Algebra

N. Perrin

Düsseldorf
Sommersemester 2014

Inhaltsverzeichnis

1 Gruppen

1.1 Wiederholung

1.1.1 Gruppen, Untergruppen

Definition 1.1.1 Eine **Gruppe** ist eine Menge G mit einer Verknüpfung $G \times G \to G$, $(x, y) \mapsto x \cdot y$ so, dass

1. Es existiert ein **neutrales Element** e in G mit $e \cdot x = x \cdot e = x$ für alle $x \in G$.
2. Die Verknüpfung ist **assoziativ** *i.e.* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in G$.
3. jedes $x \in G$ hat ein **inverses Element** $y \in G$ mit $x \cdot y = y \cdot x = e$.

Definition 1.1.2 Eine Gruppe G heißt **kommutativ** oder **abelsch** falls $x \cdot y = y \cdot x$ gilt für alle $x, y \in G$.

Beispiel 1.1.3 1. $\mathbb{Z}$ mit $+$ ist eine Gruppe.

2. Sei $n \in \mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} = \{\text{Restklassen modulo } n\}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ mit $+$ eine Gruppe.

3. Sei K ein Körper. Dann ist $\mathrm{GL}_n(K)$ mit Matrixmultiplikation eine Gruppe.

4. S_n die Permutationsgruppe mit $\circ$ der Komposition von Abbildungen als Verknüpfung ist eine Gruppe.

Lemma 1.1.4 Sei G eine Gruppe und seien x, y, z Elemente in G.

1. Das neutrale Element e_G ist eindeutig bestimmt.

2. Das inverse Element x^{-1} von x ist eindeutig bestimmt.

3. $xy = xz \Rightarrow y = z$ und $yx = zx \Rightarrow y = z$,

4. $(x^{-1})^{-1} = x$.

5. $(xy)^{-1} = y^{-1}x^{-1}$. □

Beweis. Siehe LAI. ■

Bemerkung 1.1.5 Sei $n \geq 0$ eine ganze Zahl. Aus 5. folgt per Induktion, dass $(x^n)^{-1} = (x^{-1})^n$. Wir schreiben x^{-n} für $(x^n)^{-1} = (x^{-1})^n$ also ist x^n für alle $n \in \mathbb{Z}$ definiert und es gilt $x^n x^m = x^{n+m}$ für alle $n, m \in \mathbb{Z}$.

Lemma 1.1.6 Seien G und G' zwei Gruppen und sei $(a, b) \cdot (a', b') = (aa', bb')$. Dann ist $G \times G'$ mit diesem Produkt eine Gruppe. □

Beweis. Übung. ■

Definition 1.1.7 Seien G und G' zwei Gruppen. Das Produkt $G \times G'$ mit Verknüpfung $(a, b) \cdot (a', b') = (aa', bb')$ heißt **Produkt-Gruppe** von G und G'.

Definition 1.1.8 Sei G eine Gruppe. Eine Teilmenge $H \subset G$ heißt **Untergruppe** von G falls gilt:

1. $1 \in H$,
2. $x, y \in H \Rightarrow x \cdot y^{-1} \in H$.

Lemma 1.1.9 Eine Untergruppe ist eine Gruppe. □

Beweis. Siehe LAI. ■

Beispiel 1.1.10 1. Sei G eine Gruppe. Dann ist $H = \{e_G\}$ die **Trivialuntergruppe** eine Untergruppe von G.

2. Sei $n \in \mathbb{Z}$. Dann ist $n\mathbb{Z} = \{m \in \mathbb{Z} \mid n \text{ teilt } m\}$ eine Untergruppe von $(\mathbb{Z}, +)$.

3. Sei K ein Körper. Dann ist $\mathrm{SL}_n(K)$ eine Untergruppe von $\mathrm{GL}_n(K)$.

1.1.2 Gruppenhomomorphismen

Definition 1.1.11 Seien G und G' zwei Gruppen. Eine Abbildung $f : G \to G'$ heißt **Gruppenhomomorphismus** falls für alle $x, y \in G$ gilt $f(xy) = f(x)f(y)$.

Beispiel 1.1.12 1. die Abbildung $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ ist ein Gruppenhomomorphismus.

2. Sei K ein Körper. Dann ist $\det : \mathrm{GL}_n(K) \to (K^\times, \times) = (K \setminus \{0\}, \times)$ ein Gruppenhomomorphismus.

Lemma 1.1.13 Sei $f : G \to G'$ ein Gruppenhomomorphismus dann gilt für alle $x \in G$

$$f(e_G) = e_{G'} \text{ und } f(x^{-1}) = f(x)^{-1}.$$

Beweis. Siehe LAI. ■

Definition 1.1.14 Sei $f : G \to G'$ ein Gruppenhomomorphismus, dann heißt die Teilmenge $\mathrm{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$ von G der **Kern** von f.

Lemma 1.1.15 Sei $f : G \to G'$ ein Gruppenhomomorphismus. Sei H eine Untergruppe von G und H' eine Untergruppe von G'.

1. Dann sind $f(H)$ und $f^{-1}(H')$ Untergruppen von G' und G.

2. Für $H' = \{e_{G'}\}$ ist $\mathrm{Ker}(f) = f^{-1}(H')$ eine Untergruppe von G.

3. Für $H = G$ ist das Bild $f(G)$ von f eine Untergruppe von G' □

Beweis. Siehe Übungsblatt 0. ■

Beispiel 1.1.16 Die Signatur $\varepsilon : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus. Wir Schreiben $A_n = \mathrm{Ker}\varepsilon$ für die **Alternierende Gruppe**. Die Gruppe A_n ist eine Untergruppe von S_n.

Lemma 1.1.17 Sei $f : G \to G'$ ein Gruppenhomomorphismus. Die Abbildung f ist genau dann injektiv, wenn $\mathrm{Ker}(f) = \{e_G\}$. □

Beweis. Siehe LAI. ■

Definition 1.1.18 Ein bijektiver Gruppenhomomorphismus $f : G \to G'$ heißt **Isomorphismus** oder **Gruppenisomorphismus**. Wenn $G' = G$ heißt ein Gruppenisomorphismus **Gruppenautomorphismus** oder **Automorphismus**.

Lemma 1.1.19 Sei G eine Gruppe und $g \in G$. Dann ist $\mathrm{Int}_g : G \to G$ definiert durch $\mathrm{Int}_g(h) = ghg^{-1}$ ein Gruppenautomorphismus. □

Beweis. Siehe Übungsblatt 0. ■

Definition 1.1.20 Sei G eine Gruppe und $g \in G$. Dann heißt Int_g **innerer Gruppenhomomorphismus** oder **Konjugation mit** g. Gruppenautomorphismen, die nicht dieser From sind heißen **äußere Automorphismen**.

1.1.3 Recht und Links Klassen

Definition 1.1.21 Sei G eine Gruppe und H eine Untergruppe. Man definiert die Relation $\sim$ durch

$$g' \sim g \Leftrightarrow \exists h \in H \text{ mit } g' = gh.$$

Lemma 1.1.22 Die Relation $\sim$ ist eine Äquivalenzrelation und die Klasse eines Element $g \in G$ ist die Teilmenge $\bar{g} = [g] = gH = \{gh \in G \mid h \in H\}$. Die Äquivalenzklassen heißen **Linksklassen**. □

Beweis. Siehe Übungsblatt 0. ∎

Definition 1.1.23 Sei G eine Gruppe und H eine Untergruppe.

1. Die Menge aller Äquivalenzklassen heißt **Quotient von G nach H** und ist G/H bezeichnet.

2. Die **kanonische Projektion** ist die Abbildung $G \to G/H$ definiert durch $g \mapsto \bar{g} = [g] = gH$.

Bemerkung 1.1.24 Analog kann man die Äquivalenzrelation $g' \sim_R g \Leftrightarrow \exists h \in H$ mit $g' = hg$ definieren. Die Äquivalenzklassen heißen **Rechtsklassen** $Hg = \{hg \in G \mid h \in H\}$ und die Menge aller Rechtsklassen ist $H\backslash G$. Man kann auch die kanonische Projektion $G \to H\backslash G$ durch $g \mapsto Hg$ definieren.

Satz 1.1.25 Sei G eine Gruppe und H eine Untergruppe von G.

1. Es gilt $gH \cap gH' \neq \emptyset \Rightarrow gH = g'H$ (m.a.W. $gH \neq g'H \Rightarrow gH \cap gH' = \emptyset$).

2. Es gilt $G = \bigcup_{gH \in G/H} gH$. □

Beweis. Siehe LAI. Wir geben trozdem einen Beweis.

1. Sei $gh \in gH \cap g'H$. Dann gibt es $h' \in H'$ mit $gh = g'h'$. Sei $gh'' \in gH$. Dann gilt $gh'' = ghh^{-1}h'' = g'h'h^{-1}h'' \in g'H$ also $gH \subset g'H$. Analog gilt $g'H \subset gH$.

2. Sei $g \in G$. Dann gilt $g \in gH$. Umgekehrt gilt $gH \subset G$. ∎

Korollar 1.1.26 (Satz von Lagrange) Es gilt $|G| = |G/H||H|$.

Beweis. Die Gruppe G ist die disjunkte Vereinnigung aller gH für $gH = \bar{g} \in G/H$ also gilt

$$|G| = \sum_{\bar{g} \in G/H} |gH|.$$

Aber die Abbildungen $gH \to g'H$ und $g'H \to gH$ definiert durch $a \mapsto g'g^{-1}a$ und $a \mapsto gg'^{-1}a$ sind inverse von einander. Es gilt also $|gH| = |g'H|$ für alle $g, g' \in G$ und insbesondere für $g' = e_G$ gilt $|gH| = |H|$. Daraus folgt $|G| = \sum_{\bar{g} \in G/H} |gH| = \sum_{\bar{g} \in G/H} |H| = |G/H||H|$. ∎

Definition 1.1.27 Sei G eine Gruppe und H eine Untergruppe von G.

1. Die **Ordnung** von G ist $|G|$ die Anzahl aller Elementen in G (die **Mächtigkeit** von G).

2. Der **Index** von H in G ist $[G : H] = |G/H|$.

Korollar 1.1.28 Sie G eine endliche Gruppe und H eine Untergruppe. Dann sind die Ordnung $|H|$ und der Index $[G : H]$ von H Teiler der Ordnung $|G|$ von G.

1.2 Normalteiler

Definition 1.2.1 Sei G eine Gruppe. Eine Untergruppe H von G heißt **Normalteiler** falls für alle $g \in G$ gilt $gHg^{-1} \subset H$. Man schreibt $H \triangleleft G$.

Bemerkung 1.2.2 Eine Untergruppe H ist genau dann ein Normalteiler wenn gilt $ghg^{-1} \in H$ für alle $g \in G$ und alle $h \in H$.

Lemma 1.2.3 Jede Untergruppe einer abelschen Gruppe G ist normal. □

Beweis. Klar. ■

Lemma 1.2.4 Eine Untergruppe H ist genau dann Normalteiler, wenn $gH = Hg$ für alle $g \in G$. □

Beweis. Siehe Übungsblatt 0. ■

Beispiel 1.2.5 1. Die triviale Untergruppe $\{e_G\}$ und die Gruppe G sind Normalteiler von G: $\{e_G\} \triangleleft G$ und $G \triangleleft G$.

2. $n\mathbb{Z} \triangleleft \mathbb{Z}$.

3. $\mathrm{SL}_n(K) \triangleleft \mathrm{GL}_n(K)$ aber $\mathrm{SO}_n(K) \not\triangleleft \mathrm{GL}_n(K)$.

Lemma 1.2.6 Sei $f : G \to G'$ ein Gruppenhomomorphismus und seien $H \triangleleft G$ und $H' \triangleleft G'$.

1. Dann ist $f^{-1}(H') \triangleleft G$. Insbesondere gilt $\mathrm{Ker} f \triangleleft G$.

2. Falls f sujektiv ist, gilt $f(H) \triangleleft G'$. □

Beweis. 1. Sei $g \in G$ und $h \in f^{-1}(H')$. Dann gilt $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$ also $ghg^{-1} \in f^{-1}(H')$.

2. Sei $g' \in G'$ und $h' \in f(H)$. Dann gibt es ein $h \in H$ mit $h' = f(h)$. Da f surjektiv ist gibt es ein $g \in G$ mit $f(g) = g'$. Dann gilt $g'h'g'^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}) \in f(H)$. ■

Satz 1.2.7 Sei $H \triangleleft G$. Dann ist die Verknüpfung $G/H \times G/H \to G/H$, $(\bar{g}, \bar{g}') \mapsto \overline{gg'}$ wohl definiert und G/H ist mit dieser Verknüpfung einer Gruppe. Außerdem ist die kanonische Projektion $G \to G/H$ ein Gruppenhomomorphismus. □

Beweis. Seien $a, b \in G$ mit $\bar{a} = \bar{g}$ und $\bar{b} = \bar{g}'$. Wir zeigen, dass $\overline{ab} = \overline{gg'}$. Sei $h \in H$ mit $a = gh$ und $h' \in H$ mit $b = g'h'$. Da $g'H = Hg'$ gibt es $h'' \in H$ mit $hg' = gh''$. Es gilt

$$\overline{ab} = abH = ghg'h'H = gg'h''h'H = gg'H = \overline{gg'}.$$

Die Verknüpfung ist also wohl definiert.

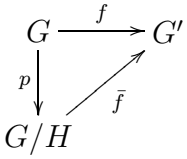
Es gilt $\bar{g}\bar{e}_G = \overline{ge_G} = \bar{g}$ und analog gilt $\bar{e}_G\bar{g} = \bar{g}$ also gilt $\bar{e}_G = e_{G/H}$. Es gilt $\bar{g}(\bar{g}'\bar{g}'') = \bar{g}\overline{g'b''} = \overline{g(g'g'')} = \overline{(gg')g''} = \overline{gg'}\bar{g}'' = (\bar{g}\bar{g}')\bar{g}''$. Es gilt $\bar{g}\overline{g^{-1}} = \overline{gg^{-1}} = \overline{e_G}$ und analog $\overline{g^{-1}}\bar{g} = \overline{e_G}$. Daraus folgt auch, dass die kanonische Projektion ein Guppenhomomorphismus ist. ∎

Definition 1.2.8 Sei H ein Normalteiler von G. Die Gruppe G/N heißt **Quotientgruppe** von G nach H.

Beispiel 1.2.9 Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist die Quotientgruppe von $\mathbb{Z}$ nach $n\mathbb{Z}$.

Satz 1.2.10 Sei $f : G \to G'$ ein Gruppenhomomorphismus, sei H ein Normalteiler von G und sei $p : G \to G/H$ die kanonische Projektion.

1. Es gibt ein eindeutig bestimmter Gruppenhomomorphismus $\bar{f} : G/H \to G'$ so, dass das Diagram



kommutiert, genau dann wenn $H \subset \mathrm{Ker}f$.

Angenommen $H \subset \mathrm{Ker}f$ und sei $\bar{f}$ wie in 1.

2. Die Abbildung $\bar{f}$ ist genau dann injektiv, wenn $H = \mathrm{Ker}f$.

3. Die Abbildung $\bar{f}$ ist genau dann surjektiv, wenn f surjektiv ist. □

Beweis. 1. Sei $\bar{f}$ wie oben und sei $h \in H$. Dann gilt $f(h) = \bar{f} \circ p(h)$. Aber $p(h) = [h] = hH = H = [e_G] = e_{G/H}$. Daraus folgt $f(h) = \bar{f}(e_{G/H}) = e_{G'}$ da $\bar{f}$ ein Gruppenhomomorphismus ist. Es folgt $H \subset \mathrm{Ker}f$.

Umgekehrt sei $H \subset \mathrm{Ker}f$. Sei $g \in G$, wir setzen $\bar{f}([g]) = f(g)$ (die ist die einzige Mögligkeit so, dass das Diagram kommutiert, dies zeigt, dass $\bar{f}$ eindeutig bestimt ist). Sei g' mit $[g'] = [g]$. Es gibt $h \in H$ mit $g' = gh$ und es gilt $f(g') = f(gh) = f(g)f(h) = f(g)e_{G'} = f(g)$. Also ist die Abbildung $\bar{f}$ wohl definiert. Außerdem gilt $\bar{f}([g][g']) = \bar{f}([gg']) = f(gg') = f(g)f(g') = \bar{f}([g])\bar{f}([g'])$ und $\bar{f}$ ist ein Gruppenhomomorphismus. Darüber hinaus gilt $\bar{f} \circ p(g) = \bar{f}([g]) = f(g)$ und das Diagram ist kommutativ.

2. Sei $\bar{f}$ injektiv. Dann gilt $\mathrm{Ker}\bar{f} = \{e_{G/H}\}$. Sei $g \in \mathrm{Ker}f$. Es gilt $\bar{f}([g]) = e_{G'}$ also $[g] \in \mathrm{Ker}\bar{f}$ und da $\bar{f}$ injetiv ist, gilt $[g] = e_{G/H}$. Es folgt $gH = [g] = e_{G/H} = H$ und $g \in H$. Also $\mathrm{Ker}f \subset H$ und da $H \subset \mathrm{Ker}f$ folgt $H = \mathrm{Ker}f$.

Umgekehrt sei $H = \mathrm{Ker}f$ und sei $[g] \in \mathrm{Ker}\bar{f}$. Es gilt $f(g) = \bar{f}([g]) = e_{G'}$ also $g \in \mathrm{Ker}f = H$. Es folgt $[g] = H = e_{G/H}$ und $\bar{f}$ ist injektiv.

3. Sei f surjektiv und sei $g' \in G'$. Dann gibt es $g \in G$ mit $f(g) = g'$. Es gilt $\bar{f}([g]) = f(g) = g'$ also ist $\bar{f}$ auch surjektiv.

Umgelehrt, sei $\bar{f}$ surjektiv und sei $g' \in G'$. Es gibt $[g] \in G/H$ mit $\bar{f}([g]) = g'$. Daraus folgt $f(g) = \bar{f}([g]) = g'$ und f ist surjektiv. ∎

Korollar 1.2.11 Sei $f : G \to G'$ ein surjektiver Gruppenhomomorphismus. Dann gilt $G/\mathrm{Ker}f \simeq G'$.

Beispiel 1.2.12 1. Es gilt $\mathrm{GL}_n(k)/\mathrm{SL}_n(K) \simeq k^\times$ (der Kernel des surjektiven Gruppenhomomorphismus $\det : \mathrm{GL}_n(k) \to k^\times$ ist $\mathrm{SL}_n(k)$).

2. Es gilt $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$ (der Kernel des surjektiven Gruppenhomomorphismus $|\cdot| : \mathbb{C}^\times \to \mathbb{R}_{>0}$ ist S^1).

3. Es gilt $\mathbb{R}/\mathbb{Z} \simeq S^1$ (der Kernel des surjektiven Gruppenhomomorphismus $r \mapsto e^{2i\pi r}$ ist $\mathbb{Z}$).

4. Es gilt $S_n/A_n \simeq \{\pm 1\}$ (der Kernel des surjektiven Gruppenhomomorphismus $\varepsilon : S_n \to \{\pm 1\}$ ist A_n).

Definition 1.2.13 Ein Diagramm $1 \longrightarrow H \xrightarrow{i} G \xrightarrow{f} G' \longrightarrow 1$ heißt **exakte Sequenz**,

- wenn alle Abbildungen Gruppenhomomorphismen sind,
- wenn i injektiv ist,
- wenn f surjektiv ist und
- wenn $i(H) = \mathrm{Ker}f$.

Bemerkung 1.2.14 Falls $1 \longrightarrow H \xrightarrow{i} G \xrightarrow{f} G' \longrightarrow 1$ eine exakte Sequenz ist, gilt $G' \simeq G/H$.

Beispiel 1.2.15 Es gibt (Siehe Übungsblatt 1) eine exakte Sequenz

$$1 \to A_3 \simeq \mathbb{Z}/3\mathbb{Z} \to S_3 \to \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \to 1.$$

Definition 1.2.16 Eine Gruppe G heißt **einfach** falls G und $\{e_G\}$ die einzige Normalteiler von G sind.

Beispiel 1.2.17 1. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist genau dann einfach, wenn p eine Primzahl ist (Siehe Übungsblatt 1).

2. Später zeigen wir, dass die Gruppe $A_n = \mathrm{Ker}(\varepsilon : S_n \to \{\pm 1\})$ einfach für $n \geq 5$ ist.

Definition 1.2.18 Sei G eine Gruppe und H eine Untergruppe. Der **Normalisator** $N_G(H)$ von H in G ist

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Lemma 1.2.19 Sei G eine Gruppe und H eine Untergruppe.

1. Der Normalisator $N_G(H)$ ist eine Untergruppe von G.

2. Es gilt $H \triangleleft N_G(H)$ (also H ist Normalteiler in $N_G(H)$).

3. Sei K eine Untergruppe von G mit $H \triangleleft K$. Dann gilt $K \subset N_G(H)$ (*i.e.* $N_G(H)$ ist die größte Untergruppe von G mit $H \triangleleft N_G(H)$). □

Beweis. 1. Es gilt $e_G H e_G^{-1} = e_G H e_G = H$ also $e_G \in N_G(H)$. Seien $a, b \in N_G(H)$. Dann gilt $aHa^{-1} = H$ und $bHb^{-1} = H$ also $b^{-1}Hb = H$. Daraus folgt

$$(ab^{-1})H(ab^{-1})^{-1} = ab^{-1}Hba^{-1} = aHa^{-1} = H$$

und $ab^{-1} \in N_G(H)$ und $N_G(H)$ ist eine Untergruppe von G.

2. Klar.

3. Sei K eine Untergruppe mit $H \triangleleft K$. Sei $k \in K$. Dann gilt $kH^{-1} \subset K$. Da K eine Gruppe ist gilt auch $k^{-1} \in K$ also $k^{-1}Hk \subset H$ und mit Linksmultiplikation mit k und Rechtsmultiplikation mit k^{-1} folgt $H \subset kHk^{-1}$. Daraus folgt $kHk^{-1} = H$ und $k \in N_G(H)$. ■

Beispiel 1.2.20 Sei $G = S_3$ und sei $H = \{(123) = \mathrm{Id}, (213)\}$ und $A_3 = \{(123) = \mathrm{Id}, (231), (312)\}$. Dann sind H und A_3 Untergruppe von G und es gilt (siehe Übungsblatt 1)

$$N_G(H) = H \text{ und } N_G(A_3) = S_3.$$

Satz 1.2.21 (Erster Isomorphiesatz) Sei G eine Gruppe, $H \triangleleft G$ ein Normalteiler von G und $K \subset G$ eine Untergruppe von G.

1. Dann gilt $HK = KH$, $KH \subset G$ ist eine Untergruppe, $H \triangleleft KH$ und $K \cap H \triangleleft K$.

2. Die Abbildung $f : K/(K \cap H) \to KH/H$ definiert durch $k(K \cap H) \mapsto kH$ ist ein Isomorphismus also

$$K/(K \cap H) \simeq KH/H.$$

Beweis. 1. Sei $h \in H$ und $k \in K$. Da H ein Normalteiler ist, gilt $khk^{-1} \in H$ und es folgt $kh \in Hk \subset HK$. Daraus folgt $KH \subset HK$. Analog gilt $k^{-1}hk \in H$ und $hk \in kH \subset KH$. Daraus folgt $HK \subset KH$ und $KH = HK$.

Da $e_G \in H$ und $e_G \in K$ gilt $e_G \in KH$. Seien $k, k' \in K$ und $h, h' \in H$ so, dass $kh, k'h' \in KH$. Es gilt $kh(k'h')^{-1} = khh'^{-1}k'^{-1} \in KHK = KKH = KH$. Daraus folgt, dass KH eine Untergruppe ist.

Da H ein Normalteiler ist, gilt $gHg^{-1} \subset H$ für alle $g \in G$. Insbesondere für alle $g \in KH$ und es folgt $H \triangleleft KH$.

Sei $g \in H \cap K$ und $k \in K$. Es gilt $kgk^{-1} \in K$ und da H ein Normalteiler ist, gilt auch $kgk^{-1} \in H$. Also $kgk^{-1} \in H \cap K$ und $H \cap K \triangleleft K$.

2. Sei $f : K \to KH/H$ die Abbildung definiert durch $f(k) = kH$. Seien $k, k' \in K$. Es gilt $f(kk') = kH \cdot k'H = kk'H = f(kk'$ also ist f ein Gruppenhomomorphismus. Seien $k \in K$ und $h \in H$. Dann gilt $f(k) = kH = khH$ und f ist surjektiv. Sei $k \in K \cap H$. Dann gilt $f(k) = kH = H = e_{KH/H}$ also $H \cap K \subset \mathrm{Ker}f$. Sei $k \in K\mathrm{Ker}f$. Dann gilt $kH = f(k) = H$ und $k \in H$ also $k \in K \cap H$. Es folgt $H \cap K = \mathrm{Ker}f$. Nach Korollar 1.2.11 folgt, dass $K/(H \cap K) \simeq KH/H$. ∎

Satz 1.2.22 (Zweiter Isomorphiesatz) Sei G eine Gruppe und seien $H \triangleleft G$ und $K \triangleleft G$ mit $K \subset H$.

1. Dann gilt $K \triangleleft H$ und $H/K \triangleleft G/K$.

2. Die Abbildung $f : (G/K)/(H/K) \to G/H$ definiert durch $gK \cdot H/K \mapsto gH$ ist ein Isomorphismus also

$$(G/K)/(H/K) \simeq G/H.$$

Beweis. 1. Sei $h \in H \subset G$. Da $K \triangleleft G$ gilt $hKh^{-1} = K$ und $K \triangleleft H$.

Die Teilmenge $H/K \subset G/K$ ist $\pi_K(H)$, wobei $\pi : G \to G/K$ die kanonische Projektion ist. Da $H \triangleleft G$ und π surjektiv folgt, dass $H/K \triangleleft G/K$.

2. Die kanonische Projektion $\pi_H : G \to G/H$ ist ein surjektiver Gruppenhomomorphismus und es gilt $K \subset H = \mathrm{Ker}\pi_H$. Daraus folgt, dass es ein surjektiver Gruppenhomomorphismus $F = \bar{\pi}_H : G/K \to G/H$ gibt mit $\pi_H = \pi_K \circ F$ also $F([g]_K) = [g]_H$.

Wir zeigen, dass $\mathrm{Ker}F = H/K$. Daraus folt, dass es ein Gruppenisomorphismus $\bar{F} : (G/K)/(H/K) \to G/H$ gibt mit $\bar{F}([[g]_K]_{H/K}) = [g]_H$. Sei $[g]_K \in \mathrm{Ker}F$. Dann gilt $[e_G]_H = F([g]_K) = [g]_H$ also $g \in H$ und $[g]_K \in H/K$. Umgekehrt, sei $[g]_K \in H/K$ also $[g]_K = [h]_K$ für ein $h \in H$ *i.e.* es gibt ein $k \in K$ mit $g = hk$. Da $K \subset H$ gilt $g \in H$. Daraus folgt $[g]_H = [e_G]_H$ und $F([g]_K) = [g]_H = [e_G]_H$ also $[g]_K \in \mathrm{Ker}F$. Umgekehrt, sei $[g]_K \in \mathrm{Ker}F$. Es gilt $[g]_H = F([g]_K) = [e_G]_H$ also $g \in H$. Daraus folgt $[g]_K \in H/K$. ∎

1.3 Zentrum

Definition 1.3.1 Sei G eine Gruppe.

1. **Das Zentrum** einer Gruppe G ist die Menge

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

2. Sei $X \subset G$ eine Teilmenge. Der **Zentralisator** von G ist die Teilmenge

$$Z_G(X) = \{g \in G \mid gx = xg \text{ für alle } x \in X\}.$$

Bemerkung 1.3.2 Es gilt $Z(G) = Z_G(G)$.

Beispiel 1.3.3 1. Sei G eine kommutative Gruppe. Dann gilt $Z(G) = G$.

2. Sei $G = S_n$. Dann gilt $Z(S_n) = \{\mathrm{Id}\}$ (Siehe Übungsblatt 2) für $n \geq 3$.

Lemma 1.3.4 Sei G eine Gruppe und $X \subset G$ eine Teilmenge.

1. Der Zentralisator $Z_G(X)$ ist eine Untergruppe.

2. Das Zentrum $Z(G)$ ist ein Normalteiler von G und $Z_G(X)$ und ist abelsch.

3. Es gilt $G/Z(G) \simeq \{\text{innere Automorphismen}\}$.

4. Falls $G/Z(G)$ zyklisch ist (siehe Definition 1.4.2 unten), gilt $G = Z(G)$ also G ist abelsch. □

Beweis. 1. Es gilt $e_G x = x e_G$ für alle $x \in G$ also ist $e_G \in Z_G(X)$. Seien $g, h \in Z_G(X)$. Es gilt $gx0xg$ und $hx = xh$ für alle $x \in X$. Daraus folgt $xh^{-1} = h^{-1}x$ für alle $x \in X$ und $xgh^{-1} = gxh^{-1} = gh^{-1}x$ *i.e.* $gh^{-1} \in Z_G(X)$.

2. Nach der Definition gilt $Z(G) \subset Z_G(X)$. Sei $z \in Z(G)$ und $g \in G$. Es gilt $gzg^{-1} = gg^{-1}z = z$ also $gzg^{-1} \in Z(G)$. Daraus folgt, dass $Z(G)$ ein Normalteiler in G und $Z_G(X)$ ist. Seien $z, z' \in Z(G)$. Es gilt $zz' = z'z$ also $Z(G)$ ist abelsch.

3. Sei $f : G \to \{\text{innere Automorphismen}\}$ definiert durch $f(g) = \mathrm{Int}_g$. Diese Abbildung ist surjectiv und es gilt $f(gh) = \mathrm{Int}_{gh} = \mathrm{Int}_g \circ \mathrm{Int}_h$ (es gilt $\mathrm{Int}_g \circ \mathrm{Int}_h(g') = \mathrm{Int}_g(hg'h^{-1} = ghg'h^{-1}g^{-1} = (gh)g'(gh)^{-1} = \mathrm{Int}_{gh}(g'))$. Die Abbildung ist also ein surjektiver Gruppenhomomorphismus. Sei $g \in \mathrm{Ker}(f)$. Es gilt $\mathrm{Int}_g = \mathrm{Id}$ also $\mathrm{Int}_g(h) = h$ für alle $h \in G$. Dies ist äquivalent zu $ghg^{-1} = h$ für alle $h \in H$ und auch zu $gh = hg$ für alle $h \in G$. Also $\mathrm{Ker}(f) = Z(G)$.

4. Seien $g, h \in G$ und sei $\pi : G \to G/Z(G)$ die kanonische projektion. Da $G/Z(G)$ zyklisch ist gibt es ein $a \in G$ mit $G/Z(G) = \langle [a] \rangle$. Insbesondere gibt es $n, m \in \mathbb{Z}$ mit $[g] = [a]^n$ und $[h] = [a^m]$. Es gibt also $z, z' \in Z(G)$ mit $g = a^n z$ und $h = a^m z'$. Daraus folgt $gh = a^n z a^m z' = a^m z' a^n z = hg$ und G ist kommutativ. ■

1.4 Erzeuger und Zyklische Gruppe

Lemma 1.4.1 Sei G eine Gruppe.

1. Sei $(H_i)_{i \in I}$ eine Familie von Untergruppen von G. Dann ist $\bigcap_{i \in I} H_i$ eine Untergruppe von G.

2. Sei A eine Teilmenge von G. Dann gibt es eine kleinste Untergruppe H mit $A \subset H$. □

Beweis. 1. Siehe Übungsblatt 1.

2. Sei $(H_i)_i$ die Familie aller Untergruppen von G die A enthalten (diese Familie ist nicht leer da G eine solche Gruppe ist). Dann ist $H = \bigcap_{i\in I} H_i$ die minimale Untergruppe die A enthält ∎

Definition 1.4.2 1. Sei G eine Gruppe und A eine Teilmenge von G. Die kleinste Untergruppe die A enthält heißt **die von A erzeugte Untergruppe** und ist $\langle A\rangle$ geschrieben. Falls A nur einelementig ist: $A = \{g\}$ schreibt man $\langle A\rangle = \langle g\rangle$.

2. Eine Teilmenge A einer Gruppe G heißt **erzeugend** (man sagt auch A **erzeugt** G) falls $G = \langle A\rangle$.

3. Eine Gruppe G heißt **zyklisch** falls es ein Element $g \in G$ gibt mit $G = \langle g\rangle$.

Beispiel 1.4.3 1. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch und 1 erzeugt $\mathbb{Z}$.

2. Sei $n \in \mathbb{Z}$. Die Gruppe $(\mathbb{Z}/n, +)$ ist zyklisch und $\bar{1}$ erzeugt $\mathbb{Z}/n\mathbb{Z}$.

3. Die einfache Transpositionen $(s_i)_{i\in[1,n-1]}$ definiert durch

$$s_i(k) = \begin{cases} k & \text{für } k \notin \{i, i+1\} \\ i+1 & \text{für } k = i \\ i & \text{für } k = i+1 \end{cases}$$

erzeugen S_n *i.e.* $S_n = \langle s_i \mid i \in [1, n-1]\rangle$ (Siehe LAII).

Lemma 1.4.4 Sei G eine Gruppe und $g \in G$. Es gilt $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$. □

Beweis. Sei $n \in \mathbb{Z}$. Da $\langle g\rangle$ eine Gruppe ist und enthält g, gilt $g^{-1} \in \langle g\rangle$ und $g^n \in \langle g\rangle$ also $\{g^n \mid n \in \mathbb{Z}\} \subset \langle g\rangle$.

Umgekehrt, seien $n, m \in \mathbb{Z}$. Dann ist $(g^n)(g^m)^{-1} = g^{n-m} \in \{g^n \mid n \in \mathbb{Z}\}$ und $e_G = g^0 \in \{g^n \mid n \in \mathbb{Z}\}$. Daraus folt, dass $\{g^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G ist und enthält g. Also $\langle g\rangle \subset \{g^n \mid n \in \mathbb{Z}\}$. ∎

Satz 1.4.5 Sei G eine zyklische Gruppe. Dann ist G isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$. □

Beweis. Sei $g \in G$ so, dass $G = \langle g\rangle$. Sei $f : \mathbb{Z} \to G$ definiert durch $f(n) = g^n$. Dies ist ein Gruppenhomomorphismus und nach dem obigen Lemma folgt $f(\mathbb{Z}) = G$. Falls f injektiv ist, ist f ein Isomorphismus und $G \simeq \mathbb{Z}$. Sonst sei $N = \mathrm{Ker} f$. Dann ist N eine Untergruppe von $\mathbb{Z}$ und es folgt $N = n\mathbb{Z}$ für eine $n \in \mathbb{Z}$ (Siehe Übunsblatt 0 oder im Beweis von Korollar 1.4.7). Es folgt (nach Korollar 1.2.11) $G = \mathbb{Z}/N = \mathbb{Z}/n\mathbb{Z}$. ∎

Korollar 1.4.6 Sei p eine Primzahl und G eine Gruppe mit $|G| = p$.

1. Sei $g \in G$ mit $g \neq e_G$. Dann gilt $G \simeq \langle g\rangle$.

2. Es gilt $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Beweis. 1. Sei $H = \langle g \rangle$. Dann gilt $e_G, g \in H$ also $|H| \geq 2$. Nach dem Satz von Lagrange gilt $|H|$ teilt p also $|H| = p = |G|$ und $H = G$.

2. Folgt vom obigen Satz. ∎

Korollar 1.4.7 Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis. Die Gruppe G ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$. Es wurde im Übungsblatt 0 gezeigt, dass die Untergruppen zyklisch sind. Wir geben dennoch einen Beweis.

Angenommen $G = \mathbb{Z}$. Sei H eine Untergruppe von $\mathbb{Z}$. Falls $H = \{0\}$ sind wir fertig. Sonst ist $H \cap \mathbb{Z}_{>0} \neq \emptyset$. Sei $m = \min\{r \in H \mid r > 0\}$. Sei $n \in H$. Dann gibt es $k \in \mathbb{Z}$ und $r \in [0, m-1]$ mit $n = km + r$. Da H eine Gruppe ist gilt $r = n - km \in H$ und da m minimal war, gilt $r = 0$. Daraus folgt $H = m\mathbb{Z}$.

Sei $G = \mathbb{Z}/n\mathbb{Z}$ und sei H eine Untergruppe von G. Sei $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = G$ die kanonische Projektion. Dann ist $\pi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$ also gibt es ein $m \in \mathbb{Z}$ mit $\pi^{-1}(H) = m\mathbb{Z}$. Da die kanonische Projektion surjektiv ist, folgt $H = \pi(\pi^{-1}(H)) = \pi(m\mathbb{Z}) = \{k[m] = [mk] \in \mathbb{Z}/n\mathbb{Z}\}$. ∎

1.5 Ordung eines Elements

Definition 1.5.1 Sei G eine Gruppe und $g \in G$. Die **Ordnung** $\mathrm{ord}(g)$ von g ist die Ordung der Gruppe $\langle g \rangle$.

Lemma 1.5.2 Es gilt $\{k \in \mathbb{Z}_{\geq 0} \mid g^k = e_G\} = \mathrm{ord}(g)\mathbb{Z}$ (wir setzen $\infty\mathbb{Z} = \{0\}$). □

Beweis. Nach Satz 1.4.5 ist die Gruppe $\langle g \rangle$ isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$.

Im ersten Fall gilt $\mathrm{ord}(g) = \infty$ und im zweiten Fall gilt $\mathrm{ord}(g) = n$. Außerdem ist die Abbildung $\mathbb{Z} \to \langle g \rangle$ bzw. $\mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ definiert durch $k \mapsto g^k$ bzw. $[k] \mapsto g^k$ ein Isomorphismus.

Im ersten Fall gilt $\{k \in \mathbb{Z}_{\geq 0} \mid g^k = e_G\} = \{0\}$. Im zweiten Fall gilt $\{k \in \mathbb{Z} \mid g^k = e_G\} = \{k \in \mathbb{Z} \mid [k] = 0 \in \mathbb{Z}/n\mathbb{Z}\} = n\mathbb{Z}$. ∎

Lemma 1.5.3 Sei G eine Gruppe und $g \in G$ mit $\mathrm{ord}(g) = n < \infty$. Dann gilt

$$\mathrm{ord}(g^m) = \frac{n}{\mathrm{ggT}(m, n)}$$

für alle $m \in \mathbb{Z}$. □

Beweis. Seien $d = \mathrm{ggT}(m, n)$, $m' = \frac{m}{d} \in \mathbb{Z}$ und $n' = \frac{n}{d} \in \mathbb{Z}$. Sei $s = \mathrm{ord}(g^m)$. Es gilt $g^{ms} = (g^m)^s = e_G$. Also gibt es $k \in \mathbb{Z}$ mit $ms = kn$. Es folgt $m's = n'k$. Da $\mathrm{ggT}(m', n') = 1$ folgt $n' | s$.

Es gilt $(g^m)^{n'} = g^{mn'} = g^{m'dn'} = g^{m'n} = (g^n)^{m'} = e_G$. Daraus folgt $s | n'$. Insgesamt folgt $s = n'$. ∎

Korollar 1.5.4 Die erzeugende Elemente von $\mathbb{Z}/n\mathbb{Z}$ sind die Klassen $[m] \in \mathbb{Z}/n\mathbb{Z}$ mit $\mathrm{ggT}(m,n) = 1$.

Beweis. Sei $[m] \in \mathbb{Z}/n\mathbb{Z}$ mit $\mathbb{Z}/n\mathbb{Z} = \langle [m] \rangle$. Dann gilt $[m] = m[1]$ und $\mathrm{ord}([1]) = n$. Daraus folgt $\mathrm{ord}(m) = n/\mathrm{ggT}(m,n)$.

Die Klasse $[m]$ ist aber genau dann erzeugend, wenn $\mathrm{ord}([m]) = n$ also $n/\mathrm{ggT}(m,n) = n$ *i.e.* $\mathrm{ggT}(m,n) = 1$. ∎

Beispiel 1.5.5 Die erzeugende Klassen in $\mathbb{Z}/4\mathbb{Z}$ sind $[1]$ und $[3]$.

Korollar 1.5.6 Sei $n \in \mathbb{Z}$. Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ hat für jedes $m|n$ genau eine Untergruppe der Ordnung m: die Gruppe

$$m\mathbb{Z}/n\mathbb{Z} = \{[km] \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

Beweis. Dies wurde im Übungsblatt 0 bewiesen. Wir geben dennoch einen Beweis. Sei H eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ und sei $d = \min\{k \in \mathbb{Z}_{>0} \mid [k] \in H\}$. Da $[0] = [n] \in H$ gilt $0 < d \leq n$. Sei $[k] \in H$. Wir schreiben $k = da + b$ mit $a, b \in \mathbb{Z}$ und $b \in [0, d-1]$. Es gilt $[k], [d] \in H$ also $[b] = [k] - a[d] \in H$. Da d minimal ist, folgt $b = 0$ und $k \in d\mathbb{Z}$. Es folgt $H = d\mathbb{Z}/n\mathbb{Z} = \{[kd] \in \mathbb{Z}/n\mathbb{Z} \mid k \in \mathbb{Z}\} = \langle [d] \rangle$. Außerdem gilt $\mathrm{ord}([d]) = \frac{n}{\mathrm{ggT}(n,d)} = \frac{n}{d} := m$. ∎

1.6 Derivierte Untergruppe

Definition 1.6.1 Sei G eine Gruppe, seien $g, h \in G$ und seien $H, K \subset G$ Untergruppen.

1. Der **Kommutator** von g und h ist $[g,h] = ghg^{-1}h^{-1}$.

2. **Der Kommutator** $[H,K]$ von H und K ist die Gruppe $[H,K] = \langle [h,k] \mid h \in H \text{ und } k \in K \rangle$.

3. **Die derivierte Gruppe** $D(G)$ von G ist die Gruppe $D(G) = [G,G]$ (manchmal wird $D(G)$ auch (G,G) bezeichnet).

Lemma 1.6.2 Sei G eine Gruppe.

1. $D(G) = \{[g_1,h_1] \cdots [g_n,h_n] \mid n \in \mathbb{Z}_{\geq 0} \text{ und } g_i, h_i \in G\}$.

2. $D(G)$ ist eine Normalteiler in G.

3. $G/D(G)$ ist abelsch.

4. Sei $N \triangleleft G$ mit G/N abelsch. Dann gilt $D(G) \subset N$. Also ist $D(G)$ die kleinste Untergruppe so, dass $G/D(G)$ abelsch ist. □

Beweis. 1. Sei $H = \{[g_1, h_1] \cdots [g_n, h_n] \mid n \in \mathbb{Z}_{\geq 0} \text{ und } g_i, h_i \in G\}$. Es gilt $H \subset D(G)$. Wir zeigen, dass H eine Untergruppe ist. Alle Produkte von Elementen aus H sind noch in H. Es gilt $[g,h]^{-1} = [h,g]$ also ist das Inverses jedes Element aus H noch in H und H ist eine Untergruppe. Daraus folgt $D(G) \subset H$ da $D(G)$ die kleinste Untergruppe die alle Kommutatoren enthält ist.

2. Seien $g, h, k \in G$. Es gilt $k[g,h]k^{-1} = [kgk^{-1}, khk^{-1}]$. Daraus folgt $k[g,h]k^{-1} \in D(G)$ und nach 1. $kD(G)k^{-1} \subset D(G)$.

3. Seien $g, h \in G$. Dann gilt $[ghg^{-1}h^{-1}] = e$ in $G/D(G)$ also $[g][h] = [h][g]$ und $G/D(G)$ ist abelsch.

4. Seien $g, h \in G$. Es gilt $[ghg^{-1}h^{-1}]_N = [g]_N[h]_N[g]_N^{-1}[h]_N^{-1} = [e_G]_N$ da G/N abelsch ist. Daraus folgt $ghg^{-1}h^{-1} \in N$ und $D(G) \subset N$. ∎

1.7 Semidirekte Produkte

Lemma 1.7.1 Seien N und H zwei Gruppen und sei $\Phi : H \to \mathrm{Aut}(N), h \mapsto \Phi_h$ ein Gruppen homomorphismus (wobei $\mathrm{Aut}(N)$ die Gruppe aller Automorphismen von N ist).

Sei $N \rtimes H := N \times_\Phi H := (N \times H, \star)$ mit

$$(n,h) \star (n',h') = (n\Phi_h(n'), hh').$$

Dann ist $N \rtimes H$ eine Gruppe mit neutralem Element (e_N, e_H) und Inverse $(n,h)^{-1} = (\Phi_{h^{-1}}(n^{-1}), h^{-1})$. □

Beweis. Es gilt $(e_N, e_H)\star(n,h) = (e_N\Phi_{e_H}(n), e_Hh) = (\mathrm{Id}_N(n), h) = (n,h)$ und $(n,h)\star(e_N, e_H) = (n\Phi_h(e_N), he_H) = (n,h)$.

