primzahl sein. Folglich haben wir eine Einbettung  $\tilde{\phi}: \mathbb{F}_p \rightarrow L$  konstruiert. Wie oben erkennt man, daß jeder Unterkörper von  $L$  das Bild von  $\tilde{\phi}$  enthalten muß. Folglich haben wir den Primkörper  $\mathbb{P}$  von  $L$  mit  $\mathbb{F}_p$  identifiziert.  $\square$

**Definition 3.3.** Man sagt, der Körper  $L$  habe *Charakteristik Null*, falls  $\mathbb{P} \cong \mathbb{Q}$ , und *Charakteristik  $p$* , falls  $\mathbb{P} \cong \mathbb{F}_p$ . Man schreibt  $\text{char } L = 0$  im ersten und  $\text{char } L = p$  im zweiten Fall.

*Bemerkung 3.4.* Es gilt  $\ker(\phi: \mathbb{Z} \rightarrow L) = \text{char } L \cdot \mathbb{Z}$  und dadurch ist die Zahl  $\text{char } L \in \mathbb{Z}_{\geq 0}$  auch eindeutig bestimmt.

#### 3.1. Körpererweiterungen.

**Definition 3.5.** Sei  $L$  ein Körper und  $K$  ein Unterkörper. Das Paar  $K \subset L$  nennt man eine *Körpererweiterung*.

Eine Körpererweiterung  $K \subset L$  wird oft auch mit dem Symbol  $L/K$  bezeichnet. Man nennt  $K$  dann auch den *Grundkörper* und  $L$  den *Erweiterungskörper*.

Seien  $a_1, a_2, \dots, a_n$  Elemente aus  $L$ . Der Durchschnitt aller Teilringe von  $L$ , die sowohl  $K$  als auch die Menge  $\{a_1, \dots, a_n\}$  enthalten, ist wieder ein Teilring und wird mit  $K[a_1, \dots, a_n] \subset L$  bezeichnet. Er wird auch der *von  $\{a_1, \dots, a_n\}$  über  $K$  erzeugte*

*Teilring* genannt. Analog ist der Durchschnitt aller Unterkörper von  $L$ , die sowohl  $K$  als auch  $\{a_1, \dots, a_n\}$  enthalten, wieder ein Unterkörper und wird mit  $K(a_1, \dots, a_n)$  bezeichnet. Er wird auch der *von  $\{a_1, \dots, a_n\}$  über  $K$  erzeugte Unterkörper* genannt.

**Übung 3.6.**  $K[a_1, \dots, a_n] = \{P(a_1, \dots, a_n) \mid P \in K[X_1, \dots, X_n]\}$ ,  $K(a_1, \dots, a_n) = \left\{ \frac{P(a_1, \dots, a_n)}{Q(a_1, \dots, a_n)} \mid P, Q \in K[X_1, \dots, X_n], Q(a_1, \dots, a_n) \neq 0 \right\}$ .

**Übung 3.7.** Man zeige  $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$  und  $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ .

Sei  $K \subset L$  eine Körpererweiterung.

**Definition 3.8.** Gibt es ein Element  $a \in L$  mit  $L = K(a)$ , so heißt die Körpererweiterung *primitiv* und  $a$  ein *primitives Element*.

Die abelsche Gruppe  $L$  zusammen mit der Multiplikation von Elementen aus  $K$  definiert auf  $L$  die Struktur eines  $K$ -Vektorraums. Wir bezeichnen mit  $[L : K] = \dim_K L \in \mathbb{N} \cup \{\infty\}$  seine Dimension.  $[L : K]$  wird auch der *Grad* der Körpererweiterung  $K \subset L$  genannt. Im Fall  $L = K(a)$  für ein  $a \in L$  heißt  $[K(a) : K]$  auch der *Grad von  $a$* . Eine *endliche Körpererweiterung* ist eine Körpererweiterung von endlichem Grad. Eine Körpererweiterung vom Grad 2 heißt *quadratische Körpererweiterung*.

**Beispiele 3.9.** Es ist  $[\mathbb{C} : \mathbb{R}] = 2$ ,  $[\mathbb{R} : \mathbb{Q}] = \infty$ ,  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ .

**Definition 3.10.** Ein Element  $a \in L$  heißt *algebraisch über  $K$* , falls es ein Polynom  $P \in K[X]$  gibt mit  $P \neq 0$  und  $P(a) = 0$ . Andernfalls heißt  $a$  *transzendent über  $K$* .

**Beispiele 3.11.** Wir werden sehen, daß jede komplexe Zahl algebraisch ist über  $\mathbb{R}$ , aber nicht unbedingt über  $\mathbb{Q}$ . Beispielsweise ist  $\pi$  nicht algebraisch über  $\mathbb{Q}$ , wie der Freiburger Mathematiker Ferdinand von Lindemann beweisen konnte. Daraus folgt übrigens die Unmöglichkeit der *Quadratur des Kreises*.

Sei  $P \in K[X]$  ein irreduzibles Polynom. Da  $K[X]$  ein Hauptidealring ist, ist  $(P) \subset K[X]$  ein maximales Ideal, also ist  $K[X]/(P)$  ein Körper, der  $K$  enthält.

**Definition 3.12.** Ein Polynom  $P \in K[X]$  heißt *normiert*, wenn sein Leitkoeffizient 1 ist.

**Satz 3.13.** Sei  $K \subset L$  eine Körpererweiterung und  $a \in L$ . Wir betrachten nun die primitive Körpererweiterung  $K \subset K(a)$ .

- (1) Ist  $a$  algebraisch über  $K$ , so gibt es ein eindeutig bestimmtes normiertes Polynom  $P \in K[X]$ , so daß  $K(a) \cong K[X]/(P)$ .  $P$  ist irreduzibel und heißt das Minimalpolynom von  $a$  über  $K$ . Es ist  $\deg P = [K(a) : K]$ .
- (2) Ist  $a$  transzendent über  $K$ , so ist  $K(a) \cong K(X)$ .

**Beispiele 3.14.**  $P(X) = X^2 + 1$  ist das Minimalpolynom von  $i \in \mathbb{C}$  und  $-i \in \mathbb{C}$  über  $\mathbb{R}$  oder  $\mathbb{Q}$ .  $P(X) = X^2 - 2$  ist das Minimalpolynom von  $\sqrt{2}$  über  $\mathbb{Q}$ .

**Beweis.** Sei  $\phi: K[X] \rightarrow K(a)$  das "Einsetzen von  $a$ ", also  $\phi(Q) = Q(a)$ . Es ist  $\text{im } \phi = K[a]$ . Sei  $I = \ker \phi$ . Wir erhalten einen Isomorphismus  $K[X]/I \cong K[a]$  von Ringen.

$a$  ist transzendent genau dann, wenn  $I = 0$ . In diesem Fall haben wir also einen Isomorphismus  $K[X] \cong K[a]$ , und aus der universellen Eigenschaft des Quotientenkörpers folgern wir einen Isomorphismus  $K(X) \cong K(a)$ .

$a$  ist algebraisch genau dann, wenn  $I \neq 0$ . In diesem Fall sei  $P \in K[X]$  das normierte Polynom kleinsten Grades in  $I$ . Dann ist  $I = (P)$  und  $P$  eindeutig bestimmt.  $I$  ist ein Primideal, da  $K[a]$  ein Integritätsbereich ist, also ist  $P$  ein irreduzibles Polynom. Dann ist  $K[X]/I$  sogar ein Körper. Also ist  $K[a]$  schon ein Körper und damit  $K[X]/I \cong K[a] = K(a)$ . Diese Identifikationen halten den Grundkörper  $K$  offenbar fest, also ist  $[K(a) : K] = \dim_K K(a) = \dim_K K[X]/I = \deg P$  (letzteres, da  $1, X, X^2, \dots, X^{\deg P-1}$  eine Basis von  $K[X]/(P)$  über  $K$  ist).  $\square$

Da  $[K(X) : K] = \infty$  ( $1, X, X^2, \dots$  sind linear unabhängig) folgern wir, daß  $a \in L$  algebraisch ist über  $K$  genau dann, wenn  $[K(a) : K]$  endlich ist.

**Satz 3.15.** Seien  $K \subset L$  und  $L \subset M$  Körpererweiterungen. Dann gilt

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

wobei wir  $a \cdot \infty = \infty \cdot a = \infty$  für alle  $a \in \mathbb{N} \cup \infty$  setzen.

*Beweis.* Sei  $(l_i)_{i \in I}$  eine Basis von  $L$  über  $K$ ,  $(m_j)_{j \in J}$  eine Basis von  $M$  über  $L$ . So ist  $(l_i m_j)_{(i,j) \in I \times J}$  eine Basis von  $M$  über  $K$ . Denn ist  $x \in M$ , so gibt es eindeutig bestimmte  $a_i \in L$  mit

$$x = \sum_{j \in J} a_j m_j,$$

und dann, für jedes  $j$ , eindeutig bestimmte  $b_{i,j} \in K$  mit

$$a_j = \sum_{i \in I} b_{i,j} l_i.$$

Also ist

$$x = \sum_{i,j} b_{i,j} l_i m_j.$$

$\square$

*Bemerkung 3.16.* Ist  $[L : K]$  endlich und  $a \in L$ , so ist  $K \subset K(a) \subset L$  und nach dem Satz ist  $[K(a) : K]$  ein Teiler von  $[L : K]$ . Also ist der Grad jedes über  $K$  algebraischen Elements aus  $L$  ein Teiler von  $[L : K]$ .

### 3.2. Algebraische Körpererweiterungen.

**Definition 3.17.** Eine Körpererweiterung  $K \subset L$  heißt *algebraisch*, wenn jedes Element  $a \in L$  algebraisch ist über  $K$ .

**Satz 3.18.** Sei  $K \subset L$  eine Körpererweiterung. Dann sind äquivalent:

- (1)  $K \subset L$  ist endlich.
- (2)  $K \subset L$  ist algebraisch und endlich erzeugt.
- (3)  $K \subset L$  wird von endlich vielen über  $K$  algebraischen Elementen erzeugt.

*Beweis.* Ist  $K \subset L$  endlich, so sicherlich endlich erzeugt und für alle  $a \in L$  ist  $[K(a) : K]$  endlich, also ist jedes  $a \in L$  algebraisch über  $K$  und  $K \subset L$  algebraisch. Also folgt (2) aus (1)

Die Implikation (2) nach (3) ist klar.

Wir zeigen nun, daß (1) aus (3) folgt. Wir nehmen an, daß  $L$  über  $K$  von den über  $K$  algebraischen Elementen  $a_1, \dots, a_n$  erzeugt wird. Dann ist  $L = K(a_1, \dots, a_n)$

endlich über  $K(a_1, \dots, a_{n-1})$ ,  $K(a_1, \dots, a_{n-1})$  endlich über  $K(a_1, \dots, a_{n-2}), \dots$ , und  $K(a_1)$  endlich über  $K$ . Nach Satz 3.15 ist  $L$  endlich über  $K$ .  $\square$

**Korollar 3.19.** *Sei  $K \subset L$  eine Körperweiterung. Die Menge aller Elemente  $a \in L$ , die algebraisch sind über  $K$ , bilden einen Unterkörper von  $L$*

*Beweis.* Sind  $a, b \in L$  algebraisch über  $K$ , so ist  $K(a, b)$  endlich über  $K$ , also ist jedes Element in  $K(a, b)$  algebraisch über  $K$ , insbesondere also  $a + b$ ,  $-a$  und  $a^{-1}$ . Folglich bilden die über  $K$  algebraischen Elemente einen Unterkörper von  $L$ .  $\square$

**Korollar 3.20.** *Sind  $K \subset L$  und  $L \subset M$  Körpererweiterungen, so ist  $M$  algebraisch über  $K$  genau dann, wenn  $M$  algebraisch über  $L$  und  $L$  algebraisch über  $K$  ist.*

*Beweis.* Ist  $M$  algebraisch über  $K$ , so ist sicherlich auch  $L$  algebraisch über  $K$ . Außerdem ist jedes Element aus  $M$  algebraisch über  $K$ , insbesondere also auch über  $L$ , damit ist  $M$  algebraisch über  $L$ . Wir haben also die eine Implikation gezeigt.

Wir nehmen nun an,  $M$  sei algebraisch über  $L$  und  $L$  sei algebraisch über  $K$ . Sei  $x \in M$  und  $P$  das Minimalpolynom von  $a$  über  $L$ . Sei  $K'$  die von den Koeffizienten von  $P$  erzeugte Erweiterung von  $K$ . Nach Satz 3.18 ist  $K'$  endlich über  $K$  (erzeugt von endlich vielen algebraischen Elementen). Da  $a$  algebraisch ist über  $K'$ , ist  $K'(a)$  endlich über  $K'$ , also muss  $K'(a)$  auch endlich über  $K$  sein. Also ist  $a$  algebraisch sogar über  $K$ .  $\square$

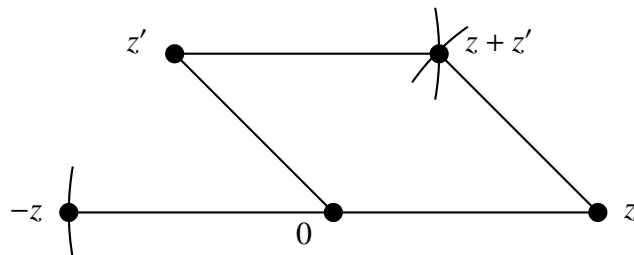
**3.3. Mit Zirkel und Lineal konstruierbare Zahlen.** Sei  $E \subset \mathbb{C}$  eine Menge. Eine Teilmenge von  $\mathbb{C}$  heißt *aus  $E$  konstruierbare Figur*, falls sie entweder eine Gerade durch zwei Punkte von  $E$  ist, oder ein Kreis, dessen Mittelpunkt in  $E$  liegt und dessen Radius der Abstand zweier Punkte in  $E$  ist. Sei  $K(E) \subset \mathbb{C}$  die Vereinigung von  $E$  mit allen Schnittpunkten zweier verschiedener aus  $E$  konstruierbaren Figuren. Wir können diese Konstruktion iterieren und  $K^2(E) = K(K(E))$ ,  $K^3(E) = K(K^2(E))$ ,  $\dots$  bilden.

Wir bezeichnen mit  $K = \bigcup_{n \in \mathbb{N}} K^n(\{0, 1\}) \subset \mathbb{C}$  die Menge der *mit Zirkel und Lineal konstruierbaren Zahlen*. Sie ist offenbar abzählbar unendlich.

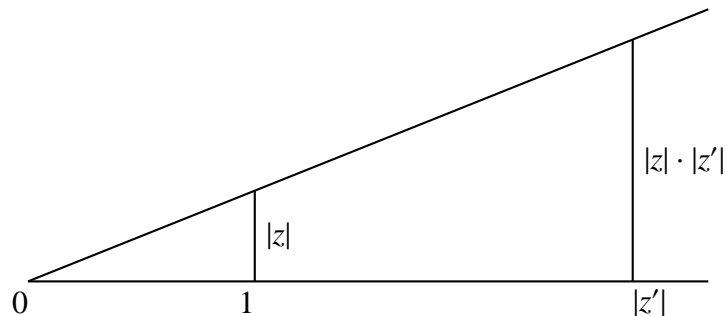
Sei  $Q \subset \mathbb{C}$  der kleinste Unterkörper von  $\mathbb{C}$ , der mit jedem Element auch seine Quadratwurzeln enthält, für den also gilt: Ist  $x \in Q$  und  $x^2 \in Q$ , so ist auch  $x \in Q$ .

**Satz 3.21.** *Es ist  $K = Q$ .*

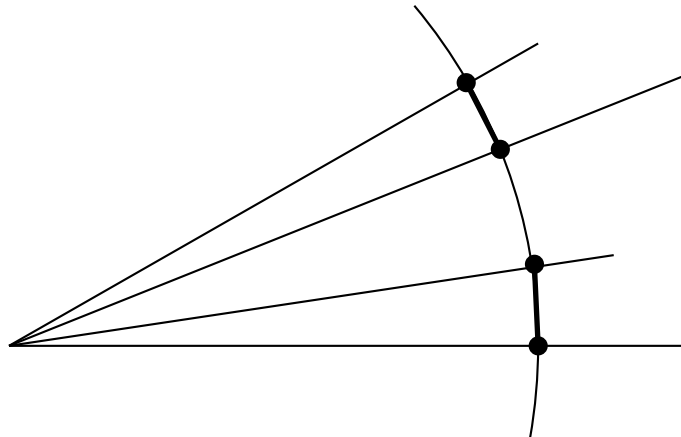
*Beweis.* Wir zeigen  $Q \subset K$ . Dazu müssen wir zeigen, daß  $K \subset \mathbb{C}$  ein Unterkörper ist, der mit jedem Element auch seine Quadratwurzeln enthält. Sicherlich bildet  $K$  eine Untergruppe der additiven Gruppe der komplexen Zahlen:



Wir wollen nun zeigen, daß mit  $z$  und  $z'$  auch  $zz'$  in  $K$  liegt. Sicherlich ist  $|z|, |z'| \in K$ . Aus der folgenden Figur wird ersichtlich, daß auch  $|z| \cdot |z'| \in K$ :

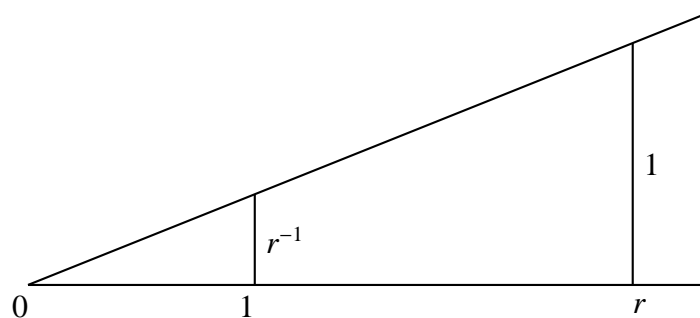


Wir schreiben nun  $z = |z| \cdot e^{i\phi}$ ,  $z' = |z'| \cdot e^{i\phi'}$ . Winkel lassen sich mit Zirkel und Lineal addieren:



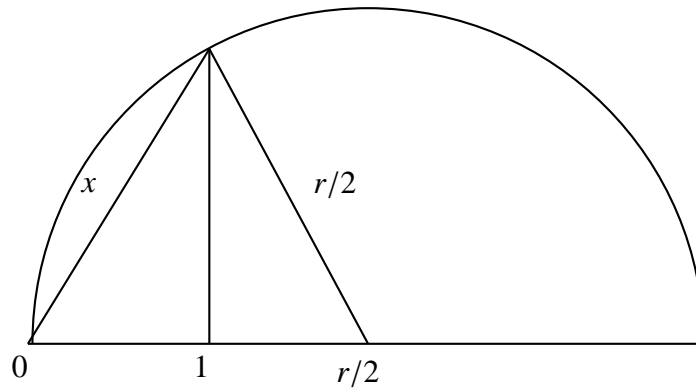
Tragen wir auf der Geraden durch 0 und  $e^{i(\phi+\phi')}$  die Länge  $|z| \cdot |z'|$  ab, haben wir also  $zz'$  konstruiert.

