Algebra I

Gabor Wiese
Université du Luxembourg
gabor.wiese@uni.lu

Gehalten an der Universität Duisburg-Essen im Wintersemester 2008/2009

Aufgeschrieben und überarbeitet von Johannes Hölken (johannes.hoelken@stud.uni-due.de)
Stand: 23. Januar 2012

Danksagungen

Die vorliegende Vorlesung basiert zu großen Teilen auf einer von Denis Vogel in Regensburg gehaltenen Veranstaltung und orientiert sich in vielen Punkten am Algebra-Buch von Siegfried Bosch.
An dieser Stelle möchte ich Denis noch einmal sehr herzlich für das Zurverfügungstellen seiner Aufzeichnungen danken.
Einen besonderen Dank möchte ich auch Johannes Hölken aussprechen für das Tippen der Mitschrift und die nachträgliche Ausarbeitung und Überarbeitung zu diesem Skript.

Gabor Wiese

Inhaltsverzeichnis

Kapitel I

Elementare Gruppentheorie

1 Gruppen und Homomorphismen

Definition 1.1 *(Monoid, Gruppe)*
Eine Menge G zusammen mit einer Abbildung

$$\begin{aligned} \bullet : G \times G &\to G \\ (g,h) &\mapsto g \bullet h \end{aligned}$$

heißt ein Monoid, falls

(i) *die Abbildung $\bullet$ assoziativ ist, d.h.*
$\forall\, a,b,c \in G: \qquad a \bullet (b \bullet c) = (a \bullet b) \bullet c$

(ii) *es ein bezüglich der Abbildung $\bullet$ neutrales Element gibt, d.h.*
$\exists\, e \in G\ \forall\, a \in G: \quad e \bullet a = a = a \bullet e$

Gilt zusätzlich, dass

(iii) *es zu jedem Element aus G ein inverses bezüglich der Abbildung $\bullet$ gibt, d.h.*
$\forall\, a \in G\ \exists\, b \in G: \quad a \bullet b = e = b \bullet a$

dann nennen wir $(G, \bullet)$ eine Gruppe. Weiter heißt eine Gruppe $(G, \bullet)$ kommutativ oder abelsch, wenn die Abbildung symmetrisch ist, d.h.

(iv) $\forall\, a,b \in G: \qquad a \bullet b = b \bullet a$

Beispiel 1 *(Gruppen / Monoiden)*

- $(\mathbb{Z}, +),\ (\mathbb{R}_+ \cup \{0\}, \cdot)$ *sind Gruppen*
- $(\mathbb{N} \cup \{0\}, +)$ *ist ein Monoid, aber keine Gruppe*

Beispiel 2 *(Allgemeine lineare Gruppe)*
Sei $\mathbb{K}$ ein Körper, wir bezeichnen die Menge der $n \times n$-Matritzen über $\mathbb{K}$ deren Determinante nicht Null ist mit

$$GL_n(\mathbb{K}) := \{A \in \mathrm{Mat}_{\mathbb{K}}(n,n) \mid \det(A) \neq 0\}$$

Die Menge $GL_n(\mathbb{K})$ bildet zusammen mit der Matritzenmultiplikation eine Gruppe und heißt die allgemeine lineare Gruppe.

Bemerkung 1.2 *Ist $(G, \bullet)$ ein Monoid, dann ist das neutrale Element e eindeutig bestimmt. Ist $(G, \bullet)$ eine Gruppe, dann ist für alle $a \in G$ das inverse Element a^{-1} eindeutig bestimmt.*

Beweis. Seien e, e' neutrale Elemente, d.h.
$\forall\, a \in G : a \bullet e = a = e \bullet a \wedge a \bullet e' = a = e' \bullet a$
$\Rightarrow e = e \bullet e' = e'$
Sei $a \in G$ hierzu seien b, c Inverse von a
$a \bullet b = e = b \bullet a \wedge a \bullet c = e = c \bullet a$
$\Rightarrow b = e \bullet b = (c \bullet a) \bullet b = c(\bullet a \bullet b) = c \bullet e = c$ □

Definition 1.3 *(Untergruppe, Untermonoid)*
Sei $(G, \bullet)$ eine Gruppe [bzw. Monoid] und $U \subseteq G$ Teilmenge. Dann ist U eine Untergruppe [bzw. Untermonoid] von G, falls die folgenden Eigenschaften gelten:

(i) *Das neutrale Element e ist in U enthalten.*

(ii) *U ist bezüglich der Abbildung $\bullet$ abgeschlossen, d.h. für alle $a, b \in U$ gilt $a \bullet b \in U$*

und falls $(G, \bullet)$ eine Gruppe ist auch:

(iii) *Zu jedem Element a aus U ist auch das Inverse a^{-1} in U enthalten, d.h. $a \in U \Rightarrow a^{-1} \in U$*

In beiden Fällen schreiben wir dann: $U \leq G$

Bemerkung 1.4 *Sei $(G, \bullet)$ eine Gruppe [bzw. ein Monoid] mit Untergruppe [bzw. Untermonoid] $U \leq G$, dann ist $(U, \bullet)$ selbst eine Gruppe [bzw. Monoid]* □

Beispiel 3 *Seien $\mathbb{K}$ ein Körper und n eine natürliche Zahl, dann ist die Menge*

$$SL_n(\mathbb{K}) := \{A \in \mathrm{Mat}_{\mathbb{K}}(n, n) \mid \det(A) = 1\} \subseteq GL_n(\mathbb{K})$$

Eine Untergruppe von $(GL_n(\mathbb{K}), \bullet)$

Bemerkung 1.5 *(Untergruppenkriterium)*
Sei $(G, \bullet)$ Gruppe mit Teilmenge $U \subseteq G$. Dann sind äquivalent:

(i) *U ist eine Untergruppe von G*

(ii) *Es gelten $U \neq \varnothing$ und $a \bullet b^{-1} \in U$ für alle $a, b \in U$*

Beweis. Wir schließen von (i) auf (ii), hierzu seien $a, b \in U$ beliebig. Da U nach Voraussetzung eine Gruppe ist folgt sofort, das $b^{-1} \in U$ enthalten ist und mit dem gleichen Argument folgt hieraus die Behauptung. Schließen wir nun von (ii) auf (i). Wir müssen die Punkte aus Definition 1.1 nachweisen. Sei also $a \in U$, dann folgt mit $a \cdot a^{-1} = e \in U$ die Existenz des neutralen Elements. Sei nun $a \in U$ beliebig, dann folgt mit $e \cdot a^{-1} = a^{-1} \in U$ die Existenz inverser Elemente und mit $a, b \in U$ zwei beliebigen Elementen folgt $b^{-1} \in U$ und somit ist auch $a \cdot (b^{-1})^{-1} = a \cdot b \in U$ enthalten. □

Bemerkung 1.6 *Seien $(G, \bullet)$ eine Gruppe und I eine Menge. Sei weiter zu jedem $i \in I$ eine Untergruppe $G_i \leq G$ gegeben, dann ist der Schnitt über alle G_i eine Untergruppe von G, d.h.*

$$\bigcap_{i \in I} G_i \quad \leq \quad G.$$

Beweis. Wir wollen das soeben bewiesene Untergruppenkriterium 1.5 benutzen, dazu müssen wir zwei Dinge nachweisen:
1. Der Schnitt über die G_i ist nicht leer, denn alle G_i sind Untergruppen, also ist das neutrale Element e in jedem G_i enthalten.
2. Für alle $a, b \in \bigcap G_i$ gilt: $a \bullet b^{-1} \in \bigcap G_i$, denn da a und b aus dem Schnitt sind, sind a und b in jedem der G_i enthalten. Alle diese G_i sind Gruppen, also sind auch b^{-1} und $a \bullet b^{-1}$ in allen G_i enthalten. Wenn aber $a \bullet b^{-1}$ in allen G_i enthalten ist, dann liegt $a \bullet b^{-1}$ auch im Schnitt. □

Definition 1.7 *(Von einer Menge erzeugte Untergruppe)*
Sei $(G, \bullet)$ Gruppe mit Teilmenge $M \subseteq G$. Die von M erzeugte Untergruppe $< M >$ von G ist definiert als der Schnitt über alle Untergruppen $U \leq G$, die M enthalten, d.h.

$$< M > \quad := \quad \bigcap_{\substack{U \leq G \\ M \subset U}} U$$

Also ist $< M >$ die kleinste Untergruppe von G, die M enthält.

Bemerkung 1.8 *Sei $(G, \bullet)$ eine Gruppe mit Teilmenge $M \subseteq G$, dann ist:*

$$< M > \quad = \quad \left\{ x_1^{\varepsilon_1} \bullet \ldots \bullet x_r^{\varepsilon_r} \,\middle|\, r \in \mathbb{N} \wedge \varepsilon_i \in \{-1, 1\} \wedge x_i \in M \right\} =: H$$

Beweis. Wir zeigen beide Inklusionen

$\subseteq$ z.zg.: $H \leq G$ und $M \subseteq H$
Direkt aus der Definition von H sind $M \subseteq H$ und $H \neq \emptyset$ klar. Seien $a, b \in H$, dann gibt es Elemente $x_1, \ldots, x_r, y_1, \ldots, y_s \in M$ mit $a = x_1^{\varepsilon_1} \bullet \ldots \bullet x_r^{\varepsilon_r}$ und $b = y_1^{\delta_1} \bullet \ldots \bullet y_s^{\delta_s}$
Wir sehen nun sofort, dass $a \bullet b^{-1} = x_1^{\varepsilon_1} \bullet \ldots \bullet x_r^{\varepsilon_r} \bullet y_s^{-\delta_s} \bullet \ldots \bullet y_1^{-\delta_1} \in H$ gilt.

$\supseteq$ Sei nun $U \leq G$ eine Untergruppe mit $M \subseteq U$, dann folgt aus der Abgeschlossenheit von U dass Elemente der Form $x_1^{\varepsilon_1} \bullet \ldots \bullet x_r^{\varepsilon_r}$ mit $x_i \in M$ in U enthalten sind.
Also ist $H \subseteq U$. Da U, bis auf die Eigenschaft M zu umfassen, beliebig war folgt:
$H \subseteq \bigcap_{\left(\substack{U \leq G \\ U \supseteq M}\right)} U =< M >$

□

Definition 1.9 *(Erzeignis, Zyklische Untergruppe)*
Sei $(G, \bullet)$ eine Gruppe und $m \in G$, dann heißt die von $\{m\}$ erzeugte Untergruppe $< m > \leq G$ eine zyklische Untergruppe. Sei $M = \{x_1, \ldots\, x_s\} \subseteq G$ eine Menge, dann heißt

$$< x_1, \ldots x_s > := < \{x_1, \ldots x_s\} > = < M >$$

das Erzeugnis der x_i.

Bemerkung 1.10 *Zyklische Gruppen sind abelsch.* □

Definition 1.11 *(Gruppen-Homomorphismus)*
Seien $(G, \bullet), (H, \circ)$ Gruppen, dann heißt $\varphi : G \to H$ ein Gruppenhomomorphismus, falls für alle $g_1, g_2 \in G$ die Eigenschaft $\varphi(g_1 \bullet g_2) = \varphi(g_1) \circ \varphi(g_2)$ gilt.
Die Menge aller Gruppenhomomorphismen von G nach H bezeichnen wir mit

$$\mathrm{Hom}(G, H) \;:=\; \big\{\varphi : G \to H \,\big|\, \varphi \text{ ist Gruppenhomomorphismus } \big\}$$

Bemerkung 1.12 *(Eigenschaften von Gruppenhomomorphismen)*
Seien φ, G, H wie in Definition 1.11 es gelten:

(i) $\quad \varphi(e_G) = e_H$
(ii) $\quad \forall\, g \in G \quad \varphi(g^{-1}) = (\varphi(g))^{-1}$
(iii) $\quad G' \leq G \quad \Rightarrow \quad \varphi(G') \leq H$
(iv) $\quad H' \leq H \quad \Rightarrow \quad \varphi^{-1}(H') \leq G$
(v) Sei ψ ein weiterer Homomorphismus mit $\psi : H \to L$,
so ist$\psi \circ \varphi$ ein Gruppenhomomorphismus von $G \to L$.

Beweis.

zu (i) Betrachte $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \Rightarrow \varphi(e_G) \cdot \varphi(e_G)^{-1} = e_H = \varphi(e_G)$

zu (ii) Für $g \in G$ gilt nach (i), dass $e_H = \varphi(e_G) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) \Leftrightarrow \varphi(g)^{-1} = \varphi(g^{-1})$

zu (iii) Nach (i) gilt $e \in G'$, seien also $\varphi(g), \varphi(h) \in \varphi(G')$ dann ist nach (ii) auch $\varphi(h^{-1}) = \varphi(h)^{-1} \in \varphi(G')$ enthalten. Betrachte: $\varphi(g) \cdot \varphi(h)^{-1} = \varphi(g \cdot h^{-1}) \in \varphi(G')$

zu (iv) Es ist $e \in \varphi^{-1}(\{e\})$ und somit gibt es mit $e \in \varphi^{-1}(H')$ ein neutrales Element. Seien nun $g, h \in \varphi^{-1}(H')$ also $\varphi(g), \varphi(h) \in H'$ dann folgt $\varphi(g \cdot h^{-1}) = \varphi(g) \cdot \varphi(h)^{-1} \in H'$ und somit $g \cdot h^{-1} \in \varphi^{-1}(H')$

zu (v) Betrachte für $g, h \in G$ die Hintereinanderausführung:
$\psi\big(\varphi(g \cdot h)\big) = \psi\big(\varphi(g) \cdot \varphi(h)\big) = \psi\big(\varphi(g)\big) \cdot \psi\big(\varphi(h)\big)$

□

Definition 1.13 *(Kern und Bild von Homomorphismen)*
Sei $\varphi : G \to H$ ein Gruppen-Homomorphismus, dann nennen wir
$\mathrm{Ker}(\varphi) := \{g \in G \,|\, \varphi(g) = e_H\}$ *den Kern von φ und*
$\mathrm{Im}(\varphi) := \{\varphi(g) \,|\, g \in G\}$ *das Bild von φ.*

Bemerkung 1.14 *(Weitere Eigenschaften von Gruppen-Homomorphismen)*
Sei φ wie in Definition 1.13, dann gelten:
(i) $\quad \mathrm{Ker}(\varphi) \leq G$
(ii) $\quad \mathrm{Im}(\varphi) \leq H$
(iii) $\quad \varphi\, injektiv \Leftrightarrow \mathrm{Ker}(\varphi) = \{e_G\}$
(iv) $\quad \varphi\, surjektiv \Leftrightarrow \mathrm{Im}(\varphi) = H$

Beweis.

zu (i) Die Menge $\{e_H\}$ ist eine triviale Untergruppe von H. Nach Bemerkung 1.12 ist $\varphi^{-1}(\{e\}) = \mathrm{Ker}(\varphi)$ eine Untergruppe von G.

zu (ii) Die Menge G ist eine triviale Untergruppe von G. Nach Bemerkung 1.12 ist $\varphi(G) = \mathrm{Im}(\varphi)$ eine Untergruppe von H.

(iii) Angenommen φ wäre injektiv und $\mathrm{Ker}(\varphi) \neq \{e_G\}$, dann gäbe es ein $g \in \mathrm{Ker}(\varphi)\backslash\{e_G\}$ aber damit folgte für alle $a \in G$, dass $\varphi(a \bullet g) = \varphi(a) \circ \varphi(g) = \varphi(a) \circ e_H = \varphi(a)$ aber dies widerspräche der Injektivität von φ, da $a \bullet g \neq a$ gilt.

(iv) Angenommen φ wäre surjektiv und $\mathrm{Im}(\varphi) \neq H$, dann gäbe es ein $h \in H\backslash\varphi(G)$, also ein Element im Bildbereich ohne Urbild, dies widerspräche aber der Surjektivität von φ. □

Definition 1.15 *(Mono-, Epi-, Iso-, Endo-, Automorphismus)*
Seien G, H Gruppen und $\varphi : G \to H$ ein Gruppenhomomorphismus.
Dann heißt φ...
(i) *Monomorphismus $\Leftrightarrow$ φ ist injektiv*
(ii) *Epimorphismus $\Leftrightarrow$ φ ist surjektiv*
(iii) *Isomorphismus $\Leftrightarrow$ φ ist bijektiv*
Ist $G = H$, so heißt $\varphi : G \to G$ Endomorphismus, ist φ ein injektiver Endomorphismus, so heißt φ Automorphismus. Weiter heißen G und H isomorph (Notation: $G \cong H$), wenn es einen Gruppenisomorphismus φ zwischen G und H gibt.
Die Menge der Isomorphismen von G nach H bezeichnen wir mit $\mathrm{Iso}(G, H)$, die Menge der Endomorphismen auf G mit $\mathrm{End}(G)$ und die Menge der Automorphismen auf G mit $\mathrm{Aut}(G)$.

Bemerkung 1.16 *Seien G, H Gruppen, dann gilt: $G \cong H \Leftrightarrow H \cong G$* □

Folgerung 1.17 *Isomorphie ist eine Äquivalenzrelation.* □

Definition und Bemerkung 1.18 *(Konjugation / Inneres eine Gruppe)*
Sei G eine Gruppe. Definiere für $a \in G$ die Abbildung

$$\begin{aligned} \varphi_a : G &\to G \\ g &\mapsto aga^{-1} \end{aligned}$$

Dann ist φ_a ein Automorphismus und heißt Konjugation mit a. Die Menge der Inneren Automorphismen $\mathrm{Inn}(G) := \left\{\varphi_a \in \mathrm{Aut}(G) \,\middle|\, a \in G\right\}$ ist eine Gruppe bezüglich der Hintereinanderausführung von Abbildungen.

Beweis. Wir beweisen zunächst die Injektivität von φ_a über den Kern:

$$\mathrm{Ker}(\varphi_a) = \{g \in G \,|\, aga^{-1} = e\} = \{g \in G \,|\, ag = a\} = \{g \in G \,|\, g = e\} = \{e_G\}$$

Aber φ_a ist auch surjektiv, da $\mathrm{Im}(\varphi_a) = G$ gilt.
Die Menge $\mathrm{Inn}(G)$ ist nicht leer, da die Identität id mit $\varphi_e(g) := ege^{-1} = g = id(g)$ ein innerer Automorphismus ist. Wir wollen das Untergruppenkriterium (Bemerkung 1.5) benutzen, seien also $\varphi_a, \varphi_b \in \mathrm{Inn}(G)$ und $g \in G$ dann gilt:

$$(\varphi_a \circ \varphi_b^{-1})(g) = \varphi_a(b^{-1}gb) = ab^{-1}gba^{-1} = ab^{-1}g(ab^{-1})^{-1} = \varphi_{ab^{-1}}(x)$$

und somit folgt $\varphi_{ab^{-1}}(x) \in \mathrm{Inn}(G)$ □

Bemerkung 1.19 *Sei $(G, \bullet)$ Gruppe, $b \in G$. Die folgenden Abbildungen sind bijektiv:*
(i) $inv : G \to G$, *mit* $g \mapsto g^{-1}$
(ii) $l_b : G \to G$, *mit* $g \mapsto b \bullet g$
(iii) $r_b : G \to G$, *mit* $g \mapsto g \bullet b$

Satz 1.20 *(Satz von Cayley)*
Jede endliche Gruppe kann als Untergruppe einer symmetrischen Gruppe aufgefasst werden.

Beweis. Sei $n = \sharp G$ dann ist $\sharp S_G \geq n$ mit der symmetrischen Gruppe

$$S_G := \left\{ \tau : G \to G \,\middle|\, \tau \text{ bijektiv} \right\}$$

Für $b \in G$ betrachte die Abbildung

$$\begin{array}{rcl} \sigma : G & \to & S_G \\ b & \mapsto & l_b \end{array}$$

Nach Bemerkung 1.19 ist l_b bijektiv und σ ist Gruppenhomomorphismus, denn für alle $g \in G$ gilt

$$\sigma(ab)(g) = l_{ab}(g) = abg = \sigma(a)(bg) = \big(\sigma(a) \circ \sigma(b)\big)(g)$$

Weiter ist $\mathrm{Ker}(\sigma) = e$, denn mit $a \in \mathrm{Ker}(\sigma)$ gilt $\sigma_a = id$ und somit ist: $\sigma_a(g) = ag = g \Rightarrow a = e$
Also ist $G \cong \mathrm{Im}(\sigma)$ und mit Bemerkung 1.14 gilt $\mathrm{Im}(\sigma) \leq S_G$ □

2 Nebenklassen und Normalteiler

Wir betrachten die Division mit Rest, es gilt: Für alle ganzen Zahlen m und n gibt es ganze Zahlen d und r mit

$$m \;=\; d \cdot n + r \quad \text{und} \quad 0 \leq r \leq n$$

Wir sagen dann m ist kongruent zu r modulo n und schreiben $m \equiv r \ mod \ n$. Wir können für $n \in \mathbb{N}_{\geq 2}$ Untergruppen von $\mathbb{Z}$ definieren mit

$$n\,\mathbb{Z} \;:=\; \left\{ n \cdot d \,\middle|\, d \in \mathbb{Z} \right\}$$

Wegen der Division mit Rest zerfällt $\mathbb{Z}$ in bestimmte Typen dieser Untergruppen, nämlich

$$\mathbb{Z} \;=\; \overset{\bullet}{\bigcup}_{r=0}^{n-1} (r + n\,\mathbb{Z}) \qquad \text{mit } r + n\,\mathbb{Z} \;:=\; \{ r + n \cdot d \,|\, d \in \mathbb{Z} \}$$

Dieses Prinzip wollen wir im Folgenden verallgemeinern.

Definition und Bemerkung 2.1 *(Linksnebenklassen)*
Sei G Gruppe und $H \leq G$, dann wird durch $g \sim h :\Leftrightarrow h^{-1}g \in H$ eine Äquivalenzrelation (ÄR) definiert. Die Äquivalenzklassen von der Form $gH := \{gh \,|\, h \in H\}$ heißen $Linksnebenklassen$. Die Menge der Linksnebenklassen wird mit G/H bezeichnet.
Bezeichne R ein Repräsentantensystem der Äquivalenzklassen, dann gilt

$$G = \overset{\bullet}{\bigcup_{g \in R}} gH \quad \text{und} \quad g_1H \bigcap g_2H = \begin{cases} \emptyset \\ g_1H = g_2H \end{cases}$$

Beweis. Wir müssen zunächst nachweisen, dass $\sim$ eine Äquivalenzrelation ist. Dazu betrachten wir die drei Eigenschaften:

Reflexivität ist gegeben, denn

$$g \sim g \;\Leftrightarrow\; g^{-1} \circ g = e \in H$$

Symmetrie ist gegeben, denn

$$g \sim h \;\Leftrightarrow\; h^{-1} \circ g \in H \;\Leftrightarrow\; (h^{-1} \circ g)^{-1} = g^{-1} \circ h \in H \;\Leftrightarrow\; h \sim g$$

Transitivität ist gegeben, denn

$$\begin{aligned} a \sim b \wedge b \sim c \;&\Leftrightarrow\; b^{-1} \circ a,\, c^{-1} \circ b \in H \\ &\Leftrightarrow\; (c^{-1} \circ b) \circ (b^{-1} \circ a) \,=\, c^{-1} \circ a \in H \;\Leftrightarrow\; a \sim c \end{aligned}$$

Nun müssen wir noch nachweisen, dass wir G als disjunkte Vereinigung der Äquivalenzklassen darstellen können. Dazu genügt es zu zeigen, dass der Schnitt zweier Äquivalenzklassen entweder leer ist oder beide Klassen identisch sind. Seien also g_1H und g_2H zwei Äquivalenzklassen mit nicht-leerem Schnitt. dann gibt es ein $g \in g_1H \cap g_2H$. Wegen $g \in g_1H$ gilt $g_1 \sim g$ und wegen $g \in g_2H$ folgt $g \sim g_2$. Wegen der Transitivität von $\sim$ folgt nun die Behauptung. □

Bemerkung 2.2 *Analog zu den Linksnebenklassen definiert man Rechtsnebenklassen durch $Hg := \{hg \,|\, h \in H\}$. Die Links- und Rechtsnebenklassen stehen durch $G/H \to H\backslash G$ mit $gH \mapsto Hg^{-1}$ in Bijektion.*

Bemerkung 2.3 *Sei G eine Gruppe mit Untergruppe $H \leq G$. Je zwei Linksnebenklassen [Rechtsnebenklassen] zu H sind gleichmächtig, d.h. es existiert eine Bijektion.*

Beweis. Betrachte: $g_1H \to g_2H$ mit $g_1H \mapsto g_2H := (g_2g_1^{-1})g_1H$ □

Definition 2.4 *(Gruppenindex, Gruppenordnung)*
Seien G und $H \leq G$ Gruppen. Der Index von H in G ist definiert als $(G : H) := \mathrm{Card}\left({}^{G}\!/_{H}\right)$. Insbesondere ist $(G : \{e\}) = \mathrm{Card}(G)$ die Ordnung von G.

Satz 2.5 *(Satz von Lagrange)*
Seien G und $H \leq G$ Gruppen. Dann gilt:

$$\mathrm{Card}(G) = \mathrm{Card}(H) \cdot (G : H)$$

Beweis. Aus Bemerkung 2.1 wissen wir, dass sich G als disjunkte Vereinigung der Linksnebenklassen schreiben lässt. Nach Bemerkung 2.3 haben alle Linksnebenklassen gleichviele Elemente, nämlich $\mathrm{Card}(H)$ Stück. □

Definition 2.6 *(Normalteiler)*
Seien G und $N \leq G$ Gruppen, dann heißt N Normalteiler von G (Notation: $N \trianglelefteq G$), wenn für alle $g \in G$ die Linksnebenklassen gleich den Rechtsnebenklassen (also $gN = Ng$) sind. Weiter definieren wir für zwei Untergruppen U, V von G das Produkt $U \cdot V := \{\, u \cdot v \,|\, u \in U \wedge v \in V \,\}$.

Beispiel 4 *(Normalteiler)*
(i) $A_n := \mathrm{Ker}(sgn : S_n \to \{\pm 1\})$ *Daher gilt:* $A_n \trianglelefteq S_n$
(ii) Jede Untergruppe einer abelschen Gruppe ist Normalteiler.

Bemerkung 2.7 *Seien* G *und* $U \leq G$ *Gruppen, dann sind äquivalent:*
(i) $U \trianglelefteq G$ *U ist Normalteiler von* G
(ii) $gUg^{-1} = U \quad \forall\, g \in G$
(iii) $gUg^{-1} \subseteq U \quad \forall g \in G$

Beweis. $(i) \Rightarrow (ii)$ ist klar nach Definition 2.6 und $(ii) \Rightarrow (iii)$ ist trivial.
$(iii) \Rightarrow (i)$: Für alle $g \in G$ gilt

$$\begin{array}{rcl} gUg^{-1} \subseteq U & \Leftrightarrow & gU \subseteq Ug \;\Leftrightarrow\; Ug^{-1} \subseteq g^{-1}U \;\Leftrightarrow\; Ug \subseteq gU \\ & \Rightarrow & Ug = gU \quad \forall\, g \in G \qquad \Rightarrow\; U \trianglelefteq G \end{array}$$

□

Bemerkung 2.8 *Seien* G, H *Gruppen und* $\varphi \in \mathrm{Hom}(G, H)$ *ein Homomorphismus, dann gelten:*
(i) *Für* $N \trianglelefteq H$ *ist* $\varphi^{-1}(N) \trianglelefteq G$
(ii) $\mathrm{Ker}(\varphi) \trianglelefteq G$
(iii) *Ist* φ *Epimorphismus und* $N \trianglelefteq G$ *dann ist* $\varphi(N)$ *Normalteiler von* H

Beweis. zu (i): $\varphi^{-1}(N)$ ist Untergruppe nach Bem. 1.12.
Seien $g \in G$ und $x \in \varphi^{-1}(N)$ dann ist $\varphi(x) \in N$. Es gilt:
$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in N\ (N \trianglelefteq G)$
$\Rightarrow gxg^{-1} \in \varphi^{-1}(N) \Rightarrow \varphi^{-1}(N) \trianglelefteq H$
zu (ii): (ii) ist Spezialfall von (i) mit $N := \{e\} \trianglelefteq H$
zu (iii): Sei $h \in H$ und $\varphi(n) \in \varphi(N)$. Aus der Surjektivität von φ folgt die Existenz von $g \in G$ mit der Eigenschaft $\varphi(g) = h$ und damit: $h\varphi(n)h^{-1} = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(ghg^{-1}) \in \varphi(N)$ □

Faktorgruppen

Zur Herleitung betrachten wir folgende Rechnung:
Sei $N \trianglelefteq G$ sowie $gN, hN \in {}^{G}\!/_{N}$, dann gilt: $gN \cdot hN = ghNN = ghN$, da $Nh = hN$.
Ist N nur Untergruppe und kein Normalteiler, so gilt die obige Rechnung im Allgemeinen nicht. Mit dieser Vorberlegung haben wir schon fast den folgenden Satz bewiesen.