Es gilt $(n,h) \star (\Phi_{h^{-1}}(n^{-1}), h^{-1}) = (n\Phi_h(\Phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n\Phi_{hh^{-1}}(n^{-1}), e_H) = (n\mathrm{Id}_N(n^{-1}), e_H) = (nn^{-1}, e_H) = (e_N, e_H)$. Es gilt auch $(\Phi_{h^{-1}}(n^{-1}), h^{-1}) \star (n,h) = (\Phi_{h^{-1}}(n^{-1})\Phi_{h^{-1}}(n), h^{-1}h) = (\Phi_{h^{-1}}(n^{-1}n), e_H) = (\Phi_{h^{-1}}(e_G), e_H) = (e_N, e_H)$.

Es gilt

$$\begin{aligned}(n,h) \star ((n',h') \star (n'',h'')) &= (n,h) \star (n'\Phi_{h'}(n''), h'h'') \\ &= (n\Phi_h(n'\Phi_{h'}(n'')), hh'h'') \\ &= (n\Phi_h(n')\Phi_{hh'}(n''), hh'h'') \\ &= (n\Phi_h(n'), hh') \star (n'', h'') \\ &= ((n,h) \star (n',h')) \star (n'',h'')\end{aligned} \quad .$$

Daraus folgt, dass $N \rtimes H$ eine Gruppe ist. ∎

Definition 1.7.2 Seien N und H zwei Gruppen und sei $\Phi : H \to \mathrm{Aut}(N), h \mapsto \Phi_h$ ein Gruppen homomorphismus. Das heißt die Gruppe $N \rtimes H := N \times_\Phi H := (N \times H, \star)$ mit Produkt $(n,h) \star (n',h') = (n\Phi_h(n'), hh')$ **semidirektes Produkt von N und H bzg. Φ.**

Beispiel 1.7.3 Sei $\Phi : H \to \mathrm{Aut}(N)$ definiert durch $\Phi_h = \mathrm{Id}_N$ für alle $h \in H$. Dann gilt

$$(n,h) \star (n',h') = (n\Phi_h(n'), hh') = (n\mathrm{Id}_N(n'), hh') = (nn', hh')$$

und das semidirekte Produkt ist die Produktgruppe.

Lemma 1.7.4 Sei $G = N \rtimes H$ und seien $N' = \{(n, e_H) \mid n \in N\}$ und $H' = \{(e_N, h) \mid h \in H\}$.

1. Dann ist H' eine Untergruppe von G und $N' \lhd G$.

2. Es gibt isomorphismen $N \simeq N'$ und $H \simeq H'$ definiert durch $n \mapsto (n, e_H)$ und $h \mapsto (e_N, h)$.

3. Es gilt $N' \cap H' = \{e_G\}$ und $G = N'H'$. □

Beweis. 1. Die Abbildung $\pi : G \to H$ definiert durch $\pi(h)$ ist ein Gruppenhomomorphismus und $\mathrm{Ker}\pi = N'$ also $N' \lhd G$. Es gilt $e_G \in H'$ und $(e_N, h) \star (e_N, h') = (e_N, hh')$ also H' ist eine Untergruppe von G.

2. Man überprüft leicht, dass diese Abbildungen injektive Gruppenhomomorphismen sind. Per Defnition sind diese Abbildungen surjektiv.

3. Es gilt $N' \cap H' = \{(e_n, e_H)\} = \{e_G\}$ und $(n,h) = (n, e_H) \star (e_N, h)$ also $G = N'H'$. ■

Satz 1.7.5 Sei G eine Gruppe, H eine Untergruppe und $N \lhd G$.

1. Falls gilt $N \cap H = \{e_G\}$ und $G = NH$. Dann ist für $\Phi : H \to \mathrm{Aut}(N)$ definiert durch $\Phi_h(n) = hnh^{-1}$ die Abbildung

$$f : N \times_\Phi H \to G,\ (n,h) \mapsto nh$$

ein Isomorphismus.

2. Falls zusätzlich gilt $H \lhd G$, so wird der Isomorphismus zu $f : N \times H \to G$. □

Beweis. 1. Es gilt

$$f((n,h) \star (n',h')) = f(n\Phi_h(n'), hh') = nhn'h^{-1}hh' = nhn'h' = f(n,h)f(n',h').$$

Daraus folgt, dass f ein Gruppenhomomorphismus ist. Da $G = N$ ist diese Abbildung surjektiv. Sei $(n,h) \in \mathrm{Ker}f$. Es gilt $nh = e_G$ also $n = h^{-1}$ und $n \in N \cap H$ also $n = e_G$. Daraus folgt $h = e_G$ und f ist injektiv also ein Isomorphismus.

2. Seien $h \in H$ und $n \in N$. Es gilt $N \ni n^{-1}(hnh^{-1}) = (n^{-1}hn)h^{-1} \in H$ also $n^{-1}hnh^{-1} = e_G$. Es folgt $hn = nh$ und $\Phi_h(n) = n$ und $N \rtimes H = N \times H$. ■

Beispiel 1.7.6 1. Sei $c = (231)$, sei $s = (213)$ und seien $N = A_3 = \{\mathrm{Id}, c, c^2\}$ und $H = \{\mathrm{Id}, s\}$. Da A_3 ein Normalteiler ist, sind $\mathrm{Int}_s : A_3 \to A_3$ und $\mathrm{Int}_{\mathrm{Id}} : A_3 \to A_3$ Gruppenautomorphismen und die Abbildung $\Phi : H \to \mathrm{Aut}(A_3)$, $\Phi_h = \mathrm{Int}_h$ ist ein Gruppenhomomorphismus.

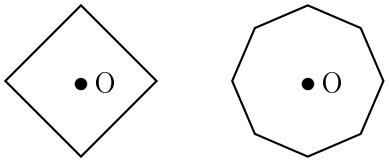
Dank dem obigen Satz zeigt man, dass die Abbildung

$$A_3 \rtimes H \to S_3,\ (n, h) \mapsto nh$$

ein Gruppenisomorphismus ist.

2. Algemeiner gilt $S_n \simeq A_n \rtimes \{\pm 1\}$.

2. Diedergruppe. Sei R_n ein regelmäßiges Polygon. Zum Beispiel $R_n = \{e^{\frac{2ik\pi}{n}} \mid k \in [0, n-1]\}$.



$n = 4$ $n = 8$

Sei D_{2n} die Gruppe aller Isometrie die R_n erhalten. Man zeigt, dass D_{2n} genau $2n$ elemente hat. Sei O das Zentrum von R_n und seien $D_1, \cdots, D_n$ die Geraden die durch O und eine Ecke laufen oder die durch O und die Mitte einer Kante laufen. Sei R die Drehung um O von $\frac{2\pi}{n}$ und seien $S_1, \cdots, S_n$ die Spiegelungen an den Geraden $D_1, \cdots, D_n$. Dann gilt

$$D_{2n} = \{\mathrm{Id}, R, \cdots, R^n, S_1, \cdots, S_n\}.$$

Die Gruppe D_{2n} enthält $N = \{\mathrm{Id}, R, \cdots, R^n\}$ und man überprüft leicht, dass $N \triangleleft D_{2n}$. Sei $H = \{\mathrm{Id}, S_1\}$. Dann ist H eine Untergruppe von G. Dank dem obigen Satz zeigt man, dass die Abbildung

$$N \rtimes H \to G,\ (n, h) \mapsto nh$$

ein Gruppenisomorphismus ist.

1.8 Operation einer Gruppe auf einer Menge

Definition 1.8.1 Sei G eine Gruppe und X eine Menge. Eine **Operation von** G **auf** X ist eine Abbildung $G \times X \to X$, $(g, x) \mapsto g \cdot x$ mit den Eigenschaften:

1. Für alle $x \in X$ gilt $e_G \cdot x = x$.
2. Für alle $g, h \in G$ und alle $x \in X$ gilt $(gh) \cdot x = g \cdot (h \cdot x)$.

Beispiel 1.8.2 1. **Die triviale Operation** $G \times X \to X$ definiert durch $g \cdot x = x$ für alle $g \in G$ und $x \in X$.

2. Die **Linkstranslation** $G \times G \to G$ definiert durch $g \cdot h = gh$ (hier ist $X = G$).

2. Die **Linkstranslation auf einem Quotient** $G \times G/H \to G/H$ definiert durch $g \cdot [g']_H = [gh]_H$ (hier ist $X = G/H$ wobei H eine Untergruppe ist).

3. Die **Konjugation** $G \times G \to G$ definiert durch $g \cdot h = ghg^{-1}$ (hier ist $X = G$).

4. $S_n \times [1, n] \to [1, n]$ definiert durch $\sigma \cdot i = \sigma(i)$.

4. $\mathrm{GL}_n(K) \times K^n \to K^n$ definiert durch $A \cdot v = Av$.

Lemma 1.8.3 Sei $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Operation.

1. Dann ist die Abbildung $\Phi(g) : X \to X$ definiert durch $\Phi(g)(x) = g \cdot x$ eine Bijektion von X und die Abbildung

$$\Phi : G \to \mathrm{Bij}(X)$$

definiert durch $g \mapsto \Phi(g)$ ein Gruppenhomomorphismus.

2. Umgekehrt, sei $\Phi : G \to \mathrm{Bij}(X)$ ein Gruppenhomomorphismus. Dann ist $G \times X \to X$ definiert durch $(g, x) \mapsto g \cdot x = \Phi(g)(x)$ eine Operation. □

Beweis. 1. Wir zeigen, dass $\Phi(gh) = \Phi(g) \circ \Phi(h)$. Es gilt

$$\Phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \Phi(g)(h \cdot x) = \Phi(g)\left(\Phi(h)(x)\right) = \left(\Phi(g) \circ \Phi(h)\right)(x).$$

Daraus folgt, dass $\Phi(g) \circ \Phi(g^{-1}) = \mathrm{Id}_X = \Phi(g^{-1}) \circ \Phi(g)$ also ist $\Phi(g)$ bijektiv mit $\Phi(g)^{-1} = \Phi(g^{-1})$ und Φ ist ein Gruppenhomomorphismus.

2. Es gilt $e_G \cdot x = \Phi(e_G)(x) = \mathrm{Id}_X(x) = x$ und $g \cdot (h \cdot x) = \Phi(g)(\Phi(h)(x)) = (\Phi(g) \circ \Phi(h))(x) = \Phi(gh)(x) = (gh) \cdot x$. ■

Definition 1.8.4 Sei $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Operation von G auf X.

1. Die Operation heißt **transitiv**, falls es für alle $x, y \in X$ ein $g \in G$ gibt mit $g \cdot x = y$.

2. Eine Operation heißt **treu** falls $(g \cdot x = x \text{ für alle } x \in X) \Rightarrow (g = e_G)$.

3. Sei $x \in X$. Die Menge $G \cdot x = \{g \cdot x \in X \mid g \in G$ heißt **Orbit** oder **Bahn** von $x \in X$.

Man schreibt $X/G = \{G \cdot x | x \in X\}$ für die Menge aler Bahnen. Diese Menge heisst **Quotient von X nach G.**

4. Ein $x \in X$ heißt **Fixpunkt** falls $g \cdot x = x$ für alle $g \in G$. Die Menge aller Fixpunkte ist X^G geschrieben.

5. Für $x \in X$ heißt $G_x = \{g \in G \mid g \cdot x = x\}$ der **Stabilisator von** x.

6. Allgemeiner heißt für $Y \subset X$ eine Teilmenge $G_Y = \{g \in G \mid g \cdot Y = Y\}$ der **Stabilisator von** Y.

Bemerkung 1.8.5 Die Operation $G \times X \to X$ ist genau dann treu, wenn der Gruppenhomomorphismus $\Phi : G \to \mathrm{Bij}(X)$ (siehe Lemma 1.8.3) injektiv ist.

Beispiel 1.8.6 1. Sei $G \times G \to G$ die Linkstranslation. Dann ist die Operation transitiv und treu. Daraus folgt

Satz 1.8.7 (Satz von Cayley) Sei G eine Gruppe der Ordnung n. Dann ist G eine Untergruppe von S_n. □

Beweis. Sei $L : G \to \mathrm{Bij}(G) \simeq S_n$ definiert durch $g \mapsto (L_g : G \to G, h \mapsto gh)$. Wir zeigen, dass L injektiv ist also dass die Operation treu ist. Sei $g \in \mathrm{Ker}L$. Es gilt $L_g = \mathrm{Id}_G$ also $L_g(h) = h$ für alle $h \in G$. Daraus folgt $gh = h$ und $g = e_G$. ■

2. Sei $G \times G/H \to G/H$ die Linkstranslation auf dem Quotient G/H. Dann ist die Operation transitiv und G_{e_G} der Stabilisator des neutrales Elements ist H.

3. Sei $G \times G \to G$ die Konjugation. Sei $h \subset G$. Dann ist der Stabilisator von h der Zentralisator von h:

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

4. Sei $X = \{H \subset G \mid H \text{ ist eine Untergruppe}\}$. Dann ist $G \times X \to X$ definiert durch $g \cdot H = gHg^{-1}$ eine Operation. Es gilt

$$G_H = \{g \in G \mid g \cdot H = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H).$$

Es gilt auch

$$X^G = \{H \in X \mid gHg^{-1} = H \text{ für alle } g \in G\} = \{H \in X \mid H \triangleleft G\}.$$

Definition 1.8.8 Sei $G \times X \to X$ eine Operation. Wir definieren auf X die Relation $x \sim y \Leftrightarrow y \in G \cdot x$.

Proposition 1.8.9 Sei $G \times X \to X$ eine Operation.

1. Die Relation $x \sim y$ ist eine Äquivalenzrelation.

2. Die Äquivalenzklassen sind die Bahnen.

3. Sei $x \in X$. Die Abbildung $G/G_x \to G \cdot x$ definiert durch $[g] \mapsto g \cdot x$ ist wohl definiert und bijektiv.

Beweis. 1. Es gilt $x = e_G \cdot x$ also $x \sim x$ und $\sim$ ist reflexiv.

Seien $x, y \in X$ mit $x \sim y$. Dann gilt $y \in G \cdot x$ also gibt es ein $g \in G$ mit $y = g \cdot x$. Dann gilt $x = g^{-1} \cdot y$ und $x \in G \cdot y$ also $y \sim x$ und $\sim$ ist symmetrisch.

Seien $x, y, z \in X$ mit $x \sim y$ und $y \sim z$. Dann gibt es $g, g' \in G$ mit $y = g \cdot x$ und $z = g' \cdot y$. Daraus folgt $z = g'g \cdot x$ und $x \sim z$ also $\sim$ ist transitiv.

2. Sei $x \in X$. Die Äquivalenzklasse von x is $\{y \in X \mid x \sim y\} = \{y \in X \mid y \in G \cdot x\} = G \cdot x$.

3. Seien $g, g' \in G$ mit $[g] = [g']$. Dann gibt es ein $h \in G_x$ mit $g' = gh$. Daraus folgt $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ und die Abbildung ist wohl definiert. Per Definition einer Bahn ist diese Abbildung surjektiv. Seien $g, g' \in G$ mit $g \cdot x = g' \cdot x$. Dann gilt $x = (g^{-1}g') \cdot x$ und $g^{-1}g' = h \in G_x$. Daraus folgt $g' = gh$ und $[g] = [g']$. Die Abbildung ist injektiv. ∎

Korollar 1.8.10 (Bahnformel) Sei $G \times X \to X$ eine Operation mit G endlich. Es gilt

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Beweis. Nach 3. im obigen Proposition gilt $|G/G_x| = |G \cdot x|$. Nach dem Satz von Lagrange gilt $|G/G_x| = [G : G_x] = |G|/|G_x|$. ∎

Satz 1.8.11 (Bahngleichung) Sei $G \times X \to X$ eine Operation mit X endlich. Dann gilt

$$|X| = \sum_{[x] \in X/G} |G \cdot x| = \sum_{[x] \in X/G} [G : G_x].$$

Beweis. Da die Bahnen die Äquivalenzklassen einer Äquivalenzrelation sind gilt

$$X = \coprod_{[x] \in X/G} G \cdot x.$$

Daraus folgt die Behauptung. ∎

Korollar 1.8.12 Sei G eine endliche Gruppe und H eine Untergruppe. Der kleinste Primteiler von $|H|$ sei großer gleich $[G : H]$. Dann ist $H \triangleleft G$

Beweis. Sei p der kleinste Primteiler von $|H|$ und sei $X = G/H$. Sei $H \times X \to X$ die Linksoperation: $h \cdot gH = hgH$. Sei $x \in X$. Nach der Bahnformel ist $|H \cdot x|$ ein Teiler von $|H|$ also $|H \cdot x| = 1$ oder $|H \cdot x| \geq p$. Nach der Bahngleichung gilt

$$p \geq [G : H] = |X| = \sum_{[x] \in X/H} |G \cdot x|.$$

Sei $x = [e_G] \in X$. Dann ist x ein Fixpunkt $|H \cdot x| = |\{x\}| = 1$. Daraus folgt

$$p - 1 \geq \sum_{[x] \in X/H,\ x \neq [e_G]} |G \cdot x|.$$

Da $|G \cdot x| = 1$ oder $|G \cdot x| \geq p$ muss $|G \cdot x| = 1$ für alle $x \in X$ gelten. Also für alle $[g] \in G/H$ gilt $[hg] = [g]$ für alle $h \in G$ *i.e.* $g^{-1}hg \in H$ für alle $g \in G$ und $h \in H$ *i.e.* $H \triangleleft G$. ∎

Beispiel 1.8.13 1. Wenn $[G : H]$ der kleinste Primteiler von $|G|$ ist, ist die Bedingung erfüllt.

2. Insbesondere wenn $[G : H] = 2$ ist die Bedigung erfüllt und $H \triangleleft G$.

Definition 1.8.14 Sei p eine Primzahl. Eine endliche Gruppe G heißt **p-Gruppe** falls $|G| = p^k$ eine Potenz von p ist.

Korollar 1.8.15 Sei G eine p-Gruppe. Dann gilt $|Z(G)| > 1$.

Beweis. Sei $|G| = p^k$. Sei $X = G$ und $G \times X \to X$ die Konjugation. Es gilt $X^G = Z(G)$: sei $z \in Z(G)$. Dann gilt $g \cdot z = gzg^{-1} = z$. Umgekehrt, sei $z \in X^G$. Dann gilt $g \cdot z = z$ für alle $g \in G$ also $gzg^{-1} = z$ für alle $g \in G$ *i.e.* $gz = zg$ für alle $g \in G$. Insbesondere gilt

$$z \in Z(G) \Leftrightarrow |G \cdot x| = 1.$$

Nach der Bahnformel folgt

$$z \in Z(G) \Leftrightarrow p \not| |G \cdot x|.$$

Nach der Bahngleichung gilt

$$p^k = |X| = \sum_{[x] \in X/H} |G \cdot x| = \sum_{[x] \in X/G,\ x \in Z(G)} |G \cdot x| + \sum_{[x] \in X/G,\ x \notin Z(G)} |G \cdot x|$$

also $p^k = |Z(G)| + \sum_{[x] \in X/G,\ x \notin Z(G)} |G \cdot x|$. Alle Terme in der Zweite Summe sind durch p teilbar also muss $|Z(G)|$ durch p teilbar sein. Daraus folgt $|Z(G)| > 1$. ∎

Satz 1.8.16 Sei p eine Primzahl und sei G eine Gruppe der Ordnung p^2. Dann gilt $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ oder $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Beweis. Fall 1: Es gebe $g \in G$ mit $\mathrm{ord}(g) = p^2$. Dann gilt $\mathbb{Z}/p^2\mathbb{Z} \simeq \langle g \rangle = G$.

Fall 2: Für alle $g \in G$ mit $g \neq e_G$ gilt $\mathrm{ord}(g) = p$. Sei $g \in G \setminus \{e_G\}$. Dann gilt $|\langle g \rangle| = p$ also es gibt $h \in G \setminus \langle g \rangle$. Sei $N = \langle g \rangle$ und $H = \langle h \rangle$. Dann $p = |N| = |H|$ der kleinste Primteiler von $|N$ und $|H|$ ist und $p \geq p = [G : N] = [G : H]$ gilt nach Korollar 1.8.12: $N \triangleleft G$ und $H \triangleleft G$. Der Durchschnitt $H \cap N$ ist eine echte Untergruppe von H da $h \in H \setminus N$. Also gilt $|H \cap N||p$ und $|H \cap N| < p$. Daraus folgt $|N \cap H| = 1$ und $N \cap H = \{e_G\}$. Da N und H normal sind gilt $\langle N, H \rangle = NH = HN$. Dies ist eine Untergruppe von G die $N \cup \{h\}$ enthält also $|NH| \geq p + 1$ und $|NH|$ teilt p^2. Daraus folgt $|NH| = p^2$ und $NH = G$. Nach dem Satz 1.7.5 folgt $G \simeq N \times H$ also $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. ∎

Bemerkung 1.8.17 Für Gruppen G der Ordnung $|G| = p^3$ ist die Klassifikation schon schwierieger: siehe Übungblatt 3 für den Fall $|G| = 8 = 2^3$. Die Gruppen der Ordnung 8 sind isomorph zu

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad D_8, \quad \mathbb{H}.$$

1.9 Symmetrische Gruppe

Definition 1.9.1 1. Ein Element $\sigma \in S_n$ heißt **r-Zykel** falls es paarweise verschiedene Elemente $x_1, \cdots, x_r \in [1,n]$ mit

$$\begin{array}{l}\sigma(x_k) = x_{k+1} \text{ für alle } k \in [1, r-1],\\ \sigma(x_r) = x_1 \text{ und}\\ \sigma(x) = x \text{ für alle } x \in [1,n] \setminus \{x_1, \cdots, x_r\}.\end{array}$$

2. Die Menge $\mathrm{Supp}(\sigma) = \{x_1, \cdots, x_r\}$ heißt **Träger des Zykels**. Die Zahl r ist die **Länge des Zykels**. Wir schreiben $[x_1, \cdots, x_r]$ für den Zykel der Länge r mit Träger $\{x_1, \cdots, x_r\}$.

3. Zwei Zykel σ, σ' heißen **fremd** falls $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$.

Bemerkung 1.9.2 Eine Transposition ist ein 2-Zykel.

Satz 1.9.3 1. Fremde Zykeln kommutieren.

2. Jedes $\gamma \in S_n$ ist ein Produkt fremder Zykel. Diese sind eindeutig bis auf Reihenfolge. □

Beweis. 1. Seien σ, σ' fremde Zykel und sei $x \in [1,n]$. Es gilt

$$\sigma(\sigma'(x)) = \left\{ \begin{array}{ll} x & \text{für } x \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma') \\ \sigma(x) & \text{für } x \in \mathrm{Supp}(\sigma) \setminus \mathrm{Supp}(\sigma') \\ \sigma'(x) & \text{für } x \notin \mathrm{Supp}(\sigma') \setminus \mathrm{Supp}(\sigma) \end{array} \right\} = \sigma'(\sigma(x)).$$

2. Sei $H = \langle \gamma \rangle$ die von γ erzeugte Untergruppe. Wir lassen H operieren auf $[1,n]$ durch $\gamma^n \cdot x = \gamma^n(x)$. Seien B eine Bahn, sei $r = |B|$ und sei $x_1 \in B$. Es gilt

$$B = \{x_1, x_2 = \gamma(x_1), \cdots, x_r = \gamma^{r-1}(x_1)\}.$$

Sei $\sigma_B = [x_1, \cdots, x_r]$. Es gilt

$$\gamma = \prod_{B \in [1,n]/H} \sigma_B.$$

Umgekehrt zerlegt jede Faktorisierung $\gamma = \prod_k \sigma_k$ die Menge X in Bahnen gegeben durch die Träger von σ_k. Diese Bahnen und also die Zerlegung ist bis auf Reihenfolge eindeutig bestimmt. ■

Beispiel 1.9.4 Sei $\gamma = (36451872) \in S_8$. Die Bahnen von γ sind $\{1,2,4,5\}$, $\{2,6,8\}$ und $\{7\}$. Es gilt also

$$\gamma = [1345][268][7] = [1345][268].$$

Korollar 1.9.5 Sei $\gamma = \sigma_1 \cdots \sigma_k$ die Zerlegung von γ als Produkt fremder Zykel und sei $r_i = \text{ord}(\sigma_i)$. Dann gilt $\text{ord}(\gamma = \text{kgV}(r_1, \cdots, r_k)$.

Beweis. Seo $d = \text{kgV}(r_1, \cdots, r_k)$. Es gilt $\gamma^d = \sigma_1^d \cdots \sigma_k^d = \text{Id}$ also $\text{ord}(\gamma)|d$. Umgekehrt für a mit $\gamma^a = \text{Id}$ gilt $\text{Id} = \gamma^a = \sigma_1^a \cdots \sigma_k^a$ und da die Träger dijunkt sind gilt $\mathfrak{g}_i^a = \text{Id}$ für alle $i \in [1, k]$ also $r_i|a$. Daraus folgt $\text{kgV}(r_1, \cdots, r_k)|a$. ∎

Lemma 1.9.6 (Konjugationsprinzip) Sei $\sigma = [x_1, \cdots, x_r]$ ein r-Zykel und sei $\gamma \in S_n$. Dann gilt

$$\gamma\sigma\gamma^{-1} = [\gamma(x_1), \cdots, \gamma(x_r)].$$

Beweis. Siehe Übungsblatt 4. ∎

Korollar 1.9.7 Sei $n \geq 0$. Es gilt $S_n = \langle [1,2], [1,2,\cdots,n] \rangle$.

Beweis. Sei $H = \langle [1,2], [1,2,\cdots,n] \rangle$. Sei $\sigma = [1,2,\cdots,n]$. Es gilt $H \ni \sigma^k[1,2]\sigma^{-k} = [\sigma^k(1), \sigma^k(2)] = [k+1, k+2]$. Da die einfache Transpositionen $[i, i+1]$ die Gruppe S_n erzeugen, gilt $H = S_n$. ∎

Definition 1.9.8 Sei $k \geq 0$. Eine Operation $G \times X \to X$ heißt **k-transitiv** falls für $x_1, \cdots x_k \in X$ paarweise verschiedene Elemente und $y_1, \cdots y_k \in X$ paarweise verschiedene Elemente es ein $g \in G$ gibt mit

$$g \cdot x_i = y_i \text{ für alle } i \in [1, k].$$

Beispiel 1.9.9 Sei $S_n \times [1, n] \to [1, n]$ die Operation $\gamma \cdot x = \gamma(x)$. Dann ist diese Operation n-transitiv.

Lemma 1.9.10 Sei $A_n \times [1, n] \to [1, n]$ die Operation gegeben durch $\gamma \cdot x = \gamma(x)$. Dann ist diese Operation $(n-2)$-transitiv. □

Beweis. Seien $x_1, \cdots x_{n-2} \in [1, n]$ paarweise verschieden und $y_1, \cdots y_{n-2} \in [1, n]$ paarweise verschieden. Seien $x_{n-1}, x_n, y_{n-1}, y_n$ so, dass

$$\{x_1, \cdots, x_n\} = [1, n] = \{y_1, \cdots, y_n\}.$$

Da S_n n-transitiv operiert gibt es $\gamma \in S_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, n]$. Fall $\gamma \in A_n$ sind wir fertig. Sonst, sei $\gamma' = \gamma \circ [x_{n-1}, x_n]$. Dann gilt $\gamma' \in A_n$ und $\gamma(x_i) = y_i$ für alle $i \in [1, n-2]$.

mente es ein $g \in G$ gibt mit

$$g \cdot x_i = y_i \text{ für alle } i \in [1, k].$$

Satz 1.9.11 1. In S_n sind alle r-Zykel sind konjugiert.

2. Für $n \geq 5$ sind alle 3-Zykel konjugiert in A_n.

3. Jedes Element in A_n ist ein Produkt gerader Anzahl von Transpositionen.

4. Ein r-Zyklus ist genau dann in A_n, wenn r ungerade ist.

5. Die Menge aller 3-Zykel erzeugt A_n. □

Beweis. 1. Seien $\sigma = [x_1, \cdots, x_r]$ und $\sigma' = [y_1, \cdots, y_r]$ zwei r-Zykel. Da S_n n-transitiv operiert, gibt es $\gamma \in S_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, r]$. Daraus folgt $\gamma\sigma\gamma^{-1} = \sigma'$.

2. Sei $\sigma = [x_1, x_2, x_3]$ und $\sigma' = [y_1, y_2, y_3]$. Da $n \geq 5$ gilt $n - 2 \geq 3$. Da A_n $n-2$-transitiv operiert gibt es $\gamma \in A_n$ mit $\gamma(x_i) = y_i$ für alle $i \in [1, 3]$. Daraus folgt $\gamma\sigma\gamma^{-1} = \sigma'$.

3. Jede Permutation ist ein Produkt von Transpositionen und per Definition von A_n sind Element in A_n Produkt gerader Anzahl von Transpositionen.

4. Sei $\sigma = [x_1, \cdots, x_r]$. Es gilt $\sigma = [x_1, x_2][x_2, x_3] \cdots [x_{r-1}, x_r]$ also ist σ ein Produkt von $r - 1$ Transpositionen und es gilt $\varepsilon(\sigma) = (-1)^r$.

4. Sei $[x_1, x_2][x_3, x_4]$ oder $[x_1, x_2][x_2, x_3]$ ein Produkt von 2 Transpositionen mit x_1, x_2, x_3, x_4 paarweise verschieden. Es gilt

$$[x_1, x_2][x_3, x_4] = [x_1, x_3, x_2][x_1, x_3, x_4] \text{ und } [x_1, x_2][x_2, x_3] = [x_1, x_2, x_3]$$

und daraus folgt, dass alle Element in A_n Produkte von 3-Zykel sind. ■

Korollar 1.9.12 Sei $n \geq 2$.

1. Es gilt $D(S_n) = A_n$.

2. Es gilt

$$D(A_n) = \begin{cases} \{\mathrm{Id}\} & \text{für } n = 2, 3 \\ V_4 & \text{für } n = 4 \\ A_n & \text{für } n \geq 5 \end{cases}$$

wobei $V_4 = \{\mathrm{Id}, [12][34], [13][24], [14][23]\}$.

Beweis. 1. Da $S_n/A_n \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ abelsch ist, gilt $D(S_n) \subset A_n$ (Lemma 1.6.2). Für $n = 2$ gilt $A_n = \{\mathrm{Id}\}$ also $A_n \subset D(S_n)$. Für $n \geq 3$ gilt

$$[a, b, c] = [b, c][a, b][b, c][a, b] = [b, c][a, b][b, c]^{-1}[a, b]^{-1} = [[b, c], [a, b]] \in D(S_n).$$

Da A_n von den 3-Zykeln erzeugt ist, gilt $A_n \subset D(S_n)$.

2. Für $n = 2, 3$ ist A_n abelsch also gilt $D(A_n) = \{\mathrm{Id}\}$. Für $n = 4$ gilt $V_4 \triangleleft A_4$ (Siehe Übungsblatt 3) und $A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ ist abelsch. Nach Lemma 1.6.2 gilt $D(A_4) \subset V_4$. Umgekehrt gilt für $a, b, c, d \in [1, 4]$ paarweise verschieden:

$$\begin{aligned}[a, b][c, d] &= [a, b, c][a, b, d][a, c, b][a, d, b] \\ &= [a, b, c][a, b, d][a, b, c]^{-1}[a, b, d]^{-1} = [[a, b, c], [a, b, d]] \in D(A_4).\end{aligned}$$

Daraus folgt $V_4 \subset D(A_4)$.

Sei $n \geq 5$, seien $a, b, c \in [1, n]$ paarweise verschieden und seien $x, y \in [1, n] \setminus \{a, b, c\}$. Es gilt

$$\begin{aligned}[a, b, c] &= [a, b, x][a, c, y][a, x, b][a, y, c] \\ &= [a, b, x][a, c, y][a, b, x]^{-1}[a, c, y]^{-1} = [[a, b, x], [a, c, y]] \in D(A_n).\end{aligned}$$

Es folgt $A_n \subset D(A_n)$ und da $D(A_n) \subset A_n$ ist die Behauptung bewiesen. ∎

Man kann eingentlich das folgende Resultat zeigen (Siehe Übungsblatt 4 für den Fall $n = 5$).

Theorem 1.9.13 Die Gruppe A_n ist einfach für $n \geq 5$. □

1.10 Sylow Sätze

Definition 1.10.1 Sei G eine Gruppe und sei p ein Primteiler von $|G|$ so, dass

$$|G| = p^\alpha m \text{ wobei } p \nmid m.$$

Eine Untergruppe von G der Ordnung p^α heißt **p-Sylowuntergruppe**.

Bemerkung 1.10.2 Sei G ine Gruppe und p eine Primzahl. Eine Untergruppe H ist genau dann eine p-Sylowuntergruppe, wenn H eine p-Gruppe ist und $[G : H]$ und p teilerfremd sind.

Beispiel 1.10.3 Sei p eine Primzahl, sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und sei $G = \mathrm{GL}_n(\mathbb{F}_p)$. Es gilt

$$|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1).$$

Um es zu zeigen, zählen wir die Basen von $\mathbb{F}_p^n$ ab. In $\mathbb{F}_p^n$ gibt es p^n Elemente. Eine Basis ist der Form $(v_1, \cdots, v_n)$. Der erste Basisvektor v_1 kann beliebig in $\mathbb{F}_p^n \setminus \{0\}$ gewählt werden also $p^n - 1$ Möglichkeiten. Der zweite Basisvektor v_2 kann beliebig in $\mathbb{F}_p^n \setminus \langle v_1 \rangle$ gewählt werden also $p^n - p$ Möglichkeiten. Nach Induktion kann v_{k+1} kann beliebig in $\mathbb{F}_p^n \setminus \langle v_1, \cdots, v_k \rangle$ gewählt werden also $p^n - p^k$ Möglichkeiten.

Sei H die Untergruppe von G, welche von oberen Dreieckmatrizen mit 1 auf der Diagonal besteht. Dann gilt

$$|H| = p^{\frac{n(n-1)}{2}}$$

und H ist eine Sylowuntergruppe von G.

Lemma 1.10.4 Sei G eine Gruppe mit $|G| = n = p^\alpha m$ mit $p \not| m$. Sei H eine Untergruppe von G und sei S eine p-Sylowuntergruppe von G. Dann gibt es ein $g \in G$ so, dass $gSg^{-1} \cap H$ eine p-Sylowuntergruppe von H ist. Insbesondere hat H auch eine p-Sylowuntergruppe. □

Beweis. Sei $X = G/S$. Sei $G \times X \to X$ die Linkstranslation auf dem Quotient $X = G/S$ definiert durch $g \cdot [g'] = [gg']$. Der Stabilisator von $[g] = gS$ ist gSg^{-1} (Siehe Übungsblatt 4).

Per Einschränkung Operiert H auf X durch $H \times X \to X$ mit $h \cdot [g'] = [hg']$. Der Stabilisator $H_{[g]}$ von $[g] = gS$ ist $gSg^{-1} \cap H$ (Siehe Übungsblatt 4).

Die Gruppen $gSg^{-1} \cap H$ sind p-Gruppen, da $|gSg^{-1} \cap H|$ die Ordnung $|S| = p^\alpha$ teilt. Wir zeigen, dass es ein g gibt so, dass $|H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ und p teilerfremd sind.

Falls es nicht der Fall ist gilt nach der Bahnformel $|H \cdot [g]| = |H|/|H_{[g]}| = |H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ und teilt p die Zahl $|H \cdot x|$ für alle $x = [g] \in X$. Nach der Bahngleichung

$$m = |G/S| = |X| = \sum_{[x] \in X/H} |H \cdot x|$$

würde m durch p teilbar sein. Ein Widerspruch. ■

Satz 1.10.5 (Erster Sylowsatz) Sei G eine Gruppe und p ein Primteiler von $|G|$. Dann hat G mindestens eine p-Sylowuntergruppe. □

Beweis. Sei G eine Gruppe und p ein Primteiler von $n = |G|$. Nach dem Satz von Cayley ist G isomorph zu einer Untergruppe von S_n. Die Gruppe S_n ist aber eine Untergruppe von $\mathrm{GL}_n(K)$ für jeden Körper K dank der Abbildung

$$\sigma \mapsto P_\sigma$$

wobei P_σ die Permutationsmatrix ist: $P_\sigma = (a_{i,j})_{i,j \in [1,n]}$ mit $a_{i,j} = \delta_{\sigma(i),j}$. Also für $K = \mathbb{F}_p$ ist G eine Untergruppe von $\mathrm{GL}_n(\mathbb{F}_p)$. Da $\mathrm{GL}_n(\mathbb{F}_p)$ eine p-Sylowuntergruppe hat, hat G auch eine p-Sylowuntergruppe nach dem obigen Lemma. ■

Korollar 1.10.6 (Satz von Cauchy) Sei G eine Gruppe und p ein Primteiler von p. Dann gibt es ein Element der Ordnung p.

Beweis. Sei $|G| = p^\alpha m$ mit $p \not| m$ und sei S eine p-Sylowuntergruppe von G. Sei $g \in S \setminus \{e_G\}$. Dann gilt $\mathrm{ord}(g) \neq 0$ und $\mathrm{ord}(g) | p^\alpha$ also $\mathrm{ord}(g) = p^k$ für $k \geq 1$. Dann gilt $\mathrm{ord}(g^{p^{k-1}}) = \frac{p^k}{\mathrm{ggT}(p^k, p^{k-1})} = \frac{p^k}{p^{k-1}} = p$. ■

Korollar 1.10.7 Eine Gruppe G ist genau dann eine p-Gruppe, wenn $\mathrm{ord}(g)$ eine Potenz von p ist für jedes $g \in G$.

Beweis. Sei G eine p-Gruppe. Nach dem Satz von Lagrange ist die Ordnung jedes Element einen Teiler von $|G|$ also eine Potenz von p.

Umgekehrt, sei G eine Gruppe die keine p-Gruppe ist. Dann gibt es einen Primteiler q von $|G|$ mit $p \neq q$ und G hat ein Element der Ordnung q. ∎

Korollar 1.10.8 Sei p eine Primzal und G eine Untergruppe von S_p so, dass p ein Teiler von $|G|$ ist und G eine Transposition enthält. Dann gilt $G = S_p$.

Beweis. Es gilt $|S_p| = p! = pm$ mit $p \not| m$. Da p die Ordnung $|G|$ teilt gilt $|G| = pm'$ mit $p \not| m'$. Sei $\sigma \in G$ der Ordnung p. Wir zeigen, dass σ ein p-Zykel ist. Sei $\sigma = c_1 \cdots c_k$ die Zerlegung von σ in Produkt von r-Zykeln mit disjunkten Träger. Es gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(\mathrm{ord}(c_1), \cdots, \mathrm{ord}(c_k))$ nach Korollar 1.9.5. Insberonde muss p die Ordnung $\mathrm{ord}(c_i)$ für ein i teilen. Für so ein i gilt $\mathrm{ord}(c_i) = p$ und c_i ist ein p-Zykel. Also enthält G eine Transposition τ und ein p-Zykel σ'.

Sei $\tau = [a, b]$. Es gibt ein $\gamma \in S_n$ so, dass $\gamma\tau\gamma^{-1} = [1, 2]$ (wähle γ mit $\gamma(a) = 1$ und $\gamma(b) = 2$). Es genügt zu zeigen, dass $G' = \gamma G\gamma^{-1} = S_n$ und es gilt $\gamma G\gamma^{-1} \ni [1, 2], \sigma = \gamma\sigma'\gamma^{-1}$ wobei σ ein p-Zykel ist. Da σ ein p-Zykel ist gibt es ein k mit $\sigma^k(1) = 2$. Außerdem gilt $\sigma^k \in \langle\sigma\rangle \setminus \{\mathrm{Id}\}$ also $1 < \mathrm{ord}(\sigma^k) | \mathrm{ord}(\sigma) = p$. Es gilt also $\mathrm{ord}(\sigma^k) = p$ und $\sigma^k = [1, 2, x_3, \cdots, x_p]$. Sei $\delta \in S_n$ mit $\delta(1) = 1$, $\delta(2) = 2$ und $\delta(x_i) = i$ für alle $i \geq 3$. Dann gilt $\delta[1, 2]\delta^{-1} = [1, 2]$ und $\delta\sigma^k\delta^{-1} = [1, 2, \cdots, p]$. Die Gruppe $G'' = \delta G'\delta^{-1}$ enthält $[1, 2]$ und $[1, 2, \cdots, p]$ also nach Korollar 1.9.7 gilt $G'' = S_p$. Daraus folgt $G' = S_p$ und $G = S_p$. ∎

Korollar 1.10.9 Seien p und q Primzahlen und G eine Gruppe der Ordnung $|G| = p^k q^l$ mit $k, l \geq 1$ so, dass $q > p^k$. Dann gilt $G \simeq K_q \rtimes K_p$ wobei K_p und K_q beliebege p- und q-Sylowuntergruppen sind.

Beweis. Nach Korollar 1.8.12 gilt $K_q \lhd G$. Sei $H = K_p \cap K_q$. Dann ist $|H|$ ein Teiler von $p^k = |K_p|$ und $q^l = |K_q|$ also $|H| = 1$ und $K_q \cap K_p = \{e_G\}$. Daraus folgt, dass die Abbildung $K_q \times K_p \to G$, $(a, b) \mapsto ab$ injektiv ist. Da $|K_p \times K_q| = p^k q^l = |G|$, folgt, dass diese Abbildung eine Bijektion ist also $G = K_q K_p$. Nach dem Satz 1.7.5 folgt $G \simeq K_q \rtimes K_p$. ∎

Satz 1.10.10 (Zweiter Sylowsatz) Sei p eine Primzahl und G eine Gruppe der Ordnung $|G| = p^\alpha m$ mit $p \not| m$.

1. Sei H eine Untergruppe von G die eine p-Gruppe ist. Dann gibt es S eine p-Sylowuntergruppe von G mit $H \subset S$.

Sei k die Anzahl aller p-Sylowuntergruppen

2. Alle p-Sylowuntergruppe sind zueinander konjuguiert.

3. Es gilt $k || G|$.

4. Es gilt $k \equiv 1 \pmod{p}$ (also k teilt m). □

Korollar 1.10.11 (Vom Satz 1.10.10.2) Sei G eine Gruppe und S ein p-Sylowuntergruppe. Dann gilt

$$S \triangleleft G \Leftrightarrow S \text{ ist der einzige } p\text{-Sylowuntergruppe von } G \Leftrightarrow k = 1.$$

Beweis. Die letze äquivalenz ist klar da k die Anzahl von p-Sylowuntergruppen ist.

($\Rightarrow$). Sei S eine p-Sylowuntergruppe mit $S \triangleleft G$. Sei T eine weitere p-Sylowuntergruppe. Nach Satz 1.10.10.2 gibt es ein $g \in G$ mit $gSg^{-1} = T$. Da aber $S \triangleleft G$, folgt $S = gSg^{-1} = T$.

($\Leftarrow$). Sei S eine p-Sylowuntergruppe und sei $g \in G$. Dann ist gSg^{-1} auch eine p-Sylowuntergruppe. Daraus folgt nach Annahme, dass $gSg^{-1} = S$ und $S \triangleleft G$. ∎

Beispiel 1.10.12 Sei G eine Gruppe der Ordnung 255. Dann ist G nicht einfach. Tatsächlich gilt $255 = 3 \times 5 \times 17$. Sei $p = 17$. Es gilt $|G| = p^\alpha m$ mit $\alpha = 1$ und $m = 3 \times 5 = 15$. Sei k die Anzahl von p-Sylowuntergruppen. Es gilt $k \equiv 1 \pmod p$ und $k|m$. Die Teiler von 15 sind 1, 3, 5 und 15. Da $3, 5, 15 \not\equiv 1 \pmod p$ gilt $k = 1$. Also ist K_{17} die einzige 17-Sylowuntergruppe und also ein Normalteiler. Es folgt, dass G nicht einfach ist.

Beweis vom Satz 1.10.10. Wir zeigen 1. und 2. Sei H eine Untergruppe von G die eine p-Gruppe ist und sei S eine p-Sylowuntergruppe. Nach Lemma 1.10.4 gibt es ein $g \in G$ so, dass $gSg^{-1} \cap H$ eine p-Sylowuntergruppe von H ist. Da H eine p-Gruppe ist, ist eine p-Sylowuntergruppe die ganze Gruppe also $gSg^{-1} \cap H = H$ *i.e.* $H \subset gSg^{-1}$. Die Untergruppe gSg^{-1} hat Ordnung $|S| = p^\alpha$ und ist also eine p-Sylowuntergruppe. Daraus folgt 1.