Um zu zeigen, daß  $K \subset \mathbb{C}$  ein Unterkörper ist, müssen wir nur noch zeigen, daß mit  $z$  auch  $z^{-1}$  in  $K$  liegt. Natürlich können wir mit einem Winkel auch sein negatives konstruieren, und es reicht zu zeigen, daß mit  $r \in \mathbb{R} \cap K \subset \mathbb{C}$  auch  $r^{-1} \in K$  liegt. Das erkennt man anhand folgender Konstruktion:



Schließlich müssen wir zeigen, daß mit  $z$  auch seine Quadratwurzeln  $\pm \sqrt{z}$  in  $K$  liegen. Man erkennt leicht, daß mit einem Winkel auch der halbe Winkel konstruierbar ist. Es genügt also zu zeigen, daß mit  $r \in \mathbb{R} \cap K$  auch seine positive

Quadratwurzel  $\sqrt{r}$  in  $K$  liegt. Wir nehmen ohne Einschränkung an, daß  $r/2 > 1$ , und betrachten folgende Konstruktion:



Nach dem Satz von Pythagoras ist  $x^2 - 1 = (r/2)^2 - (r/2 - 1)^2$ , also  $x^2 = 1 - r - 1 = r$ , also  $x = \sqrt{r}$ .

Also ist  $Q \subset K$ . Wir müssen noch  $K \subset Q$  zeigen. Dazu reicht es zu zeigen, daß  $Q$  "stabil ist unter elementaren Konstruktionen", in Formeln  $K(Q) = Q$ . Es ist  $Q = \overline{Q} = \{\bar{z} \in \mathbb{C} \mid z \in Q\}$ , denn auch der Körper  $\overline{Q}$  ist stabil unter dem Bilden von Quadratwurzeln. Also ist  $z = x + iy$  (mit  $x, y \in \mathbb{R}$ ) in  $Q$  genau dann, wenn  $x, y \in Q$ . Nun werden die mit Zirkel und Lineal aus  $Q$  konstruierbaren Figuren durch Gleichungen  $(x - a)^2 + (y - b)^2 = c$  bzw.  $ax + by = c$  mit  $a, b, c \in \mathbb{R} \cap Q$  beschrieben. Simultane Lösungen zweier verschiedener Gleichungen lassen sich schreiben als Linearkombinationen von Elementen aus  $Q$  oder Quadratwurzeln aus  $Q$ , liegen also wieder in  $Q$ .  $\square$

**Korollar 3.22.** *Jede konstruierbare Zahl ist algebraisch und ihr Grad über  $\mathbb{Q}$  ist eine Zweierpotenz.*

*Beweis.* Sei  $z \in K$ . Dann entsteht  $z$  nach endlich vielen geometrischen Konstruktionen. Es gibt also eine Kette von quadratischen Erweiterungen  $\mathbb{Q} \subset K_1 \subset K_2 \subset \dots \subset K_r$  mit  $z \in K_r$ . Es ist  $[K_r : \mathbb{Q}] = 2^r$ , also ist  $z$  algebraisch und der Grad von  $z$  ist Teiler von  $2^r$ , also eine Zweierpotenz.  $\square$

**Korollar 3.23.** (1) *Delisches Problem: "Nicht jeder konstruierbare Würfel läßt sich verdoppeln", genauer: die dritten Wurzeln von 2 sind nicht konstruierbar.*

(2) *"Nicht jeder konstruierbare Winkel läßt sich in drei Teile teilen", genauer:  $e^{2\pi i/3}$  ist konstruierbar, aber  $e^{2\pi i/9}$  nicht.*

(3) *Das regelmäßige Siebeneck läßt sich nicht konstruieren.*

*Beweis.* Ad (1): Eine dritte Wurzel aus 2 hat den Grad 3 über  $\mathbb{Q}$ , ist also nicht konstruierbar.

Ad (2): Die Einheitswurzel  $\zeta = e^{2\pi i/9}$  ist Nullstelle des Polynoms  $X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$ , also Nullstelle des Polynoms  $X^6 + X^3 + 1$ . Dieses Polynom ist aber irreduzibel, denn substituieren wir  $X = Y + 1$ , so ist  $(Y + 1)^6 + (Y + 1)^3 + 1$  irreduzibel nach dem Eisensteinkriterium, denn in  $\mathbb{F}_3[X]$  ist  $X^9 - 1 = (X - 1)^9$  und  $(X^3 - 1) = (X - 1)^3$ , also  $X^6 + X^3 + 1 = (X - 1)^6 = Y^6$ . Also ist  $X^6 + X^3 + 1$  das Minimalpolynom von  $\zeta$ ,  $\zeta$  hat also den Grad 6 und ist folglich nicht konstruierbar.

Ad (3): Das regelmäßige Siebeneck ist konstruierbar genau dann, wenn die Einheitswurzel  $\zeta = e^{2\pi i/7}$  konstruierbar ist.  $\zeta$  ist Nullstelle des Kreisteilungspolynoms  $\Phi_7 = X^6 + X^5 + \dots + 1$ . Nach Lemma 2.56 ist  $\Phi_7$  irreduzibel. Also ist  $\Phi_7$  das Minimalpolynom von  $\zeta$ , also ist der Grad von  $\zeta$  über  $\mathbb{Q}$  gleich 6,  $\zeta$  damit nicht konstruierbar.  $\square$

### 3.4. Die Quadratur des Kreises.

**Satz 3.24** (Ferdinand von Lindemann, auf dem Freiburger Schloßberg, 1882).  $\pi$  ist *transzendent*.

Den Beweis geben wir in Kapitel 5.

**Korollar 3.25.** *Ein Kreis läßt sich nicht quadrieren. Genauer: Es gibt keine Konstruktion mit Zirkel und Lineal, die zu einem gegebenen Kreis ein flächengleiches Quadrat liefern würde.*

*Beweis.* Dazu müßte man ein Quadrat der Seitenlänge  $\sqrt{\pi}$  konstruieren können. Wäre  $\sqrt{\pi}$  konstruierbar, so wäre auch  $\pi$  konstruierbar, also algebraisch, was dem Satz von Lindemann widerspräche.  $\square$

**3.5. Einschub: Endliche Untergruppen der Drehgruppe.** Sei  $SO(3) \subset GL(\mathbb{R}^3)$  die Drehgruppe des euklidischen Raumes  $\mathbb{R}^3$ . Ist  $A \subset \mathbb{R}^3$  eine Teilmenge, so nennen wir  $g \in SO(3)$  eine *Symmetrie von A*, falls  $g.A = A$  gilt.

**Satz 3.26.** *Jede endliche Untergruppe der Drehgruppe  $SO(3)$  ist genau eine der folgenden Gruppen:*

- (1) *Eine zyklische Gruppe der Ordnung  $n \geq 1$ , bestehend aus allen Drehungen um eine feste Achse um den Winkel  $2\pi k/n$ .*
- (2) *Die Symmetriegruppe eines ebenen gleichseitigen  $n$ -Ecks für  $n > 2$  oder die Gruppe aller Elemente, die zwei orthogonale Geraden durch den Nullpunkt jeweils in sich überführen (Fall  $n = 2$ ). Dies sind die Diedergruppen der Ordnung  $2n$ .*
- (3) *Die Tetraedegruppe aller Symmetrien eines Tetraeders (12 Elemente).*
- (4) *Die Würfelgruppe aller Symmetrien eines Würfels (24 Elemente).*
- (5) *Die Ikosaedergruppe (20 Flächen) aller Symmetrien eines Ikosaeders (60 Elemente).*

*Beweis.* (unvollständig)

Sei  $G \subset SO(3)$  unsere Gruppe. Jedem  $g \in G$ ,  $g \neq e$  ordnen wir die beiden Schnittpunkte der Einheitssphäre mit der Drehachse von  $g$  zu und nennen diese Pole. Sei  $P$  die Menge der Pole und  $M = \{(g, p) \mid g \in G, g \neq e, p \text{ Pol von } g\}$ . So ist  $|M| = 2(|G| - 1)$ .

Die Gruppe  $G$  operiert auf  $P$  ( $p$  Pol von  $g$ , so  $hp$  Pol von  $hgh^{-1}$ ). Für  $p \in P$  sei  $G_p$  sein Stabilisator. Dann besteht  $G_p$  aus  $e$  und der Menge aller  $g \in G$  mit Pol  $p$ . Wir erhalten  $|M| = \sum_{p \in P} (|G_p| - 1)$ . Also erhalten wir

$$2(|G| - 1) = \sum_{p \in P} (|G_p| - 1).$$

Seien  $P_1, \dots, P_r$  die Bahnen von  $G$  auf  $P$ , und  $n_i = |G|/|P_i| = |G_p|$ , falls  $p \in P_i$ . Somit  $\sum_{p \in P} (|G_p| - 1) = \sum_{i=1}^r |P_i|(n_i - 1) = \sum_{i=1}^r |G|/n_i(n_i - 1)$  und mit obiger Gleichung erhalten wir

$$2 \left( 1 - \frac{1}{|G|} \right) = \sum_{i=1}^r \left( 1 - \frac{1}{n_i} \right)$$

Jeder Summand der rechten Seite ist mindestens  $1/2$ , deshalb ist  $r \leq 3$ .

Ist  $r = 0$  so ist  $G = \{e\}$ .

Ist  $r = 1$ , so  $|G| \geq 2$ , also  $2 \left( 1 - \frac{1}{|G|} \right) \geq 1 > 1 - \frac{1}{n_1}$ , was der hergeleiteten Identität widerspricht.

Ist  $r = 2$ , so  $2/|G| = 1/n_1 + 1/n_2$ , also  $n_1 = n_2 = |G|$ . Also werden alle Pole von jedem Gruppenelement festgehalten. Es gibt also genau zwei Pole und unsere Gruppe ist zyklisch.

Ist  $r = 3$ , so

$$\frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} - 1.$$

ObdA  $n_1 \leq n_2 \leq n_3$ . So  $n_1 = 2$ . Ist  $n_2 = 2$ , so  $2n_3 = |G|$ , also  $|P_3| = 2$  und die Elemente aus  $P_3$  liegen sich notwendigerweise gegenüber (sonst könnte ein Element mit Drehachse durch einen Punkt von  $P_3$  den Orbit  $P_3$  nicht erhalten). Jedes Element  $g \in G \setminus G_3$  muß die beiden Elemente in  $P_3$  vertauschen. Jede Drehachse ist also entweder die Achse durch die beiden Punkte aus  $P_3$ , oder orthogonal zu dieser. Dann ist  $G$  die Diedergruppe (Ecken des  $n$ -Ecks = Schnittpunkte aller orthogonalen Achsen mit Einheitskugel).

$n_2 \geq 4$  ist nicht möglich, denn  $\frac{1}{2} + \frac{1}{n_2} + \frac{1}{n_3} > 1$  ergibt  $n_3 < 4$ .

Ist  $n_2 = 3$ , so gibt es die Möglichkeiten  $n_3 = 3, 4, 5$  mit  $|G| = 12, 24, 60$ . Dies ergibt die Symmetriegruppen des Tetraeders, des Würfels, und des Ikosaeders.

Hinweise: Drehachsen beim Würfel: Durch Ecken, Kantenmitten und Seitenmitten gibt Polorbite der Ordnung 8, 12, 6.

Drehachsen beim Tetraeder: Durch Ecken und Seitenmitten (und gegenüberliegende Seitenmitte). 1. Bahn: 4 Ecken. 2. Bahn: Antipoden der 4 Ecken, 3. Bahn: 6 Schnittpunkte der restlichen Drehachsen.  $\square$

**3.6. Endliche Körper.** Ein Körper mit endlich vielen Elementen heißt *endlicher Körper*. In diesem Abschnitt wollen wir die endlichen Körper klassifizieren.

**Satz 3.27.** *Ist  $K$  ein endlicher Körper mit  $m$  Elementen, so ist  $m$  eine Primzahlpotenz, also  $m = p^n$  für eine Primzahl  $p$  und ein  $n \geq 1$ . Zu jeder Primzahlpotenz  $p^n$  gibt es bis auf Isomorphie genau einen Körper mit  $p^n$  Elementen. Wir bezeichnen diesen mit  $\mathbb{F}_{p^n}$ .*

Zum Beweis benötigen wir einige Hilfssätze.

**Lemma 3.28.** *Sei  $K$  ein Körper und  $P \in K[X]$  ein nicht konstantes Polynom. So gibt es eine Körpererweiterung  $K \subset L$ , so daß  $P$  in  $L$  eine Nullstelle besitzt.*

*Beweis.* Es reicht, das Lemma für  $P$  irreduzibel zu beweisen. Sei  $T$  eine weitere Variable. Wir fassen  $P$  als Element des Polynomring  $K[T]$  auf und wählen  $L := K[T]/(P)$  mit der natürlichen Inklusion von  $K$ . Da  $P$  irreduzibel ist, ist  $L$  ein Körper. Nun betrachten wir  $P$  wieder als Polynom in  $K[X] \subset L[X]$ . Sei  $\bar{T} \in L$  das Bild von

$T \in K[T]$  unter der Projektion  $K[T] \rightarrow K[T]/(P)$ . So ist  $\bar{T} \in L$  eine Nullstelle von  $P$ , denn es gilt  $P(\bar{T}) = \overline{P(T)} = 0$  in  $L$ .  $\square$

**Proposition 3.29.** *Sei  $K$  ein Körper und  $P \in K[X]$  ein nicht-konstantes Polynom. Dann gibt es eine Körpererweiterung  $K \subset L$ , so daß  $P$  über  $L$  in Linearfaktoren zerfällt.*

*Beweis.* Wir müssen das Lemma nur mehrmals anwenden.  $\square$

**Lemma 3.30.** *Sei  $q = p^n$  eine Primzahlpotenz und  $L$  ein Körper der Charakteristik  $p$ , indem das Polynom  $X^q - X$  vollständig in Linearfaktoren zerfällt. Dann bilden die Nullstellen dieses Polynoms einen Unterkörper von  $L$  der Kardinalität  $q$ .*

*Beweis.* Da  $p$  die Charakteristik von  $L$  ist, ist die Abbildung  $\text{Fr}: L \rightarrow L, \text{Fr}(a) = a^p$  ein Körperhomomorphismus. Also ist auch  $\text{Fr}^n: L \rightarrow L, a \rightarrow a^q$  ein Körperhomomorphismus. Die Nullstellen des Polynoms  $X^q - X$  in  $L$  sind genau die Fixpunkte von  $\text{Fr}^n$  und bilden deshalb einen Unterkörper. Ist  $a$  eine solche Nullstelle, so gilt

$$(X - a)((X - a)^{q-1} - 1) = (X - a)^q - (X - a) = X^q - a^q - X + a = X^q - X$$

und somit ist  $a$  nur eine einfache Nullstelle von  $X^q - X$ . Also gibt es genau  $q$  Nullstellen von  $X^q - X$  in  $L$ .  $\square$

Wir benötigen noch ein weiteres Resultat, bevor wir Satz 3.27 beweisen können. Ist  $K$  ein Körper, so ist  $K^\times = K \setminus \{0\}$  eine multiplikative Gruppe.

**Satz 3.31.** *Eine endliche Untergruppe der multiplikativen Gruppe eines Körpers  $K$  ist zyklisch.*

*Beweis.* Sei  $G \subset K^\times$  eine endliche Untergruppe und

$$M := \{n \in \mathbb{N} \mid \text{es gibt ein } g \in G \text{ mit } \text{ord } g = n\}.$$

Dann enthält  $M$  mit jedem  $n$  auch alle Teiler von  $n$ . Sind  $m, n \in M$  teilerfremd, so folgt  $m \cdot n \in M$ . Sei nun  $n \in M$  maximal. Dann ist jedes Element aus  $M$  also Teiler von  $n$ . Insbesondere ist jedes  $g \in G$  Nullstelle des Polynoms  $X^n - 1$ . Dieses Polynom hat aber höchstens  $n$  Nullstellen, also ist  $|G| \leq n$ . Da es aber ein Element der Ordnung  $n$  in  $G$  gibt, ist  $|G| = n$ , folglich ist  $G$  zyklisch.  $\square$

*Beweis von Satz 3.27.* Sei  $\mathbb{F}$  ein endlicher Körper. So ist  $\text{char } \mathbb{F} = p > 0$  eine Primzahl.  $\mathbb{F}$  ist damit ein Vektorraum über  $\mathbb{F}_p$  von endlicher Dimension  $n$ , hat also  $q = p^n$  Elemente. Somit ist die Kardinalität jedes endlichen Körpers eine Primzahlpotenz.