Definition und Satz 2.9 *(Faktorgruppe, Quotient)*
Sei G *Gruppe und* $N \trianglelefteq G$*. Dann ist* ${}^{G}\!/_{N}$ *zusammen mit*
$\cdot : {}^{G}\!/_{N} \times {}^{G}\!/_{N} \to {}^{G}\!/_{N}$*, mit* $(gN, hN) \mapsto gN \cdot hN$ *eine Gruppe.*
${}^{G}\!/_{N}$ *heißt Faktorgruppe von* $G\, modulo\, N$ *oder auch Quotient.*

Beweis. Nach der vorangegangenen Rechnung müssen wir nur noch zeigen, dass ${}^{G}\!/_{N}$ eine Gruppe ist, dazu gehen wir Definition 1.1 durch.
Das neutrale Element in ${}^{G}\!/_{N}$ ist die Nebenklasse eN, denn

$$eN \cdot gN = gN = gN \cdot eN \quad \forall\, g \in G$$

Weiter gilt das Assoziativgesetz:

$$(g_1N \cdot g_2N) \cdot g_3N = g_1g_2g_3N = g_1N \cdot (g_2N \cdot g_3N)$$

und es gibt Inverse zu jeder Nebenklasse:

$$gN \cdot g^{-1}N = gg^{-1}N = eN = g^{-1}gN = g^{-1}N \cdot gN$$

□

Definition und Bemerkung 2.10 *(kanonische/natürliche Projektion)*
Seien G und $N \trianglelefteq G$ Gruppen. Dann definiert die Abbildung $\pi : G \to {}^{G}\!/_{N}$, mit $g \mapsto gN$ einen surjektiven Gruppenhomomorphismus den wir die natürliche (oder kanonische) Projektion nennen. Es gilt weiter: $Ker(\pi) = N$.

Beweis. Die Surjektivität ist unmittelbar klar, da gN alle $g \in G$ durchläuft. Daher werden alle Nebenklassen getroffen. Weiter ist π ein Homomorphismus, da $\pi(gh) = ghN = gN \cdot hN = \pi(g)\pi(h)$ gilt. Betrachte den Kern von π: $\mathrm{Ker}(\pi) = \{g \in G \,|\, gN = N\} = \{g \in G \,|\, g \in N\} = N$ □

Bemerkung 2.11 *Seien G und $N \leq G$ Gruppen. Dann sind äquivalent:*

(a) *N ist Normalteiler von G*

(b) *Es gibt eine Gruppe H und einen Gruppenhomomorphismus $\varphi \in \mathrm{Hom}(G, H)$ mit der Eigenschaft, dass $\mathrm{Ker}(\varphi) = N$ ist.*

Beweis.
(b) ⇒ (a) folgt direkt aus Bemerkung 2.8.
(a) ⇒ (b): Wähle $H := {}^{G}\!/_{N}$ und $\varphi := \pi$, so folgt die Behauptung aus Bemerkung 2.10. □

Satz 2.12 *Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Weiter sei $\pi : G \to {}^{G}\!/_{N}$ die natürliche Projektion. Die Abbildung*

$$\begin{array}{rcl} \Theta : \left\{ U \subseteq {}^{G}\!/_{N} \,\middle|\, U \trianglelefteq {}^{G}\!/_{N} \right\} & \to & \left\{ H \trianglelefteq G \,\middle|\, N \subseteq H \right\} \\ U & \mapsto & \pi^{-1}(U) \end{array}$$

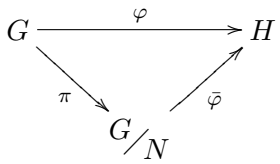
ist inklusionserhaltend und bijektiv.

Beweis. Θ ist Wohldefiniert, denn nach Bemerkung 1.12 ist $\pi^{-1}(H)$ Untergruppe von G. Weiterhin gibt es eine Umkehrabbildung mit $H \mapsto \pi(H)$, denn

$$\begin{array}{ll} 1.) & \pi^{-1}\pi(H) = H \\ \text{"}\subseteq\text{"} & x \in \pi^{-1}(\pi(H)) \Rightarrow \pi(x) = \pi(h) \quad \text{für } h \in H \\ & \Rightarrow \pi(x-h) = e \Rightarrow x - h \in \mathrm{Ker}(\pi) = N \subseteq H \Rightarrow x \in H \\ \text{"}\supseteq\text{"} & h \in H, \pi(h) \in \pi(H) \Rightarrow h \in \pi^{-1}\pi(H) \\ 2.) & \pi\pi^{-1}(U) = U \qquad U \leq G/N \\ \text{"}\subseteq\text{"} & x \in \pi\pi^{-1}(U) \Rightarrow x = \pi(y), \text{ mit } y \in \pi^{-1}(U) \Longrightarrow x = \pi(y) \in U \\ \text{"}\supseteq\text{"} & u \in U, \text{ da } \pi \text{ surjektiv } \exists\, g \in G \text{ mit } \pi(g) = u \Rightarrow g \in \pi^{-1}(U) \Rightarrow u \in \pi\pi^{-1}(U) \end{array}$$

Inklusionserhaltend: $V \subseteq U \Rightarrow \pi^{-1}(V) \subseteq \pi^{-1}(U)$ ist allgemeine Eigenschaft von Abbildungen. Beide Abbildungen bilden Normalteiler auf Normalteiler ab. □

Satz 2.13 *(Universelle Abbildungseigenschaft der Faktorgruppe)*
Seien G und $N \trianglelefteq G$ Gruppen und $\varphi \in Hom(G,H)$ ein Homomorphismus mit $N \subseteq Ker(\varphi)$ und π die natürliche Projektion, dann gibt es genau einen Gruppen-Homomorphismus $\bar{\varphi} : {}^{G}\!/_{N} \to H$ derart, dass das folgende Diagramm kommutiert, d.h. $\varphi = \bar{\varphi} \circ \pi$

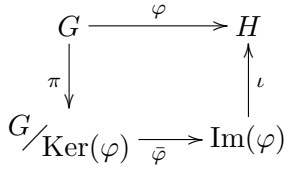


Beweis. Um die Existenz von $\bar{\varphi}$ zu zeigen geben wir es einfach an: $\bar{\varphi}(gN) := \varphi(g)$. Wir müssen nun zeigen, dass $\bar{\varphi}$ wohldefiniert ist. dazu betrachten wir:

$$\forall\, n \in N\ \forall g \in G \quad \bar{\varphi}(gN) = \varphi(gn) = \varphi(g)\,\varphi(n) = \varphi(g)$$

Die Homomorphieeigenschaft müssen wir nicht zeigen, da $\bar{\varphi}$ diese Eigenschaft durch unsere Definition direkt von φ bekommt und somit folgt unmittelbar $\varphi(g) = \bar{\varphi}(gN) = \bar{\varphi}(\pi(g))$
Die Eindeutigkeit ergibt sich mit dem gleichen Argument wie in Bemerkung 2.10 direkt aus der Surjektivität von π. □

Satz 2.14 *(Homomorphiesatz)*
Seien G, H Gruppen und $\varphi \in \mathrm{Hom}(G,H)$ ein Homomorphismus, sowie ι die Inklusionsabbildung $\mathrm{Im}(\bar{\varphi}) \subseteq H$. Dann gibt $\bar{\varphi}$ aus Satz 2.13 einen eindeutig bestimmten Gruppen-Isomorphismus $\bar{\varphi} : {}^{G}\!/_{Ker(\varphi)} \to Im(\varphi)$, mit der Eigenschaft, dass das untenstehende Diagramm kommutiert.



Beweis. Wir weisen zunächst die Bijektivität nach:
$\bar{\varphi}$ ist injektiv, denn $\bar{\varphi}(gN) = \varphi(g) = e \Rightarrow g \in \mathrm{Ker}(\varphi) = N \Rightarrow gN = N \Rightarrow \mathrm{Ker}(\bar{\varphi}) = \{eN\}$
$\bar{\varphi}$ ist direkt nach Definition surjektiv, da $\mathrm{Im}(\bar{\varphi}) = \mathrm{Im}(\varphi)$
Die Eindeutigkeit von $\bar{\varphi}$ folgt unmittelbar aus der universellen Abbildungseigenschaft der Faktorgruppe Satz 2.13. □

Bemerkung 2.15 *Es seien G eine Gruppe und $U,\ V \leq G$. Es gelten:*
(1) $(U \trianglelefteq G \vee V \trianglelefteq G) \Rightarrow U \cdot V \leq G$
(2) $(U \trianglelefteq G \wedge V \trianglelefteq G) \Rightarrow U \cdot V \trianglelefteq G$

Beweis. Seien $U, V \neq \varnothing$ und seien $u, u' \in U$ und $v, v' \in V$ dann betrachte $uv \cdot (u'v')^{-1} = u \cdot v \cdot v'^{-1} \cdot u'^{-1}$ Es gilt $v \cdot v'^{-1} \cdot u'^{-1} \cdot v' \cdot v^{-1} \in U$ Um diesen Term zu erhalten können wir die obige Gleichung mit $e = v' \cdot v^{-1} \cdot v \cdot v'^{-1}$ erweitern, d.h.

$$(u \cdot v \cdot v'^{-1} \cdot u'^{-1} = u \cdot (v \cdot v'^{-1} \cdot u'^{-1} \cdot v' \cdot v^{-1}) \cdot v \cdot v'^{-1} \in U \cdot V$$

Wir haben nun Teil (1) bewiesen für (2) betrachte $g \cdot u \cdot v \cdot g^{-1} = gug^{-1} \cdot gvg^{-1} \in U \cdot V$ mit $g \in G, u \in U$ und $v \in V$ □

Bemerkung 2.16 *Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler von G. Dann gelten:*
(i) $N \trianglelefteq U \cdot N$
(ii) $U \bigcap N \trianglelefteq U$

Beweis. zu (i): Es seien $n_1, n_2 \in N,\ u \in U$, dann ist

$$(u\,n_2)\,n_1\,(u\,n_2)^{-1} = \quad u \bullet \underbrace{n_2 \bullet n_1 \bullet n_2^{-1}}_{\in N} \bullet u^{-1} \quad \in N$$

zu (ii): Sei nun $n \in U \bigcap N,\ u \in U$. Dann ist $u\,n\,u^{-1}$ sowohl in U als auch in N enthalten, also $u\,n\,u^{-1} \in N \bigcap U$ □

Satz 2.17 *(I. Isomorphiesatz)*
Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $N \trianglelefteq G$ ein Normalteiler. Dann induzieren die Abbildungen

$$\iota : U \ni u \mapsto u \bullet e \in U \cdot N \quad \text{ und } \pi : U \cdot N \to {}^{(U \cdot N)}\!/_{N}$$

einen Gruppenisomorphismus. Insbesondere gilt

$${}^{U}\!/_{U \bigcap N} \cong {}^{(U \cdot N)}\!/_{N}$$

Beweis. Sei $\Phi := \pi \circ \iota : U \to {}^{(U \cdot N)}\!/_{N}$. Dann ist Φ surjektiv und für den Kern gilt

$$\mathrm{Ker}(\Phi) = U \bigcap N$$

mit Satz 2.14 folgt nun schon die Behauptung. □

Satz 2.18 *(II. Isomorphiesatz)*
Sei G eine Gruppe und $N \trianglelefteq G,\ H \trianglelefteq G$ mit $N \subseteq H$. Dann ist:

$$\begin{array}{ccc} {}^{G}\!/_{N}\!/_{H}\!/_{N} & \longrightarrow & {}^{G}\!/_{H} \\ gN\left({}^{H}\!/_{N}\right) & \mapsto & gH \end{array}$$

Gruppen-Isomorphismus.

Beweis. Die Abbildung

$$\begin{array}{rccc} \varphi : & {}^{G}\!/_{N} & \to & {}^{G}\!/_{H} \\ & gN & \mapsto & gH \end{array}$$

ist ein surjektiver Gruppenhomomorphismus und es gilt

$$\mathrm{Ker}(\varphi) = \{gN \in {}^{G}\!/_{N} \,|\, gN \subseteq H\} = \{gN \,|\, gN \in {}^{H}\!/_{N}\} = {}^{H}\!/_{N}$$

Mit Satz 2.14 folgt die Behauptung. □

3 Abelsche und zyklische Gruppen

Definition 3.1 *(endlich erzeugte und zyklische Gruppen)*
Sei G eine Gruppe, dann heißt G endlich erzeugt, falls es Elemente $x_1, ..., x_r \in G$ mit $r \in \mathbb{N}$ gibt, so dass das Erzeugnis der x_i bereits die gesamte Gruppe ist. Also: $< x_1, ..., x_r >= G$.
G heißt zyklisch, falls es ein x in G gibt, dass G erzeugt, also $\exists\, x \in G : \quad < x >= G$

Bemerkung 3.2 *Sei G Gruppe. Dann sind äquivalent:*
(i) G ist zyklisch
(ii) $\exists\ \varphi : \mathbb{Z} \twoheadrightarrow G$, ist surjektiver Gruppenhomomorphismus.

Beweis. Wir schließen von (i) auf (ii), d.h. nach Voraussetzung und Bemerkung 1.10 können wir G explizit angeben als $G = \{x^n \,|\, n \in \mathbb{Z}\}$ setze also $\varphi(n) := x^n$. In der anderen Richtung ist $G :=< \varphi(1) >$, denn $\varphi(n) = \varphi(1)^n$ □

Bemerkung 3.3 *Jede Untergruppe von $\mathbb{Z}$ ist von der Form $n\mathbb{Z}$, für $n \in \mathbb{N}_0$*

Beweis. Sei $U \leq \mathbb{Z}$ eine Untergruppe. Ohne Einschränkung sei $\{0\} \neq U$. Bilde $M := U \bigcap \mathbb{N}_{>0}$
Wir definieren $n := \min\{m > 0 \,|\, m \in M\}$ und behaupten: $U = n\mathbb{Z}$.
Die Relation $n\mathbb{Z} \subseteq U$ ist sofort klar, denn n ist das Minimum der $0 < m \in M$
Sei nun $m \in M$ beliebig gewählt, dann gibt die Division mit Rest die Existenz von Zahlen $a, r \in \mathbb{N}$ mit $0 \leq r < n$ und $m = a \cdot n + r$. Diese Gleichung können wir umstellen zu $r = m - a \cdot n \in U$.
Da n minimal gewählt ist, folgt unmittelbar $r = 0$. Wir schließen. dass $m = an$ ist und können U nun schreiben als: $U = \{0\} \bigcup M \bigcup \{-m \,|\, m \in M\}$. Also gilt $U \subseteq n\mathbb{Z}$
Wir haben beide Inklusionen gezeigt, also folgt $n\mathbb{Z} = U$ □

Folgerung 3.4 *Sei G zyklisch, dann gilt:*

$$\underbrace{G \cong \mathbb{Z}}_{\text{falls } \sharp G = \infty} \quad \vee \quad \underbrace{G \cong \mathbb{Z}/n\mathbb{Z}}_{\text{falls } \sharp G = k < \infty}$$

Beweis. Sei $\varphi \in \mathrm{Hom}(\mathbb{Z}, G)$ ein surjektiver Gruppenhomomorphismus. Ein solcher existiert nach Bemerkung 3.2, da G zyklisch ist. Insbesondere ist $\mathrm{Ker}(\varphi) \leq \mathbb{Z}$ eine Untergruppe. Nach der vorangegangenen Bemerkung 3.3 gibt es also ein $n \in \mathbb{N}_0$, so dass $\mathrm{Ker}(\varphi) = n\,\mathbb{Z}$ ist. Mit dem Homomorphiesatz 2.14 gilt nun

$$G \;=\; \mathrm{Im}(\varphi) \;\cong\; {}^{\mathbb{Z}}\!/_{\mathrm{Ker}(\varphi)} \;=\; {}^{\mathbb{Z}}\!/_{n\,\mathbb{Z}}$$

Ist nun $\sharp G = \infty$ so gilt $\mathrm{Ker}(\varphi) = \{0\}$ und wegen ${}^{\mathbb{Z}}\!/_{0\,\mathbb{Z}} \;=\; \mathbb{Z}$ folgt die Behauptung. □

Bemerkung 3.5 *Sei G zyklische Gruppe und $U \leq G$. Dann gelten:*
(i) U ist zyklisch
(ii) ${}^{G}\!/_{U}$ ist zyklisch

Beweis. Da G zyklisch ist, gibt es einen Gruppenepimorphismus $\varphi : \mathbb{Z} \twoheadrightarrow G$.
zu (ii): Mit der kanonischen Projektion π erhalten wir einen Gruppenepimorphismus

$$\psi : \mathbb{Z} \overset{\varphi}{\twoheadrightarrow} G \overset{\pi}{\twoheadrightarrow} {}^{G}\!/_{U}$$

somit ist G/U nach Bemerkung 3.2 zyklisch.
zu (i): Nach Bemerkung 1.12 ist $\varphi^{-1}(U)$ eine Untergruppe von $\mathbb{Z}$, daher folgt mit Bemerkung 3.3 die Isomorphie von $\varphi^{-1}(U) \cong n\mathbb{Z}$ für ein $n \in \mathbb{N}$ Betrachte nun

$$\varphi^{-1}(U) \overset{\varphi}{\twoheadrightarrow} U$$

mit dem Homomorphiesatz (2.14) folgt nun $\varphi^{-1}(U)/\mathrm{Ker}(\varphi) \cong U$ somit ist U zyklisch als Quotient der zyklischen Gruppe $\varphi^{-1}(U)$ mit $\mathrm{Ker}(\varphi)$. □

Definition 3.6 *(Elementordnung)*
Sei G eine Gruppe und $x \in G$. Dann ist die Ordnung von x definiert als:

$$\mathrm{Ord}(x) := \min\{n \in \mathbb{N}_{>0} \mid x^n = e\}$$

Existiert dieses Minimum nicht, dann definieren wir: $\mathrm{Ord}(x) := +\infty$

Bemerkung 3.7 *Sei die Gruppe $G =< x >$ zyklisch, dann gilt:*

$$\mathrm{Ord}(x) = \mathrm{Ord}(G) = \mathrm{Card}(G)$$

Beweis. Wir unterscheiden in zwei Fälle: Zunächst sei $\mathrm{Ord}(x) = \infty$ dies ist genau dann der Fall, wenn $\mathrm{Ord}(< x >) = \infty$, denn $e, x, x^2, \ldots, x^t$ sind paarweise verschieden für alle $t < \infty$. Betrachten wir nun den anderen Fall $\mathrm{Ord}(x) = n < \infty$. Die Elemente $e, x, x^2, \ldots, x^{n-1}$ sind paarweise verschieden, denn aus $x^a = x^b$ mit $n < a < b$ folgt $x^a \cdot x^{-b} = x^{a-b} = e$ Dies ist jedoch ein Widerspruch, da $a - b$ nach unserer Voraussetzung zwischen n und 0 liegt. Weiter ist $G :=< x >= \{e, x, x^2, \ldots, x^{n-1}\}$. □

Bemerkung 3.8 *Sei G eine endlich erzeugte Gruppe und $x \in G$, dann teilt die Ordnung von x die Ordnung von G, also* $\mathrm{Ord}(x) \mid \mathrm{Ord}(G)$ *d.h. es gibt ein $c \in \mathbb{N}_{>0}$, so dass* $\mathrm{Ord}(x) \cdot c = \mathrm{Ord}(G)$ *ist.*

Beweis. Der Satz von Lagrange (2.5) gibt uns die Zerlegung $\mathrm{Ord}(G) = \mathrm{Ord}(< x >) \cdot \mathrm{Ord}(G :< x >)$ □

Bemerkung 3.9 *Seien p eine Primzahl und G eine Gruppe mit p Elementen (*$\mathrm{Card}(G) = p$*). Dann ist G eine zyklische Gruppe.*

Beweis. Sei $x \in G \backslash \{e\}$ mit der soeben bewiesenen Bemerkung 3.8 folgt $\mathrm{Ord}(x) = p$. Diese Aussage ist aber äquivalent dazu, dass x die Gruppe erzeugt ($< x >= G$) also ist G zyklisch. □

Satz 3.10 *(kleiner Fermat der Gruppentheorie)*
Sei G eine endlich erzeugte Gruppe und $x \in G$ eine Gruppenelement, dann gilt: $x^{\mathrm{Ord}(G)} = e$

Beweis. Aus dem Satz von Lagrange 2.5 folgt $\mathrm{Ord}(G) = \mathrm{Ord}(x) \cdot (G :< x >)$
Betrachte also $e^{(G:<x>)} = e = x^{\mathrm{Ord}(x)} \Rightarrow e = (x^{\mathrm{Ord}(x)})^{(G:<x>)} = x^{\mathrm{Ord}(G)}$ □

Definition und Bemerkung 3.11 *(Direktes Produkt)*
Für alle $i \in I$ seien Gruppen G_i gegeben. Dann ist das kartesische Produkt: $\prod_{i \in I} G_i$ zusammen mit komponentenweiser Verknüpfung das direkte Produkt der G_i.

$$\prod_{i \in I} G_i \text{ ist Gruppe}$$

Beweis. Wir müssen die drei Gruppenkriterien aus Definition 1.1 nachweisen:

zu 1.1 (i) Die komponentenweise definierte Verknüpfung ist komponentenweise assoziativ.

zu 1.1 (ii) Es gibt ein neutrales Element $e \in \prod G_i$, denn sei für $i \in I$ das neutrale Element in G_i mit e_i bezeichnet, dann setze $e := (\ldots, e_i, \ldots)$. Für alle $g = (\ldots, g_i, \ldots) \in \prod G_i$ gilt dann:

$$\begin{aligned} e \circ g &= (\ldots, e_i \circ g_i, \ldots) = (\ldots, g_i, \ldots) \\ &= g = (\ldots, g_i, \ldots) = (\ldots, g_i \circ e_i, \ldots) = g \circ e \end{aligned}$$

zu 1.1 (iii) Zu jedem $g = (\ldots, g_i, \ldots) \in \prod G_i$ gibt es ein inverses Element, nämlich

$$g^{-1} = (\ldots, g_i^{-1}, \ldots) \in \prod G_i$$

□

Satz 3.12 *(Hauptsatz über endlich erzeugte abelsche Gruppen)*
Sei G eine endlich erzeugte, abelsche Gruppe, dann gibt es eindeutig bestimmte $r, s \in \mathbb{N}$ und $d_1, ..., d_s \in \mathbb{N}_{>0}$ mit $d_i \mid d_j$ für $i \leq j$, so dass

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$$

Beweis. Folgt in Algebra II

Anmerkung: Sind $n, m \in \mathbb{N}_{>0}$ teilerfremd, dann gilt $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}$

Beispiel 5 *Wir bestimmen alle abelschen Gruppen mit $\sharp G = 12$ mit dem Hauptsatz:*
Da G endlich ist, muss $r = 0$ gelten. Es gibt nur zwei Zerlegungen der 12, die die Bedingung $d_i \mid d_j$ für $i \leq j$ erfüllen, nämlich $12 = 12$ und $12 = 2 \cdot 6$. Also folgt mit dem Satz

$$G \cong \mathbb{Z}/12\,\mathbb{Z} \qquad \text{oder} \qquad G \cong \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/6\,\mathbb{Z}$$

Kapitel II

Ringe

4 Ringe und Ideale

Definition 4.1 *(Ringe, Unterringe, Ringhomomorphismen und Körper)*
Eine Menge R zusammen mit Abbildungen

$$+, \cdot : R \times R \to R$$

heißt Ring (mit Einselement), falls gelten

(i) $(R, +)$ *ist eine abelsche Gruppe. Das neutrale Element bezüglich $+$ nennen wir $0 := e_+$*

(ii) $(R\backslash\{0\}, \cdot)$ *ist ein Monoid. Das neutrale Element bezüglich $\cdot$ nennen wir $1 := e$.*

(iii) *(iii) Für alle $a, b, c \in R$ gilt*

- *Das links-Distributivgesetz: $a \cdot (b + c) = ab + ac$*
- *Das rechts-Distributivgesetz: $(a + b) \cdot c = ac + bc$*

Zur Vereinfachung definieren wir: $R\backslash\{0\} := R^0$. Mit dieser setzung heißt ein Ring R

- *kommutativ, falls $(R^0, \cdot)$ kommutativer Monoid ist.*
- *Schiefkörper, falls $(R^0, \cdot)$ eine Gruppe ist.*
- *Körper, falls $(R^0, \cdot)$ eine abelsche Gruppe ist.*

Eine Teilmenge $S \subseteq R$ heißt ein Unterring, falls

(i) $(S, +)$ *eine Untergruppe von $(R, +)$ ist und*

(ii) $(S^0, \cdot)$ *ein Untermonoid von $(R^0, \cdot)$ ist.*

Seien R, S Ringe. Eine Abbildung $\varphi : R \to S$ heißt Ringhomomorphismus, falls φ mit beiden Abbildungen verträglich und unitär ist, das heißt falls für alle $a, b \in R$ die folgenden Bedingungen gelten:

$$\begin{array}{lrcl} (i) & \varphi(a+b) & = & \varphi(a) + \varphi(b) \\ (ii) & \varphi(a \cdot b) & = & \varphi(a) \cdot \varphi(b) \\ (iii) & \varphi(1) & = & 1 \end{array}$$

Der Einfachheit halber behalten wir die Notationen $\mathrm{Hom}(R, S)$, $\mathrm{Iso}(R, S)$, $\mathrm{End}(R)$, usw. für die entsprechenden Mengen von Homomorphismen bei.

Bemerkung 4.2 *Seien R, S Ringe*
(a) Gilt in R, dass $e_+ = 0 = 1 = e_\bullet$, dann ist $R = \{0\}$. Wir nennen R den „0-Ring".
(b) Sei $\varphi \in \mathrm{Iso}(R, S)$, dann ist $\varphi^{-1} \in \mathrm{Iso}(S, R)$

Beweis. Zu (a) Für alle $r \in R$ gilt $r = r \cdot 1 = r \cdot 0 = r \cdot (1 - 1) = r - r = 0$
Zu (b) Für alle $s, t \in S$ gilt $\varphi\Big(\varphi^{-1}(t) \cdot \varphi^{-1}(s)\Big) = \varphi\Big(\varphi^{-1}(t)\Big) \cdot \varphi\Big(\varphi^{-1}(s)\Big) = t \cdot s$
Es folgt $\varphi^{-1}(t) \cdot \varphi^{-1}(s) = \varphi^{-1}(t \cdot s)$ □

Beispiel 6 *Die Mengen $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathrm{Mat}_{\mathbb{K}}(n, n)$ (Ring der $n \times n$-Matritzen über dem Körper $\mathbb{K}$), $\mathrm{End}_{\mathbb{K}}(V)$ (Endomorphismenring über dem $\mathbb{K}$-Vektorraum V) sowie $R[X]$ (Polynomring über dem Ring R) sind Ringe.*

Anmerkung Sei R ein Ring. Ein Polynom $\sum a_n X^n \in R[X]$ ist ein formaler Ausdruck, also nichts weiter, als die Koeffizientenfolge $(a_0, a_1, \ldots, a_n)$. Wir wollen in Zukunft $R[X]$ genauer untersuchen, daher ein ausführlicheres

Beispiel 7 *Sei R ein kommutativer Ring und $m \in \mathbb{N}_{>0}$, dann ist $R[X_1, \ldots, X_m]$ der Polynomring in m Variablen, also:*

$$R[X_1, \ldots, X_m] = \left\{ \sum_{(n_1, \ldots, n_m) \in \mathbb{N} \times \ldots \times \mathbb{N}} a_{(n_1, \ldots, n_m)} \cdot X_1^{n_1} \cdot \ldots \cdot X_m^{n_m} \;\middle|\; \text{fast alle } a_{(n_1, \ldots, n_m)} = 0 \right\}$$

Hierbei heißt „fast alle": Alle bis auf endlich viele Ausnahmen.

Anmerkung Der Polynomring in m Variablen lässt sich als Polynomring in einer Variable über dem Ring $R[X_1, \ldots, X_{m-1}]$ auffassen, also $R[X_1, \ldots, X_m] = R[X_1, \ldots, X_{m-1}][X_m]$

Ab hier betrachten wir nur noch kommutative Ringe mit Einselement

Seien R, S Ringe und $\varphi \in \mathrm{Hom}(R, S)$ ein Ringhomomorphismus. Wir können sofort zwei besondere Eigenschaften von $\mathrm{Ker}(\varphi) = \{\, r \in R \mid \varphi(r) = 0 \,\}$ feststellen:

(i) Da φ unter anderem auch ein Gruppenhmomorphismus ist, wissen wir aus dem Kapitel über Gruppen, dass $(\mathrm{Ker}(\varphi), +)$ eine (ablesche) Untergruppe von $(R, +)$ ist.