Falls H eine pSylowuntergruppe ist gilt $H \subset gSg^{-1}$ und $|H| = p^\alpha = |gSg^{-1}|$ und es folgt $H = gSg^{-1}$. Dies zeigt 2.

3. Wir betrachten $X = \{p\text{-Sylowuntergruppen}\}$ und die Operation $G \times X \to X$ definiert durch $g \cdot S = gSg^{-1}$. Nach 2. ist diese Operation Transitiv also gilt $G \cdot S = X$. Nach der Bahnformel folgt, dass $k = |X| = |G \cdot S|$ ein teiler von $|G|$ ist.

4. Sei S eine p-Sylowuntergruppe. Wir betrachten die Einschränkungen der obigen Operation auf S *i.e.* $S \times X \to X$ definiert durch $s \cdot T = sTs^{-1}$. Sei $S \cdot T$ eine Bahn dieser Operation. Nach der Bahnformel teilt $|S \cdot T|$ die Ordnung $|S|$ also gilt

$$|S \cdot T| = \begin{cases} 1 & \text{für } S \cdot T = \{T\} \text{ } i.e. \text{ } T \text{ Fixpunkt oder} \\ pa & \text{für ein } a \in \mathbb{N}. \end{cases}$$

Sei also X^S die Fixpunkte. Es gilt nach der Bahngleichung:

$$|X| = \sum_{[x] \in X/S} |S \cdot x| = \sum_{x \in X^S} |S \cdot x| + \sum_{[x] \in X/S, x \notin X^S} |S \cdot x| = |X^S| + pb.$$

Also gilt $k = |X| \equiv |X^S| \pmod p$. Es genügt zu zeigen, dass $X^S = \{S\}$ also $|X^S| = 1$. Sei $T \in X^S$. Also ist T eine p-Sylowuntergruppe mit $sTs^{-1} = T$ für alle $s \in S$. Sei

$H = \langle S, T\rangle$. Dann sind S und T p-Sylowuntergruppe von H (beide sind schon p-Sylowuntergruppe von G). Außerdem gilt $T \subset N_H(T)$ und weil $sTs^{-1} = T$ für alle $s \in S$ gilt auch $S \subset N_H(T)$. Also gilt $H = \langle S, T\rangle \subset N_H(T)$. Daraus folgt $H = N_H(T)$ *i.e.* $T \triangleleft H$. Nach Korollar 1.10.11 hat H genau eine p-Sylowuntergruppe. Es folgt $S = T$. ∎

Korollar 1.10.13 (Primärzerlegung abelscher Gruppen) Sei G eine endliche abelsche Gruppe. Dann ist für jeder Primteiler p von G die p-Sylowuntergruppe K_p von G eindeutig durch

$$K_p = \{g \in G \mid \text{ord}(g) \text{ ist Potenz von } p\}$$

gegeben und es gilt

$$G = \prod_{p \text{ Primteiler von } |G|} K_p.$$

Beweis. Sei K_p eine p-Sylowuntergruppe. Da G abelsch ist K_p ein Normalteiler also ist K_p die einzige p-Sylowuntergruppe. Da $|K_p|$ eine Potenz von p ist gilt $K_p \subset \{g \in G \mid \text{ord}(g) \text{ ist Potenz von } p\}$. Umgekehrt, sei $g \in G$ so, dass ord(g) eine Potenz von p ist. Dann ist $\langle g\rangle$ eine p-Gruppe und also in einer p-Sylowuntergruppe enthalten. Es folgt $g \in K_p$ da K_p die einzige p-Sylowuntergruppe ist.

Seien $p_1, \cdots, p_k$ die Primteiler von $|G|$ und sei $f : \prod_{i=1}^k K_{p_i} \to G$ definiert durch $f(x_1, \cdots, x_k) = x_1 \cdots x_k$. Da G kommutativ ist ist f ein Gruppenhomomorphismus. Sei $(x_1, \cdots, x_k) \in \text{Ker} f$. Dann gilt $x_1 x_2 \cdots x_k = e_G$. Sei ord$(x_i) = p_i^{\alpha_i}$. Es folgt

$$e_G = (x_1 \cdots x_k)^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = x_1^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}}.$$

Da $\text{ggT}(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 1$ gibt es $a, b \in \mathbb{Z}$ mit $ap_1^{\alpha_1} + bp_2^{\alpha_2} \cdots p_k^{\alpha_k} = 1$. Es folgt

$$x_1 = x_1^{ap_1^{\alpha_1} + bp_2^{\alpha_2} \cdots p_k^{\alpha_k}} = e_G.$$

Analog gilt $x_i = e_G$ für alle i und f ist injektiv. Sei

$$|G| = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Es gilt $|K_{p_i}| = p_i^{\beta_i}$ und $|\prod_{i=1}^k K_{p_i}| = |G|$. Daraus folgt, dass f bijektiv ist also ein Isomorphismus. ∎

Beispiel 1.10.14 Sei G eine abelsche Gruppe der Ordnung $|G| = p_1 \cdots p_k$. Dann gilt

$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \mathbb{Z}/p_k\mathbb{Z}.$$

Man kann sogar zeigen:

Theorem 1.10.15 Sei G eine endliche abelsche Gruppe. Dann gibt es Zahlen $a_1, \cdots, a_k \in \mathbb{N}$ mit

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}.$$

1.11 Auflösbare Gruppen

Definition 1.11.1 Sei G eine Gruppe. Die **k-te derivierte Untergruppe** $D^k(G)$ ist definiert per Induktion durch

$$D^0(G) = G,\ D^1(G) = D(G) \text{ und } D^{k+1}(G) = D(D^k(G)).$$

Beispiel 1.11.2 1. Für $n \geq 5$ gilt $D^0(S_n) = S_n$, $D^1(S_n) = D(S_n) = A_n$, $D^2(S_n) = D(D(S_n)) = D(A_n) = A_n$ und per Induktion $D^k(S_n) = A_n$ für alle $k \geq 1$.

2. Für $n = 4$ gilt $D^0(S_4) = S_4$, $D^1(S_4) = A_4$, $D^2(S_4) = D(A_4) = V_4$, $D^3(S_4) = D(V_4) = \{\mathrm{Id}\}$ und $D^k(S_4) = \{\mathrm{Id}\}$ für alle $k \geq 3$.

Bemerkung 1.11.3 Sei G eine Gruppe. Es gilt

$$G = D^0(G) \triangleright D^1(G) \triangleright \cdots \triangleright D^k(G) \triangleright D^{k+1}(G) \triangleright \cdots$$

und $D^k(G)/D^{k+1}(G)$ ist abelsch.

Definition 1.11.4 Eine Gruppe G heißt **auflösbar** wenn es eine Folge von Untergruppen $(G_i)_{i\in[1,m]}$ gibt mit

- $G_0 = G$ und $G_m = \{e_G\}$,
- $G_{i+1} \triangleleft G_i$ und
- G_i/G_{i+1} ist abelsch.

Beispiel 1.11.5 1. Sei G abelsch, dann ist G auflösbar mit $G_1 = \{e_G\} \triangleleft G_1 = G$.

2. Die Gruppen S_n und A_n sind für $n \leq 4$ auflösbar mit den Folgen

$$\{\mathrm{Id}\} = A_1 = S_1,\quad \{\mathrm{Id}\} = A_2 \triangleleft S_2,\quad \{\mathrm{Id}\} \triangleleft A_3 \triangleleft S_3 \text{ und } \{\mathrm{Id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

Satz 1.11.6 Eine Gruppe G ist genau dann auflösbar, wenn es ein m gibt mit $D^m(G) = \{e_G\}$. □

Beweis. ($\Leftarrow$). Sei $G_i = D^i(G)$. Dann ist G_i eine Folge von Untergruppen, die die Definition der Auflösbarkeit erfüllt.

($\Rightarrow$). Sei $(G_i)_{i\in[1,m]}$ eine Folge von Untergruppen mit $G_0 = G$, $G_r = \{e_G\}$, $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} ist abelsch. Wir zeigen, dass $D^i(G) \subset G_i$ per Induktion nach i. Daraus folgt, dass $D^m(G) \subset G_m = \{e_G\}$ also $D^m(G) = \{e_G\}$.

Es gilt $D^0(G) = G = G_0$. Angenommen gilt $D^i(G) \subset G_i$. Da G_i/G_{i+1} abelsch ist gilt $D(G_i) \subset G_{i+1}$. Daraus folgt

$$D^{i+1}(G) = D(D^i(G)) \subset D(G_i) \subset G_{i+1}.$$

Korollar 1.11.7 Die Gruppen S_n und A_n sind für $n \geq 5$ nicht auflösbar.

Beweis. Es gilt $D^k(S_n) = D^k(A_n) = A_n$ für $k \geq 2$ und $n \geq 5$. ∎

Satz 1.11.8 Sei $f : G \to G'$ ein Gruppenhomomorphismus und sei H eine Untergruppe von G.

1. Es gilt $f(D(H)) = D(f(H))$.

2. Es gilt $f(D^k(G)) \subset D^k(G')$ für alle k.

3. Falls f surjektiv ist, gilt $f(D^k(G)) = D^k(G')$ für alle k. □

Beweis. 1. Folgt aus $f([a,b]) = [f(a), f(b)]$.

2. Per Induktion nach k. Es gilt $f(D^0(G)) = f(G) \subset G' = D^0(G')$. Angenommen gilt $f(D^k(G)) \subset D^k(G')$. Dann gilt nach 1. $f(D^{k+1}(G)) = f(D(D^k(G))) = D(f(D^k(G))) \subset D(D^k(G')) = D^{k+1}(G)$.

3. Per Induktion nach k. Es gilt $f(D^0(G)) = f(G) = G' = D^0(G')$. Angenommen gilt $f(D^k(G)) = D^k(G')$. Dann gilt nach 1. $f(D^{k+1}(G)) = f(D(D^k(G))) = D(f(D^k(G))) = D(D^k(G')) = D^{k+1}(G)$. ∎

Korollar 1.11.9 Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler.

1. Falls G auflösbar ist gilt H, N und G/N sind auflösbar.

2. Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. 1. Sei m mit $D^m(G) = \{e_G\}$. Es gilt $D^m(H) \subset D^m(G)$ also ist H auflösbar. Das gleiche gilt für N. Nach dem obigen Satz mit $f : G \to G/N$ die kanonische Projektion gilt $f(D^m(G)) = D^m(G/N)$ also $D^m(G/N) = \{e_{G/N}\}$.

2. ($\Rightarrow$). Folgt aus 1.

($\Leftarrow$). Seien m und r mit $D^m(N) = \{e_G\}$ und $D^r(G/N) = \{e_{G/N}\}$. Sei $f : G \to G/N$ die kanonische Projektion. Nach dem obigen Satz gilt $f(D^r(G)) = D^r(G/N) = \{e_{G/N}\}$. Also gilt $D^r(G) \subset \mathrm{Ker} f = N$. Daraus folgt $D^{m+r}(G) = D^m(D^r(G)) \subset D^m(N) = \{e_G\}$. ∎

Korollar 1.11.10 Seien $G_1, \cdots, G_r$, H und N Gruppen.

1. Das Produkt $G_1 \times \cdots \times G_r$ ist genau dann auflösbar, wenn G_i für alle $i \in [1,r]$ auflösbar ist.

2. Das semidirekte Produkt $N \rtimes H$ ist genau dann auflösbar, wenn N und H auflösbar sind.

Beweis. Siehe Übungsblatt 5. ∎

Korollar 1.11.11 Jede p-Gruppe ist auflösbar.

Beweis. Siehe Übungsblatt 5. ∎

Satz 1.11.12 Sei G endlich auflösbar. Jede Folge von Untergruppen $(G_i)_{i\in[1,r]}$ mit $G_0 = G$, $G_r = \{e_G\}$, $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} abelsch lässt sich verfeinern in einer Folge von Untergruppen $(G'_i)_{i\in[1,r]}$ mit

- $G'_0 = G$ und $G'_r = \{e_G\}$,
- $G'_{i+1} \triangleleft G'_i$ und
- $G'_i/G'_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ für eine Primzahl p_i. □

Beweis. Sei $(G_i)_{i\in[1,r]}$ eine Folge die sich nicht verfeinern lässt aber mit ein k so, dass G_k/G_{k+1} nicht von Primzahlordnung. Sei p ein Primteiler von G_k/G_{k+1} und $x \in G_k/G_{k+1}$ ein Element der Ordnung p ist (Satz von Cauchy). Dann gilt $\{e\} \subsetneq \langle x\rangle \subsetneq G_k/G_{k+1}$. Da G_k/G_{k+1} abelsch ist gilt $\langle x\rangle \triangleleft G_k/G_{k+1}$. Sei $\pi : G_k \to G_k/G_{k+1}$ die kanonische Projektion und $H = \pi^{-1}(\langle x\rangle)$. Es gilt $G_{k+1} \subsetneq H \subsetneq G_k$ und $G_{k+1} \triangleleft H \triangleleft G_k$. Ein Widerspruch zur nicht Verfeinbarkeit. ∎

Beispiel 1.11.13 Es gilt $S_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} A_4 \overset{\mathbb{Z}/3\mathbb{Z}}{\triangleright} V_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} \{\mathrm{Id}, [12][34]\} \overset{\mathbb{Z}/2\mathbb{Z}}{\triangleright} \{\mathrm{Id}\}$.

2 Ringe

2.1 Grundbegriffe

2.1.1 Definition

Definition 2.1.1 1. Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+ : R \times R \to R,\ (a,b) \mapsto a+b$ und $\times : R \times R \to R,\ (a,b) \mapsto ab$ so, dass

- $(R,+)$ ist eine kommutative Gruppe mit 0_R als neutrales Element,
- $(ab)c = a(bc)$ für alle $a,b,c \in R$,
- $a(b+c) = ab+ac$ und $ba+ca = (b+c)a$ für alle $a,b,c \in R$,
- es gibt ein $1_R \in R$ mit $a \cdot 1_R = 1_R \cdot a = a$ für alle $a \in R$.

2. Falls $\times$ kommutativ ist *i.e.* $ab = ba$ für alle $a,b \in R$ heißt R **kommutativer Ring**.

Bemerkung 2.1.2 Sei R ein Ring.

1. Falls $1_R = 0_R$ gilt $R = \{0_R\}$. In diesem Fall heißt R der **Nullring**.

2. Für alle $a,b \in R$ gilt

- $0_R \cdot a = a \cdot 0_R = 0_R$
- $(-a)(-b) = ab$

Beispiel 2.1.3 1. $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ und $(\mathbb{C},+,\times)$ sind Ringe.

2. $(\mathbb{Z}/n\mathbb{Z},+,\times)$ in ein Ring.

3. Sei K ein Körper. $(M_n(K),+,\times)$ ist ein Ring, wobei $+$ bzw. $\times$ Matrixaddition bzw. Matrixmultiplikation sind.

4. Für $x \in \mathbb{C}$, sei $x \mapsto \bar{x}$ die komplexe Konjugation. Die Menge der Quaternionen

$$\mathbf{H} = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \in M_2(\mathbb{C}) \mid x,y \in \mathbb{C} \right\}$$

mit Matrixaddition und Matrixmultiplikation ist ein nicht kommutativer Ring.

Definition 2.1.4 Seien R und R' zwei Ringe. Das Produkt $R \times R'$ mit $(a, a') + (b, b') = (a+b, a'+b')$ und $(a, a')(b, b') = (ab, a'b')$ ist ein Ring und heißt **Produktring** von R und R'.

Definition 2.1.5 Sei R ein Ring.

1. Ein Element $a \in R$ heißt **Einheit** oder **invertierbar** falls es ein $b \in R$ gibt mit $ab = ba = 1_R$. Mann schreibt $R^\times$ für die Menge aller Einheiten:

$$R^\times = \{a \in R \mid a \text{ is eine Einheit}\}.$$

2. Ein Element $a \in R$ heißt **Nullteiler** falls es ein $b \in R \setminus \{0_R\}$ gibt mit $ab = 0_R$ oder $ba = 0_R$.

Bemerkung 2.1.6 Sei R ein Ring.

1. Die Menge $(R^\times, \times)$ ist eine Gruppe. Insbesondere ist für $a \in R^\times$ das Element $b \in R$ mit $ab = ba = 1_R$ ein Element in $R^\times$ und ist eindeutig bestimmt. Wir schreiben $b = a^{-1}$.

2. Es gilt $R^\times \subset R \setminus \{\text{Nullteiler}\}$: sei $b \in R$ mit $ab = 0_R$ oder $ba = 0_R$. Es gilt $0_R = a^{-1}ab = b$ oder $0_R = baa^{-1} = b$.

Definition 2.1.7 Sei R ein Ring.

1. R heißt **Nullteilerfrei** falls ($a \in R$ Nullteiler $\Rightarrow a = 0$).

2. R heißt **Intergritätring** falls $R \neq \{0_R\}$, R kommtativ und Nullteilerfrei ist.

3. R heißt **Schiefkörper** falls $R^\times = R \setminus \{0_R\}$.

4. R heißt **Körper** falls R ein kommutativer Schiefkörper ist.

Beispiel 2.1.8 1. Der Ring $\mathbb{Z}$ ist ein Integritätsring.

2. Der Ring $R = \mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsring: Es gilt $[2] \neq 0_R$ aber $[2][2] = [4] = 0_R$.

3. Der Ring $\mathbf{H}$ ist ein nicht kommutativer Schiefkörper.

Bemerkung 2.1.9 Sei R ein nullteilerfreier Ring und S ein Unterring. Dann ist S nullteilerfrei.

Definition 2.1.10 Sei R ein Ring.

1. Der **Polynomring zu** R ist

$$R[X] = \{\sum_{k=0}^{\infty} r_k X^k \mid r_k \neq 0 \text{ nur für endlich viele } k\}$$

mit

$$\left(\sum_{k=0}^{\infty} r_k X^k\right) + \left(\sum_{k=0}^{\infty} r'_k X^k\right) = \sum_{k=0}^{\infty} (r_k + r'_k) X^k$$

und

$$\left(\sum_{k=0}^{\infty} r_k X^k\right) \times \left(\sum_{k=0}^{\infty} r'_k X^k\right) = \sum_{k=0}^{\infty} \left(\sum_{a+b=k} r_a r'_b\right) X^k.$$

2. Per Induktion definiert man den **Polynomring mit n Unbekannten zu R** als

$$R[X_1, \cdots, X_n] = (R[X_1, \cdots, X_{n-1}])[X_n].$$

Bemerkung 2.1.11 Sei R ein Ring.

1. Sei P ein Polynom in $R[X]$. Dann definiert P eine polynomiale Abbildung $f_P : R \to R$ durch $f_P(r) = P(r)$.

2. Man sollte aber Polynome und polynomiale Abbildungen nicht verwechseln. Zum Beispiel für $R = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ sind die Polynome $P = 0$ und $Q = X + X^2$ verschieden aber die Abbildungen die sie definieren sind $f_P : \mathbb{F}_2 \to \mathbb{F}_2$ und $f_Q : \mathbb{F}_2 \to \mathbb{F}_2$ und es gilt $f_P(x) = 0 = f_Q(x)$ für alle $x \in \mathbb{F}_2$ also $f_P = f_Q$.

Lemma 2.1.12 Sei R ein nullteilerfreier Ring. Dann ist $R[X]$ nullteilerfrei. □

Beweis. Seien $P, Q \in R[X]\backslash\{0\}$. Wir schreiben $P = \sum_{k=0}^{n} r_k X^k$ und $m = \sum_{k=0}^{m} s_k X^k$ mit $r_n \neq 0 \neq s_m$. Es gilt

$$PQ = \sum_{k=0}^{nm} \left(\sum_{a+b=k} r_a s_b\right) X^k = \sum_{k=0}^{nm} t_k X^k.$$

Insbesondere gilt $t_{nm} = r_n s_m$. Da R nulteilerfrei ist gilt $t_{nm} \neq 0$ also $PQ \neq 0$. ■

2.1.2 Ringhomomorphismus

Definition 2.1.13 Ein **Ringhomomorphismus** ist eine Abbildung $f : R \to R'$, wobei R und R' ringe sind so, dass für alle $a, b \in R$ gilt

$$f(a + b) = f(a) + f(b),\ f(ab) = f(a)f(b) \text{ und } f(1_R) = 1_{R'}.$$

Lemma 2.1.14 Sei $f : R \to R'$ ein Ringhomomorphismus.

1. Dann gilt $f(R^\times) \subset R'^\times$.

2. Die induzierte Abbildung $f : R^\times \to R'^\times$ ist ein Gruppenhomomorphismus. □

Beweis. Übung. ■

2.1.3 Unterringe und Ideale

Definition 2.1.15 Sei R ein Ring.

1. Eine Untergruppe $R' \subset R$ heißt **Unterring** falls

   - $1_R \in R'$ und
   - $ab \in R'$ für alle $a, b \in R'$.

2. Eine Untergruppe $I \subset R$ heißt **Ideal** falls $ab, ba \in I$ für alle $a \in I$ und alle $b \in R$.

Lemma 2.1.16 Sei R ein Ring und I ein Ideal. Dann gilt

$$I = R \Leftrightarrow 1_R \in I.$$

Beweis. Übung. ∎

Beispiel 2.1.17 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbf{H}$ sind Unterringe.

2. Sei R ein Ring. Die Menge $\{0_R\}$ ist ein Ideal und heißt **Nullideal**.

3. Sei R ein kommutativer Ring und $r \in R$. Dann ist $(r) = rR = \{ra \in R \mid a \in R\}$ ein Ideal.

4. Zum Beispiel ist $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal. Alle Ideale in $\mathbb{Z}$ sind dieser Form (schon alle Untergruppen sind dieser Form!).

5. Sei K ein Körper und $R = K[X]$. Dann sind alle Ideale I in R der Form $I = (P)$ für ein $P \in K[X]$ (Siehe LAII Übungsblatt 8 Übung 1).

Lemma 2.1.18 Sei $f : R \to R'$ ein Ringhomomorphismus, seien $S \subset R$ und $S' \subset R'$ Unterringe und $I \subset R$ und $I' \subset R'$ Ideale.

1. Dann sind $f(S)$ und $f^{-1}(S')$ Unterringe von R' und R. Insbesondere ist $\mathrm{Im} f$ ein Unterring.

2. 1. Dann ist $f^{-1}(I')$ ein Ideal von R. Insbesondere ist $\mathrm{Ker} f$ ein Ideal.

3. Falls f surjektiv ist, ist $f(I)$ ein Ideal in R'. □

Beweis. Bilder und Urbilder von Untergruppen sind Untergruppen.

1. Es gilt $1_R \in S$ also $1_{R'} = f(1_R) \in f(S)$. Seien $f(a), f(b) \in f(S)$ mit $a, b \in S$. Dann gilt $ab \in S$ und $f(a)f(b) = f(ab) \in f(S)$.

Es gilt $f(1_R) = 1_{R'} \in S'$ also $1_R \in f^{-1}(S')$. Seien $a, b \in f^{-1}(S')$ also $f(a), f(b) \in S'$. Dann gilt $f(ab) = f(a)f(b) \in S'$ also $ab \in f^{-1}(S')$.

2. Sei $a \in f^{-1}(I')$ und $b \in R$. Dann gilt $f(a) \in I'$ und $f(ab) = f(a)f(b) \in I'$ und $f(ba) = f(b)f(a) \in I'$.

3. Sei $f(a) \in f(I)$ mit $a \in I$ und sei $b' \in R'$. Da f surjektiv ist, gibt es ein $b \in R$ mit $f(b) = b'$. Es folgt $ab, ba \in I$ und $f(a)f(b) = f(ab) \in f(I)$ und $f(b)f(a) = f(ba) \in f(I)$. ∎

2.1.4 Quotienten

Sei R ein Ring und I ein Ideal. Dann ist $(R/I, +)$ eine Gruppe und die kanonische Projektion $\pi : R \to R/I$ ist ein Gruppenhomomorphismus.

Lemma 2.1.19 Sei R ein Ring und I ein Ideal.

1. Dann ist die Verknüpfung $\times : R/I \times R/I \to R/I$, $([a], [b] \mapsto [ab]$ wohl definiert.

2. $(R/I, +, \times)$ ist ein Ring und die kanonische Projektion $\pi : R \to R/I$ ist ein Ringhomomorphismus. □

Beweis. 1. Seien $a', b' \in R$ mit $[a'] = [a]$ und $[b'] = [b]$. Es gibt $c, d \in I$ mit $a' = a + c$ und $b' = b + d$. Dann gilt $a'b' = ab + ad + cb + cd$ und da $ad, cb, cd \in I$ gilt $[a'b'] = [ab]$.

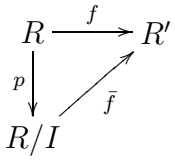
2. Übung. ∎

Definition 2.1.20 Sei R ein Ring und I ein Ideal. Dann heißt R/I mit $[a] + [b] = [a + b]$ und $[a][b] = [ab]$ der **Quotientring**.

Bemerkung 2.1.21 Sei R ein Ring und I ein Ideal. Dann gilt $I = \mathrm{Ker}\pi$, wobei $\pi : R \to R/I$ die kanonische Projektion. Also ist jeder Ideal der Kern eines Ringhomomorphismus.

Satz 2.1.22 Sei $f : R \to R'$ ein Ringhomomorphismus, sei I ein Ideal von R und sei $\pi : R \to R/I$ die kanonische Projektion.

1. Es gibt ein eindeutig bestimmter Ringhomomorphismus $\bar{f} : R/I \to R'$ so, dass das Diagram



kommutiert, genau dann wenn $I \subset \mathrm{Ker}f$.

Angenommen $I \subset \mathrm{Ker}f$ und sei $\bar{f}$ wie in 1.

2. Die Abbildung $\bar{f}$ ist genau dann injektiv, wenn $I = \mathrm{Ker}f$.

3. Die Abbildung $\bar{f}$ ist genau dann surjektiv, wenn f surjektiv ist. □

Beweis. 1. Nach Satz 1.2.10.1 existiert ein eindeutig bestimmter Gruppenhomomorphismus $\bar{f}$ wie oben genau dann, wenn $I \subset \mathrm{Ker} f$. Wir zeigen, dass $\bar{f}$ ein Ringhomomorphismus ist. Es gilt $\bar{f}([1_{R/I}]) = \bar{f}(\pi(1_R)) = f(1_R) = 1_{R'}$. Seien $a, b \in R$. Es gilt $\bar{f}([a][b]) = \bar{f}([ab]) = \bar{f}(\pi(ab) = f(ab) = f(a)f(b) = \bar{f}([a])\bar{f}([b])$.

2. Folgt aus Satz 1.2.10.2.

3. Folgt aus Satz 1.2.10.3. ∎

Korollar 2.1.23 Sei $f : R \to R'$ ein surjektiver Ringhomomorphismus. Dann gilt $R/\mathrm{Ker} f \simeq R'$.

Beispiel 2.1.24 Es gilt $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$.

2.1.5 Erzeuger

Lemma 2.1.25 Sei R ein Ring. Sei $(R_a)_{a\in A}$ ein Familie von Unterringe und sei $(I_a)_{a\in A}$ eine Familie von Ideale. Seien I und J zwei Ideale.

1. Dann ist $\bigcap_{a\in A} R_a$ ein Unterring

2. Dann sind $\bigcap_{a\in A} I_a$, $I + J = \{a + b \in R \mid a \in I, b \in J\}$ Ideale.

3. Sei $A \subset R$ eine Teilmenge. Dann gibt es ein kleinster Unterring S mit $A \subset S$.

4. Sei $A \subset R$ eine Teilmenge. Dann gibt es ein kleinstes Ideal I mit $A \subset I$. □

Beweis. 1 + 2 Übung.

3 + 4. Der kleinste Unterring bzw. das kleinste Ideal sind

$$\bigcap_{S\supset A,\ S \text{ Unterring}} S \text{ und } \bigcap_{I\supset A,\ I \text{ Ideal}} I.$$

Definition 2.1.26 Sei R ein Ring, A eine Teilmenge in R, S ein Unterring und I, J Ideale in R.

1. Der kleinste Unterring die S und A enthält heißt **der von S und A erzeugte Unterring**.

Man schreibt $S[A]$ für den von S und A erzeugten Unterring.

2. Das kleinste Ideal die A enthält heißt **das von A erzeugte Ideal**.

Man schreibt (A) für das von A erzeugte Ideal. Falls $A = \{a\}$ schreibt man $(A) = (a)$. Ein solches Ideal heißt **Hauptideal**.

2. **Die Summe von I und J** ist das Ideal $I + J = \{a + b \in R \mid a \in I, b \in J\}$.

3. **Das Produktideal von I und J** ist $IJ = (ab \mid a \in I, b \in J)$ *i.e.* das von Produkte ab mit $a \in I$ und $b \in J$ erzeugte Ideal.

Beispiel 2.1.27 1. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ ist der von $\sqrt{2}$ erzeugte Unterring von $\mathbb{R}$.

2. Allgemeiner gilt für R kommutativ, $S \subset R$ Unterring und $r \in R$:

$$S[r] = \{P(r) \in R \mid P \in S[X]\}.$$

3. Sei R ein kommutativer Ring und $r \in R$. Dann gilt $(r) = \{ra \in R \mid a \in R\}$.

Bemerkung 2.1.28 Es gilt $IJ \subset I \cap J$.

2.1.6 Isomorphiesätze

Satz 2.1.29 (Erster Isomorphiesatz) Sei R ein Ring und seien I, J Ideale.

1. Dann ist I ein Ideal in $I + J$ und $I \cap J$ ist ein Ideal in J.

2. Die Abbildung $J/(I \cap J) \to (I + J)/I$, $[a]_{I\cap J} \mapsto [a]_I$ ist wohl definiert und ein Gruppenisomorphimus. □

Beweis. 1. Klar.

2. Folgt aus dem ersten Isomorphiesatz für Gruppen. ■

Satz 2.1.30 (Zweiter Isomorphiesatz) Sei R ein Ring und I ein Ideal. Sei $J \supset I$ eine Untergruppe.

1. Dann ist J genau dann ein Ideal in R, wenn J/I ein Ideal in R/I ist.

2. Die Abbildung $(R/I)/(J/I) \to R/J$, $[[a]_I]_{J/I} \mapsto [a]_J$ ist wohl definiert und ein Ringisomorphimus. □

Beweis. 1. Sei J ein Ideal und seien $[a] \in J/I$ und $[b] \in R/I$. Dann gilt $[a][b] = [ab] \in J/I$ und $[b][a] = [ba] \in J/I$ da $ab, ba \in J$.

Umgekehrt sei J/I ein Ideal. Seien $a \in J$ und $b \in R$. Dann gilt $[ab] = [a][b] \in J/I$ und $[ba] = [b][a] \in J/I$ also $ab, ba \in J$.

2. Aus dem zweiten Isomorphiesatz für Gruppen folgt, dass die Abbildung wohl definiert ist und ein Gruppenisomorphismus. Aber per Definition des Produkts ist diese Abbildung ein Ringhomomorphismus. ■

Korollar 2.1.31 Sei R ein Ring und I ein Ideal in R und $\pi : R \to R/I$ die kanonische Projektion. Dann ist die Abbildung

$$\{\ J \text{ Ideal von } R \mid J \supset I\} \to \{\ \bar{J} \text{ Ideal von } R/I\ \},\ J \mapsto \pi(J) = J/I$$

bijektiv und es gilt $R/J \simeq (R/I)/\pi(J) = (R/I)/(J/I)$.

Beweis. Die Umkehrabbildung ist $\bar{J} \mapsto \pi^{-1}(\bar{J})$. ■

2.1.7 Primideale und maximale Ideale

Lemma 2.1.32 Sei R ein kommutativer Ring. Es gilt

$$R \text{ Körper } \Leftrightarrow \text{ die einzige Ideale in } R \text{ sind } R \text{ und } 0.$$

Beweis. ($\Rightarrow$). Sei I ein Ideal mit $I \neq 0$. Sei $a \in I$ mit $a \neq$. Dann ist a invertierbar und es gilt $1_R = a^{-1}a \in I$ also $I = R$.

($\Leftarrow$). Sei $a \in R$ mit $a \neq 0$ und sei $I = (a)$. Dann gilt $I \neq 0$ also $I = R$ und $1_R \in I$. Es gibt also ein $r \in R$ mit $ra = ar = 1_R$ also a ist invertierbar. ∎

Lemma 2.1.33 Sei $f : K \to R$ ein Ringhomomorphismus mit K ein Körper und $R \neq 0$. Dann ist f injektiv. □

Beweis. Der Kern Ker$f$ ist ein Ideal. und $f(1_K) = 1_R \neq 0_R$ also gilt Ker$f \neq K$. Da K ein Körper ist hat K nur zwei Ideale: K und 0. Es folgt Ker$f = 0$. ∎

Definition 2.1.34 Sei R ein Ring und I ein Ideal.

1. Das Ideal I heiß **Primideal**, wenn $I \neq R$ und für $a, b \in R$ gilt

$$(ab \in I) \Rightarrow (a \in I \text{ oder } b \in I).$$

1. Das Ideal I heiß **maximal**, wenn $I \neq R$ und für J ein Ideal gilt

$$(I \subset J) \Rightarrow (J = I \text{ oder } J = R).$$

Beispiel 2.1.35 Sei $R = \mathbb{Z}$. Dann ist $n\mathbb{Z}$ genau dann ein Primideal, wenn $n = 0$ oder n eine Primzahl ist.

Lemma 2.1.36 Sei R ein kommutativer Ring und I ein Ideal.

1. Das Ideal I ist genau dann ein Primideal, wenn A/I ein Integritätsring ist.

2. Das Ideal I ist genau dann maximal, wenn A/I ein Körper ist. □

Beweis. Das Ideal ist genau dann echt ($I \neq R$), wenn $R/I \neq 0$.

1. Sei I Primideal und seien $[a], [b] \in R/I$ mit $[a][b] = [0]$. Es gilt $[ab] = [0]$ also $ab \in I$. Da I Primideal ist, gilt $a \in I$ oder $b \in I$ also $[a] = [0]$ oder $[b] = [0]$.

Umgekehrt, sei R/I Integritätsring und seien $a, b \in R$ mit $ab \in I$. Dann gilt $[a][b] = [ab] = [0]$ also $[a] = [0]$ oder $[b] = [0]$. Daraus folgt $a \in I$ oder $b \in I$.

2. Sei $\pi : R \to R/I$ die kanonische Projektion. Sei I maximal und sei $\bar{J}$ ein Ideal in R/I. Dann ist $\pi^{-1}(\bar{J})$ ein Ideal in R mit $I \subset \pi^{-1}(\bar{J})$. Da I maximal ist, folgt $\pi^{-1}(\bar{J}) = I$ oder $\pi^{-1}(\bar{J}) = R$. Es folgt $\bar{J} = \pi(\pi^{-1}(\bar{J})) = I/I = ([0])$ oder $\bar{J} = R/I$. Nach dem Lemma 2.1.32 folgt, dass R/I ein Körper ist.

Umgekehrt, sei R/I ein Körper und sei J ein Ideal mit $I \subset J$. Dann ist $\pi(J)$ ein Ideal in R/I also nach Lemma 2.1.32 gilt $\pi(J) = ([0])$ oder $\pi(J) = R/I$. Daraus folgt $J = \pi^{-1}(\pi(J)) = I$ oder $J = R$ und I ist maximal. ∎

Beispiel 2.1.37 Sei $R = \mathbb{Z}[X]$. Dann ist (X) ein Primideal aber nicht maximal: es gilt $\mathbb{Z}[X]/(X) = \mathbb{Z}$ Integritätsring aber kein Körper. Das Ideal $(X, 2) \supset (X)$ ist maximal: $\mathbb{Z}[X]/(X, 2) \simeq \mathbb{Z}/(2) = \mathbb{F}_2$ ist ein Körper. Das Ideal (X^2) ist kein Primideal.

Korollar 2.1.38 Ein maximales Ideal ist ein Primideal.

Beweis. Ein Körper ist immer ein Integritätsring. ∎

Beispiel 2.1.39 1. Das Ideal $I = (X^2+1)$ ist ein Primideal und sogar ein maximales Ideal in $\mathbb{R}[X]$: es gilt $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ aber kein Primideal in $\mathbb{C}[X]$: es gilt $X-i \notin I$, $X + i \notin I$ aber $(X - i)(X + i) = X^2 + 1 \in I$.

2. Sei $x \in \mathbb{R}^n$, sei $R = C^0(\mathbb{R}^n, \mathbb{R})$ und $\mathfrak{M}_x = \{f \in R \mid f(x) = 0\}$. Dann gilt $R/\mathfrak{M}_x \simeq \mathbb{R}$ und $\mathfrak{M}_x$ ist ein maximales Ideal in R.

Bemerkung 2.1.40 Aus dem Auswahl-Axiom kann man Zeigen

Satz 2.1.41 (Satz von Krull) Sei R ein Ring und I ein Ideal mit $I \neq R$. Dann gibt est ein maximales Ideal $\mathfrak{M}$ mit $I \subset \mathfrak{M}$. □

Lemma 2.1.42 Sei $f : R \to R'$ ein Ringhomomorphismus zwischen zwei kommutativen Ringe und sei I' ein Ideal in R'.

1. Es gilt (I' Primideal) $\Rightarrow$ ($f^{-1}(I')$ Primideal).

Sei f surjektiv

2. Es gilt (I' Primideal) $\Leftrightarrow$ ($f^{-1}(I')$ Primideal).

3. Es gilt (I' maximales Ideal) $\Leftrightarrow$ (I' maximales Ideal). □

Beweis. 1. Seien $a, b \in R$ mit $ab \in f^{-1}(I')$. Es gilt $f(a)f(b) = f(ab) \in I'$ also $f(a) \in I'$ oder $f(b) \in I'$. Daraus folgt $a \in f^{-1}(I')$ oder $b \in f^{-1}(I')$.

Da f surjektiv ist gilt $R' \simeq R/\mathrm{Ker}f$ und nach identifizierung von R' mit $R/\mathrm{Ker}f$ ist die Abbildung $f : R \to R'$ mit der kanonischen Projektion $\pi : R \to R/\mathrm{Ker}f$ identifiziert.

2 und 3. Sei I' ein Ideal in $R' = R/\mathrm{Ker}f$. Sei $I = \pi^{-1}(I')$. Es gilt $I \supset J$ und $I/J = \pi(I) = I'$. Nach dem zwieten Isomorphiesatz gilt

$$R/I \simeq (R/J)/(I/J) = R'/I'.$$

Insbesondere ist R/I genau dann Integritätsring bzw. Körper, wenn R'/I' Integritätsring bzw. Körper ist. ∎

Beispiel 2.1.43 1. Sei $f : \mathbb{R}[X] \to \mathbb{C}[X]$ und $I = (X^2 + 1) \subset \mathbb{C}[X]$. Dann gilt $f^{-1}(I) = (X^2+1) \subset \mathbb{R}[X]$ und $f^{-1}(I)$ ist ein Primideal und maximal aber I ist nicht maximal und kein Primideal.

2. Sei $f : \mathbb{Z} \to \mathbb{Q}$ die enthaltung. Sei $I = (0) \subset \mathbb{Q}$. Dann gilt $f^{-1}(I) = (0) \subset \mathbb{Z}$. Das Ideal I ist ein Primideal in $\mathbb{Q}$ und sogar maximal aber $f^{-1}(I)$ ist ein Primideal aber nicht maximal.

2.1.8 Teilerfremde Ideale

In diesem Abschnitt ist R ein kommutativer Ring.

Definition 2.1.44 Zwei Elemente $a, b \in R$ heißen **teilerfremd** falls

$$(c \mid a \text{ und } c|b \;\Rightarrow\; c \in R^\times) \text{ für alle } c \in R.$$

Beispiel 2.1.45 1. Seien $n, m \in \mathbb{Z}$. Dann sind n und m genau dann teilerfremd, wenn $\mathrm{ggT}(n, m) = 1$.

2. Sei K ein Körper und $R = K[X, Y]$. Dann sind X und Y teilerfremd: sei P mit $P|X$ und $P|Y$. Dann gilt $P = \lambda$ oder $P = \lambda X$ für $\lambda \in K^\times$ und $P = \lambda$ oder $P = \lambda Y$ für $\lambda \in K^\times$. Es folgt $P = \lambda \in K^\times \subset R^\times$.

Definition 2.1.46 Sei R ein Ring. Zwei Ideale I und J heißen **teilerfremd** falls $I + J = R$.

Beispiel 2.1.47 1. Sei $R = \mathbb{Z}$, $I = n\mathbb{Z} = (n)$ und $J = m\mathbb{Z} = (m)$. Dann sind I und J genau dann teilerfremd, wenn n und m teilerfremd sind.

2. Sei K ein Körper und $R = K[X, Y]$. Seien $I = (X)$ und $J = (Y)$. Dann sind I und J nicht teilerfremd: es gilt $I + J = (X) + (Y)$. Sei $P \in I + J$. Dann gibt es Polynome $S, T \in R$ mit $P = XR + YT$. Daraus folgt $P(0, 0) = 0$. Insbesondere gilt $1 \notin I + J$ und $I + J \neq R$.

Lemma 2.1.48 Sei R ein kommutativer Ring. Seien $a, b \in R$ und $I = (a)$, $J = (b)$.

1. Es gilt: (I und I sind teilerfremd) $\Rightarrow$ (a und b sind teilerfremd).

Sei R ein Hauptidealring *i.e.* alle Ideale I' sind der Form $I' = (a')$ für ein $a' \in R$.

2. Es gilt: (I und I sind teilerfremd) $\Leftrightarrow$ (a und b sind teilerfremd). □

Beweis. 1. Es gilt $(a) + (b) = I + J = R$. Es gibt also $x, y \in R$ mit $1 = ax + by$. Sei $c \in R$ mit $c|a$ und $c|b$. Es gibt also $\alpha, \beta \in R$ mit $a = c\alpha$ und $b = c\beta$. Daraus folgt

$$1 = ax + by = c\alpha x + c\beta y = c(\alpha x + \beta y)$$

und c ist invertierbar.

2. ($\Rightarrow$) folgt aus 1. ($\Leftarrow$). Da R ein Hauptidealring ist gibt es ein $c \in R$ mit $(a) + (b) = I + J = (c)$. Es genügt zu zeigen, dass $c \in R^\times$ gilt: daraus folgt $(c) = R$. Es gilt $a \in (a) + (b) = (c)$ also gibt es ein $\alpha \in R$ mit $a = c\alpha$ *i.e.* $c|a$. Analog gilt $c|b$. Da a und b teilerfremd sind folgt $c \in R^\times$. ■

Satz 2.1.49 (Chinesischer Restsatz) Sei R ein kommutativer Ring und $I_1, \cdots, I_n$ paarweise teilerfremde Ideale. Dann ist die Abbildung

$$R/\bigcap_k I_k \to \prod_k R/I_k,\ [a] \mapsto ([a]_{R/I_1}, \cdots, [a]_{R/I_n}).$$

wohl definiert und ein Isomorphismus. □

Beweis. Die Abbildung $f' : R \to \prod_k R/I_k,\ a \mapsto ([a]_{R/I_1}, \cdots, [a]_{R/I_n})$ ist wohl definiert. Die obige Abbildung f wird wohl definiert sei sobald $\bigcap_k I_k \subset \mathrm{Ker} f'$. Sei $a \in \bigcap_k I_k$. Dann gilt $a \in I_k$ für alle k. Daraus folgt $[a]_{R/I_k} = [0]_{R/I_k}$ und $a \in \mathrm{Ker} f'$.

Wir zeigen $\mathrm{Ker} f' = \bigcap_k I_k$. Sei $a \in \mathrm{Ker} f'$. Dann gilt $[a]_{R/I_k} = [0]_{R/I_k}$ für alle k also gilt $a \in I_k$ für alle k und es folgt $a \in \bigcap_k I_k$. Daraus folgt, dass f injektiv ist.

Es bleibt zu zeigen, dass f surjektiv ist. Es genügt jetzt zu zeigen, dass f' surjektiv ist. Sei $j \in [1, n]$. Wir zeigen zuerst, dass I_j und $\bigcap_{k \neq j} I_k$ teilerfremd sind. Für $k \neq j$ sind I_j und I_k teilerfremd also $I_j + I_k = R$ und es gibt $a_{j,k} \in I_j$ und $b_k \in I_k$ mit $1 = a_{j,k} + b_k$ Daraus folgt

$$1 = \prod_{k \neq j} (a_{j,k} + b_k) = c_j + \prod_{k \neq j} b_k$$

wobei $c_j \in I_j$. Da $b_k \in I_k$ gilt $\prod_{k \neq j} b_k \in I_k$ für alle $k \neq j$ also $\prod_{k \neq j} b_k \in \bigcap_{k \neq j} I_k$. Daraus folgt $1 \in I_j + \bigcap_{k \neq j} I_k$ und $R = I_j + \bigcap_{k \neq j} I_k$. Sei $d_j = \prod_{k \neq j} b_k$. Es gilt $c_j + d_j = 1$, $c_j \in I_j$ und $d_j \in \cap_{k \neq j} I_k$.