Die multiplikative Gruppe  $\mathbb{F}^\times$  hat Ordnung  $q - 1$  und nach Satz 3.31 ist sie zyklisch, also ist jedes Element von  $\mathbb{F}^\times$  Nullstelle des Polynoms  $X^{q-1} - 1$ . Somit ist jedes Element von  $\mathbb{F}$  Nullstelle von  $X^q - X$ . Da dieses Polynom höchstens  $q$  Nullstellen hat, zerfällt es also vollständig über  $\mathbb{F}$ . Außerdem ist  $\mathbb{F}_p \subset \mathbb{F}$  primitiv (da  $\mathbb{F}^\times$  sogar zyklisch ist). Also ist das Minimalpolynom eines Erzeugers  $a \in \mathbb{F}$  ein irreduzibler Faktor von  $X^q - X$  vom Grad  $n$ . Umgekehrt ist eine Nullstelle in  $\mathbb{F}$  eines irreduziblen Faktors vom Grad  $n$  von  $X^q - X$  ein Erzeuger von  $\mathbb{F}$  über  $\mathbb{F}_p$  (da sie ja eine Körpererweiterung vom Grad  $n$  erzeugt). Somit ist

$$\mathbb{F} \cong \mathbb{F}_p[X]/(P)$$

für *jeden* irreduziblen Faktor vom Grad  $n$  von  $X^q - X$ . Also sind je zwei Körper der Kardinalität  $p^n$  isomorph.

Wir müssen nur noch zeigen, daß es zu jeder Primzahlpotenz  $q = p^n$  tatsächlich einen Körper mit  $q$  Elementen gibt. Nach Proposition 3.29 gibt es eine Körpererweiterung  $\mathbb{F}_p \subset L$ , in der  $X^q - X$  vollständig in Linearfaktoren zerfällt. Nach Lemma 3.30 bilden die Nullstellen dieses Polynoms in  $L$  einen Körper der Kardinalität  $q$ .  $\square$

**Satz 3.32.** *Sind  $\mathbb{F}$  und  $\mathbb{F}'$  endliche Körper, so gibt es eine Einbettung  $\mathbb{F} \hookrightarrow \mathbb{F}'$  genau dann, wenn  $|\mathbb{F}'|$  eine Potenz von  $|\mathbb{F}|$  ist.*

*Beweis.* Daß die Bedingung notwendig ist, sieht man daran, daß  $\mathbb{F}'$  unter einer Einbettung  $\mathbb{F} \hookrightarrow \mathbb{F}'$  ein  $\mathbb{F}$ -Vektorraum wird. Ist umgekehrt  $\mathbb{F} \cong \mathbb{F}_{p^n}$  und  $\mathbb{F}' = \mathbb{F}_{p^m}$  mit  $n|m$ , so betrachten wir auf  $\mathbb{F}'$  die Frobeniusabbildung  $\text{Fr}: \mathbb{F}' \rightarrow \mathbb{F}'$ ,  $x \mapsto x^p$ . Dann ist die Fixpunktmenge von  $\text{Fr}^n$  ein Unterkörper von  $\mathbb{F}'$ . Wir behaupten, daß er  $p^n$  Elemente enthält. Jedes Element in  $\mathbb{F}'$  ist Nullstelle des Polynoms  $X^{p^m} - X$ . Das Polynom  $X^{p^n} - X$  ist aber ein Teiler von  $X^{p^m} - X$ : Denn  $q - 1$  teilt  $q^r - 1$  für jedes  $r$  und  $X^{q-1} - 1$  teilt  $X^{q^r-1} - 1$  für jedes  $r$ , also teilt  $X^q - X$  das Polynom  $X^{q^r} - X$  für alle  $q, r$ . Damit teilt  $X^{p^n} - X$  das Polynom  $X^{p^m} - X$ , also zerfällt  $X^{p^n} - X$  über  $\mathbb{F}'$  vollständig in Linearfaktoren. Außerdem hat  $X^{p^n} - X$  keine mehrfache Nullstelle, da  $X^{p^n} - X = (X - a)((X - a)^{p^n-1} - 1)$  (wie oben). Damit hat  $X^{p^n} - X$  genau  $p^n$  verschiedene Nullstellen, die einen Unterkörper mit  $p^n$  Elementen bilden. Also gibt es eine Inklusion  $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^m}$  für  $n|m$ .  $\square$

**3.7. Zerfällungskörper.** Ist  $K \subset L$  eine Körpererweiterung und  $P \in K[X]$ , so können wir  $P$  auch als Element in  $L[X]$  auffassen und uns fragen, wann  $P$  über  $L$  (also in  $L[X]$ ) vollständig in Linearfaktoren zerfällt.

**Definition 3.33.** Sei  $K$  ein Körper und  $P \in K[X]$  ein Polynom. Eine Körpererweiterung  $K \subset L$  heißt *Zerfällungskörper* von  $P$  über  $K$ , falls  $P$  in  $L[X]$  in Linearfaktoren zerfällt und  $L$  über  $K$  erzeugt wird von den Nullstellen von  $P$ .

*Beispiele 3.34.* (1)  $\mathbb{R} \subset \mathbb{C}$  ist der Zerfällungskörper von  $X^2 + 1$ .

(2)  $\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/n})$  ein Zerfällungskörper von  $X^n - 1$ .

(3)  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$  ist kein Zerfällungskörper.

Für jedes Polynom  $P \in K[X]$  gibt es einen Zerfällungskörper, denn nach Satz 3.29 gibt es eine Körpererweiterung, in der das Polynom  $P$  zerfällt und wir können also den von den Nullstellen von  $P$  erzeugten Unterkörper wählen. Wir zeigen nun, in welchem Sinne ein Zerfällungskörper  $K \subset L$  die *kleinste* Körpererweiterung ist, in der  $P$  vollständig in Linearfaktoren zerfällt.

**Satz 3.35.** *Ist  $K \subset L$  der Zerfällungskörper von  $P \in K[X]$  über  $K$ , und  $K \subset L'$  eine Körpererweiterung mit der Eigenschaft, daß  $P$  über  $L'$  vollständig in Linearfaktoren zerfällt, so gibt es ein  $\phi: L \rightarrow L'$ , so daß das Diagramm*

$$\begin{array}{ccc} L & \xrightarrow{\phi} & L' \\ & \swarrow \subset & \nearrow \subset \\ & K & \end{array}$$

*kommutiert.*

Insbesondere sind je zwei Zerfällungskörper von  $P$  isomorph:

**Satz 3.36.** Sind  $K \subset L$  und  $K \subset L'$  zwei Zerfällungskörper des Polynoms  $P \in K[X]$ , so gibt es einen Isomorphismus  $\phi: L \xrightarrow{\sim} L'$  mit  $\phi|_K = \text{id}_K$ .

Um die Sätze zu beweisen brauchen wir einige Aussagen darüber, wann sich eine Inklusion  $K \subset L'$  zu einer Inklusion  $L \subset L'$  ausdehnen läßt. Genauer gesagt suchen wir also einen Homomorphismus  $\phi: L \rightarrow L'$  mit  $\phi(a) = a$  für alle  $a \in K$  (Erinnerung: Alle Homomorphismen zwischen Körpern sind injektiv!). Diagrammatisch ausgedrückt suchen wir ein  $\phi: L \rightarrow L'$ , so daß

$$\begin{array}{ccc} L & \xrightarrow{\phi} & L' \\ & \swarrow \subset & \nearrow \subset \\ & K & \end{array}$$

kommutiert. Wir nennen ein solches  $\phi$  im folgenden kurz eine *Ausdehnung* von  $K \subset L'$  oder noch kürzer eine *Ausdehnung*.

Ist nun  $L = K(a)$  eine primitive algebraische Körpererweiterung,  $P \in K[X]$  das Minimalpolynom von  $a$  über  $K$  und  $\phi: K(a) \rightarrow L'$  eine Ausdehnung von  $K \subset L'$ , so gilt  $0 = \phi(P(a)) = P(\phi(a)) = 0$  in  $L'$ . Somit können wir jeder Ausdehnung  $\phi$  eine Nullstelle des Polynoms  $P$  in  $L'$  zuordnen.

**Lemma 3.37.** Die obige Abbildung liefert eine Bijektion

$$\left\{ \begin{array}{l} \text{Ausdehnungen} \\ \phi: K(a) \rightarrow L' \text{ von } K \subset L' \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{l} \text{Nullstellen in } L' \text{ des Minimal-} \\ \text{polynoms } P \text{ von } a \end{array} \right\}$$

$$\phi \mapsto \phi(a).$$

Es gibt also höchstens  $\deg P = [K(a) : K]$  mögliche Ausdehnungen.

*Beweis.* Die Abbildung ist injektiv, da eine Ausdehnung  $\phi: K(a) \rightarrow L'$  durch das Bild von  $a$  eindeutig bestimmt ist. Ist umgekehrt  $b \in L'$  eine Nullstelle von  $P$ , so können wir zunächst die Auswertung an  $b$ , also den Homomorphismus  $\phi': K[X] \rightarrow L'$ ,  $Q \mapsto Q(b)$ , definieren. Dann ist  $\phi'(P) = 0$  und wir erhalten einen Homomorphismus  $K[X]/(P) \rightarrow L'$  von Körpern. Nach Satz 3.13 gibt es einen Isomorphismus  $K(a) \cong K[X]/(P)$ , der auf  $K$  die Identität ist, und die Verkettung mit  $\phi'$  liefert uns eine Ausdehnung  $\phi$ . Also ist obige Abbildung auch surjektiv.  $\square$

*Anmerkung 3.38.* Seien  $K \subset L$  und  $K \subset M$  Körpererweiterungen. Per Induktion zeigt man, daß es höchstens  $[L : K]$  verschiedene Ausdehnungen  $\phi: L \rightarrow M$  von  $K \subset M$  geben kann (vgl. Lemma 4.5).

**Proposition 3.39.** Sei  $K \subset K(a_1, \dots, a_n)$  eine algebraische Körpererweiterung und  $K \subset L'$  eine Körpererweiterung mit der Eigenschaft, daß die Minimalpolynome der  $a_i$  über  $L'$  vollständig in Linearfaktoren zerfallen. Dann gibt es eine Ausdehnung  $\phi: K(a_1, \dots, a_n) \rightarrow L'$  von  $K \subset L'$ .

*Beweis.* Wir wenden obiges Lemma mehrmals an (und wählen in jedem Schritt passende Nullstellen).  $\square$

*Beweis von Satz 3.35.* Sind  $a_1, \dots, a_n$  die Nullstellen von  $P$  in  $L$ , so ist also  $L = K(a_1, \dots, a_n)$ . Es gibt also, nach Proposition 3.39, eine Ausdehnung  $L \rightarrow L'$ .  $\square$

*Beweis von Satz 3.36.* Nach Satz 3.35 gibt es Ausdehnungen  $\phi: L \rightarrow L'$  und  $\phi': L' \rightarrow L$ . Nun ist die Verkettung  $\phi' \circ \phi: L \rightarrow L$  linear über  $K$  und injektiv.  $L$  ist aber über  $K$  ein endlich dimensionaler  $K$  Vektorraum, also ist  $\phi' \circ \phi$  bijektiv. Da auch  $\phi'$  injektiv ist, muß  $\phi$  schon bijektiv sein, also ein Isomorphismus.  $\square$

**Lemma 3.40.** *Sei  $K \subset L$  der Zerfällungskörper von  $P \in K[X]$  und  $K \subset M$  eine beliebige Körpererweiterung. Dann ist das Bild einer Ausdehnung  $\phi: L \rightarrow M$  von  $K \subset M$  unabhängig von  $\phi$ .*

*Beweis.* Sei  $\phi: L \rightarrow M$  eine Ausdehnung. Dann wird  $\phi(L)$  erzeugt über  $K$  von den Nullstellen des Polynoms  $P$  in  $M$ .  $\square$

### 3.8. Normale Körpererweiterungen.

**Definition 3.41.** Eine Körpererweiterung  $K \subset L$  heißt *normal*, falls sie algebraisch ist und jedes über  $K$  irreduzible Polynom, das in  $L$  eine Nullstelle hat, über  $L$  schon vollständig in Linearfaktoren zerfällt.

*Beispiel 3.42.* Die Erweiterung  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$  ist nicht normal, denn  $P(X) = X^3 - 2$  hat zwar eine Nullstelle in  $\mathbb{Q}(\sqrt[3]{2})$ , zerfällt in  $\mathbb{Q}(\sqrt[3]{2})[X]$  aber nicht in Linearfaktoren.

**Satz 3.43.** *Sei  $K \subset L$  eine endliche Körpererweiterung. Dann ist  $K \subset L$  genau dann normal, wenn  $L$  der Zerfällungskörper eines Polynoms über  $K$  ist.*

*Beweis.* Ist  $K \subset L$  normal und endlich, so ist  $L = K(a_1, \dots, a_n)$  für gewisse algebraische Elemente  $a_1, \dots, a_n \in L$ . Sei  $P$  das Produkt der Minimalpolynome der  $a_i$  über  $K$ . Dann zerfällt  $P$  über  $L$  in Linearfaktoren, somit ist  $L$  der Zerfällungskörper von  $P$  über  $K$ .

Sei nun  $L$  der Zerfällungskörper des Polynoms  $P$  über  $K$ . Sei  $Q \in K[X]$  irreduzibel mit einer Nullstelle  $a \in L$ . Wir müssen zeigen, daß  $Q$  über  $L$  vollständig in Linearfaktoren zerfällt. Sei  $L \subset M$  eine Körpererweiterung, in der  $Q$  vollständig in Linearfaktoren zerfällt. Ist nun  $b \in M$  eine Nullstelle von  $Q$ , so gibt es nach Lemma 3.37 eine Ausdehnung  $K(a) \rightarrow M$  mit  $a \mapsto b$ . Da  $L$  in  $M$  enthalten ist, zerfällt  $P$  auch in  $M$  vollständig. Nach Satz 3.35 können wir also  $K(a) \rightarrow M$  weiter ausdehnen und erhalten eine Ausdehnung  $\phi: L \rightarrow M$  von  $K \subset M$  mit  $b \in \phi(L)$  (Bemerkung:  $L$  ist natürlich auch der Zerfällungskörper von  $P$  über  $K(a)$ ). Aber auch unsere Inklusion  $L \subset M$  mit der wir gestartet sind, ist eine Ausdehnung von  $K \subset M$ , also gilt  $\phi(L) = L$  nach Lemma 3.40. Insbesondere liegt unsere Nullstelle  $b$  schon in  $L$ . Also zerfällt  $Q$  schon über  $L$  und  $K \subset L$  ist normal.  $\square$

Sei  $K \subset L$  eine endliche Erweiterung. Im folgenden Satz wollen wir zeigen, daß es eine *kleinste* Erweiterung  $L \subset N$  gibt, so daß  $K \subset N$  normal ist.

**Satz 3.44.** *Sei  $K \subset L$  eine endliche Körpererweiterung. Dann gibt es eine Körpererweiterung  $L \subset N$ , so daß  $K \subset N$  normal ist und die die Eigenschaft hat, daß es für jede Erweiterung  $L \subset N'$ , so daß  $K \subset N'$  normal ist, einen Homomorphismus  $\phi: N \rightarrow N'$  mit  $\phi|_L = \text{id}_L$  gibt.*

*Beweis.* Seien  $a_1, \dots, a_n \in L$  Erzeuger von  $L$  über  $K$ . Sei  $P \in K[X]$  das Produkt der Minimalpolynome der  $a_i$ . Der Zerfällungskörper  $N$  von  $P$  über  $L$  ist normal über  $K$ . Ist  $L \subset N'$  eine weitere Erweiterung, so daß  $K \subset N'$  normal ist, so zerfällt  $P$

über  $N'$  in Linearfaktoren, denn wegen  $L \subset N'$  hat jeder irreduzible Faktor von  $P$  eine Nullstelle in  $N'$ . Nach Satz 3.35 gibt es also eine Ausdehnung  $\phi: N \rightarrow N'$  von  $L \subset N$ .  $\square$

**3.9. Separable Körpererweiterungen.** Sei  $K$  ein Körper.

**Definition 3.45.** (1) Ein Polynom  $P \in K[X]$  heißt *separabel*, falls es in seinem Zerfällungskörper  $K \subset L$  nur einfache Nullstellen hat.

(2) Sei  $K \subset L$  eine Körpererweiterung. Dann heißt  $a \in L$  *separabel über  $K$* , falls  $a$  algebraisch ist über  $K$  und sein Minimalpolynom separabel ist.

(3) Die Körpererweiterung  $K \subset L$  heißt *separabel*, wenn jedes Element aus  $L$  separabel ist über  $K$ .

*Anmerkung 3.46.* Sei  $P \in K[X]$  und  $K \subset L$  sein Zerfällungskörper. Dann hat  $P$  in  $L$  nur einfache Nullstellen, wenn es in jeder Körpererweiterung  $K \subset M$  höchstens einfache Nullstellen hat. Zum Beweis bilden wir den Zerfällungskörper  $M \subset L'$  von  $P$  über  $M$  und wenden Satz 3.35 an. Wir erhalten ein  $\phi: L \rightarrow L'$ . Die Nullstellen von  $P$  in  $L'$  sind dann genau die Bilder der Nullstellen von  $P$  in  $L$  unter  $\phi$ , also sind alle verschieden.