(ii) Ist $r \in \mathrm{Ker}(\varphi)$ und $x \in R$, dann gilt

$$\varphi(xr) = \varphi(x) \cdot \varphi(r) = \varphi(x) \cdot 0 = 0$$

Daher ist $x \cdot r \in \mathrm{Ker}(\varphi)$

Diese Eigenschaften des Kerns von Ringhomomorphismen wollen wir im Begriff des Ideals verallgemeinern. Dazu die nächste

Definition 4.3 *(Ideale)*
Eine Teilmenge $\mathfrak{a} \subseteq R$ heißt Ideal, (wir schreiben dann $\mathfrak{a} \trianglelefteq R$,) falls
(i) $\mathfrak{a}$ ist Untergruppe bzgl. der Addition: $(\mathfrak{a}, +) \leq (R, +)$
(ii) $\mathfrak{a}$ ist multiplikativ Abgeschlossen: $\forall\, a \in \mathfrak{a}\ \forall\, x \in R:\ x \cdot a \in \mathfrak{a}$

Beispiel 8 *Alle Ideale in $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$ für $n \in \mathbb{N}$*

Bemerkung 4.4 *Sei R ein Ring und $\mathfrak{a} \subseteq R$, dann sind äquivalent:*
(i) $\mathfrak{a}$ *ist ein Ideal von R und (ii)* $\forall\, a, b \in \mathfrak{a}\ \forall\, x \in R:\ a + b \in \mathfrak{a} \wedge x \cdot a \in \mathfrak{a}$

Beweis. $(i) \Rightarrow (ii)$ ist klar nach Definition 4.3
$(ii) \Rightarrow (i)$ Seien $a, b \in \mathfrak{a} \Rightarrow (-1) \cdot b \in \mathfrak{a} \Rightarrow a - b \in \mathfrak{a} \Rightarrow (\mathfrak{a}, +) \leq (R, +)$ □

Bemerkung 4.5 *Seien R, S Ringe und $\varphi \in \mathrm{Hom}(R, S)$. Dann gelten:*
(a) Ist $\mathfrak{b} \trianglelefteq S$ ein Ideal, dann ist auch $\varphi^{-1}(\mathfrak{b}) \trianglelefteq R$ ein Ideal.
(b) Ist φ surjektiv und $\mathfrak{a} \trianglelefteq R$ ein Ideal, dann ist auch $\varphi(\mathfrak{a}) \trianglelefteq S$ ein Ideal
(c) $\mathrm{Im}(\varphi) \subseteq S$ *ist Unterring*
(d) $\mathrm{Ker}(\varphi) \trianglelefteq R$ *ist ein Ideal*

Beweis. zu a)
Wir haben in Bemerkung 1.12 die Untergruppeneigenschaft $(\varphi^{-1}(\mathfrak{b}), +) \leq (R, +)$ nachgewiesen. Sei $r \in \varphi^{-1}(\mathfrak{b})$ und $x \in R$, also $\varphi(r) \in \mathfrak{b}$, dann gilt $\varphi(xr) = \varphi(x) \cdot \varphi(r) \in \mathfrak{b}$. Daher ist $xr \in \varphi^{-1}(\mathfrak{b})$
zu b)
Auch hier ist mit Bemerkung 1.12 sofort klar, dass $\varphi(\mathfrak{a})$ eine Untergruppe ist. Sei $\varphi(a) \in \varphi(\mathfrak{a})$ und $x \in S$. Da φ surjektiv ist, existiert ein $y \in R$ mit $\varphi(y) = x$ also

$$x \cdot \varphi(a) = \varphi(y) \cdot \varphi(a) = \varphi(ya) \in \varphi(\mathfrak{a})$$

zu c)
Die Untergruppeneigenschaft von $\mathrm{Im}(\varphi)$ in S haben wir bereits in Bemerkung 1.12 gezeigt. Seien $\varphi(q), \varphi(r) \in \varphi(R) = \mathrm{Im}(\varphi)$, Dann ist auch $\varphi(q) \cdot \varphi(r) = \varphi(q \cdot r) \in \mathrm{Im}(\varphi)$
d) ist klar. □

Wir erinnern uns an Faktorgruppen: Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler, dann ist ${}^{G}\!/_{N}$ eine Gruppe. Wir wollen diese Konstruktion nun auf Ringe übertragen: Sei also R ein Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal. Wir wissen, dass $(\mathfrak{a}, +)$ Normalteiler von $(R, +)$ ist und können daher die Faktorgruppe ${}^{(R,+)}\!/_{(\mathfrak{a},+)}$ bilden (Vergleiche Satz 2.9).
Damit ${}^{R}\!/_{\mathfrak{a}}$ auch ein Ring wird führen wir zusätzlich eine Multiplikation ein:

$$\begin{array}{rccc} \cdot: & {}^{R}\!/_{\mathfrak{a}} \times {}^{R}\!/_{\mathfrak{a}} & \to & {}^{R}\!/_{\mathfrak{a}} \\ & (x + \mathfrak{a}, y + \mathfrak{a}) & \mapsto & (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = xy + \mathfrak{a} \end{array}$$

Die Wohldefiniertheit ist hierbei nicht trivial:

$$\begin{array}{rcl} x + \mathfrak{a} = x' + \mathfrak{a} & \wedge & y + \mathfrak{a} = y' + \mathfrak{a} \\ (x' + \mathfrak{a}) \cdot (y' + \mathfrak{a}) & = & x'y' + \mathfrak{a} \\ & = & (x - (x - x') + \mathfrak{a}) \cdot (Y - (y - y') + \mathfrak{a} \\ & = & (x - (x - x')) \cdot (y - (y - y')) + \mathfrak{a} \\ & = & xy - x\underbrace{(y - y')}_{\in \mathfrak{a}} - y\underbrace{(x - x')}_{\in \mathfrak{a}} + \underbrace{(x - x')(y - y')}_{\in \mathfrak{a}} + \mathfrak{a} \\ & = & xy + \mathfrak{a} = (x + \mathfrak{a}) \cdot (y + \mathfrak{a}) \end{array}$$

Die Assoziativität und Distributivität erbt ${}^{R}\!/_{\mathfrak{a}}$ von R. ${}^{R}\!/_{\mathfrak{a}}$ ist also ein Ring bzgl. $\cdot$ und +. Damit haben wir die Wohldefiniertheit der folgenden Definition bereits gezeigt.

Definition und Bemerkung 4.6 *(Quotienten-, Faktorring, natürliche Projektion)*
Ist R ein Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal, dann ist ${}^{R}\!/_{\mathfrak{a}}$ ein Ring und heißt Faktor- oder Quotientenring. Die natürliche Projektion $\pi : R \to {}^{R}\!/_{\mathfrak{a}}$ ist surjektiver Ringhomomorphismus mit $\mathrm{Ker}(\pi) = \mathfrak{a}$. (Vergleiche Bemerkung 2.10)

Satz 4.7 *Seien die Bezeichnungen wie in der vorangegangenen Bemerkung 4.6, dann ist*

$$\begin{array}{rcl} \{\mathfrak{b} \mid \mathfrak{b} \trianglelefteq {}^{R}\!/_{\mathfrak{a}}\} & \to & \{\mathfrak{c} \mid \mathfrak{a} \subseteq \mathfrak{c}\} \\ \mathfrak{b} & \mapsto & \pi^{-1}(\mathfrak{b}) \end{array}$$

eine Bijektion mit der Umkehrabbildung $R \supseteq \mathfrak{c} \mapsto \pi(\mathfrak{c}) \in {}^{R}\!/_{\mathfrak{a}}$

Beweis. Nach Bemerkung 4.5 sind $\pi^{-1}(\mathfrak{b})\}$ und $\pi(\mathfrak{c})$ Ideale. Es bleibt $\pi \circ \pi^{-1} = id$ zu zeigen. Dieser Beweis verläuft analog zum Beweis aus Satz 2.12. □

Satz 4.8 *(Homomorphiesatz)*
Seien R, S Ringe und $\varphi \in Hom(R, S)$, dann gibt es einen eindeutig bestimmten Ring-Isomorphismus:

$$\bar{\varphi} : {}^{R}\!/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi)$$

mit der Eigenschaft, dass das untenstehende Diagramm kommutiert.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ {}^{R}\!/_{\mathrm{Ker}(\varphi)} & \xrightarrow[\bar{\varphi}]{} & \mathrm{Im}(\varphi) \end{array}$$

Hierbei bezeichnen π die natürliche Projektion und ι die natürliche Inklusion.

Beweis. Der Beweis erfolgt analog zum Homomorphiesatz für Gruppen (2.14). Es genügt zusätzlich zu prüfen, ob $\bar{\varphi}$ Ring-Homomorphismus ist. Da wir auch schon wissen, das $\bar{\varphi}$ ein Gruppenhomomorphismus ist genügen

$$\bar{\varphi}((x + \mathfrak{a})(y + \mathfrak{a})) = \bar{\varphi}(xy + \mathfrak{a}) = \varphi(xy) = \varphi(x)\,\varphi(y) = \bar{\varphi}(x + \mathfrak{a})\,\bar{\varphi}(y + \mathfrak{a})$$

$$\text{und} \qquad \bar{\varphi}(1 + \mathfrak{a}) = \varphi(1) = 1$$

□

5 Primideale und Maximalideale

Wir betrachten die (bis auf Einheiten) eindeutige Primfaktorzerlegung in $\mathbb{Z}$. Für $z \in \mathbb{Z}$ gilt

$$z \;=\; \varepsilon \cdot p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$$

Mit paarweise verschiedenen Primzahlen p_i und $\varepsilon \in \mathbb{Z}^\times$. Wir können folgern, dass für ein $n \in \mathbb{N}_{\geq 2}$ gilt: n ist genau dann eine Primzahl, wenn für alle Produkte $ab \in \mathbb{Z}$ gilt:
Wenn n teilt ab [Notation: $n|ab$] so folgt n teilt bereits eine der Zahlen a oder b, also $n|a \vee n|b$.
Wir wollen diese Eigenschaft im Begriff des Primideals verallgemeinern

Definition 5.1 *(Einheiten, Nullteiler, maximale-, Haupt- und Primideale)*
Seien R ein Ring und $x \in R$, dann heißt x

... eine Einheit, falls es ein $y \in R$ gibt, so dass $x \cdot y = 1_R$ ist.
Die Menge $R^\times := \{x \in R \,|\, \exists\, y \in R \; x \cdot y = 1\}$ der Einheiten in R heißt Einheitengruppe von R und bildet eine multiplikative Gruppe.

... ein Nullteiler, falls es ein $y \in R\backslash\{0\}$ gibt, so dass $x \cdot y = 0$ ist.
R heißt Nullteilerfrei oder Integritätsbereich, falls R nicht der Nullring ist und $R\backslash\{0\}$ keine Nullteiler enthält.

Sei nun $\mathfrak{a} \lhd R$ ein Ideal mit $\mathfrak{a} \neq R$. $\mathfrak{a}$ heißt genau dann

... Primideal, wenn daraus, dass das Produkt zweier Elemente aus R in $\mathfrak{a}$ liegt folgt, das bereits eines der Elemente in $\mathfrak{a}$ ist, also $a \cdot b \in \mathfrak{a} \;\Rightarrow\; a \in \mathfrak{a} \;\vee\; b \in \mathfrak{a}$.
Die Menge aller Primideale in R bezeichnen wir als das Spektrum von R und schreiben $\mathfrak{a} \in \mathrm{Spec}(R)$

... Maximalideal, wenn für alle Ideale $\mathfrak{b} \trianglelefteq R$ die $\mathfrak{a}$ enthalten ($\mathfrak{a} \subseteq \mathfrak{b}$) gilt: $\mathfrak{a} = \mathfrak{b}$ oder $\mathfrak{b} = R$
Die Menge aller Maximalideale in R bezeichnen wir als das maximale Spektrum von R und schreiben $\mathfrak{a} \in \mathrm{Max}(R)$

Für ein Element $x \in R$ heißt $(x) := \{rx \,|\, r \in R\} = xR$ das Hauptideal von x.

Anmerkung Mit dieser Definition gilt: $n \in \mathbb{Z}$ ist genau dann eine Primzahl wenn $(n) := n\mathbb{Z}$ ein Primideal in $\mathbb{Z}$ ist.

Beispiel 9 *(Nullteiler / Einheiten)*
Die Ringe $\mathbb{Z}$ und $\mathbb{Q}$ sind Nullteiler frei. Der Ring $\mathbb{Z}\!\diagup_{4\,\mathbb{Z}}$ hingegen nicht, denn

$$2 \cdot 2 \;=\; 4 \equiv 0\,(mod)\,4 \quad \text{und} \quad \bar{2} \neq \bar{0}$$

Der Ring $\mathbb{Z}$ hat die Einheiten 1 und -1 und es gilt $\mathbb{Z}^\times \;=\; \{+1, -1\}$. In $\mathbb{Q}$ sind alle Elemnte ausser der 0 Einheiten, dass heißt $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Bemerkung 5.2 *(Eigenschaften von Idealen)*
Seien $S \neq \{0\} \neq R$ Ringe, $x, y \in R$ und $\mathfrak{a} \trianglelefteq R$. Es gelten:

(a) $(x) = R \Leftrightarrow x \in R^\times$
(b) R *sei ein Integritätsring, dann gilt:* $(x) = (y) \Leftrightarrow \exists \varepsilon \in R^\times \; x = \varepsilon \cdot y$
(c) es sind äquivalent:
- *(i)* R *ist ein Körper*
- *(ii)* $R^\times = R \backslash \{0\}$
- *(iii)* $(0), R$ *sind die einzigen Ideale in* R
- *(iv) Für alle* $\varphi \in \mathrm{Hom}(R, S)$ *gilt:* φ *ist injektiv.*

(d) $\mathfrak{a}$ *ist Primideal* $\Leftrightarrow {}^{R}\!/_{\mathfrak{a}}$ *ist ein Integritätsring*
(e) $\mathfrak{a}$ *ist Maximalideal* $\Leftrightarrow {}^{R}\!/_{\mathfrak{a}}$ *ist Körper*
(f) Maximalideale sind Primideale

Beweis.

zu (a) Sei $(x) = R$, dann ist $1_R \in (x)$ und somit gibt es ein $y \in R$ mit der Eigenschaft $x \cdot y = 1_R$. Sei $x \in R^\times$, dann gibt es ein $y \in R$ mit der Eigenschaft, dass $1_R = x \cdot y$, also ist $1_R \in (x)$.

zu (b) Seien $x, y \in R$. Wir beweisen zunächst die $\Leftarrow$ Richtung: Also gibt es ein $\varepsilon \in R^\times$, so dass $x = \varepsilon \cdot y$ Dann ist aber $x \in (y)$ also $(x) \subseteq (y)$. Da ε eine Einheit ist, gibt es ein Inverses ε^{-1}, so dass $x \cdot \varepsilon^{-1} = x$. Dann ist aber $y \in (x)$ also $(y) \subseteq (x)$.
Zur $\Rightarrow$ Richtung: Da $(x) = (y)$ gilt ist $x \in (y)$ also gibt es ein $a \in R$, so dass $x = a \cdot y$ gilt. Weiter ist $y \in (x)$ also gibt es ein $b \in R$, so dass $y = b \cdot x$ gilt. Es gilt also: $x = a \cdot y = a \cdot b \cdot x$ Nach Umformen erhalten wir $0 = x(1 - ab)$. Das heißt aber, dass $x = 0$ oder $ab = 1$ gelten muss. Im ersten Fall ist auch $y = 0$, da wir $(x) = (y)$ Vorausgesetzt haben wähle also $\varepsilon = 1 \in R^\times$. Im zweiten Fall ist $a \in R^\times$ die gesuchte Einheit.

zu (c) Die Äquivalenz zwischen **(i) und (ii)** ist trivial. Für den Schluss **von (i) auf (iii)** sei $(0) \neq \mathfrak{a} \triangleleft R$ ein Ideal und $x \in \mathfrak{a}$ ein Element, dann folgt $x^{-1} \cdot x \in \mathfrak{a}$ also ist $1_R \in \mathfrak{a} = R$. Für den Schluss **von (iii) auf (iv)** betrachte $\mathrm{Ker}(\varphi)$. Nach Bemerkung 4.5 ist der Kern ein Ideal also gilt $\mathrm{Ker}(\varphi) = (0)$ oder $\mathrm{Ker}(\varphi) = R$. Der zweite Fall ist aber ausgeschlossen, da $\varphi(1) = 1 \neq 0$ gilt. Wir schließen zum Schluss noch **von (iv) auf (ii)** dazu sei x keine Einheit, also $x \in R \backslash R^\times$, dann ist $(x) \neq R$. Betrachte nun die natürliche Projektion $\pi : R \to {}^{R}\!/_{(x)} =: S$. Diese ist, da S nicht der Nullring ist, nach Voraussetzung injektiv also gilt $\mathrm{Ker}(\pi) = (x) = 0$. Also gilt $R^\times = R \backslash \{0\}$.

zu (d) Sei $\mathfrak{a} \triangleleft R$ ein Ideal mit $\mathfrak{a} \neq R$. Für die $\Rightarrow$-Richtung sei $(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = \mathfrak{a}$, dann ist $xy \in \mathfrak{a}$ und somit ist $x \in \mathfrak{a}$ oder $y \in \mathfrak{a}$, da $\mathfrak{a}$ ein Primideal ist. Also ist ${}^{R}\!/_{\mathfrak{a}}$ Nullteilerfrei.
Für die $\Leftarrow$-Richtung sei nun $xy \in \mathfrak{a}$ Betrachte: $(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = (xy + \mathfrak{a}) = \mathfrak{a}$ Also ist bereits $x + \mathfrak{a} = \mathfrak{a}$ oder $y + \mathfrak{a} = \mathfrak{a}$ und somit $x \in \mathfrak{a}$ oder $y \in \mathfrak{a}$.

zu (e) Sei $\mathfrak{a} \triangleleft R$ ein von R echt verschiedenes Ideal. Auch hier sind wieder zwei Richtungen zu Zeigen, wir beginnen mit der $\Rightarrow$-Richtung: Da $\mathfrak{a}$ nach Vorraussetzung Maximal ist kann ${}^{R}\!/_{\mathfrak{a}}$ nur die Ideale R und (0) enthalten, somit folgt aus (c) die Behauptung.
In der Gegenrichtung ist ${}^{R}\!/_{\mathfrak{a}}$ ein Körper nach Voraussetzung, enthält somit nur die Ideale R und (0) es folgt sofort die Behauptung.

zu (f) Körper sind Integritätsbereiche, somit folgt die Behauptung aus den Teilen (d) und (e). □

Folgerung 5.3 *Sei $n \in \mathbb{N}_{>1}$, dann sind äquivalent:*
(i) n *ist Primzahl*
(ii) $(n) \trianglelefteq \mathbb{Z}$ *ist ein Primideal*
(iii) $\mathbb{Z}/n\mathbb{Z}$ *ist nullteilerfrei*
(iv) $(n) \trianglelefteq \mathbb{Z}$ *ist ein Maximalideal*
(v) $\mathbb{Z}/n\mathbb{Z}$ *ist ein Körper (Notation:* $\mathbb{F}_n$*)*

Beweis. Die Äquivalenzen von (ii) und (iii) und von (iv) und (v) haben wir in Bemerkung 5.2 gesehen. Für den Schluss von (i) auf (ii) sei $ab \in (n)$. Also gibt es ein $c \in \mathbb{Z}$ so dass $n \cdot c = ab$ gilt, das heißt aber nichts anderes als $n|ab$. Da n eine Primzahl ist gilt nun entweder $n|a$ oder $n|b$. Wie oben können wir schließen, dass dann $a \in (n)$ oder $b \in (n)$ gelten muss. In der Gegenrichtung folgt aus $ab \in (n)$ sofort, dass $a \in (n)$ oder $b \in (n)$ also $n|a$ oder $n|b$.
Wir schließen nun von (iii) auf (v), dazu sei $\bar{x} = x + n\,\mathbb{Z} \in \mathbb{Z}/n\,\mathbb{Z}\backslash\{0\}$. Wegen der Division mit Rest gibt es ein $y \in \mathbb{Z}$, so dass

$$x \cdot y \;\equiv\; 1 \;\; (mod)\, n$$

gilt. Dann ist aber $\bar{y} = y + n\,\mathbb{Z}$ das Inverse von $\bar{x} = x + n\,\mathbb{Z}$. Da $\bar{x}$ beliebig war folgt, dass jedes Element ausser der Null eine Einheit ist. Nach Bemerkung 5.2 ist $\mathbb{Z}/n\,\mathbb{Z}$ also ein Körper.
Der letzte Schluss von (iv) auf (ii) ist trivial, da Maximalideale immer Primideale sind. □

Folgerung 5.4 *Primideale von* $\mathbb{Z} = \{(p) \trianglelefteq \mathbb{Z} \,|\, p\,prim \vee p = 0\,\}$
Maximalideale von $\mathbb{Z} = \{(p) \trianglelefteq \mathbb{Z} \,|\, p\,prim\}$ □

Satz 5.5 *Sei R ein Ring, dann besitzt R ein Maximalideal.*

Beweis. Sei $\mathfrak{M} := \{\, \mathfrak{a} \trianglelefteq R \,|\, \mathfrak{a} \neq R\,\}$, dann ist $\mathfrak{M}$ halb-geordnet bzgl. „$\subseteq$".
D.h. $\mathfrak{a} \subseteq \mathfrak{a}$, und falls $\mathfrak{a} \subseteq \mathfrak{b} \wedge \mathfrak{b} \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b}$

Behauptung 1 *Jede totalgeordnete Teilmenge $\{\mathfrak{a}_i \,|\, i \in I\} \subseteq \mathfrak{M}$ besitzt eine obere Schranke.*
In Formeln $\forall\, i, j \in I \;\; \mathfrak{a}_i \subseteq \mathfrak{a}_j \;\vee\; \mathfrak{a}_j \subseteq \mathfrak{a}_i$ $^{(*)}$.
Die obere Schranke ist: $\mathfrak{a} := \bigcup_{i \in I} \mathfrak{a}_i$ *mit* $\forall\, i \in I \;\; \mathfrak{a}_i \subseteq \mathfrak{a},\;\; \mathfrak{a} \subseteq \mathfrak{M}$

Beweis. $\mathfrak{a} \neq R$, da $1 \notin \mathfrak{a}_i\, \forall\, i \in I$. Es genügt also zu zeigen, dass $\mathfrak{a} \lhd R$ ein Ideal ist.
Sei $a \in \mathfrak{a}$ und $r \in R \;\Rightarrow \exists\, i \in I \; a \in \mathfrak{a}_i \Rightarrow \; r \cdot a \in \mathfrak{a}_i \subseteq \mathfrak{a}$ Seien nun $a, b \in \mathfrak{a} \Rightarrow \exists\, i, j \in I \; a \in \mathfrak{a}_i \;\wedge\; b \in \mathfrak{a}_j$
$\overset{(*)}{\Longrightarrow} a, b \in \mathfrak{a}_i \;\vee\; a, b \in \mathfrak{a}_j \Longrightarrow \; a + b \in \mathfrak{a}_i \subseteq \mathfrak{a} \;\vee\; a + b \in \mathfrak{a}_j \subseteq \mathfrak{a}$ △

Nun können wir *Zorns Lemma* anwenden: $\mathfrak{M}$ besitzt maximale Elemente, also Maximalideale. □

Folgerung 5.6 *In jedem Ring R gelten:*
1) Jedes Ideal $\mathfrak{a} \lhd R$ ist in einem Maximalideal $\mathfrak{m} \lhd R$ enthalten.
2) Jede nicht Einheit $x \in R\backslash R^{\times}$ ist in einem Maximalideal $\mathfrak{m} \lhd R$ enthalten.

Beweis. zu 1)
Betrachte die natürliche Projektion $\pi : R \to R/\mathfrak{a}$. Sei nun $\bar{\mathfrak{m}} \lhd R/\mathfrak{a}$ ein Maximalideal nach Satz 5.5. Dann ist $\pi^{-1}(\bar{\mathfrak{m}}) \lhd R$ ein Maximalideal, dass $\mathfrak{a}$ enthält.
(2) folgt aus (1) mit $\mathfrak{a} = (x)$ □

Bemerkung 5.7 *Es seien R ein Ring, $\mathfrak{p} \lhd R$ ein Primideal und $S := R\backslash\mathfrak{p}$, dann ist S eine multiplikativ abgeschlossene Teilmenge von R. D.h.* $1 \in S \;\wedge\; s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S$

Beweis. da $\mathfrak{p}$ ein echt von R verschiedenes Ideal ist, ist $1_R \notin \mathfrak{p}$ also ist $1_R \in S$
Sind $s_1, s_2 \in S$ dann sind diese nicht in $\mathfrak{p}$ enthalten. Da $\mathfrak{p}$ ein Primideal ist, gilt $s_1 \cdot s_2 \notin \mathfrak{p}$ ist also ein Element in S. □

Definition und Satz 5.8 *(Lokalisierung von R bei $\mathfrak{p}$)*
Es seien R ein Ring, $\mathfrak{p} \lhd R$ ein Primideal und $S := R \backslash \mathfrak{p}$. Dann gelten:

(a) Auf $R \times S$ wird durch $(r, s) \sim (r', s') :\Leftrightarrow \exists t \in S\ t \cdot (rs' - r's) = 0$
eine Äquivalenzrelation definiert. Wir bezeichnen die Äquivalenzklassen bzgl. „$\sim$" mit $\frac{r}{s}$.
(Ist R zusätzlich Integritätsbereich und $0 \neq S$ dann gilt: $(r, s) \sim (r', s') \Leftrightarrow rs' - r's = 0$)
(b) Die Menge der Äquivalenzklassen „$S^{-1}R$" wird zu einem Ring mittels
$\frac{r}{s} + \frac{r'}{s'} := \frac{rs'+r's}{ss'}$ und $\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$
Für $S^{-1}R$ schreiben wir auch $R_\mathfrak{p}$ und nennen dies die Lokalisierung von R bei $\mathfrak{p}$.

Beweis. Sowohl das $\sim$ eine Äquivalenzrelation ist (a) also auch, dass „$S^{-1}R$" ein Ring ist (b), wird durch einfaches Nachrechnen gezeigt. □

Folgerung 5.9 *Sei R ein Integritätsbereich und $S := R\backslash\{0\}$. Dann ist S nach Bemerkung 5.7 multiplikativ abgeschlossen und es gilt: $S^{-1}(R) = \mathrm{Quot}(R) = Q(R) = \mathrm{Frac}(R)$ ist der Quotientenkörper von R*

Beweis. Jedes $\frac{r}{s}$ mit $r \neq 0$ hat multiplikatives Inverses: $\frac{s}{r}$. □

Beispiel 10 *(Quotientenkörper)*
- Der Quotientenkörper von $\mathbb{Z}$ ist $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$
- Der Quotientenkörper von $\mathbb{Q}$ ist $\mathrm{Quot}(\mathbb{Q}) = \mathbb{Q}$, denn $\mathbb{Q}$ ist bereits ein Körper.

Bemerkung 5.10 *R sei ein Integritätsbereich und $S \subsetneq R$ multiplikativ abgeschlossen mit $0 \neq S$, dann ist $\varphi \in \mathrm{Hom}(R, S^{-1}R)$ mit $\varphi(r) \mapsto \frac{r}{1}$ injektiv.*

Beweis. Die Homomorphieigenschaft rechnet mensch leicht nach.
Zur injektivität: $\mathrm{Ker}(\varphi) = \{\, r \in R \,|\, \frac{r}{1} = 0\} = \{\, r \in R \,|\, \exists t \in S :\ tr = 0\} = \{\, r \in R \,|\, r = 0\}$ □

6 Euklidische Ringe

Definition 6.1 *(euklidischer Ring)*
Sei R Integritätsring. Wenn es eine Abbildung $\gamma : R \to \mathbb{N}$ gibt, so dass es für alle $a, b \in R$ mit $b \neq 0$ Elemente $c, d \in R$ gibt, mit der Eigenschaft $a = c \cdot b + r$ mit $\gamma(r) < \gamma(b) \vee r = 0$
dann heißt R euklidischer Ring.

Beispiel 11 *Sei K ein Körper, dann ist der Polynomring $K[X]$ über K ein euklidischer Ring. Beliebige Körper und der Ring der ganzen Zahlen $\mathbb{Z}$ sind euklidische Ringe.*

Beispiel 12 *(Der Ring der Gaussschen Zahlen $\mathbb{Z}[i]$ ist euklidisch)*
$\mathbb{Z}[i] := \{ x + iy \,|\, x, y \in \mathbb{Z} \wedge i^2 = -1 \}$ *ist euklidischer Ring mit*

$$\begin{array}{rccc} \gamma: & \mathbb{Z}[i] & \to & \mathbb{N} \\ & x+iy & \mapsto & x^2+y^2 = |x+iy|^2 \end{array}$$

Seien $a+ib, c+id \in \mathbb{Z}[i]$ und $c+id \neq 0$. Suche hierzu $x+iy, r+is \in \mathbb{Z}[i]$ mit

$$a+ib = (c+id)(x+iy) + (r+is) \text{ und } \gamma(r+is) < \gamma(c+id) \wedge r+is = 0_{\mathbb{C}}$$

$\frac{a+ib}{c+id} \in \mathbb{C}$. *Es gibt $x+iy \in \mathbb{Z}[i]$ mit* $\gamma(\frac{a+ib}{c+id} - (x+iy)) < \left(\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{2} < 1$
***Bemerkung**: γ ist multiplikativ.*
$a+ib = (c+id)(x+iy) + (r+is)$
$\Rightarrow \gamma(r+is) = \gamma\Big((a+ib) - (c+id)(x+iy)\Big)$
$= \gamma(c+id) \cdot \gamma\left(\frac{a+bi}{c+di} - (x+iy)\right) < \gamma(c+id)$

Definition 6.2 *(Hauptidealring)*
Sei R ein Integritätsring, dann heißt R Hauptidealring (HIR, pid), wenn es für alle Ideale $\mathfrak{a} \trianglelefteq R$ ein $a \in R$ gibt, dass $\mathfrak{a}$ erzeugt, also $\mathfrak{a} = (a) = aR$

Satz 6.3 *Jeder euklidische Ring ist ein Hauptidealring*

Beweis. Sei R ein euklidischer Ring und $\mathfrak{a} \lhd R$ ein Ideal. Wähle $a \in \mathfrak{a}$, so dass $a \neq 0$ und $\gamma(a)$ minimal ist.