Sei $\pi_j : R \to R/I_j$ die kanonische Projektion. Es gilt $\pi_j(c_j) = [c_j]_{R/I_j} = [0]_{R/I_j}$ da $c_j \in I_j$. Es gilt $\pi_j(d_j) = \pi_j(1 - c_j) = \pi_j(1) = [1]_{R/I_j}$. Und es gilt $\pi_j(d_\ell) = [d_\ell]_{R/I_j} = [0]_{R/I_j}$ für $\ell \neq j$ da $d_\ell \in \bigcap_{k \neq \ell} I_k$ und $j \in \{k \mid k \neq \ell\}$.

Sei $([a_1]_{R/I_1}, \cdots, [a_n]_{R/I_n}) \in \prod_k R/I_k$ und sei

$$a = \sum_{\ell=1}^{n} d_\ell a_\ell.$$

Es gilt

$$\pi_j(a) = \sum_{\ell=1}^{n} \pi_j(d_\ell)\pi_j(a_\ell) = [a_j]_{R/I_j}.$$

Daraus folgt $f(a) = ([a_1]_{R/I_1}, \cdots, [a_n]_{R/I_n})$ und f ist surjektiv. ∎

Korollar 2.1.50 Seien $n, m \in \mathbb{Z}$ teilerfremd. Es gilt

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Beweis. Da n und m teilerfremd sind, gilt $n\mathbb{Z} \cap m\mathbb{Z} = mn\mathbb{Z}$. ∎

Lemma 2.1.51 Sei $n \in \mathbb{Z}$. Dann gilt

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[m] \in \mathbb{Z}/n\mathbb{Z} \mid m \text{ und } n \text{ sind teilerfremd}\}.$$

Beweis. Siehe Übungsblatt 6. ∎

Definition 2.1.52 Die **Eulersche φ-Funktion** ist die Abbildung $\varphi : \mathbb{Z}_{>0} \to \mathbb{N}$ definiert durch

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{[m] \in \mathbb{Z}/n\mathbb{Z} \mid m \text{ und } n \text{ sind teilerfremd}\}|.$$

Bemerkung 2.1.53 Es gilt $\varphi(1) = 1$ und $\varphi(p) = p - 1$ für p ein Primzahl.

Lemma 2.1.54 Sei p ein Primzahl und $\alpha \in \mathbb{N}_{>0}$. Es gilt $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

Beweis. Ein Element $m \in [1, p^\alpha]$ is genau dann teilerfremd mit p^α, wenn p kein Teiler von m ist. Die Elemente in $[1, p^\alpha]$ die durch p teilbar sind, sind die Elemente pk mit $k \in [1, p^{\alpha-1}]$. Es sind also genau $p^{\alpha-1}$ Elemente die durch p teilbar sind und $p^\alpha - p^{\alpha-1}$ Elemente die durch p nicht teilbar sind. ∎

Lemma 2.1.55 Seien $R_1, \cdots, R_n$ Ringe. Es gilt $(\prod_k R_k)^\times = \prod_k (R_k^\times)$. □

Beweis. Übung. ∎

Korollar 2.1.56 Sei $n \in \mathbb{Z}$ und $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primzahlzerlegung. Es gilt

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_1 - 1}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Beweis. Da die Zahlen $p_i^{\alpha_i}$ paarweise teilerfremd sind, sind die Ideale $p_i^{\alpha_i}\mathbb{Z}$ paarweise teilerfremd und es gilt

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\cap_i p_i^{\alpha_i}\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Nach dem obigen Lemma gilt

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times| = \prod_i |(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times| = \prod_i \varphi(p_i^{\alpha_i}).$$

Nach Lemma 2.1.54 folgt die Aussage. ∎

Satz 2.1.57 Sei $n \in \mathbb{Z}$. Dann ist die Abbildung

$$\Phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

definiert durch $a \mapsto \Phi_a$, wobei $\Phi_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ x \mapsto ax$ ist ein Gruppenisomorphismus. □

Beweis. Siehe Übungsblatt 6. ∎

2.2 Quotientkörper

In diesem Abschnitt ist R ein Integritätsring.

Definition 2.2.1 Sei $\sim$ die Relation auf $R \times (R \setminus \{0\})$ definiert durch

$$(a, b) \simeq (c, d) \Leftrightarrow ad = bc.$$

Lemma 2.2.2 Die Relation $\sim$ ist eine Äquivalenzrelation. □

Beweis. Es gilt $ab = ba$ also $(a, b) \sim (a, b)$. Seien $(a, b) \sim (c, d)$. Es gilt $ad = bc$ also $cb = da$ und es folgt $(c, d) \sim (a, b)$. Seien $(a, b) \sim (c, d) \sim (e, f)$. Es gilt $ad = bc$ und $cf = de$. Daraus folgt $adf = bcf = bde$. Da $d \neq 0$ und R Integritätsring folgt $af = be$ also $(a, b) \sim (e, f)$. ■

Definition 2.2.3 Sei $\mathrm{Frac}(R) = (R \times (R \setminus \{0\}))\,/\,\sim$ die Menge aller Äquivalenzklassen für $\sim$. Wir Schreiben $\frac{a}{b}$ für die Äquivalenzklasse $[(a, b)]$ von (a, b).

Satz 2.2.4 Sei R ein Integritätsring.

1. Die Menge $\mathrm{Frac}(R)$ mit $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ ist ein Körper.

2. Die Abbildung $R \to \mathrm{Frac}(R)$, $a \mapsto \frac{a}{1}$ is ein injektiver Ringhomomorphimus. □

Beweis. 1. Zuerst zeigen wir , dass die Addition und die Multiplikation wohl definiert sind. Sei $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$. Dann gilt $\frac{ac}{bd} = \frac{acb'd'}{bdb'd'} = \frac{ba'c'd}{bdb'd'} = \frac{a'c'}{b'd'}$. Analog ist die Addition wohl definiert.

Da das Produkt in R assoziativ und kommutativ ist ist das Produkt in $\mathrm{Frac}(R)$ auch kommutativ und assoziativ. Da R ein kommutativer Ring folgt, dass $+$ kommutativ ist. Man überprüft leicht, dass $\frac{0}{1}$ ein neutrales Element für $+$ ist und es gilt $\frac{a}{b} + \frac{-a}{b} = \frac{0}{b} = \frac{0}{1}$ also ist $(\mathrm{Frac}(R), +)$ eine kommutative Gruppe. Distributivitätsgesetzt überprüft man leicht. Es gilt $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b}$ also ist $\frac{1}{1}$ ein neutrales Element für die Multiplikation.

Sei $\frac{a}{b} \neq \frac{0}{1}$. Dann gilt $a \neq 0$ also ist $\frac{b}{a}$ wohl definiert. Es gilt $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$. Also ist $\mathrm{Frac}(R)$ ein Körper.

2. Es gilt $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$ also ist die Abbildung ein Ringhomomorphismus. Sei $\frac{a}{1}$ im Kernel. Es gilt $\frac{a}{1} = \frac{0}{1}$ und es folgt $a = 0$. ■

2.3 Noethersche Ringe

In diesem Abschnitt arbeiten wir mit kommutative Ringe.

Definition 2.3.1 Sei R ein kommutativer Ring und I ein Ideal.

1. I heißt **endlich erzeugt** falls es endlich viele Elemente $a_1, \cdots, a_n \in R$ gibt mit $I = (a_1, \cdots, a_n)$.

2. Ein Ring heißt **noetherscher Ring** falls alle Ideale endlich erzeugt sind.

Beispiel 2.3.2 1. Ein Hauptidealring ist ein notherscher Ring (alle Ideale sind von einem Element erzeugt).

2. Insesondere sind $\mathbb{Z}$ und $K[X]$ mit K ein Körper noethersche Ringe.

Satz 2.3.3 Sei R ein kommutativer Ring. Die folgende Aussagen sind äquivalent:

1. R ist ein noetherscher Ring.
2. Jede aufsteigende Kette $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ von Ideale ist stationär *i.e.* es gibt ein $N \in \mathbb{N}$ mit $I_n = I_N$ für alle $n \geq N$.
3. Jede (nicht leere) Familie $(I_\lambda)_{\lambda \in \Lambda}$ von Ideale hat ein maximales Element. □

Beweis. (1. $\Rightarrow$ 2.) Sei $I = \bigcup_n I_n$. Dann ist I ein Ideal: seien $a, b \in I$, dann gibt es n, m mit $a \in I_n$ und $b \in I_m$. Ohne Einschränkung können wir annehmen $n \leq m$. Also $a \in I_n \subset I_m$ und $a + b \in I_m \subset I$. Sei jetzt $c \in R$. Dann gilt $ac \in I_n$ also $ac \in I$.

Da R noethersch ist gibt es Elemente $a_1, \cdots, a_k \in R$ mit $I = (a_1, \cdots, a_k)$. Per Definition von I gibt es Zahlen n_i mit $a_i \in I_{n_i}$ für jedes i. Sei $N = \max_i\{n_i\}$. Dann gilt $a_i \in I_{n_i} \subset I_N$ für jedes i. Daraus folgt $I = (a_1, \cdots, a_k) \subset I_N$ und also $I = I_N$. Es folgt $I_n \subset I = I_N$ für alle n und $I_n = I_N$ für alle $n \geq N$.

(2. $\Rightarrow$ 3.) Angenommen habe die Familie $(I_\lambda)_{\lambda \in \Lambda}$ kein maximales Element. Wir konstruiren per Induktion nach n ein nicht stationäre aufsteigende Kette von Ideale. Sei $I_1 := I_{\lambda_1}$ ein Elemente in der Familie. Da I_1 nicht maximal ist gibt es ein $\lambda_2 \in \Lambda$ mit $I_1 \subsetneq I_2 := I_{\lambda_2}$. Sei die Kette $I_1 \subsetneq \cdots \subsetneq I_n$ konstruiert. Da I_n kein maximales Element ist gibt es ein $\lambda_{n+1} \in \Lambda$ mit $I_n \subsetneq I_{n+1} := I_{\lambda_{n+1}}$.

(3. $\Rightarrow$ 1.) Sei I ein Ideal und $E = \{J \text{ endlich erzeugtes Ideal mit } J \subset I\}$. Da $(0) \subset E$ ist E eine nicht leere Familie von Ideale und hat also ein maximales Element J. Falls $J \subsetneq I$ gibt es ein $a \in I$ mit $a \notin J$. Dann ist $J + (a)$ endlich erzeugt und es gilt $J \subsetneq J + (a) \subset I$. Ein Widerspruch zur Maximalität. ■

Beispiel 2.3.4 3. Der Ring $R = \mathbb{R}[x_1, \cdots, X_n, \cdots]$ mit unendlich viele Unbekannten ist nicht noethersch: es gibt eine nicht stationäre unendliche aufsteigende Kette von Ideale: $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n) \subsetneq \cdots$

Theorem 2.3.5 Sei R ein noetherscher Ring. Dann ist $R[X]$ auch noethersch. □

Korollar 2.3.6 Sei R ein noetherscher Ring. Dann ist $R[X_1, \cdots, X_n]$ auch noethersch.

2.4 Teilbarkeit

In diesem Abschnitt arbeiten wir mit kommutative Ringe.

2.4.1 Assoziierte, irreduzibel und Primelemente

Definition 2.4.1 Sei R ein kommutativer Ring und seien $a, b \in R$. Das Element a **teilt** b oder ist **ein Teiler von** b (oder b ist von a teilbar) falls es ein $c \in R$ gibt mit $b = ac$. Man schreibt $a|b$.

Bemerkung 2.4.2 Sei R ein kommutativer Ring und $a, b \in R$.

1. Es gilt $a|b \Leftrightarrow (b) \subset (a)$.

2. Sei a invertierbar und $b \in R$, dann gilt $(b) \subset R = (a)$ also $a|b$.

Definition 2.4.3 Sei R ein kommutativer Ring. Man definiert die Relation $\mathcal{R}$ auf R durch

$$a\mathcal{R}b \Leftrightarrow a|b \text{ und } b|a \Leftrightarrow (a) = (b).$$

Bemerkung 2.4.4 Aus der Definition folgt, dass $\mathcal{R}$ eine Äquivalenzrelation ist.

Lemma 2.4.5 Sei R ein Integritätsring und $a, b \in R$. Es gilt

$$a\mathcal{R}b \Leftrightarrow (\exists u \in R^\times \text{ mit } a = ub).$$

Beweis. Falls $a = ub$ mit $u \in R^\times$ gilt $b|a$ und $b = u^{-1}a$ also $a|b$ und $a\mathcal{R}b$. Umgekehrt, sei $a\mathcal{R}b$. Dann gibt es $c, d \in R$ mit $a = bc$ und $b = ad$. Daraus folgt $ab = abcd$ also $ab(1 - cd) = 0$. Falls $a = 0$ folgt $b = ad = 0$ und es gilt $a = 0 = 1 \cdot 0 = 1 \cdot b$. Anlog für $b = 0$. Wir können also annehmen, dass $a \neq 0$ und $b \neq 0$. Da R ein Intergritätsring ist folgt von $ab(1 - cd) = 0$, dass $cd = 1$ und c und d sind invertierbar. Die Aussage folgt. ∎

Ab jetzt ist R ein Integritätsring.

Definition 2.4.6 Elemente $a, b \in R$ heißen **assoziiert** falls $a\mathcal{R}b$.

Satz 2.4.7 Sei $HI(R)$ die Menge aller Hauptideale in R. Die Abbildung

$$R/\mathcal{R} \to HI(R),\ a \mapsto (a)$$

ist eine Bijektion. □

Beweis. Übung. ∎

Definition 2.4.8 Sei $a \in R$ mit $a \neq 0$ und $a \notin R^\times$.

1. Dann heißt a **Primelement** falls gilt

$$(a|bc \Leftrightarrow a|b \text{ oder } a|c) \text{ für alle } b, c \in R.$$

2. Dann heißt a **irreduzibel** falls gilt

$$(a = bc \Rightarrow b \in R^\times \text{ oder } c \in R^\times) \text{ für alle } b, c \in R.$$

3. Falls a nicht irreduzibel ist heisst a **reduzibel**.

Beispiel 2.4.9 Für $R = \mathbb{Z}$ sind die irreduzibel und die Primelemente die Primzahlen.

Satz 2.4.10 Sei $a \in R$ mit $a \neq 0$ und $a \notin R^\times$.

1. Es gilt a Primelemente $\Rightarrow$ a irreduzibel.

2. Es gilt a Primelement $\Leftrightarrow$ (a) Primideal.

3. Es gilt a irreduzibel $\Leftrightarrow$ (für alle $b \in R \setminus R^\times$ gilt $(a) \subset (b) \Rightarrow (a) = (b)$) *i.e.* (a) ist maximal unter allen Hauptidealen. □

Beweis. 1. Seien $b, c \in R$ mit $a = bc$. Da a ein Primelement ist gilt $a|b$ oder $a|c$. Ohne Beschränkung können wir annehmen, dass $a|b$. Da $a = bc$ gilt $b|a$ also $a\mathcal{R}b$ und es gibt ein $u \in R^\times$ mit $a = bu$. Es folgt $bc = a = bu$ und da R ein Integritätsring ist folgt $c = u \in R^\times$.

2. Per Definition.

3. ($\Rightarrow$). Sei $a \in R$ irreduzibel und $b \in R \setminus R^\times$. Angenommen $(a) \subset (b)$, dann gilt $b|a$ und es gibt ein $c \in R$ mit $a = bc$. Da a irreduzibel ist, folgt $c \in R^\times$. Also $a\mathcal{R}b$ und $(a) = (b)$.

($\Leftarrow$). Sei $a \in R$ und seien $b, c \in R$ mit $a = bc$ und $b \notin R^\times$. Es gilt $b|a$ also $(a) \subset (b)$ und nach Annahme gilt $(a) = (b)$. Daraus folgt $a\mathcal{R}b$ also es gibt ein $u \in R^\times$ mit $a = bu$. Es folgt $bc = a = bu$ und da R ein Integritätsring ist folgt $c = u \in R^\times$. ■

Beispiel 2.4.11 Sei $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$. Dann ist $3 \in R$ irreduzibel aber kein Primelement. Seien $x, y \in R$ mit $xy = 3$. Wir schreiben $x = a + bi\sqrt{5}$ und $y = c + di\sqrt{5}$. Sei $x \mapsto \bar{x}$ die komplexe Konjugation. Es gilt

$$9 = 3 \times \bar{3} = xy\bar{x}\bar{y} = x\bar{x}y\bar{y} = (a^2 + 5b^2)(c^2 + 5d^2).$$

Es folgt $a^2+5b^2 \in \{1,3,9\}$. Die einzige möglichkeiten für x und y sind also

a^2+5b^2	1	3	9
x	± 1	keine Lösung	± 3 $\pm(2+i\sqrt{5})$ $\pm(2-i\sqrt{5})$
c^2+5d^2	9	3	1
y	± 3 $\pm(2+i\sqrt{5})$ $\pm(2-i\sqrt{5})$	keine Lösung	± 1.

Insbesondere gilt $x \in R^\times$ oder $y \in R^\times$ also 3 ist irreduzibel. Analog kann man auch zeigen, dass $2+i\sqrt{5}$ und $2-i\sqrt{5}$ irreduzibel sind.

Es gilt aber $3|9 = (2+i\sqrt{5})(2-i\sqrt{5})$ und 3 teilt weder $2+i\sqrt{5}$ nor $2-i\sqrt{5}$: es gilt

$$\frac{2+i\sqrt{5}}{3} = \frac{2}{3} + \frac{1}{3}i\sqrt{5} \notin R \text{ und } \frac{2-i\sqrt{5}}{3} = \frac{2}{3} - \frac{1}{3}i\sqrt{5} \notin R.$$

Daraus folgt, dass 3 kein Primelement ist.

Definition 2.4.12 Sei R ein Intergritätsring.

1. Ein Ideal I heißt **Hauptideal** falls es ein $a \in R$ gibt mit $I = (a)$.

2. Der Ring R heißt **Hauptidealring** falls alle Ideale in R Hauptideale sind.

Satz 2.4.13 Sei R ein Hauptidealring und $a \in R$ mit $a \neq 0$ und $a \notin R^\times$. Dann gilt

$$(a \text{ Primelement}) \Leftrightarrow (a \text{ irreduzibel}) \Leftrightarrow ((a) \text{ Primideal}) \Leftrightarrow ((a) \text{ maximales Ideal}).$$

Beweis. (a Primelement) $\Rightarrow$ (a irreduzibel) folgt aus Satz 2.4.10.1.

(a Primelement) $\Leftrightarrow$ ((a) Primideal) folgt aus Satz 2.4.10.2.

((a) maximales Ideal) $\Rightarrow$ ((a) Primideal) folgt aus Korollar 2.1.38.

Da R ein Hauptidealring ist folgt aus folgt aus Satz 2.4.10.3: (a irreduzibel) $\Leftrightarrow$ ((a) maximales Ideal).

Die folgende Implikationen haben wir gezeigt:

$$\begin{array}{ccc} (a \text{ Primelement}) & \Longrightarrow & (a \text{ irreduzibel}) \\ \Updownarrow & & \Updownarrow \\ ((a) \text{ Primideal}) & \Longleftarrow & ((a) \text{ maximales Ideal}). \end{array}$$

Es folgt, dass alle Aussagen äquivalent sind. ∎

2.4.2 Faktorielle Ringe

In diesem Abschnitt ist R ein Integritätsring.

Definition 2.4.14 Sei R ein Integritätsring und $a \in R$.

1. Eine **Primzerlegung von** a is eine Sequenz $p_1, \cdots, p_r \in R$ mit p_i Primelement für alle i und $a \mathcal{R} p_1 \cdots p_r$.

2. Eine **Zerlegung von** a **in irreduziblen Elementen** is eine Sequenz $p_1, \cdots, p_r \in R$ mit p_i irreduzibel für alle i und $a \mathcal{R} p_1 \cdots p_r$.

Beispiel 2.4.15 In $R = \mathbb{Z}$ ist die Primzerlegung eine Zerlegung in irreduziblen Elementen.

Lemma 2.4.16 Sei R ein Integritätsring. Sei $a \mathcal{R} p_1 \cdots p_r$ eine Primzerlegungen und $a \mathcal{R} q_1 \cdots q_s$ eine Zerlegungen in irrediziblen Elementen. Dann gilt $r = s$ und $p_i \mathcal{R} q_i$ modulo Umnummerierung. □

Beweis. Per Induktion nach $r+s$. Für $r+s = 0$ ist die Aussage klar. Die Behauptung sei wahr für $r + s - 1$. Es gilt $p_1 \mathcal{R} q_1 \cdots q_s$. Da p_1 eine Primzahl ist folgt, dass es ein $i \in [1, s]$ gibt mit $p_1 | q_i$. Sei $b \in R$ mit $q_i = p_1 b$. Da q_i irreduzibel ist, folgt $p_1 \in R^\times$ oder $b \in R^\times$. Da p_1 Primelement ist $p_1 \notin R^\times$ also $b \in R^\times$ und $p_1 \mathcal{R} q_i$. Es folgt $p_2 \cdots p_r \mathcal{R} \prod_{k \neq i} q_k$ und die Behauptung folgt nach Induktionsannahme. ∎

Korollar 2.4.17 Jede Primzerlegung ist bis auf Reihenfolge eindeutig bestimmt.

Beispiel 2.4.18 In $R = \mathbb{Z}[i\sqrt{5}]$ sind

$$3 \times 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$$

zwei Zerlegungen in irreduziblen Elementen. Es gilt aber $3 \not\mathcal{R} 2 + i\sqrt{5}$ und $3 \not\mathcal{R} 2 - i\sqrt{5}$.

Definition 2.4.19 Ein Integritätsring R heißt **faktoriell** falls gilt

(E) (**Existenz**) Jedes $a \in R \setminus \{0\}$ hat eine Zerlegung in irreduziblen Elemente;

(U) (**Einzigkeit = Uniqueness**) Diese Zerlegung ist bis auf Reihenfolge eindeutig.

Die Haupteigenschaft hier ist (U): zum Beispiel erfüllt $\mathbb{Z}[i\sqrt{5}]$ die Eigenschaft (E) aber nicht (U).

Satz 2.4.20 Sei R ein noetherscher Integritätsring. Dann gilt (E). □

Beweis. Wir betrachten die folgende Familie von Ideale:

$A = \{(a) \text{ Hauptideal} \mid a \neq 0 \text{ und } a \text{ hat keine Zerlegung in irreduziblen Elementen}\}$.

Insbesondere für $(a) \in A$ gilt $a \notin R^\times$ und a ist nicht irreduzibel. Angenommen (E) sei falsch. Dann ist A nicht leer. Da R noethersch ist gibt es ein maximales Element $(a) \in A$. Da a nicht irreduzibel ist gibt es $b, c \in R \setminus R^\times$ mit $a = bc$. Es gilt also $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Aber da (a) maximal war gilt $(b), (c) \notin A$. Es gibt also Zerlegungen in irreduziblen Elementen $b\mathcal{R}p_1 \cdots p_r$ und $c\mathcal{R}q_1 \cdots q_s$. Daraus folgt $a\mathcal{R}p_1 \cdots p_r q_1 \cdots q_s$ und a hat auch eine Zerlegung in irreduziblen Elementen. Ein Widerspruch zu $(a) \in A$. ∎

Satz 2.4.21 Sei R ein Integritätsring mit (E). Die folgende Aussagen sind äquivalent:

1. R ist faktoriell;
2. (**Lemma von Euklid**) Es gilt (a Primelement) $\Leftrightarrow$ (a irreduzibel).
3. (**Satz von Gauß**) Es gilt ($a|bc$ und a und b sind teilerfremd) $\Rightarrow$ (a teilt c). □

Beweis. (2 $\Rightarrow$ 1). Folgt vom Lemma 2.4.16.

(3 $\Rightarrow$ 2). Sei a irreduzibel und seien $b, c \in R$ mit $a|bc$. Falls $a|b$ sind wir fertig. Andernfalls sei d mit $d|a$ und $d|b$. Da a irreduzibel folgt $d \in R^\times$ oder $d\mathcal{R}a$. Im lezten Fall folgt $a|b$ ein Widerspruch also $d \in R^\times$ und a und b sind teilerfremd. Nach Annahme gilt $a|c$.

(1 $\Rightarrow$ 3). Seien $a, b, c \in R$ mit $a|bc$ und a und b teilerfremd. Sei $d \in R$ mit $ad = bc$ und seien $a\mathcal{R}p_1 \cdots p_r$, $b\mathcal{R}q_1 \cdots q_s$, $c\mathcal{R}n_1 \cdots n_t$ und $d\mathcal{R}m_1 \cdots m_u$ die Zerlegungen von a, b, c, d in irreduziblen Elementen. Es gilt

$$p_1 \cdots p_r m_1 \cdots m_u \mathcal{R} q_1 \cdots q_s n_1 \cdots n_t.$$

Da dies zwei Zerlegungen in irreduziblen Elementen sind folgt: für jedes p_i gibt es ein j mit $p_i\mathcal{R}q_j$ oder ein k mit $p_i\mathcal{R}n_k$. Da a und b teilerfremd sind kommt der erste Fall nicht vor. Modulo Umnummerierung können wir annehmen $p_1\mathcal{R}n_1$. Wir können also durch p_1 teilen. Es gilt

$$p_2 \cdots p_r m_1 \cdots m_u \mathcal{R} q_1 \cdots q_s n_2 \cdots n_t.$$

Analog gibt es für p_2 ein j mit $p_2 = q_j$ oder $p_2 = n_k$ und da a und b teilerfremd sind kommer der erste Fall nicht vor. Nach Umnummerierung gilt $p_2\mathcal{R}n_2$. Per Induktion folgt $t \geq r$ und $p_i\mathcal{R}n_i$ für alle i. Daraus folgt $a = p_1 \cdots p_r \mathcal{R} n_1 \cdots n_r | n_1 \cdots n_t$ und $a|c$. ∎

Korollar 2.4.22 Ein Hauptidealring ist faktoriell.

Beweis. Sei R ein Hauptidealring. Dann ist R noethersch also (E) gilt. Dann gilt auch das Lemma von Euklid (Satz 2.4.13) und (U) gilt. ∎

Satz 2.4.23 Sei R ein Integritätsring. Die folgende Aussagen sind äquivalent:

1. R ist faktoriell;
2. Jedes $a \in R \setminus \{0\}$ hat eine Primzerlegung. □

Beweis. (2 $\Rightarrow$ 1). Eine Primzerlegung ist eine Zerlegung in irreduziblen Elementen also folgt (E). Nach Lemma 2.4.16 folgt (U).

(1 $\Rightarrow$ 2). Nach dem obigen Satz gilt (a irreduzibel) $\Leftrightarrow$ (a Primelement). Die Aussage 2. folgt jetzt nach (E). ∎

Definition 2.4.24 Sei R ein faktorieller Ring und seien $a, b \in R$. Seien

$$a \mathcal{R} p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ und } b \mathcal{R} p_1^{\beta_1} \cdots p_r^{\beta_r}$$

die Primzerlegungen von a und b.

1. **Der größter gemeinsame Teiler von** a **und** b ist

$$\mathrm{ggT}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_r^{\min(\alpha_r, \beta_r)}.$$

Der ggT ist nur modulo invertierbare Elementen wohl definiert.

1. **Das kleinste gemeinsame Viefache von** a **und** b ist

$$\mathrm{kgV}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

Das kgV ist nur modulo invertierbare Elementen wohl definiert.

Bemerkung 2.4.25 Sei R faktoriell und seien $a, b \in R$. Die Elemente a, b sind genau dann teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$.

Lemma 2.4.26 Sei R ein Hauptidealring (also faktoriell). Seien $a_1, \cdots, a_n \in R$.

1. Es gilt $(a_1) + \cdots + (a_n) = (a_1, \cdots, a_n) = (\mathrm{ggT}(a_1, \cdots, a_n))$.
2. Es gilt $(a_1) \cap \cdots \cap (a_n) = (\mathrm{kgV}(a_1, \cdots, a_n))$.
3. Es gilt $(a_1) \cdots (a_n) = (a_1 \cdots a_n)$. □

Beweis. Sei $a_i \mathcal{R} p_1^{\alpha_{i,1}} \cdots p_r^{\alpha_{i,r}}$ die Primzerlegung und seien $\beta_k = \max_i(\alpha_{i,k})$ und $\gamma_k = \min_i(\alpha_{i,k})$. Es gilt $\mathrm{kgV}(a_1, \cdots, a_n) = p_1^{\beta_1} \cdots p_r^{\beta_r}$ und $\mathrm{ggT}(a_1, \cdots, a_n) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$.

1. Die Gleichung $(a_1) + \cdots + (a_n) = (a_1, \cdots, a_n)$ gilt in jedem kommutativen Ring: sei $a \in (a_1) + \cdots + (a_n)$. Dann gibt es $x_1, \cdots x_n \in R$ mit $a = \sum_i x_i a_i \in (a_1, \cdots, a_n)$. Umgekehrt, es gilt $a_i \in (a_1) + \cdots (a_n)$ für jedes $i \in [1, n]$. Daraus folgt $(a_1, \cdots, a_n) \subset (a_1) + \cdots + (a_n)$.

Sei $a \in R$ mit $(a) = (a_1, \cdots, a_n)$. Dann gilt $a_i \in (a)$ für jedes i. Daraus folgt $a | a_i$ für jedes i. Sei $a \mathcal{R} p_1^{\delta_1} \cdots p_r^{\delta_r}$ die Primzerlegung von a. Es folgt $\delta_k \leq \min_i(\alpha_{i,k}) = \gamma_k$. Sei $b = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$. Es gilt $a|b$ und $b|a_i$ für jedes i. Es gilt aber auch $a = \sum_i x_i a_i$ also $b|a$. Daraus folgt $a \mathcal{R} b$ und $a = b$.

2. Sei $a \in R$ mit $(a) = (a_1) \cap \cdots \cap (a_n)$ und sei $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$. Es gilt $a_i | b$ für jedes i also $b \in (a_1) \cap \cdots (a_n) = (a)$. Daraus folgt $a|b$. Sei $a \mathcal{R} p_1^{\delta_1} \cdots p_r^{\delta_r}$ die Primzerlegung von a. Es gilt $\delta_k \leq \beta_k$. Es gilt auch $a \in (a_i)$ also $a_i | a$ für jedes i. Daraus folgt $\delta_k \geq \alpha_{i,k}$ für jedes k und $\delta_k = \beta_k$ also $a = b$.

3. Sei $a \in R$ mit $(a) = (a_1) \cdots (a_n)$ und sei $b = a_1 \cdots a_n$. Es gilt $b \in (a_1) \cdots (a_n) = (a)$ also $a|b$. Es gilt auch $a \in (a_1) \cdots (a_n)$ also a is eine Summe von Elementen der Form $x_1 a_1 \cdots x_n a_n = b x_1 \cdots x_n$. Daraus folgt $b|a$ und $a \mathcal{R} b$ also $(a) = (b)$. ∎

2.4.3 Satz von Gauß

Sei R ein faktorieller Ring.

Lemma 2.4.27 Es gilt ($R[X]$ Hauptidealring $\Leftrightarrow$ R Körper). □

Beweis. Siehe Übungsblatt 8. ∎

Beispiel 2.4.28 Sei $R = \mathbb{Z}$. Der Ring $R[X] = \mathbb{Z}[X]$ ist kein Haupidealring da $I = (X, 2)$ kein Hauptideal ist: Sei $P \in \mathbb{Z}[X]$ mit $I = (P)$. Es folgt $2 \in (P)$ also $P|2$ und $P = \pm 2$. Aber es folgt auch $P|X$. Ein Widerspruch.

Definition 2.4.29 Sei $P = a_0 + \cdots + a_n X^n \in R[X]$ mit $p \neq 0$.

1. Der **Inhalt** von P ist $c(P) = \mathrm{ggT}(a_0, \cdots, a_n)$. Der Inhalt ist nur bis auf einem Element von $R^\times$ definiert.

2. Das Polynom P heißt **primitiv** falls $c(P) = \mathrm{ggT}(a_0, \cdots, a_n) = 1$.

Bemerkung 2.4.30 1. Sei $P \in R[X]$ mit $p \neq 0$. Das Element P ist genau dann primitiv, wenn es kein Primelement $p \in R$ gibt mit $p|P$.

2. Sei $P = a_0 + \cdots + a_n X^n$ primitiv und $a \in R$ dann gilt

$$c(aP) = \mathrm{ggT}(aa_0, \cdots, aa_n) = a\,\mathrm{ggT}(a_0, \cdots, a_n) = a.$$

Lemma 2.4.31 (Lemma von Gauß) Seien $P, Q \in R[X]$. Dann gilt

$$c(PQ) \mathcal{R} c(P)c(Q) \text{ i.a.W } c(PQ) = c(P)c(Q) \text{ (modulo } R^\times).$$

Beweis. Erster Fall: $c(P) = c(Q) = 1$. Wir zeigen $c(PQ) = 1$. Sei $p \in R$ ein Primelement mit $p|PQ$. Wir arbeiten in $R' = R/(p)[X] = R[X]/(p)$. Da p ein Primelement ist, ist (p) ein Primideal in R also ist $R/(p)$ ein Integritätsring. Daraus folgt, dass $R' = R/(p)[X]$ ein Integritätsring ist. Da $p|PQ$ gilt $[PQ] = [0]$ in R'. Es folgt $[P] = [0]$ oder $[Q] = [0]$ in R'. Es folgt $p|P$ oder $p|Q$ also $c(P) \neq 1$ oder $c(Q) \neq 1$.

Im allgemein: sei $a = c(P)$ und $b = c(Q)$. Sei $P' = \frac{1}{a}P \in R[X]$ und $Q' = \frac{1}{b}Q \in R[X]$. Es gilt $c(P') = c(Q') = 1$. Daraus folgt $c(P'Q') = 1$ Es gilt also $c(PQ) = c(aP'bQ') = c(abP'Q') = ab\ c(P'Q') = ab = c(P)c(Q)$. ∎

Satz 2.4.32 Sei R faktoriell und $K = \text{Frac}(R)$. Es gilt

$$(P \in R[X] \setminus R \text{ irreduzibel}) \Leftrightarrow (P \text{ ist primitiv in } R[X] \text{ und irreduzibel in } K[X]).$$

Beweis. ($\Leftarrow$). Sei $P = a_0 + \cdots + a_n X^n \in R[X]$ primitiv mit P irreduzibel in $K[X]$. Seien $Q, S \in R[X]$ mit $P = QS$. Da P irreduzibel in $K[X]$ folgt $Q \in K[X]^\times$ oder $S \in K[X]^\times$. Aber es gilt $(K[X])^\times = K^\times$ also $Q \in R[X] \cap K = R$ oder $S \in R[X] \cap K = R$. Also ist Q oder ist S ein teiler von $\text{ggT}(a_0, \cdots, a_n) = 1$ *i.e.* $Q \in R^\times$ oder $S \in R^\times$.

($\Rightarrow$). Falls es ein Primelement $p \in R$ gibt mit $p|P$, gilt $P = pQ$ mit $\deg(Q) > 0$ also $Q \notin (R[X])^\times$ und $p \notin R^\times = (R[X])^\times$. Also ist P nicht irreduzibel. Widerspruch. Daraus folgt P primitiv.

Seien $Q, S \in K[X]$ mit $P = QS$. Wir schreiben $Q = \sum_k \frac{q_k}{r_k} X^k$ und $S = \sum_k \frac{s_k}{t_k} X^k$ mit maximalen gekürzten Brüchen $\frac{q_k}{r_k}$ und $\frac{s_k}{t_k}$. Seien

$$a = \text{ggT}(q_k),\ b = \text{kgV}(r_k) \text{ und } c = \text{ggT}(s_k)\ d = \text{kgV}(t_k).$$

Es gilt $Q' = \frac{a}{b}Q \in R[X]$ und $S' = \frac{c}{d}S \in R[X]$ und beide Polynome sind primitiv in $R[X]$. Es gilt also

$$bd = c(bdP) = c(bdQS) = c(acQ'S') = c(aQ'cS')\ \mathcal{R}\ c(aQ')c(cS') = ac.$$

Es folgt $\frac{a}{b}\frac{c}{d} = u \in R^\times$ und $P = uQ'S'$. Da P irreduzibel ist folgt $Q' \in (R[X])^\times$ oder $S' \in (R[X])^\times$ also $Q = \frac{a}{b}Q' \in (K[X])^\times$ oder $S = \frac{c}{d}S' \in (K[X])^\times$ ∎

Bemerkung 2.4.33 Für $p \in R$ gilt

$$p \text{ irreduzibel in } R[X] \Leftrightarrow p \text{ irreduzibel in } R.$$

Satz 2.4.34 (Satz von Gauß) Sei R faktoriell. Dann ist $R[X]$ faktoriell. □

Beweis. Wir zeigen (E) für $R[X]$. Sei $K = \mathrm{Frac}(R)$. Da $K[X]$ noethersch ist ($K[X]$ ist ein Hauptidealring) ist (E) in $K[X]$ wahr.

Sei $P \in R[X]$ und sei $a = c(P)$. Es gilt $P = aP'$ mit $c(P') = 1$. Das Element a lässt sich als Produkt von irreduziblen darstellen $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ mit p_i irreduzibel in R. Da (E) für $K[X]$ wahr ist gibt es irreduzible Polynome $P_1, \cdots, P_s \in K[X]$ mit $P' = P_1^{\beta_1} \cdots P_r^{\beta_s}$. Seien $a_i, b_i \in R$ mit

$$P_i = \frac{a_i}{b_i} P_i' \text{ wobei } P_i' \in R[X] \text{ mit } c(P_i) = 1.$$

Da P_i irreduzibel ist ist auch P_i' irreduzibel in $K[X]$ und also in $R[X]$ (nach dem obigen Satz). Es gilt also

$$P = aP' = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \frac{a_1^{\beta_1} \cdots a_s^{\beta_s}}{b_1^{\beta_1} \cdots b_s^{\beta_s}} (P_1')^{\beta_1} \cdots (P_s')^{\beta_s}.$$

Es folgt

$$b_1^{\beta_1} \cdots b_s^{\beta_s} P = a a_1^{\beta_1} \cdots a_s^{\beta_s} (P_1')^{\beta_1} \cdots (P_s')^{\beta_s}$$

und

$$a b_1^{\beta_1} \cdots b_s^{\beta_s} = c(b_1^{\beta_1} \cdots b_s^{\beta_s} P) \mathcal{R} a a_1^{\beta_1} \cdots a_s^{\beta_s} c(P_1')^{\beta_1} \cdots c(P_s')^{\beta_s} = a a_1^{\beta_1} \cdots a_s^{\beta_s}.$$

Daraus folgt $\frac{a_1^{\beta_1} \cdots a_s^{\beta_s}}{b_1^{\beta_1} \cdots b_s^{\beta_s}} = u \in R^\times$ und

$$P = u p_1^{\alpha_1} \cdots p_r^{\alpha_r} (P_1')^{\beta_1} \cdots (P_s')^{\beta_s}.$$

Dies zeigt (E).

Um (U) zu zeigen, genügt es zu zeigen: $P \in R[X]$ irreduzibel $\Rightarrow$ P Prielement *i.e.* (P) Primideal.

Fall 1: $P = p \in R$. Dann gilt $R[X]/(P) = R[X]/(p) = (R/(p))[X]$. Da p irreduzibel ist und R faktoriell ist (p) Primideal i nR. Es folgt $R/(p)$ ist ein Integritätsring und $R/(p)[X]$ ist ein Integritätsring.

Fall 2: $P \in R[X] \setminus R$. Wir haben ein injektiver Ringhomomorphismus $R \to K$, $a \mapsto \frac{a}{1}$. Damit erhalten wir ein injektiver Ringhomomorphismus $R[X] \to K[X]$ definiert durch $P = \sum_k a_k X^k \mapsto \sum_k \frac{a_k}{1} X^k$. Dank Komposition mit der kanonischen Projektion $K[X] \to K[X]/(P)$ haben wir ein Ringhomomorphismus

$$f : A[X] \to K[X]/(P).$$

Wir zeigen, dass $\mathrm{Ker} f = (P) \subset R[X]$. Daraus wird folgen, dass es ein injektiver Ringhomomorphismus

$$A[X]/(P) \to K[X]/(P)$$

gibt. In diesem Fall ist $A[X]/(P)$ ein Unterring von $K[X]/(P)$ und da P irreduzibel in $K[X]$ ist, ist $K[X]/(P)$ ein Integritätsring also $R[X]/(P)$ auch.

Wir zeigen $\mathrm{Ker} f = (P) \subset R[X]$. Sei $Q \in (P) \subset R[X]$ *i.e.* $Q = PS$ mit $S \in R[X]$. Dann gilt $S \in K[X]$ und $Q \in (P) \subset K[X]$ also $f(Q) = [0]$. Umgekehrt, sei $Q \in \mathrm{Ker} f$. Es gilt $f(Q) = [0]$ also $f(Q) \in (P) \subset K[X]$. Es gibt also $S \in K[X]$ mit $Q = PS$. Seien $a, b \in R$ mit $S = \frac{a}{b} S'$ und $S' \in R[X]$ und $c(S') = 1$. Sei $c = c(Q)$ und $Q' \in R[X]$ primitiv mit $Q = cQ'$. Es gilt

$$cbQ' = aPS'.$$

Daraus folgt $cb = c(cbQ') = c(aPS') \mathcal{R} ac(P)c(S') = a$. Daraus folgt, dass es ein $u \in R^\times$ gibt mit $ubc = a$ also $\frac{a}{b} = uc \in R$. Es folgt $S \in R[X]$ und $Q \in (P) \subset R[X]$.∎

2.5 Anwendung: irreduzible Polynome

Sei R ein Integritätsring und sei $K = \mathrm{Frac}(R)$.

Lemma 2.5.1 Sei $P \in K[X]$ irreduzibel. Dann ist $K[X]/(P)$ ein Körper. □

Beweis. Das Polynom ist ein Primelement (da $K[X]$ faktoriell ist). Daraus folgt, dass $K[X]/(P)$ ein Integritätsring ist. Sei $[Q] \neq [0]$ in $K[X]/(P)$. Die Abbildung $K[X]/(P) \to K[X]/(P)$, $[S] \mapsto [Q][S]$ ist also injektiv. Aber $K[X]/(P)$ ist auch ein endlich dimensionaler K-Vektorraum und diese Abbildung ist K-linear also ei nIsomorphismus. Es folgt, dass diese Abbildung surjektiv ist. Es gibt also ein $[S] \in K[X]/(P)$ mit $[Q][S] = [1]$ *i.e.* $[Q]$ ist invertierbar. ∎

Es ist also wichtig Irreduzibilitätskriterien für $P \in K[X]$ zu haben.

Satz 2.5.2 (Irreduzibilitätskriterium von Eisenstein) Seien R faktoriell, $P = a_n X^n + \cdots + a_0 \in R[X] \setminus R$ und $p \in R$ ein Primelement mit

1. $p \nmid a_n$,
2. $p | a_k$ für $k \in [0, n-1]$ und
3. $p^2 \nmid a_0$.

Dann ist P irreduzibel in $K[X]$. Falls P primitiv ist ist P irreduzibel in $R[X]$. □

Beweis. Der zweite Teil folgt aus dem Satz 2.4.32.

Ohne Einschränkung können wir annehmen, dass P primitiv ist. Nach dem Satz 2.4.32 genügt es zu zeigen, dass P irreduzibel in $R[X]$. Seien $Q, S \in R[X]$ mit $P = QS$ und $0 < q = \deg Q, s = \deg S < n$. Wir schreiben $Q = \sum_{k=1}^{q} b_k X^k$ und $S = \sum_{k=1}^{s} c_k X^k$.

Da p ein Primelement ist ist $R/(p)$ ein Integritätsring und $R/(p)[X]$ ist auch ein Integritätsring. Sei $L = \mathrm{Frac}(R/(p))$. In $L[X]$ gilt

$$[a_n]X^n = [P] = [Q][R] = ([b_q]X^q + \cdots + [b_0])([c_r]X^r + \cdots + [c_0]).$$

Es folgt $[b_q][c_s] = [a_n] \neq 0$ also $[b_q] \neq 0$ und $[c_s] \neq 0$. Die Polynome $[Q], [S]$ sind beide nicht konstant. Aber $L[X]$ ist faktoriell also ist nach der obigen Gleichung X der einzige Primteiler von $[Q]$ und $[S]$. Es folgt, dass X teilt $[Q]$ und $[S]$ und also $[b_0] = 0$ und $[c_0] = 0$. Daraus folgt $p|b_0$ und $p|c_0$ also $p^2|b_0c_0 = a_0$. Ein Widerspruch.∎

Beispiel 2.5.3 1. Sei $R = \mathbb{Z}$. Das Polynom $P = X^4 - 6$ ist irreduzibel in $\mathbb{Z}[X]$: Eisenstein mit $p = 2$ oder $p = 3$.