*Beispiel 3.47.*  $\mathbb{F}_p(T^p) \subset \mathbb{F}_p(T)$  ist nicht separabel, denn das Minimalpolynom von  $T$  über  $\mathbb{F}_p(T^p)$  ist  $X^p - T^p = (X - T)^p$ , hat also mehrfache Nullstellen.

*Übung 3.48.*  $\mathbb{F}_p \subset \mathbb{F}_{p^n}$  ist separabel.

**Proposition 3.49.** Sei  $P \in K[X]$  ein irreduzibles Polynom.

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

(2) Ist  $\text{char } K = p$ , so ist  $P$  separabel genau dann, wenn  $P$  nicht von der Form  $P(X) = Q(X^p)$  für ein  $Q \in K[X]$  ist.

Zum Beweis benötigen wir einige Aussagen über die *formale Ableitung*  $P' \in K[X]$  eines Polynoms  $P \in K[X]$ , die wie folgt definiert wird: Ist

$$P(X) = a_0 + a_1X + \cdots + a_nX^n,$$

so definieren wir

$$P'(X) := a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Man prüft leicht nach, daß  $(P + Q)' = P' + Q'$  und  $(PQ)' = P'Q + PQ'$  gilt.

**Lemma 3.50.** Ein Polynom  $P \in K[X]$  ist genau dann separabel, wenn  $P$  und  $P'$  in  $K[X]$  teilerfremd sind.

Aus dem Lemma folgt: Ein irreduzibles Polynom  $P'$  ist genau dann separabel, wenn seine Ableitung nicht Null ist.

*Bemerkung 3.51.* Zwei Polynome  $P, Q \in K[X]$  sind *teilerfremd*, wenn jeder gemeinsame Teiler eine Einheit ist.

*Beweis.* Sei  $K \subset L$  der Zerfällungskörper von  $P$ . Wir behaupten, daß  $P$  und  $P'$  teilerfremd sind in  $K[X]$  genau dann, wenn  $P$  und  $P'$  teilerfremd sind in  $L[X]$ . Sind nämlich  $P$  und  $P'$  teilerfremd in  $L[X]$ , so sicherlich auch in  $K[X]$ . Sind  $P$  und  $P'$  teilerfremd in  $K[X]$ , so gibt es  $Q, R \in K[X]$  mit  $PQ + P'R = 1$  (denn das von  $P$  und  $P'$  erzeugte Ideal in  $K[X]$  ist ein Hauptideal und wird erzeugt von einem

gemeinsamen Teiler von  $P$  und  $P'$ , ist also gleich  $K[X]$ ). Diese Gleichung gilt auch in  $L[X]$ , jeder gemeinsame Teiler von  $P$  und  $P'$  ist also auch Teiler von 1, damit eine Einheit. Also sind  $P$  und  $P'$  teilerfremd in  $L[X]$ .

Hat  $P$  in  $L$  die mehrfache Nullstelle  $a$ , so ist  $P = (X - a)^2 Q$  für ein  $Q \in L[X]$ , und  $P' = 2(X - a)Q + (X - a)^2 Q'$ . Damit ist  $X - a$  Teiler von  $P$  und  $P'$ , also sind  $P$  und  $P'$  nicht teilerfremd.

Sind  $P$  und  $P'$  nicht teilerfremd in  $K[X]$ , so auch nicht in  $L[X]$ . Dann gibt es also ein  $a \in L$ , so daß  $X - a$  sowohl  $P$  als auch  $P'$  teilt. Somit ist  $P(X) = (X - a)Q$  für ein  $Q \in L[X]$ , also  $P'(X) = Q + (X - a)Q'$ , und aus  $P'(a) = 0$  folgt  $Q(a) = 0$ . Dann hat  $P$  aber eine doppelte Nullstelle  $a$ .  $\square$

*Beweis der Proposition 3.49.* Ist  $P$  nicht separabel, so sind nach obigem Lemma  $P$  und  $P'$  nicht teilerfremd. Ist  $P$  zusätzlich irreduzibel, so muß  $P' = 0$  folgen. Ist  $\text{char } K = 0$ , so muß  $P$  ein konstantes Polynom sein und das steht im Widerspruch zur Irreduzibilität. Ist  $\text{char } K = p$  und  $P(X) = a_0 + a_1X + \cdots + a_nX^n$ , so muß aus  $a_i \neq 0$  folgen, daß  $p|i$ . Also gibt es  $Q \in K[X]$  mit  $P(X) = Q(X^p)$ .  $\square$

**Definition 3.52.** Ein Körper  $K$  heißt *perfekt*, falls entweder seine Charakteristik Null ist oder  $\text{char } K = p > 0$  und es für jedes  $x \in K$  eine  $p$ -te Wurzel (also ein  $y$  mit  $y^p = x$ ) gibt.

**Satz 3.53.** *Ist  $K$  perfekt, so ist jede algebraische Körpererweiterung separabel.*

*Beweis.* In Charakteristik Null ist jedes irreduzible Polynom separabel, also ist auch jede Körpererweiterung separabel. Sei nun  $\text{char } K = p > 0$ ,  $K \subset L$  eine Körpererweiterung und  $a \in L$  ein Element mit nicht separablem Minimalpolynom  $P \in K[X]$ . So ist  $P$  von der Form  $P(X) = b_0 + b_1X^p + \cdots + b_nX^{np}$ . Wählen wir  $p$ -te Wurzeln  $a_i$  der  $b_i$ , so ist also  $P(X) = a_0^p + (a_1X)^p + \cdots + (a_nX^n)^p = (a_0 + a_1X + \cdots + a_nX^n)^p$ , also nicht irreduzibel. Das ist ein Widerspruch. Also gibt es kein  $a \in L$  mit nicht separablem Minimalpolynom, also ist  $K \subset L$  separabel.  $\square$

**Satz 3.54.** *Für eine Körpererweiterung  $K \subset L$  sind äquivalent:*

- (1)  $K \subset L$  ist separabel.
- (2)  $L$  wird über  $K$  von separablen Elementen erzeugt.

*Ist  $K \subset L$  endlich, so sind zusätzlich äquivalent:*

- (3) Für jede Körpererweiterung  $L \subset N$ , so daß  $K \subset N$  normal ist, gilt: Die Anzahl der Ausdehnungen  $\phi: L \rightarrow N$  von  $K \subset N$  ist  $[L: K]$ .
- (4) Es gibt eine Körpererweiterung  $K \subset N$  für die gilt: Die Anzahl der Ausdehnungen  $\phi: L \rightarrow N$  von  $K \subset N$  ist  $[L: K]$ .

*Bemerkung 3.55.* In (3) und (4) ist die Bedingung, daß  $N$  eine Erweiterung von  $L$  sei, etwas künstlich. Der Grund hierfür ist, daß wir ausschließen müssen, daß  $N$  zu klein ist, bspw. müssen wir  $N = K$  im allgemeinen ausnehmen. Die Bedingung  $L \subset N$  kann ersetzt werden durch die Bedingung: Es gibt *mindestens eine* Ausdehnung  $L \rightarrow N$  von  $K \subset N$ . Wissen wir zum Beispiel, daß die Minimalpolynome von Erzeugern von  $L$  in  $N$  zerfallen (oder auch nur eine Nullstelle haben), so ist unsere Bedingung erfüllt.

*Beweis.* Wir nehmen zunächst an,  $K \subset L$  sei eine endliche Erweiterung. Daß (2) aus (1) folgt, ist klar. Um zu zeigen, daß (3) aus (2) folgt, nehmen wir zunächst an, daß  $L = K(a)$ . Da  $a$  separabel ist über  $K$ , ist das Minimalpolynom von  $a$  über  $K$  separabel, hat also  $[K(a) : K]$  verschiedene Nullstellen in  $N$ . Nach Lemma 3.37 gibt es also genau  $[K(a) : K]$  verschiedene Ausdehnungen. Wir erhalten nun den allgemeinen Fall per Induktion. Dazu nehmen wir an, es gäbe  $[K(a_1, \dots, a_n) : K]$  verschiedene Ausdehnungen  $\phi: K(a_1, \dots, a_n) \rightarrow N$  von  $K \subset N$ . Nach dem eben Bewiesenen können wir jede dieser Ausdehnungen auf genau  $[K(a_1, \dots, a_{n+1}) : K(a_1, \dots, a_n)]$  verschiedene Weisen ausdehnen zu einem Homomorphismus  $K(a_1, \dots, a_{n+1}) \rightarrow N$ . Es gibt also genau  $[K(a_1, \dots, a_{n+1}) : K(a_1, \dots, a_n)] \cdot [K(a_1, \dots, a_n) : K] = [K(a_1, \dots, a_{n+1}) : K]$  verschiedene Ausdehnungen  $K(a_1, \dots, a_{n+1}) \rightarrow N$  von  $K \subset N$ . Damit folgt also (3) aus (2).

(4) ist ein Spezialfall von (3). (Man beachte Satz 3.44).

Wir zeigen nun, daß (1) aus (4) folgt. Ist  $K \subset L$  nicht separabel, so gibt es ein  $a \in L$  mit nicht separablem Minimalpolynom  $P$  über  $K$ . Dann gibt es höchstens  $[K(a) : K] - 1$  verschiedene Ausdehnungen  $\phi: K(a) \rightarrow N$  von  $K \subset N$ . Aber dann kann es höchstens  $[L : K] - 1$  verschiedene Ausdehnungen  $\phi: L \rightarrow N$  geben.

Schließlich müssen wir noch zeigen, daß (1) und (2) für nicht endliche Körpererweiterungen  $K \subset L$  äquivalent sind. Dies folgt aber daraus, daß (1) und (2) für jeden endlichen Zwischenkörper  $K \subset K(a_1, \dots, a_n) \subset L$  äquivalent sind.  $\square$

**Satz 3.56** (Satz vom primitiven Element). *Ist  $K \subset L$  eine endliche separable Körpererweiterung, so gibt es ein  $a \in L$  mit  $L = K(a)$ .*

*Beweis.* Sei  $L \subset N$  eine Erweiterung, so daß  $K \subset N$  normal ist (die gibt es nach Satz 3.44). Da  $K \subset L$  separabel ist, gibt es genau  $[L : K]$  Ausdehnungen  $L \rightarrow N$  von  $K \subset N$ . Für zwei Ausdehnungen  $\phi, \psi: L \rightarrow N$  ist die Menge  $\{x \in L \mid \phi(x) = \psi(x)\}$  ein Unterkörper von  $L$ , der  $K$  enthält, insbesondere also ein  $K$ -Untervektorraum von  $L$ .

Ist nun  $K$  endlich, so ist auch  $L$  endlich und nach 3.31 ist  $L^\times$  zyklisch und der Satz folgt. Ist  $K$  unendlich, so kann der  $K$ -Vektorraum  $L$  nicht durch endlich viele echte Untervektorräume überdeckt werden (Übung!). Es gibt also ein  $a \in L$  mit der Eigenschaft, daß aus  $\phi(a) = \psi(a)$  für Ausdehnungen  $\phi, \psi: L \rightarrow N$  schon  $\phi = \psi$  folgt. Restrangieren liefert eine Injektion

$$\left\{ \begin{array}{l} \text{Ausdehnungen } L \rightarrow N \\ \text{von } K \subset N \end{array} \right\} \hookrightarrow \left\{ \begin{array}{l} \text{Ausdehnungen } K(a) \rightarrow N \\ \text{von } K \subset N \end{array} \right\}$$

Da nun die Menge rechts höchstens  $[K(a) : K]$  Elemente, die Menge links aber  $[L : K]$  Elemente hat (und natürlich  $[K(a) : K] \leq [L : K]$  gilt), folgt  $[K(a) : K] = [L : K]$ , und somit  $L = K(a)$ .  $\square$

*Übung 3.57.* Sei  $K \subset M \subset L$  eine Körperkette.

- (1)  $K \subset L$  ist separabel genau dann, wenn  $K \subset M$  und  $M \subset L$  separabel sind.
- (2) Ist  $K \subset L$  normal, so ist  $M \subset L$  normal. Geben Sie ein Beispiel an für den Fall, daß  $K \subset L$  normal ist,  $K \subset M$  aber nicht.

Wir betrachten die Körperkette  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$  (hier sind jeweils die positiven reellen Wurzeln gemeint). Dann sind  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$  und  $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$  normal, da vom Grad 2, aber  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$  ist nicht normal.

## 4. G

### 4.1. Die Galoisgruppe.

**Definition 4.1.** Sei  $K \subset L$  eine Körpererweiterung. Die Menge der bijektiven Ringhomomorphismen  $L \rightarrow L$ , die  $K$  punktweise festhalten, heißt die *Galoisgruppe* von  $L$  über  $K$ . Sie wird mit  $\text{Gal}(L/K)$  notiert.

*Beispiele 4.2.* (1) Die Galoisgruppe von  $\mathbb{R} \subset \mathbb{C}$  ist die Gruppe mit zwei Elementen, bestehend aus der Identität und der komplexen Konjugation.

(2) Die Galoisgruppe von  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$  ist trivial.

(3) Ist  $p$  eine Primzahl, so ist der Frobenius  $\text{Fr}: \mathbb{F}_{p^m} \rightarrow \mathbb{F}_{p^m}$ ,  $\text{Fr}(x) = x^p$  ein Element in  $\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ . Allgemeiner ist  $\text{Fr}^n$  ein Element in  $\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$ .

*Anmerkung 4.3.* Ist  $K \subset L$  endlich, so ist schon jeder Ringhomomorphismus  $\phi: L \rightarrow L$ , der  $K$  punktweise festhält, eine Bijektion. Denn  $\phi$  ist injektiv als Homomorphismus zwischen Körpern, und, da  $L$  ein endlich dimensionaler  $K$ -Vektorraum ist, schon ein Isomorphismus von  $K$ -Vektorräumen.

**Proposition 4.4.** *Es gilt  $|\text{Gal}(L/K)| \leq [L : K]$ .*

Wir zeigen folgende stärkere Aussage:

**Lemma 4.5.** *Sind  $K \subset L$  und  $K \subset M$  Körpererweiterungen, so gibt höchstens  $[L : K]$  Ausdehnungen  $L \rightarrow M$  von  $K \subset M$ .*

*Beweis.* Wir können  $[L : K] < \infty$  annehmen. Wir argumentieren dann per Induktion über  $[L : K]$ . Gibt es keinen echten Zwischenkörper  $K \subset L' \subset L$ , so ist  $L = K(a)$  für jedes  $a \in L$ ,  $a \notin K$ . Damit gibt es, nach Lemma 3.37, so viele Homomorphismen  $K(a) \rightarrow M$  über  $K$  wie es Nullstellen des Minimalpolynoms von  $a$  in  $M$  gibt, also höchstens  $[L : K]$  viele.

Ansonsten wählen wir einen echten Zwischenkörper  $K \subset L' \subset L$ . Per Induktion gibt es höchstens  $[L' : K]$  Ausdehnungen  $L' \rightarrow M$  und, über jeder dieser Ausdehnungen, höchstens  $[L : L']$  Ausdehnungen  $L \rightarrow M$ . Insgesamt erhalten wir also höchstens  $[L : L'] \cdot [L' : K] = [L : K]$  Ausdehnungen.  $\square$

*Die folgende Proposition wurde in der Vorlesung im Wintersemester 06/07 ausgelassen!*

**Proposition 4.6.** *Sei  $p^n$  eine Primzahlpotenz und  $m \geq 1$ . So ist  $\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$  eine zyklische Gruppe der Ordnung  $m$ , erzeugt von der Frobeniusabbildung  $\text{Fr}^n: x \mapsto x^{p^n}$ .*

*Beweis.* Sei  $\gamma = \text{Fr}^n \in \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$ . So hat  $\gamma^r$  höchstens  $p^{rn}$  Fixpunkte (Nullstellen des Polynoms  $X^{p^{rn}} - X$ ). Insbesondere sind  $\text{id} = \gamma^0, \gamma, \gamma^2, \dots, \gamma^{m-1}$  paarweise verschieden. Also erzeugt  $\gamma$  in  $\text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$  eine zyklische Untergruppe der Ordnung  $m$ . Nach Proposition 4.4 hat die Galoisgruppe aber höchstens  $m$  Elemente.  $\square$

## 4.2. Galoisweiterungen.

**Definition 4.7.** Eine separable und normale Körpererweiterung heißt *Galoisweiterung*.

Ist  $M$  eine Menge und  $G \times M \rightarrow M$ ,  $(g, m) \mapsto g.m$  eine Operation einer Gruppe  $G$  auf  $M$ , so sei  $M^G = \{m \in M \mid g.m = m \text{ für alle } g \in G\}$  die Menge der Invarianten.

Sei  $K \subset L$  eine Körpererweiterung mit Galoisgruppe  $G = \text{Gal}(L/K)$ .  $G$  operiert, per Definition, auf der  $L$  zugrundeliegenden Menge.

**Satz 4.8.** Sei  $K \subset L$  eine endliche Erweiterung. Dann sind äquivalent:

- (1)  $K \subset L$  ist eine Galoisweiterung.
- (2) Es ist  $|\text{Gal}(L/K)| = [L : K]$ .
- (3) Es ist  $K = L^{\text{Gal}(L/K)} = \{a \in L \mid \gamma(a) = a \text{ für alle } \gamma \in \text{Gal}(L/K)\}$ .
- (4) Für jedes  $a \in L$  ist  $\prod_{b \in \text{Gal}(L/K).a} (X - b)$  das Minimalpolynom über  $K$ .