Behauptung *Das Ideal $\mathfrak{a}$ wird von a erzeugt, also $(a) = \mathfrak{a}$*

Beweis. Das (a) in $\mathfrak{a}$ enthalten ist ist klar, betrachten wir also die andere Inklusion. Sei hierzu $x \in \mathfrak{a}$, dann gibt es $r, c \in R$ mit der Eigenschaft $x = c \cdot a + r$ so dass $\gamma(r) < \gamma(a)$ oder $r = 0$. Es muss $r = 0$ und somit $x = ca \in (a)$ gelten, denn sonst ist $0 \neq r = x - ca \in \mathfrak{a}$ und $\gamma(r) < \gamma(a)$. Wir hatten a aber gerade so gewählt, dass $\gamma(a)$ minimal ist. □

Bemerkung 6.4 *Sei R ein Hauptidealring und $(p) \trianglelefteq R$ ein Primideal mit $0 \neq (p) \neq R$, dann ist (p) ein Maximalideal*

Beweis. Nach Satz 5.5 ist (p) in einem Maximalideal $(m) \lhd R$ enthalten, es gilt also $p = r \cdot m$ mit $r \in R$. Hieraus folgt, dass $rm \in (p)$ liegt und da (p) nach Vorraussetzung ein Primideal ist folgt sofort $r \in (p)$ oder $m \in (p)$. Ist $m \in (p)$, so folgt $(m) \subseteq (p) \subseteq (m)$ also $(m) = (p)$ andernfalls wäre $r = p \cdot s$ mit $s \in R$ und somit folgte $r \cdot m = p = r \cdot s$. Da R ein Integritätsring ist dürfen wir schließen, dass dann $sm = 1$ gelte, also m eine Einheit von R wäre. Dies liefert einen Widerspruch zur Maximalität von (m). □

Bemerkung 6.5 *(Hauptidalringe sind noethersche Ringe)*
Sei R ein Hauptidealring, dann wird jede aufsteigende Idealkette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_n \quad n \in \mathbb{N} \cup \{\infty\}$$

stationär, mit anderen Worten es gibt ein $N \in \mathbb{N}$ so dass für alle $i \geq N$ gilt $\mathfrak{a}_i = \mathfrak{a}_N$

Beweis. Definiere

$$\mathfrak{a} := \bigcup_{i=1}^{\infty} \mathfrak{a}_i$$

Wir haben bereits in Satz 5.5 gesehen, dass $\mathfrak{a}$ dann ein Ideal ist. Da R ein Hauptidealring ist gibt es ein $a \in \mathfrak{a}$ mit $(a) = \mathfrak{a}$. Insbesondere gibt es also $\mathfrak{a}_N$ mit $a \in \mathfrak{a}_N$ für ein $N \in \mathbb{N}$. Damit gilt aber

$$(a) \subseteq \mathfrak{a}_N \subseteq (a) = \mathfrak{a}$$

Also folgt sofort $\mathfrak{a} = (a) = \mathfrak{a}_N$. Da die Idealkette aufsteigend war ist alles gezeigt. □

Definition 6.6 *(Teilerfremd, Addition, Multiplikation von Idealen)*
Seien R ein Ring und $\mathfrak{a}, \mathfrak{b} \lhd R$ Ideale. Setze

$$\begin{aligned}
\mathfrak{a} + \mathfrak{b} &:= \left\{ \sum_{i=1}^{n} (a_i + b_i) \,|\, n \in \mathbb{N} \wedge a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b} \right\} = \{ a + b \,|\, a \in \mathfrak{a} \wedge b \in \mathfrak{b} \} \\
\mathfrak{a} \cdot \mathfrak{b} &:= \left\{ \sum_{i=1}^{n} (a_i \cdot b_i) \,|\, n \in \mathbb{N} \wedge a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b} \right\} = \{ a \cdot b \,|\, a \in \mathfrak{a} \wedge b \in \mathfrak{b} \} \\
\mathfrak{a}^n &:= \prod_{i=1}^{n} \mathfrak{a}
\end{aligned}$$

$\mathfrak{a}$ und $\mathfrak{b}$ heißen genau dann Teilerfremd, wenn $\mathfrak{a} + \mathfrak{b}$ bereits der gesamte Ring ist.
Seien $x_1, \ldots, x_n \in R$ setze $(x_1, \ldots, x_n) := (x_1) + \ldots + (x_n)$

Bemerkung 6.7 *In jedem Hauptidealring R gelten:*
(i) Seien $(p_1), (p_2) \trianglelefteq R$ Primideale mit $(p_1) \neq 0 \neq (p_2)$ dann gilt $(p_1) + (p_2) = R \vee (p_1) = (p_2)$
(ii) Seien $x_1, \ldots, x_n \in R$, dann ist

$$\prod_{i=1}^{n} (x_i) = \left(\prod_{i=1}^{n} x_i \right)$$

Beweis. zu i) Setze $(p_1) + (p_2) = (a)$, dann sind $(p_1), (p_2) \subseteq (a)$. Da (p_1) und (p_2) nach Bemerkung 6.4 Maximalideale sind folgt $(a) = (p_1) = (p_2)$ oder $(a) = R$.
zu ii) Es genügt die Behauptung für zwei Ideale $(a), (b) \lhd R$ zu zeigen. Sei zunächst $x \in (a) \cdot (b)$ dann können wir x schreiben als $\sum r_i a \cdot s_i b$ mit $r_i, s_i \in R$. Nach Umformung also $x = (\sum r_i s_i)\, ab \in (ab)$. Sei nun $x \in (ab)$, dann lässt sich x schreiben als $x = r \cdot ab = (r \cdot a) \cdot b \in (a) \cdot (b)$ mit $r \in R$ □

Satz 6.8 *Sei R ein Hauptidealring, dann besitzt jedes nicht-Nullideal $(a) \lhd R$ eine bis auf Vertauschung eindeutige Zerlegung in Maximalideale, also $(a) = (p_1) \cdot \ldots \cdot (p_r)$ mit $r \in \mathbb{N}$*

Beweis. Die Existenz dieser Zerlegung beweisen wir Konstruktiv, hierzu setzen wir zunächst $a_0 := a$ und betrachten den Sonderfall, dass $a_o \in R^\times$ eine Einheit ist. Dann ist die gesuchte Zerlegung das leere Produkt. Im Hauptfall betrachte

- Nach Satz 5.5 gibt es ein Maximalideal (p_1) mit $a_0 \in (p_1)$, dann können wir a_0 aber darstellen als $a_0 = p_1 \cdot a_1$ mit $a_1 \in R$. Ist a_1 eine Einheit, dann sind die Ideale (a_0) und (p_1) gleich, ist a_0 eine nicht-Einheit, dann ist das von a_0 erzeugte Ideal echt in (a_1) enthalten.

- Nach Satz 5.5 gibt es ein Maximalideal (p_2) mit $a_1 \in (p_2)$, dann können wir wiederum a_1 darstellen als $a_1 = p_2 \cdot a_2$ mit $a_2 \in R$. Ist a_2 eine Einheit, dann sind die Ideale (a_1) und (p_2) gleich, ist a_2 eine nicht-Einheit, dann ist das von a_1 erzeugte Ideal echt in (a_2) enthalten.
- ...

Annahme: Der oben konstruierte Prozess ist endlos, dann gibt es eine unendliche Idealkette

$$(a_0) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \dots$$

Dies ist aber ein Widerspruch zur Bemerkung 6.5.
Zum Beweis der Eindeutigkeit seien $(p_1) \cdot \ldots \cdot (p_r) = (a) = (q_1) \cdot \ldots \cdot (q_m)$ zwei (nicht notwendig verschiedene) Zerlegungen von (a), dann ist $(q_1) \cdot \ldots \cdot (q_m) = (q_1 \cdot \ldots q_m) \subseteq (p_1)$. Es gibt also einen Index i derart, dass $q_i \in (p_1)$ also $(q_i) \subseteq (p_1)$ gilt. Da sowohl (q_i) als auch p_1 Maximalideale sind müssen diese Assoziert sein, also $q_i = \varepsilon p_1$ mit $\varepsilon \in R^\times$. Wir dürfen nun schliesen, dass es ein $\delta \in R^\times$ gibt, so dass

$$\begin{aligned} \delta \cdot p_1 \cdot \ldots \cdot p_r &= q_1 \cdot \ldots \cdot q_m \\ &= \varepsilon \cdot p_1 \cdot q_1 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_m \end{aligned}$$

Da R ein Integritätsbereich ist folgt

$$\delta \cdot p_2 \cdot \ldots \cdot p_r = \varepsilon \cdot q_1 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_m$$

Gehen wir zurück zu den von dem p_j und q_l erzeugten Hauptidealen erhalten wir

$$(p_2) \cdot \ldots \cdot (p_r) = (q_1) \cdot \ldots \cdot (q_{i-1} \cdot (q_{i+1}) \cdot \ldots \cdot (q_m)$$

Setze dieses Verfahren induktiv fort. □

Bemerkung 6.9 *Seien R ein Hauptidealring und $\mathfrak{a} \trianglelefteq R$ mit $\mathfrak{a} \neq (0)$, dann besitzt $\mathfrak{a}$ eine Zerlegung der Form:*

$$\mathfrak{a} = (p_1)^{l_1} \cdot \ldots \cdot (p_n)^{l_n}$$

mit paarweise teilerfremden Maximalidealen (p_i). Diese Zerlegung ist bis auf Vertauschung eindeutig.

Beweis. (1) Existenz
Sei $\mathfrak{a} = (a_0)$ und o.B.d.A. $a_0 \notin R^\times$ mit Folgerung 5.6 gibt es ein Maximalideal $(p_1) \lhd R$ so dass $a_0 \in (p_1)$ enthalten ist. Wir können a_0 also schreiben als $a_0 = p_1 \cdot a_1$ mit $a_1 \in R$
1. Fall $(a_1 \in R^\times)$ dann ist $\mathfrak{a} = (a_0) = (P_1 \cdot a_1) = (p_1)$ und die Existenz ist bewiesen.
2. Fall $(a_1 \notin R^\times)$ dann ist (a_0) in (a_1) enthalten also gibt es mit Folgerung 5.6 ein Maximalideal $(p_2) \lhd R$ derart, dass $a_1 \in (p_2)$ enthalten ist. Wir können a_1 also schreiben als $a_1 = p_2 \cdot a_2$
Dieses Verfahren wiederholen wir solange, bis diese Folge durch Fall 1 abbricht, oder, nach Bemerkung 6.5, stationär wird.
(2) Eindeutigkeit:
Seien $(p_1)^{l_1} \cdot \ldots \cdot (p_n)^{l_n} = \mathfrak{a} = (q_1)^{f_1} \cdot \ldots \cdot (q_m)^{f_m} \leq (q_1)$
insbesondere ist dann $(p_1)^{l_1} \cdot \ldots \cdot (p_n)^{l_n} \in (q_1)$
Da (q_1) ein Primideal ist gibt es einen Index i, so dass $p_i \in (q_1)$ liegt. Es folgt sofort, dass $(p_i) = (q_1)$,

denn $(p_i), (q_1)$ sind Maximalideale.
Wir können p_i also schreiben als $p_i = \varepsilon \cdot q_1$ mit $\varepsilon \in R^\times$ damit gilt

$$\begin{aligned} p_1^{l_1} \cdot \ldots p_i^{l_i - 1} \cdot p_i \cdot \ldots \cdot p_n^{l_n} &= \varepsilon q_1 \cdot p_1^{l_1} \cdot \ldots p_i^{l_i - 1} \cdot \ldots \cdot p_n^{l_n} \\ &= \delta q_1^{f_1} \cdot \ldots \cdot q_m^{f_m} \end{aligned}$$

mit $\delta \in R^\times$ teile nun durch q_1 und erhalte $p_1^{l_1} \cdot \ldots p_i^{l_i - 1} \cdot \ldots \cdot p_n^{l_n} = \varepsilon^{-1}\delta q_1^{f_1 - 1} \cdot \ldots \cdot q_m^{f_m}$
Setze dieses Verfahren nun induktiv fort. □

7 Faktorielle Ringe

Definition 7.1 *(Teiler und Assoziertheit)*
Seien R ein Integritätsring und $a, b \in R$, dann heißt b Teiler von a (Notation: $b|a$), falls es ein $c \in R$ gibt, mit der Eigenschaft $a = bc$
Die Elemente a, b heißen Assoziert (Notation: $a \hat{=} b$), falls es ein $\varepsilon \in R^\times$ gibt, mit der Eigenschaft $a = \varepsilon b$ (Nach Bemerkung 5.2 heißt das $(a) = (b)$)

Definition 7.2 *(Irreduzible- und Primelemente)*
Sei R ein Ring.
Ein Element $p \in R \backslash R^\times$ heißt Primelement, falls das von p erzeugte Hauptideal (p) ein Primideal ist.
Ein Element $r \in R \backslash R^\times$ heißt irreduzibel oder unzerlegbar, falls aus $r = ab$ stets folgt, dass einer der beiden Faktoren eine Einheit ist, d.h. $a \in R^\times$ oder $b \in R^\times$.

Bemerkung 7.3 *In Integritätsringen sind Primelemente irreduzibel.*

Beweis. Sei R ein Integritätsring und $p \in R$ ein Primelement. Weiter seien $a, b \in R$ mit $p = ab$ dann teilt p das Produkt ab und somit teilt p bereits a oder b nach Voraussetzung. O.B.d.A. gelte: $p|a$ dann gibt es ein $a' \in R$ derart, dass $a = pa'$ Wir können p also schreiben als $p = ab = pa'b$. Da R nullteilerfrei ist folgt: $1 = a'b$ also ist $b \in R^\times$ und p ist irreduzibel. □

Bemerkung 7.4 *R sei Integritätsring und a eine nicht-Einheit, also $a \in R \backslash R^\times$. Seien weiter Primelemente $p_1, \ldots, p_r \in R$ und irreduzible Elemente $q_1, \ldots, q_s \in R$ mit der Eigenschaft*

$$p_1 \cdot \ldots \cdot p_r = a = q_1 \cdot \ldots \cdot q_s$$

gegeben. Dann gilt: $r = s$ und für alle $i = 1, \ldots, s$ gibt es ein j mit der Eigenschaft $p_i \hat{=} q_j$

Beweis. Es gilt: $p_1 | q_1 \cdot \ldots \cdot q_s \Rightarrow \exists\, i \in \{1, \ldots, s\}\ p_1 | q_i \Rightarrow p_1 \hat{=} q_i$ teile nun p_1 aus der Gleichung und fahre induktiv fort mit p_2 □

Satz 7.5 *Es sind äquivalent:*
(a) $\forall\, a \in R \backslash R^\times\ \exists\, q_1, \ldots, q_s \in R$ irreduzibel $\quad a = q_1 \cdot \ldots \cdot q_s$
Diese Zerlegung ist Eindeutig bis auf Reihenfolge und Assoziiertheit.
(b) $\forall\, a \in R \backslash R^\times\ \exists\, p_1, \ldots, p_s \in R$ Primelemente $\quad a = p_1 \cdot \ldots \cdot p_s$

Beweis. zu „(b) ⇒ (a)":
Die p_i sind irreduzibel nach Bemerkung 7.3 und die Eindeutigkeit folgt sofort aus 7.4
zu „(a) ⇒ (b)":
Es genügt hier zu zeigen, dass jedes irreduzible Element ein Primelement ist.

Sei also $p \in R \backslash R^\times$ irreduzibel und $a, b \in R$ mit $p|ab$
Wir betrachten zunächst den Sonderfall, dass $a = 0 \vee b = 0 \vee a \in R^\times \vee b \in R^\times$. In diesem Fall ist die Aussage immer wahr. Betrachten wir nun den Hauptfall:
nach (a) gilt: $a = a_1 \cdot \ldots \cdot a_r \wedge b = b_1 \cdot \ldots \cdot b_s$ mit a_i, b_i irreduzibel $\forall\, i, j$ Es folgt, dass p das Produkt aller a_i, b_j teilen muss, also $p|a_1 \cdot \ldots \cdot a_r \cdot b_1 \cdot \ldots \cdot b_s$. Das heißt es gibt entweder einen Index i derart, dass $p \hat{=} a_i$ oder einen Index j mit der Eigenschaft $p \hat{=} b_j$ also folgt, dass $p|a$ oder $p|b$ □

Definition 7.6 *(Faktorring oder ZPE-Ring)*
Sei R ein Integritätsring, dann heißt R faktorieller Ring, oder ZPE-Ring (Zerlegung in Primelemente), falls die äquivalenten Bedingungen aus Satz 7.5 gelten.

Bemerkung 7.7 *In einem faktoriellen Ring ist jedes irreduzieble Element ein Primelement.* □

Folgerung 7.8 *Hauptidealringe sind faktoriell.*

Beweis. Sei R ein Hauptidealring, und $a \in R \backslash \{0 \cup R^\times\}$ eine nicht-Einheit dann leifert Satz 6.8 eine Zerlegung des von a erzeugten Hauptideals in Primideale (p_i) also $(a) = (p_1)^{d_1} \cdot \ldots \cdot (p_r)^{d_r}$. Dies liefert in kanonischer Weise eine Zerlegung in Primelemente von a durch $a = p_1^{d_1} \cdot \ldots \cdot p_r^{d_r}$ □

Folgerung 7.9 *Euklidische Ringe sind faktorielle Ringe.*

Beweis. Euklidische Ringe sind Hauptidealringe nach Satz 6.3. □

Definition und Bemerkung 7.10 *(Zerlegung in Primfaktoren)*
Sei R ein faktorieller Ring und $\mathfrak{P}$ ein Vertretersystem der Primelemente bis auf Assoziertheit. Dann lässt sich jedes Element $a \in R \backslash \{0\}$ eindeutig schreiben als

$$a = \varepsilon \prod_{p \in \mathfrak{P}} p^{v_p(a)} \quad \text{mit } \varepsilon \in R^\times \text{ und } v_p(a) \in \mathbb{Z}$$

□

Definition 7.11 *(größter gemeinsamer Teiler)*
Sei R ein Integritätsring dann heißt $b \in R$ größter gemeinsamer Teiler von $x_1, \ldots, x_n \in R \backslash \{0\}$, falls
(i) für alle $1 \leq i \leq n$ gilt b teilt x_i und
(ii) wenn aus der Existenz eines $a \in R$, das ebenfalls die Eigenschaft hat alle x_i zu teilen, folgt, dass a auch b teilt.
Wir schreiben dann $b = \mathrm{ggT}(x_1, \ldots, x_n)$
***Anmerkung:** In allgemeinen Ringen muss es keinen größten gemeinsamen Teiler geben. Jedoch ist er, wenn es einen gibt, bis auf Assoziertheit eindeutig bestimmt.*

Bemerkung 7.12 *Seien R ein faktorieller Ring, $\mathfrak{P}$ wie in Definition 7.10 und $x_1, \ldots x_n \in R \backslash \{0\}$. Dann ist:*

$$\prod_{p \in \mathfrak{P}} p^{min\{v_p(x_1), \ldots, v_p(x_2)\}}$$

ein größter gemeinsamer Teiler von $x_1, \ldots, x_n$. □

Bemerkung 7.13 *Seien R ein Hauptidealring und $x_1, \ldots, x_n \in R\backslash\{0\}$, dann ist $(x_1) + \ldots + (x_n) = (x_1, \ldots, x_n) = (d)$ und d ist ein größter gemeinsamer Teiler von $x_1, \ldots, x_n$*

Beweis. Sei $(d) := (x_1, \ldots, x_n)$ dann sind die x_i in (d) für alle i enthalten, also teilt d alle x_i . Nach Definition teilt d dann auch den größten gemeinsamen Teiler der $x_1, \ldots, x_n$. Definiere nun $a := \mathrm{ggT}(x_1, \ldots, x_n)$ dann folgt sofort, dass für alle i gilt $x_i \in (a)$ also ist $(d) \subseteq (a)$. Diese Inklusion können wir zu $a|d$ übersetzen, damit folgt jedoch sofort die Assoziiertheit von a und d. □

Satz 7.14 *(Euklidischer Algorithmus)*
Sei R ein euklidischer Ring mit der Normfunktion δ wie in Definition 6.1. Seien weiter $a, b \in R\backslash\{0\}$.

$$\begin{aligned} a &= q_1 \cdot b + a_2 && \text{mit } q_1, a_2 \in R \text{ und } \delta(a_2) < \delta(b) \vee a_2 = 0 \\ b &= q_2 \cdot a_2 + a_3 && \text{mit } q_2, a_3 \in R \text{ und } \delta(a_3) < \delta(a_2) \vee a_3 = 0 \\ a_2 &= q_3 \cdot a_3 + a_4 && \text{mit } q_3, a_4 \in R \text{ und } \delta(a_4) < \delta(a_3) \vee a_4 = 0 \\ &\ldots \end{aligned}$$

Es gibt ein minimales $n \in \mathbb{N}_{>0}$, so dass $a_{n+1} = 0$ also $a_{n-1} = a_n q_n + 0$
Dann ist $a_n = \mathrm{ggT}(a, b)$ und es existieren $\alpha, \beta \in R : a_n = \alpha a + \beta b$

Beweis. Dieser Algorithmus bricht ab, denn wegen $\delta(a_1) > \delta(a_2) > \delta(a_3) > \ldots$ wird $0_{\mathbb{N}}$ erreicht. Weiter gilt, dass a_n teilt a_{n-1} also teilt a_n auch a_{n-2} und so weiter, daher folgt, dass a_n teilt a_0 und a_n teilt a_1. Wegen $a_n = \alpha \cdot a + \beta \cdot b$ gilt für ein $d \in R$ mit der Eigenschaft a und b zu teilen, dass d auch a_n teilt. Also ist $a_n = \mathrm{ggT}(a, b)$. □

Beispiel 13 *(Kongruenzen in $\mathbb{Z}$ - Anwendung des chinesischen Restsatzes)*
Seien $a, b \in \mathbb{Z}$ teilerfremd, d.h. $\mathrm{ggT}(a, b) \hat{=} 1$. Wir suchen ein $x \in \mathbb{Z}$ für das gilt:
$x \equiv m$ *mod* a
$x \equiv n$ *mod* b
Da a und b teilerfremd finde mit Satz 7.14 Elemente α und β, so dass $1 = \alpha a + \beta b$. Wir stellen fest:
$\alpha a \equiv 1$ *mod* $b \wedge \alpha a \equiv 0$ *mod* a
$\beta b \equiv 0$ *mod* $b \wedge \beta b \equiv 1$ *mod* a
Setze also $x := m \cdot \beta b + n \cdot \alpha a$ ✓

Definition und Bemerkung 7.15 *(Direktes Produkt von Ringen)*
Sei I eine Indexmenge und für alle $i \in I$ seien Ringe R_i gegeben, dann ist das karthesische Produkt der Ringe R_i zusammen mit komponentenweiser Addition und Multiplikation ein Ring (Notation: $\prod_{i \in I} R_i$). Wir nennen $\prod_{i \in I} R_i$ das direkte Produkt der Ringe R_i.

Beweis. Nachrechnen der Ringeigenschaften. □

Satz 7.16 *(chinesischer Restsatz)*
Sei R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq R$ seien Ideale. Die Abbildung

$$\begin{aligned} \varphi : R &\to \prod_{i=1}^{n} R/\mathfrak{a}_i \\ r &\mapsto (r + \mathfrak{a}_i, \ldots, r + \mathfrak{a}_n) \end{aligned}$$

ist Ringhomomorphismus mit den Eigenschaften:
(i) φ *ist surjektiv* $\Leftrightarrow \forall\, i \neq j \quad \mathfrak{a}_i + \mathfrak{a}_j = (1)$ *(paarweise Teilerfremd)*
(ii) $\mathrm{Ker}(\varphi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$
(iii) φ *ist injektiv* $\Leftrightarrow \bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$

Beweis. Das φ ein Ringhomomorphismus ist, ist klar, da φ die natürliche Projektion $R \to {}^{R}\!/_{\mathfrak{a}_i}$ in jeder Komponente ist.
zu (i) „⇒“
Seien $i \neq j$ beliebig wir finden ein $r \in R$ mit der Eigenschaft:
$\varphi(r) = (0, \ldots, 0, 1, 0, \ldots, 0) =: e_i$ (1 in der i-ten Komponente, sonst Nullen)
Für alle $j \neq i$ ist $r \in \mathfrak{a}_j$, da $0 = r + \mathfrak{a}_j$ betrachte
$\varphi(1 - r) = (1, \ldots, 1) - e_i \Rightarrow 1 - r + \mathfrak{a}_i = 0 \Rightarrow 1 - r \in \mathfrak{a}_i$ Also ist $1 = (1 - r) + r \in \mathfrak{a}_i + \mathfrak{a}_j$
Somit gilt $1 \in \mathfrak{a}_i + \mathfrak{a}_j = R$
zu (i) „⇐“
Es genügt hier zu zeigen, dass für jedes i gilt $e_i \in \mathrm{Im}(\varphi)$. Seien hierzu i, j beliebig mit $i \neq j$, wähle ein $x_j \in \mathfrak{a}_j$ und ein $y_i \in \mathfrak{a}_i$ derart, dass $1 = x_j + y_i$. Definiere

$$\begin{aligned} r &:= \prod_{\substack{j=1 \\ i \neq j}}^{n} x_j = \prod_{\substack{i=1 \\ i \neq j}}^{n} (1 - y_i) \ \in \mathfrak{a}_j \ \forall\, i \neq j \\ &= 1 + \tilde{y} \text{ mit } \tilde{y} \in \mathfrak{a}_i \end{aligned}$$

Wir haben gezeigt, dass $\varphi(r) = e_i$ ist, also e_i im Bild von φ liegt, somit folgt die Behauptung.
(ii) und (iii) sind aus den entsprechenden Definitonen klar. □

Bemerkung 7.17 *Sei R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale*[1]*. Dann gilt*

$$\bigcap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i$$

Beweis. Wir beweisen zunächst eine weitere Behauptung, und führen den Beweis dann anschließend per Induktion:

Behauptung 1 $\prod_{i=1}^{n-1} \mathfrak{a}_i$ *und* $\mathfrak{a}_n$ *sind Teilerfremd.*

Beweis. Wähle $x_i \in \mathfrak{a}_i$ und $y_i \in \mathfrak{a}_n$ mit $1 = x_i + y_i$ für $i = 1, \ldots, n-1$, dann folgt

$$1 = \prod_{i=1}^{n-1} (x_i + y_i) = \prod_{i=1}^{n-1} x_i \ + \tilde{y} \quad \tilde{y} \in \mathfrak{a}_n$$

$$\Rightarrow \ 1 \in \prod_{i=1}^{n-1} \mathfrak{a}_i \ + \mathfrak{a}_n$$

△

Wir setzen den Induktionsanfang bei $n = 2$
Zu zeigen: $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \cdot \mathfrak{a}_2$ für $1 = \mathfrak{a}_1 + \mathfrak{a}_2$

[1] Vergleiche Satz 7.16 (i)

Sei $a \in \mathfrak{a}_1 \wedge b \in \mathfrak{a}_2$ mit $1 = a + b$
$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$ ist klar nach Def. ($\mathfrak{a}_1 \cdot \mathfrak{a}_2 := \{a \cdot b \,|\, a \in \mathfrak{a}_1 \wedge b \in \mathfrak{a}_2\}$)
zu „$\supseteq$: Sei $r \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ dann ist $r = r \cdot 1 = r(a + b) = ra + rb \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$
Die eigentliche Induktion ist mit der zuvor bewiesenen Behauptung 1 leicht. □

Folgerung 7.18 *Sei R ein Hauptidealring und $\mathfrak{a} \trianglelefteq R$ ein Ideal mit der Eigenschaft*[2] $\mathfrak{a} = \prod_{i=1}^{n} (p_i)^{e_i}$ *und die p_i paarweise Teilerfremd. Dann ist*

$$R/\mathfrak{a} \cong \prod_{i=1}^{n} R/(p_i^{e_i})$$

□

Beispiel 14 *Es gilt* $\mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ *denn* $18 = 2 \cdot 3^2$ *und* $(2), (3) \lhd \mathbb{Z}$ *sind Teilerfremd.*

8 Der Satz von Gauß

Definition und Bemerkung 8.1 *(Zerlegung in Primelemente*[3]*)*
Sei R ein faktorieller Ring und $K := \mathrm{Quot}(R)$ sein Quotientenkörper. Sei weiter $\mathfrak{P} \subset R$ ein Vertretersystem der Primelemente bezüglich Assoziertheit in R. Dann lässt sich jedes $x \in K \backslash \{0\}$ eindeutig als ein Produkt von Primelementen schreiben:

$$x = \varepsilon \prod_{p \in \mathfrak{P}} p^{v_p(x)} \quad \text{mit } v_p(x) \in \mathbb{Z} \text{ und fast alle } v_p(x) = 0 \text{ sowie } \varepsilon \in R^\times$$

□

Beispiel 15 *$R = \mathbb{Z}, K = \mathbb{Q}$ und $x = -\frac{7}{36}$ Dann gilt*
$\mathfrak{P} = \{p \in \mathbb{Z}$ prim $\,|\, p > 0\}$ und $x = (-1) \cdot 2^{-2} \cdot 3^{-2} \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot \ldots$
Also: $v_2(x) = v_3(x) = -2$ und $v_7(x) = 1$ und für alle $p \in \mathfrak{P} \backslash \{2, 3, 7\}$ gilt $v_p(x) = 0$

Bemerkung 8.2 *Seien die Voraussetzungen wie eben, dann gelten:*
(i) $x \in R \Leftrightarrow$ für alle $p \in \mathfrak{P}$ gilt $v_p(x) \geq 0$
(ii) für alle $p \in \mathfrak{P}$ gilt $v_p(xy) = v_p(x) + v_p(y)$
(iii) $x \in R^\times \Leftrightarrow$ für alle $p \in \mathfrak{P}$ gilt $v_p(x) = 0$ □

Definition 8.3 *(Primpotenzen)*
Seien $R, K, \mathfrak{P}$ wie in Bemerkung 8.1 gegeben. Zusätzlich sei $f(X) := \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom, dann setze: $v_p(f) := \min_i \{v_p(a_i)\}$.