2. Allgemeiner sei $d \in \mathbb{Z}$ so, dass d hat ein Primteiler p mit Vielfachkeit 1. Dann ist $X^n - d$ irreduzibel für alle $n \in \mathbb{N}$: Eisenstein mit p.

3. Sei K ein Körper und $R = K[X, Y]$. Dann ist $P = Y^2 - X(X-1)(X-\lambda)$ für $\lambda \in K \setminus \{0, 1\}$ irreduzibel: Eisenstein mit $R = K[X]$ und $p = X$.

Definition 2.5.4 Sei $n \in \mathbb{N}$. Das n-te **Kreisteilungspolynom** ist

$$\Phi_n = \prod_{\substack{\mathrm{ggT}(k,n)=1 \\ k=1}}^{n} (X - e^{\frac{2ik\pi}{n}}).$$

Korollar 2.5.5 Sei $p \in \mathbb{Z}$ eine Primzahl.

1. Es gilt $\Phi_p = X^{p-1} + \cdots + X + 1$.

2. Das Polynom Φ_p ist irreduzibel in $\mathbb{Z}[X]$.

Beweis. 1. In $\mathbb{Q}[X]$ gilt

$$\Phi_p = \prod_{\substack{\mathrm{ggT}(k,p)=1 \\ k=1}}^{p} (X - e^{\frac{2ik\pi}{n}}) = \prod_{k=1}^{p-1} (X - e^{\frac{2ik\pi}{n}}) = \frac{X^p - 1}{X - 1}.$$

Daraus folgt die Aussage.

2. Sei $Y = X - 1$ und sei $P(Y) = \Phi_p(X) = \Phi_p(Y+1)$. Wir zeigen zuerst ($P$ irreduzibel $\Leftrightarrow$ Φ_p irreduzibel).

($\Rightarrow$). Seien Q, S mit $\Phi_p = QS$. Dann gilt $P(Y) = \Phi_p(Y+1) = Q(Y+1)S(Y+1)$. Seien $Q'(Y) = Q(Y+1)$ und $S'(Y) = S(Y+1)$. Es gilt $P = Q'S'$ also Q' ist invertierbar oder S' ist invertierbar. Es folgt Q ist invertierbar oder S ist invertierbar. Also Φ_p ist irreduzibel.

($\Leftarrow$). Analog.

Es genügt zu zeigen, dass P irreduzibel ist. Es gilt

$$P(Y) = \Phi_p(Y+1) = \frac{(Y+1)^p - 1}{(Y+1) - 1} = Y^{p-1} + \binom{p}{p-1} Y^{p-2} + \cdots + \binom{p}{1}.$$

Es gilt $p|\binom{p}{k}$ für $0 < k < p$ und $p^2 \not| p = \binom{p}{1}$. Nach Eisenstein folgt, dass P irreduzibel ist. ∎

Satz 2.5.6 (Reduktionsverfahren) Seien R faktoriell, $P = a_n X^n + \cdots + a_0 \in R[X] \setminus R$ und I ein Primideal in R mit $a_n \notin I$. Sei $K = \mathrm{Frac}(R)$.

Dann gilt ($[P]$ irreduzibel in $(R/I)[X] \Rightarrow P$ irreduzibel in $K[X]$). □

Beweis. Ohne Einschränkung können wir annehmen, dass P primitiv ist. Wir zeigen, dass P irreduzibel in $R[X]$ ist. Seien $Q, S \in R[X]$ mit $P = QS$. Es gilt $[P] = [Q][S]$ und da $[P]$ irreduzibel ist folgt $[Q]$ invertierbar oder $[R]$ invertierbar. Insbesondere gilt $\deg([Q]) = 0$ oder $\deg([S]) = 0$. Da $\deg([Q]) \leq \deg Q$ und $\deg([S]) \leq \deg S$, folgt $\deg(P) \geq \deg P - \deg(Q) = \deg(S) \geq deg([S]) = \deg([P]) - \deg([Q]) = \deg([P]) = \deg(P)$ oder $\deg(P) \geq \deg P - \deg(S) = \deg(Q) \geq \deg([Q]) = \deg([P]) - \deg([S]) = \deg([P]) = \deg(P)$. In beide Fälle haben wir überall gleichungen und $\deg(Q) = 0$ oder $\deg(S) = 0$. Es folgt Q invertierbar oder S invertierbar. ∎

Bemerkung 2.5.7 Das Polynom ist nicht unbedingt irreduzibel in $R[X]$: Für $R = \mathbb{Z}[X]$, $I = (3)$ und $P = 2X$ gilt $[P] = [X]$ irreduzibel also $P = 2X$ ist irreduzibel in $\mathbb{Q}[X]$ aber nicht in $\mathbb{Z}[X]$. Die Primzerlegung von P ist $P = 2 \cdot X$.

Beispiel 2.5.8 Sei $P = X^3 + 462X^2 + 2433X - 67691 \in \mathbb{Z}[X]$. Dann ist P irreduzibel: Sei $I = (2)$. Es gilt $[P] = X^3 + X + 1 \in \mathbb{F}_2[X]$. Dieses Polynom ist irreduzibel da es keine Nullstelle in $\mathbb{F}_2$ gibt.

3 Körper

3.1 Grundbegriffe

Definition 3.1.1 1. Sei R ein Integritätsring und $f : \mathbb{Z} \to R$, $n \mapsto n \cdot 1_K$ und sei $\mathrm{Ker} f = (p)$. Die Zahl p heißt **Charakteristik von** R.

2. Das Bild $\mathrm{Im} f$ von f ist ein Integritätsunterring von R und heißt **Primring von** R.

Bemerkung 3.1.2 Sei R ein Integritätsring und $p = \mathrm{char}(R)$. Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\mathrm{Ker} f \simeq \mathrm{Im} f$ ein Integritätsring ist muss (p) ein Primideal sein. Also $p = 0$ oder p ist eine Primzahl. Es gilt

$$\text{Primring von } R \ = \begin{cases} \mathbb{Z} & \text{falls } \mathrm{char}(R) = 0 \\ \mathbb{Z}/p\mathbb{Z} & \text{falls } \mathrm{char}(R) = p. \end{cases}$$

Definition 3.1.3 1. Ein **Körper** ist ein kommutativer Ring K mit $K^\times = K \setminus \{0\}$.

2. Seien K, L zwei Körper. Eine Abbildung $\varphi : K \to L$ heißt **Körperhomomorphismus**. falls es ein Ringhomomorphismus ist.

2. Sei K ein Körper. Ein Teilkörper k von K ist ein Unterring von K so, dass $(x \in k \setminus \{0\} \Rightarrow x^{-1} \in k)$.

3. **Der Primkörper** P_K eines Körpers K ist

$$P_K = \bigcap_{k \subset K \text{ Teilkörper}} k.$$

Lemma 3.1.4 Sei K ein Körper. Es gilt

$$P_K = \begin{cases} \mathbb{Q} & \text{falls } \mathrm{char}(R) = 0 \\ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} & \text{falls } \mathrm{char}(R) = p. \end{cases}$$

Beweis. Sei $k \subset K$ ein Teilkörper. Es gilt $1_K \in k$ und also $\mathrm{Im} f \subset k$. Seien $a, b \in \mathrm{Im} f \subset k$ mit $b \neq 0$. Dann ist $\frac{a}{b} \in k$. Es folgt $\mathrm{Frac}(\mathrm{Im} f) \subset k$. Daraus folgt die Aussage. ∎

Lemma 3.1.5 Sei $\varphi : K \to L$ ein Körperhomomorphismus. Dann ist φ injektiv. □

Beweis. Folgt aus Lemma 2.1.33. ∎

Lemma 3.1.6 Sei $K \subset L$ ein Teilkörper. Dann ist L ein K-Vektorraum. □

Beweis. Die Addition ist die übliche Addition in L. Die Skalarmultiplikation von $a \in K$ mit $x \in L$ ist dank dem Produkt $ax \in L$ in L defniert. Die Eigenschaften eines Vektorraums folgen aus den Eigenschaften des Körpes L. ∎

Definition 3.1.7 Sei K ein Körper.

1. Ein Körperhomomorphismus $K \subset L$ heißt **Körpererweiterung** von K.

2. Der **Grad** der Körpererweiterung $K \subset L$ ist $[L : K] = \dim_K L$.

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

4. Ein Körper L' heißt **Zwischenkörper** der Erweiterung $K \subset L$ falls $K \subset L' \subset L$. falls

Beispiel 3.1.8 1. $\mathbb{R} \subset \mathbb{C}$ ist von Grad 2: $[\mathbb{C} : \mathbb{R}] = 2$.

2. Man zeigt, dass die Erweiterung $\mathbb{Q} \subset \mathbb{R}$ nicht endlich ist.

Bemerkung 3.1.9 Sei $K \subset L$ eine Erweiterung mit K und L endlich. Dann gilt

$$|L| = |K|^n, \text{ wobei } n = [L : K].$$

Satz 3.1.10 (Gradformel) Seien $K \subset L \subset M$ Erweiterungen, sei $(e_i)_{i\in I}$ eine Basis von L als K-Vektorraum und sei $(f_j)_{j\in J}$ eine Basis von M als L-Vektorraum.

Dann ist $(e_i f_j)_{i\in I\ j\in J}$ eine Basis von M als K-Vektorraum. □

Beweis. Wir zeigen, dass $(e_i f_j)_{i\in I\ j\in J}$ linear unabhängig ist. Seien Skalare $(\lambda_{i,j})_{i\in I\ j\in J}$ mit

$$\sum_{i\in I\ j\in J} \lambda_{i,j} e_i f_j = 0.$$

Es gilt

$$\sum_{j\in J} \left(\sum_{i\in I} \lambda_{i,j} e_i \right) f_j = 0.$$

Da $(f_j)_{j\in J}$ linear unabhängig ist gilt

$$\sum_{i\in I} \lambda_{i,j} e_i = 0$$

für alle $j \in J$. Da $(e_i)_{i\in I}$ linear unabhängig ist gilt $\lambda_{i,j} = 0$ für alle i und alle j.

Wir zeigen, dass $(e_i f_j)_{i\in I\ j\in J}$ ein EZS ist. Sei $m \in M$. Es gibt Skalare $\mu_j \in L$ mit

$$x = \sum_j \mu_j f_j.$$

Es gibt auch Skalare $\lambda_{i,j}$ mit

$$\mu_j = \sum_i \lambda_{i,j} e_i.$$

Es folgt

$$x = \sum_{i,j} \lambda_{i,j} e_i f_j$$

und die Aussage folgt. ∎

Korollar 3.1.11 Seien $K \subset L \subset M$ Erweiterungen. Es gilt

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

Korollar 3.1.12 Seien $K \subset L$ eine Erweiterung so, dass $[L : K]$ eine Primzahl ist. Dann hat $K \subset L$ keine Zwischenkörper.

3.2 Algebraische und transzendente Elemente

Definition 3.2.1 Sei K ein Körper.

1. Der Ring $K[X]$ ist ein Integritätsring. Der Quotientkörper $\mathrm{Frac}(K[X])$ dieses Ringes heißt **der rationale Funktionkörper** und ist $K(X)$ bezeichnet.

2. Die Elementen in $K(X)$ heißen **rationale Funktionen** und sind der Form

$$\frac{P}{Q}$$

wobei $P \in K[X]$ und $Q \in K[X] \setminus \{0\}$.

Bemerkung 3.2.2 Es gilt $[K(X) : K] = \infty$.

Lemma 3.2.3 Sei $K \subset L$ eine Erweiterung, sei $(K_i)_{i\in I}$ eine Familie von Teilkörpern von L und sei $A \subset L$ eine Teilmenge.

1. Dann ist $\bigcap_{i\in I} K_i$ ein Teilkörper von L.

2. Es gibt ein minimaler Teilkörper $K(A)$ von L der A und K enthält.

3. Für $A = \{x_1, \cdots, x_n\}$ gilt

$$K(A) = \left\{ \frac{P(x_1, \cdots, x_n)}{Q(x_1, \cdots, x_n)} \mid P, Q \in K[X_1, \cdots, X_n] \right\}.$$

Beweis. 1. Übung.

2. Es gilt

$$K(A) = \bigcap_{\substack{K' \subset L \text{ Unterkörper} \\ K \cup A \subset K'}} K'.$$

3. Übung. ∎

Definition 3.2.4 Sei $K \subset L$ eine Erweiterung und sei $A \subset L$ eine Teilmenge.

1. Der Körper $K(A)$ heißt **der von A über K erzeugte Teilkörper von L.**

Für $A = \{a\}$ Schreiben wir $K(A) = K(a)$.

2. Die Erweiterung $K \subset L$ heißt **einfach** falls es ein $a \in L$ gibt mit $L = K(a)$.

3. Für $a \in L$ heißt $[K(a) : K]$ **der Grad von a über K**

Definition 3.2.5 Sei $K \subset L$ eine Erweiterung und $a \in L$.

1. Das Element a heißt **algebraisch über** K, falls es ein $P \in K[X] \setminus \{0\}$ gibt $P(a) = 0$.

2. Falls a nicht algebraisch ist heißt a **transzendent**.

Beispiel 3.2.6 1. $i = \sqrt{-1} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ und $\mathbb{Q}$.

2. $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$.

3. $X \in K(X)$ ist transzendent über K.

4. Man zeigt, dass e und π transzendent über $\mathbb{Q}$ sind (aber nicht über $\mathbb{R}$).

Lemma 3.2.7 Sei $K \subset L$ eine Erweiterung und $a \in L^\times$.

1. Die Abbildung $\mathrm{ev}_a : K[X] \to L$, $P \mapsto P(a)$ ist ein Ringhomomorphismus.

2. Es gilt (ev_a injektiv) $\Leftrightarrow$ (a transzendent).

In diesem fall gilt $K[X] \simeq \mathrm{Im}(\mathrm{ev}_a) = K[a] \subsetneq K(a) \simeq K(X)$.

3. Sei $(P) = \mathrm{Ker}(\mathrm{ev}_a)$. Dann ist (P) ein Primideal. Es gilt

$$((P) \text{ maximal}) \Leftrightarrow (P \text{ irreduzibel}) \Leftrightarrow (a \text{ algebraisch}).$$

In diesem Fall gilt $K(a) = K[a] = \mathrm{Im}(\mathrm{ev}_a)$ und $[K(a) : K] = \deg P$. □

Beweis. 1. Übung.

2. Die erste Aussage folgt aus der Definition. Da ev_a injektiv ist, gilt $\mathrm{Im}(\mathrm{ev}_a) \simeq K[X]$. Da $P(a) \neq 0$ für $P \neq 0$ haben wir ein Körperhomomorphismus $K(X) \to K(a) \subset L$ definiert durch $\frac{P}{Q} \mapsto \frac{P(a)}{Q(a)}$. Diese Abbildung ist injektiv (als Körperhomomorphismus) und surjektiv nach dem obigen Lemma. Daraus folgt $K[a] \simeq K[X] \subsetneq K(X) = K(a)$.

3. Der Quotient $K[X]/(P)$ ist ein Unterring von L also ist ein Integritätsring. Daraus folgt, dass (P) ein Primideal ist. Da $K[X]$ ein Hauptidealring ist, folgt die erste Äquivalenz aus dem Satz 2.4.13. Falls P irreduzibel ist gilt $P \neq 0$ und nach der Definition ist a algebraisch. Umgekehrt falls a algebraisch ist ist $(P) = \mathrm{Ker}(\mathrm{ev}_a)$ nicht trivial und ein Primideal. Die Aussage folgt aus dem Satz 2.4.13.

Wenn a algebraisch ist ist $K[a] = \mathrm{Im}(\mathrm{ev}_a) \simeq K[X]/(P)$ ein Körper (da (P) maximal ist). Aber es gilt $K[a] \subset K(a)$ und da $K(a)$ der von a über K erzeugte Körper ist folgt $K[a] = K(a)$. Daraus folgt die letzte Aussage. ∎

Definition 3.2.8 Sei $K \subset L$ eine Erweiterung und $a \in L$ algebraisch. **Das minimal Polynom** von a über K ist das normierte Polynom χ_a so, dass $\mathrm{Ker}(\mathrm{ev}_a) = (\chi_a)$.

Bemerkung 3.2.9 Sei $K \subset L$ eine Erweiterung und $a \in L$ algebraisch.

1. Das Polynom χ_a is irreduzibel: Das Ideal $\mathrm{Ker}(\mathrm{ev}_a) = (\chi_a)$ ist ein Primideal also ist χ_a irreduzibel.

2. Es gilt $\deg \chi_a = [K(a) : K]$.

3. Für $Q \in K[X]$ mit $Q(a) = 0$ gilt $\chi_a | Q$.

Beispiel 3.2.10 Die Zahlen $\sqrt{2}$, $i = \sqrt{-1}$, $\sqrt[3]{2}$ sind algebraisch. Es gilt

$$\chi_{\sqrt{2}} = X^2 - 2,\ \chi_{\sqrt{-1}} = X^2 + 1 \text{ und } \chi_{\sqrt[3]{2}} = X^3 - 2.$$

Satz 3.2.11 Sei $K \subset L$ eine Erweiterung und $a \in L$. Die folgende Aussagen sind äquivalent:

1. a is algebraisch,
2. $K[a] = K(a)$,
3. $[K(a) : K] < \infty$. □

Beweis. (1. $\Leftrightarrow$ 2.) Folgt aus dem obigen Lemma.

(1. $\Rightarrow$ 3.) Folgt aus dem obigen Lemma: Es gilt $\chi_a \neq 0$ und $[K(a) : K] = \deg(\chi_a) < \infty$.

(3. $\Rightarrow$ 1.) Folgt aus dem obigen Lemma: Für a transcendent gilt $K(a) \simeq K(X)$ und also $[K(a) : K] = \infty$. ∎

Lemma 3.2.12 Sei $K \subset L$ eine Erweiterung und $a \in L$. Es gilt $[K(a) : K] | [L : K]$.□

Beweis. Wir haben Erweiterungen $K \subset K(a) \subset L$. Nach der Gradformel gilt $[L : K] = [L : K(a)][K(a) : K]$. ∎

Definition 3.2.13 Eine Erweiterung $K \subset L$ heißt **algebraisch** falls jedes $a \in L$ algebraisch über K ist. Ansonsten heißt $K \subset L$ **transzendent**.

Lemma 3.2.14 Sei $K \subset L$ ein endliche Erweiterung. Dann ist $K \subset L$ algebraisch.□

Beweis. Sei $a \in L$. Es gilt $[L : K] = [L : K(a)][K(a) : K]$. Insbesondere gilt $[K(a) : K] < \infty$ und a ist algebraisch. ∎

Satz 3.2.15 Sei $K \subset L$ eine Erweiterung. Sei

$$M = \{a \in L \mid a \text{ ist algebraisch über K }\}.$$

Dann ist M ein Zwischenkörper. □

Beweis. Seien $a, b \in M$. Sei $K(a, b)$ der von a, b erzeugte Teilkörper. Es gilt $K(a, b) = (K(a))(b)$ und da b algebraisch über K ist, ist b auch algebraisch über $K(a)$. Es folgt $[K(a, b) : K(a)] = [(K(a))(b) : K(a)] < \infty$. Daraus folgt $[K(a, b) : K] = [K(a, b) : K(a)][K(a) : K]\infty$, weil a algebraisch über K ist. Also ist $K(a, b)$ endlich über K und alle Elemente in $K(a, b)$ sind algebraisch über K *i.e.* $K(a, b) \subset M$. Es folgt $-a \in M$, $a + b \in M$, $ab \in M$ und $a^{-1} \in M$. Also M ist ein Teilkörper von L. ∎

Definition 3.2.16 Sei $K \subset L$ eine Erweiterung. Dann heiß

$$\overline{K} = M = \{a \in L \mid a \text{ ist algebraisch über K }\}$$

der algebraische Abschluß von K **in** L.

Beispiel 3.2.17 1. Nicht alle algebraische Erweiterungen sind endlich. Sei $K = \mathbb{Q}$, sei $K_n = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_n})$ wobei p_n die n-te Primzahl ist und sei

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_n}, \cdots).$$

Dann gilt

$$K = K_0 \subsetneq K_1 \subsetneq K_2 \cdots \subsetneq K_n \subsetneq \cdots \subsetneq L.$$

Sei $M = \{a \in L \mid a \text{ ist algebraisch über K }\}$. Dann gilt $\sqrt{p_n} \in M$ für alle n also $M = L$, weil M ein Körper ist. Es folgt, dass L algebraisch über K ist. Aber $[L : K] = \infty$.

2. Sei $K = \mathbb{Q}$ und $L = \mathbb{C}$. Dann ist

$$\overline{\mathbb{Q}} = M = \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q} \}$$

algebraisch über $\mathbb{Q}$ aber nicht endlich (es gilt $\sqrt{p} \in \overline{\mathbb{Q}}$ für alle Primzahl $\mathbb{Q}$). Es gilt auch $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$, z.B. sind π und e nicht algebraisch (Anderer Beweis: $\overline{\mathbb{Q}}$ ist die Menge aller Nullstellen von Polynomen $P \in \mathbb{Q}[X]$. Da es nur endlich viele Nullstellen gibt und da $\mathbb{Q}[X]$ abzählbar ist, ist auch $\overline{\mathbb{Q}}$ abzählbar und also $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$).

Satz 3.2.18 Sei $K \subset L$ eine Erweiterung. Dann sind die folgende Aussagen äquivalent:

1. Die Erweiterung $K \subset L$ ist endlich.
2. Es gibt algebraische Elemente $a_1, \cdots, a_n \in L$ mit $L = K(a_1, \cdots, a_n)$. □

Beweis. (1. $\Leftrightarrow$ 2.) Sei $(a_1, \cdots, a_n)$ eine Basis von L über K. Dann sind $a_1, \cdots, a_n$ algebraisch und $L = K(a_1, \cdots, a_n)$.

(2. $\Leftrightarrow$ 1.) Per Induktion nach n. Für $n = 1$ gilt $[L : K] = [K(a_1) : K] < \infty$, weil a_1 ist algebraisch.

Angenommen $[K(a_1, \cdots, a_{n-1}) : K] < \infty$. Da a_n algebraisch über K ist, ist a_n algebraisch über $K(a_1, \cdots, a_{n-1})$. Es folgt

$$[L : K] = [K(a_1, \cdots, a_{n-1})(a_n) : K(a_1, \cdots, a_{n-1})][K(a_1, \cdots, a_{n-1}) : K] < \infty.$$

Satz 3.2.19 Seien $K \subset L$ und $L \subset M$ algebraische Erweiterungen. Dann ist $K \subset M$ algebraisch. □

Beweis. Sei $a \in M$. Da a algebraisch über L ist gibt est $P \in L[X]$ mit $P(a) = 0$. Wir schreiben $P = X^n + b_{n-1}X^{n-1} + \cdots + b_0$ mit $b_i \in L$. Sei $K' = K(b_0, \cdots, b_{n-1})$. Da $K \subset L$ algebraisch ist ist $K \subset K'$ auch algebraisch und es gilt also $[K' : K] < \infty$. Es gilt also

$$[K'(a) : K] = [K'(a) : K'][K' : K] < \infty$$

und $K'(a)$ ist algebraisch über K also ist auch a algebraisch über K. ■

Definition 3.2.20 Ein Körper K heißt **algebraisch abgeschlossen** falls jedes Polynom $P \in K[X]$ mit $\deg P \geq 1$ eine Nullstelle hat.

Satz 3.2.21 Sei K ein Körper. Die folgende Aussagen sind äquivalent:

1. Der Körper K ist algebraisch abgeschlossen.
2. Jedes Polynom $P \in K[X]$ mit $\deg P \geq 1$ ist Produkt von Polynome von Grad 1.
3. Die irreduzible Elemente in $K[X]$ sind assoziiert zu einem Element der Form $X - a$ für $a \in K$
4. Für jede algebraische Erweiterung $K \subset L$ gilt $K = L$. □

Beweis. (1. $\Rightarrow$ 2.) Sei $P \in K[X]$ mit $\deg P \geq 1$. Per Induktion nach $\deg P$. Für $\deg P = 1$ ist die Aussage klar. Für $\deg P > 1$: sei a eine Nullstelle von P. Dann gilt $P = (X - a)Q$ für ein $Q \in K[X]$ mit $\deg Q = \deg P - 1$. Per Induktion ist Q ein Produkt von Polynome von Grad 1 und die Aussage folgt.

(2. $\Rightarrow$ 3.) Sei P irreduzibel. Dann gilt $\deg P \geq 1$: Elemente von Grad 0 sind invertierbar oder Null. Dann ist P produkt von Polynome von Grad 1. Da P irreduzibel ist gibt es nur ein Faktor. Es folgt $\deg P = 1$.

(3. $\Rightarrow$ 4.) Sei $K \subset L$ eine algebraisch Erweiterung und sei $a \in L$. Dann ist $\chi_a \in K[X]$ irreduzibel und normiert. Es ist also von Grad 1 und normiert. Da a eine Nullstelle von χ_a ist gilt $\chi_a = X - a$. Aber $\chi_a \in K[X]$ also $a \in K$.

(4. $\Rightarrow$ 1.) Sei $P \in K[X]$ mit $\deg P \geq 1$. Sei Q ein normiertes irreduzible Polynom mit $Q|P$ und $\deg Q \geq 1$. Es genügt zu zeigen, dass Q eine Nullstelle hat. Da Q irreduzibel ist ist (Q) ein maximales Ideal. Also ist $L = K[X]/(Q)$ ein Körper. Es gilt $K \subset L$ und $[L : K] = \deg Q < \infty$. Also ist die Erweiterung $K \subset L$ algebraisch und es gilt $K = L$. Es folgt $\deg Q = [L : K] = 1$ und $Q = X - a$ für ein $a \in K$. Also ist $a \in K$ eine Nullstelle von Q. ∎

Satz 3.2.22 (Gauß-d'Alembertscher Fundamentalsatz der Algebra)

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen. □

Beweis. Sei $P \in \mathbb{C}[X] \setminus \mathbb{C}$. Angenommen P hätte keine Nullstelle. Dann wäre $f(z) = \frac{1}{P(z)}$ eine ganze holomorphe Funktion über z mit $\lim_{|z|\to\infty} f(z) = 0$. Nach dem Satz von Liouville muss f konstant sein. Ein Widerspruch da P nicht konstant ist. ∎

3.3 Konstruktionen mit Zirkel und Lineal

In diesem Abschnitt werden wir drei Probleme von den alten griechischen Mathematikern Pythagoras und Euklid lösen:

- die Verdopplung des Würferls,
- die Quadratur des Kreises und
- das Dreiteilen von Winkeln.

Definition 3.3.1 Sei M eine Teilmenge der euklidischen Ebene E mit mindestens 2 Elemente.

1. Wir betrachten die folgende Menge $\mathrm{GK}(M)$ von Geraden und Kreisen:

- die Geraden (P, Q) durch zwei Punkte P, Q aus M,
- die Kreise C mit Mittelpunkt $P \in M$ durch einen Punkt $Q \in M$ und

- die Kreise C mit Mittelpunkt $P \in M$ und Radius den Abstand zwischen Q und S, wobei $Q, S \in M$.

2. Die Menge aller Punkte die dank Punkte aus M in einem Schritt konstruierbar sind ist die Teilmenge $\text{Konst}_1(M)$ aus E aller Punkte die im Schnitt von zwei verschiedenen Elementen aus $\text{GK}(M)$ enthalten sind.

3. Die Menge $\text{Konst}_n(M)$ aller Punkte die dank Punkte aus M in n Schritt konstruierbar sind ist per Induktion wie folgt definiert

- $\text{Konst}_0(M) = M$,
- $\text{Konst}_{n+1}(M) = \text{Konst}_1(\text{Konst}_n(M))$.

4. Die Menge $\text{Konst}(M)$ aller Punkte die dank Punkte aus M konstruierbar sind ist

$$\text{Konst}(M) = \bigcup_{n=0}^{\infty} \text{Konst}_n(M).$$

Seien P_0 und P_1 zwei Punkte in der euklidischen Ebene E (ohne Einschränkung $P_0 = 0$ und $P_1 = 1$). Das Hauptproblem der Konstruktionen mit Zirkel und Lineal ist die folgende Frage:

welche Punkte P der Ebene sind dank P_0 und P_1 konstruierbar?

In anderen Wörter wollen wir die Menge

$$W = \text{Konst}(\{(0,0);(1,0)\})$$

bestimmen.

Definition 3.3.2 1. Eine komplexe Zahl $z \in \mathbb{C}$ heißt **konstruierbar**, falls z ein konstruierbares Punkt in der Ebene E darstellt (*i.e.* $z \in W$).

2. Eine reelle Zahl $x \in \mathbb{R}$ heißt **konstruierbar** falls $(x, 0)$ eine konstruierbare komplexe Zahl ist. Sei $W_{\mathbb{R}}$ die Menge aller Konstruierbare reelle Zahlen.

Lemma 3.3.3 1. Gegeben P, Q zwei Punkte in W. Dann ist die Mittelsenkrechte G der Punkte P und Q konstruierbar.

2. Gegeben P, Q, R drei Punkte in W. Dann kann man dank Zirkel und Lineal die Gerade G, die parallel zur Gerade (P, Q) ist und durch R geht konstruieren.

3. Sei G eine Konstruierbare Gerade und $P \in G$ ein konstruierbarer Punkt. Dann ist die Gerade G', die Senkrecht zu G ist und durch P geht konstruierbar. □

Beweis. 1. Sei C der Kreis mit Mittelpunkt P der durch Q geht und C' der Kreis mit Mittelpunkt Q der durch P geht. Seien $\{R, S\} = C \cap C'$. Dann gilt $G = (RS)$.

2. Sei C der Kreis mit Mittelpunkt P und Radius den Abstand zwischen Q und R und C der Kreis mit Mittelpunkt R und Radius den Abstand zwischen Q und P. Dann gilt $C \cap C' = \{S, S'\}$ so, dass $PQRS$ und $PRQS'$ Parallelogramme sind. Es gilt $G = (RS)$.

3. Sei C der Kreis mit Mittelpunkt P und Radius 1 und seien $\{Q, R\} = C \cap G$. Dann ist G' die Mittelsenkrechte der Punkte Q und R. ∎

Korollar 3.3.4 In der komplexen Ebene E sind die horizontale Achse H und die vertikale Achse V konstruierbar.

Lemma 3.3.5 Sei $z = x + iy \in \mathbb{C}$. Dann gilt

$$z \in W \Leftrightarrow x, y \in W_{\mathbb{R}}.$$

Beweis. ($\Rightarrow$) Sei $z = x + iy \in W$. Sei G die Gerade, die parallel zur vertikalen Achse ist und durch z geht. Dann ist $(x, 0)$ der Schnittpunkt von G mit der horizontalen Achse H und $x \in W_{\mathbb{R}}$. Sei G' die Gerade, die parallel zur horizontalen Achse ist und durch z geht. Dann ist $(0, y)$ der Schnittpunkt von G' mit der vertikalen Achse V. Sei C der Kreis mit Mittelpunkten $(0, 0)$, der durch $(0, y)$ geht. Dann gilt $H \cap C = \{(-y, 0), (y, 0)$.

($\Leftarrow$) Seien $x, y \in W_{\mathbb{R}}$. Dann gilt $(x, 0), (y, 0) \in W$. Wie oben folgt $(0, y) \in W$. Sei G die Gerade die Senkrecht zu H ist und durch $(x, 0)$ geht und sei G' die Gerade die Senkrecht zu V ist und durch $(0, y)$ geht. Dann gilt $z = G \cap G'$. ∎

Bemerkung 3.3.6 Wenn man die Menge W charakterisieren möchtet, genügt es also die Menge $W_{\mathbb{R}}$ zu charakterisieren.

Korollar 3.3.7 Es gilt

$$W_{\mathbb{R}} = \{x \in \mathbb{R} \mid \exists y \in \mathbb{R} \text{ mit } x + iy \in W\} \text{ und } W = \{x + iy \in \mathbb{C} \mid x, y \in W_{\mathbb{R}}\}.$$

Satz 3.3.8 Es gilt $\mathbb{Q} \subset W_{\mathbb{R}} \subset \mathbb{R}$ und $W_{\mathbb{R}}$ ist ein Körper. □

Beweis. Wir zeigen, dass $W_{\mathbb{R}}$ ein Körper ist. Daraus folgt die Behauptung $\mathbb{Q} \subset W$. Seien $x, y \in W_{\mathbb{R}}$. Dann sind $(x, 0), (y, 0)$,$(0, x)$ und $(0, y)$ in W.

Sei C der Kreis mit Mittelpunkt $(x, 0)$ und Radius $|y|$. Dann gilt $\{(x - y, 0), (x + y, 0)\} = C \cap H$. Daraus folgt $x - y \in W_{\mathbb{R}}$ und $(W_{\mathbb{R}}, +)$ ist eine Gruppe.

Sei G die Gerade, die parallel zur Gerade $((0, y), (x, 0))$ ist und durch $(0, 1)$ geht. Dann Dann gilt $(\frac{x}{y}, 0) = G \cap H$ und $\frac{x}{y} \in W_{\mathbb{R}}$. Es folgt, dass W_R ein Körper ist. ∎

Korollar 3.3.9 Sei $z \mapsto \bar{z}$ die komplexe konjugation.

1. Es gilt $\overline{W} = W$.

2. Es gilt $\mathbb{Q} \subset W \subset \mathbb{C}$ und W ist ein Körper.

Beweis. 1. Sei $z = x + iy \in W$. Dann gilt $x, y \in W_{\mathbb{R}}$ also $x, -y \in W_{\mathbb{R}}$ und also $x - iy \in W$.

2. Es gilt $\mathbb{Q} \subset W_{\mathbb{R}} \subset W$. Seien $z = x + iy$ und $z' = x' + iy'$ in W. Dann gilt $x, y, x', y' \in W_{\mathbb{R}}$. Insbesondere gilt

$$-x' \in W_{\mathbb{R}},\ -y' \in W_{\mathbb{R}},\ \frac{xx' + yy'}{x^2 + y^2} \in W_{\mathbb{R}} \text{ und } \frac{xy' - x'y}{x^2 + y^2} \in W_{\mathbb{R}}.$$

Daraus folgt $z - z' = (x - x') + i(y - y') \in W$ und

$$\frac{z'}{z} = \frac{xx' + yy'}{x^2 + y^2} + i\frac{xy' - x'y}{x^2 + y^2} \in W.$$

Es folgt, dass W ein Körper ist. ∎

Lemma 3.3.10 Sei $x \in W_{\mathbb{R}}$ mit $x > 0$. Dann gilt $\sqrt{x} \in W_{\mathbb{R}}$. □

Beweis. Seien $a = \frac{x-1}{2}$ und $b = \frac{x+1}{2}$. Dann gilt $a, b \in W_{\mathbb{R}}$. Es gilt auch $b^2 - a^2 = (b - a)(b + a) = 1 \cdot x = x$.

Sei G die Gerade die Senkrecht zur horizontalen Achse ist und durch $(a, 0)$ geht. Sei C der Kreis mit Mittelpunkt $(0, 0)$ und Radius b. Sei z ein Punkt im Schnitt $C \cap G$. Nach dem Satz von Pythagoras ist der Abstand zwischen z und $(a, 0)$ gleich $\sqrt{b^2 - a^2} = \sqrt{x}$. ∎

Korollar 3.3.11 Sei $z \in W$. Dann gilt $\sqrt{z} \in W$.

Beweis. Wir schreiben $z = \varrho e^{i\theta}$. Es gilt $\sqrt{z} = \pm\sqrt{\varrho}e^{i\frac{\theta}{2}}$. Es genügt also zu zeigen, dass $\sqrt{\varrho} \in W$ und $\pm e^{i\frac{\theta}{2}} \in W$.

Wir schreiben $z = x + iy$. Es gilt $x, y \in W_{\mathbb{R}}$ also $\varrho^2 = x^2 + y^2 \in W_{\mathbb{R}}$ und aus dem obigen Lemma folgt $\varrho \in W_{\mathbb{R}} \subset W$ und $\sqrt{\varrho} \in W_{\mathbb{R}} \subset W$. Daraus folgt $e^{i\theta} = \frac{z}{\varrho} \in W$.

Sei C der Kreis mit Mittelpunkt $(0, 0)$ und Radius 1 und sei G die Mittelsenkrechte der Punkte $(1, 0)$ und $e^{i\theta}$. Dann gilt $\{\pm e^{i\frac{\theta}{2}}\} = G \cap C \subset W$. ∎

Lemma 3.3.12 Sei $K \subset W_{\mathbb{R}}$ ein Teilkörper und sei

$$M = K(i) = \{a + ib \in \mathbb{C} \mid a, b \in K\}$$

die Menge aller Punkte in der Ebene mit koordinaten in K.

1. Sei $z \in \mathbb{C}$ mit $[M(z) : M] \leq 2$. Dann gilt $z \in W$.

2. Sei $z = x + iy \in \mathrm{Konst}_1(M)$. Dann gilt $M(z) : M] \leq 2$ und $[K(x, y) : K] \leq 2$. □

Beweis. 1. Sei $z \in \mathbb{C}$ mit $[M(z) : M] \leq 2$. Für $[M(z) : M] = 1$ ist die Aussage klar. Für $[M(z) : M] = 2$ gibt es ein Polynom $P \in M[X]$ mit $P(z) = 0$ und $\deg P = 2$. Nach der pq-Formel genügt es zu zeigen, dass für $z' \in M$ gilt $\sqrt{z'} \in W$. Dies folgt aus dem obigen Korollar.

2. Seien G und G' zwei Geraden aus $\mathrm{GK}(M)$ die sich in einem Punkt schneiden. Es gilt $G = (z_1 z_2)$ mit $z_1 = x_1 + iy_1 \in M$ und $z_2 = x_2 + iy_2 \in M$ und es gilt $G' = (z_1' z_2')$ mit $z_1' = x_1' + iy_1' \in M$ und $z_2' = x_2' + iy_2' \in M$. Dann sind die Punkte in G der form $(z_1 - z_2)t + z_2$ mit $t \in R$. Die Punkte in G' sind der form der form $(z_1' - z_2')t' + z_2'$ mit $t' \in R$. Sei $z = G \cap G'$. Es gilt $z = (z_1 - z_2)t + z_2 = (z_1' - z_2')t' + z_2'$. Es folgt

$$\begin{cases} t(x_1 - x_2) - t'(x_1' - x_2') = x_2' - x_2 \\ t(y_1 - x_2) - t'(y_1' - y_2') = y_2' - y_2 \end{cases}$$

Dies ist ein lineares System und hat eine Lösung (da sich G und G' in einem Punkt schneiden. Diese Lösung ist im Körper K enthalten da alle x_i, x_i', y_i und y_i' in d K enthalten sind. Es folgt $z \in M$ und $x, y \in K$.

Sei G eine Gerade aus $\mathrm{GK}(M)$ und C ein Kreis aus $\mathrm{GK}(M)$. Es gilt $G = (z_1 z_2)$ mit $z_1 = x_1 + iy_1 \in M$. Dann sind die Punkte in G der form $z = (z_1 - z_2)t + z_2$ mit $t \in \mathbb{R}$. Ein Punkt $z \in C$ erfüllt eine Gleichung der Form $|z - z_0|^2 = r^2$, wobei $z_0 = a + ib \in M$ und $a, b, r \in K$. Dies liefert eine Quadratische Gleichung für t:

$$(t(x_1 - x_2) - a)^2 + (t(y_1 - y_2) - b)^2 = r^2.$$

Es folgt, dass $[M(t) : M] \leq 2$ und $[K(t) : K] = 2$. Da $z \in M(t)$, folgt $M(z) : M] \leq 2$. Da $x, y \in K(t)$ folgt $[K(x, y) : K] \leq 2$.

Seien C und C' zwei Kreise aus $\mathrm{GK}(M)$. Ein Punkt $z = x + iy \in C$ erfüllt eine Gleichung der Form $|z - z_0|^2 = r^2$, wobei $z_0 = a + ib \in M$ und $a, b, r \in K$. Ein Punkt $z = x + iy \in C'$ erfüllt eine Gleichung der Form $|z - z_0'|^2 = R^2$, wobei $z_0 = c + id \in M$ und $c, d, R \in K$. Die Differenz der Gleichungen ist ein Gleichung in x, y von Grad 1:

$$2x(a - c) + 2y(b - d) + c^2 + d^2 - a^2 - b^2 = R^2 - r^2.$$

Dies ist die Gleichung einer Gerade $G \in \mathrm{GK}(M)$. Es gilt also $C \cap C' = G \cap C$ und die Aussage folgt aus dem obigen Fall. ∎

Satz 3.3.13 Sei $z \in \mathbb{C}$. Dann sind die folgende Aussagen äquivalent:

1. $z \in W$.
2. Es gibt eine folge von Körpererweiterungen $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$ mit $[K_{i+1} : K_i] = 2$ und $z \in K_n$. □

Beweis. (1. $\Rightarrow$ 2.) Sei $z_1 = x_1 + iy_1, \cdots, z_n x_n + iy_n = z$ eine Folge von Punkten so, dass $z_{j+1} \in \text{Konst}_1(\{0, 1, z_1, \cdots, z_j)$. Sei $K_j = \mathbb{Q}(x_1, y_1, \cdots, x_j, y_j)$ und $M_j = K_j(i)$ für $j \in [1, n]$. Dann gilt $z_1, \cdots, z_j \in M_j$ und $[M_{j+1} : M_j] \leq 2$ nach Punkt 2 des obigen Lemmas. Daraus folgt die Behauptung.

(2. $\Rightarrow$ 1.) Folgt nach Induktion aus dem Punkt 1 des obigen Lemmas.

Korollar 3.3.14 (Wantzel) Sei $z \in W$. Dann ist z algebraisch über $\mathbb{Q}$ und es gilt $[\mathbb{Q}(z) : \mathbb{Q}] = 2^k$ für ein $k \in \mathbb{N}$.

Beweis. Für eine folge von Körpererweiterungen $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$ mit $[K_{i+1} : K_i] = 2$ und $z \in K_n$ gilt (per Induktion nach n) $[K_n : \mathbb{Q}] = 2^n$. Da $z \in K_n$ gilt $\mathbb{Q}(z) \subset K_n$ und $[\mathbb{Q}(z) : \mathbb{Q}]$ ist ein Teiler von 2^n. ∎

Korollar 3.3.15 Das Delische Problem der Würfelverdopplung (Konstruktion von $\sqrt[3]{2}$) ist nicht möglich.

Beweis. Es gilt $\sqrt[3]{2} \notin W$, weil $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. ∎

Theorem 3.3.16 (Lindemann) Die Zahl π ist transzendent über $\mathbb{Q}$. □

Korollar 3.3.17 Die Quadratur des Kreises (Konstruktion von π) ist nicht möglich.

Korollar 3.3.18 Das Dreiteilen von Winkeln (Konstruktion von $e^{i\frac{\theta}{3}}$ aus $\mathbb{Q}(e^{i\theta})$) ist nicht für alle Winkel möglich.

Beweis. Sei $\theta = \frac{\pi}{3}$. Dann gilt $e^{i\theta} = \frac{1+i\sqrt{3}}{2}$. Da $i \in W$ und $\sqrt{3} \in W$ (es gilt $[\mathbb{Q}(\sqrt{3} : \mathbb{Q}] = 2$) gilt $e^{i\theta} \in W$. Falls $e^{i\frac{\theta}{3}}$ aus $\mathbb{Q}(e^{i\theta})$ konstruierbar ist gilt $e^{i\frac{\theta}{3}} \in W$ und also $\cos\frac{\pi}{9} \in W$. Es folgt $[Q(\cos\frac{\pi}{9}) : \mathbb{Q}] = 2^k$ für ein k.

Dank der Formel $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, gilt aber für $x = \cos\frac{\pi}{9}$:

$$8x^3 - 6x - 1 = 0.$$

Dieses Polynom ist primitiv über $\mathbb{Z}$. Es hat auch keine Nullstelle: sei $y \in \mathbb{Z}$ eine Nullstelle. Dann gilt $y(8y^2 - 6) = 1$ und $y \in \mathbb{Z}^\times$ also $y = \pm 1$. Aber $8(1)^3 - 6(1) - 1 = 1$ und $8(-1)^3 - 6(-1) - 1 = -3$. Ein Widerspruch. Es folgt, dass dieses Polynom irreduzibel über $\mathbb{Z}$ ist und also auch über $\mathbb{Q}$. Daraus folgt $[\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$ und $\cos\frac{\pi}{9} \notin W$. ∎

Konstruirbare regelmäßige n-Ecke.