*Beweis.* Nach Satz 3.54 ist  $|\text{Gal}(L/K)| = [L : K]$  für jede normale und separable Erweiterung  $K \subset L$ . Also folgt (2) aus (1). Sei  $L' = L^{\text{Gal}(L/K)}$ . Dann ist  $\text{Gal}(L/K) = \text{Gal}(L/L')$ . Gilt (2), so folgt  $[L : K] = |\text{Gal}(L/K)| = |\text{Gal}(L/L')| \leq [L : L']$ , aber natürlich gilt auch  $[L : L'] \leq [L : K]$ , also folgt  $[L : L'] = [L : K]$  und damit  $L = L'$ , also (3).

Wir zeigen nun, daß (4) aus (3) folgt. Sei  $a \in L$  und  $P \in K[X]$  sein Minimalpolynom. Ist  $\gamma \in \text{Gal}(L/K)$ , so ist  $\gamma(a)$  eine Nullstelle von  $P$ . Somit ist  $Q(X) = \prod_{b \in \text{Gal}(L/K).a} (X - b)$  ein Teiler von  $P$ . Nun operiert  $\text{Gal}(L/K)$  auch auf  $L[X]$  durch Ringautomorphismen (koeffizientenweise, es ist also  $\gamma(a_0 + \dots + a_n X^n) := \gamma(a_0) + \dots + \gamma(a_n) X^n$ ). Offensichtlich ist, für  $R \in L[X]$ ,  $\gamma(R(X)) = R(X)$  für alle  $\gamma \in \text{Gal}(L/K)$  genau dann, wenn  $R(X) \in L^{\text{Gal}(L/K)}[X] = K[X] \subset L[X]$ . Nun ist

$$\begin{aligned} \gamma(Q(X)) &= \gamma \left( \prod_{b \in \text{Gal}(L/K).a} (X - b) \right) \\ &= \prod_{b \in \text{Gal}(L/K).a} (X - \gamma(b)) \\ &= Q(X), \end{aligned}$$

also  $Q(X) \in K[X]$ . Da  $P$  irreduzibel ist und  $Q$  normiert, ist also  $P = Q$ , und damit haben wir Aussage (4) gezeigt.

Gilt (4), so ist  $K \subset L$  sicherlich separabel und normal, also Galois. □

**4.3. Die Galois Korrespondenz.** Sei  $K \subset L$  eine Körpererweiterung und  $K \subset M \subset L$  ein Zwischenkörper. So ist  $\text{Gal}(L/M) \subset \text{Gal}(L/K)$  die Untergruppe aller Automorphismen, die sogar  $M$  festhalten. Ist umgekehrt  $H \subset \text{Gal}(L/K)$  eine Untergruppe, so können wir den Fixkörper

$$L^H = \{a \in L \mid \gamma(a) = a \text{ für alle } \gamma \in H\}$$

bilden. Er enthält  $K$ .

*Erinnerung:* Ist  $K \subset L$  separabel, so sind auch  $K \subset M$  und  $M \subset L$  separabel. Ist  $K \subset L$  normal, so ist auch  $M \subset L$  normal. Aber  $K \subset M$  ist dann nicht notwendigerweise normal (Bsp:  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3} \sqrt[3]{2}, e^{4\pi i/3} \sqrt[3]{2})$ ).

**Satz 4.9** (Galois Korrespondenz). Sei  $K \subset L$  eine endliche Galoisweiterung.

(1) *Die Abbildung*

$$\left\{ \begin{array}{l} \text{Zwischenkörper} \\ K \subset M \subset L \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{Untergruppen von} \\ \text{Gal}(L/K) \end{array} \right\}$$

$$M \xrightarrow{\alpha} \text{Gal}(L/M)$$

ist eine Bijektion mit Inversem  $\beta: H \mapsto L^H$ .

(2) *Unter der Bijektion in (1) entsprechen die Zwischenkörper  $K \subset M \subset L$ , so daß  $K \subset M$  normal ist, den Normalteilern von  $\text{Gal}(L/K)$ .*

(3) *Ist  $H \subset \text{Gal}(L/K)$  ein Normalteiler und  $\gamma \in \text{Gal}(L/K)$ , so ist  $\gamma(L^H) = L^H$  und die Restriktion  $\text{Gal}(L/K) \rightarrow \text{Gal}(L^H/K)$  liefert einen Isomorphismus*

$$\text{Gal}(L/K)/H \xrightarrow{\sim} \text{Gal}(L^H/K).$$

*Beweis.* Wir zeigen, daß  $\beta \circ \alpha = \text{id}$ . Sei dazu  $K \subset M \subset L$  ein Zwischenkörper. Wir müssen zeigen, daß  $M = L^{\text{Gal}(L/M)}$ . Nun ist  $M \subset L$  Galois (vgl. Übung 3.57), also folgt die Aussage aus der Charakterisierung (3) in Satz 4.8.

*Anmerkung 4.10.* Es gilt sogar allgemein (Satz von Artin): Ist  $L$  ein Körper und  $G$  eine endliche Gruppe von Automorphismen von  $L$ , so ist  $L^G \subset L$  endlich Galois mit Galoisgruppe  $G$ . Das ist nicht schwer zu beweisen (vgl. Lang: Algebra).

Wir zeigen, daß  $\alpha \circ \beta = \text{id}$ . Sei dazu  $H \subset \text{Gal}(L/K)$  eine Untergruppe. Wir müssen  $H = \text{Gal}(L/L^H)$  zeigen. Sicherlich ist  $H \subset \text{Gal}(L/L^H)$ . Nach dem Satz vom primitiven Element 3.56 gibt es  $a \in L$  mit  $L = K(a)$ . Wir betrachten das Polynom  $Q(X) := \prod_{b \in H.a} (X - b) \in L[X]$  und zeigen wie im Beweis von Satz 4.8, daß  $Q(X) \in L^H[X]$ . Außerdem ist  $Q(a) = 0$ . Das Minimalpolynom von  $a$  über  $L^H$  ist also ein Teiler von  $Q$  und hat deshalb höchstens den Grad  $|H|$ . Weiter ist  $a$  natürlich auch ein primitives Element der Erweiterung  $L^H \subset L$ , also ist  $[L : L^H] \leq |H|$ , also  $|\text{Gal}(L/L^H)| \leq [L : L^H] \leq |H|$ , und aus  $H \subset \text{Gal}(L/L^H)$  folgern wir  $H = \text{Gal}(L/L^H)$ . Damit haben wir Teil (1) des Satzes gezeigt.

Wir zeigen nun den zweiten Teil. Sei  $H \subset \text{Gal}(L/K)$  eine Untergruppe,  $m \in L^H$  und  $\gamma \in \text{Gal}(L/K)$ . Dann ist  $\gamma(L^H) = L^{\gamma H \gamma^{-1}}$ . Nach Teil (1) unserer Korrespondenz ist also  $\gamma(L^H) = L^H$  genau dann, wenn  $\gamma H \gamma^{-1} = H$ . Also ist  $L^H$  stabil unter der Operation von  $\text{Gal}(L/K)$  genau dann, wenn  $H \subset \text{Gal}(L/K)$  normal ist.

Wir behaupten, daß  $L^H$  stabil ist unter  $\text{Gal}(L/K)$  genau dann, wenn  $K \subset L^H$  normal ist: Ist  $K \subset L^H$  normal, so ist  $L^H$  invariant unter  $\text{Gal}(L/K)$  nach Lemma 3.40. Wir zeigen nun die Umkehrung. Sei also  $L^H$  invariant unter  $\text{Gal}(L/K)$ . Sei  $a \in L^H$  und  $b \in L$  eine Nullstelle des Minimalpolynoms von  $a$  über  $K$ . Wir wollen nun zeigen, daß  $b \in L^H$ . Daraus können wir dann schließen, daß  $K \subset L^H$  ein Zerfällungskörper, also normal ist (der Zerfällungskörper des Produkts der Minimalpolynome von endlich vielen Erzeugern, beispielsweise).

Wir wollen also  $b \in L^H$  zeigen. Nun gibt es ein  $\gamma \in \text{Gal}(L/K)$  mit  $\gamma(a) = b$ , denn wir finden, nach Lemma 3.37, eine Ausdehnung  $\phi: K(a) \rightarrow L$  mit  $\phi(a) = b$  und können diese weiter ausdehnen zu einem Element  $\gamma: L \rightarrow L$  der Galoisgruppe. Wegen  $\gamma(L^H) = L^H$  ist also  $b \in L^H$ .

Wir haben also gezeigt, daß  $H \subset \text{Gal}(L/K)$  ein Normalteiler ist genau dann, wenn  $K \subset L^H$  normal ist.

Wir zeigen nun die letzte Aussage. Für eine normale Untergruppe  $H \subset \text{Gal}(L/K)$  und  $\gamma \in \text{Gal}(L/K)$  ist  $\gamma(L^H) = L^H$ . Also induziert das Einschränken eine Abbildung

$\text{Gal}(L/K) \rightarrow \text{Gal}(L^H/K)$ . Der Kern dieser Abbildung ist  $H$  (nach (1)) und wir erhalten eine injektive Abbildung  $\text{Gal}(L/K)/H \hookrightarrow \text{Gal}(L^H/K)$ . Nun ist  $K \subset L^H$  eine Galois-erweiterung (normal nach Wahl von  $H$  und separabel in jedem Fall, vgl. Übung 3.57), also hat die Gruppe rechts  $[L^H : K]$  Elemente, während die Gruppe links  $[L : K]/|H| = [L : K]/[L : L^H] = [L^H : K]$  Elemente hat, damit ist unsere Abbildung also bijektiv.  $\square$

#### 4.4. Der Hauptsatz der Algebra.

**Satz 4.11.** *Der Körper  $\mathbb{C}$  ist algebraisch abgeschlossen.*

*Anmerkung 4.12.* Wir definieren  $\mathbb{C}$  als den Zerfällungskörper über  $\mathbb{R}$  des irreduziblen Polynoms  $X^2 + 1$ :

$$\mathbb{C} = \mathbb{R}[X]/(X^2 + 1).$$

Die einzigen Eigenschaften der Erweiterung  $\mathbb{R} \subset \mathbb{C}$ , die wir im Beweis benutzen werden, sind, daß  $\mathbb{R} \subset \mathbb{C}$  eine separable (Charakteristik Null) Körpererweiterung vom Grad zwei ist, daß *jedes* Polynom in  $\mathbb{C}[X]$  vom Grad zwei über  $\mathbb{C}$  vollständig zerfällt (Übung!), und daß jedes Polynom aus  $\mathbb{R}[X]$  von ungeradem Grad in  $\mathbb{R}$  eine Nullstelle hat.

*Beweis.* Wir zeigen, daß jede endliche Erweiterung von  $\mathbb{C}$  trivial ist. Dann muß jedes irreduzible Polynom in  $\mathbb{C}[X]$  schon Grad 1 haben, und dies ist gleichbedeutend damit, daß  $\mathbb{C}$  algebraisch abgeschlossen ist.

Erster Schritt: Es gibt keine endliche Erweiterung  $\mathbb{R} \subset L$  mit ungeradem Grad  $> 1$ . Denn der Grad des Minimalpolynoms eines  $a \in L$  ist dann ungerade, also ist das Minimalpolynom linear. Dann ist aber  $\mathbb{R} = L$ .

Zweiter Schritt: Der Grad jeder endlichen Galois-erweiterung  $\mathbb{R} \subset L$  ist eine Zweierpotenz. Denn ist  $\mathbb{R} \subset L$  eine nicht triviale Galois-erweiterung mit Galoisgruppe  $G = \text{Gal}(L/\mathbb{R})$ , so wählen wir eine 2-Sylow  $S \subset \text{Gal}(L/\mathbb{R})$ . Dann ist  $[L^S : \mathbb{R}]$  ungerade, also  $\mathbb{R} = L^S$  nach Schritt 1, und deshalb  $S = \text{Gal}(L/\mathbb{R})$  nach der Galois-korrespondenz.

Dritter Schritt: Es gibt keine Erweiterung  $\mathbb{C} \subset L$  vom Grad 2. Denn es gibt keine irreduziblen Polynome vom Grad 2 über  $\mathbb{C}$ .

Letzter Schritt: Sei also  $\mathbb{C} \subset L$  eine endliche Erweiterung. Aufgrund von Satz 3.44 können wir annehmen, daß  $\mathbb{R} \subset L$  normal, also Galois ist. Dann ist  $\text{Gal}(L/\mathbb{R})$  eine 2-Gruppe. Dann ist auch  $G = \text{Gal}(L/\mathbb{C})$  eine 2-Gruppe. Wir wollen zeigen, daß  $G$  die triviale Gruppe ist, denn dann ist  $L = \mathbb{C}$  nach der Galois-korrespondenz ( $\mathbb{C} \subset L$  ist ebenfalls Galois!). Ist  $G \neq \{e\}$ , so gibt es nach dem Satz über die Struktur von  $p$ -Gruppen 1.81 einen Normalteiler  $H \subset G$  vom Index 2. Da  $H$  ein Normalteiler ist, ist  $\mathbb{C} \subset L^H$  Galois vom Grad  $[L^H : \mathbb{C}] = |\text{Gal}(L^H/\mathbb{C})| = |\text{Gal}(L/\mathbb{C})|/|H| = 2$ , was der Aussage im dritten Schritt widerspricht. Also ist  $G$  trivial und damit  $L = \mathbb{C}$ .  $\square$

4.5.  **$n$ -te Einheitswurzeln.** Sei  $K$  ein Körper und  $n \geq 2$ .

**Definition 4.13.** Die Menge  $\mu_n = \mu_n(K) := \{\zeta \in K \mid \zeta^n = 1\}$  heißt die *Menge der  $n$ -ten Einheitswurzeln* in  $K$ .

Die Menge  $\mu_n$  ist offenbar eine endliche Untergruppe der multiplikativen Gruppe  $K^\times$ . Nach Satz 3.31 ist  $\mu_n$  zyklisch.

Die  $n$ -ten Einheitswurzeln sind gerade die Nullstellen des Polynoms  $X^n - 1 \in K[X]$ . Ist  $\text{char } K$  kein Teiler von  $n$ , so ist das Polynom  $X^n - 1$  nach Lemma 3.50 separabel (die formale Ableitung  $nX^{n-1}$  ist nicht Null, also teilerfremd zu  $X^n - 1$ ). In seinem Zerfällungskörper hat  $X^n - 1$  also  $n$  verschiedene Nullstellen.

**Definition 4.14.** Wir sagen,  $K$  enthält alle  $n$ -ten Einheitswurzeln, wenn das Polynom  $X^n - 1$  über  $K$  vollständig in Linearfaktoren zerfällt.

Ist  $\text{char } K$  kein Teiler von  $n$  und enthält  $K$  alle  $n$ -ten Einheitswurzeln, so ist  $\mu_n$  also eine zyklische Gruppe der Ordnung  $n$ , also isomorph zu  $\mathbb{Z}/n\mathbb{Z}$ .

**4.6. Galoisgruppen der Kreisteilungskörper.** In diesem Abschnitt arbeiten wir über dem Grundkörper  $K = \mathbb{Q}$ .

**Definition 4.15.** Der Zerfällungskörper  $\mathbb{Q} \subset L$  des Polynoms  $X^n - 1$  über  $\mathbb{Q}$  heißt der  $n$ -te Kreisteilungskörper.

*Bemerkung 4.16.* Da  $X^n - 1$  vollständig in Linearfaktoren über  $\mathbb{C}$  zerfällt, gibt es eine Inklusion  $L \subset \mathbb{C}$  über  $\mathbb{Q}$ . Das Bild dieser Inklusion ist der von den komplexen  $n$ -ten Einheitswurzeln  $e^{2\pi ik/n}$ ,  $k = 0, \dots, n-1$  über  $\mathbb{Q}$  erzeugte Unterkörper. Daher der Name Kreisteilungskörper.

Wir stellen uns den  $n$ -ten Kreisteilungskörper von nun an in  $\mathbb{C}$  eingebettet vor.

**Definition 4.17.** Eine  $n$ -te Einheitswurzel  $\zeta \in \mathbb{C}$  der Ordnung  $n$  heißt *primitive  $n$ -te Einheitswurzel*.

Die primitiven  $n$ -ten Einheitswurzeln sind also genau die Erzeuger der zyklischen Gruppe  $\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$ , und genau diejenigen  $n$ -ten Einheitswurzeln, die den  $n$ -ten Kreisteilungskörper  $\mathbb{Q} \subset L$  erzeugen.

Wir definieren

$$\text{End}_{Gr}(\mu_n) = \{\phi: \mu_n \rightarrow \mu_n \mid \phi \text{ ist ein Homomorphismus von Gruppen}\},$$

die Menge der *Endomorphismen von  $\mu_n$* , und

$$\text{Aut}_{Gr}(\mu_n) = \{\phi \in \text{End}_{Gr}(\mu_n) \mid \phi \text{ ist bijektiv}\},$$

die Menge der *Automorphismen von  $\mu_n$* . Nach Wahl einer primitiven  $n$ -ten Einheitswurzel  $\zeta$  ist die Abbildung  $\text{Aut}_{Gr}(\mu_n) \rightarrow \mu_n$ ,  $\phi \mapsto \phi(\zeta)$ , eine Bijektion zwischen der Menge  $\text{Aut}_{Gr}(\mu_n)$  und der Menge der primitiven  $n$ -ten Einheitswurzeln.