Bemerkung 8.4 *Seien $\mathfrak{P}$,K, R wie in Bemerkung 8.1 und f wie eben gegeben. Es gelten:*
(i) $v_p(f) \neq 0$ für höchstens endlich viele $p \in \mathfrak{P}$
(i) $v_p(f) \geq 0 \; \forall p \in \mathfrak{P} \; \Rightarrow f(X) \in R[X]$ □

[2] Vergleiche Bemerkung 6.9
[3] Vergleiche Bemerkung 7.10

Satz 8.5 *Seien $\mathfrak{P}$,K, R wie in Bemerkung 8.1. Weiter seien $f(X) := \sum_{i=0}^{n} a_i X^i$ und $g(X) := \sum_{i=0}^{n} b_i X^i$ Polynome mit Koeffizienten in K. Es gilt:*

$$v_p(f \cdot g) = v_p(f) + v_p(g) \quad \forall\, p \in \mathfrak{P}$$

Beweis. Zunächst grenzen wir das Problem auf einen Sonderfall ein, den wir im Folgenden beweisen werden.
(1.) Wir können o.B.d.A. annehmen, dass $f, g \in R[X]$ liegen, denn für $\alpha \in K\backslash\{0\}$ gilt:
$v_p(\alpha f) = v_p(\alpha) + v_p(f)$. Wähle also $\alpha, \beta \in K\backslash\{0\}$ derart, dass $\alpha f, \beta g \in R[X]$ und betrachte:

$$\begin{aligned} v_p(\alpha f \cdot \beta g) &= v_p(\alpha\beta \cdot fg) = v_p(\alpha\beta) + v_p(fg) \\ &= v_p(\alpha) + v_p(\beta) + v_p(f) + v_p(g) = v_p(\alpha) + v_p(f) + v_p(\beta) + v_p(g) \\ &= v_p(\alpha f) + v_p(\beta g) \end{aligned}$$

(2.) Wir können weiterhin o.B.d.A. annehmen, dass $f, g \in R[X]$ die Eigenschaft $v_p(f) = 0 = v_p(g)$ besitzen, denn:
Seien $d_f := \mathrm{ggT}(a_1, \ldots, a_n)$ und $d_g := \mathrm{ggT}(b_1, \ldots, b_m)$ die größten gemeinsamen Teiler der Koeffizienten von f und g, dann gilt nach Definition 8.3:

$$v_p(\frac{1}{d_f} \cdot f) = -v_p(d_f) + v_p(f) = 0 \quad \text{(Analog für } d_g\text{)}$$

(3.) Wir haben nun auf den Sonderfall $f, g \in R[X]$ mit $v_p(g) = 0 = v_p(f)$ reduziert und wollen Zeigen, dass $v_p(fg) = 0$ gilt. Hierzu betrachte die folgende Abbildung:

$$\begin{aligned} \pi : R[X] &\to {}^{R}\!/_{(p)}[X] \\ \sum c_r X^r &\mapsto \sum \hat{\pi}(c_r) X^r \end{aligned}$$

wobei hier $\hat{\pi}$ die natürliche Projektion von R nach ${}^{R}\!/_{(p)}$ ist. Da $v_p(f) = 0$ ist, gilt $\pi(f) \neq 0$ ebenso folgt $\pi(g) \neq 0$. Da $(p) \trianglelefteq R$ prim ist, folgt mit Bemerkung 5.2, dass ${}^{R}\!/_{(p)}$ ein Integritätsring ist.
Es gilt $\pi(f) \cdot \pi(g) = \pi(fg) \neq 0 \;\Rightarrow\; v_p(fg) = 0$ □

Definition 8.6 *(primitive und normierte Polynome)*
Seien R, K und $\mathfrak{P}$ wie in Bemerkung 8.1 gegeben. Ein Polynom $f = \sum_{i=0}^{n} a_i X^i$ heißt genau dann primitiv, wenn für alle $p \in \mathfrak{P}$ gilt $v_p(f) = 0$ mit anderen Worten, wenn $\mathrm{ggT}(a_0, \ldots, a_n) \hat{=} 1$ gilt.
f heißt normiert, falls der höchste Koeffizient von f gleich 1 ist. (Notation: $hK(f) = a_n$).

Anmerkung Insbesondere sind normierte Polynome primitiv.

Folgerung 8.7 *Sei R ein faktorieller Ring und $h \in R[T]$ sowie $f, g \in K[T]$ seien normierte Polynome mit $h = f \cdot g$, dann sind bereits $f, g \in R[T]$.*

Beweis. Es gilt $0 = v_p(h) = v_p(fg) = v_p(f) + v_p(g)$. Da h, f, g normiert sind gilt weiter $v_p(f) \leq 0$ und $v_p(g) \leq 0$ somit folgt $v_p(f) = v_p(g) = 0$ □

Bemerkung 8.8 *Sei $f \in K[X]$, mit K wie in Bemerkung 8.1. Dann gibt es ein $a \in K\backslash\{0\}$, so dass das Polynom $\tilde{f} := \frac{1}{a} \cdot f$ primitiv ist.*

Beweis. Sei $\mathfrak{P}$ wieder wie in Bemerkung 8.1, dann definiere

$$a := \prod_{p \in \mathfrak{P}} p^{v_p(f)}$$

Dieses a erfüllt die Anforderung, denn für alle $p \in \mathfrak{P}$ gilt $v_p(\frac{1}{a}f) = v_p(f) - v_p(a) = 0$ □

Satz 8.9 *(Satz von Gauß)*

In jedem faktoriellen Ring R gelten:
(a) $R[X]$ ist faktorieller Ring
(b) Sei $f \in R[X]$ und $K := \mathrm{Quot}(R)$, dann sind äquivalent:
i) $f \in R[X]$ ist ein Primelement
ii) f ist vom Typ I: f ist ein Primelement von R
oder vom Typ II: f ist primitiv und prim in $K[X]$

Beweis. Wir zeigen zunächst im Teil (b) nur den Schluss von (ii) auf (i). Dafür nehmen wir uns als erstes ein f vom Typ I her. Sei also $f \in R$ ein Primelement, dann ist zu zeigen, dass $(f) \trianglelefteq R[X]$ ein Primideal ist. Betrachte hierzu

$$\begin{array}{rccc} \varphi: & R[X] & \to & {}^{R}\!/_{(f)_R}[X] \\ & \sum a_n X^n & \mapsto & \sum \bar{a}_n X^n \text{ mit } \bar{a}_n := a_n + (f)_R \end{array}$$

Dann ist $\mathrm{Ker}(\varphi) = (f) \trianglelefteq R$ auch ein Ideal im Polynomring mit dem Homomorphiesatz 4.8 folgt nun die Injektivität von

$${}^{R[X]}\!/_{(f)_{R[X]}} \hookrightarrow {}^{R}\!/_{(f)_R}[X]$$

Es folgt sofort, dass ${}^{R}\!/_{(f)}[X]$ ein integritätsring ist, da $(f) \trianglelefteq R$ prim ist nach Voraussetzung. Somit muss auch der enthaltene Ring ${}^{R[X]}\!/_{(f)_{R[X]}}$ ein Integritätsring sein. Dann ist $(f) \trianglelefteq R[X]$ ein Primideal. Nun sei f vom Typ II, also sei $f \in K[X]$ primitiv und ein Primelement. Es ist zu zeigen, dass $f \in R[X]$ prim ist, dass also für alle Produkte $gh \in R[X]$ die von f geteilt werden ($f|gh$) gilt, dass f bereits h oder g teilt. Seien nun $g, h \in R[X]$ ein solches Produkt mit $f|gh$. Da $f \in K[X]$ ein Primelement ist wissen wir schon dass in $K[X]$ eines der Polynome g oder h von f geteilt wird. Wir wollen o.B.d.A. annehmen, dass f das g teile. Dann gibt es ein $q \in K[X]$ mit der Eigenschaft, dass $g = f \cdot q$ ist. Daher gilt für alle $p \in \mathfrak{P} \subset R$ dass $0 \leq v_p(g) = v_p(f) + v_p(q)$ ist da $v_p(f) = 0$ ist. Aus der Primitivität von f folgt $v_p(q) \geq 0$ also liegt $q \in R[X]$ Damit wird g von f bereits in $R[X]$ geteilt. Nun betrachten wir den Teil (a) genauer, und erledigen den zweiten Teil von (b) gleich mit. Wir müssen dazu zeigen, dass jedes $f \in R[X]\backslash\{0\}$ Produkt von Elementen des Typs I oder II ist, denn dann folgt insbesondere, dass $R[X]$ ein faktorieller Ring ist.
Es gibt ein $a \in K\backslash\{0\} = K^\times$, so dass $\tilde{f} := \frac{1}{a} \cdot f \in K[X]$ primitiv ist [Wähle ein $a \hat{=} \mathrm{ggT}(\mathrm{Koeff}(f))$] Es gilt dann für alle Primelemente p von R, dass $0 = v_p(\tilde{f}) = -v_p(a) + v_p(f)$ ist, also $v_p(a) = v_p(f) \geq 0$ gilt. Insbesondere gilt $a \neq 0$ daher finden wir eine Zerlegung in Primelemente

$$a = \prod_{i=1}^{m} \bar{a}_i \in R \quad \text{wobei die } \bar{a}_i \text{ vom Typ I sind.}$$

Wir betrachten nun wieder das primitive Polynom $\tilde{f} \in K[X]$ und benutzen die Zerlegung in Primelemente in diesem Ring und erhalten

$$\tilde{f} = \eta \cdot \prod_{i=1}^{n} \tilde{f}_i$$

mit den Eigenschaften, dass $\eta \in K^\times = K\backslash\{0\}$ liegt, alle Polynome $\tilde{f}_i$ in $R[X]$ primitiv sind und in $K[X]$ sogar Primpolynome sind. Für alle i gilt also, dass die $\tilde{f}_i$ vom Typ II sind.
Wir haben für alle Primelemente aus R die Gleichung

$$0 = v_p(\tilde{f}) = v_p(\eta) + \sum_{i=1}^{n} v_p(\tilde{f}_i)$$

Da die Summanden für alle i den Wert 0 haben gilt: $v_p(\eta) = 0$, das heißt, dass η bereits in $R^\times$ liegt und wir nun f darstellen können durch

$$f = a \cdot \tilde{f} = \eta \cdot \prod_{i=1}^{m} \bar{a}_i \cdot \prod_{i=1}^{n} \tilde{f}_i$$

Damit haben wir (a) gezeigt, aber nach (a) gilt nun, dass $f \in R[X]$ ein Produkt von Elementen des Typs I oder des Typs II ist. Da Primelemente irreduziebel sind, ist f ein Primelement vom Typ I oder vom Typ II. Damit ist auch der Schluss von (i) auf (ii) vom Satzteil (b) gezeigt. □

Folgerung 8.10 *Sei R ein faktorieller Ring, $K := \mathrm{Quot}(R)$ sein Quotientenkörper und $f \in R[X]\backslash R$ ein primitives Polynom. Dann sind äquivalent:*
(i) $f \in R[X]$ ist Primelement
(ii) $f \in K[X]$ ist Primelement

Beweis. Die Behauptung folgt direkt aus dem Satz von Gauß 8.9. □

Folgerung 8.11 *Ist R ein faktorieller-Ring, so ist auch der Polynomring in endlich vielen Variablen $R[X_1, \ldots, X_n]$ ein faktorieller Ring.*

Beweis. Induktiv. Beachte: $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ □

Anmerkung Ist K ein Körper, so ist $K[X, Y]$ ein faktorieller Ring, aber kein Hauptidealring(!), denn das Ideal (X, Y) lässt sich nicht von einem Element allein erzeugen.

Bemerkung 8.12 *Sei R ein Integritätsring und $f = \sum_{n=0}^{d} a_n x^n \in R[X]$ ein Polynom, dann hat f höchstens d Nullstellen.* □

9 Irreduziblitätskriterien

In diesem Unterabschnitt ist R immer ein faktorieller Ring, und $K := \mathrm{Quot}(R)$ sein Quotientenkörper.

Erinnerung In faktoriellen Ringen sind Primelemente und irreduzible Elemente dasselbe.

Bemerkung 9.1 *Seien $f \in K[X]$ ein Polynom mit $\mathrm{Grad}(f) = \deg(f) \geq 1$ und $a \in K^\times$ derart, dass $\tilde{f} = \frac{1}{a} \cdot f \in R[X]$ ein primitives Polynom ist. Dann sind äquivalent:*
(i) f ist irreduzibel in $K[X]$
(ii) $\tilde{f}$ ist irreduzibel in $K[X]$
(iii) $\tilde{f}$ ist irreduzibel in $R[X]$

Beweis. Diese Bemerkung folgt sofort aus den Sätzen 8.9 und 8.10 □

Satz 9.2 *(Reduktionskriterium)*
Sei $p \in R$ ein Primelement und $f \in R[X]$ ein Polynom. Wir nehmen an, dass der höchste Koeffizient von f (hK(f)) nicht von p geteilt wird.
Betrachte die Abbildung φ aus dem Satz von Gauß (8.9):

$$\begin{aligned} \varphi_p : \ R[X] \quad &\to \quad {}^{R}\!/_{(p)}[X] \\ \sum a_n X^n \quad &\mapsto \quad \sum \bar{a}_n X^n \quad \text{mit } \bar{a}_n := a_n + (p) \end{aligned}$$

Es gelten:
(a) ist f primitiv und $\varphi_p(f)$ irreduzibel in ${}^{R}\!/_{(p)}[X]$, dann ist f bereits in $R[X]$ irreduzibel.
(b) ist $\varphi_p(f)$ irreduzibel in ${}^{R}\!/_{(p)}[X]$, dann ist f irreduzibel in $K[X]$.

Beweis. zu (a):
Annahme f ließe sich darstellen durch $f = g \cdot h$ mit $g, h \in R[X] \backslash R^\times$ dann folgt aus der Primitivität von f, dass der der Grad beider Polynome größer 0 ist (Also $\deg(g) \geq 0 \leq \deg(h)$). Da p nicht den höchsten Koeffizienten von f teilt, kann p auch kein Teiler der höchsten Koeffizienten von g und h sein. Das heißt aber, dass $\varphi(f) = \varphi(g) \cdot \varphi(h)$ ist. Dies liefert einen Widerspruch, da $\deg(\varphi(g)) = \deg(g) \geq 0$ und $\deg(\varphi(h)) = \deg(h) \geq 0$ sind.
zu (b):
Sei $\tilde{f} := \frac{1}{c} \cdot f \in R[X]$ ein primitives Polynom wobei $c \in R$ mit der Eigenschaft $v_p(c) = v_p(f) \geq 0$ ist. Es gilt, dass p weder c noch den höchsten Koeffizienten von f teilt, daher ist $\varphi(\tilde{f}) = \varphi(\frac{1}{c}) \cdot \varphi(f) \neq 0$ Da $\varphi(\tilde{f})$ irreduzibel in ${}^{R}\!/_{(p)}[X]$ ist, ist $\tilde{f}$ irreduzibel in $R[X] \subset K[X]$. Damit ist auch f irreduzibel in $K[X]$. □

Beispiel 16 $R = \mathbb{Z}, \quad f = X^3 + 5X^2 + 4X + 13 \in \mathbb{Z}[X]$
f ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$, denn modulo 2 erhalten wir:
$\varphi_2(f) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$
$\varphi_2(f)$ ist irreduzibel, da $\varphi_2(f)$ keine Nullstelle in $\mathbb{F}_2$ hat, und $\deg(f) \leq 3$ ist.

Satz 9.3 *(Eisenstein Kriterium)*
Es seien $f = \sum_{n=0}^{d} a_n x^n \in R[X]$ ein primitives Polynom und $p \in R$ ein Primelement mit den Eigenschaften p teilt nicht den höchsten Koeffizienten von f ($p \nmid a_d$) aber alle anderen Koeffizienten von f, also $p | a_i$ für alle $i = 0, \ldots, d-1$ weiter gelte $p^2 \nmid a_0$. Dann ist $f \in R[X]$ irreduzibel

Beweis. Wir nehmen an, dass $f = gh$ mit hK$(g) = b_r$ und hK$(h) = c_s$ Es gilt dann:
$a_d = b_r \cdot c_s \Rightarrow p \nmid b_r \wedge p \nmid c_s$ und weiter können wir sagen:
$a_o = b_0 \cdot c_0 \wedge p | a_0 \wedge p^2 \nmid a_0 \Rightarrow (p | c_0 \wedge p \nmid b_0) \vee (p \nmid c_0 \wedge p | b_0)$

Es gelte o.B.d.A.: $p|c_0 \wedge p \nmid b_0$ dann gibt es ein $t \in \{1, \ldots, r\}$ minimal, mit $p \nmid b_t$. Wenn wir Polynome in Summenschreibweise multiplizieren erhalten wir für a_t die folgende Gleichung:

$$a_t = \sum_{i=0}^{t} b_i c_{t-i} = \left(\sum_{i=0}^{t-1} b_i c_{t_i} \right) + b_t c_0$$

Das heißt, dass p die Summe $\sum_{i=0}^{t-1} b_i c_{t-i}$ teilt, aber nicht den letzten Summanden $b_t \cdot c_o$. Dies ist aber ein Widerspruch dazu, dass p entweder c_0 oder b_t teilt. □

Beispiel 17 *zu den Irreduzibilitätskriterien*
(a) $R = \mathbb{Z},\ f = X^3 + 5X^2 + 25X + 15 \in \mathbb{Z}[X]$ *ist primitiv.*
f *ist irreduzibel nach Eisenstein mit* $p = 5$

(b) $g = X^4 + 3X^3 + 5XY^2 + Y + 3 \in \mathbb{Z}[X, Y]$
Anmerkung Y *ist prim in* $\mathbb{Z}[X, Y]$ *denn* $\mathbb{Z}[X, Y]/(Y) \hookrightarrow \mathbb{Z}[X]$ *ist ein Integritätsring.*
1. Reduktion nach Satz (9.2) mit $p = Y$
$g' = X^4 + 3X^3 + 3 \in \mathbb{Z}[X]$ *modulo* (Y)
2. nach Eisenstein (9.3) ist g' *irred. mit* $p = 3$

(c) Sei p *eine Primzahl und* $\varphi_p(X) := \sum_{i=1}^{p} X^{p-i} \in \mathbb{Z}[X]$
Wir wollen mit Eisenstein zeigen, dass φ_p *irreduzibel ist.*
Wir wissen $\mathbb{Z}[X] \tilde{\to} \mathbb{Z}[Y]$ *sind isomorph, mit* $X \mapsto Y - 1 \ \Rightarrow X + 1 = Y$.
Betrachte also: $\varphi_p(X + 1)$*, es gilt:* $\varphi_p(X)$ *ist genau dann irreduzibel, wenn* $\varphi_p(X + 1)$ *irreduzibel ist. Wenn wir die geometrische Summe auf* φ_p *anwenden, erhalten wir eine einfachere Schreibweise für* φ_p

$$\begin{aligned} \varphi_p(X) &= \sum_{i=1}^{p} X^{p-i} = \frac{X^p - 1}{X - 1} \\ \Rightarrow \varphi_p(X + 1) &= \frac{(X+1)^p - 1}{X} = \frac{1}{X} \left[\left(\sum_{i=0}^{p} \binom{p}{i} X^i \right) - 1 \right] \text{ (Binomische Formel)} \\ &\quad \text{Wir ziehen den Term für } i = 0 \text{ aus der Summe} \\ &\quad \text{und erhalten nach Umsummieren:} \\ &= \sum_{i=1}^{p} \binom{p}{i} X^{i-1} \end{aligned}$$

dies ist ein „Eisensteinpolynom“ (d.h. φ_p *erfüllt das Eisenstein-Kriterium (Satz 9.3)) für* p*, denn* $hK(\varphi_p(X + 1)) = 1$ *und* p *teilt nicht die* 1*. Die anderen Koeffizienten sind* $\binom{p}{i} =: a_i$ *für* $i = 1, \ldots, p - 1$ *und es gilt:* $p|a_i$ *für alle* $i = 1, \ldots, p$*. Der konstante Koeffizient ist* p *und es ist klar, dass* p^2 *nicht* p *teilt. Es folgt also, dass* $\varphi_p(X)$ *irreduzibel in* $\mathbb{Z}[X]$ *ist.*

Definition 9.4 *(Das* p*-te Kreisteilungspolynom)*
Wir nennen φ_p *aus Beispiel 17 (c) das „*p*-te Kreisteilungspolynom“ oder auch zyklotonisches Polynom.*

Beispiel 18 *Sei K ein Körper, und $S := K[T]$, sowie $S[X] = K[T, X]$*
Das Polynom $X^n - T \in S[X]$ ist irreduzibel nach Eisenstein, denn T ist ein Primelement im Ring $S = K[T]$. Betrachte dazu den folgenden Isomorphismus

$$\begin{array}{rcl} R/(T) & \tilde{\to} & K \\ f & \mapsto & f(0) \end{array}$$

Es gilt $T \nmid 1$ und $T^2 \nmid T$ also teilt T alle Koeffizienten von $X^n - T$ ausser hK$(X^n - T) = 1$

Kapitel III

Algebraische Körpererweiterungen

10 Charakteristik

Bemerkung 10.1 *Sei R ein Integritätsring, es gelten:*

(a) Entweder

(i) $n \cdot 1 = \sum_{i=1}^{n} 1 \neq 0$ *für alle* $n \in \mathbb{N}_{>0}$

oder

(ii) es gibt ein minimales $n \in \mathbb{N}_{>0}$*, mit:* $n \cdot 1 = \sum_{i=1}^{n} 1 = 0$*, dann ist* n *eine Primzahl.*

(b) Sei $\varphi_R \in \mathrm{Hom}(\mathbb{Z}, R)$*, dann ist* $\varphi_R(n) = \sum_{i=1}^{n} 1 = n \cdot 1$ *eindeutig bestimmt.*

Im Fall (i) ist $\mathrm{Ker}(\varphi_R) = (0)$
Im Fall (ii) ist $\mathrm{Ker}(\varphi_R) = (n)$

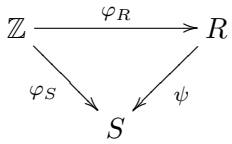
Beweis. zu a):
Wenn n nicht prim ist, also $n = ab$ mit $1 < a < n$, dann gilt, dass $0 = n \cdot 1 = a \cdot (b \cdot 1) = (a \cdot 1)(b \cdot 1)$ ist. Also folgt, da R ein Integritätsbereich ist, dass $a \cdot 1 = 0$ oder $b \cdot 1 = 0$ gelten muss. Dies ist aber ein Widerspruch zur Minimalität von n.
zu b):
(i) $\mathrm{Ker}(\varphi_R) = \{n \in \mathbb{Z} \,|\, n = 0\} = (0)$
(ii) $\mathrm{Ker}(\varphi_R) = (n)$, da $(n) \in Ker(\varphi_R)$ und (n) maximal, sowie $\varphi_R(1) \neq 0$ □

Definition 10.2 *(Charakteristik)*
Die Bezeichnungen seien wie in Bemerkung 10.1. Im Fall (i) setze $\mathrm{Char}(R) = 0$ *und im Fall (ii) setze* $\mathrm{Char}(R) = n$*. Wir nennen* $\mathrm{Char}(R)$ *die Charakteristik von* R

Beispiel 19 *(Cahrakteristik)*
$\mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{C}) = \mathrm{Char}(\mathbb{Q}[X]) = 0$ *und* $\mathrm{Char}(\mathbb{F}_{p^n}) = p$

Bemerkung 10.3 *R, S seien Integritätsringe, es gelten:*
(a) Wenn es einen injektives $\psi \in \mathrm{Hom}(R, S)$ *gibt, dann ist* $\mathrm{Char}(R) = \mathrm{Char}(S)$.
(b) Ist $\mathrm{Char}(R) \neq \mathrm{Char}(S)$*, und R, S Körper, so ist* $\mathrm{Hom}(R, S) = \varnothing$
(c) $\mathrm{Char}(R) = \mathrm{Char}(\mathrm{Quot}(R))$

Beweis. Für den Teil (a) betrachten wir das folgende, kommutierende Diagramm:



Da ψ injektiv ist, gilt $\mathrm{Ker}(\varphi_R) = \mathrm{Ker}(\varphi_S)$, die Behauptung folgt nun aus Bemerkung 10.1 Teil (b). Teil (b) ist klar, denn Körperhomomorphismen sind injektiv.
Für (c) betrachte $\phi \in \mathrm{Hom}(R, \mathrm{Quot}(R))$ mit $\phi(r) = \frac{r}{1}$ aus Bemerkung 5.10. Wir wissen, dass ϕ injektiv ist, mit Teil (a) folgt nun die Behauptung. □

Bemerkung 10.4 *R sei Integritätsring, dann gelten*
(a) Ist $\mathrm{Char}(R) = 0$, dann ist $\varphi_R \in \mathrm{Hom}(\mathbb{Z}, R)$ injektiv.
(b) Ist $\mathrm{Char}(R) = p > 0$, dann gibt es genau ein injektives $\chi \in \mathrm{Hom}(\mathbb{F}_p, R)$
(c) Ist $\mathrm{Char}(R) = 0$ und R ein Körper, dann gibt es genau ein injektives $\xi \in \mathrm{Hom}(\mathbb{Q}, R)$

Anmerkungen
zu (b): Ist R ein Körper, dann ist $\mathbb{F}_p$ der kleinste Teilkörper von R.
zu (c): $\mathbb{Q}$ ist der kleinste Teilkörper von R.
Definition Der kleinste Teilkörper eines Körpers heißt Primkörper.

Definition und Bemerkung 10.5 *(Frobenius-Automorphismus)*
(a) Sei R ein Integritätsring mit $\mathrm{Char}(R) = p > 0$. Dann ist die folgende Abbildung ein Ringhomomorphismus:

$$\begin{aligned} \mathrm{Frob} : R &\to R \\ x &\mapsto x^p \end{aligned}$$

(b) Sei K ein Körper mit $\mathrm{Char}(K) = p$, dann ist $\mathrm{Frob} \in \mathrm{Aut}(K, K)$.
Wir nennen Frob den Frobenius-Automorphismus.

Beweis. zu (a):
Klar sind zunächst zwei Eigenschaften von Ringhomomorphismen $\mathrm{Frob}(xy) = \mathrm{Frob}(x) \cdot \mathrm{Frob}(y)$ und $\mathrm{Frob}(1) = 1$. Wir betrachten $\mathrm{Frob}(x + y)$ genauer:

$$\begin{aligned} \mathrm{Frob}(x+y) &= (x+y)^p \\ &= x^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} \right) + y^p \\ &= x^p + y^p \qquad \text{nach Beispiel 18} \\ &= \mathrm{Frob}(x) + \mathrm{Frob}(y) \end{aligned}$$

zu (b):
Nach (a) ist Frob ein Homomorphismus, also $\mathrm{Frob} \in \mathrm{Hom}(K, K)$. Da Körperhomomorphismen injektiv sind ist Frob injektiv und, weil K ein endlicher Körper ist, ist Frob auch surjektiv. □

Bemerkung 10.6 *Sei K ein Körper, mit $\mathrm{Char}(K) = p > 0$, Dann ist $M := \{ x \in K \mid x^p = x \} \cong \mathbb{F}_p$*

Beweis. Nach Bemerkung 10.4 gibt es ein injektiven $\chi \in \mathrm{Hom}(\mathbb{F}_p, K)$.
Für $a \in \mathbb{F}_p$ gilt $a^p = a$, denn $a = 0 \Rightarrow a^p = 0$ Sei nun $\alpha \in \mathbb{F}_p^\times = \mathbb{F}_p \backslash \{0\}$, dann gilt: $a^{p-1} = 1$, da $\mathrm{Card}(\mathbb{F}_p^\times) = p - 1$ und $\mathbb{F}_p^\times$-Gruppe (verwende den kleinen Fermat der Gruppentheorie (3.10))
Es gilt also $\mathrm{Im}(\chi) \subseteq M$
Weiter ist $\mathrm{Card}(M) \leq p$, denn $x \in M$ ist Nullstelle des Polynoms $X^p - X \in K[X]$ und nach Bemerkung 8.12 hat $X^p - X$ höchstens p-Nullstellen. Es gilt daher $\mathrm{Card}(\mathrm{Im}(\chi)) = \mathrm{Card}(\mathbb{F}_p)$. Also ist χ bijektiv. □

11 Algebraische Körpererweiterungen

Definition 11.1 *(Körpererweiterung und der Grad von L über K)*
Seien K, L Körper. Ist $K \subseteq L$, dann sagen wir L ist „Erweiterungskörper" oder „Körpererweiterung" von K (Notation: L/K sprich: „L über K"). Vermöge der Abbildung

$$\begin{aligned} K \times L &\to L \\ (x, y) &\mapsto x \cdot y \end{aligned}$$

wird L zu einem K-Vektorraum. Den Grad von L über K definieren wir durch

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

Ist $[K : L] < \infty$, so heißt L/K endliche Körpererweiterung.

Beispiel 20 *(Körpererweiterungen)*
$\mathbb{C}/\mathbb{R}$: $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = 2 \qquad (\mathbb{C} \cong \mathbb{R}^2)$
$\mathbb{R}/\mathbb{Q}$: $[\mathbb{R} : \mathbb{Q}] = \infty$, *denn $\mathbb{Q}$ ist abzählbar und $\mathbb{R}$ ist überabzählbar.*

Satz 11.2 *(Gradsatz)*
Seien $M/L/K$ Körpererweiterungen. Es gilt:

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

Beweis. Wir betrachten zunächst den Sonderfall, dass die Körpererweiterungen M/L und L/K endlich sind mit $[M : L] = n, [L : K] = m$, dann lassen sich M und L als direkte Summen schreiben:

$$M = \bigoplus_{i=1}^{n} L := L^{[M:L]} \quad \wedge \quad L = \bigoplus_{i=1}^{m} K := K^{[L:K]}$$

Es gilt also

$$M = \left(K^{[L:K]}\right)^{[M:L]} = K^{[L:K][M:L]}$$

Wir betrachten nun den Fall, dass $[M : L] = \infty$ ist. Dann gibt es $x_1, \ldots, x_i, \ldots \in M$ so dass die Menge $\{x_1, \ldots, x_i, \ldots\}$ L-linearunabhängig ist. Diese ist aber auch K-linearunabhängig also ist der Grad von M über K nicht endlich ($[M : K] = \infty$).
Der letzte Fall ist trivial, denn sei $[L : K] = \infty$, dann ist $[M : K] = \dim_K(M) = \infty$, denn $L \subseteq M$
□

Folgerung 11.3 *Es sei L/K eine Körpererweiterung vom Grad $[L:K]=p$ wobei p eine Primzahl ist. Dann ist jeder Körper M mit $K \subseteq M \subseteq L$ gleich K oder gleich L.*

Beweis. Nach dem Gradsatz 11.2 gilt, dass $[L:K]=[L:M][M:K]=p$ ist. Da p eine Primzahl ist muss $[L:M]=1$ oder $[M:K]=1$ gelten, also $M=L$ oder $M=K$ □

Definition und Bemerkung 11.4 *(algebraische Elemente)*
Sei L/K eine Körpererweiterung und $\alpha \in L$ ein Element.
α heißt genau dann algebraisch über K, wenn es ein $0 \neq f \in K[X]$ gibt mit $f(\alpha)=0$. Diese Aussage ist äquivalent dazu, dass $\varphi_\alpha \in \mathrm{Hom}(K[X],L)$ mit $f \mapsto f(\alpha)$ nich injektiv ist. Ist $\alpha \in L$ nicht algebraisch über K, dann heißt α transzenent über K.