Lemma 3.3.19 Seien $m, a \in \mathbb{N}$ mit $a, m \geq 2$ so, dass $p = a^m + 1$ eine Primzahl ist. Dann gilt $m = 2^n$ für ein $n \in \mathbb{N}$ und a ist gerade. □

Beweis. Falls m keine Potenz von 2 ist, dann hat m ein ungeraden Primteiler p und es gilt $m = qr$. Daraus folgt

$$a^m + 1 = a^{qr} - (-1)^q = (a^r)^q - (-1)^q = (a^r + 1)((a^r)^{q-1} - (a^r)^{q-2} + ... + 1).$$

Dies folgt aus der Formel $X^q - Y^q = (X - Y)(X^{q-1} + X^{q-2}Y + \cdots + Y^{q-1})$. Also ist $a^r + 1$ ein Teiler von $a^m + 1$. Da $a^m + 1$ eine Primzahl ist, muss $a^r + 1 = 1$ oder $a^r + 1 = a^m + 1$ gelten. Es folgt $a = 0$ oder $r = m$. Ein Widerspruch. Daraus folgt, dass es ein $n \in \mathbb{N}$ gibt mit $m = 2^n$.

Außerdem gilt $a^m + 1 \geq 3$ also muss $a^m + 1$ ungerade sein. Es folgt, dass a gerade sein muss. ∎

Definition 3.3.20 Die Zahlen der Form $2^{2^n} + 1$ heißen **Fermat-Zahlen**.

Beispiel 3.3.21 1. **(Fermat).** Für $n = 0$, 1, 2, 3, 4 sind die Zahlen 3, 5, 17, 257 und 65537 Fermat-Primzahlen.

2. **(Euler).** Für $n = 5$ ist die Zahl $2^{2^5} + 1 = 4\,294\,967\,297$ keine Primzahl: Es gilt

$$2^{16} = 65536 = 641 \times 102 + 154 \equiv 154 \pmod{641} \text{ also}$$

$$2^{32} = (2^{16})^2 \equiv 154^2 = 23716 = 641 \times 36 + 640 \equiv -1 \pmod{641}. \text{ Es folgt}$$

$$2^{2^5} + 1 = 2^{32} + 1 \equiv 0 \pmod{641}.$$

3. Es ist nicht bekannt, ob es weitere Fermat-Primzahlen gibt...

Satz 3.3.22 (Gauß,Wantzel) Falls das regelmäßiges n-Eck konstruierbar ist (*i.e.* $e^{\frac{2i\pi}{n}} \in W$), dann wird n nur von 2 und Fermat-Primzahlen geteilt. □

Beweis. Falls das regelmäßiges n-Eck konstruierbar ist, ist für p ein Teiler von n das regelmäßiges p-Eck auch konstruierbar. Aber für p eine Primzahl ist $\Phi_p = X^{p-1} + \cdots + 1$ irreduzibel und $\Phi_p(e^{\frac{2i\pi}{p}}) = 0$. Es folgt $\chi_{e^{\frac{2i\pi}{p}}} = \Phi_p$ und $[\mathbb{Q}(e^{\frac{2i\pi}{p}}) : \mathbb{Q}] = p - 1$. Da $e^{\frac{2i\pi}{p}} \in W$ gilt $p - 1 = 2^m$ für ein m also $2^m + 1 = p$ ist eine Primzahl. Aus dem obigen Lemma folgt $p = 2$ (für $m = 0$) oder $p = 2^{2^n} + 1$ für ein n. ∎

Bemerkung 3.3.23 Man zeigt, dass das regelmäßiges n-Eck genau dann konstruierbar ist, wenn $n = 2^m p_1 \cdots p_r$, wobei $p_1, \cdots, p_r$ verschiedene Fermat-Primzahlen sind.

4 Galois Theorie

4.1 Zerfallungskörper

Definition 4.1.1 Sei $K \subset L$ eine Erweiterung. Die **Galois-Gruppe der Erweiterung** ist

$$\mathrm{Gal}(L/K) = \{f \in \mathrm{Aut}(L) \mid f|_K = \mathrm{Id}_K\}.$$

Beispiel 4.1.2 1. Es gilt $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}_\mathbb{C}, \sigma\}$, wobei σ die komplexe Konjugation ist.

2. Sei $P_K \subset K$ der Primkörper. Dann gilt $f|_{P_K} = \mathrm{Id}_{P_K}$ für $f \in \mathrm{Aut}(K)$ Also $\mathrm{Gal}(K/P_K) = \mathrm{Aut}(K)$.

Satz 4.1.3 Sei $f : K \to K'$ ein Körperisomorphismus.

1. Dann ist $F : K[X] \to K'[X]$ definiert durch $F(a_nX^n + \cdots + a_0) = f(a_n)X^n + \cdots + f(a_0)$ ein Ringisomorphismus.

Seien $K \subset L$ und $K' \subset L'$ Körpererweiterungen und sei $a \in L$.

2. Sei $\widehat{f} : K(a) \to L'$ eine Fortsetzung von f. Dann ist $\widehat{f}(a)$ eine Nullstelle a' von dem irreduziblen Polynom $F(\chi_a)$.

3. Sei a' eine Nullstelle von $F(\chi_a)$. Dann gibt es genau eine Fortsetzung $\widehat{f} : K(a) \to L'$ von f mit $\widehat{f}(a) = a'$. Der Körperhomomorphismus $\widehat{f}$ ist ein Isomorphismus

$$\widehat{f} : K(a) \simeq K'(a').$$

Beweis. 1. Übung.

2. Wir schreiben $\chi_a = X^n + b_{n-1}X^{n-1} + \cdots + b_0$. Es gilt $0 = \widehat{f}(0) = \widehat{f}(\chi_a(a)) = \widehat{f}(a^n + b_{n-1}a^{n-1} + \cdots + b_0) = \widehat{f}(a)^n + f(b_{n-1})\widehat{f}(a)^{n-1} + \cdots + f(b_0) = F(\chi_a)(\widehat{f}(a))$. Es folgt, dass $a' = \widehat{f}(a)$ eine Nullstelle von $F(\chi_a)$ ist. Da F ein Isomorphimus ist und χ_a irreduzibel ist, folgt, dass $F(\chi_a)$ auch irreduzibel ist.

3. Wir zeigen, dass die Fortsetzung $\widehat{f}$ eindeutig ist: Es gilt $K(a) \simeq K[X]/(\chi_a)$, wobei $a \leftrightarrow [X]$. Also ist ein Element in $K(a)$ der Form $[Q]$ für $Q = b_nX^n + \cdots + b_0 \in K[X]$ *i.e.* der Form $b_na^n + \cdots + b_0$. Dann gilt $\widehat{f}([Q]) = \widehat{f}(b_n)\widehat{f}(a)^n + \cdots + \widehat{f}(b_0) = f(b_n)\widehat{f}(a)^n + \cdots + f(b_0) = f(b_n)(a')^n + \cdots + f(b_0)$ und $\widehat{f}$ ist eindeutig bestimmt.

Wir zeigen, dass es eine Forsetzung gibt. Sei $f' : K[X] \to L$ der Ringhomomorphismus definiert durch $f'(P) = f'(b_nX^n + \cdots + b_0) = f(b_n)(a')^n + \cdots + f(b_0) = F(P)(a)$. Da $F(\chi_a)(a') = 0$, gilt $f'(\chi_a) = F(\chi_a)(a') = 0$ also $(\chi_a) \subset \mathrm{Ker}f'$. Daraus folgt, dass es ein Ringhomomorphismus $\widehat{f} : K[X]/(\chi_a) \to L$ definiert durch $\widehat{f}|_K = f$ und $\widehat{f}([X]) = a'$ gibt. Da $K(a) \simeq K[X]/(\chi_a)$ folgt, dass $\widehat{f}$ existiert.

Es gilt $\mathrm{Im}\widehat{f} = K'(a')$: Von $f(K) = K'$ folgt $K' \subset \mathrm{Im}\widehat{f}$ und da $\widehat{f}(a) = a'$ folgt $K'(a') \subset \mathrm{Im}\widehat{f}$. Umgekehrt gilt für $Q \in K[X]$ die Gleichung $\widehat{f}([Q]) = f'(Q) = F(Q)(a') \in K'(a')$, weil $F(Q) \in K'[X]$. Es folgt $\mathrm{Im}\widehat{f} \subset K'(a')$. Die Abbildung $\widehat{f}$ ist also ein surjektiver Körperhomomorphismus $\widehat{f} : K(a) \to K'(a')$. Es ist also auch injektiv und ein Isomorphismus. ∎

Bemerkung 4.1.4 Die Anzahl der verschiedenen Fortsetzungen $\widehat{f} : K(a) \to L'$ von einem Körper Isomorphismus $f : K \to K'$ ist die Anzahl von Nullstellen von $F(P)$ in K' und also immer kleiner gleich $\deg(P)$.

Korollar 4.1.5 Sei $K \subset L$ eine Erweiterung und seien $a, a' \in L$ mit $\chi_a = \chi_{a'}$.

1. Dann gibt es genau ein Isomorphismus $\widehat{f} : K(a) \to K(a')$ mit $\widehat{f}|_K = \mathrm{Id}_K$ und $\widehat{f}(a) = a'$.

2. Alle Einbettungen $\widehat{f} : K(a) \to L$ mit $\widehat{f}|_K = \mathrm{Id}_K$ haben diese From.

3. Insbesondere gilt

$$|\mathrm{Gal}(K(a)/K)| = |\{\text{Nullstellen von } \chi_a \text{ in } K(a)\}|.$$

Beispiel 4.1.6 1. Das Polynom $X^2 - 2 \in \mathbb{Q}[X]$ ist das Minimalpolynom von $\pm\sqrt{2}$ also gilt $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})| = 2$. Die Elemente in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ sind $\widehat{f} = \mathrm{Id}_{\mathbb{Q}(\sqrt{2})}$ und $\widehat{f} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ definiert durch

$$\widehat{f}(a + b\sqrt{2}) = a - b\sqrt{2}.$$

2. Sei $d \in \mathbb{Z}$ so, dass d kein Quadrat ist. Dann ist das Polynom $X^2 - d \in \mathbb{Q}[X]$ das Minimalpolynom von $\pm\sqrt{d}$ also gilt $|\mathrm{Gal}(\mathbb{Q}(\sqrt{d}) : \mathbb{Q})| = 2$. Die Elemente in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d}) : \mathbb{Q})$ sind $\widehat{f} = \mathrm{Id}_{\mathbb{Q}(\sqrt{d})}$ und $\widehat{f} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ definiert durch

$$\widehat{f}(a + b\sqrt{d}) = a - b\sqrt{d}.$$

3. Das Gleiche gilt für $i = \sqrt{-1}$ über $\mathbb{R}$: Das Polynom $X^2 + 1 \in \mathbb{R}[X]$ ist das Minimalpolynom von $\pm i = \pm\sqrt{-1}$ also gilt $|\mathrm{Gal}(\mathbb{C} : \mathbb{R})| = |\mathrm{Gal}(\mathbb{R}(i) : \mathbb{R})| = 2$. Die Elemente in $\mathrm{Gal}(\mathbb{C} : \mathbb{R})$ sind $\widehat{f} = \mathrm{Id}_{\mathbb{C}}$ und $\widehat{f} : \mathbb{C} \to \mathbb{C}$ definiert durch

$$\widehat{f}(a + bi) = a - bi.$$

4. Das Polynom $P = X^3 - 2 \in \mathbb{Q}[X]$ ist das Minimalpolynom von $\sqrt[3]{2}$ aber $\mathbb{Q}(\sqrt[3]{2})$ enthält keine weitere Nullstelle von P (die weitere Nullstellen sind $\sqrt[3]{2}e^{\frac{2i\pi}{3}}$ und $\sqrt[3]{2}e^{-\frac{2i\pi}{3}}$). Es gilt also $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})| = 1$. Das einzige Element ist $\widehat{f} = \mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}$.

5. Sei p eine Primzahl. Das Polynom $\Phi_p = X^{p-1} + \cdots + X + 1 \in \mathbb{Q}[X]$ ist das Minimalpolynom von $e^{\frac{2i\pi}{p}}$ und $\mathbb{Q}(e^{\frac{2i\pi}{p}})$ enthält alle weitere Nullstellen von Φ_p: die Zahlen $e^{\frac{2ik\pi}{p}}$ für $k \in [1, p-1]$. Es gilt also $|\mathrm{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{p}})| = p - 1$. Die Elemente sind gegeben durch

$$\widehat{f}(e^{\frac{2i\pi}{p}}) = e^{\frac{2ik\pi}{p}} \text{ für } k \in [1, p-1] \ .$$

Definition 4.1.7 Sei K ein Körper und $P \in K[X] \setminus K$ mit $\deg(P) = n$ ein Polynom.

Ein Zerfallungskörper von P ist eine Erweiterung $K \subset L$ so, dass

(a) Alle Nullstellen $a_1, \cdots, a_n$ von P sind in L (*i.e.* P zerfällt in lineare Faktoren $\lambda \prod_{i=1}^{n}(X - a_i)$ in $L[X]$) und

(b) $L = K(a_1, \cdots, a_n)$ (*i.e.* ist die kleinste Erweiterung die (a) erfüllt).

Bemerkung 4.1.8 Sei L ein Zerfallungskörper von P über K. Dann gilt $L = K(a_1, \cdots, a_n)$, wobei $a_1, \cdots, a_n$ die Nullstellen von P sind. Insbesondere sind $a_1, \cdots, a_n$ algebraisch über K und aus dem Satz 3.2.18 folgt

$$[L : K] < \infty$$

also ist ein Zerfallungskörper eine endliche Erweiterung.

Lemma 4.1.9 Seien K ein Körper, $P \in K[X] \setminus K$ und L ein Zerfallungskörper von P. Sei $M = \{\text{Nullstellen von } P \text{ in } L\}$.

Dann ist die Abbildung $\iota : \mathrm{Gal}(L/K) \to \mathrm{Bij}(M)$ definiert durch $\widehat{f} \mapsto \widehat{f}|_M$ ein injektiver Gruppenhomomorphismus. □

Beweis. Nach dem obigen Korollar gilt $\widehat{f}(a) \in M$ für $a \in M$ also ist die Abbildung ι wohl definiert und ein Gruppenhomomorphismus. Sei $\widehat{f} \in \mathrm{Ker}\iota$. Es gilt $\widehat{f}|_M = \mathrm{Id}_M$. Sei $M = \{a_1, \cdots, a_n\}$. Es gilt per Definition eines Zerfallungskörper $L = K(a_1, \cdots, a_n)$. Da $\widehat{f}|_K = \mathrm{Id}_K$ und $\widehat{f}(a_i) = a_i$ für alle i folgt $\widehat{f} = \mathrm{Id}_L$ und ι ist injektiv. ■

Bemerkung 4.1.10 Sei L ein Zerfallungskörper. Es gilt also $|\mathrm{Gal}(L/K)| < \infty$.

Satz 4.1.11 Sei $f : K \to K'$ ein Körperisomorphismus und $F : K[X] \to K'[X]$ der induzierte Ringisomorphismus. Sei $P \in K[X] \setminus K$ und seien L und L' Zerfallungskörper von P und $P' = F(P)$.

Sei a eine Nullstelle von P und a' eine Nullstelle von $F(\chi_a)$. Dann existiert ein (nicht unbedingt eindeutiger) Isomorphismus $\widehat{f} : L \to L'$ mit $\widehat{f}|_K = f$, $\widehat{f}(a) = a'$ und

$$\widehat{f}(\{\text{Nullstellen von } P \text{ in } L\}) = \{\text{Nullstellen von } P' \text{ in } L'\}.$$

Beweis. Per Induktion nach $n = |\{a \in L \setminus K \mid P(a) = 0\}$.

Für $n = 0$ gilt $P(X) = \lambda \prod_i (X - a_i)$ und $P' = f(\lambda) \prod_i (X - f(a_i))$. Also $\chi_{a_i} = X - a_i$ und $F(\chi_{a_i}) = X - f(a_i)$ und auch $L = K$ und $L' = K'$. Dann ist $\widehat{f} = f$ ein Isomorphismus, der die Behauptung erfüllt.

Die Behauptung sei wahr für Polynome mit weniger als n Nullstellen in $L \setminus K$. Nach Satz 4.1.3 gibt es ein Isomorphismus $\widehat{f'} : K(a) \simeq K'(a')$ mit $\widehat{f'}|_K = f$ und $\widehat{f'}(a) = a'$. Dann hat P höchstens $n - 1$ Nullstellen in $L \setminus K(a)$. Nach Induktion gibt es ein Isomorphismus $\widehat{f} : L \to L'$ mit $\widehat{f}|_{K(a)} = \widehat{f'}$ und

$$\widehat{f}(\{\text{Nullstellen von } P \text{ in } L\}) = \{\text{Nullstellen von } P' \text{ in } L'\}.$$

Der Isomorphismus $\widehat{f}$ erfüllt die Behauptung. ∎

Korollar 4.1.12 Sei $P \in K[X]$ und L ein Zerfallungskörper von P. Dann operiert $\mathrm{Gal}(L/K)$ transitiv auf der Nullstellenmenge jedes irreduziblen Teilers von P.

Korollar 4.1.13 Sei $P \in K[X]$ irreduzibel und L ein Zerfallungskörper von P. Dann operiert $\mathrm{Gal}(L/K)$ transitiv auf der Nullstellenmenge von P.

Insbesondere sei m die Anzahl der Nullstellen von P. Dann m teilt $|\mathrm{Gal}(L/K)|$ und $|\mathrm{Gal}(L/K)|$ teilt $m!$.

Beweis. Da $\mathrm{Gal}(L/K)$ transitiv auf $\{\text{Nullstellen von } P\}$ operiert folgt von der Bahnformel, dass $m = |\text{eine Bahn}|$ teilt $|\mathrm{Gal}(L/K)|$.

Nach Lemma 4.1.9 ist $|\mathrm{Gal}(L/K)|$ eine Untergruppe von $\mathrm{Bij}(\{\text{Nullstellen von } P\})$. Nach Lagrange-Satz folgt, dass $|\mathrm{Gal}(L/K)|$ die Zahl $m!$ teilt. ∎

Satz 4.1.14 Sei $P \in K[X] \setminus K$.

1. Dann hat P einen Zerfallungskörper L.

2. Alle Zerfallungskörper von P sind isomorph: Für je zwei Zerfallungskörper L und L' von P gibt es einen Isomorphismus $\widehat{f} : L \to L'$ mit $\widehat{f}|_K = \mathrm{Id}_K$ und

$$\widehat{f}(\{\text{Nullstellen von } P \text{ in } L\}) = \{\text{Nullstellen von } P \text{ in } L'\}.$$

Der Isomorphismus $\widehat{f}$ induziert dank $\varphi \mapsto \widehat{f}\varphi\widehat{f}^{-1}$ ein Isomorphismus

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K).$$

Beweis. 1. Per Induktion nach $\deg P$. Für $\deg P = 1$ gilt $L = K$ und die Aussage ist klar. Sei Q ein irreduzibler Teiler von P und $M = K[X]/(Q)$. Dann ist M ein Körper mit $[M : K] = \deg Q$ so, dass für $a = [X]$ gilt $M = K(a)$ und $P(a) = 0$. Wir schreiben $P(X) = R(X)(X - a)$ mit $R \in K(a)[X]$. Es gilt $\deg R = \deg P - 1$ und nach Induktionsannahme gibt es ein Zerfallungskörper L von R. Über L zerfällt R in Produkt von lineare Faktoren. Daraus folgt, dass P auch in Produkt von linear Faktoren über L zerfällt. Seien $a_2, \cdots, a_m$ die Nullstellen von R. Wir setzen $a_1 = a$. Dann sind $a_1, \cdots, a_m$ die Nullstellen von P. Es gilt $L = K(a)(a_2, \cdots, a_m) = K(a_1, \cdots, a_m)$ also ist L ein Zerfallungskörper von P über K.

2. Die erste Aussage folgt aus dem Satz 4.1.11. Die Umkehrabbildung von $\varphi \mapsto \widehat{f}\varphi\widehat{f}^{-1}$ ist $\psi \mapsto \widehat{f}^{-1}\psi\widehat{f}$ ∎

Definition 4.1.15 Sei $P \in K[X]$.

1. **Der Zerfallungskörper von** P **über** K ist bis auf Isomorphie eindeutig bestimmt und wird mit $D_K(P)$ bezeichnet.

2. Die Gruppe $\mathrm{Gal}(D_K(P)/K)$ ist auch bis auf Isomorphie eindeutig bestimmt. Wir schreiben $\mathrm{Gal}(P) = \mathrm{Gal}(D_K(P)/K)$. Diese Gruppe heißt **die Galois-Gruppe von** P.

Beispiel 4.1.16 1. Sei $P = X^3 - 2 \in \mathbb{Q}[X]$. Dann gilt

$$D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2i\pi}{3}}, \sqrt[3]{2}e^{-\frac{2i\pi}{3}}) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2i\pi}{3}}).$$

2. 1. Sei $P = X^4 - 2 \in \mathbb{Q}[X]$. Dann gilt

$$D_{\mathbb{Q}}(P) = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

4.2 Normale und separable Erweiterungen

4.2.1 Normale Erweiterungen

Definition 4.2.1 Eine Erweiterung $K \subset L$ heißt **normal**, falls jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle hat, in Linearfaktoren über L zerfällt.

Beispiel 4.2.2 1. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal, weil $P(X) = X^3 - 2 \in \mathbb{Q}[X]$ eine Nullstelle in $\mathbb{Q}(\sqrt[3]{2})$ hat, aber zerfällt in lineare Faktoren nicht.

2. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}e^{\frac{2i\pi}{3}})$ ist nicht normal, weil $P(X) = X^3 - 2 \in \mathbb{Q}[X]$ eine Nullstelle in $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2i\pi}{3}})$ hat aber nicht in Linearfaktoren zerfällt.

3. Es gilt $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}e^{\frac{2i\pi}{3}}) \subset \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2i\pi}{3}})$ und die Abbildung

$$\widehat{f} : \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2i\pi}{3}}) \to \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2i\pi}{3}})$$

mit $\widehat{f}(\sqrt[3]{2}) = \sqrt[3]{2}e^{\frac{2i\pi}{3}}$ ist ein Isomorphismus und bildet $\mathbb{Q}(\sqrt[3]{2})$ auf $\mathbb{Q}(\sqrt[3]{2}e^{\frac{2i\pi}{3}})$ ab.

Satz 4.2.3 Sei $K \subset L$ eine endliche Erweiterung. Die folgende Aussagen sind äquivalent:

1. Die Erweiterung $K \subset L$ ist normal.
2. Es gilt $L = D_K(P)$ für ein $P \in K[X]$.
3. Für alle Erweiterungen $L \subset M$ und Körperhomomorphismen $\widehat{f} : L \to M$ mit $\widehat{f}|_K = \mathrm{Id}_K$ gilt $\widehat{f}(L) = L$. □

Beweis. (1. $\Rightarrow$ 2.) Es gibt algebraische Elemente $a_1, \cdots, a_n$ mit $L = K(a_1, \cdots, a_n)$. Sei $P = \prod_i \chi_{a_i}$. Wir zeigen, dass $L = D_K(P)$. Es gilt $D_K(P) = K(\{\text{Nullstellen von } P)$. Da alle a_i Nullstellen von P sind folgt $L \subset D_K(P)$.

Sei a eine Nullstelle von P. Dann gibt es ein i so, dass a eine Nullstelle von χ_{a_i} ist. Da χ_{a_i} die Nullstelle a_i in L besitzt und $K \subset L$ ist normal, zerfällt χ_{a_i} in Linearfaktoren über L. Insbesondere gilt $a \in L$ und $D_K(P) = K(\{\text{Nullstellen von } P) \subset L$.

(2. $\Rightarrow$ 3.) Sei $P \in K[X]$ so, dass $L = D_K(P)$. Es gilt $L = K(\{\text{Nullstellen von } P)$ Sei $L \subset M$ eine Erweiterung und $\widehat{f} : L \to M$ mit $\widehat{f}|_K = \mathrm{Id}_K$. Sei a eine Nullstelle von P. Es gilt $P(\widehat{f}(a)) = \widehat{f}(P(a)) = 0$ also ist $\widehat{f}(a)$ eine Nullstelle von P und es folgt $\widehat{f}(a) \subset L$. Da $L = K(\{\text{Nullstellen von } P)$ folgt $\widehat{f}(L) \subset L$. Da $\widehat{f} : L \to L$ injektiv ist und $[L : K] < \infty$ folgt $\widehat{f}(L) = L$.

(3. $\Rightarrow$ 1.) Sei $P \in K[X]$ irreduzibel so, dass P eine Nullstelle $a \in L$ hat. Seien $a_1, \cdots, a_n \in L$ so, dass $L = K(a, a_1, \cdots, a_n)$. Wir setzen $Q = P\chi_{a_1} \cdots \chi_{a_n}$ und $M = D_K(Q)$. Es gilt $L \subset M$. Seien $x_0 = a, x_1, \cdots, x_m$ die Wurzeln von P. Es gilt $x_0 = a, x_1, \cdots, x_m \in M$. Nach Satz 4.1.11 gibt es für jedes $i \in [1, m]$ ein Körperisomorphismus $\widehat{f} : M \to M$ mit $\widehat{f}|_K = \mathrm{Id}_K$ und $\widehat{f}(a) = x_i$. Daraus folgt $x_i = \widehat{f}(a) \in L$ und alle Wurzeln von P sind in L enthalten. ■

Definition 4.2.4 Sei $K \subset L$ eine Erweiterung. Eine **normale Hülle** zu L über K ist eine normale Erweiterung $K \subset M$ so, dass kein Zwischenkörper $L \subset M' \subset M$ normal über K ist.

Korollar 4.2.5 Jede Endliche Erweiterung hat eine normale Hülle.

Beweis. Es gibt algebraische Elemente $a_1, \cdots, a_n \in L$ so, dass $L = K(a_1, \cdots, a_n)$. Sei $P = \chi_{a_1} \cdots \chi_{a_n}$ und $M = D_K(P)$. Dann ist M normal über K.

Sei M' ein Zwischenkörper mit $K \subset L \subset M' \subset M$ mit M' normal über K. Für alle i hat χ_{a_i} die Nullstelle $a_i \in L \subset M'$. Da M' normal über K ist sind alle Nullstellen von χ_{a_i} für alle i in M' enthalten. Insbesondere sind alle Nullstellen von P in M' enthalten. Da M, über K, von den Nullstellen von P erzeugt ist gilt $M \subset M'$ und also $M = M'$. ■

4.2.2 Separable Erweiterungen

Definition 4.2.6 Sei K ein Körper, sei $P \in K[X]$ und sei $K \subset L$ eine Erweiterung.

1. **Die Vielfachheit einer Nullstelle** a von P ist die maximale Potenz $n \in \mathbb{N}$, für die $(X-a)^n | P$.

2. Eine Nullstelle a von P heißt **einfach** falls die Vielfachheit von a gleich 1 ist.

3. Das Polynom P heißt **separabel**, falls jeder irreduzibler Teiler Q von P in seinem Zerfallungskörper nur einfache Nullstellen hat.

Ansonsten heißt P **inseparabel**.

4. Der Körper K heißt **perfekt** (oder **vollkommen**) falls jedes $P \in K[X]$ separabel ist.

5. Ein Element $a \in L$ heißt **separabel** über K, falls $\chi_a \in K[X]$ separabel ist.

6. Die Erweiterung $K \subset L$ heißt **separabel**, wenn jedes $a \in L$ separabel über K ist.

7. Die Ableitung von $P = a_n X^n + \cdots + a_0$ ist $P' = n a_n X^{n-1} + \cdots a_1$.

Beispiel 4.2.7 Sei $K = \mathbb{F}_2(Y)$ und $P = X^2 - Y \in K[X]$. Dann ist P irreduzibel und $\sqrt{Y}$ ist eine Nullstelle von P. Es gilt

$$P(X) = X^2 - Y = X^2 - (\sqrt{Y})^2 = (X - \sqrt{Y})^2$$

also ist P inseparabel. In diesem Fall gilt auch $P' = 2X = 0$.

Satz 4.2.8 Sei $P \in K[X]$ und $L = D_K(P)$.

1. Es gilt

$$\{a \in L \mid a \text{ mehrfache Nullstelle von } P\} = \{a \in L \mid a \text{ Nullstelle von } \mathrm{ggT}(P, P')\}.$$

2. Sei P irreduzibel. Dann gilt (P ist inseparabel) $\Leftrightarrow$ ($P' = 0$). □

Beweis. 1. Sei a eine mehrfache Nullstelle. Dann gilt $P(X) = (X-a)^2 Q(X)$. Daraus folgt $P' = 2(X-a)Q + (X-a)^2 Q'$ und also ist $X - a$ ein Teiler von P und P'. Daraus folgt, dass $X - a$ ein Teiler von $\mathrm{ggT}(P, P')$ ist und a ist eine Nullstelle von $\mathrm{ggT}(P, P')$.

Umgekehrt, sei a eine einfache Nullstelle von P. Dann gilt $P(X) = (X-a)Q(X)$ mit $Q(a) \neq 0$. Daraus folgt, $P'(X) = Q(X) + (X-a)Q'(X)$ und $P'(a) = Q(a) \neq 0$. Also ist $X - a$ kein Teiler von P' und also kein Teiler von $\mathrm{ggT}(P, P')$ und a ist nicht eine Nullstelle von $\mathrm{ggT}(P, P')$.

2. Sei P irreduzibel und $Q = \mathrm{ggT}(P, P')$. Da Q ein Teiler von P ist gilt: $Q \in K[X]^\times$ oder $Q = \lambda P$ für ein $\lambda \in K$. Im ersten Fall hat $\mathrm{ggT}(P, P')$ keine Nullstelle. Im zweiten

Fall gilt $P' = 0$ (sonst gilt $\deg P' \leq \deg P - 1$ und $\deg(P) = \deg(\mathrm{ggT}(P, P')) \leq \deg P - 1$ ein Widerspruch).

Das Polynom P ist genau dann inseparabel, wenn P eine mehrfache Nullstelle a hat. Dies ist nach 1. äquivalent zu $\mathrm{ggT}(P, P')(a) = 0$ *i.e.* $P' = 0$. ∎

Korollar 4.2.9 Sei K mit $\mathrm{char}(K) = 0$. Dann ist K perfekt.

Beweis. Für $P \in K[X]$ irreduzibel gilt $P' \neq 0$. ∎

4.2.3 Galois Theorie

Definition 4.2.10 Sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}(L)$. Der **Fixkörper von G in L** ist

$$L^G = \{a \in L \mid f(a) = a \text{ für alle } f \in G\}.$$

Lemma 4.2.11 Sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}(L)$. Dann ist L^G ein Teilkörper von L. □

Beweis. Seien $a, b \in L^G$ mit $b \neq 0$. Es gilt $f(a - b) = f(a) - f(b) = a - b$ und $f\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)} = \frac{a}{b}$. ∎

Definition 4.2.12 Eine Körper Erweiterung heißt **Galois**, wenn es eine endliche Untergruppe $G \subset \mathrm{Aut}(L)$ gibt mit $K = L^G$.

Beispiel 4.2.13 1. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ist Galois: Es gilt

$$\mathbb{Q} = \mathbb{Q}(\sqrt{2})^{\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})}.$$

2. Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist nicht Galois: Es gilt

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}\}$$

also gilt für jede Untergruppe $G \subset \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ die Gleichung

$$\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2}).$$

Die Hauptsätze der Galois Theorie sind die folgende zwei Sätze.

Satz 4.2.14 (Charakterisierung von Galois Erweiterungen) Sei $K \subset L$ eine Erweiterung. Die folgende Aussagen sind äquivalent:

1. Die Erweiterung $K \subset L$ ist Galois.
2. Es gilt $[L : K] = |\mathrm{Gal}(L/K)| < \infty$.

3. Die Erweiterung $K \subset L$ ist endlich, normal und separabel.
4. Es gilt $L = D_K(P)$ für $P \in K[X]$ separabel. □

Satz 4.2.15 (Hauptsatz der Galois Theorie) Sei $K \subset L$ eine Galois Erweiterung. Sei $G = \mathrm{Gal}(L/K)$. Sei

$$\mathcal{Z}_{L/K} = \{\text{Zwischenkörper } M\colon K \subset M \subset L\}$$

die Menge aller Zwischenkörper und sei

$$\mathcal{U}_G = \{H \text{ Untergruppe von } G\}$$

die Menge aller Untergruppen von G.

Seien $\Phi : \mathcal{U}_G \to \mathcal{Z}_{L/K}$ und $\Psi : \mathcal{Z}_{L/K} \to \mathcal{U}_G$ die Abbildungen definiert durch

$$\Phi(H) = L^H \text{ und } \Psi(M) = \mathrm{Gal}(L/M).$$

1. Dann sind Φ und Ψ bijektiv und inverse zueinander.

2. Für alle $M \in \mathcal{Z}_{L/K}$ ist die Erweiterung $M \subset L$ Galois und es gilt

$$[L : M] = |\mathrm{Gal}(L/M)| = |\Psi(M)|.$$

3. Sei $M \in \mathcal{Z}_{L/K}$. Es gilt

$$(K \subset M \text{ Galois}) \Leftrightarrow (\Psi(M) = \mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K) = G).$$

In diesem Fall induziert die Einschränkungsabbildung einen surjektiven Gruppenhomomorphismus $G \to \mathrm{Gal}(M/K),\ f \mapsto f|_M$ mit Kern $\mathrm{Gal}(L/M)$. Insbesondere gilt

$$\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

Beispiel 4.2.16 Sei $K = \mathbb{Q}$ und $L = D_K(P)$ mit $P = X^3 - 2$. Wir setzen $j = e^{\frac{2i\pi}{3}}$. Seien

$$z_1 = \sqrt[3]{2},\ z_2 = j\sqrt[3]{2} \text{ und } z_3 = j^2\sqrt[3]{2}$$

die Nullstellen von P. Es gilt

$$L = \mathbb{Q}(z_1, z_2, z_3) = \mathbb{Q}(\sqrt[3]{2}, j).$$

Da P separabel ist, ist die Erweiterung $K \subset L$ Galois. Wir haben die folgende Zwischenkörper:

$$\mathbb{Q}(z_1),\ \mathbb{Q}(z_2),\ \mathbb{Q}(z_3) \text{ und } \mathbb{Q}(j).$$

Da P das Minimalpolynom von z_1, z_2, z_3 ist gilt $[\mathbb{Q}(z_i) : \mathbb{Q}] = 3$ für alle i und $3|[L : K]$. Da $\Phi_2 = X^2 + X + 1$ das Minimalpolynom von j ist gilt $[\mathbb{Q}(j) : \mathbb{Q}] = 2$

und $2|[L:K]$. Daraus folgt $6|[L:K] = \mathrm{Gal}(L/K)$. Aber nach Lemma 4.1.9 ist $\mathrm{Gal}(L/K)$ eine Untergruppe von $\mathrm{Bij}(\{z_1, z_2, z_3\}) \simeq S_3$. Daraus folgt $\mathrm{Gal}(L/K) \simeq S_3$ und $[L:K] = 6$.

Die Gruppe S_3 hat genau 6 Untergrupen H:

$$\{\mathrm{Id}\},\ \{\mathrm{Id}, [12]\},\ \{\mathrm{Id}, [13]\},\ \{\mathrm{Id}, [23]\},\ A_3 = \{\mathrm{Id}, [123], [132]\} \text{ und } S_3.$$

Die Zwischen Erweiterungen $M = \Phi(H)$ sind

$$L,\ \mathbb{Q}(z_3),\ \mathbb{Q}(z_2),\ \mathbb{Q}(z_1),\ \mathbb{Q}(j) \text{ und } K.$$

Die Zwischenkörper $\mathbb{Q}(z_3), \mathbb{Q}(z_2), \mathbb{Q}(z_1)$ sind nicht Galois über $\mathbb{Q}$ aber $\mathbb{Q}(j)$ is Galois über $\mathbb{Q}$.

Zur Vorbereitung des Beweis beweisen wir Hilfsätze.

Bemerkung 4.2.17 Seien L und L' Körper. Dann ist $\mathrm{Abb}(L, L')$ die Menge aller Abbildungen $f : L \to L'$ ein L'-Vektorraum dank

$$(f + f')(a) = f(a) + f'(a) \text{ und } (\lambda f)(a) = \lambda f(a)$$

für alle $a \in L$, $\lambda \in L'$ und $f, f' \in \mathrm{Abb}(L, L')$.

Lemma 4.2.18 Seien $f_1, \cdots, f_n : L \to L'$ paarweise verschiedene Körperhomomorphismen. Dann ist $(f_1, \cdots, f_n)$ ein linear unabhängiges System in $\mathrm{Abb}(L, L')$. □

Beweis. Angenommen $(f_1, \cdots, f_n)$ sei linear abhängig. Sei $(f_{i_1}, \cdots, f_{i_r})$ ein minimales linear abhängiges System. Modulo Umnummerirung können wir annehmen, dass $(f_1, \cdots, f_r)$ ein minimales linear abhängiges System ist. Da f_1 injektiv ist also $f_1 \neq 0$ gilt $r \geq 2$. Es gibt also Skalare $\lambda_1, \cdots, \lambda_r \in (L')^\times$ mit

$$\sum_{i=1}^{r} \lambda_i f_i = 0.$$

Sei $a \in L$ mit $f_1(a) \neq f_2(a)$. Für alle $x \in L$ gilt

$$\begin{array}{ll} \sum_{i=2}^r \lambda_i (f_i(a) - f_1(a)) f_i(x) & = \sum_{i=1}^r \lambda_i (f_i(a) - f_1(a)) f_i(x) \\ & = \sum_{i=1}^r \lambda_i f_i(a) f_i(x) - f_1(a) \sum_{i=1}^r \lambda_i f_i(x) \\ & = \sum_{i=1}^r \lambda_i f_i(ax) - f_1(a) \left(\sum_{i=1}^r \lambda_i f_i\right)(x) \\ & = \left(\sum_{i=1}^r \lambda_i f_i\right)(ax) - 0 = 0. \end{array}$$

Es folgt

$$\sum_{i=2}^{r} \lambda_i (f_i(a) - f_1(a)) f_i = 0$$

ein Widerspruch zur Minimalität. ∎

Lemma 4.2.19 Seien $f_1, \cdots, f_n : L \to L'$ paarweise verschiedene Körperhomomorphismen. Sei

$$K = \{a \in L \mid f_1(a) = \cdots = f_n(a)\}.$$

Dann ist K ein Teilkörper von L und es gilt $[L : K] \geq n$. □

Beweis. Seien $a, b \in K$ mit $b \neq 0$. Es gilt $f_i(a-b) = f_i(a) - f_i(b) = f_j(a) - f_j(b) = f_j(a-b)$ und $f_i\left(\frac{a}{b}\right) = \frac{f_i(a)}{f_i(b)} = \frac{f_j(a)}{f_j(b)} = f_j\left(\frac{a}{b}\right)$. Daraus folgt, dass K ein Teilkörper von L ist.

Sei $a_1, \cdots, a_m$ eine Basis von L über K mit $m < n$. Das System mit Variablen $x_1, \cdots, x_n$:

$$\begin{cases} \sum_{i=1}^n x_i f_i(a_1) = 0 \\ \vdots \\ \sum_{i=1}^n x_i f_i(a_k) = 0 \\ \vdots \\ \sum_{i=1}^n x_i f_i(a_m) = 0 \end{cases}$$

hat eine nicht triviale Lösung $(x_1, \cdots, x_n) \in (L')^n$ (eine Lösung ist ein Vektor im Kern der Matrix $(f_j(a_i)) \in M_{m,n}(L')$ und da $m < n$ ist der Kern nicht Null).

Für $a \in L$ gibt es Skalare λ_k mit $a = \sum_{K=1}^m \lambda_k a_k$. Da $\lambda_k \in K$ gilt $f_1(\lambda_k) = \cdots = f_n(\lambda_k)$. Wir setzen $\Lambda_k = f_1(\lambda_k) = \cdots = f_n(\lambda_k)$. Es folgt

$$\left(\sum_{i=1}^n x_i f_i\right)(a) = \sum_{i=1}^n \sum_{k=1}^m x_i f_i(\lambda_k) f_i(a_k) = \sum_{k=1}^m \Lambda_k \left(\sum_{i=1}^n x_i f_i(a_k)\right) = 0.$$

Daraus folgt $\sum_i x_i f_i = 0$. Ein Widerspruch zum obigen Lemma. ∎

Definition 4.2.20 Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Die **G-Spur** von L ist die Abbildung $\mathrm{Tr}_G : L \to L$ definiert durch

$$\mathrm{Tr}_G(a) = \sum_{f \in G} f(a).$$

Lemma 4.2.21 Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Dann ist Tr_G eine L^G lineare Abbildung und es gilt $\mathrm{ImTr}_G = \mathrm{Tr}_G(L) = L^G$. □

Beweis. Sei $a \in L$ und $\lambda \in L^G$. Es gilt

$$\mathrm{Tr}_G(\lambda a) = \sum_{f \in G} f(\lambda a) = \sum_{f \in G} f(\lambda) f(a) = \sum_{f \in G} \lambda f(a) = \lambda \sum_{f \in G} f(a) = \lambda \mathrm{Tr}_G(a).$$

Sei $\in L$ und $g \in G$. Es gilt

$$g(\mathrm{Tr}_G(a)) = g \sum_{f \in G} f(a) = \sum_{f \in G} gf(a) = \sum_{gf \in G} gf(a) = \mathrm{Tr}_G(a)$$

also $L^G \subset \mathrm{ImTr}_G = \mathrm{Tr}_G(L)$. Da die Familie $(f)_{f \in G}$ linear unabhängig ist gilt $\mathrm{Tr}_G \neq 0$. Die Abbildung $\mathrm{Tr}_G : L \to L^G$ ist L^G-linear und nicht null. Da $\dim_{L^G} L^G = 1$ folgt, dass $\mathrm{Tr}_G(L) = \mathrm{ImTr}_G = L^G$. ∎

Lemma 4.2.22 Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Sei $K = L^G$. Es gilt

$$[L : K] = |G|.$$

Beweis. Sei $G = \{f_1, \cdot, f_n\}$. Es gilt $K \subset M = \{a \in L \mid f_1(a) = \cdots = f_n(a)\}$. Nach Lemma 4.2.19 gilt $[L : M] \geq n$. Daraus folgt $[L : K] \geq [L : M] \geq n$.

Sei $(a_1, \cdots, a_m)$ mit $m > n$ ein System von Elementen in L. Wir zeigen, dass $(a_1, \cdots, a_m)$ linear abhängig über K ist. Das System mit Variablen $x_1, \cdots, x_m$:

$$\begin{cases} \sum_{i=1}^m x_i f_1^{-1}(a_i) = 0 \\ \vdots \\ \sum_{i=1}^m x_i f_k^{-1}(a_i) = 0 \\ \vdots \\ \sum_{i=1}^m x_i f_n^{-1}(a_i) = 0 \end{cases}$$

hat eine nicht triviale Lösung $(x_1, \cdots, x_m) \in L^m$ (eine Lösung ist ein Vektor im Kern der Matrix $(f_i^{-1}(a_j)) \in M_{n,m}(L)$ und da $m > n$ ist der Kern nicht Null). Sei $i_0 \in [1, m]$ mit $x_{i_0} \neq 0$ und sei $c \in L$ mit $\mathrm{Tr}_G(c) \neq 0$. Für alle $k \in [1, n]$ gilt

$$\sum_{i=1}^m f_k^{-1}(a_i)\frac{cx_i}{x_{i_0}} = 0 \text{ also } \sum_{i=1}^m a_i f_k\left(\frac{cx_i}{x_{i_0}}\right) = 0.$$

Wir summieren über k. Es folgt

$$0 = \sum_{k=1}^n \sum_{i=1}^m a_i f_k\left(\frac{cx_i}{x_{i_0}}\right) = \sum_{i=1}^m \sum_{k=1}^n a_i f_k\left(\frac{cx_i}{x_{i_0}}\right) = \sum_{i=1}^m a_i \mathrm{Tr}_G\left(\frac{cx_i}{x_{i_0}}\right).$$

Da $\mathrm{Tr}_G\left(\frac{cx_i}{x_{i_0}}\right) \in L^G = K$ und $\mathrm{Tr}_G\left(\frac{cx_{i_0}}{x_{i_0}}\right) = \mathrm{Tr}_G(c) \neq 0$ ist das System $(a_1, \cdots, a_m)$ linear abhängig über K. ∎

Lemma 4.2.23 Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Sei $K = L^G$. Es gilt

$$\mathrm{Gal}(L/K) = G.$$

Insbesondere für $K \subset L$ Galois gilt $K = L^{\mathrm{Gal}(L/K)}$. □

Beweis. Sei $f \in G$. Dann gilt $f \in \mathrm{Aut}(L)$ und $f(a) = a$ für $a \in K = L^G$. Es folgt $f \in \mathrm{Gal}(L/K)$. Also $G \subset \mathrm{Gal}(L/K)$.