Jedes  $k \in \mathbb{Z}$  induziert einen Gruppenhomomorphismus  $\phi_k: \mu_n \rightarrow \mu_n$ ,  $\zeta \mapsto \zeta^k$ . Wir erhalten einen Homomorphismus  $\phi: \mathbb{Z} \rightarrow \text{End}_{Gr}(\mu_n)$ ,  $k \mapsto \phi_k$  mit Kern  $n\mathbb{Z}$ . Da  $\mu_n$  zyklisch ist, ist dieser Homomorphismus auch surjektiv, also ist

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \text{End}_{Gr}(\mu_n).$$

Dabei entsprechen die multiplikativ invertierbaren Elemente in  $\mathbb{Z}/n\mathbb{Z}$  den Automorphismen, also

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Aut}_{Gr}(\mu_n).$$

Sei  $\mathbb{Q} \subset L$  der  $n$ -te Kreisteilungskörper. Ein  $\phi \in \text{Gal}(L/\mathbb{Q})$  bildet die Menge  $\mu_n$  bijektiv auf sich ab und ist sogar ein Automorphismus der Gruppe  $\mu_n$ . Wir erhalten also eine Abbildung

$$\phi: \text{Gal}(L/\mathbb{Q}) \rightarrow \text{Aut}_{Gr}(\mu_n).$$

$\phi$  ist injektiv, da  $L$  über  $\mathbb{Q}$  von  $\mu_n$  erzeugt wird.

Wir erinnern noch einmal an das  $n$ -te Kreisteilungspolynom

$$\Phi_n(X) = \prod_{\text{ord } \zeta = n} (X - \zeta).$$

$\Phi_n$  ist ein Teiler von  $X^n - 1$  und wir haben in Abschnitt 2.14 schon gezeigt, daß  $\Phi_n$  ganzzahlige Koeffizienten hat.

**Satz 4.18.** (1) Das  $n$ -te Kreisteilungspolynom  $\Phi_n(X) \in \mathbb{Q}[X]$  ist irreduzibel für alle  $n \geq 1$ .

(2) Die oben definierte Abbildung  $\text{Gal}(L/\mathbb{Q}) \rightarrow \text{Aut}_{Gr}(\mu_n)$  ist bijektiv.

(3) Sind  $\zeta, \xi \in \mathbb{C}$  zwei primitive  $n$ -te Einheitswurzeln, so gibt es genau ein  $\phi \in \text{Gal}(L/\mathbb{Q})$  mit  $\phi(\zeta) = \xi$ .

*Beweis.* Wir zeigen (1).  $\Phi_n$  ist sogar ein primitives Polynom in  $\mathbb{Z}[X]$  und nach 2.50 reicht es zu zeigen, daß  $\Phi_n$  in  $\mathbb{Z}[X]$  irreduzibel ist. Sei dazu  $\Phi_n = F \cdot G$  eine Zerlegung in  $\mathbb{Z}[X]$  und  $F$  keine Einheit. Sei  $\zeta \in \mathbb{C}$  eine Nullstelle von  $F$  und  $p$  eine Primzahl, die  $n$  nicht teilt. Wir behaupten, daß  $F(\zeta^p) = 0$ . Ansonsten müßte  $G(\zeta^p) = 0$  sein. Im Ring  $\mathbb{F}_p[X]$  ist dann  $\overline{G(\zeta^p)} = \overline{G(\zeta)}^p = 0$ . Also haben  $\overline{F(X)}$  und  $\overline{G(X)}$  die gemeinsame Nullstelle  $\zeta$ . Da  $X^n - 1$  über  $\mathbb{F}_p$  separabel ist ( $p$  ist kein Teiler von  $n$ ), erhalten wir einen Widerspruch.

Wir haben also gezeigt, daß mit jeder Nullstelle  $\zeta$  von  $F$  auch  $\zeta^p$  Nullstelle ist von  $F$  für alle zu  $n$  teilerfremden primen  $p$ . Dann ist aber jede primitive Einheitswurzel Nullstelle von  $F$ , also  $F$  ein Vielfaches von  $\Phi_n$  und damit  $G$  eine Einheit. Wir haben also (1) gezeigt.

Unsere Abbildung  $\text{Gal}(L/\mathbb{Q}) \rightarrow \text{Aut}(\mu_n)$  ist injektiv. Sei  $\zeta$  eine primitive  $n$ -te Einheitswurzel. Dann ist  $L = \mathbb{Q}(\zeta)$ . Nach (1) ist  $\Phi_n(X)$  das Minimalpolynom von  $\zeta$  über  $\mathbb{Q}$ , also gilt

$$[L : \mathbb{Q}] = \deg \Phi_n.$$

Somit ist  $|\text{Gal}(L/\mathbb{Q})| = \deg \Phi_n = \text{Anzahl der primitiven } n\text{-ten Einheitswurzeln} = |\text{Aut}(\mu_n)|$ , also ist unsere Abbildung bijektiv.

Teil (3) folgt sofort daraus, daß  $\mu_n$  eine zyklische Gruppe ist. □

**Definition 4.19.** Die Abbildung  $\phi: \mathbb{N} \rightarrow \mathbb{N}$ ,  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$  heißt *Eulersche  $\phi$ -Funktion*.

Es ist

$$\begin{aligned} \phi(n) &= \text{Anzahl der zu } n \text{ teilerfremden } d \in \mathbb{Z} \text{ mit } 1 \leq d \leq n \\ &= \text{Anzahl der primitiven } n\text{-ten Einheitswurzeln} \\ &= \text{Anzahl der } \zeta \in \mathbb{C}^\times \text{ der Ordnung } n \\ &= \text{Grad des } n\text{-ten Kreisteilungspolynoms } \Phi_n \in \mathbb{Q}[X] \\ &= \text{Grad des } n\text{-ten Kreisteilungskörpers } \mathbb{Q} \subset L \end{aligned}$$

**Satz 4.20.** Das regelmäßige  $n$ -Eck ist konstruierbar genau dann, wenn  $\phi(n)$  eine Zweierpotenz ist.

*Beweis.* Sei  $\zeta \in \mathbb{C}$  eine primitive  $n$ -te Einheitswurzel. Das regelmäßige  $n$ -Eck ist konstruierbar genau dann, wenn  $\zeta$  konstruierbar ist. Ist  $\zeta$  konstruierbar, dann ist, nach Korollar 3.22,  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$  eine Zweierpotenz.

Ist  $\phi(n)$  umgekehrt eine Zweierpotenz, so ist  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  eine 2-Gruppe. Nach der Galois-Korrespondenz und dem Satz über die Struktur von  $p$ -Gruppen 1.81 gibt es eine Körperkette

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m = \mathbb{Q}(\zeta)$$

mit  $[K_i : K_{i-1}] = 2$  für  $i = 1, \dots, m$ . Also ist  $\zeta$  konstruierbar, denn  $\zeta$  entsteht durch sukzessives Wurzelziehen.  $\square$

Wir wollen die  $n$  mit der Eigenschaft, daß  $\phi(n)$  eine Zweierpotenz ist, noch genauer beschreiben.

**Lemma 4.21.** (1) *Es ist  $\phi(mn) = \phi(m)\phi(n)$ , wenn  $m$  und  $n$  teilerfremd sind.*

(2) *Ist  $p$  prim und  $r \geq 1$ , so ist  $\phi(p^r) = p^{r-1}(p-1)$ .*

*Ist also  $n = p_1^{r_1} \cdots p_k^{r_k}$  und die  $p_i$  paarweise verschieden, so ist*

$$\phi(n) = (p_1 - 1) \cdots (p_k - 1) p_1^{r_1-1} \cdots p_k^{r_k-1}.$$

*Insbesondere ist  $\phi(n)$  also eine Zweierpotenz genau dann, wenn  $n$  von der Form  $2^m p_1 \cdots p_k$  mit paarweise verschiedenen Primzahlen  $p_i$  der Form  $2^l + 1$  (Fermatsche Primzahlen) ist.*

*Beweis.* Nach dem Chinesischen Restsatz ist  $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  für teilerfremde  $m, n \in \mathbb{Z}$  (sogar als Ringe!). Insbesondere ist

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Also ist  $\phi(mn) = \phi(m) \cdot \phi(n)$ .

Ist  $p$  eine Primzahl,  $r \geq 1$  und  $1 \leq n \leq p^r$ , so sind  $p^r$  und  $n$  genau dann teilerfremd, wenn  $n$  kein Vielfaches von  $p$  ist. Es gibt aber  $p^{r-1}$  Vielfache von  $p$  zwischen 1 und  $p^r$ , damit ist  $\phi(p^r) = p^r - p^{r-1}$ .  $\square$

**4.7. Adjunktion  $n$ -ter Wurzeln.** Sei  $K$  ein Körper. Ist die Charakteristik von  $K$  kein Teiler von  $n$ , so ist das Polynom  $X^n - 1 \in K[X]$  separabel nach Lemma 3.50. Dies setzen wir von nun an voraus.

**Definition 4.22.** Eine *zyklische* bzw. *abelsche* Erweiterung ist eine Galois-erweiterung  $K \subset L$  mit zyklischer bzw. abelscher Galoisgruppe.

**Definition 4.23.** Wir sagen, eine Körpererweiterung  $K \subset L$  *entsteht durch Adjunktion einer  $n$ -ten Wurzel*, falls es ein  $a \in L$  gibt mit  $L = K(a)$  und  $a^n \in K$ .

**Satz 4.24.** *Sei  $K$  ein Körper und  $n \in \mathbb{N}$ ,  $n \geq 2$  kein Vielfaches von  $\text{char } K$ . Der Körper  $K$  enthalte alle  $n$ -ten Einheitswurzeln (siehe Definition 4.14).*

- (1) *Eine zyklische Erweiterung von  $K$  vom Grad  $n$  entsteht durch Adjunktion einer  $n$ -ten Wurzel.*
- (2) *Entsteht  $K \subset L$  durch Adjunktion einer  $n$ -ten Wurzel, so ist  $K \subset L$  zyklisch und der Grad  $[L : K]$  ist ein Teiler von  $n$ .*

*Beweis.* Wir zeigen Teil (1). Sei  $K \subset L$  eine zyklische Erweiterung vom Grad  $n$  und  $\gamma \in \text{Gal}(L/K)$  ein Erzeuger.

*Behauptung:* Die Abbildungen  $\text{id} = \gamma^0, \gamma, \dots, \gamma^{n-1}: L \rightarrow L$  sind  $L$ -linear unabhängig (im  $L$ -Vektorraum aller Abbildungen der Menge  $L$  in den Körper  $L$ ).

*Begründung:* Sei  $a_0 \cdot \gamma^0 + a_1 \cdot \gamma + \dots + a_{n-1} \cdot \gamma^{n-1} = 0$  eine nicht triviale Linearkombination mit  $\{|i \mid a_i \neq 0\}$  minimal. Wir wählen ein  $l \in L$  und definieren  $b_i = \gamma^i(l)$ . Es ergibt sich für alle  $x \in L$  die Gleichung

$$a_0 \gamma^0(lx) + \dots + a_{n-1} \gamma^{n-1}(lx) = a_0 b_0 \gamma^0(x) + \dots + a_{n-1} b_{n-1} \gamma^{n-1}(x) = 0,$$

also

$$a_0 b_0 \gamma^0 + \dots + a_{n-1} b_{n-1} \gamma^{n-1} = 0.$$

Ist nun  $a_i \neq 0$ , so ziehen wir das  $b_i$ -fache der ursprünglichen Gleichung ab und erhalten

$$a_0(b_0 - b_i) \gamma^0 + \dots + 0 \cdot \gamma^i + \dots + a_{n-1}(b_{n-1} - b_i) \gamma^{n-1} = 0.$$

War nun auch  $a_j \neq 0$  für ein  $j \neq i$ , so wählen wir  $l$  mit  $\gamma^j(l) \neq \gamma^i(l)$  und erhalten also eine nicht triviale Darstellung der Null mit kleinerer Länge, was unseren Voraussetzungen widerspricht. Damit ist die Behauptung bewiesen.

Wir wählen nun eine primitive  $n$ -te Einheitswurzel  $\zeta \in K$ . Dann gilt

$$\text{id} + \zeta \gamma + \dots + \zeta^{n-1} \gamma^{n-1} \neq 0,$$

es gibt also ein  $b \in L$  mit  $a := b + \zeta \gamma(b) + \dots + \zeta^{n-1} \gamma^{n-1}(b) \neq 0$ . Es ist  $\gamma(a) = \zeta^{-1} a$  und  $\gamma^i(a) = \zeta^{-i} a$ . Also ist  $a \neq \gamma^i(a)$  für alle  $i = 1, \dots, n-1$ , somit ist  $\text{Gal}(L/K(a)) \subset \text{Gal}(L/K)$  die triviale Untergruppe, also  $K(a) = L$ . Es gilt aber auch  $\gamma(a^n) = (\zeta a)^n = a^n$ , also  $a^n \in K$ . Damit haben wir (1) gezeigt.

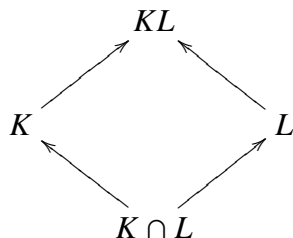
Nun zeigen wir Teil (2). Sei  $L = K(a)$  mit  $a^n \in K$ . Die Nullstellen von  $X^n - a^n$  sind die Elemente  $\zeta a$ , wobei  $\zeta$  die  $n$ -ten Einheitswurzeln durchläuft. Also ist  $K \subset K(a)$  der Zerfällungskörper von  $X^n - a^n$ . Das Polynom  $X^n - a^n$  ist separabel nach unserer Voraussetzung an  $n$ , also ist  $K \subset L$  Galois.

Der Grad von  $K \subset L$  ist die Ordnung der Galoisgruppe  $\text{Gal}(L/K)$ . Jedes Element der Galoisgruppe bildet  $a$  ab auf  $\xi a$  für ein eindeutig bestimmtes  $\xi \in \mu_n$ . Dies liefert einen injektiven Homomorphismus  $\sigma: \text{Gal}(L/K) \hookrightarrow \mu_n$  von Gruppen. Also ist  $|\text{Gal}(L/K)|$  ein Teiler von  $n$ , und  $\text{Gal}(L/K)$  ist zyklisch als Untergruppe einer zyklischen Gruppe.  $\square$

**Satz 4.25** (Translationssatz). *Seien  $K \subset M$  und  $L \subset M$  Körpererweiterungen mit der Eigenschaft, daß  $K \cap L \subset K$  endlich und Galois ist. Sei  $KL \subset M$  der von  $K$  und  $L$  in  $M$  erzeugte Unterkörper. Dann ist  $L \subset KL$  endlich und Galois und die Restriktion liefert einen Isomorphismus*

$$\text{Gal}(KL/L) \xrightarrow{\sim} \text{Gal}(K/K \cap L).$$

Wir veranschaulichen die Relationen zwischen den Körpern in folgendem Diagramm:



*Beweis.* Ist  $K \cap L \subset K$  separabel, so wird  $L \subset KL$  erzeugt von separablen Elementen, ist also separabel. Ist  $K \cap L \subset K$  Zerfällungskörper von  $P \in (K \cap L)[X]$ , so ist

$L \subset KL$  Zerfällungskörper von  $P \in L[X]$ . Also ist  $L \subset KL$  Galois und endlich. Jedes  $\gamma \in \text{Gal}(KL/L)$  fixiert den Unterkörper  $K \cap L$ . Da  $K$  normal ist über  $K \cap L$ , induziert  $\gamma$  also eine Abbildung  $\gamma' : K \rightarrow K$ , also ein Element in  $\text{Gal}(K/K \cap L)$ . Ist  $\gamma'$  die Identität, so war  $\gamma$  schon die Identität, da  $\gamma$  auch  $L$  fixiert. Wir erhalten eine *injektive* Abbildung

$$\text{Gal}(KL/L) \hookrightarrow \text{Gal}(K/K \cap L).$$

Das Bild dieser Abbildung hat aber den Fixkörper  $K \cap L$ . Nach der Galois-Korrespondenz ist unsere Abbildung also eine Bijektion.  $\square$

#### 4.8. Auflösbarkeit polynomialer Gleichungen in Charakteristik Null.

**Definition 4.26.** Eine Körpererweiterung  $K \subset M$  heißt *Radikalerweiterung*, wenn es eine Kette von Körpererweiterungen

$$K = K_0 \subset K_1 \subset \dots \subset K_r = M$$

gibt, so daß  $K_i$  aus  $K_{i-1}$  durch Adjunktion einer  $n_i$ -ten Wurzel entsteht (für ein  $n_i \in \mathbb{N}$ ).

**Definition 4.27.** Sei  $K$  ein Körper,  $P \in K[X]$  und  $K \subset L$  der Zerfällungskörper von  $P$ . Wir sagen, die Gleichung  $P(X) = 0$  *läßt sich auflösen durch Radikale über  $K$* , falls es eine Erweiterung  $L \subset M$  gibt, so daß  $K \subset M$  eine Radikalerweiterung ist.

*Bemerkung 4.28.* Die Definition wird verständlich, wenn wir uns klarmachen, daß jedes Element  $m \in M$  aus einer Radikalerweiterung  $K \subset M$  sich durch sukzessives Wurzelziehen aus Elementen in  $K$  erhalten läßt. Beispielsweise liegt das Element

$$3 + \sqrt[15]{4 + \sqrt[27]{3, 27 + \sqrt[517]{-7}}}$$

in einer Radikalerweiterung von  $\mathbb{Q}$ . Hier müssen wir jedoch beachten, daß Wurzelausdrücke wie  $\sqrt[17]{27}$  einer *Wahl* einer 17-ten Wurzel von 27 entsprechen, also keineswegs wohlbestimmt sind. Unser Ausdruck oben steht für insgesamt  $15 \cdot 27 \cdot 517 = 209385$  verschiedene komplexe Zahlen.