Beweis. Wir wollen zeigen, dass die beiden Aussagen tatsächlich äquivalent sind.
„⇒“ $f \neq 0$ und $f \in \mathrm{Ker}(\varphi_\alpha)$ daher ist φ_α nicht injektiv.
„⇐“ φ_α nicht injektiv, also gibt es ein $f \neq 0 \wedge f \in \mathrm{Ker}(\varphi_\alpha)$ dieses erfüllt die Bedingung $f(\alpha)=0$
□

Beispiel 21 *(Algebraische / transzendente Elemente)*
Wir betrachten Elemente aus $\mathbb{R}$ über $\mathbb{Q}$:
$\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn $\sqrt{2}$ ist Nullstelle von $f(X) := X^2-2 \in \mathbb{Q}[X]\backslash\{0\}$.
$\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$, denn es gibt kein Polynom aus $\mathbb{Q}[X]\backslash\{0\}$, dass die Nullstelle π hat.

Definition 11.5 *(algebraisch abhängige Elemente)*
Sei L/K eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n$ Elemente aus L.
$\alpha_1, \ldots, \alpha_n$ heißen genau dann algebraisch abhängig über K, wenn es ein $f \in K[x_1,\ldots,x_n]\backslash\{0\}$ mit der Eigenschaft $f(\alpha_1, \ldots, \alpha_n)=0$ gibt, also genau dann, wenn $\varphi \in \mathrm{Hom}(K[X_1,\ldots,X_n],L)$, mit $\varphi(f)=f(\alpha_1, \ldots, \alpha_n)$ nicht injektiv ist.
Sind $\alpha_1, \ldots, \alpha_n \in L$ nicht algebraisch abhängig, so heißen sie algebraisch unabhängig. Verkürzt schreiben wir a.u. (analog zu l.u. für linear unabhängig).

Beispiel 22 *Obwohl π - wie in Beispiel 21 gesehen - über $\mathbb{Q}$ transzendent ist, sind $\{\pi,\pi^2\}$ algebraisch abhängig über $\mathbb{Q}$, denn $f(X,Y)=X^2-Y$ erfüllt die Bedingung $f(\pi,\pi^2)=0$.*

Definition 11.6 *(algebraische Körpererweiterungen)*
Sei L/K eine Körpererweiterung. Diese heißt genau dann algebraische Körpererweiterung, wenn alle $\alpha \in L$ algebraisch über K sind. Ansonsten heißt L/K transzendent (Also wenn es ein $\alpha \in L$ gibt, welches über K transzendent ist, gibt.)

Beispiel 23 *$\mathbb{C}/\mathbb{R}$ ist algebraisch, denn für alle $z=a+ib \in \mathbb{C}$ ist z eine Nullstelle von f mit $f=(X-(a+ib))(X-(a-ib))=X^2-2aX+a^2+b^2 \in \mathbb{R}[X]$*
Betrachte: $K(T)=\mathrm{Quot}(K[T])$ Dann ist $K(T)/K$ transzendent, denn T ist nicht algebraisch über K, da die folgende Abbildung φ_T injektiv ist.

$$\begin{array}{rccc} \varphi_T: & K[X] & \to & K(T) \\ & \sum a_n X^n & \mapsto & \sum a_n T^n \end{array}$$

Definition und Bemerkung 11.7 *(Minimalpolynom von α)*
Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K, dann existiert ein eineutiges normiertes Polynom $f_\alpha \in K[X]$, so dass $(f_\alpha)=\mathrm{Ker}(\varphi_\alpha) \trianglelefteq K[X]$ ist.
Wir nennen f_α das „Minimalpolynom“ von α über K.

Beweis. Der Kern von φ_α ist ein Primideal, denn der Faktorring ${}^{K[X]}\!/_{\mathrm{Ker}(\varphi_\alpha)} \subseteq L$ ist ein Integritätsbereich. Weiter ist $K[X]$ ein Hauptidealring also hat $\mathrm{Ker}(\varphi_\alpha)$ einen (bis auf Assoziiertheit eindeutigen) Erzeuger. Setze $\mathrm{Ker}(\varphi_\alpha) =: (f_\alpha)$. Insbesondere ist (f_α) nach Bemerkung 6.4 ein Maximalideal und somit ist f_α irreduzibel. Die Eindeutigkeit folgt durch die Normierung. □

Definition 11.8 *(Teilkörper, K adjungiert α)*
L/K sei eine Körpererweiterung und $\alpha \in L$ ein Element. Wir setzen:

$$K[\alpha] := \left\{ \sum_{i=1}^{n} c_i \alpha^i \mid n \in \mathbb{N} \wedge c_0, \ldots, c_n \in K \right\}$$

$K[\alpha]$ ist der kleinste Ring der zwischen K und L liegt und der α enthält.
$K(\alpha) := \mathrm{Quot}(K[\alpha])$ heißt der von K und α erzeugte Teilkörper von L.
Wir sagen auch „K adjungiert α“ bzw. „K - alpha“.

Bemerkung 11.9 *L/K sei eine Körpererweiterung und $\alpha \in L$ sei algebraisch über K, dann induziert der Homomorphismus*

$$\begin{aligned} \varphi_\alpha : K[X] &\to L \\ f &\mapsto f(\alpha) \end{aligned}$$

einen Körper Isomorphismus zwischen ${}^{K[X]}\!/_{(f_\alpha)}$ und $K[\alpha]$ wobei f_α das Minimalpolynom von α über K ist.
Insbesondere ist dann $K[\alpha] = K(\alpha)$. Sei $\deg(f_\alpha) =: d$, dann ist die Menge $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ eine K-Basis von $K[\alpha]$. Daher gilt weiter

$$[K[\alpha] : K] = \deg(f_\alpha) = d$$

Beweis. *Sei $f_\alpha = \sum_{n=0}^{d} b_n x^n$ Es ist zu zeigen, dass $\alpha^{-1} \in K[\alpha]$ liegt.*

$$\begin{aligned} 0 &= \alpha^d + b_{d-1}\alpha^{d-1} + \ldots + b_1\alpha^1 + b_0 \\ \Leftrightarrow -b_0 &= \alpha\left(\alpha^{d-1} + b_{d-1} + \ldots + b_1\right) \\ \Leftrightarrow \alpha^{-1} &= -\frac{1}{b_0}(\alpha^{d-1} + b_{d-q}\alpha^{d-2} + \ldots + b_1) \end{aligned}$$

denn $b_0 \neq 0$, sonst wäre $f_\alpha = X \cdot \left(\sum_{n=1}^{d} b_n X^{n-1}\right)$, aber dann wäre das Minimalpolynom von α nicht irreduzibel. Dies ist ein Widerspruch. □

Bemerkung 11.10 *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Betrachte den K-Vektorraum-Homomorphismus:*

$$\begin{aligned} l_\alpha : L &\to L \\ \beta &\mapsto \alpha\beta \end{aligned}$$

dann ist f_α das aus der linearen Algebra bekannte Minimalpolynom von l_α.

Beweis. Die Summe über die $a_n \cdot \alpha^n$ ist genau dann Null, wenn $\sum a_n \, l_\alpha^n$ die Nullabbildung ist. Es gilt

$$\sum a_n \, l_\alpha^n(\beta) = \sum a_n \, \alpha^n(\beta) = 0 \quad \text{für alle } \beta \in L$$

□

Bemerkung 11.11 *Jede endliche Körpererweiterung ist algebraisch.*

Beweis. Sei $[L : K] = n \in \mathbb{N}$ und $\alpha \in L$.
Wir müssen zeigen, dass α algebraisch über K ist. Es gilt $\{1, \alpha, \ldots, \alpha^n\}$ ist K-linear abhängig, da $\dim_K(L) = n$. D.h. es existieren $c_0, \ldots c_n \in K$ mit

$$\sum_{i=1}^{n} c_i \, \alpha^i = 0$$

also hat $f = \sum_{i=0}^{n} c_i x^i$ die Nullstelle α. Somit erfüllt jedes $\alpha \in L$ die Bedingung aus Definition 11.4.
□

Folgerung 11.12 *Sei L/K eine Körpererweiterung und $\alpha \in L$ ein algebraisches Element, dann ist $K(\alpha)/K$ algebraisch, denn $[K(\alpha)/K] = \deg(f_\alpha) < \infty$* □

Definition 11.13 *(endliche erzeugte Körpererweiterungen)*
Es seien L/K eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Wir setzen

$$K[S] := \{\, f(\alpha_1, \ldots, \alpha_n) \,|\, n \in \mathbb{N} \wedge f \in K[x_1, \ldots, x_n] \wedge \alpha_1, \ldots, \alpha_n \in S \,\}$$

$K[S]$ isr der kleinste Ring mit den Eigenschaften zwischen K und L zu liegen und S zu enthalten.
Weiter definieren wir $K(S) := \mathrm{Quot}(\, K[S]\,)$
Ist $\mathrm{Card}(S) = n < \infty$, dann gilt: $K(S) = K(\alpha_1, \ldots, \alpha_n)$
$K(\alpha)$ heißt einfach, und $K(S)$ heißt enlich erzeugt, wenn S endlich ist.

Beispiel 24 $\mathbb{C} = \mathbb{R}(i)$ *mit* $i^2 = -1$ *ist einfach.*

Satz 11.14 *Sei L/K eine Körpererweiterung und die Elemente $\alpha_1, \ldots, \alpha_n \in L$ algebraisch über K, dann ist $K(\alpha_1, \ldots, \alpha_n)$ eine algebraische Körpererweiterung von K.*

Beweis. Bemerke: Analog zum Polynomring gilt:

$$K(\alpha_a, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$$

Nach dem Gradsatz 11.2 gilt die folgende Gleichung

$$[K(\alpha_1, \ldots \alpha_n) : K] = [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots \alpha_{n-1})] \cdot [K(\alpha_1, \ldots, \alpha_{n-1}) : K]$$

Nach Induktion folgt, dass $K(\alpha_1, \ldots, \alpha_n)$ endlich und somit algebraisch ist. □

Folgerung 11.15 *Sei L/K eine Körpererweiterung, dann sind äquivalent:*
(i) L/K ist endlich (d.h. $[L : K] < \infty$)
(ii) L/K ist endlich und algebraisch
(iii) L/K wird von endlich vielen algebraischen Elementen erzeugt.

Beweis. Der Schluss von (i) auf (ii) ist nach Bemerkung 11.11 klar, und der soeben bewiesene Satz 11.14 gibt uns den Schluss von (iii) auf (i). Betrachten wir den Schluss von (ii) auf (iii): Bilde hierzu mit $\alpha \in L \backslash K$ den Zwischenkörper $K(\alpha)$. Es gilt

$$K \subsetneq K(\alpha) \subseteq L \text{ also } [L:K] = [L:K(\alpha)] \cdot [K(\alpha):K] \text{ und } [L:K(\alpha)] < [L:K]$$

Setze nun induktiv fort. □

Bemerkung 11.16 *Sei L/K eine Körpererweiterung, dann sind äquivalent:*
(i) L/K ist algebraisch
(ii) L wird über K von algebraischen Elemnten erzeugt.

Beweis. „(i) $\Rightarrow$ (ii)“
L wird über K von L erzeugt (d.h. $L = K(L)$). Nach Vorraussetzung ist jedes Element aus L algebraisch über K.
„(ii) $\Rightarrow$ (ii)“
Seien $\alpha \in L$ und S eine Menge algebraischer Elemente, mit der Eigenschaft: $K(S) = L$. Dann gibt es enlich viele Elemente aus S, die linearkombiniert α ergeben. In Formeln: Es gibt $s_1, \ldots, s_n \in S$ hierzu $k_i \in K$ mit

$$\sum_{i=1}^{n} k_i \cdot \underbrace{\tilde{s}_1^i \cdot \ldots \cdot \tilde{s}_m^i}_{=: s_i \in S} \;=\; \sum_{i=1}^{n} k_i s_i \;=\; \alpha$$

Formell heißt das, dass es ein $f \in K[X_1 \ldots, X_n]$ gibt, so dass $f(s_1, \ldots, s_n) = \alpha$. Daher ist α bereits in $K(s_1, \ldots, s_n)$ enthalten. Dies ist aber eine endliche Erweiterung über K, daher algebraisch. Da α beliebig war, und α nach obigem Beweis algebraisch ist folgt, dass L/K algebraisch ist. □

Definition 11.17 *(Der algebraische Abschluss von K in L)*
Sei L/K eine Körpererweiterung, dann heißt

$$M := \{\, \alpha \in L \,|\, \alpha \text{ algebraisch über } K \,\}$$

der algebraische Abschluss von K in L.

Folgerung 11.18 *Seien alle Bezeichnungen wie in Definition 11.17. Es gelten:*
(i) M ist Körper
(ii) M/K ist eine algebraische Körpererweiterung.

Beweis. Zu (i):
Seien $\alpha, \beta \in M$. Es gilt: $K(\alpha, \beta)$ ist algebraisch über K. Hieraus folgt, dass $K(\alpha, \beta)$ in M enthalten ist. Insbesondere gilt daher, dass die Elemente $\alpha - \beta, \alpha \cdot \beta^{-1} \in K(\alpha, \beta)$ in M enthalten ist. Somit ist M ein Körper.
Zu (ii) ist nichts zu zeigen, denn dies war der Inhalt von Definition 11.6 □

Beispiel 25 *(Algebraischer Abschluss von $\mathbb{Q}$ in $\mathbb{C}$)*
Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{Q}$ und setzen $\bar{\mathbb{Q}} := \{ x \in \mathbb{C} \mid x$ algebraisch über $\mathbb{Q} \}$. Dann ist $\bar{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Es gelten:
(1) $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$, denn
seien $n \in \mathbb{N}$ und p prim. Das Polynom $X^n - p \in \mathbb{Q}[X]$ ist irred. nach Eisenstein. Da $\bar{\mathbb{Q}}$ algebraischer Abschluss in $\mathbb{C}$ ist, enthält $\bar{\mathbb{Q}}$ die Nullstellen von $X^n - p$. Sei also $\alpha^n - p = 0$, für $\alpha \in \mathbb{C}$, dann gilt: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^n - p) = n$, denn $X^n - p$ ist irreduzibel. Da $n \in \mathbb{N}$ beliebig und $\bar{\mathbb{Q}} \supseteq \mathbb{Q}(\alpha)$ kann $\bar{\mathbb{Q}}/\mathbb{Q}$ nicht endlich sein.
(2) $\bar{\mathbb{Q}}$ ist abzählbar, denn aus $\mathbb{Q}$ ist abzählbar folgt $\mathbb{Q}[X]$ abzählbar.
Damit sind die Nullstellen aller Polynome in $\mathbb{Q}[X]$ abzählbar.
(3) Da $\mathbb{C}$ überabzählbar ist, gibt es überabzählbar viele transzendente Elemente in $\mathbb{C}$

Satz 11.19 *Seien $M/L/K$ Körpererweiterungen, dann gelten:*
(a) Sei $\alpha \in M$ algebraisch über L und L/K algebraisch, dann ist α algebraisch über K.
(b) M/K ist genau dann algebraisch , wenn M/L und L/K algebraisch sind.

Beweis. Zu (a):
Sei $\alpha \in M$ algebrisch über L, dann gibt es ein Minimalpolynom $f_\alpha = \sum_{i=0}^{d} a_i X^i \in L[X]$ zu α. Da L/K algebraisch ist gilt: $K(a_o, \ldots, a_d)$ ist endlich. Also folgt mit Dem Gradsatz 11.2

$$[K(a_0, \ldots, a_d)(\alpha) : K] = [K(a_0, \ldots, a_d)(\alpha) : K(a_0, \ldots, a_d)] \cdot [K(a_0, \ldots, a_d) : K] < \infty$$

Also ist α algebraisch über K.
Zu (b):
Die Richtung „$\Rightarrow$“ ist trivial. Zu „$\Leftarrow$“:
Sei $\alpha \in M$. Nach Voraussetzung ist α algebraisch über L. Mit (a) folgt dann sofort die Behauptung.
□

12 Der algebraische Abschluss

Bemerkung 12.1 *Es sei K ein Körper und $f \in K[X]$ mit $\deg(f) \geq 1$, dann gibt es eine Körpererweiterung L/K und ein Element $\alpha \in L$ mit $f(\alpha) = 0$.*

Beweis. O.B.d.A. sei f irreduzibel (sonst betrachte einen irreduziblen Faktor von f).
Es gilt: $(f) \trianglelefteq K[X]$ ist ein Maximalideal. Betrachte die Abbildung $\phi \in Hom(K, L)$

$$\phi : K \xrightarrow{\iota} K[X] \xrightarrow{\pi} {}^{K[X]}\!/_{(f)} =: L$$

Wobei ι die natürliche Inklusion und π die natürliche Projektion sind.
Wir führen die Bezeichnungen $\alpha := \pi(X)$ und $f(X) =: \sum_{n=0}^{d} b_n X^n$ ein. Mit diesen gilt dann

$$f(\alpha) = \sum_{n=0}^{d} b_n \pi(X)^n = \pi\left(\sum_{n=0}^{d} b_n X^n\right) = \pi(f) = 0_L$$

□

Definition 12.2 *(algebraisch abgeschlossen)*
Sei K ein Körper. K heißt genau dann algebraisch abgeschlossen, wenn es für alle $f \in K[X]$ mit $\deg(f) \geq 1$ ein $k \in K$ mit der Eigenschaft $f(k) = 0$ gibt. Diese Definition ist äquivalent dazu, dass jedes Polynom f über K in Lienarfaktoren zerfällt, also dass es für alle $f \in K[X]$ ein $c \in K^\times$ und $\alpha_1, \ldots, \alpha_n \in K$ gibt, so dass sich f darstellen lässt als $f(X) = c \cdot (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$

Bemerkung 12.3 *Sei K ein Körper, dann sind äquivalent:*
(i) K ist algebraisch abgeschlossen.
(ii) Es gibt keine algebraische Körpererweiterung L/K mit $L \neq K$.

Beweis. „(i) $\Rightarrow$ (ii)“:
Sei L/K algebraisch und $\alpha \in L$, sei weiter $f_\alpha \in K[X]$ das Minimalpolynom von α. Nach Voraussetzung liegen alle Nullstellen von f_α bereits in K, also liegt auch α bereits in K und daher folgt $K = L$
„(ii) $\Rightarrow$ (i)“:
Sei $f \in K[X]$ irreduzibel mit $\deg(f) \geq 1$, dann ist $L := {}^{K[X]}\!/_{(f)}$ ein algebraischer Erweiterungskörper von K. Das heißt nach Vorraussetzung ist $L = K$ und somit gilt: $[L : K] = \deg(f) = 1$ also hat f bereits in K eine Nullstelle. □

Bemerkung 12.4 *Sei K ein Körper. Es gibt eine Körpererweiterung L/K, so dass jedes $f \in K[X]$ mit $\deg(f) \geq 1$ eine Nullstelle in L hat.*

Beweis. Wir definieren uns zunächst eine Hilfsmenge

$$M := \{\, f \in K[X] \mid \deg(f) \geq 1 \,\}$$

Dann führen wir noch Notationen zur Vereinfachung der Schreibweise ein. Wir schreiben $\underline{X}$ für das $\sharp M$-Tupel von X-en und setzen $R := K[X_f \mid f \in M]$[1]. Sei nun $\mathfrak{a} = (f(X_f) \mid f \in M) \trianglelefteq R$ das heißt $\mathfrak{a}$ wird von allen $f(X_f)$ erzeugt.

Behauptung 1 $\mathfrak{a} \neq R$ *Mit anderen Worten:* $1 \notin \mathfrak{a}$

Beweis. Wir führen einen Beweis per Widerspruch und nehmen daher an, dass $1 \in \mathfrak{a}$ gelte. Daraus folgt nun, dass es $f_1, \ldots, f_n \in M$ und $g_1, \ldots, g_n \in R$ gibt, so dass sich 1 darstellen lässt als

$$1 \quad = \quad \sum_{i=1}^{n} g_i(\underline{X}) \cdot f_i(X_{f_i}) \tag{12.1}$$

Sei K'/K eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in K'$ Elemente gerade so gewählt, dass $f_i(\alpha_i) = 0$ ist für alle $i = 1, \ldots, n$. Ein solches K' existiert nach Bemerkung 12.1. Nun ersetze für $i = 1, \ldots, n$ die X_{f_i} in Gleichung (12.1) durch α_i und 0 sonst. Wir erhalten:

$$1 = \sum_{i=1}^{n} g_i(\underline{X})\, f_i(\alpha_i) = 0$$

Dies ist ein offensichtlicher Widerspruch, also war unsere Annahme falsch. △
Aus der Behauptung folgt, dass es ein Maximalideal $\mathfrak{m} \trianglelefteq R$ mit $\mathfrak{a} \subseteq \mathfrak{m}$ gibt.

[1] $R := K[X_f \mid f \in M]$ heißt in Worten: R ist der Polynomring in sovielen Variablen, wie es Elemente in M gibt.

Setze nun $L := {}^{R}\!/_{\mathfrak{m}}$. Dies ist eine Körpererweiterung von K und L/K erfüllt die Forderung, denn sei $f \in K[X]$ mit $\deg(f) \geq 1$ dann betrachte die natürliche Projektion

$$\pi : R \to {}^{R}\!/_{\mathfrak{m}}$$

Setze nun $\alpha := \pi(X_f)$ und vergleiche mit dem Beweis zu Bemerkung 12.1. □

Satz 12.5 *Zu jedem Körper gibt es einen algebraisch abgeschlossenen Erweiterungskörper.*

Beweis. Sei K ein Körper dann setze $K_0 := K$. Definiere K_{i+1} als den Körper L_i (zu K_i) aus Bemerkung 12.4. Setze:

$$L := \bigcup_{i=0}^{\infty} K_i$$

Dieser Körper erfüllt Die Forderung, denn Sei $f \in L[X]$ mit $\deg(f) \geq 1$. Wir wissen, dass es ein n mit der Eigenschaft $f \in K_n[X]$ gibt. Da jeder der (endlich vielen) Koeffizienten in einem K_m liegt, setze $n := \max\{m\}$, dann hat f eine Nullstelle in $K_{n+1} \subseteq L$. □

Beispiel 26 *Ist L/K eine algebraische Körpererweiterung und $\alpha \in L$ ein Element, dann Betrachte:*

$$\begin{array}{rccc} ev_\alpha[X]: & K[X] & \to & L \\ & \sum a_n X^n & \mapsto & \sum a_n \alpha^n \end{array}$$

Offensichtlich ist dann $\mathrm{Ker}(ev_\alpha[X])$ das vom Minimalpolynom von α erzeugte Hauptideal (f_α) . Aus dem Homomorphiesatz folgt nun:

$${K[X]}\!/_{(f_\alpha)} \tilde{\to} \mathrm{Im}(f_\alpha) \;=\; K(\alpha) \subseteq L$$

Beispiel 27 *Wir betrachten $K = \mathbb{Q}, \alpha = \sqrt{2}$*
Das Minimalpolynom von $\sqrt{2}$ ist $f_\alpha = X^2 - 2$ Wie in Beispiel 26 gezeigt, folgt dann

$${\mathbb{Q}[X]}\!/_{(X^2-2)} \tilde{\to} \mathbb{Q}(\sqrt{2})$$

Beispiel 28 *Wir betrachten den Fall $K = \mathbb{Q},\ \zeta_5 := e^{\frac{2}{5}\pi i} \in \mathbb{C}$ mit $(\zeta_5)^5 = 1$.*
Das Minimalpolynom von ζ_5 ist $f_{\zeta_5} = X^4 + X^3 + X^2 + X + 1 = \varphi_5$
φ_5 ist irred. nach Eisenstein und Beispiel 17 (c). Mit dem Homomorphiesatz folgt nun wieder

$${\mathbb{Q}[X]}\!/_{(\varphi_5)} \tilde{\to} \mathbb{Q}(\zeta_5) \subseteq \mathbb{C}$$

Beispiel 29 *(Berechnung des Minimalpolynoms)*
Seien $K := \mathbb{Q}$ und $\alpha := \zeta_3 := e^{\frac{2}{3}\pi i}$
Mit Rechnen sehen wir ein, dass $\alpha^2 = -(1+\alpha)$ und $\alpha^3 = 1$ sind. Das Minimalpolynom von α muss also $(X^3 - 1)$ teilen. eine Polynomdivision mit $(X-1)$ liefert $X^2 + X + 1 =: g$ als einen Faktor von $X^3 - 1$. Da g irreduzibel ist, ist g das Minimalpolynom von α.

Definition 12.6 *(algebraischer Abschluss)*
Sei K ein Körper. Ein algebraisch abgeschlossener Erweiterungskörper L von K heißt algebraischer Abschluss von K, falls L/K algebraisch ist. Wir bezeichnen diese Erweiterungskörper mit $\bar{K}$.

Bemerkung 12.7 *Zu jedem Körper K gibt es einen algebraischen Abschluss.*

Beweis. Wähle eine algebraisch abgeschlossene Körpererweiterung L/K nach Satz 12.5, dann ist $\bar{K} := \{ x \in L \mid x \text{ algebraisch über } K \}$ ein algebraischer Abschluss von K. □

Notation (Algebraischer Abschluss)
- Der algebraische Abschluss von $\mathbb{Q}$ ist $\bar{\mathbb{Q}}$
- Der algebraische Abschluss von $\mathbb{F}_p$ ist $\bar{\mathbb{F}}_p$
- Seien L, K Körper und $\sigma \in \mathrm{Hom}(K, L)$ sowie $f \in K[X]$ mit höchstem Koeffizienten a_d, dann definieren wir

$$(\sigma(f))(X) := f^\sigma(X) := \sum_{n=0}^{d} \sigma(a_n) X^n \in L[X]$$

Definition und Bemerkung 12.8 *(Fortsetzungen von Homomorphismen)*
Sei L/K eine Körpererweiterung und $\alpha \in L$ ein über K algebraisches Element mit Minimalpolynom $f \in K[X]$. Sei weiter $\sigma \in \mathrm{Hom}(K, L)$. Setze $K' := K(\alpha)$. Es gelten:
(i) Ist $\sigma' \in \mathrm{Hom}(K', L)$ mit $\sigma'_{|K} = \sigma$, dann ist $\sigma'(\alpha)$ eine Nullstelle von f^σ
(ii) Für alle Nullstellen β von $\sigma(f)$ gibt es ein $\sigma' \in \mathrm{Hom}(K', L)$ mit $\sigma'_{|K} = \sigma$, so dass $\sigma'(\alpha) = \beta$.
Homomorphismen mit der Eigenschaft (i) nennen wir Fortsetzungen.
(ii) besagt insbesondere: Es gibt genau so viele Fortsetzungen von σ, wie $\sigma(f) = f^\sigma$ Nullstellen hat.

Beweis. Sei $f := \sum_{n=0}^{d} a_n x^n$ gegeben. Zum Beweis von (i) betrachte die folgende Gleichung:

$$\begin{aligned}
[\sigma(f)](\sigma'(\alpha)) &= \sum_{n=0}^{d} \sigma(a_n)(\sigma'(\alpha))^n \\
&= \sum_{n=0}^{d} \sigma'(a_n)(\sigma'(\alpha))^n \quad \text{denn: } \sigma'_{|K} = \sigma \\
&= \sigma'\left(\sum_{n=0}^{d} a_n \alpha^n\right) \qquad \text{denn: } \sigma' \in Hom(K', L) \\
&= \sigma'(0) = 0
\end{aligned}$$

zu (ii): Sei $\beta \in L$ eine Nullstelle von $\sigma(f)$. Wir betrachten:

$$\varphi : K[X] \xrightarrow{g \mapsto \sigma(g)} L[X] \xrightarrow{X \mapsto \beta} L$$

Nach Teil (i) ist $f \in Ker(\varphi)$. Da das Minimalpolynom f irreduzibel ist, ist $(f) \trianglelefteq K[X]$ ein Maximalideal. Weiter gilt $1 \notin (f)$ daher ist $(f) = Ker(\varphi)$. Betrachte die folgende, injektive Abbildung

$$\begin{aligned}
\bar{\varphi} : {}^{K[X]}\!/_{(f)} &\hookrightarrow L \\
X &\mapsto \beta
\end{aligned}$$

Wir wissen ${}^{K[X]}\!/_{(f)} \cong K' := K(\alpha)$, denn die Abbildung

$$\begin{aligned}
\psi : {}^{K[X]}\!/_{(f)} &\to K' \\
X &\mapsto \alpha \\
k &\mapsto k
\end{aligned}$$

ist ein Isomorphismus. Die gewünschte Fortsetzung von σ ist also:

$$\begin{array}{rccc} \sigma' : K' & \xrightarrow{\psi^{-1}} & K[X]/(f) & \xrightarrow{\bar{\varphi}} L \\ \alpha & \mapsto & X & \mapsto \beta \end{array}$$

Nach dieser Konstruktion ist $\sigma'_{|K} = \sigma$. Wir müssen nun noch die Eindeutigkeit beweisen:
Sei hierzu $\{1, \alpha, \ldots, \alpha^{d-1}\}$ eine Basis von K' als K-Vektorraum. Alle $\chi \in \mathrm{Hom}(K', L)$ mit $\chi_{|K} = \sigma$ sind eindeutig gegeben durch:

$$\chi\left(\sum r_s \alpha^s\right) = \sum \sigma(r_s)(\chi(\alpha))^s$$

□

Satz 12.9 *Es seien K'/K eine algebraische Körpererweiterung und L ein algebraischer abgeschlossener Körper. Weiter sei $\sigma \in \mathrm{Hom}(K, L)$. Es gelten:*
(a) σ besitzt eine Fortsetzung $\sigma' \in \mathrm{Hom}(K', L)$
(b) Ist $K' = \bar{K}$ und die Erweiterung $L/\mathrm{Im}(\sigma)$ algebraisch, dann ist jede Fortsetzung σ' von σ ein Element in $\mathrm{Iso}(K', L)$.