Sei $a \in L^{\mathrm{Gal}(L/K)}$ und $f \in G$. Da $f \in \mathrm{Gal}(L/K)$ gilt $f(a) = a$ und $a \in L^G$. Es gilt also $K \subset K^{\mathrm{Gal}(L/K)} \subset L^G = K$ und $L^{\mathrm{Gal}(L/K)} = K = L^G$. Nach dem obigen Lemma gilt $|\mathrm{Gal}(L/K)| = [L : K] = |G|$. Daraus folgt die Aussage.

Für $K \subset L$ Galois gibt es $G \subset \mathrm{Aut}(L)$ endlich mit $K = L^G$ und es folgt $G = \mathrm{Gal}(L/K)$ also $K = L^{\mathrm{Gal}(L/K)}$. ∎

Beweis vom Satz 4.2.14. (1. $\Rightarrow$ 2.) Folgt aus Lemma 4.2.22 und Lemma 4.2.23.

(2. $\Rightarrow$ 1.) Es gilt $K \subset L^{\mathrm{Gal}(L/K)} \subset L$ und nach Lemma 4.2.22 und per Annahme gilt $[L : L^{\mathrm{Gal}(L/K)}] = |\mathrm{Gal}(L/K)| = [L : K]$. Daraus folgt $K = L^{\mathrm{Gal}(L/K)}$ und $K \subset L$ Galois.

(1. $\Rightarrow$ 3.) Sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$ mit $K = L^G$. Es gilt $[L : K] = |G| < \infty$ nach Lemma 4.2.22 also ist die Erweiterung endlich. Sei $a \in L$ und $\chi_a \in K[X]$ das Minimalpolynom von a über K. Sei $G \cdot a = \{f(a) \in L | f \in G\}$. Wir zeigen

$$\chi_a = \prod_{b \in G \cdot a} (X - b).$$

Es folgt, dass alle Nullstellen von χ_a einfach sind und in L enthalten sind. Daraus folgt, dass $K \subset L$ normal und separabel ist.

Sei $P = \prod_{b \in G \cdot a}(X - b)$. Sei $f \in G$ und $F : L[X] \to L[X]$ definiert durch $f(a_n X^n + \cdots + a_0) = f(a_n)X^n + \cdots + f(a_0)$. Es gilt

$$F(P) = F(\prod_{b \in G \cdot a} (X - b)) = \prod_{b \in G \cdot a} (X - f(b)) = \prod_{b \in G \cdot a} (X - b).$$

Daraus folgt $P \in K[X]$. Da $P(a) = 0$ gilt $\chi_a | P$. Sei $b \in G \cdot a$. Da gilt $b = f(a)$ für ein $f \in G$. Es gilt $\chi_a(b) = \chi_a(f(a)) = f((\chi_a)(a)) = 0$. Also sind alle $g \in G \cdot a$ Nullstellen von χ_a und es folgt $P | \chi_a$. Daraus folgt $P = \chi_a$.

(3. $\Rightarrow$ 4.) Nach Satz 4.2.3 gilt $L = D_K(P)$ für ein $P \in K[X]$. Da $K \subset L$ separabel ist, ist P separabel.

(4. $\Rightarrow$ 1.) Sei $P \in K[X]$ separabel und $L = D_K(P)$. Sei $G = \mathrm{Gal}(L/K)$. Nach Lemma 4.1.9 gilt $G \subset \mathrm{Bij}(\{\text{Nullstellen von } P\})$ also $|G| \leq (\deg P)!$. Wir zeigen, dass die Erweiterung $K \subset L$ Galois ist nach Induktion über $N = |\{\text{Nullstellen von } P \text{ in } L \setminus K\}|$.

Für $N = 0$ gilt $K = L = L^G$ und die Aussage ist klar.

Für $N \geq 1$, sei $a \in L \setminus K$ eine Nullstele von P. Dann gilt auch $L = D_{K(a)}(P)$ und nach Induktionsvoraussetzung ist $K(a) \subset L$ Galois. Sei also H eine endliche Untergruppe von $\mathrm{Aut}(L)$ mit $K(a) = L^H$. Es gilt $H \subset \mathrm{Gal}(L/K) = G$. Sei $\chi_a \in K[X]$ das Minimalpolynom von a über K. Es gilt $\chi_a | P$. Sei $n = \deg \chi_a$ und $a_1 = a, a_2, \cdots, a_n \in L$ die Nullstellen von χ_a. Da P separabel ist sind diese Nullstellen paarweise verschieden. Nach Satz 4.1.11 gibt es für jedes $k \in [1, n]$ ein $f_k \in G$ mit $f_k(a) = a_k$. Sei $b \in L^G \subset L^H = K(a)$. Dann ist b von der Form $b = Q(a)$ für ein $Q \in K[X]$. Dank der Restdivision mit χ_a gilt $Q = \chi_a R + S$ mit $\deg S < n$ und $b = Q(a) = \chi_a(a)R(a) + S(a) = S(a)$. Sei $T(X) = S(X) - b \in K^G[X]$. Es gilt

$$0 = f_k(S(a) - b) = f_k(T(a)) = T(f_k(a)) = T(a_k).$$

Daraus folgt, dass T mindenstens $n > \deg T$ Nullstellen hat. Es folgt $T = 0$ also $S(X) = b$ und da $S \in K[X]$ folgt $b \in K$. Daraus folgt $L^G \subset K$. Die Enthaltung $K \subset L^G$ ist klar also $K = L^G$. ∎

Lemma 4.2.24 Sei $K \subset L$ eine Galois erweiterung und M ein Zwischenkörper. Dann ist $M \subset L$ Galois. □

Beweis. Sei $G = \mathrm{Gal}(L/K)$ und $H = \mathrm{Gal}(L/M)$. Wir zeigen $M = L^H$. Es gilt $M \subset L^H$. Umgekehrt, seien $\{\mathrm{Id}_L = f_1, \cdots, f_r\} \subset G$ ein Repräsentantensystem des Quotients G/H *i.e.* mit $\{[f_1], \cdots, [f_r]\} = G/H$.

Die Einschränkungen $f_1|_M, \cdots, f_r|_M$ sind paarweise verschieden: falls $f_i|_M = f_j|_L$ gilt folgt $f_i \circ f_j^{-1} \in H$ also $[f_i] = [f_j]$ und $i = j$.

Sei $a \in M$ mit $a = f_1(a) = \cdots = f_r(a)$. Wir zeigen $a \in L^G = K$. Sei $f \in G$ und $[f] \in G/H$ die Klasse von f im Quotient. Dann gibt es ein i mit $[f] = [f_i]$. Daraus folgt, dass es ein $h \in H$ gibt mit $f = f_i h$. Da $h(a) = a$, folgt $f(a) = f_i h(a) = f_i(a) = a$. Also $a \in L^G = K$. Daraus folgt

$$K = L^G \subset \{a \in M \mid f_1(a) = \cdots = f_r(a)\} \subset K$$

und beide Menge sind gleich. Nach Lemma 4.2.19 und Lemma 4.2.22 folgt

$$\begin{aligned} |G| &= [L : K] = [L : L^H][L^H : M][M : K] \\ &= |H|[L^H : M][M : K] \geq |H|[L^H : M]r = |H|[L^H : M]|G/H| = |G|[L^H : M]. \end{aligned}$$

Daraus folgt $[L^H : M] = 1$ und $M = L^H$. ■

Lemma 4.2.25 (Konjugationsprinzip) Seien $K \subset M \subset L$ Erweiterungen und sei $f \in \mathrm{Gal}(L/K)$. Dann gilt

$$\mathrm{Gal}(L/f(M)) = f\mathrm{Gal}(L/M)f^{-1}.$$

Beweis. Sei $g \in \mathrm{Gal}(L/M)$. Dann gilt $fgf^{-1} \in \mathrm{Aut}(L)$ und für $b = f(a) \in f(M)$ gilt $fgf^{-1}(b) = fgf^{-1}f(a) = fg(a) = f(a) = b$ also $fgf^{-1} \in \mathrm{Gal}(L/f(M))$. Daraus folgt $f\mathrm{Gal}(L/M)f^{-1} \subset \mathrm{Gal}(L/f(M))$. Es folgt auch $f^{-1}\mathrm{Gal}(L/f(M))f \subset \mathrm{Gal}(L/f^{-1}f(M)) = \mathrm{Gal}(L/M)$ und also $\mathrm{Gal}(L/f(M)) \subset f\mathrm{Gal}(L/M)f^{-1}$. Daraus folgt die Aussage. ■

Lemma 4.2.26 Sei $K \subset L$ Galois und $K \subset M \subset L$ so, dass für alle $f \in \mathrm{Gal}(L/K)$ gilt $f(M) = M$. Dann ist

$$\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$$

definert durch $\mathrm{res}(f) = f|_M$ ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\mathrm{res}) = \mathrm{Gal}(L/M)$ und $K \subset M$ ist Galois. □

Beweis. Die Abbildung ist ein Gruppenhomomorphismus (Übung). Es gilt

$$\mathrm{Ker}(\mathrm{res}) = \{f \in \mathrm{Gal}(L/K) \mid f|_M = \mathrm{Id}_M\} = \mathrm{Gal}(L/M).$$

Sei $G = \mathrm{Im}(\mathrm{res})$ das Bild von res. Es gilt $M^G = M^{\mathrm{Gal}(L/K)}$. Da $K \subset L$ Galois ist, gilt $K \subset M^G = M^{\mathrm{Gal}(L/K)} \subset L^{\mathrm{Gal}(L/K)} = K$ nach Lemma 4.2.23. Daraus folgt $M^G = K$ und nach Lemma 4.2.23 folgt $G = \mathrm{Gal}(M/K)$. ■

Lemma 4.2.27 Seien $K \subset M \subset L$ Erweiterungen mit $K \subset L$ Galois. Dann sind äquivalent:

1. Die Erweiterung $K \subset M$ ist Galois.
2. Für alle $f \in \mathrm{Gal}(L/K)$ gilt $f(M) = M$.
3. $\mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$. □

Beweis. (1. $\Rightarrow$ 2.) Nach Lemma 4.2.19, Lemma 4.2.22 und Lemma 4.2.23 gilt

$$|\mathrm{Gal}(M/K)| \leq |\{f|_M : M \to L \mid f \in \mathrm{Gal}(L/K)\}| \leq [M : K] = |\mathrm{Gal}(M/K)|.$$

Also gilt die Gleichung überall und jedes $f|_M$ für $f \in \mathrm{Gal}(L/K)$ liegt bereits in $\mathrm{Gal}(M/K)$ also $f(M) = M$.

(2. $\Rightarrow$ 1.) Folgt aus Lemma 4.2.26

(2. $\Rightarrow$ 3.) Folgt aus Lemma 4.2.26: $\mathrm{Gal}(L/M)$ ist der Kern von res.

(3. $\Rightarrow$ 2.) Sei $f \in \mathrm{Gal}(L/K)$. Da $f(M) \subset L$ und $M \subset L$ Galois sind (nach Lemma 4.2.24) gilt $M = L^{\mathrm{Gal}(L/M)}$ und $f(M) = L^{\mathrm{Gal}(L/f(M))}$ (nach Lemma 4.2.23). Nach Lemma 4.2.25 gilt $\mathrm{Gal}(L/f(M)) = f\mathrm{Gal}(L/M)f^{-1} = \mathrm{Gal}(L/M)$ nach Annahme. Es folgt $f(M) = M$. ■

Beweis vom Satz 4.2.15. 1. Sei $K \subset L$ eine Galois Erweiterung. Sei M ein Zwischenkörper und H eine Untergruppe von $G = \mathrm{Gal}(L/K)$. Nach Lemma 4.2.23 gilt

$$\Psi(\Phi(H)) = \Psi(L^H) = \mathrm{Gal}(L/L^H) = H.$$

Es gilt

$$\Phi(\Psi(M)) = \Phi(\mathrm{Gal}(L/M)) = L^{\mathrm{Gal}(L/M)}.$$

Nach Lemma 4.2.24 ist $M \subset L$ Galois und nach Lemma 4.2.23 folgt $M = L^{\mathrm{Gal}(L/M)}$.

2.Die erste AUssage folgt aus Lemma 4.2.24 und die Gleichung aus Lemma 4.2.22.

3. Die erste Aussage folgt aus Lemma 4.2.27 und die letzte Aussage aus Lemma 4.2.26. ■

Beweis. Sei $G = \mathrm{Gal}(M/K)$, $N = \mathrm{Gal}(M/L)$ und $H = \mathrm{Gal}(L/K)$. Dann gilt $K = L^H$ und $L = M^N$. Wir zeigen $K = M^G$. Die Enthaltung $K \subset M^G$ ist klar. Sei $x \in M^G$. Da $N \subset G$ folgt $x \in M^G \subset M^N$ also $x \in L$. Sei jetzt $f \in \mathrm{Gal}(L/K)$. Da $L \subset M$ normal ist, gibt es nach Satz 4.1.11 ein $g \in \mathrm{Gal}(M/K)$ mit $g|_L = f$. Es folgt $f(x) = g(x) = x$ und also $x \in L^H = K$. ■

4.2.4 Algebraischer Abschluß

Definition 4.2.28 Sei K ein Körper. Ein **algebraischer Abschluß** von K ist eine Erweiterung $K \subset \overline{K}$ mit

- $K \subset \overline{K}$ ist algebraisch
- $\overline{K}$ ist algebraisch abgeschlossen.

Beispiel 4.2.29 1. Ein algebraischer Abschluß von $\mathbb{C}$ ist $\mathbb{C}$.

2. Ein algebraischer Abschluß von $\mathbb{R}$ ist $\mathbb{C}$.

3. Ein algebraischer Abschluß von $\mathbb{Q}$ ist

$$\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q} \}.$$

4. Der Körper $\mathbb{C}$ ist kein algebraischer Abschluß von $\mathbb{Q}$, weil die Erweiterung $\mathbb{Q} \subset \mathbb{C}$ nicht algebraisch ist.

Theorem 4.2.30 (Steinitz) Jeder Körper hat einen algebraischen Abschluß. □

4.3 Endliche Körper

4.3.1 Existenz

Lemma 4.3.1 Sei R ein kommutativer Ring mit $\text{char}(R) = p > 0$. Für $n \in \mathbb{N}_{>0}$, sei $q = p^n$.

1. Dann ist die Abbildung $\text{Fr}_R : R \to R$ definiert durch $\text{Fr}_R(x) = x^p$ ein Ringhomomorphismus.

2. Dann ist die Abbildung $\text{Fr}_{R,q} : R \to R$ definiert durch $\text{Fr}_R(x) = x^q$ ein Ringhomomorphismus. □

Beweis. 1. Es gilt $\text{Fr}_R(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$. Aber $p | \binom{p}{k}$ für alle $k \in [1, p-1]$. Daraus folgt $\text{Fr}_R(x+y) = x^p + y^p = \text{Fr}_R(x) + \text{Fr}_R(y)$. Es filgt $\text{Fr}_R(xy) = (xy)^p = x^p y^p = \text{Fr}_R(x)\text{Fr}_R(y)$.

2. Es gilt $\text{Fr}_{q,R}(x) = x^q = x^{p^n} = (x^p)^n = \text{Fr}_R^n(x)$. Die Aussage folgt aus 1. ■

Definition 4.3.2 Sei R ein kommutativer Ring mit $\text{char}(R) = p > 0$. Die Abbildung $\text{Fr}_R : R \to R$ definiert durch $\text{Fr}_R(x) = x^p$ heißt **Frobenius-Homomorphismus**.

Lemma 4.3.3 Sei K ein endlicher Körper mit $\mathrm{char}(K) = p$.

1. Dann ist Fr_K ein Automorphismus.

2. Falls $K = \mathbb{F}_p$ gilt $\mathrm{Fr}_K = \mathrm{Id}_K$. □

Beweis. 1. Die Abbildung Fr_K ist ein Körperhomomorphismus also ist injektiv. Da K endlich ist ist Fr_K bijektiv.

2. Sei $x \in \mathbb{F}_p$. Falls $x = 0$ gilt $\mathrm{Fr}_K(x) = \mathrm{Fr}_K(0) = 0 = x$. Sei also $x \in \mathbb{F}_p^\times$. Es gilt $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ also ist die Gruppe $(\mathbb{F}_p^\times, \cdot)$ der Ordnung $p-1$. Es folgt, dass $x^{p-1} = 1$ und also $\mathrm{Fr}_K(x) = x^p = x$. ∎

Lemma 4.3.4 Seien $K \subset L$ zwei endlicher Körper und seien $q = |K|$ und $q' = [L]$.

1. Dann gilt $[L : K] = n < \infty$ und $q' = q^n$.

2. Insbesondere für $p = \mathrm{char}(K)$ gilt $q = |K| = p^m$ für ein $m \in \mathbb{N}_{>0}$. □

Beweis. 1. Da L endlich ist ist L ein endlicher Vektorraum über K. Sei $n = [L : K]$. Es gilt $L \simeq K^n$. Daraus folgt die Aussage.

2. Es gilt $\mathbb{F}_p = P_K \subset K$. Sei $m = [K : \mathbb{F}_p]$. Die Aussage folgt aus 1. ∎

Satz 4.3.5 Sei p eine Primzahl und $n \in \mathbb{N}_{>0}$. Sei $q = p^n$.

Dann gibt es modulo isomorphismus genau ein Körper K mit q Elemente: der Zerfallungskörper von $X^q - X$ über $\mathbb{F}_p$. □

Beweis. Wir zeigen, dass es ein Körper mit q Elemente gibt. Sei $K = D_{\mathbb{F}_p}(X^q - X)$ der Zerfallungskörper von $X^q - X$ über F_p. Es gilt $\mathbb{F}_p \subset K$ also $\mathrm{char}(K) = p$. Sei

$$M = \{x \in K \mid x^q - x = 0\}.$$

Wir zeigen, dass M ein Körper ist: Seien $x, y \in M$. Dann gilt $(x-y)^q = \mathrm{Fr}_{K,q}(x-y) = \mathrm{Fr}_{K,q}(x) - \mathrm{Fr}_{K,q}(y) = x^q - y^q = x - y$ also $x - y \in M$. Es gilt auch $(xy^{-1})^q = x^q (y^q)^{-1} = xy^{-1}$ also $xy^{-1} \in M$.

Außerdem gilt für $P(X) = X^q - X$: $\frac{dP}{dX}(X) = qX^{q-1} - 1 = -1$ da $\mathrm{char}(K) = p | q$. Es folgt $\mathrm{ggT}(P, \frac{dP}{dX}) = 1$ und die Nullstellen von P sind von Vielfachheit 1. Es sind also genau q solche Nullstellen. Daraus folgt $|M| = q$.

Wir zeigen jetzt die Eindeutigkeit. Sei M ein Körper mit q Elemente. Sei $x \in M^\times$. Da $|M^\times| = q - 1$ gilt $x^{q-1} = 1$ und also $x^q - x = 0$. Für $x = 0 \in M$ gilt auch $x^q - x = 0$. Es gilt also $x^q - x = 0$ für alle $x \in M$ und $M = D_{\mathbb{F}_p}(X^q - X)$. ∎

Definition 4.3.6 Für p eine Primzahl, $n \in \mathbb{N}$ und $q = p^n$ schreiben wir $\mathbb{F}_q$ für den Körper mit q Elemente.

4.3.2 Primitives Element

Satz 4.3.7 Sei p eine Primzahl und $q = p^n$. Es gibt einen Gruppenisomorphismus

$$(\mathbb{F}_q^\times, \times) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +).$$

Insbesondere ist $\mathbb{F}_q^\times$ eine Zyklische Gruppe. □

Beweis. Die Gruppe $\mathbb{F}_q^\times$ ist kommutativ. Sei $m = \max\{\mathrm{ord}(g) \mid g \in \mathbb{F}_q^\times\}$ und sei

$$H = \{x \in \mathbb{F}_q^\times \mid \mathrm{ord}(x) | m\}.$$

Dann ist H eine Untergruppe von $\mathbb{F}_q^\times$: für $x, y \in H$ gilt $(xy^{-1})^m = x^m (y^m)^{-1} = 1$ also $\mathrm{ord}(xy^{-1}) | m$. Sei $h \in H$ mit $\mathrm{ord}(h) = m$. Dann gilt $\langle h \rangle \subset H$ und $|\langle h \rangle| = \mathrm{ord}(h) = m$. Umgekehrt gilt $x^m = 1$ für alle $x \in H$ also gilt $H \subset \{\text{Nullstellen von } X^m - 1\}$ und $|H| \leq m$. Daraus folgt $H = \langle h \rangle$.

Wir Zeigen, dass $H = G$. Angenommen $H \subsetneq G$. Sei $g \in G \setminus H$. Dann gilt $r = \mathrm{ord}(g) \not| m$. Sei $d = \mathrm{ggT}(r, m)$ und $s = \frac{r}{d}$. Dann gilt $\mathrm{ggT}(s, m) = 1$ und $\mathrm{ord}(g^d) = s$. Wir zeigen, dass $\mathrm{ord}(g^d h) > m$. Ein Widerspruch zur Maximalität von m.

Sei $a \in \mathbb{N}$ mit $(g^d h)^a = 1$. Dann gilt $(g^d)^a = (h^{-1})^a$ also $\mathrm{ord}((g^d)^a) | \mathrm{ord}(g^d) = s$ und $\mathrm{ord}((g^d)^a) = \mathrm{ord}((h^{-1})^a) | \mathrm{ord}(h) = m$. Daraus folgt, dass beide Ordnungen gleich 1 sind und $(g^d)^a = 1 = h^a$. Insbesondere gilt $s = \mathrm{ord}(g^d) | a$ und $m = \mathrm{ord}(h) | a$. Daraus folgt $sm | a$ und $\mathrm{ord}(g^d h) = sm > m$. ∎

Bemerkung 4.3.8 Der obige Beweis gilt auch für K ein beliebiger Körper und $G \subset K^\times$ eine endliche Untergruppe: jede endliche Untergruppe G von $K^\times$ ist zyklisch.

Korollar 4.3.9 (Satz vom primitiven Element) Sei $K \subset L$ eine Erweiterung mit K und L endlich. Sei $\xi \in L^\times$ ein Erzeuger dieser Gruppe.

1. Dann gilt $L = K(\xi)$.

2. Sei χ_ξ das Minimalpolynom von ξ über K. Es gilt $\deg \chi_\xi = [L : K]$.

Beweis. 1. Da $\xi \in L$ gilt $K(\xi) \subset L$. Umgekehrt, da ξ ein Erzeuger von $L^\times$ ist gilt $L^\times \subset K(\xi)$. Daraus folgt $L \subset K(\xi)$.

2. Folgt direkt aus 1. ∎

4.3.3 Galois Gruppe

Satz 4.3.10 Sei p eine Primzahl, $n \in \mathbb{N}$ und $q = p^n$. Sei $m \in \mathbb{N}$.

1. Die Erweiterung $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ ist Galois.

2. Die Gruppe $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is zyklisch und hat $\mathrm{Fr}_{\mathbb{F}_{q^m},q}$ als Erzeuger:

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \mathrm{Fr}_{\mathbb{F}_{q^m},q} \rangle \simeq \mathbb{Z}/m\mathbb{Z}.$$

Beweis. 1. Nach Satz 4.3.5 gilt $\mathbb{F}_{q^m} = \mathbb{F}_{p^{mn}} = D_{\mathbb{F}_p}(X^{p^{mn}} - X)$ also ist $\mathbb{F}_p \subset \mathbb{F}_{q^m}$ normal. Da für $P = X^{p^{mn}} - X$ gilt $P' = -1 \neq 0$, gilt P ist separabel und $\mathbb{F}_p \subset \mathbb{F}_{q^m}$ ist separabel also Galois. Insbesondere gilt $|\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)| = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$.

2. Sei $x \in \mathbb{F}_q^\times$. Da $|\mathbb{F}_q^\times| = q - 1$, folgt $x^{q-1} = 1$. Für alle $x \in \mathbb{F}_q$ gilt also $x^q = x$. Daraus folgt $\mathrm{Fr}_{\mathbb{F}_{q^m},q}(x) = x$. Da $\mathrm{Fr}_{\mathbb{F}_{q^m},q} \in \mathrm{Aut}(\mathbb{F}_{q^m})$ folgt $\mathrm{Fr}_{\mathbb{F}_{q^m},q} \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Sei $d = \mathrm{ord}(\mathrm{Fr}_{\mathbb{F}_{q^m},q})$ die Ordnung von $\mathrm{Fr}_{\mathbb{F}_{q^m},q}$. Es gilt $d \leq m$. Für alle $x \in \mathbb{F}_{q^m}$ gilt auch:

$$x = \mathrm{Fr}^d_{\mathbb{F}_{q^m},q}(x) = x^{q^d}.$$

Also hat das Polynom $X^{q^d} - X$ mindestens $|\mathbb{F}_{q^m}| = q^m$ Nullstellen. Daraus folgt $d \geq m$ und also $d = m$. Da $|\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)| = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$, folgt die Aussage. ∎

4.4 Satz vom primitiven Element

Satz 4.4.1 Sei $K \subset L$ eine endliche und separable Erweiterung.

1. Es gibt eine Erweiterung $L \subset M$ so, dass die Erweiterung $K \subset M$ Galois ist.

2. Die Erweiterung $K \subset L$ hat nur endlich viele Zwischenkörper. □

Beweis. 1. Seien $a_1, \cdots, a_n$ßnL mit $L = K(a_1, \cdots, a_n)$. Sei $P = \chi_{a_1} \cdots \chi_{a_n}$, wobei χ_{a_i} das Minimalpolynom von a_i über K ist. Dann ist P separabel über K, weil alle a_i separabel über K sind. Sei $M = D_K(P)$. Die Erweiterung $K \subset M$ ist Galois.

2. Die Zwischenkörper $K \subset L' \subset M$ sind in Bijektion mit den Untergruppen von $\mathrm{Gal}(M/K)$. Da es nur endlich viele soche Untergruppen gibt, gibt es endlich viele Zwischenkörper $K \subset L' \subset M$. Insbesondere gibt es endlich viele Zwischenkörper $K \subset L' \subset L$. ∎

Satz 4.4.2 (Satz vom primitiven Element) Sei $K \subset L$ eine endliche und separable Erweiterung. Dann gibt es ein $\xi \in L$ mit $L = K(\xi)$. □

Beweis. Für L endlich folgt die Aussage aus Korollar 4.3.9. Sei also K unendlich. Sei n minimal mit $L = K(a_1, \cdots, a_n)$. Angenommen $n \geq 2$. Für jedes $t \in K$ ist $K(a_1 + ta_2)$ ein Zwischenkörper. Da es nur endlich viele Zwischekörper $K \subset M \subset L$ gibt und da K unendlich ist, gibt es $t, s \in K$ mit $t \neq s$ und $K(a_1+ta_2) = K(a_1+sa_2)$. Daraus folgt, dass

$$a_1 = \frac{s(a_1+ta_2)-t(a_1+sa_2)}{s-t} \in K(a_1 + ta_2) = K(a_1 + sa_2)$$
$$a_2 = \frac{(a_1+ta_2)-(a_1+sa_2)}{t-s} \in K(a_1 + ta_2) = K(a_1 + sa_2).$$

Daraus folgt $K(a_1+ta_2) = K(a_1, a_2)$ und $L = K(a_1, \cdots, a_n) = K(a_1+ta_2, a_3, \cdots, a_n)$. Widerspruch zur Minimalität von n. ∎

4.5 Einheitswurzeln und Kreisteilungskörper

Definition 4.5.1 Sei K ein Körper und $n \in \mathbb{N}$.

1. **Die Gruppe der n-ten Einheitswurzeln** $E_n(K)$ von K ist die Gruppe der Nullstellen von $X^n - 1$ in $K_n = D_K(X^n - 1)$.

2. Der Körper $K_n = D_K(X^n - 1)$ heißt **Kreisteilungskörper**.

Beispiel 4.5.2 1. Für $K = \mathbb{C}$ gilt $E_n(\mathbb{C}) = \{e^{\frac{2ik\pi}{n}} \mid k \in [0, n-1]\}$.

2. Für $q = p^n$ gilt $E_{q-1}(\mathbb{F}_p) = \mathbb{F}_q^\times$.

Lemma 4.5.3 Sei $n \in \mathbb{N}$ und p eine Primzahl.

1. Falls $\mathrm{char}(K) \not| n$, gilt $|E_n(K)| = n$. In dem Fall gibt es ein Gruppenisomorphismus

$$E_n(K) \simeq \mathbb{Z}/n\mathbb{Z}.$$

2. Falls $\mathrm{char}(K) = p$ und $n = pm$ gilt $E_n(K) = E_m(K)$ und $K_n = K_m$. □

Beweis. 1. Sei $P = X^n - 1$. Es gilt $E_n(K) = \{x \in D_K(P) \mid P(x) = 0\}$. Insbesondere gilt $|E_n(K)| \leq n$. Falls $\mathrm{char}(K) = p \not| n$, gilt $P' \neq 0$ und P ist separabel. Das Polynom P hat also n paarweise verschiedene Nullstellen und $|E_n(K)| = n$.

Nach der Bemerkung 4.3.8 ist die endliche Gruppe $E_n(K)$ zyzlisch.

2. Es gilt $X^n - 1 = (X^m)^p - 1 = (X^m - 1)^p$. Daraus folgt $E_n(K) = E_m(K)$ und $K_n = K_m$. ∎

Lemma 4.5.4 Sei $n \in \mathbb{N}$ und d ein Teiler von n.

1. Es gilt $K_d \subset K_n$.

2. Die Erweiterung $K \subset K_n$ ist Galois. □

Beweis. 1. Sei m mit $n = dm$. Es gilt

$$X^n - 1 = ((X^d)^m - 1) = (X^d - 1)(X^{d(m-1)} + X^{d(m-2)} + \cdots + X^d + 1).$$

Daraus folgt $E_d(K) \subset E_n(K)$ und $K_d \subset K_n$.

2. Nach dem obigen Lemma können wir ohne Einschränkung annehmen, dass gilt $\mathrm{ggT}(n, \mathrm{char}(K)) = 1$. Dann ist $P = X^n - 1$ separabel und $K_n = D_K(P)$ ist Galois. ∎

Sei $n \in \mathbb{N}$ und K ein Körper mit $\mathrm{ggT}(n, \mathrm{char}(K)) = 1$.

Definition 4.5.5 Die Menge der **primitiven Einheitswurzeln** ist

$$PE_n(K) = \{\zeta \in E_n(K) \mid \mathrm{ord}(\zeta) = n\}.$$

Bemerkung 4.5.6 Sei $n \in \mathbb{N}$ und K ein Körper.

1. Es gilt $E_n(K) \simeq \mathbb{Z}/n\mathbb{Z}$. Mit dieser Identifikation gilt $PE_n(K) = (\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere gilt

$$|PE_n(K)| = \varphi(n),$$

wobei $\varphi(n)$ die Eulersche φ-Funktion ist.

2. Es gilt

$$E_n(K) = \coprod_{d|n} PE_n(K).$$

Definition 4.5.7 Das n-te Kreisteilungspolynom über K ist

$$\Phi_{n,K} = \prod_{\zeta \in PE_n(K)} (X - \zeta) \in K_n(X).$$

Lemma 4.5.8 Sei $n \in \mathbb{N}$.

1. Es gilt $\deg \Phi_{n,K} = \varphi(n)$ und

$$X^n - 1 = \prod_{d|n} \Phi_{d,K}.$$

2. Es gilt

$$n = \sum_{d|n} \varphi(d).$$

Beweis. 1. Die Aussagen folgen aus der obigen Bemerkung.

2. Folgt aus 1: $n = \deg(X^n - 1) = \deg(\prod_{d|n} \Phi_{d,K}) = \sum_{d|n} \varphi(d)$. ∎

Beispiel 4.5.9 Für p eine Primzahl mit $\mathrm{ggT}(p, \mathrm{char}(K)) = 1$ gilt

$$\Phi_{p,K}(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1.$$

Satz 4.5.10 Sei $\zeta \in PE_n(K)$. Es gilt $K_n = K(\zeta)$. □

Beweis. Da $\mathrm{ggT}(n, \mathrm{char}(K)) = 1$ gilt $|E_n(K)| = n$ und $|\{\zeta^k \mid k \in \mathbb{Z}\}| = \mathrm{ord}(\zeta) = n$. Daraus folgt $E_n(K) = \{\zeta^k \mid k \in \mathbb{Z}\}$ und $K_n = K(\zeta)$. ■

Lemma 4.5.11 Sei R ein Ring und K ein Körper mit $R \subset K$. Seien $P, Q \in R[X]$ mit Leitkoeffizient 1 und mit $P = QT$, wobei $T \in K[X]$.

Dann gilt $T \in R[X]$ und T hat Leitkoeffizient 1. □

Beweis. Wir schreiben dank der Restdivision $P = QS + U$ mit $S, U \in R[X]$ und $\deg U < \deg Q$. In $K[X]$ gilt $QT = P = QS + R$ also $R = Q(T - S)$. Mit $\deg U < \deg Q$ folgt $T = S \in R[X]$. Es gilt auch Leitkoeffizient von $P =$ Leitkoeffizient von $Q \cdot$ Leitkoeffizient von T. ■

Lemma 4.5.12 Sei R der Primring von K also

$$R = \begin{cases} \mathbb{Z} & \text{für } \mathrm{char}\, K = 0, \\ \mathbb{F}_p & \text{für } \mathrm{char}\, K = p. \end{cases}$$

Dann gilt $\Phi_{n,K} \in R[X]$. □

Beweis. Per Induktion über n. Für $n = 1$ ist die Aussage klar: $\Phi_1(X) = X - 1$. Die Behauptung sei wahr für alle $\Phi_{m,K}$ mit $m < n$. Dann ist $X^n - 1 = \Phi_{n,K} Q$ mit $Q = \prod_{d|n, d<n} \Phi_{d,K} \in R[X]$. Aus dem obigen Lemma folgt $\Phi_{n,K} \in R[X]$ und $\Phi_{n,K}$ hat Leitkoeffizient 1. ■

Lemma 4.5.13 Es gilt $\mathrm{Gal}(K_n/K) \subset (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$, insbesondere ist diese Gruppe abelsch. □

Beweis. Sei $\zeta \in PE_n(K)$. Jedes $f \in \mathrm{Gal}(K_n/K)$ permutiert die Nullstellen von $\Phi_{n,K}$. Daraus folgt, dass es ein $m_f \in (\mathbb{Z}/n\mathbb{Z})^\times$ gibt mit $f(\zeta) = \zeta^{m_f}$. Wir betrachten die Abbildung $F : \mathrm{Gal}(K_n/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ definiert durch $F(f) = m_f$. Dies ist ein Gruppenhomomorphismus: Für $f, g \in \mathrm{Gal}(K_n/K)$ gilt $f(\zeta) = \zeta^{m_f}$ und $g(\zeta) = \zeta^{m_g}$ also $(f \circ g)(\zeta) = f(\zeta^{m_g}) = f(\zeta)^{m_g} = (\zeta^{m_f})^{m_g} = \zeta_{m_f m_g}$. Daraus folgt $F(fg) = F(f)F(g)$. Es genügt zu zeigen, dass F injektiv ist. Sei $f \in \mathrm{Ker}(F)$ also $F(f) = 1$. Dann gilt $f(\zeta) = \zeta$. Da $K_n = K(\zeta)$ folgt $f = \mathrm{Id}_{K_n}$. ■

Satz 4.5.14 Sei $K = \mathbb{Q}$. Dann ist $\Phi_n = \Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$ irreduzibel und somit für $\zeta \in PE_n(\mathbb{Q})$ gilt:

$$K_n = \mathbb{Q}(\zeta) \simeq \mathbb{Q}[X]/(\Phi_n).$$

Außerdem gilt

$$[K_n : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) \text{ und } \mathrm{Gal}(K_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}.$$

Beweis. Sei $\zeta \in PE_n(\mathbb{Q})$ und P das Minimalpolynom von ζ über $\mathbb{Q}$. Dann gilt $P|X^n - 1$. Es genügt zu zeigen, dass $\deg P = \varphi(n)$ gilt.

Schritt 1: Sei p eine Primzahl mit $p \not| n$. Wir zeigen $P(\zeta^p) = 0$.

Sei Q das Minimalpolynom von ζ^p über $\mathbb{Q}$. Wir zeigen, dass $P, Q \in \mathbb{Z}[X]$: Da $p \not| n$, gilt $\zeta^p \in PE_n(K)$ also $\Phi_n(\zeta^p) = 0$. Da $\mathbb{Z}[X]$ faktoriel ist und $\Phi_n \in \mathbb{Z}[X]$ können wir Φ_n in irreduzible Polynome in $\mathbb{Z}[X]$ zerlegen. Es gibt also $f_1, \cdots, f_r \in \mathbb{Z}[X]$ irreduzibel mit $\Phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$. Da das Leitkoeffizient von Φ_n gleich 1 ist, sind die Leitkoeffizienten von alle f_i auch 1. Da ζ und ζ^p Nullstellen von Φ_n sind gibt es ein zewi Elemente $i, j \in [!, r]$ mit $f_i(\zeta) = 0$ und $f_j(\zeta^p) = 0$. Da beide irreduzible Polynome mit Koeffizienten in $\mathbb{Z} \subset \mathbb{Q}$ und mit Leitkoeffizient 1 sind folgt $P = f_i \in \mathbb{Z}[X]$ und $Q = f_j \in \mathbb{Z}[X]$.

Angenommen $Q \neq P$ gilt $X^n - 1 = PQT$ für ein $T \in \mathbb{Z}[X]$ nach Lemma 4.5.11. Sei $U(X) = Q(X^p)$. Es gilt $U(\zeta) = Q(\zeta^p)$ also $P|U$ und es gibt ein $S \in \mathbb{Z}[X]$ mit $U = PS$ also $Q(X^p) = P(X)S(X)$. Sei $\mathrm{mod}_p : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ die Reduktion modulo p. Wir schreiben $Q(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_0$. Da $a^p = a$ für alle $a \in \mathbb{F}_p$ gilt

$$\begin{aligned}
\mathrm{red}_p(Q(X^p)) &= (X^p)^k + a_{k-1}(X^p)^{k-1} + \cdots + a_0 \\
&= (X^p)^k + a_{k-1}^p(X^p)^{k-1} + \cdots + a_0^p \\
&= (X^k)^p + a_{k-1}^p(X^{k-1})^p + \cdots + a_0^p \\
&= (X^k + a_{k-1}X^{k-1} + \cdots + a_0)^p. \\
&= (\mathrm{res}_p(Q(X)))^p.
\end{aligned}$$

Es gilt also $\mathrm{res}_p(Q)^p = \mathrm{res}_p(P)\mathrm{res}_p(S)$ und $\mathrm{ggT}(\mathrm{res}_p(Q), \mathrm{res}_p(P)) \neq 1$ also hat $\mathrm{res}_p(X^n - 1) = \mathrm{res}_p(Q)\mathrm{res}_p(P)\mathrm{res}_p(T)$ mehrfache Nullstellen. Ein Widerspruch zum Lemma 4.5.3.

Es gilt also $P = Q$ und $P(\zeta^p) = 0$.

Schritt 2. Sei $\zeta' \in PE_n(K)$. Dann gilt $\zeta' = \zeta^m$ für $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ mit $p_i \not| n$ für alle i. Nach Schritt 1 ist ζ^{p_1} eine Nullstelle von P und auch $\zeta^{p_1^2}$, und per Induktion $P(\zeta^m) = 0$. Wir haben also, dass $PE_n(K)$ eine Teilmenge der Nullstellen von P ist. Da $\deg P \leq \varphi(n)$ und $|PE_n(K)| = \varphi(n)$ folgt $\deg P = \varphi(n)$. ∎

Sei W die Menge aller konstruirbare komplexe Zahlen (siehe Definition 3.3.1). Dies ist ein Körper.

Satz 4.5.15 Sei $z \in \mathbb{C}$ und sei $\chi_z \in \mathbb{Q}[X]$ das Minimalpolynom von z über $\mathbb{Q}$. Sei $K = D_{\mathbb{Q}}(\chi_z)$. Dann gilt

$$([K : \mathbb{Q}] = 2^m \text{ für ein } m \in \mathbb{N}) \Rightarrow (z \in W).$$

Beweis. Da $\operatorname{char} K = 0$ gilt, ist χ_z separabel und $\mathbb{Q} \subset K$ ist Galois. Sei $G = \operatorname{Gal}(K/\mathbb{Q})$ die Galoisgruppe. Es gilt $|G| = [K : \mathbb{Q}] = 2^m$ also ist G eine 2-Gruppe. Nach Korollar 1.11.11 und Satz 1.11.12 gibt es eine Folge von Untergruppen

$$\{e_G\} = G_m \triangleleft \cdots \triangleleft G_0 = G$$

mit $G_i/G_{i+1} \simeq \mathbb{Z}/2\mathbb{Z}$. Nach dem Hauptsatz der Galoistheorie gibt es also eine Folge von Körpererweiterungen

$$K \supset \cdots \supset K_0 = \mathbb{Q}$$

mit $[K_{i+1} : K_i] = 2$. Nach Satz 3.3.13 gilt $z \in W$. ∎

Satz 4.5.16 (Gauß-Wantzel) Sei $n \in \mathbb{N}$. Die folgende Aussagen sind äquivalent:

1. Das Regelmäßige n-Eck ist konstruierbar.
2. Es gibt ein $m \in \mathbb{N}$ mit $\varphi(n) = 2^m$.
3. Es gibt $r, s \in \mathbb{N}$ und $p_1, \cdots, p_r$ paarweise verschiedene Fermatprimzahlen mit $n = 2^s p_1 \cdots p_r$. □

Beweis. Sei Sei $z = e^{\frac{2i\pi}{n}}$ und $\Phi_n = \chi_z$. Es gilt $D_{\mathbb{Q}}(\chi_z) = \mathbb{Q}_n = \mathbb{Q}(z)$. Das Regelmäßiges n-Eck ist genau dann konstruiebar, wenn $z \in W$.

(1. $\Rightarrow$ 2.) Für $z \in W$ gilt $\varphi(n) = [\mathbb{Q}(z) : \mathbb{Q}] = 2^m$ für ein $m \in \mathbb{N}$ nach Korollar 3.3.14.

(2. $\Rightarrow$ 1.) Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(z)$ ist Galois von Grad $[\mathbb{Q}(z) : \mathbb{Q}] = \varphi(n) = 2^m$. Die Aussage folgt aus dem obigen Satz.

(2. $\Leftrightarrow$ 3.) Sei $n = 2^s p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primzerlegung von n. Es gilt $\varphi(n) = 2^{s-1} p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$. Die Behauptung $\varphi(n) = 2^m$ ist äquivalent zu $\alpha_i = 1$ für alle i und $p_i - 1$ ist eine Potenz von 2 *i.e.* p_i ist eine Fermatprimzahl. ∎

4.6 Radikalerweiterungen

Beispiel 4.6.1 Seien $a, b, c, d \in \mathbb{Q}$.

1. Sei $P = aX^2 + bX + c$. Dann lassen sich die Nullstellen von P durch

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ und } \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

bestimmen.

2. Sei $P = aX^3 + bX^2 + cX + d$. Dann ist

$$\sqrt[3]{\left(\frac{bc}{6a^2} - \frac{b^3}{27a^3} - \frac{d}{2a}\right) + \sqrt{\left(\frac{bc}{6a^2} - \frac{b^3}{27a^3} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}}$$
$$+ \sqrt[3]{\left(\frac{bc}{6a^2} - \frac{b^3}{27a^3} - \frac{d}{2a}\right) - \sqrt{\left(\frac{bc}{6a^2} - \frac{b^3}{27a^3} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

eine Nullstelle von P. Damit kann man P als Produkt von Polynome von Grad 1 und 2 schreiben und dank 1. alle Nullstellen finden.

3. Dies ist auch für Polynome von Grad 4 möglich.

In diesem Abschnitt wollen wir die Frage: *kann mann alle Nullstellen eines Polynom $P \in \mathbb{Q}[X]$ durch das sukzessive Ziehen von Wurzeln berechnen?* antworten.

Definition 4.6.2 Ein Polynom $P \in K[X]$ heißt **rein** falls $P(X) = X^n - a$ mit $\operatorname{char} K \not| n$ und $a \in K$. Jede Nullstelle von P heißt n-te Wurzel aus a.