Der Satz 4.31 wird besagen, daß sich die Nullstellen eines *allgemeinen* Polynoms  $n$ -ten Grades für  $n \geq 5$  *nicht* durch Wurzelausdrücke in den Koeffizienten angeben lassen.

**Satz 4.29.** *Sei  $K$  ein Körper der Charakteristik  $\text{char } K = 0$  und  $P \in K[X]$ . So sind äquivalent:*

- (1) *Die Gleichung  $P(X) = 0$  läßt sich auflösen durch Radikale über  $K$ .*
- (2) *Die Galoisgruppe des Zerfällungskörpers von  $P$  über  $K$  ist auflösbar.*

*Beweis.* Wir zeigen, daß (1) aus (2) folgt. Sei  $L$  der Zerfällungskörper von  $P$  über  $K$ . Wir müssen zeigen, daß sich  $L$  in eine Radikalerweiterung von  $K$  einbetten läßt. Nach Voraussetzung ist  $\text{Gal}(L/K)$  auflösbar. Es gibt also eine Reihe von Untergruppen

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\},$$

so daß  $G_i$  Normalteiler in  $G_{i-1}$  ist und  $G_{i-1}/G_i$  abelsch. Wir können sogar annehmen, daß  $G_{i-1}/G_i$  zyklisch ist. Die zugehörige Reihe von Fixkörpern

$$K = K_0 \subset K_1 \subset \dots \subset K_n = L$$

ist, nach der Galoiskorrespondenz, eine Reihe zyklischer Erweiterungen (insbesondere Galois). Sei  $n$  der Grad von  $K \subset L$ . Enthält  $K$  nun alle  $n$ -ten Einheitswurzeln, so folgern wir aus Satz 4.24, daß  $K \subset L$  eine Radikalerweiterung ist. Sei ansonsten  $\zeta$  eine primitive  $n$ -te Einheitswurzel von  $K$  (beispielsweise in einem Zerfällungskörper von  $X^n - 1$  über  $K$ ). Nach Adjunktion von  $\zeta$  erhalten wir eine Körperkette

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \cdots \subset K_n(\zeta) = L(\zeta).$$

Für  $i > 1$  ist  $K_{i-1}(\zeta) \subset K_i(\zeta)$  Galois mit  $\text{Gal}(K_i(\zeta)/K_{i-1}(\zeta)) = \text{Gal}(K_i/K_{i-1})$  nach dem Translationssatz, also ist  $K_{i-1}(\zeta) \subset K_i(\zeta)$  zyklisch und entsteht nach Satz 4.24 durch Adjunktion einer  $n_i$ -ten Wurzel (für geeignetes  $n_i$ ). Da auch  $K_0 \subset K_0(\zeta)$  durch Adjunktion einer  $n = n_0$ -ten Wurzel entsteht, ist  $K \subset L(\zeta)$  also eine Radikalerweiterung. Also läßt sich  $K \subset L$  in eine Radikalerweiterung einbetten.

Wir zeigen nun, daß (2) aus (1) folgt. Sei wieder  $L$  der Zerfällungskörper von  $P$  über  $K$ . Dann läßt sich also  $L$  einbetten in eine Radikalerweiterung  $K \subset M$ . Es gibt also eine Reihe

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = M$$

mit  $K_i = K_{i-1}(a)$  und  $a^{n_i} \in K_{i-1}$ . Sei  $n = n_1 \cdots n_m$ . Adjungieren wir zu  $L$  eine primitive  $n$ -te Einheitswurzel, so ist auch

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \cdots \subset K_m(\zeta) = M(\zeta)$$

eine Radikalerweiterung. Aber  $K \subset M(\zeta)$  muß nicht Galois sein, wir können also noch nichts über die Galoisgruppe  $\text{Gal}(M(\zeta)/K)$  aussagen.

Sei nun  $M(\zeta) \subset N$  so, daß  $K \subset N$  normal ist, und  $\tilde{M} \subset N$  der von den Bildern  $\phi(M(\zeta)) \subset N$  unter allen Ausdehnungen  $\phi: M(\zeta) \rightarrow N$  über  $K$  erzeugte Unterkörper. Dann ist  $K \subset \tilde{M}$  normal, also Galois und wird erzeugt von  $\zeta$  und den  $\phi(a_i)$  für alle  $i = 1, \dots, m$  und alle Ausdehnungen  $\phi$ .

Sei  $n = p_1 \cdots p_k$  nun eine Zerlegung in Primfaktoren, und  $\zeta_i$  eine primitive  $p_i$ -te Einheitswurzel über  $K$ . Wir verfeinern  $K \subset K(\zeta)$  nun zu  $K \subset K(\zeta_1) \subset K(\zeta_1, \zeta_2) \subset \cdots \subset K(\zeta_1, \dots, \zeta_n) = K(\zeta)$ . Nun ist jeder Schritt entweder eine triviale Erweiterung oder eine Galoiserweiterung von primem Grad, also zyklisch, insbesondere abelsch. Zu  $K(\zeta)$  adjungieren wir nun sukzessive erst alle  $\phi(a_1)$  (für alle  $\phi: M(\zeta) \rightarrow N$ ), dann alle  $\phi(a_2), \dots$ . Jeder Erweiterungsschritt ist dann zyklisch nach Satz 4.24.

Wir erreichen also eine Körperkette

$$K = \tilde{M}_0 \subset \tilde{M}_1 \subset \cdots \subset \tilde{M}_l = \tilde{M},$$

so daß  $\tilde{M}_i \subset \tilde{M}_{i+1}$  zyklisch, insbesondere Galois ist. Die Kette von Untergruppen

$$G = \text{Gal}(\tilde{M}/K) \supset \text{Gal}(\tilde{M}/\tilde{M}_1) \supset \cdots \supset \text{Gal}(\tilde{M}/\tilde{M}) = \{e\}$$

hat nun die Eigenschaft, daß  $\text{Gal}(\tilde{M}/\tilde{M}_{i+1}) \subset \text{Gal}(\tilde{M}/\tilde{M}_i)$  ein Normalteiler ist (da  $\tilde{M}_i \subset \tilde{M}_{i+1}$  normal ist), und  $\text{Gal}(\tilde{M}/\tilde{M}_i)/\text{Gal}(\tilde{M}/\tilde{M}_{i+1}) = \text{Gal}(\tilde{M}_{i+1}/\tilde{M}_i)$  ist zyklisch, insbesondere abelsch.

Also ist  $\text{Gal}(\tilde{M}/K)$  auflösbar. Wir können  $\text{Gal}(L/K)$  als Untergruppe in  $\text{Gal}(\tilde{M}/K)$  auffassen. Also ist auch  $\text{Gal}(L/K)$  auflösbar.  $\square$

#### 4.9. Die allgemeine polynomiale Gleichung vom Grad $\geq 5$ ist nicht auflösbar.

Sei  $F$  ein Körper und  $F[X_1, \dots, X_n]$  der Polynomring über  $F$  in  $n$  Variablen,  $L = F(X_1, \dots, X_n)$  sein Quotientenkörper. Die symmetrische Gruppe  $S_n$  operiert auf  $L$  (durch Ringhomomorphismen) mittels Vertauschens der Variablen: Einem  $\sigma \in S_n$  ordnen wir den Ringhomomorphismus zu, der  $a \in F$  auf sich abbildet und  $X_i$  auf  $X_{\sigma(i)}$ . Sei  $K = L^{S_n}$  der Fixkörper.

*Übung 4.30.* Das Polynom  $P(T) = \prod_{i=1}^n (T - X_i)$  ist in  $K[T]$ , und  $K \subset L$  ist sein Zerfällungskörper. Insbesondere ist  $K \subset L$  normal. Die offensichtliche Abbildung  $S_n \rightarrow \text{Gal}(L/K)$  ist ein Isomorphismus.

Die Koeffizienten von  $P(T)$  heißen die *elementarsymmetrischen Polynome*. Sie sind algebraisch unabhängig über  $K$ . Deshalb nennt man die Gleichung  $P(T) = 0$  auch die *allgemeine Gleichung  $n$ -ten Grades* (vgl. Kapitel 5.1).

**Satz 4.31.** Sei  $\text{char } K = 0$ . Dann ist die allgemeine Gleichung  $n$ -ten Grades nicht auflösbar für  $n \geq 5$ .

*Beweis.* Das folgt sofort aus Satz 4.29, der obigen Übung und der Tatsache, daß die Gruppe  $S_n$  für  $n \geq 5$  nicht auflösbar ist (Satz 1.85).  $\square$

Es kann also keine Formel für die Nullstellen eines Polynoms  $n$ -ten Grades geben für  $n \geq 5$ . Ist  $n = 2, 3, 4$ , so ist  $S_n$  auflösbar und es gibt tatsächlich Formeln für die Nullstellen (Mitternachtsformel, Cardanosche Formel, vgl. Bosch: Algebra, Kapitel 6).

4.10. **Der algebraische Abschluß.** Wir wollen zeigen, daß jeder Körper sich in einen algebraisch abgeschlossenen Körper einbetten läßt.

Erinnerung: Ein Körper  $K$  heißt *algebraisch abgeschlossen*, falls jedes nicht konstante Polynom  $P \in K[X]$  eine Nullstelle in  $K$  hat. Wir haben gezeigt in Satz 2.19, daß dies äquivalent dazu ist, daß jedes Polynom in  $K[X]$  über  $K$  in Linearfaktoren zerfällt.

Sei  $K$  ein Körper.

**Definition 4.32.** Eine algebraische Erweiterung  $K \subset \bar{K}$  mit algebraisch abgeschlossenem  $\bar{K}$  heißt *algebraischer Abschluß* von  $K$ .

**Satz 4.33.** Zu jedem Körper  $K$  gibt es einen algebraischen Abschluß  $K \subset \bar{K}$ . Je zwei algebraische Abschlüsse sind isomorph: Ist  $K \subset \bar{K}'$  ein weiterer algebraischer Abschluß, so gibt es einen Isomorphismus  $\phi: \bar{K} \rightarrow \bar{K}'$  mit  $\phi|_K = \text{id}_K$ .

Der Beweis der Existenz und Eindeutigkeit eines algebraischen Abschlusses benutzt transzendente Methoden der Mengenlehre, nämlich das Lemma von Zorn. Für dessen Formulierung brauchen wir den Begriff einer partiellen Ordnung auf einer Menge  $X$ . Ist also  $X$  eine Menge, so ist eine partielle Ordnung auf  $X$  eine Relation  $\leq \subset X \times X$  mit den Eigenschaften

- (1)  $x \leq x$  für alle  $x \in X$ ,
- (2) aus  $x \leq y$  und  $y \leq x$  folgt  $x = y$  für alle  $x, y \in X$  und
- (3) aus  $x \leq y$  und  $y \leq z$  folgt  $x \leq z$  für alle  $x, y, z \in X$ .

Gilt zusätzlich für alle  $x, y \in X$  entweder  $x \leq y$  oder  $y \leq x$ , so nennt man  $\leq$  eine *totale Ordnung*.

*Beispiele 4.34.* Die natürlichen Zahlen  $\geq 1$  sind partiell, aber nicht total geordnet bzgl. der Teilbarkeitsrelation:  $n \leq m$  genau dann, wenn  $n \mid m$ . Die Menge aller Teilmengen einer Menge ist partiell geordnet bzgl. Inklusion. Letzteres ist eine Totalordnung genau dann, wenn  $X$  höchstens ein Element enthält.

Ist  $(X, \leq)$  eine partiell geordnete Menge und  $Y \subset X$  eine Teilmenge, so heißt  $x \in X$  eine *obere Schranke* für  $Y$ , falls  $y \leq x$  für alle  $y \in Y$  gilt. Ein Element  $x \in X$  mit der Eigenschaft, daß aus  $y \leq x$  für  $y \in X$  folgt, daß  $x = y$ , heißt *maximales Element* in  $X$ .

**Lemma 4.35** (Lemma von Zorn). *Ist  $(X, \leq)$  eine partiell geordnete Menge, so daß jede total geordnete Teilmenge  $Y \subset X$  eine obere Schranke besitzt, so gibt es in  $X$  mindestens ein maximales Element.*

Man kann das Lemma von Zorn aus dem Auswahlaxiom herleiten. Es lautet:

*Jede surjektive Abbildung zwischen zwei Mengen besitzt ein Rechtsinverses.*

Das Lemma von Zorn und das Auswahlaxiom sind sogar äquivalent. Beide Aussagen können weder bewiesen noch widerlegt werden innerhalb der klassischen Mengenlehre und werden deshalb als Axiom hinzugefügt.

*Beweis des Satzes.* Sei  $F = K[X] \setminus K$  die Menge aller nicht konstanten Polynome. Wir betrachten den Polynomring  $R = K[X_f]_{f \in F}$  in unendlich vielen Variablen  $X_f$  und darin das von den Polynomen  $f(X_f)$  erzeugte Ideal  $F$ . Dies ist ein echtes Ideal, denn sonst gibt es  $g_1, \dots, g_n \in R$  und  $f_1, \dots, f_n \in F$  mit

$$1 = g_1 f_1(X_{f_1}) + \dots + g_n f_n(X_{f_n}).$$

Ist nun  $K \subset L$  ein Erweiterungskörper von  $K$ , indem alle  $f_i$  Nullstellen haben (dies gibt es nach Satz 3.29), so könnten wir diese Nullstellen einsetzen und erhielten  $1 = 0$ .

Die Menge aller echten Ideale in  $R$  ist bzgl. Inklusion partiell geordnet, und die Vereinigung einer total geordneten Menge von echten Idealen ist ein echtes Ideal (denn die 1 ist in keinem Ideal enthalten, also auch nicht in der Vereinigung). Nach dem Lemma von Zorn gibt es also ein maximales echtes Ideal  $J \subset R$  mit  $I \subset J$ .

Wir definieren dann  $K_1 := R/J$ .  $K_1$  ist ein Körper und wird über  $K$  erzeugt von den Nebenklassen der  $\overline{X}_f$ , und  $\overline{X}_f$  ist eine Nullstelle von  $f$ .  $K \subset K_1$  ist also erzeugt von algebraischen Elementen und deshalb eine algebraische Körpererweiterung. Nun hat jedes Polynom aus  $K[X]$  in  $K_1$  eine Nullstelle. Wir wiederholen obige Konstruktion und finden eine Körpererweiterung  $K_1 \subset K_2$ , so daß jedes nicht-konstante Polynom aus  $K_1[X]$  in  $K_2$  eine Nullstelle hat. Wir erhalten eine Körperkette

$$K \subset K_1 \subset K_2 \subset \dots$$

und definieren  $\overline{K}$  als die Vereinigung aller  $K_i$ . Die Erweiterung  $K \subset \overline{K}$  ist algebraisch, da jedes Element aus  $\overline{K}$  schon in einem  $K_i$  liegt und  $K \subset K_i$  algebraisch ist. Außerdem ist  $\overline{K}$  algebraisch abgeschlossen, denn ist  $P \in \overline{K}[X]$ , so liegen die Koeffizienten von  $P$  schon in einem  $K_i$ , also hat  $P$  in  $K_{i+1}$ , also auch in  $\overline{K}$ , eine Nullstelle.

Zur Eindeutigkeit: Seien  $K \subset \bar{K}$  und  $K \subset \bar{K}'$  algebraische Abschlüsse. Wir betrachten die Menge

$$X = \left\{ (L, L', \phi) \mid \begin{array}{l} K \subset L \subset \bar{K}, K \subset L' \subset \bar{K}' \text{ sind Zwischenkörper,} \\ \phi: L \xrightarrow{\sim} L' \text{ ist Isomorphismus über } K \end{array} \right\}.$$

Diese Menge trägt eine partielle Ordnung: wir definieren  $(L, L', \phi) \leq (M, M', \psi)$  falls  $L \subset M$ ,  $L' \subset M'$  und  $\psi|_L = \phi$ . Ist  $Y \subset X$  eine total geordnete Teilmenge, so ist  $(\bigcup L, \bigcup L', \bigcup \phi) \in X$  (die Vereinigung sollen über alle  $(L, L', \phi) \in Y$  genommen werden) eine obere Schranke für  $Y$ .

Wir finden nach dem Lemma von Zorn also ein maximales Element  $(L, L', \phi) \in X$ . Wir wollen zeigen, daß  $L = \bar{K}$  und  $L' = \bar{K}'$  ist, also  $\phi: \bar{K} \rightarrow \bar{K}'$  uns den gewünschten Isomorphismus liefert. Ist  $L \neq \bar{K}$ , so gibt es ein  $a \in \bar{K} \setminus L$ . Sei  $P$  das Minimalpolynom von  $a$  über  $L$  ( $a$  ist algebraisch über  $K$ , also auch über  $L$ ). Dann hat  $\phi(P)$  eine Nullstelle  $b$  in  $\bar{K}'$ . Nach Satz 3.39 läßt sich  $\phi$  also fortsetzen zu einem Isomorphismus  $\phi: L(a) \rightarrow L'(b)$ , was unserer Maximalität widerspricht. Also ist  $L = \bar{K}$ . Dann ist  $L' = \phi(L) \subset \bar{K}'$  ein algebraisch abgeschlossener Körper. Jedes  $b \in \bar{K}'$  ist aber algebraisch über  $L'$ , ist in  $L'$  also schon enthalten. Damit ist  $L' = \bar{K}'$ , was zu zeigen war.  $\square$

Die folgenden beiden Sätze wurden in der Vorlesung im Wintersemester 2006/07 nicht behandelt.