Beweis. Zu (a):
Ist K' endlich folgt die Behauptung direkt aus Definition 12.8. Ansonsten betrachte die folgende Hilfsmenge:

$$M := \{\, (F, \tau) \,|F \text{ ist Zwischenkörper von } K \text{ und } K' \text{ und } \tau \in \mathrm{Hom}(F, L) \text{ ist Fortsetzung von } \sigma \,\}$$

Es gibt eine Halbordnung auf M, gegeben durch

$$(F_1, \tau_1) \leq (F_2, \tau_2) :\Leftrightarrow F_1 \leq F_2 \wedge \tau_{2|F_1} = \tau_1$$

Weiter ist M nicht leer, da $(K, \sigma) \in M$ und Jede halbgeordnete Kette $(F_1, \tau_1) \leq \ldots \leq (F_n, \tau_n) \leq \ldots$ besitzt eine obere Schranke, nämlich

$$(F, \tau) \text{ mit } F := \bigcup_{i \in I} F_i$$

Hierbei ist $\tau : F \to L$ gegeben durch $\tau(x) = \tau_s(x)$, falls $x \in F_s$. Wir können also Zorns Lemma anwenden, und folgern, dass es ein maximales Tupel (F, τ) gibt. Angenommen: $F \neq K'$, dann gäbe es ein $\alpha \in K' \backslash F$. Es folgte zunächst einmal, dass α algebraisch über K wäre. Betrachte in dieser Situation $F(\alpha) \subseteq K'$. Nach Definition 12.8 gibt es eine Fortsetzung $\tau' \in \mathrm{Hom}(F(\alpha), L)$. Dies widerspricht aber der Folgerung aus Zorns Lemma, dass (F, τ) ein maximales Element in M ist.
Zu (b):
Wähle nach (a) eine Fortsetzung: $\sigma' \in \mathrm{Hom}(K', L)$ von σ. Da σ' ein Körperhomomorphismus ist, hat σ' einen trivialen Kern und bildet isomorph auf sein Bild ab. Wenn aber $\mathrm{Im}(\sigma') \cong K' = \bar{K}$ gilt, dann ist auch $\mathrm{Im}(\sigma')$ algebraisch abgeschlossen. Nach Vorraussetzung ist $L/\mathrm{Im}(\sigma)$ eine algebraische Körpererweiterung. Es gilt: $\mathrm{Im}(\sigma')$ ist Zwischenkörper von L und $\mathrm{Im}(\sigma)$ daher ist nach Satz 11.19 ist $L/\mathrm{Im}(\sigma')$ eine algebraische Körpererweiterung. Nach Definition 12.2 ist dann $L = \mathrm{Im}(\sigma')$. □

Folgerung 12.10 *Seien K ein Körper und K_1, K_2 zwei algebraische Abschlüsse von K, dann gibt es einen Körperisomorphismus $\sigma : K_1 \to K_2$.*

Beweis. Da K ein Unterkörper von K_1 und K_2 ist, ist $id_K \in \mathrm{Hom}(K_1, K_2)$. Nach Satz 12.9 gibt es eine Fortsetzung $\sigma \in \mathrm{Iso}(K_1, K_2)$ von id_K □

Anmerkung Je zwei algebraische Abschlüsse von K sind Isomorph, aber es gibt keine kanonische Wahl des Isomorphismus.

13 Zerfällungskörper

Definition 13.1 *(K-Homomorphismus)*
Sei K ein Körper und L_1/K sowie L_2/K seien Körpererweiterungen.
$\sigma \in \mathrm{Hom}(L_1, L_2)$ heißt K-Homomorphismus, falls σ eingeschränkt auf K die Identität auf K ist, also $\sigma_{|K} = id_K$.
Die Menge der K-Homomorphismen von L_1 nach L_2 heben wir von der Menge aller Homomorphismen zwischen diesen Körpern durch einen Index K ab und bezeichnen sie mit $\mathrm{Hom}_K(L_1, L_2)$.

Beispiel 30 *Sei $\zeta_5 := e^{\frac{2\pi i}{5}} \in \mathbb{C}$, Wir betrachten $\mathbb{Q}(\zeta_5)/\mathbb{Q}$*
Das Minimalpolynom zu ζ_5 ist $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ also ist der Grad der Körpererweiterung $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \deg(f) = 4$
faktorisieren wir f in $\mathbb{C}[X]$, dann erhalten wir folgende Darstellung von f

$$f(X) = (X - \zeta_5) \cdot (X - \zeta_5^2) \cdot (X - \zeta_5^3) \cdot (X - \zeta_5^4)$$

denn $\zeta_5^i \neq \zeta_5^j$ für $i \neq j$. Weiter gilt $(\zeta_5^5)^i = (\zeta_5^i)^5 = 1^i = 1$ Also ist $\zeta_5^i \in \mathbb{C}$ eine Nullstelle von f
In diesem Fall sind alle Nullstellen von f bereits im Erweiterungskörper $\mathbb{Q}(\zeta_5)$ enthalten.

Beispiel 31 *Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$, dann ist $g(X) = X^3 - 2$ das Minimalpolynom von α.*
Damit wir g in $\mathbb{C}[X]$ faktorisieren können brauchen wir $\zeta_3 := e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Es ist

$$g(X) = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})$$

denn $\mathrm{Card}(\{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}) = 3$ und $\left(\zeta_3\sqrt[3]{2}\right)^3 = \zeta_3^3\left(\sqrt[3]{2}\right)^3 = 2$
Da $\zeta_3\sqrt[3]{2}$ keine reelle Zahl ist und wir $\mathbb{Q}(\sqrt[3]{2})$ darstellen können als

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\} \subseteq \mathbb{R}$$

folgt, dass $\zeta_3\sqrt[3]{2}$ nicht im Erweiterungskörper $\mathbb{Q}(\sqrt[3]{2})$ enthalten ist, also nicht alle Nullstellen von g in $\mathbb{Q}(\sqrt[3]{2})$ enthalten sind.

Definition 13.2 *(Zerfällungskörper)*
Seien K ein Körper und I eine Menge. Weiter sei $(f_i)_{i\in I}$ eine Familie von Polynomen mit $f_i \in K[X]$ und $\deg(f_i) \geqslant 1$.
Eine Körpererweiterung L/K heißt Zerfällungskörper der $(f_i)_{i\in I}$, falls:
(a) Jedes f_i über L in Linearfaktoren zerfällt. Also, dass es $\alpha_{i,j} \in L$ und $c \in L$ gibt so dass sich f_i darstellenlässt als

$$c \cdot \prod(X - \alpha_{i,j}) = f_i(X) \in L[X]$$

(b) L wird über K von den Nullstellen der f_i erzeugt.

Beispiel 32 *Wir betrachten $K = \mathbb{Q}$. Ein Zerfällungskörper der Familie $\{X^2 - 3,\, X^2 - 2\}$ ist $\mathbb{Q}(\sqrt{2}, \sqrt{3}) =: L$, denn beide Polynome zerfallen über L in Linearfaktoren.*

$$(X^2 - 2) = (X - \sqrt{2}) \cdot (X + \sqrt{2}) \qquad (X^3 - 3) = (X - \sqrt{3}) \cdot (X + \sqrt{3})$$

Weiter gilt, dass L von $\sqrt{2}$ und $\sqrt{3}$ erzeugt wird.

Beispiel 33 *Ein Zerfällungskörper von $X^3 - 2$ ist $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.*
De Bedingung (a) ist klar nach Beispiel 25. Zur Bedingung (b):
Die Nullstellenmenge von $X^3 - 2$ ist $\{\sqrt[3]{2},\, \zeta_3\sqrt[3]{2},\, \zeta_3^2\sqrt[3]{2}\}$
Wir müssen nun die folgende Gleichheit zeigen

$$\mathbb{Q}(\sqrt[3]{2},\, \zeta_3\sqrt[3]{2},\, \zeta_3^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2},\, \zeta_3)$$

Die „$\subseteq$"-Inklusion ist klar und zur Gegenrichtung betrachte $\zeta_3 = \zeta_3^2\sqrt[3]{2}\zeta_3\sqrt[3]{2}$

Bemerkung 13.3 *(Eindeutigkeit des Zerfällungskörpers)*
Seien die Bezeichnungen wie in Definition 13.2. Wähle $\bar{K}$ einen algebraischen Abschluss von K. Weiter sei $S \subseteq \bar{K}$ die Nullstellenmenge der Familie $(f_i)_{i\in I}$.
(i) Dann ist $K(S)$ ein Zerfällungskörper der Familie $(f_i)_{i\in I}$.
(ii) Ist $L \subseteq \bar{K}$ ein weiterer Zerfällungskörper der $(f_i)_{i\in I}$, dann sind L und $K(S)$ gleich.

Beweis. Zu (i): Die Bedingung 13.2 (a) ist klar und (b) ist durch die Definition von $K(S)$ erfüllt.
Die (ii)-te Aussage ist klar, denn Die Nullstellenmenge im algebraischen Abschluss ist eindeutig bestimmt. □

Satz 13.4 *Seien K und $(f_i)_{i\in I}$ wie in Definition 13.2 gegeben und seien L_1 und L_2 je Zerfällungskörper der Familie $(f_i)_{i\in I}$ sowie $\bar{L_2}$ ein algebraischer Abschluss von L_2.*
Dann gibt jedes $\sigma \in \mathrm{Hom}_K(L_1, \bar{L_2})$ einen K-Isomorphismus $\sigma : L_1 \tilde{\to} L_2$.

Beweis. Wir betrachten drei Fälle:
1. Fall: Sei $\mathrm{Card}(I) = 1$, dann besteht die Familie der $(f_i)_{i\in I}$ aus nur einem Polynom $f := f_1$, wir finden in L_1 eine Darstellung in Linearfaktoren

$$f(X) = c\prod_{n=1}^{d}(X - \alpha_n) \in L_1[X]$$

wobei alle α_n sowie c Elemente aus L_1 sind. Wende nun σ auf f an

$$\sigma(f(X)) = \sigma(c)\prod(X - \sigma(\alpha_n)) \in \bar{L_2}[X]$$

Da L_2 ebenfalls ein Zerfällungskörper von f ist und L_2 ein Unterkörper von $\bar{L_2}$ ist, können wir L_2 beschreiben durch

$$L_2 = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_d)) = \sigma(K(\alpha_1, \ldots, \alpha_d)) = \sigma(L_1)$$

2. Fall: Sei $\mathrm{Card}(I) = n \in \mathbb{N}$, also besteht die Familie der $(f_i)_{i\in I}$ aus nur endlich vielen Polynomen, dann definiere

$$f := \prod_{i\in I} f_i$$

Dann sind der Zerfällungskörper von f und der Zerfällungskörper der Familie $((f_i)_{i\in I})$ gleich. Aus dem ersten Fall folgt nun die Existenz des K-Isomorphismuses.
3. Fall: Sei $\mathrm{Card}(I) = \infty$), dann definiere die Hilfsmenge

$$M := \{\, J \mid J \subseteq I \text{ und } \mathrm{Card}(J) < \infty \,\}$$

Jeder Zerfällungskörper der Familie der $(f_i)_{i\in I}$ lässt sich darstellen als Vereinigung über aller Zerfällungskörper der Familien $(f_j)_{j\in J}$ mit $J \in M$. Aus (2) folgt dann die Behauptung. □

Folgerung 13.5 *Seien K und die Familie $(f_i)_{i\in I}$ wie in Definition 13.2 gegeben, dann sind je zwei Zerfälungskörper der Familie $(f_i)_{i\in I}$ K-Isomorph.*

Beweis. Seien L_1 und L_2 zwei Zerfällungskörper der Familie der $(f_i)_{i\in I}$ und $\bar{L_2}$ ein algebraischer Abschluss von L_2. Nach Satz 12.9 lässt sich die Inklusion $\iota : K \to \bar{L_2}$ fortsetzen zu $\sigma : L_1 \to \bar{L_2}$ und mit Satz 13.4 folgt dann sofort die Behauptung. □

Anmerkung Der Isomorphismus aus Folgerung 13.5 ist nicht kanonisch.

Definition und Satz 13.6 *(normale Körpererweiterung)*
Sei L/K eine algebraische Körpererweiterung, dann sind äquivalent:

(i) Für alle K-Homomorphismen $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, wobei $\bar{L}$ ein algebraischer Abschluss von L ist, gilt $\sigma \in \mathrm{Aut}_K(L, L)$, genauer:
Ist $\iota \in \mathrm{Hom}_K(L, \bar{L})$ die natürliche Inklusion, dann gilt: $\mathrm{Im}(\iota) = \mathrm{Im}(\sigma) = L \subseteq \bar{L}$
(ii) L ist ein Zerfällungskörper einer Familie nicht konstanter Polynome in $K[X]$
(iii) Für jedes irreduzible Polynom $f \in K[X]$, dass eine Nullstelle in L hat, gilt:
f zerfällt vollständig in Linearfaktoren.

Sind die Bedingungen (i), (ii) und (iii) erfüllt, dann heißt L/K eine normale Körpererweiterung.

Beweis. Per Ringschluss beginnend mit „(i) ⇒ (iii)“:
Sei $f \in K[X]$ ein irreduzibles Polynom und seien $\alpha \in L$ und $\beta \in \bar{L}$ Nullstellen von f. Nach Bemerkung 12.8 (b) gibt es ein $\sigma \in \mathrm{Hom}_K(K(\alpha), \bar{L})$ derart, dass die Gleichung $\sigma(\alpha) = \beta$ erfüllt ist. Nach Satz 12.9 gibt es eine Fortsetzung $\sigma' \in \mathrm{Hom}_K(L, \bar{L})$ welches die Gleichung $\sigma'(\alpha) = \beta$ ebenfalls erfüllt. Nach Vorraussetzung ist $\sigma'(L) = L$ also liegt insbesondere $\sigma'(\alpha) = \beta$ bereits in L. Das heißt, dass alle Nullstellen von f bereits in L liegen.
Zu „(iii) ⇒ (ii)“:
Da L/K algebraisch ist, gibt es eine Teilmenge $S \subseteq L$ die L erzeugt, also $K(S) = L$. Weiter bezeichne f_s das Minimalpolynom zu $s \in S$. Dann ist L ein Zerfällungskörper der Familie $(f_s)_{s\in S}$, denn jedes Polynom f_s zerfällt nach Vorraussetzung über L in Linearfaktoren und L wird nach Definition von den Nullstellen der f_s erzeugt.
Zu „(ii) ⇒ (i)“:
Sei $(f_i)_{i\in I}$ eine Familie nichtkonstanter Polynome und L ein Zerfällungskörper dieser Familie. Weiter sei $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, dann ist $\sigma(L)$ ebenfalls ein Zerfällungskörper der Familie $((f_i)_{i\in I})$. Nach Bemerkung 13.3 ist sind L und $\sigma(L)$ Teilmengen von $\bar{L}$, also $\mathrm{Im}(\sigma) = \sigma(L) = L$. □

Beispiel 34 *zu Satz 13.6 (i):*
Es sei $\sqrt{2}$ die eindeutige Lösung von $X^2 - 2 = 0$. Wir kennen bereits die natürliche Inklusion:

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

aber es gibt auch folgenden $\mathbb{Q}$-Homomorphismus

$$\begin{array}{rcl} \sigma : \mathbb{Q}(\sqrt{2}) & \to & \mathbb{C} \\ a + \sqrt{2}b & \mapsto & a - \sqrt{2}b \end{array}$$

Es gilt $\mathrm{Im}(\sigma) = \mathrm{Im}(\iota)$, denn

$$\begin{array}{rcl} \mathbb{Q}(\sqrt{2}) \cong {}^{\mathbb{Q}}\!/_{(X^2-2)} & \to & \mathbb{C} \\ X & \mapsto & -\sqrt{2} \end{array}$$

Betrachten wir hingegen $\sqrt[3]{2}$ mit dem Minimalpolynom $f_{\sqrt[3]{2}} = X^3 - 2$ und

$$\begin{array}{rcl} \iota : \mathbb{Q}(\sqrt[3]{2}) & \hookrightarrow & \mathbb{C} \\ \sigma : {}^{\mathbb{Q}[X]}\!/_{(X^3-2)} & \to & \mathbb{C} \\ X & \mapsto & \zeta_3 \sqrt[3]{2} \end{array}$$

In diesem Fall gilt: $\mathrm{Im}(\sigma) \neq \mathrm{Im}(\iota)$.

Beispiel 35 *zu (13.6):*
- Es sei K ein Körper mit algebraischen Abschluss $\bar{K}$, dann ist $\bar{K}/K$ normal.
- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine normale Körpererweiterung.
- $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ ist eine normale Körpererweiterung.
- $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ ist eine normale Körpererweiterung.
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist <u>keine</u>(!) normale Körpererweiterung.

Bemerkung 13.7 *Es seien $M/L/K$ algebraische Körpererweiterungen. Weiter sei M/K normal, dann ist auch M/L normal.*

Beweis. Nach Vorraussetzung ist M ein Zerfällungskörper einer Familie von Polynomen aus $K[X]$. Da diese Familie auch in $L[X]$ enthalten ist, ist M auch Zerfällungskörper einer Familie von Polynomen aus $L[X]$. □

Anmerkung: L/K ist im Allgemeinen keine normale Körpererweiterung. Ein Gegenbeispiel ist der Fall: $M := \bar{\mathbb{Q}}, L := \mathbb{Q}(\sqrt[3]{2}), K := \mathbb{Q}$
Falls M/L und L/K normal sind, gilt im Allgemeinen <u>nicht</u>, dass auch M/K normal ist.

Bemerkung 13.8 *Sei L/K eine Körpererweiterung vom Grad 2, dann ist L/K normal.*

Beweis. Es gilt die Bedingung (ii) aus Satz 13.6, denn für $\alpha \in L \backslash K$ ist der Grad des zugehörigen Minimalpolynoms f_α gleich 2 also ist L ein Zerfällungskörper von f_α, denn nach Polynomdivision $f_\alpha : (X - \alpha) = g$ folgt, dass der Grad von g gleich 1 ist. Also sind alle Nullstellen des Minimalpolynoms f_α bereits Elemente aus L. □

Definition 13.9 *(Die normale Hülle)*
Sei L/K eine algebraische Körpererweiterung. Ein Erweiterungskörper N/L heißt normale Hülle oder normaler Abschluss von L/K, falls:
(i) N/K normal ist, und
(ii) es keinen Teilkörper L' mit $L \subset L' \subsetneq N$ gibt, der über K normal ist.

Satz 13.10 *(Eigenschaften der normalen Hülle)*
Ist L/K eine algebraische Körpererweiterung, dann gelten:

(a) *Es gibt eine normale Hülle N von L/K.*

(b) *Sei $M/L/K$ eine algebraische Körpererweiterung derart, dass M/K normal ist. Dann gilt für jede normale Hülle N von M/L: $N = K(\sigma_i(L)|i \in I)$ mit $(\sigma_i)_{i\in I} = \mathrm{Hom}_K(L, M)$*

(c) *Je zwei normale Hüllen N_1 und N_2 von L/K sind K-Isomorph.*

(d) *Ist die Körpererweiterung L/K von endlichem Grad, so ist auch der Erweiterungsgrad $[N : K]$ endlich.*

Beweis. Teil (a) folgt sofort aus (b) mit $M := \bar{L}$.
Zu (b): Sei $L = K(S)$ mit einer Teilmenge $S \subseteq L$. Seien für alle $s \in S$ die Minimalpolynome mit $f_s \in K[X]$ bezeichnet. Wähle nun einen Zerfällungskörper $N \subseteq \bar{M}$ der Familie der $(f_s)_{s\in S}$, damit ist N/K normal.

Behauptung *N ist eine normale Hülle von L/K.*

Beweis. Wir haben schon gezeigt, dass N normal ist, also bleibt die Bedingung (ii) aus Definition 13.9 zu prüfen:
Sei L'/N eine normale Körpererweiterung mit $L \subseteq L' \subseteq N$, dann zerfallen für alle $s \in S$ die Minimalpolynome f_s über L', denn $f_s(s) = 0$ und $s \in L'$.
Das heißt, dass alle Nullstellen der Polynome der Famile $(f_s)_{s\in S}$ bereits in L' enthalten sind, also ist L' selbst ein Zerfällungskörper der Familie $(f_s)_{s\in S}$
Wir haben bereits gezeigt, dass dann $L' \cong N$ gilt. $\triangle$

Wir müssen noch zeigen, dass $N = K(\sigma_i(L)|i \in I)$ ist.
$\supseteq$ Seien $\sigma \in \mathrm{Hom}_K(L, M)$ und $s \in S$, dann gilt
$\sigma(f_s(s)) = f_s(\sigma(s)) = 0$ also ist $\sigma(s) \in N$ eine Nullstelle des Minimalpolynoms f_s von s. Damit ist $\mathrm{Im}(\sigma) = \sigma(L)$ eine Teilmenge von N.
$\subseteq$ N wird über K von den Nullstellen der $(f_s)_{s\in S}$ erzeugt.
Sei also α eine Nullstelle von einem $f_t \in (f_s)_{s\in S}$. Nach Bemerkung 12.8 (b) existiert ein $\sigma \in \mathrm{Hom}_K(K(S), \bar{M})$ welches die Gleichung $\sigma(t) = \alpha$ erfüllt.
Setze σ fort zu $\sigma' \in \mathrm{Hom}(L, \bar{M})$ mit $\sigma'(t) = \alpha$.
Da M/K normal ist, ist $\sigma' \in \mathrm{Hom}(L, M)$, also ist $\alpha \in \mathrm{Im}(\sigma')$ einer Teilmenge von $K(\sigma_i(L)|i \in I)$

Zu d) Ist der Körpergrad $[L : K]$ endlich, dann gibt es eine endliche Teilmenge $S \subseteq L$ mit $L = K(S)$ und N ist Zerfällungskörper von nur endlich vielen Polynomen, nämlich den Minimalpolynomen der $s \in S$. Daher ist auch $[N : K]$ endlich.

Zu c) Die Körper N_1 und N_2 sind Zerfällungskörper der Familie $(f_s)_{s\in S}$ damit sind N_1 und N_2 nach Folgerung 13.5 K-Isomorph. $\square$

14 Separable und Inseparable Körpererweiterungen

Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom, weiter seien $\bar{K}/K$ ein algebraischer Abschluss, sowie $\alpha \in \bar{K}$ eine Nullstelle von f und M die Menge der Nullstellen von f in $\bar{K}$. Betrachte die folgende Abbildung:

$$\begin{array}{rcll} \varphi : M & \to & \mathrm{Hom}_K(K(\alpha), \bar{K}) & \\ \beta & \mapsto & \sigma & \text{mit } \sigma(\alpha) = \beta \end{array}$$

Da diese Zuordnung nach Bemerkung 12.8 (b) eindeutig ist folgt sofort, dass φ bijektiv ist.

Beispiel 36 *Seien $\mathbb{F}_p(T) := Quot(\mathbb{F}_p[T])$ und p eine Primzahl, dann betrachte das Polynom $f(X) := X^p - T \in \mathbb{F}_p(T)[X]$. Nach dem Eisensteinkriterium[2] ist f irreduzibel.*
Sei nun K ein algebraischer Abschluss von $\mathbb{F}_p(T)$ und $t \in K$ eine Nullstelle von f. Das heißt, dass t die Gleichung $t^p = T$ erfüllt. Dann gilt

$$f(X) = X^p - T = X^p - t^p \overset{(3.10)}{=} (X - t)^p \in K[X]$$

Obwohl der Grad von f gleich p ist, hat f nur eine einzige Nullstelle.

Diese im Beispiel gesehene Eigenschaft von Nullstellen wollen wir zu einer allgemeinen Definition erheben.

Definition 14.1 *(Vielfachheit von Nullstellen und separable Polynome)*
Sei K ein Körper und $\bar{K}$ ein algebraischer Abschluss von K. Weiter sei $f \in K[X]$ ein Polynom.
1.) Sei $\alpha \in \bar{K}$ eine Nullstelle von f. Die Nullstelle α hat die Vielfachheit $v \in \mathbb{N}$, falls $(X - \alpha)^v$ das Polynom $f(X)$ in $\bar{K}[X]$ teilt und $(X - \alpha)^{v+1}$ das Polynom $f(X)$ in $\bar{K}[X]$ nicht teilt.
2.) f heißt separabel, falls jede Nullstelle α aus $\bar{K}$ die Vielfachheit $v_\alpha = 1$ besitzt. Sonst heißt f inseparabel.

Satz 14.2 *Sei K ein Körper und $f \in K[X]$ ein irreduzibles(!) Polynom. f ist genau dann separabel, wenn die Ableitung f' von f nicht das Nullpolynom ist. Hierbei bezeichnet f' die formale Ableitung von f.*

Um uns den Beweis dieses Satzes zu vereinfachen, halten wir folgende Bemerkungen fest:

Bemerkung 14.3 *Die Ableitungsregeln aus der Analysis gelten.*
(Insbesondere gelten die Ketten- und die Produktregel.) □

Bemerkung 14.4 *Seien L/K eine Körpererweiterung und $f, g \in K[X]$ Polynome, dann unterscheiden sich die größten gemeinsamen Teiler von f und g in $K[X]$ und $L[X]$ nur um eine Einheit aus $L[X]^\times$.*

$$d_K := \mathrm{ggT}_{K[X]}(f, g) \hat{=} \mathrm{ggT}_{L[X]}(f, g) =: d_L$$

Beweis. Es gelten

$$\begin{array}{rll} d_K = f \cdot F_K + g \cdot G_K & \in K[X] & \text{mit } F_K, G_K \in K[X] \subseteq L[X] \\ d_L = f \cdot F_L + g \cdot G_L & \in L[X] & \text{mit } F_L, G_L \in L[X] \end{array}$$

Also teilt d_K die Polynome g und f in $K[X] \subseteq L[X]$ und d_L teilt die Polynome f und g in $L[X]$ □

[2] Satz 9.3

Bemerkung 14.5 *Seien K ein Körper mit algebraischem Abschluss $\bar{K}/K$ und $f \in K[X]$ ein nicht notwendig irreduzibles Polynom, sowie $\alpha \in \bar{K}$ eine Nullstelle von f. Es sind äquivalent:*
(1) Vielfachheit von α ist größer als 1.
(2) α ist eine Nullstelle der Ableitung f' von f.
(3) α ist eine Nullstelle des größten gemeinsamen Teilers von f und f'.

Beweis. O.B.d.A. sei f normiert. Setze $a_1 := \alpha$ und faktorisiere f in $\bar{K}[X]$

$$\begin{aligned} f(X) &= \prod_{i=1}^{d}(x - a_i) \\ f'(X) &= \sum_{j=1}^{d} \prod_{\substack{i=1 \\ i\neq j}}(x - a_i) \end{aligned}$$

Durch Einsetzen von α in f' erhalten wir

$$f'(\alpha) = \prod_{i=1}^{d}(\alpha - a_1)$$

Also ist die Vielfachheit von α genau dann größer als Eins, wenn $f'(\alpha) = 0$ ist. Also genau dann, wenn α eine Nullstelle des größten gemeinsamen Teilers von f und f' in $L[X]$ ist. nach Bemerkung 14.4 ist α dann auch eine Nullstelle vom größten gemeinsamen Teiler in $K[X]$. □

Beweis. Wir zeigen nun beide Richtungen der Äquivalenz aus Satz 14.2.
Sei f irreduzibel und $\alpha \in \bar{K}$ eine Nullstelle von f.

„⇒“: Annahme: $f' = 0$, dann ist der größte gemeinsame Teiler von f und f' das Polynom f.
Da α eine Nullstelle von f ist, ist es dann auch eine Nullstelle des größten gemeinsamen Teilers. Nach Bemerkung 14.5 ist dann die Vielfachheit von α größer als eins, also muss f inseparabel sein. Dies ist jedoch offensichtlich falsch!

....⇐“Annahme: „f ist inseparabel“
Mit Bemerkung 14.5 gibt es dann ein $\alpha \in \bar{K}$, welches sowohl eine Nullstelle von f als auch eine Nullstelle von f' ist. Da f nach Vorraussetzung irreduzibel ist, ist f das Minimalpolynom von α und weiter hat die Ableitung f' von f kleineren Grad, also muss f' das Nullpolynom sein, denn sonst wäre f' das Minimalpolynom von α.
Dies liefert einen Widerspruch! □

Folgerung 14.6 *Sei K ein Körper mit $\mathrm{Char}(K) = 0$, dann ist jedes irreduzible Polynom $f \in K[X]$ mit $\deg(f) \geq 1$ separabel.*

Beweis. Die formale Ableitung f' von f ist nicht das Nullpolynom, denn es gilt $\deg(f') = \deg(f) - 1$. Mit Satz 14.2 folgt die Behauptung dann sofort. □

Beispiel 37 *Wir haben in Beispiel 36 gesehen, dass $f := X^p - T \in \mathbb{F}_p(T)[X]$ ein inseparables Polynom ist. Wir können dies nun wesentlich einfacher zeigen, denn es gilt*

$$f'(X) = pX^{p-1} = 0 \in \mathbb{F}_p(T)[X]$$

Bemerkung 14.7 *Es seien K ein Körper mit $\mathrm{Char}(K) = p > 0$ und $\bar{K}/K$ ein algebraischer Abschluss. Weiter seien $r \in \mathbb{N}$ und $\alpha \in K$ gegeben. Dann existiert genau ein $\beta \in \bar{K}$ mit $\beta^{p^r} = \alpha$*

Beweis. Nach dem kleinen Fermat (3.10) ist $\beta \in \bar{K}$ die einzige Nullstelle von

$$X^{p^n} - \alpha = X - \beta^{p^n} = (X - \beta)^{p^n}$$

□

Satz 14.8 *Seien K ein Körper mit $\mathrm{Char}(K) = p > 0$ und $f \in K[X]$ ein irreduzibles Polynom. Definiere*

$$r := \max_{m \geq 0} \left\{ h \in K[X] \,|\, h(X^{p^m}) = f(X) \right\}$$

Dann sei $g \in K[X]$ ein Polynom mit $g(X^{p^r}) = f(X)$. Es gelten:
(a) $g(X)$ irreduzibel und separabel.
(b) Jede Nullstelle von f hat die Vielfachheit p^r.
(c) Die Nullstellen von f sind genau die p-ten Wurzeln der Nullstellen von g.