Satz 4.6.3 Sei $a \in K^\times$ und $L = D_K(P)$ der Zerfallungskörper von $P = X^n - a$ mit $\operatorname{char} K \not| n$.

1. Es gilt $K \subset L$ ist Galois.

2. Für eine beliebige Nullstelle b von P ist

$$P = \prod_{\zeta \in E_n(K)} (X - \zeta b)$$

über L und $L = K_n(b)$.

3. Es gilt $\operatorname{Gal}(L/K_n) \subset \mathbb{Z}/n\mathbb{Z}$, insbesondere ist $\operatorname{Gal}(L/K_n)$ zyklisch. Für P irreduzibel über K_n gilt $\operatorname{Gal}(L/K_n) = \mathbb{Z}/n\mathbb{Z}$. □

Beweis. 1. Es gilt $P' = nX^{n-1} \neq 0$ also ist P separabel und $K \subset D_K(P) = L$ ist Galois.

2. Da P separabel ist, hat P genau n Nullstellen: die Elemente ζb für $\zeta \in E_n(K)$. Es folgt $L = K(b, E_n(K)) = K_n(b)$.

3. Sei $\zeta \in PE_n(K)$ eine primitive n-te Einheitswurzel und b eine Nullstelle von P. Jedes $f \in \operatorname{Gal}(L/K_n)$ permutiert die Nullstellen von P also $f(b) = \zeta^{m_f} b$ für ein $m_f \in \mathbb{Z}/n\mathbb{Z}$. Die Abbildung $\varphi : \operatorname{Gal}(L/K_n) \to \mathbb{Z}/n\mathbb{Z}$ definiert durch $f \mapsto m_f$ ist ein Gruppenhomomorphismus und injektiv: Es gilt $f \circ f'(b) = f(\zeta^{m_{f'}} b) = \zeta^{m_{f'}} f(b) = \zeta m_f m_{f'} b$ also $\varphi(ff') = m_f m_{f'} = \varphi(f)\varphi(f')$. Es gilt auch für $\varphi(f) = 1 : m_f = 1$ also $f(b) = b$ und da $L = K_n(b)$ folgt $f = \mathrm{Id}_L$. Daraus folgt $\operatorname{Gal}(L/K_n) \subset \mathbb{Z}/n\mathbb{Z}$.

Für P irreduzibel über K_n gilt $n = [K_n(b) : K_n] = [L : K_n] = |\operatorname{Gal}(L/K_n)|$ und also $\operatorname{Gal}(L/K_n) = \mathbb{Z}/n\mathbb{Z}$. ■

Satz 4.6.4 Sei $n \in \mathbb{N}$ und K ein Körper mit $E_n(K) \subset K$. Sei $K \subset L$ eine Galois Erweiterung mit $\operatorname{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$. Dann gibt es ein $b \in L$ mit $a = b^n \in K$ mit

$$L = K(b) \simeq K[X]/(X^n - a)$$

also $K \subset L$ ist rein. □

Beweis. Sei $\zeta \in PE_n(K) \subset K$ und sei $f \in \mathrm{Gal}(L/K)$ ein Erzeuger der Gruppe. Dann sind $\mathrm{Id}_L = f^0, f, \cdots, f^{n-1}$ linear unabhängig. Sei also $x \in L$ mit $\sum_{k=0}^{n-1} \zeta^k f^k(x) \neq 0$. Setze

$$b = \sum_{k=0}^{n-1} \zeta^k f^k(x) \in L.$$

Es gilt

$$\zeta f(b) = \zeta \sum_{k=0}^{n-1} \zeta^k f^{k+1}(x) = \sum_{k=0}^{n-1} \zeta^{k+1} f^{k+1}(x) = \sum_{k=0}^{n-1} \zeta^k f^k(x) = b.$$

Daraus folgt $f(b^n) = f(b)^n = b^n$ und also für $a = b^n$ gilt $f^k(a) = a$ für alle k. Daraus folgt $a \in L^{\mathrm{Gal}(L/K)} = K$.

Es gilt $f(b) = \zeta^{-1} b$ und also $f^k(b) = \zeta^{-k} b$. Daraus folgt, dass $\mathrm{Gal}(L/K(b)) = \{id_L\}$ und also $L = K(b)$. Es folgt auch $[K(b) : K] = [L : K] = n$ und das Minimalpolynom χ_b von b über K hat Grad n. Da b eine Nullstelle von $P = X^n - a \in K[X]$ ist, gilt $\chi_b = P$. ∎

Beispiel 4.6.5 Sei $K = \mathbb{Q} \subset L$ mit $[L : K] = 2$. Sei $a \in L \backslash K$. Dann gilt $\deg(\chi_a) > 1$ und $\deg(\chi_a) | [L : K] = 2$ also $\deg(\chi_a) = 2$. Es folgt $L = D_K(\chi_a)$ und $K \subset L$ ist Galois mit $|\mathrm{Gal}(L/K)| = [L : K] = 2$. Es folgt $\mathrm{Gal}(L/K) = \mathbb{Z}/2\mathbb{Z}$ und $K \subset L$ ist rein.

Für $\chi_a = X^2 + pX + q$ gilt $L = \mathbb{Q}(\sqrt{\Delta})$, wobei $\Delta = p^2 - 4q$ **die Diskriminante von** P ist.

Satz 4.6.6 Sei $n \in \mathbb{N}$ mit $\mathrm{char}\, K \not| n$, sei $a \in K^\times$, sei $P = X^n - a$ und sei $L = D_K(P)$ Dann gilt

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K_n) \rtimes \mathrm{Gal}(K_n/K) \subset \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times,$$

wobei die Operation von $(\mathbb{Z}/n\mathbb{Z})^\times \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ (x, y) \mapsto xy$ induziert ist. □

Beweis. Sei $\zeta \in PE_n(K)$ und b eine n-te Wurzel aus a. Dann gilt $K \subset K_n = K(\zeta) \subset L = K(\zeta, b)$. Alle Erweiterungen sind Galois also ist $N = \mathrm{Gal}(L/K_n)$ ein Normalteiler von $G = \mathrm{Gal}(L/K)$.

Für jedes $f \in \mathrm{Gal}(K_n/K)$ gibt es ein eindeutiges Element $\varphi(f) \in \mathrm{Gal}(L/K)$ definiert durch $\varphi|_{K_n} = f$ und $\varphi(f)(b) = b$. Dies definiert eine Abbildung $\varphi : \mathrm{Gal}(K_n/K) \to \mathrm{Gal}(L/K)$. Da $\varphi(f)$ eindeutig durch $\varphi|_{K_n} = f$ und $\varphi(f)(b) = b$ bestimmt ist gilt $\varphi(ff') = \varphi(f)\varphi(f')$ also φ ist ein injektiver Gruppenhomomorphimsus. Daraus folgt, dass $G = \mathrm{Gal}(L/K)$ eine Untergruppe H besitzt, die isomorph zu $\mathrm{Gal}(K_n/K)$ ist. Ein Element in H ist der Form $\varphi(f)$ für ein $f \in \mathrm{Gal}(K_n/K)$. Falls $\varphi(f) \in N = \mathrm{Gal}(L/K_n)$ gilt $\varphi(f)|_{K_n} = \mathrm{Id}_{K_n}$ also $f = \mathrm{Id}_{K_n}$ und $\varphi(f) = \mathrm{Id}_L$. Daraus folgt, dass $H \cap N = \{e_G\}$. Aus dem Satz 1.7.5 folgt $G = N \rtimes H$.

Die Operation von H über N ist gegeben durch $(h, n) \mapsto hnh^{-1}$. Die Abbildung $N = \mathrm{Gal}(L/K_n) \subset \mathbb{Z}/n\mathbb{Z}$ ist gegeben durch $f \mapsto m_f$, wobei $f(b) = \zeta^{m_f} b$. Die

Abbildung $H = \mathrm{Gal}(K_n/K) \subset (\mathbb{Z}/n\mathbb{Z})^\times$ ist gegeben durch $h \mapsto n_h$, wobei $h(\zeta) = \zeta^{n_h}$ und $h(b) = b$. Es folgt $hfh^{-1}(b) = hf(b) = h(\zeta^{m_f} b) = \zeta^{n_h m_f} b$ also $n_h \cdot m_f = m_{hfh^{-1}} = n_h m_f$. ∎

Korollar 4.6.7 Sei $a \in \mathbb{Q} = K$ mit $P = X^n - a$ irreduzibel über $\mathbb{Q}_n$ und sei $L = D_{\mathbb{Q}}(P)$. Dann gilt

$$\mathrm{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^\times.$$

Definition 4.6.8 Eine Erweiterung $K \subset L$ heißt **radikal** falls es eine Kette von Erweiterungen

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r+1} = L$$

gibt mit $L_{i+1} = L_i(b_i)$, wobei $a_i = b_i^{n_i} \in L_i$ für alle i.

Satz 4.6.9 Sei $\mathrm{char}\, K = 0$ und $K \subset L$ eine radikale Erweiterung. Dann existiert eine Erweiterung $L \subset M$ so, dass $K \subset M$ galois und radikal ist. □

Beweis. Per Induktion nach $[L : K]$. Für $L = K$ ist die Aussage klar mit $M = K$. Die Behauptung sei wahr für Erweiterungen $K \subset K'$ mit $[K' : K] < [L : K]$. Die Behauptung ist insbesondere wahr für K_r in einer Kette wie in Definition 4.6.8. Es gibt also eine Galois und radikale Erweiterung $K \subset M_r$ mit $M_r \supset K_r$. Es gibt also ein separables Polynom $Q \in K[X]$ mit $M_r = D_K(Q)$. Sei $G = \mathrm{Gal}(M_r/K)$ und

$$P = \prod_{f \in G} (X^{n_r} - f(a_r)),$$

wobei $a_r = b_r^{n_r}$. Es gilt $f(P) = P$ für jedes $f \in G$ also $P \in K[X]$. Sei $M = D_K(PQ)$. Es gilt $M_r \subset M$. Da $L = K_r(b_r)$, $b_r \in M$ und $K_r \subset M_r$, gilt $L \subset M$. Da $\mathrm{char}\, K = 0$ folgt, dass PQ separabel ist also $K \subset M$ ist Galois. Da M durch Ajunktion der n_r-ten Wurzeln der $f(a_r)$ für alle $f \in G$ entsteht, ist $M_r \subset M$ radikal und auch $K \subset M$, weil $K \subset M_r$ radikal ist. ∎

Lemma 4.6.10 Sei $\mathrm{char}\, K = 0$ und $K \subset L$ eine Galois Erweiterung. Dann ist $K \subset L_n$ auch Galois und $\mathrm{Gal}(L_n/K_n) \subset \mathrm{Gal}(L/K)$. □

Beweis. Sei $P \in K[X]$ mit $L = D_K(P)$. Dann gilt $L_n = D_K((X^n - 1)P)$ und also $K \subset L_n$ ist Galois (jede Erweiterung ist separabel in Charakteristik 0). Nach dem Hauptsatz der Galois Theorie gilt $\mathrm{Gal}(L_n/K_n) \subset \mathrm{Gal}(L_n/K)$ und $\mathrm{Gal}(L_n/K)/\mathrm{Gal}(L_n/L) \simeq \mathrm{Gal}(L/K)$. Wir betrachten die Komposition: $\mathrm{Gal}(L_n/K_n) \to \mathrm{Gal}((L/K)$. Der Kern ist $\mathrm{Gal}(L_n/K_n) \cap \mathrm{Gal}(L_n/L)$. Sei $f \in \mathrm{Gal}(L_n/K_n) \cap \mathrm{Gal}(L_n/L)$. Dann gilt $f|_{K_n} = \mathrm{Id}_{K_n}$ und $f|_L = \mathrm{Id}_L$. Da $L_n = L(E_n) = L(K_n)$ folgt $f = \mathrm{Id}_{L_n}$ und die Abbildung ist injektiv. ∎

Satz 4.6.11 Sei $\mathrm{char}\, K = 0$, sei $P \in K[X]$ und $L = D_K(P)$. Die folgende Aussagen sind äquivalent:

1. Es gibt eine Radikalerweiterung $K \subset M$ mit $M \supset L$.
2. $\mathrm{Gal}(L/K)$ ist auflösbar.

M.a.W. lassen sich die Nullstellen von P durch das sukzessive Ziehen von Wurzeln genau dann berechnen, wenn $\mathrm{Gal}(D_{\mathbb{Q}}(P)/\mathbb{Q})$ auflösbar ist. □

Korollar 4.6.12 Sei $\mathrm{char}\, K = 0$, sei $P \in K[X]$ und $L = D_K(P)$. Die folgende Aussagen sind äquivalent:

1. Die Nullstellen von P lassen sich durch das sukzessive Ziehen von Wurzeln berechnen.
2. $\mathrm{Gal}(L/K)$ ist auflösbar.

Beweis. ($\Leftarrow$). Sei $G = \mathrm{Gal}(L/K)$ und $G = G_0 \supset \cdots \supset G_m = \{e_G\}$ eine Kette von Untergruppen mit $G_{i+1} \triangleleft G_i$ und G_i/G_{i+1} abelsch. Ohne Einschränkung kann man (dank Satz 1.11.12) annehmen, dass G_i/G_{i+1} zyklisch (*i..e* der Form $\mathbb{Z}/r\mathbb{Z}$) ist. Sei $n = |G|$ und $L_i = (L^{G_i})_n$.

Die Erweiterung $L^{G_{i-1}} \subset L$ ist Galois (per Definition) und da $G_i \triangleleft G_{i-1}$ ist nach dem Hauptsatz der Galoistheorie die Erweiterung $L^{G_{i-1}} \subset L^{G_i}$ auch Galois.

Nach dem obigen Lemma ist $L_i \subset L_{i-1}$ Galois und $\mathrm{Gal}(L_i/L_{i-1}) \subset \mathrm{Gal}(L^{G_i}/L^{G_{i-1}}) = G_{i-1}/G_i$ (die letzte Gleichung folgt aus dem Hauptsatz der Galoisthorie). Diese Gruppe ist also Zyklisch der Ordnung ein Teiler von n. Nach Satz 4.6.4 existiert für jedes i ein $b_{i-1} \in L_i$ mit $L_i = L_{i-1}(b_{i-1})$ und $b_{i-1}^n \in L_{i-1}$. Somit ist $M = L_m$ eine Radikale Erweiterung von K und es gilt $M = L_m \supset L^{G_m} = L$.

($\Rightarrow$). Dank Satz 4.6.9 können wir ohne Einschränkung annehmen, dass $K \subset M$ Galois ist. Sei $K = L_0 \subset \cdots \subset L_m = M$ eine Kette von Erweiterungen mit $L_{i+1} = L_i(b_i)$ und $b_i^{n_i} \in L_i$. Sei $n = \prod_i n_i$ und $L_i' = (L_i)_n$. Es gilt $L_m' = M_n$ und $K \subset M_n$ ist Galois also auch $L_i' \subset M_n$ für alle i. Es gilt $L_{i+1}' = L_i'(b_i) = (L_i)_n(b_i)$ also ist $L_{i+1}' = D_{L_i}(X^{n_i} - b_i^{n_i})$ und $L_i \subset L_{i+1}'$ ist Galois mit $\mathrm{Gal}(L_{i+1}'/L_i')$ zyklisch also abelsch (Satz 4.6.3). Daraus folgt, dass $L_i' \subset L_{i+1}'$ Galois ist. Es folgt $\mathrm{Gal}(M_n/L_{i+1}') \triangleleft \mathrm{Gal}(M_n/L_i')$. Es gilt auch

$$\mathrm{Gal}(M_n/L_i')/\mathrm{Gal}(M_n/L_{i+1}') \simeq \mathrm{Gal}(L_{i+1}'/L_i') \text{ ist zyklisch also abelsch.}$$

Es gilt auch $K \subset K_n$ ist Galois also gilt $\mathrm{Gal}(M_n/K_n) \triangleleft \mathrm{Gal}(M_n/K)$ und es gilt

$$\mathrm{Gal}(M_n/K)/\mathrm{Gal}(M_n/K_n) \simeq \mathrm{Gal}(K_n/K) \text{ ist zyklisch also abelsch.}$$

Die Folge

$$\{e\} = \mathrm{Gal}(M_n/L_m') \subset \cdots \subset \mathrm{Gal}(M_n/L_0') = \mathrm{Gal}(M_n/K_n) \subset \mathrm{Gal}(M_n/K)$$

ist eine Reihe von Normalteiler mit abelschen Quotienten also ist $\mathrm{Gal}(M_n/K)$ auflösbar und auch die Quotientgruppe $\mathrm{Gal}(M/K)$. ■

Bemerkung 4.6.13 Sei $P \in \mathbb{Q}[X]$ ein Polynom von Grad ≤ 4 und $K = D_{\mathbb{Q}}(P)$. Dann ist $\mathbb{Q} \subset K$ Galois und die Galois Gruppe ist eine Untergruppe der Gruppe Bij({Nullstellen von P}. Insbesondere ist $\mathrm{Gal}(K/\mathbb{Q})$ eine Untergruppe von S_4. Da S_4 auflösbar ist (mit der Folge:

$$\{\mathrm{Id}\} \triangleleft \{\mathrm{Id}, [12][34], [13][24], [14][23]\} \triangleleft A_4 \triangleleft S_4),$$

folgt, dass alle Nullstellen von P durch das sukzessive Ziehen von Wurzeln berechnenbar sind.

Wir zeigen, dass es, ab $\deg P \geq 5$, nicht mehr wahr ist.

Satz 4.6.14 Sei $P \in \mathbb{Q}[X]$ irreduzibel mit $\deg P = p$ eine Primzahl so, dass P genau $p-2$ reelle Nullstellen hat. Sei $L = D_{\mathbb{Q}}(P)$.

Dann gilt $\mathrm{Gal}(L/\mathbb{Q}) = S_p$. □

Beweis. Wir betrachten die Gruppe $G = \mathrm{Gal}(L/\mathbb{Q})$ als Untergruppe von der Gruppe Bij({Nullstellen von P}) $\simeq S_p$ (da $\mathrm{char}\,\mathbb{Q} = 0$ ist P separabel und hat also p paarweise verschiedene Nullstellen).

Da nicht alle Nullstellen reel sind gilt $L \cap \mathbb{R} \subsetneq L$. Da $\mathbb{Q} \subset L$ Galois ist, ist $L \cap \mathbb{R} \subset L$ auch Galois also gilt $\mathrm{Gal}(L/L\cap\mathbb{R}) \neq \{e\}$. Die Galois Gruppe $\mathrm{Gal}(L/L\cap\mathbb{R})$ permutiert also die beide nicht relle Nullstellen und wirkt trivial auf die anderen *i.e.* G enthält eine Transposition. Außerdem für $a \in L$ eine Nullstelle gilt $\mathbb{Q} \subset \mathbb{Q}(a) \subset L$ und $p = \deg P = [\mathbb{Q}(a) : \mathbb{Q}]|[L : \mathbb{Q}]$.

Nach Korollar 1.10.8 folgt $G = S_p$. ■

Beispiel 4.6.15 Sei $P = X^5 - 16X + 2$. Nach Eisenstein ist P irreduzibel. Es gilt

$$P(-1) = 17, P(1) = -13$$

also hat P mindestens 3 paarweise vershiedene reelle Nullstellen. Es gilt auch $P' = 5X^4 - 16$ also hat P' zwei reele Nullstellen und also hat P' genau drei reelle Nullstellen. Es folgt

$$\mathrm{Gal}(D_{\mathbb{Q}}(P)/\mathbb{Q}) = S_5$$

und diese Gruppe ist nicht auflösbar also können die Nullstellen von P nicht durch suzessives Wurzelziehen bescrhieben werden.

Korollar 4.6.16 Sei G eine endliche Gruppe. Dann gibt est eine Galois Erweiterung $K \subset L$ mit $\mathrm{char}\, K = 0$ mit $\mathrm{Gal}(L/K) = G$.

Beweis. Sei $G \subset S_p$ eine Einbettung mit $p \geq |G|$. Sei $P \in \mathbb{Q}[X]$ wie im obigen Satz und $L = D_{\mathbb{Q}}(P)$. Dann ist $\mathbb{Q} \subset L$ Galois mit $\mathrm{Gal}(L/\mathbb{Q}) = S_p$. Sei $K = L^G$, es gilt $\mathrm{Gal}(L/K) = G$. ■

5 Diskriminante

5.1 Resultante

Sei K ein Körper und seien $P = a_p X^p + \cdots + a_0$ und $Q = b_q X^q + \cdots + b_0$ Polynome in $K[X]$.

Für $n \in \mathbb{N}$ schreiben wir $K[X]_n = \langle 1, \cdots, X^n \rangle$. Sei

$$\begin{aligned} \Phi_{P,Q} : \quad & K[X]_{q-1} \times K[X]_{p-1} \to K[X]_{p+q-1} \\ & (U, V) \mapsto UP + VQ. \end{aligned}$$

Die Abbildung $\Phi_{P,Q}$ ist eine lineare Abbildung. Wir betrachten die Basen $\mathcal{B} = ((X^{q-1}, 0), \cdots, (1, 0), (0, X^{p-1}), \cdots, (0, 1))$ von $K[X]_{q-1} \times K[X]_{p-1}$ und $\mathcal{C} = (X^{p+q-1}, \cdots, 1)$ von $K[X]_{p+q-1}$. Es gilt

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{P,Q}) = \begin{pmatrix} a_p & 0 & \ddots & 0 & b_q & 0 & 0 & \cdots & 0 & 0 \\ a_{p-1} & a_p & \ddots & 0 & b_{q-1} & b_q & 0 & \ddots & 0 & 0 \\ \vdots & a_{p-1} & \ddots & 0 & \vdots & b_{q-1} & b_q & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & a_p & \vdots & \vdots & b_{q-1} & \ddots & 0 & 0 \\ a_1 & \vdots & \ddots & a_{p-1} & b_0 & \vdots & \vdots & \ddots & b_q & 0 \\ a_0 & a_1 & \ddots & \vdots & 0 & b_0 & \vdots & \ddots & b_{q-1} & b_q \\ 0 & a_0 & \ddots & \vdots & 0 & 0 & b_0 & \ddots & \vdots & b_{q-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_1 & \vdots & \vdots & 0 & \ddots & b_0 & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & 0 & \cdots & 0 & b_0 \end{pmatrix} \in M_{p+q}(K).$$

Definition 5.1.1 Die Matrix $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{P,Q})$ heißt **Sylvestermatrix von P und Q** und die Determinante $\mathrm{Res}(P, Q) = \det(\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{P,Q}))$ heißt **Resultante von P und Q**.

Lemma 5.1.2 Es gilt $\mathrm{Res}(Q, P) = (-1)^{pq}\mathrm{Res}(P, Q)$. □

Beweis. Um $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{Q,P})$ von $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{P,Q})$ zu erreichen muss man die p letzte Spalten mit den q ersten Spalten vertauchen und damit pq Spalten transponieren. Daraus folgt die Aussage. ■

Lemma 5.1.3 Die folgende Aussagen sind äquivalent:

1. $\mathrm{Res}(P,Q) = 0$
2. Es gibt $(U,V) \in K[X]_{q-1} \times K[X]_{p-1}$ nicht beide null mit $UP + VQ = 0$. □

Beweis. Da $\dim(K[X]_{q-1} \times K[X]_{p-1}) = \dim(K[X]_{p+q-1}$ ist $\Phi_{P,Q}$ genau dann bijektiv, wenn es injektiv ist. Also gilt $\mathrm{Res}(P,Q) = 0$ genau dann, wenn $\mathrm{Ker}\Phi_{P,Q} \neq 0$ *i.e.*, wenn es $(U,V) \in K[X]_{q-1} \times K[X]_{p-1}$ nicht beide null gibt mit $UP + VQ = 0$. ∎

Lemma 5.1.4 Die folgende Aussagen sind äquivalent:

1. $\mathrm{ggT}(P,Q) \neq 1$
2. Es gibt $(U,V) \in K[X]_{q-1} \times K[X]_{p-1}$ nicht beide null mit $UP + VQ = 0$. □

Beweis. Sei $R = \mathrm{ggT}(P,Q)$. Dann ist $U = -Q/R$ und $V = P/R$ eine Lösung der Gleichung $UP + VQ = 0$. Umgekehrt, für $\mathrm{ggT}(P,Q) = 1$ und (U,V) eine Lösung mit $UP + VQ = 0$ gilt $P|VQ$ also $P|V$ und $\deg(V) \geq \deg(P) = p$ oder $V = 0$ also $V = 0$. Analog gilt $U = 0$. ∎

Korollar 5.1.5 Es gilt $\mathrm{Res}(P,Q) = 0 \Leftrightarrow \mathrm{ggT}(P,Q) \neq 1$.

Sei R der Ring $R = K[X]/(P)$ und sei $m_Q : R \to R$ die Abbildung definiert durch $m_Q([A]) = [QA]$.

Lemma 5.1.6 Die Abbildung m_Q ist linear und es gilt

$$\mathrm{Res}(P,Q) = a_p^q \det(m_Q).$$

Beweis. Die Abbildung m_Q ist linear (Übung).

Sei $\theta : K[X]_{q-1} \times K[X]_{p-1} \to K[X]_{p+q-1}$ definiert durch $\theta(U,V) = UP + V$. Diese Abbildung ist Linear und es gilt

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\theta) = \begin{pmatrix} a_p & 0 & \ddots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ a_{p-1} & a_p & \ddots & 0 & 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & a_{p-1} & \ddots & 0 & \vdots & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & a_p & \vdots & \vdots & 0 & \ddots & 0 & 0 \\ a_1 & \vdots & \ddots & a_{p-1} & 1 & \vdots & \vdots & \ddots & 0 & 0 \\ a_0 & a_1 & \ddots & \vdots & 0 & 1 & \vdots & \ddots & 0 & 0 \\ 0 & a_0 & \ddots & \vdots & 0 & 0 & 1 & \ddots & \vdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_1 & \vdots & \vdots & 0 & \ddots & 1 & \vdots \\ 0 & 0 & \cdots & a_0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Insbesondere gilt $\det(\theta) = a_p^q \neq 0$ und θ ist invertierbar. Wir setzen $\varphi = \Phi_{P,Q} \circ \theta^{-1}$. Es gilt

$$\det(\varphi) = \det(\Phi_{P,Q}) \det(\theta)^{-1} = a_p^{-q} \mathrm{Res}(P,Q).$$

Da θ bijektiv ist, sind alle Elemente in $K[X]_{p+q-1}$ der Form $UP + V$ und es gilt

$$\varphi(UP + V) = \varphi(\theta(U,V)) = \Phi_{P,Q}(U,V) = UP + VQ.$$

Sei $\mathcal{C} = (1, X, \cdots, X^{p-1}, P, XP, \cdots X^q P)$. Dies ist eine Basis von $K[X]_{p+q-1}$. Es gilt $\varphi(X^i P) = X^i P$ für alle $i \in [1, q-1]$. Für $j \in [1, p-1]$ gilt $\varphi(X^j) = X^j Q$. Sei Sei $X^j Q = A_j P + B_j$ die Restdivision von $X^j Q$ nach P, wobei $\deg(B_j) \leq p-1$. Es gilt $\deg(A_j) \leq q + j - p$. Wir schreiben $A_j = \alpha_{j,0} + \cdots + \alpha_{j,q+j-p} X^{q+j-p}$ und $B_j = \beta_{j,0} + \cdots + \beta_{j,p-1} X^{p-1}$. Die Matrix von φ in der Basis $\mathcal{C}'$ ist also

$$\mathrm{Mat}_{\mathcal{C}'}(\varphi) = \begin{pmatrix} \beta_{0,0} & \cdots & \beta_{p-1,0} & 0 & 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots & & & & \vdots \\ \beta_{0,m_1} & \cdots & \beta_{p-1,p-1} & 0 & 0 & \cdots & 0 & 0 \\ \alpha_{0,0} & \cdots & \alpha_{0,p-1} & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & & \vdots & 0 & \ddots & \ddots & & \vdots \\ \alpha_{0,q-p} & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \vdots & \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \alpha_{p-1,p+q-1} & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Sei M die Matrix $M = (\beta_{i,j})_{i,j \in [0,p-1]}$. Es gilt $\det(\varphi) = \det(M)$.

Wir zeigen, dass M die Matrix von m_Q in der Basis $\mathcal{D} = ([1], \cdots, [X^{p-1}])$ ist: Es gilt $m_Q([X^j]) = [X^j Q] = [A_j P + B_j] = [B_j] = \beta_{j,0}[1] + \cdots + \beta_{j,p-1}[X^{p-1}]$. Dies zeigt die Behauptung $\mathrm{Mat}_{\mathfrak{D}}(m_Q) = M$. Es folgt

$$\mathrm{Res}(P,Q) = a_p^q \det(\varphi) = a_p^q \det(M) = a_p^q \det(\mathrm{Mat}_{\mathfrak{D}}(m_Q)) = a_p^q \det(m_Q)$$

und das Lemma folgt. ∎

Korollar 5.1.7 Für $Q = X - \beta$ gilt $\mathrm{Res}(P,Q) = (-1)^p P(\beta)$.

Beweis. Es gilt $\mathrm{Res}(P,Q) = (-1)^p \mathrm{Res}(Q,P)$. Sei $m_P : K[X]/(Q) \to K[X]/(Q)$ definiert durch $m_P([A]) = [AP]$. Es gilt $\mathrm{Res}(Q,P) = \det(m_P)$. Für $A \in A[X]$ gilt $[A] = A(\beta) \in K$. Es folgt, dass $m_P([A]) = [AP] = A(\beta)P(\beta)$ und m_P ist die Abbildung $m_P : K \to K,\ a \mapsto P(\beta)a$. Insbesondere gilt $\det(m_P) = P(\beta)$. ∎

Korollar 5.1.8 Es gilt $\mathrm{Res}(P, Q_1 Q_2) = \mathrm{Res}(P,Q_1)\mathrm{Res}(P,Q_2)$. und $\mathrm{Res}(P_1 P_2, Q) = \mathrm{Res}(P_1,Q)\mathrm{Res}(P_1,Q)$.

Beweis. Die zweite Aussage folge aus der ersten Aussage und Lemma 5.1.2.

Sei $q_1 = \deg(Q_1)$ und $q_2 = \deg(Q_2)$. Es gilt $\mathrm{Res}(P, Q_1Q_2) = a_p^{q_1+q_2} \det(m_{Q_1Q_2})$. Es gilt aber $m_{Q_1Q_2}(A) = [Q_1Q_2A] = m_{Q_1}(m_{Q_2}(A))$ also $m_{Q_1Q_2} = m_{Q_1}m_{Q_2}$. Daraus folgt $\det(m_{Q_1Q_2}) = \det(m_{Q_1})\det(m_{Q_2})$. Es gilt also

$$\mathrm{Res}(P, Q_1Q_2) = a_p^{q_1} \det(m_{Q_1}) a_p^{q_2} \det(m_{Q_2}) = \mathrm{Res}(P, Q_1)\mathrm{Res}(P, Q_2).$$

Daraus folgt die erste Aussage. ∎

Korollar 5.1.9 Sei $L = D_K(PQ)$ und $\alpha_1, \cdots, \alpha_p \in L$ und $\beta_1, \cdots, \beta_q \in L$ mit

$$P = a_p \prod_{i=1}^{p} (X - \alpha_i) \text{ und } Q = b_q \prod_{j=1}^{q} (X - \beta_j).$$

Es gilt

$$\mathrm{Res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

Beweis. Per Induktion nach q. Für $q = 0$ gilt $\mathcal{B} =$ und

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\Phi_{P,Q}) = \begin{pmatrix} b_q & 0 & \cdots & 0 \\ 0 & b_q & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b_q \end{pmatrix}.$$

Daraus folgt $\mathrm{Res}(P, Q) = b_q^p = a_p^q b_q^p$.

Sei $q > 0$. Angenommen die Aussage sei wahr für $q - 1$. Sei $Q_1 = b_q \prod_{j=1}^{q-1} (X - \beta_j)$ und $Q_2 = X - \beta_q$ Es gilt

$$\mathrm{Res}(P, Q) = \mathrm{Res}(P, Q_1)\mathrm{Res}(P, Q_2) = a_p^{q-1} b_q^p \left(\prod_{i=1}^{p} \prod_{j=1}^{q-1} (\alpha_i - \beta_j) \right) (-1)^p P(\beta_q).$$

Es folgt

$$\mathrm{Res}(P, Q) = a_p^{q-1} b_q^p \left(\prod_{i=1}^{p} \prod_{j=1}^{q-1} (\alpha_i - \beta_j) \right) (-1)^p a_p \left(\prod_{i=1}^{p} (\beta_q - \alpha_i) \right) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

Daraus folgt die Aussage. ∎

Korollar 5.1.10 Sei $M = D_K(P)$ und $\alpha_1, \cdots, \alpha_p \in L$ die Nullstellen von P. Es gilt

$$\mathrm{Res}(P, Q) = a_p^q \prod_{i=1}^{p} Q(\alpha_i).$$

Beweis. Sei $L = D_K(PQ)$ und $\beta_1, \cdots, \beta_q$ die Nullstellen von Q in M. Es gilt $Q(\alpha_i) = b_q \prod_{j=1}^{q}(\alpha_i - \beta_j)$. Daraus folgt

$$a_p^q \prod_{i=1}^{p} Q(\alpha_i) = a_p^q \prod_{i=1}^{p} \left(b_q \prod_{j=1}^{q} (\alpha_i - \beta_j) \right) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j) = \mathrm{Res}(P, Q)$$

nach dem obigen Korollar. ∎

5.2 Diskriminante

Definition 5.2.1 Sei $P \in K[X]$ mit $\deg P = p$ und $L = D_K(P)$. Seien $\alpha_1, \cdots, \alpha_p \in L$ die Nullstellen von P. **Die Diskriminante von** P ist das Element $\Delta(P) \in L$ definiert durch

$$\Delta(P) = (-1)^{\frac{p(p-1)}{2}} a_p^{2p-2} \prod_{\substack{i,j=1 \\ i \neq j}}^{p} (\alpha_i - \alpha_j).$$

Bemerkung 5.2.2 1. Da es schwer die Nullstellen eines Polynoms zu berechnen ist, ist es *a priori* schwer die Diskriminante zu bestimmen.

2. Es gilt auch

$$\Delta(P) = a_p^{2p-2} \prod_{\substack{i,j=1 \\ i < j}}^{p} (\alpha_i - \alpha_j)^2.$$

3. Sei $P \in \mathbb{Q}[X]$. Wenn alle Nullstellen von P reelle Zahlen sind gilt $\Delta(P) \geq 0$.

Beispiel 5.2.3 Für $P = X^2 + pX + q$ sind die Nullstellen $z_1 = -\frac{p}{2} + \frac{\sqrt{p^2-4q}}{2}$ und $z_2 = -\frac{p}{2} - \frac{\sqrt{p^2-4q}}{2}$. Daraus folgt

$$\Delta(P) = -(z_1 - z_2)(z_2 - z_1) = p^2 - 4q.$$

Allgemeiner, für $P = aX^2 + bX + c$ gilt

$$\Delta(P) = b^2 - 4ac.$$

Satz 5.2.4 Es gilt $\Delta(P) = 0$ genau dann, wenn P mehrfache Nullstellen hat. □

Beweis. Es gilt $\Delta(P) = 0$ genau dann, wenn es ein Paar (α_i, α_j) gibt mit $i \neq j$ und $\alpha_i = \alpha_j$. ∎

Satz 5.2.5 Sei $P \in K[X]$ separabel. Es gilt $\Delta(P) \in K$ □

Beweis. Die Erweiterung $K \subset L = D_K(P)$ ist Galois. Seien $\alpha_1, \cdots, a_p$ die Nullstellen von P. Sei $G = \mathrm{Gal}(L/K)$. Es gilt $K = L^G$. Sei $\sigma \in G$. Wir betrachten σ als Permutation der Nulstellen von P. Es gilt $\sigma(\alpha_i) = \alpha_{\sigma(i)}$. Daraus folgt

$$\sigma(\Delta(P)) = \sigma(a_p)^{2p-2} \prod_{\substack{i,j=1 \\ i \neq j}}^{p} (\sigma(\alpha_i) - \sigma(\alpha_j)) = a_p^{2p-2} \prod_{\substack{i,j=1 \\ i \neq j}}^{p} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) \text{ also}$$

$$\sigma(\Delta(P)) = \sigma(a_p)^{2p-2} \prod_{\substack{i,j=1 \\ \sigma^{-1}(i) \neq \sigma^{-1}(j)}}^{p} (\alpha_i - \alpha_j) = a_p^{2p-2} \prod_{\substack{i,j=1 \\ i \neq j}}^{p} (\alpha_i - \alpha_j) = \Delta(P).$$

Es folgt $\Delta(P) \in L^G = K$. ∎

Satz 5.2.6 Es gilt

$$\Delta(P) = (-1)^{\frac{p(p-1)}{2}} \frac{\mathrm{Res}(P, P')}{a_p},$$

wobei P' die Ableitung von P ist. □

Beweis. Sei $M = D_K(P)$ und seien $\alpha_1, \cdots, \alpha_p \in L$ die Nullstellen von P. Es gilt $\mathrm{Res}(P, P') = a_p^{p-1} \prod_{i=1}^{p} P'(\alpha_i)$. Aber es gilt

$$P' = a_p \sum_{j=1}^{p} \left(\prod_{\substack{k=1 \\ k \neq j}}^{p} (X - \alpha_k) \right).$$

Daraus folgt

$$P'(\alpha_i) = a_p \prod_{\substack{k=1 \\ k \neq i}}^{p} (\alpha_i - \alpha_k)$$

und

$$\mathrm{Res}(P, P') = a_p^{p-1} \prod_{i=1}^{p} P'(\alpha_i) = a_p^{p-1} \prod_{i=1}^{p} \left(a_p \prod_{\substack{k=1 \\ k \neq i}}^{p} (\alpha_i - \alpha_k) \right) = a_p^{2p-1} \prod_{\substack{i,j=1 \\ i \neq j}}^{p} (\alpha_i - \alpha_j).$$

Daraus folgt die Aussage. ∎

Bemerkung 5.2.7 Mit diesem Satz kann man die Diskriminante leicht berechnen: es ist ein Determinante.

Beispiel 5.2.8 Sei $P = X^3 + qX + q \in K[X]$. Es gilt

$$\Delta(P) = (-1)^{\frac{3(3-1)}{2}} \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{vmatrix} = -(4p^3 + 27q^2).$$

Zur Erinerung,

$$\begin{aligned} z &= \sqrt[3]{\frac{q}{2} + \sqrt{\frac{4p^3+27q^2}{4\cdot 27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{4p^3+27q^2}{4\cdot 27}}} \\ &= \sqrt[3]{\frac{q}{2} + \sqrt{-\frac{\Delta(P)}{4\cdot 27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{-\frac{\Delta(P)}{4\cdot 27}}} \end{aligned}$$

ist eine Nullstelle von P.

Satz 5.2.9 Sei $P \in K[X]$ separabel und $L = D_K(P)$. Sei $G = \mathrm{Gal}(L/K)$. Wir betrachten G als untergruppe von S_p. Es gilt

$$(\Delta(P) = \delta^2 \text{ mit } \delta \in K) \Leftrightarrow (\mathrm{Gal}(L/K) \subset A_p).$$

Beweis. Es gilt

$$\Delta(P) = a_p^{2p-2} \prod_{\substack{i,j=1 \\ i<j}}^{p} (\alpha_i - \alpha_j)^2$$

also ist $\Delta(P)$ genau dann ein Quadrat in K, wenn

$$\delta = \prod_{\substack{i,j=1 \\ i<j}}^{p} (\alpha_i - \alpha_j)^2 \in K.$$

Sei $\sigma \in G$. Es gilt

$$\begin{aligned} \sigma(\delta) &= \prod_{\substack{i,j=1 \\ i<j}}^{p} (\sigma(\alpha_i) - \sigma(\alpha_j))^2 \\ &= \prod_{\substack{i,j=1 \\ i<j}}^{p} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2 \\ &= \prod_{\substack{i,j=1 \\ \sigma^{-1}(i)<s^{-1}(j)}}^{p} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\varepsilon(\sigma)} \prod_{\substack{i,j=1 \\ i<j}}^{p} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\varepsilon(\sigma)} \delta. \end{aligned}$$

Insbesondere gilt

$$\delta \in K \Leftrightarrow \sigma(\delta) = \delta \text{ für alle } \sigma \in G \Leftrightarrow \varepsilon(\sigma) = 1 \text{ für alle } \sigma \in G \Leftrightarrow \sigma \in A_p.$$

Daraus folgt die Aussage. ∎

Satz 5.2.10 (Polynome von Grad 3) Sei $P \in \mathbb{Q}[X]$ irreduzibel mit $\deg P = 3$. Sei $L = D_{\mathbb{Q}}(P)$ und seien z_1, z_2, z_3 die Nullstellen von P.

1. Falls $\Delta(P)$ ein Quadrat in $\mathbb{Q}$ ist, gilt

$$\mathrm{Gal}(L/K) \simeq A_3 \text{ und } L = \mathbb{Q}(z_i) \text{ für alle } i \in [1.3].$$

Die Erweiterung $\mathbb{Q} \subset L$ hat keinen nicht trivialen Zwischenkörper.

2. Falls $\Delta(P)$ kein Quadrat in $\mathbb{Q}$ ist, gilt

$$\mathrm{Gal}(L/K) \simeq S_3$$

Die Erweiterung $\mathbb{Q} \subset L$ hat 4 nicht trivialen Zwischenkörper:

$$\mathbb{Q}\left(\sqrt{\Delta(P)}\right), \mathbb{Q}(z_1), \mathbb{Q}(z_2), \mathbb{Q}(z_3).$$

3. Es gilt $(\Delta(P) > 0) \Leftrightarrow (z_i \in \mathbb{R}$ für alle $i \in [1,3])$. □

Beweis. Die Erweiterung $\mathbb{Q} \subset L$ ist Galois und die Nullstellen sind paarweise verschieden. Da P irreduzibel ist gilt $\chi_{z_i} = P$ für alle $i \in [1,3]$. Insbesondere gilt $[\mathbb{Q}(z_i) : \mathbb{Q}] = 3$ für alle $i \in [1,3]$. Da $\mathbb{Q}(z_i) \subset L$ für alle i, folgt $[L : Q] \geq 3$ und $|\mathrm{Gal}(L/\mathbb{Q}) \geq 3$.

1. Nach dem obigen Satz und da $\Delta(P)$ ein Quadrat i $\mathbb{Q}$ ist, gilt $\mathrm{Gal}(L/K) \subset A_3$ also $[L : \mathbb{Q}] \leq 3$. Es folgt $[L : \mathbb{Q}] = 3$ und $\mathrm{Gal}(L/K) = A_3$ und $L = \mathbb{Q}(z_i)$ für alle $i \in [1,3]$. Da $[L : \mathbb{Q}]$ ein Primzahl ist gibt es kein Zwischenkörper.

2. Sei $\Delta = \Delta(P)$. Es gilt $3 = [\mathbb{Q}(z_1) : \mathbb{Q}]|[L : \mathbb{Q}]$ und $2 = [\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}]|[L : \mathbb{Q}]$. Daraus folgt $6|[L : \mathbb{Q}]$. Da $\mathrm{Gal}(L/\mathbb{Q}) \subset S_3$ gilt $|\mathrm{Gal}(L/\mathbb{Q})| \leq 6$ und also $[L : \mathbb{Q}] \leq 6$. Es folgt $[L : \mathbb{Q}] = 6$ und $\mathrm{Gal}(L/\mathbb{Q}) = S_3$. Da S_3 nur 4 echte Untergruppe hat, hat die Erweiterung $\mathbb{Q} \subset L$ nur 4 Zwischenkörper.

3. Das Polynom P har immer eine reelle Nullstelle. Ohne einschränkung können wir annehmen, dass $z_1 \in \mathbb{R}$.

Angenommen $z_i \in \mathbb{R}$ für alle $i \in [1,3]$. Es gilt $(z_i - z_j)^2 > 0$ für alle $i, j \in [1,3]$ also $\Delta(P) > 0$.

Umgekehrt nehmen wir an, dass nicht alle Nullstellen von P reelle Zahlen sind. Da $P \in \mathbb{Q}[X]$, gilt also $z_3 = \bar{z}_2$ mit $z_2, z_3 \in \mathbb{C} \setminus R$. Daraus folgt $(z_1 - z_2)(z_1 - z_3) \in \mathbb{R}$ und also $(z_1 - z_2)^2(z_1 - z_3)^2 > \in \mathbb{R}_{>0}$. Wir schreiben $z_2 = x + iy$ und $z_3 = x - iy$ mit $y \neq 0$. Es gilt $(z_2 - z_3)^2 = (2iy)^2 = -4y^2 < 0$. Es folgt $\Delta(P) < 0$. ■

Index