**Satz 4.36.** *Sei  $K$  ein Körper und  $K \subset \bar{K}$  sein algebraischer Abschluß. Dann läßt sich jede algebraische Erweiterung  $K \subset L$  in  $K \subset \bar{K}$  einbetten, d.h. es gibt eine Ausdehnung  $\phi: L \rightarrow \bar{K}$  von  $K \subset \bar{K}$ .*

*Beweis.* Ist  $L \subset \bar{L}$  ein algebraischer Abschluß von  $L$ . Dann ist  $K \subset \bar{L}$  ebenfalls ein algebraischer Abschluß, es gibt also einen Isomorphismus  $\phi: \bar{L} \rightarrow \bar{K}$ , insbesondere also eine Einbettung  $L \rightarrow \bar{K}$  über  $K$ .  $\square$

**Satz 4.37.** *Sei  $K$  ein Körper und  $K \subset \bar{K}$  sein algebraischer Abschluß. Eine endliche algebraische Körpererweiterung  $K \subset L$  ist*

- (1) normal genau dann, wenn je zwei Einbettungen  $L \rightarrow \bar{K}$  über  $K$  dasselbe Bild haben, und
- (2) separabel genau dann, wenn es genau  $[L : K]$  verschiedene Einbettungen  $\phi: L \rightarrow \bar{K}$  gibt.

*Anmerkung 4.38.* Die Charakterisierungen im Satz werden in der Literatur oftmals auch als Definitionen benutzt. Die Anzahl der Einbettungen  $\phi: L \rightarrow \bar{K}$  wird auch der *Separabilitätsgrad* von  $K \subset L$  genannt.

*Beweis.* Ist  $K \subset L$  normal, so wird das Bild jeder Einbettung  $L \rightarrow \bar{K}$  von den Nullstellen der Minimalpolynome aller Elemente aus  $L$  erzeugt, ist also unabhängig.

Sei andererseits das Bild jeder Einbettung  $L \rightarrow \bar{K}$  unabhängig von der Wahl. Wir wählen eine feste Einbettung  $L \subset \bar{K}$ . Sei  $P \in K[X]$  ein irreduzibles Polynom, das eine Nullstelle  $a \in L$  hat. Sei  $b \in \bar{K}$  eine weitere Nullstelle. Dann gibt es eine Ausdehnung  $\phi: K(a) \rightarrow \bar{K}$  mit  $a \mapsto b$ , und eine weitere Ausdehnung dieser

Abbildung zu  $\phi: L \rightarrow \overline{K}$ . Nach Voraussetzung ist  $\phi(L) = L$ , insbesondere liegt  $b$  schon in  $L$  und damit zerfällt  $P$  über  $L$  schon vollständig. Also ist  $K \subset L$  normal.

Im Fall separabler Erweiterungen haben wir die Aussage schon in Satz 3.54 gezeigt.  $\square$

## 5. D T $\pi$

Die Zahl  $\pi$  ist für uns die kleinste positive reelle Zahl mit  $e^{i\pi} = -1$ .

**Satz 5.1** (Ferdinand von Lindemann, auf dem Freiburger Schloßberg, 1882). *Die Zahl  $\pi$  ist transzendent über  $\mathbb{Q}$ .*

Zum Beweis des Satzes brauchen wir Resultate über *symmetrische Polynome*.

**5.1. Symmetrische Polynome.** Sei  $R$  ein beliebiger Ring und  $R[X_1, \dots, X_n]$  der Polynomring über  $R$  in  $n$  Variablen. Sei  $\sigma \in S_n$ . So definiert  $\sigma$  einen Ringhomomorphismus  $\sigma: R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ , den wir ebenfalls mit  $\sigma$  bezeichnen, durch  $r \mapsto r$  für alle  $r \in R$  und  $X_i \mapsto X_{\sigma(i)}$ .

**Definition 5.2.** Ein Polynom  $P \in R[X_1, \dots, X_n]$  heißt *symmetrisch*, falls  $\sigma(P) = P$  gilt für alle  $\sigma \in S_n$ .

*Beispiel 5.3.*  $1, X_1 + X_2, X_1X_2 - 1 \in R[X_1, X_2]$  sind symmetrisch,  $X_1 - X_2, X_1 \in R[X_1, X_2]$  nicht.

Summen und Produkte symmetrischer Polynome sind symmetrisch. Wir bezeichnen mit  $R[X_1, \dots, X_n]^{S_n} \subset R[X_1, \dots, X_n]$  den Unterring der symmetrischen Polynome. Seien die Polynome  $s_1, \dots, s_n \in R[X_1, \dots, X_n]$  definiert durch folgende Gleichung im Ring  $R[X_1, \dots, X_n][T]$ :

$$(T - X_1) \cdots (T - X_n) = T^n - s_1 T^{n-1} + s_2 T^{n-2} \pm \dots \pm s_n.$$

Das Polynom links bleibt invariant unter Permutationen der  $X_i$ , folglich sind die Koeffizienten  $s_1, \dots, s_n$  rechts symmetrische Polynome. Man nennt sie die *elementarsymmetrischen Polynome*. Beispielsweise ist  $s_1 = X_1 + \dots + X_n$  und  $s_n = X_1 \cdots X_n$ .

**Satz 5.4.** *Jedes symmetrische Polynom läßt sich schreiben als Polynom in den elementarsymmetrischen Polynomen. Die elementarsymmetrischen Polynome sind algebraisch unabhängig über  $R$ . Es ist also*

$$R[X_1, \dots, X_n]^{S_n} = R[s_1, \dots, s_n].$$

(Rechts ist der Polynomring in den "Variablen"  $s_1, \dots, s_n$  gemeint, nicht nur der von den  $s_i$  erzeugte Unterring.)

*Beweis.* Natürlich ist der von  $s_1, \dots, s_n$  über  $R$  erzeugte Ring in der linken Seite enthalten. Wir müssen also die Umkehrung zeigen. Für ein  $n$ -Tupel  $\alpha = (i_1, \dots, i_n) \in \mathbb{N}^n$  natürlicher Zahlen sei  $X^\alpha = X_1^{i_1} \cdots X_n^{i_n}$ . Jedes Polynom  $P \in R[X_1, \dots, X_n]$  läßt sich dann schreiben als Summe  $P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha$  für eindeutig bestimmte  $c_\alpha \in R$ , und fast alle  $c_\alpha$  verschwinden.

Wir betrachten nun auf  $\mathbb{N}^n$  die lexikografische Anordnung, definiert durch

$$(i_1, \dots, i_n) \geq (j_1, \dots, j_n) \quad \text{falls } i_1 > j_1 \text{ oder } i_1 = j_1 \\ \text{und } (i_2, \dots, i_n) \geq (j_2, \dots, j_n).$$

Sei  $P \in R[X_1, \dots, X_n]^{S_n}$ ,  $P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \neq 0$  und sei  $\alpha = (i_1, \dots, i_n)$  der bzgl. unserer Anordnung maximale Index mit  $c_\alpha \neq 0$  (diesen nennen wir im folgenden Leitindex). Da  $P$  symmetrisch ist, gilt  $i_1 \geq i_2 \geq \dots \geq i_n$ . Das Polynom  $s_1^{i_1-i_2} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$  hat ebenfalls den Leitindex  $\alpha$  und ist symmetrisch. Dann hat  $P - c_\alpha s_1^{i_1-i_2} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$  kleineren Leitindex und ist ebenfalls symmetrisch. Da es keine unendlichen monoton abfallenden Folgen in der lexikographischen Anordnung gibt, können wir per Induktion annehmen, daß  $P - c_\alpha s_1^{i_1-i_2} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n} \in R[s_1, \dots, s_n]$ . Dann ist auch  $P \in R[s_1, \dots, s_n]$ .

Wir müssen noch zeigen, daß  $s_1, \dots, s_n$  algebraisch unabhängig sind über  $R$ . Ist nun eine Linearkombination von Monomen  $s_1^{m_1} \dots s_n^{m_n}$  gleich Null, so müssen alle Koeffizienten verschwinden, da diese Monome paarweise verschiedene Leitindizes haben. ( $s_1^{m_1} \dots s_n^{m_n}$  hat Leitindex  $(m_1 + \dots + m_n, m_2 + \dots + m_n, \dots, m_n)$ .)  $\square$

**5.2. Der Beweis des Satzes von Lindemann.** Wir nehmen an,  $\pi$  sei nicht transzendent, also algebraisch über  $\mathbb{Q}$ . Dann ist auch  $i\pi$  algebraisch und erfüllt damit eine polynomiale Gleichung  $Q(i\pi) = 0$  mit Koeffizienten in  $\mathbb{Q}$ . Die komplexen Nullstellen dieser Gleichung seien  $\alpha_1 = i\pi, \alpha_2, \dots, \alpha_m$ . Also ist  $\prod_{i=1}^m (X - \alpha_i) \in \mathbb{Q}[X]$ .

**Lemma 5.5.** *Ist  $P \in \mathbb{Q}[T_1, \dots, T_n]^{S_n}$  ein symmetrisches Polynom, so ist  $P(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$ .*

*Beweis des Lemmas.*  $P$  ist ein Polynom in den elementarsymmetrischen Polynomen, mit Koeffizienten in  $\mathbb{Q}$ . Setzen wir die  $\alpha_i$  aber in ein elementarsymmetrisches Polynom ein, erhalten wir eine rationale Zahl, da  $\prod_{i=1}^n (X - \alpha_i) \in \mathbb{Q}[X]$ .  $\square$

Wegen  $e^{\alpha_1} = -1$  ist

$$\begin{aligned} 0 &= (1 + e^{\alpha_1}) \dots (1 + e^{\alpha_n}) \\ &= 1 + e^{\alpha_1} + \dots + e^{\alpha_n} + e^{\alpha_1 + \alpha_2} + \dots + e^{\alpha_1 + \dots + \alpha_n} \\ &= 1 + e^{\gamma_1} + \dots + e^{\gamma_r}. \end{aligned}$$

Wir haben hier die  $\gamma_i$  durch Ausmultiplizieren erhalten, die  $\gamma_i$  sollen also alle Ausdrücke  $\alpha_1, \dots, \alpha_n, \alpha_1 + \alpha_2, \dots, \alpha_1 + \dots + \alpha_n$  durchlaufen.

Nun ist

$$\prod_{i=1}^r (X - \gamma_i) \in \mathbb{Q}[X],$$

denn die Koeffizienten dieses Polynoms sind symmetrisch in den  $\gamma_i$ , also auch symmetrisch in den  $\alpha_1, \dots, \alpha_n$ . Diese Aussagen führen wir nun zum Widerspruch.

**Satz 5.6.** *Es kann keine Zahlen  $\gamma_1, \dots, \gamma_r \in \mathbb{C}$  geben, so daß*

$$\prod_{i=1}^r (X - \gamma_i) \in \mathbb{Q}[X]$$

und

$$e^{\gamma_1} + \dots + e^{\gamma_r} \in \mathbb{Z}_{<0}.$$

*Beweis.* Wir können alle  $\gamma_i$ , die  $= 0$  sind, ignorieren und nehmen deshalb an, alle  $\gamma_i$  seien nicht Null. Sei  $c \in \mathbb{Z}$  so, daß  $\theta(X) := c \prod_{i=1}^r (X - \gamma_i) \in \mathbb{Z}[X]$ . Die Zahlen  $d = c\gamma_1 \dots \gamma_r \in \mathbb{Z}$  ( $d$  ist nicht Null) und  $f = e^{\gamma_1} + \dots + e^{\gamma_r} \in \mathbb{Z}_{<0}$  brauchen wir später.

Für beliebiges  $n \in \mathbb{N}$  setzen wir  $s = rn - 1$  und definieren

$$P(X) = P_n(X) = c^s X^{n-1} \frac{\theta(X)^n}{(n-1)!},$$

ein Polynom in  $\mathbb{Q}[X]$  vom Grad  $rn + n - 1 = s + n$ . Sei

$$F(X) = P(X) + P'(X) + P''(X) + \dots$$

Wir betrachten unsere Polynome nun als differenzierbare Abbildungen von  $\mathbb{R}$  nach  $\mathbb{R}$ . Um das zu kennzeichnen, schreiben wir von nun ab  $P(x)$  statt  $P(X)$ . Wir berechnen

$$\begin{aligned} \frac{d}{dx}(e^{-x}F(x)) &= -e^{-x}F(x) + e^{-x} \frac{d}{dx}F(x) \\ &= -e^{-x}(P(x) + P'(x) + \dots) + e^{-x}(P'(x) + P''(x) + \dots) \\ &= -e^{-x}P(x). \end{aligned}$$

Also ist, für alle  $x \in \mathbb{R}$ ,

$$- \int_0^x e^{-y}P(y)dy = e^{-x}F(x) - F(0).$$

Setzen wir  $y = \lambda x$  und multiplizieren mit  $e^x$ , so erhalten wir

$$F(x) - e^x F(0) = -xe^x \int_0^1 e^{-\lambda x} P(\lambda x) d\lambda.$$

Wir schließen, daß diese Identität auch für *komplexe*  $x \in \mathbb{C}$  gültig ist, da wir sie als Identität im Ring der Potenzreihen  $\mathbb{R}[[x]]$  lesen können. Nun setzen wir für  $x$  die Zahlen  $\gamma_1, \dots, \gamma_r$  ein und summieren. Es ergibt sich

$$\sum_{i=1}^r F(\gamma_i) - f \cdot F(0) = - \sum_{i=1}^r \gamma_i e^{\gamma_i} \int_0^1 e^{-\lambda \gamma_i} P(\lambda \gamma_i) d\lambda.$$

Strebt nun  $n$  gegen unendlich, so konvergiert der Ausdruck rechts gegen Null, da

$$\sup_{0 \leq \lambda \leq 1} |P(\lambda \gamma_i)| \leq \frac{\text{const}}{(n-1)!} \cdot \sup_{0 \leq \lambda \leq 1} \{(|\lambda \gamma_i| + 1)|\theta(\lambda \gamma_i)| + 1\}^n \xrightarrow{n \rightarrow \infty} 0.$$

Wir erhalten den gewünschten Widerspruch, wenn wir folgende Behauptung beweisen:

*Behauptung:* Ist  $n = p$  prim und genügend groß, so ist  $\sum_{i=1}^r F(\gamma_i) + f \cdot F(0)$  eine ganze Zahl ungleich Null.

*Begründung:* Wir zeigen zunächst, daß

$$\sum_{i=1}^r P^{(t)}(\gamma_i) \in n\mathbb{Z}$$

für alle  $t \in \mathbb{N}$ . Wenn wir  $P(X)$   $t$ -mal ableiten, erhalten wir ein Polynom in  $X$ ,  $\theta(X)$  und den Ableitungen von  $\theta$  nach der Produktregel. Wir können nach Potenzen von  $\theta(X)$  ordnen und erhalten

$$P^{(t)}(X) = Q_n \cdot \theta(X)^n + \dots + Q_1 \cdot \theta(X) + Q_0,$$

wobei die  $Q_i$  Polynome in  $X$  und den Ableitungen von  $\theta(X)$  sind. Ein Beitrag zu  $Q_0$  entsteht durch mindestens  $n$ -faches Ableiten von  $\theta(X)^n$ . Wir erkennen, daß  $Q_0 = n \cdot c^s \tilde{Q}_0$ , wobei  $\tilde{Q}_0$  ein Polynom in  $X$  mit *ganzzahligen* Koeffizienten ist.

Wegen  $\theta(\gamma_i) = 0$  ist

$$\sum_{i=1}^r P^{(t)}(\gamma_i) = \sum_{i=1}^r Q_0(\gamma_i) = nc^s \sum_{i=1}^r \tilde{Q}_0(\gamma_i).$$

Nun ist  $\sum_{i=1}^r \tilde{Q}_0(\gamma_i)$  ein symmetrisches Polynom in den  $\gamma_i$  mit ganzzahligen Koeffizienten. Der Grad von  $\tilde{Q}_0$  ist jedoch *höchstens*  $rn + n - 1 - n = s$ . Damit läßt sich  $\sum_{i=1}^r \tilde{Q}_0(\gamma_i)$  als Polynom mit  $\mathbb{Z}$ -Koeffizienten vom Grad höchstens  $s$  in den elementarsymmetrischen Polynomen der  $\gamma_1, \dots, \gamma_r$  schreiben. Setzen wir die  $\gamma_1, \dots, \gamma_r$  aber in ein elementarsymmetrisches Polynom ein, erhalten wir eine Zahl aus  $\frac{\mathbb{Z}}{c}$ . Also ist  $c^s \sum_{i=1}^r \tilde{Q}_0(\gamma_i)$  eine ganze Zahl und damit  $\sum_{i=1}^r P^{(t)}(\gamma_i) \in n\mathbb{Z}$ .

Nun betrachten wir  $F(0)$ . Es ist  $P^{(t)}(0) = 0$  für  $0 \leq t < n-1$ ,  $P^{(n-1)}(0) = c^s \theta(0)^n = d^n$ , und  $P^{(t)}(0) \in n\mathbb{Z}$ , falls  $n \leq t$ .

Insgesamt ist also

$$\sum_{i=1}^r F(\gamma_i) + f \cdot F(0) \in fc^s d^n + n\mathbb{Z}.$$

Wählen wir nun  $n = p$  prim und so groß, daß  $p$  weder  $c, d$  noch  $f$  teilt, so steht links eine nicht verschwindende, ganze Zahl. Das war unsere Behauptung.  $\square$

*Danksagung:* Ich danke allen Studenten, die mich auf Fehler jeglicher Natur im Skript aufmerksam gemacht haben. Fassung vom 15. März 2007.