Beweis. zu (a):
Wäre g reduzibel, also $g_1 \cdot g_2 = g$ mit Polynomen $g_i \in K[X]$ so ließe sich f darstellen als

$$f(X) \;=\; g(X^{p^r}) \;=\; g_1(X^{p^r}) \cdot g_2(X^{p^r})$$

Also wäre auch f reduzibel. Dies widerspricht der Voraussetzung.
Zur Separabilität betrachte

$$f := \sum_{n=0}^{d} a_n \cdot X^n \quad \text{und} \quad f' = \sum_{n=1}^{d} n a_n \cdot X^{n-1}$$

Damit f' das Nullpolynom sein kann müssen alle Koeffizienten na_n Null sein. Also muss die Gleichung $a_n = 0$ für alle $n \in \mathbb{N}$ gelten, die nicht von p geteilt werden. Dann gibt es ein $h(X) \in K[X]$ derart, dass die Bedingung $h(X^p) = f(X)$ erfüllt wird. Wir können $h(X)$ explizit darstellen durch

$$h(X) = \sum_{\substack{j=0 \\ p|j}}^{d} a_{\frac{j}{p}} X^{\frac{j}{p}}$$

Ist $h(X)$ separabel folgt die Behauptung, sonst setze die Konstruktion von g induktiv fort, bis ein separables Polynom $h(X)$ gefunden ist.
Zu (b) und (c):
Da g separabel ist, gibt es Elemente $\alpha_i \in \bar{K}[X]$ so dass wie g darstellen können als

$$g = \prod_{i=1}^{e} (X - \alpha_i) \in \bar{K}[X]$$

Nach Bemerkung 14.7 gibt es zu jedem α_i ein $\beta_i \in \bar{K}$ welches die Bedingung $\beta_i^{p^r} = \alpha_i$ erfüllt. Wir können f dann darstellen durch

$$f(X) = g(X^{p^r}) = \prod_{i=1}^{e} (X - \beta_i)^{p^r}$$

□

Definition 14.9 *(Separable Körpererweiterungen und vollkommene Körper)*
Sei L/K eine algebraische Körpererweiterung
- Ein Element $\alpha \in L$ heißt separabel, falls das Minimalpolynom $f_\alpha \in K[X]$ separabel über K ist.
- Die Körpererweiterung L/K heißt separabel, falls jedes $\alpha \in L$ separabel ist.
- Ist L/K nicht separabel, so nennen wir L/K inseparabel.
- K heißt perfekt oder vollkommen, falls jede algebraische Körpererweiterung K'/K separabel ist.

Folgerung 14.10 *Jeder Körper K mit $\mathrm{Char}(K) = 0$ ist vollkommen.*

Beweis. Die Behauptung folgt direkt aus Folgerung 14.6 □

Beispiel 38 *(vollkommene Körper)*
- Jeder algebraisch abgeschlossene Körper ist vollkommen.
- Der Körper $\mathbb{F}_p(T)$ ist nicht vollkommen, denn $f(X) = X^p - T \in \mathbb{F}_p(T)[X]$ ist inseparabel.

Definition 14.11 *(Der Separabilitätsgrad)*
Sei L/K algebraische Körpererweiterung. Hierzu wähle einen algebraischen Abschluss $\bar{K}$ von K. Der Separabilitätsgrad von L/K ist definiert als $[L : K]_S := \mathrm{Card}\left(\mathrm{Hom}_K(L, \bar{K})\right)$.

Bemerkung 14.12 *Wir übernehmen die Bezeichnungen aus Definition 14.11. Weiter sei $\alpha \in \bar{K}$ ein Element mit Minimalpolynom $f_\alpha \in K[X]$. Es gelten:*

1. *Der Separabilitätsgrad von $K(\alpha)/K$ ist gleich der Anzahl der Nullstellen von f_α in $\bar{K}$ und weiter gilt $[K(\alpha) : K]_S \leq [K(\alpha) : K]$*
2. *Das Element α ist genau dann separabel über K, wenn f_α separabel ist, also wenn $[K(\alpha) : K] := \deg(f_\alpha) = [K(\alpha) : K]_S$ gilt.*
3. *Ist $\mathrm{Char}(K) = p > 0$ mit einer Primzahl p, dann ist $[K(\alpha) : K]_S \cdot p^r = [K(\alpha) : K]$. Hierbei ist p^r wie in Satz 14.8, das heißt $f_\alpha(X) = h(X^{p^r})$ mit $h \in K[X]$ separabel.*

Beweis. Teil (1) haben wir bereits in der Motivation zu begin dieses Abschnittes gezeigt. (2) ist direkt mit der Definition klar, und (3) ist eine Folgerung aus Satz 14.8. □

Satz 14.13 *(Gradsatz II)*
Seien $M/L/K$ algebraische Körpererweiterungen, dann gilt:

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

Beweis. Fixiere einen algebraischen Abschluss $\bar{K}$ von K. Da wir wissen, dass die Mengen der K bzw. der L-Homomorphismen von L bzw. M nach $\bar{K}$ endlich sind nummerieren wir diese Elemente durch:

$$\mathrm{Hom}_K(L, \bar{K}) = \{\, \sigma_i \mid i \in I \,\} \text{ und } \mathrm{Hom}_L(M, \bar{K}) = \{\, \tau_j \mid j \in J \,\}$$

Wähle nach Satz 12.9 eine Fortsetzung $\bar{\sigma}_i \in \mathrm{Hom}(\bar{K}, \bar{K})$ von σ_i für alle $i \in I$.

Behauptung 1 *Wir können die Menge der K-Homomorphismen von M nach $\bar{K}$ darstellen durch*

$$\mathrm{Hom}_K(M, \bar{K}) = \{\, \bar{\sigma}_i \circ \tau_j \mid i \in I \wedge j \in J \,\}$$

Beweis. Die Inklusion „$\supseteq$“ ist klar, betrachten wir also die andere Richtung:
Sei hierzu $\tau \in \mathrm{Hom}_K(M, \bar{K})$ beliebig aber fest, dann ist $\tau_{|_L} = \sigma_i$ für ein $i \in I$. Insbesondere gilt

$$\bar{\sigma}_i^{-1} \circ \tau_{|_L} = \bar{\sigma}_i^{-1} \circ \sigma_i = id_L$$

Daher ist $\bar{\sigma}_i^{-1} \circ \tau$ ein L-Homomorphismus von M nach $\bar{K}$ und es gilt $\bar{\sigma}_i^{-1} \circ \tau = \tau_j$ für ein $j \in J$. Wir können $\tau \in \mathrm{Hom}(M, \bar{K})$ also darstellen durch $\tau = \bar{\sigma}_i \circ \tau_j$ △

Behauptung 2 *Gilt $\bar{\sigma}_i \circ \tau_j = \bar{\sigma}_k \circ \tau_l$ dann ist $i = k$ und $j = l$.*

Beweis. Es sei $\bar{\sigma}_i \circ \tau_{j|_L} = \bar{\sigma}_k \circ \tau_{l|_L}$ dann sind die Einschränkungen von $\bar{\sigma}_i$ und $\bar{\sigma}_k$ auf L identisch und es folgt, dass $\sigma_i = \sigma_k$ ist. Da wir die Elemente in $\mathrm{Hom}_K(L, \bar{K})$ eindeutig nummeriert haben folgt, dass $i = k$ ist. Betrachte nun $\bar{\sigma}_i^{-1} \circ \bar{\sigma}_i \circ \tau_j = \bar{\sigma}_i^{-1} \circ \bar{\sigma}_k \circ \tau_l \Leftrightarrow \tau_j = \tau_l \Leftrightarrow j = l$ △

Aus den Behauptungen 1 und 2 folgt nun die Multiplikativität der Separabilitätsgrade, denn:

$$\mathrm{Card}\left(\mathrm{Hom}_K(M, \bar{K})\right) = \mathrm{Card}(I) \cdot \mathrm{Card}(J)$$

□

Folgerung 14.14 *Sei L/K eine endliche Körpererweiterung dann gelten*
(a) L/K ist genau dann separabel, wenn $[L : K] = [L : K]_S$ ist.
(b) Ist die Charakteristik von K gleich Null, so ist L/K separabel.
(c) Ist $\mathrm{Char}(K) = p > 0$, dann ist $[L : K] = p^r \cdot [L : K]_S$ für ein $r \in \mathbb{N}$.

Beweis. Ist L/K eine einfache Körpererweiterung, dann folgen die Aussagen direkt aus Bemerkung 14.12. Ansonsten gibt es, da L/K eine endliche Körpererweiterung ist, eine endliche Menge $\{\alpha_1, \ldots, \alpha_n\} \subset L$ die L erzeugt. Durch Multiplikation der Erweiterungs- bzw. Separabilitätsgrade der $K(\alpha_i)$ nach Satz 14.13 folgen nun die Aussagen. □

Satz 14.15 *Sei L/K eine endliche Körpererweiterung, dann sind äquivalent[3]:*
(i) L/K ist separabel.
(ii) L/K wird von separablen Elementen erzeugt.
(iii) $[L : K] = [L : K]_S$

Beweis. Ist L/K eine separable Körpererweiterung, dann ist jedes $\alpha \in L$ ist per Definition separabel über K. Insbesondere sind alle Elemente der Erzeugendenmenge $E \subseteq L$ separabel über K. Dies beweist die Implikation von (i) nach (ii). Sei nun $\{\alpha_1, \ldots, \alpha_n\} =: E \subset L$ die Erzeugendenmenge von L. Nach Vorraussetzung sind alle $\alpha_i \in E$ separabel über K. Nach Bemerkung 14.12 gelten dann die folgenden Gleichungen

$$\begin{aligned} [K(\alpha_1) : K] &= [K(\alpha_1) : K]_S \\ [K(\alpha_1, \alpha_2) : K(\alpha_1)] &= [K(\alpha_1, \alpha_2) : K(\alpha_1)]_S \\ &\vdots \end{aligned}$$

Dann gilt wegen der Multiplikativität der Körper- und Separabilitätsgrade

$$\begin{aligned} [K(E) : K] &= [K(\alpha_1, \ldots, \alpha_n) : K] \\ &= [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot \ldots \cdot [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \\ &= [K(\alpha_1) : K]_S \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)]_S \cdot \ldots \cdot [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})]_S \\ &= [K(E) : K]_S \end{aligned}$$

[3] In Folgerung 11.15 haben wir bereits eine ähnliche äquivalenz für algebraische Körpererweiterungen gezeigt.

Damit ist der Schluss von (ii) auf (iii) bewiesen. Für die letzte Implikation von (iii) zurück auf (i) müssen wir zeigen, dass jedes $\alpha \in L$ separabel über K ist. Sei also $\alpha \in L$ ein Element mit Minimalpolynom $f_\alpha \in K[X]$. Ohne Beschränkung der Allgemeinheit sei die Charakteristik von K eine Primzahl p und nicht Null[4], dann gibt es nach Satz 14.8 ein separables Polynom $g(X) \in K[X]$, welches die Bedingung $f_\alpha(X) = g(X^{p^r})$ erfüllt. Nach Bemerkung 14.12 (3) gilt dann

$$[K(\alpha) : K] \;=\; p^r \, [K(\alpha) : K]_S$$

und mit dem Gradsatz II 14.13 folgt

$$\begin{aligned} [L : K] &= [L : K(\alpha)] \cdot [K(\alpha) : K] \\ &= [L : K(\alpha)] \cdot p^r \, [K(\alpha) : K]_S \\ &\geq [L : K(\alpha)]_S \cdot [K(\alpha) : K] \cdot p^r \\ &= [L : K]_S \cdot p^r \end{aligned}$$

Also muss $p^r = 1$ sein und $\alpha \in L$ ist separabel über K. □

Folgerung 14.16 *Sei K ein Körper mit $\mathrm{Char}(K) = p > 0$ sowie L/K eine Körpererweiterung deren Körpererweiterungsgrad $[L : K]$ nicht von p geteilt wird, dann ist L/K separabel.*

Beweis. Es gilt $p \nmid [L : K] = p^r [L : K]_S$ also folgt $r = 0$ □

Folgerung 14.17 *Sei L/K eine nicht notwendig endliche, algebraische Körpererweiterung genau dann ist L/K separabel, wenn L/K von separablen Elementen erzeugt wird.*

Beweis. Die $\Rightarrow$-Richtung ist direkt nach der Definiton klar, betrachten wir also die andere Implikation: Nach Vorraussetzung ist $L = K(E)$, wobei alle Elemente aus E separabel über K sind. Wir definieren die Hilfsmenge $M := \{\, T \subset E \mid \mathrm{Card}(T) < \infty \,\}$, dann können wir L schreiben als

$$L = \bigcup_{T \in M} K(T)$$

Jede Körpererweiterung $K(T)/K$ ist endlich somit nach Satz 14.15 separabel. Also ist auch $K(E) = L/K$ separabel, denn jedes $\alpha \in L$ liegt in einem Teilkörper $K(T)$ und ist somit separabel. □

Folgerung 14.18 *Ist L/K eine separable, algebraische Körpererweiterung, dann ist der Separabilitätsgrad gleich dem Körpergrad.*

Beweis. Ist $[K : L] < \infty$ so ist nichts zu zeigen.
Sei $n \in \mathbb{N}$ beliebig und die Menge $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$ linear unabhängig. Es gilt:

$$[L : K]_S \geq [K(\alpha_1, \ldots, \alpha_n) : K]_S = [K(\alpha_1, \ldots, \alpha_n) : K] = n$$

□

Folgerung 14.19 *Seien $M/L/K$ algebraische Körpererweiterungen. Die Erweiterung M/Kist genau dann separabel, wenn die Erweiterungen M/L und L/K separabel sind.*

[4] Ist die Charakteristik von K hier gleich Null, so ist nichts zu zeigen.

Beweis. Der Schluss von der Separabilität von M/K auf die Separabilität von M/L und L/K ist trivial, zum Beweis der Gegenrichtung sei $\alpha \in M$ ein Element mit dem Minimalpolynom

$$f_\alpha = \sum_{i=1}^{d} c_i \cdot X^i \in L[X]$$

Wir betrachten den von den Koeffizienten von f_α erzeugten Erweiterungskörper $L' := K(c_0, \ldots, c_d)$ von K. Dann ist L'/K eine endliche, separable Körpererweiterungrweiterung. Nach Vorraussetzung ist α separabel über L und L' ist ein Teilkörper von L. Daraus folgt: Die Körpererweiterung $L'(\alpha)/K$ ist separabel also ist α separabel über K. □

Definition und Satz 14.20 *(Satz vom primitiven Element)*
Es sei L/K eine Körpererweiterung.
Ein Element $a \in L$ heißt primitiv, falls L über K von a erzeugt wird, das heißt wenn $L = K(a)$ gilt.
Ist L/K endlich und separabel, dann existiert ein solches primitives Element a.

Beweis. 1. Fall ($\mathrm{Card}(K) < \infty$): nach Aufgabe 5 vom 9. Übungsblatt ist $L^\times$ eine zyklische Gruppe. Wähle also den Erzeuger von $L^\times$ als a.
2. Fall ($\sharp K = \infty$): Nach Induktion genügt es ein $y \in L$ zu finden, mit $K(y) = K(\alpha, \beta)$ für $\alpha, \beta \in L$. Seien $f_\alpha,\ f_\beta \in K[X]$ die Minimalpolynome zu α bzw. β und $\bar{K}$ ein algebraischer Abschluss von K, der L enthält. Seien weiter $a_1, \ldots, a_n \in \bar{K}[X]$ Nullstellen von f_α und $b_1, \ldots, b_m \in \bar{K}$ Nullstellen von f_β. Wähle $a_1 = \alpha$ und $b_1 = \beta$ sowie ein $x \in K$ mit $x \neq \frac{\alpha - a_i}{\beta - b_j}$
Dann gilt: $a_i \neq \alpha - x\beta + xb_j$ Wähle nun $y := \alpha - x\beta$.

Behauptung 1 $K(y) = K(\alpha, \beta)$

Beweis. Es gilt $0 = f_\alpha(\alpha) = f_\alpha(y + x\beta)$
Sei $h_\alpha(X) := f_\alpha(y + xX) \in K(y)[X]$ eim Polynom, dann gelten die Gleichungen

$$h_\alpha(b_j) = f_\alpha(y + xb_j) \neq 0 \text{ und } h_\alpha(\beta) = f_\alpha(y + x\beta) = 0$$

Dann sind die größte gemeinsame Teiler h_α von f_β in $\bar{K}[X]$ und $K(y)[X]$ assoziiert zum konstanten Polynom $X - \beta$. Daher sind $\alpha, \beta \in K(y)$ damit ist $K(\alpha, \beta)$ in $K(y)$ enthalten. □

Definition 14.21 *(rein inseparabel)*

(i) Sei K ein Körper. Ein Polynom $f \in K[X]$ heißt rein inseparabel über K, falls f im algebraischen Abschluss $\bar{K}$ genau eine Nullstelle besitzt.
(ii) Sei L/K eine algebraische Körpererweiterung. $\alpha \in L$ heißt rein inseparabel über K, falls Das Minimalpolynom $f_\alpha \in K[X]$ zu α rein inseparabel über K ist.
(iii) Sei L/K eine algebraische Körpererweiterung. L/K heißt rein inseparabel, falls jedes $\alpha \in L$ rein inseparabel über K ist.

Bemerkung 14.22 *K sei ein Körper mit $\mathrm{Char}(K) = p > 0$ und L/K sei eine algebraische Körpererweiterung. Weiter sei $\alpha \in L$ ein rein inseparables Element mit Minimalpolynom f_α. Dann existieren Elemente $c \in K$ und $r \in \mathbb{N}$, so dass:*

$$f_\alpha = X^{p^r} - c \in K[X]$$

Beweis. Nach Satz 14.8 ist $f_\alpha = h(X^{p^r}$ mit einem irreduzieblen, separablen Polynom $h(X) \in K[X]$. Dann ist $h(X) = X - c$ □

Bemerkung 14.23 *Ist L/K eine algebraische Körpererweiterung, dann sind äquivalent:*
(i) L ist rein inseparabel über K
(ii) L wird über K von rein inseparablen Elementen erzeugt.
(iii) $[L : K]_S = 1$
(iv) Für alle $\alpha \in L$ gibt es ein $r \in \mathbb{N}$ derart, dass $\alpha^{p^r} \in K$

Beweis. Die Implikation von (i) auf (ii) ist trivial, denn mit L als Erzeugendenmenge ist nichts zu zeigen. Für den Schluss von (ii) auf (iii) sei $S \subseteq L$ die Erzeugendenmenge von L. Nach Vorraussetzung sind alle Elemente in S inseparabel. Sei nun M die Familie der endlichen Teilmengen von S, dann lässt sich L darstellen als

$$L = \bigcup_{T \in M} K(T)$$

Da T endlich ist benenne die Elemente aus T mit $T = \{\alpha_1, \ldots, \alpha_n\}$, dann folgt nach dem Gradsatz 14.13 die folgende Gleichung

$$\begin{aligned} [K(T) : K]_S &= [K(\alpha_1, \ldots, \alpha_n) : K]_S \\ &= [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})]_S \cdot \ldots \cdot [K(\alpha_1) : K]_S \\ &= \prod_{i=1}^{n} 1 \; = \; 1 \end{aligned}$$

Ist $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ nicht die Identität, dann gibt es ein T derart, dass $\sigma_{|K(T)}$ nicht die Identität ist. Damit ist der Schluss von (ii) auf (iii) bewiesen. Für den nächsten Schritt sei nun $\alpha \in L$ ein Element mit Minimalpolynom $f_\alpha(X) = h(X^{p^r}) \in K[X]$. Da nach Vorraussetzung $[L : K]_S = 1$ ist, ist auch $[K(\alpha) : K]_S = 1$ und somit ist $h(X) = X - c \in K[X]$ also folgt, dass $\alpha^{p^r} = c \in K$ ist. Also ist auch der Schritt von (iii) auf (iv) bewiesen. Wir müssen nun nurnoch die Implikation von (iv) zurück auf (i) zeigen. Es gilt, dass das Minimalpolynom $f_\alpha(X)$ von α das Polynom $X^{p^r} - \alpha^{p^r}$ im Polynomring $K[X]$ teilt, also ist α inseparabel. □

Folgerung 14.24 *Seien $M/L/K$ algebraische Körpererweiterungen. Die Erweiterung M/L ist genau dann rein inseparabel, wenn M/L und L/K rein inseparabel sind.*

Beweis. Es ist genau dann $[M : K]_S = [M : L]_S \cdot [L : K]_S = 1$, wenn $[M : L]_s = 1$ und $[L : K]_S = 1$ □

Definition und Satz 14.25 *(Der separable Abschluss)*
Sei L/K eine algebraische Körpererweiterung. Setze: $K_S := \{\alpha \in L \mid \alpha$ separabel über $K\}$.
Dann ist K_S der eindeutig bestimmte Zwischenkörper $L/K_S/K$ mit den Eigenschaften:
(1) L/K_S ist rein inseparabel
(2) K_S/K ist separabel
Es gelten $[L : K]_S = [K_S : K] = [K_S : K]_S$ und ist L/K normal, dann ist auch K_S/K normal.
K_S heißt separabler Abschluss von K in L.
Sei $\bar{K}/K$ ein algebraischer Abschluss, dann heißt $\bar{K}_S := \{\alpha \in \bar{K} \mid \alpha$ separabel über $K\}$ der separable Abschluss von K.

Beweis.
- K_S ist ein Körper, denn seien $\alpha, \beta \in K_S$, dann sind $\alpha \cdot \beta^{-1}, \alpha - \beta \in K[\alpha, \beta] \subseteq K_S$
- K_S/K ist separabel per Definition.
- Sei $\alpha \in L$ und $f_\alpha \in K_S[X]$ das zugehörige Minimalpolynom, dann ist $f_\alpha(X) = h(X^{p^r})$ mit $r \in \mathbb{N}$ und $h \in K_S$ irreduzibel und separabel.
  Weiter ist h das Minimalpolynom zu α^{p^r}, dann ist $c := \alpha^{p^r}$ separabel über K_S und somit auch über K. Also liegt $c = \alpha^{p^r}$ bereits in K_S
  $h = X - c \Rightarrow f_\alpha$ rein inseparabel $\Rightarrow \alpha$ rein inseparabel.
- $[L : K]_S = [L : K_S]_S \cdot [K_S : K]_S = 1 \cdot [K_S : K]$
- (Eindeutigkeit:) Sei L/K' eine inseparable Körpererweiterung und K'/K separabel, dann ist nach Definition K' ein Teilkörper von K_S
  Angenommen $K' \neq K_S$. Wähle $\alpha \in K_S \backslash K'$, dann ist α separabel. Gleichzeitig folgt aber, dass α rein inseparabel ist. Das ist offensichtlich falsch! □

Definition und Satz 14.26 *(Der rein inseparable Abschluss)*
Sei L/K eine normale algebraische Körpererweiterung, dann setze:

$$K_i := \{\, \alpha \in L \,|\, \forall\, \sigma \in \mathrm{Hom}_K(L, L) \,:\, \sigma(\alpha) = \alpha \}$$

Dann ist K_i der eindeutig bestimmte Zwischenkörper $L/K_i/K$ mit den Eigenschaften:
(1) L/K_i ist separabel
(2) K_i/K ist rein inseparabel
Wir nennen K_i den rein inseparablen Abschluss von K in L. Ist $L = \bar{K}$ ein algebraischer Abschluss von K, dann heißt K_i der rein inseparable Abschluss von K.

Beweis. Ist $\bar{L}/L$ ein algebraischer Abschluss, so gilt: $\mathrm{Hom}_K(L, \bar{L}) = \mathrm{Hom}_K(L, L)$, denn nach Voraussetzung ist L/K ist normal.Wir weisen zunächst nach, dass K_i ein Körper ist. Seien $\alpha, \beta \in K_i$, dann gelten $\sigma(\alpha) = \alpha$ und $\sigma(\beta) = \beta$ für alle $\sigma \in \mathrm{Hom}_K(L, \bar{L})$ nach Voraussetzung. Damit gelten auch

$$\sigma(\alpha\beta^{-1}) = \alpha\beta^{-1} \quad \text{und} \quad \sigma(\alpha - \beta) = \alpha - \beta$$

Also $\alpha\beta^{-1}, \alpha - \beta \in K_i$.
Für den Nachweis von (2) sei nun $\sigma \in \mathrm{Hom}_K(K_i, L)$, dann existiert nach Satz 12.9 eine Fortsetzung $\sigma' \in \mathrm{Hom}_K(L, L)$ mit $\sigma'_{|_K} = \sigma = id_{K_i}$ also ist $[K_i : K]_S = 1$ und damit ist K_i/K rein inseparabel.
Wir zeigen nun die Eindeutigkeit von K_i. Dazu sei $L/K'/K$ ein Zwischenkörper, derart dass K'/K rein inseparabel ist, dann ist jedes $\sigma \in \mathrm{Hom}_K(K', \bar{L})$ die Identität auf K', da K' rein inseparabel ist. Also ist $\sigma(k) = k$ für alle $k \in K'$ und alle $\sigma \in \mathrm{Hom}_K(K', \bar{L}) \subseteq \mathrm{Hom}_K(L, \bar{L})$. Damit ist K' in K_i enthalten und K_i/K ist die größte rein inseparable Erweiterung in L.
Als letztes müssen wir noch zeigen, dass (1) gilt, also das L/K_i separabel ist. Dazu sei $\alpha \in L$ beliebig aber fest gewählt. Numeriere $\{\sigma(\alpha) \,|\, \sigma \in \mathrm{Hom}_K(L, L)\} =: \{\alpha = \alpha_1, \alpha_2, \ldots\}$ Diese Menge ist endlich, da die α_i Nullstellen vom Minimalpolynom f_α sind. Setze

$$f(X) := \prod_{i=1}^{n} (x - \alpha_i)$$

dann ist f ein separables Polynom mit $f(\alpha) = 0$. Da jedes $\sigma \in \mathrm{Hom}_K(L, L)$ die α_i nur permutiert, gilt

$$\sigma(f(X)) = \prod (X - \sigma(\alpha_i)) = f(X)$$

Für alle $\sigma \in \mathrm{Hom}_K(L, L)$. Daher ist $f \in K_i[X]$ und somit α separabel über K_i □

15 Endliche Körper

Bemerkung 15.1 *Sei K ein endlicher Körper, dann gelten*
(a) $\mathrm{Char}(K) = p > 0$ *mit p einer Primzahl.*
(b) $\mathrm{Card}(K) = p^m$ *mit $m \in \mathbb{N}$ einer natürlichen Zahl.*
(c) Für $\mathrm{Frob}_p(x) = x^p$ *gilt:* $\mathrm{Frob}_p \in \mathrm{Aut}(K, K)$

Beweis. Die Behauptungen (a) und (c) sind bereits bekannt.
Zu b) K ist ein $\mathbb{F}_p$ - Vektorraum mit Dimension $\dim_{\mathbb{F}_p}(K) = m$ also hat K genau p^m Elemente □

Satz 15.2 *Sei $\mathbb{P} \subseteq \mathbb{Z}$ die Menge der positiven Primzahlen. Für alle $p \in \mathbb{P}$ und für alle $m \in \mathbb{N}$ gibt es bis auf Isomorphie eindeutig bestimmte Körper mit p^m Elementen. (Notation: $\mathbb{F}_{p^m}$ oder $GF(p, m)$) Diese Körper entstehen als Zerfällungskörper der Polynome $f(X) = X^{p^m} - X \in \mathbb{F}_p[X]$ über $\mathbb{F}_p$ Die Körpererweiterung $\mathbb{F}_{p^m}/\mathbb{F}_p$ ist normal, endlich und separabel.*

Beweis. Sei N ein Zerfällungskörper von $f(X) = X^{p^m} - X$, wir faktosisieren f in N:

$$f = \prod_{i=1}^{p^m}(X - \alpha_i) \quad \text{mit } \alpha_i \in N \ \ \forall\, i = 1 \dots p^m$$

Wir definieren die Nullstellenmenge von f in N als $M := \{\alpha_1, \dots, \alpha_{p^m}\}$

Behauptung 1 *M ist ein Körper*

Beweis. Betrachte die folgende Rechnung:

$$\begin{aligned}(\alpha_i \pm \alpha_j)^{p^m} &= \mathrm{Frob}_p^m(\alpha_i \pm \alpha_j) = \mathrm{Frob}_p^m(\alpha_i) \pm \mathrm{Frob}_p^m(\alpha_j) \\ &= \alpha_i^{p^m} \pm \alpha_j^{p^m} = \alpha_i \pm \alpha_j \ \in M\end{aligned}$$

Mit einer analogen Rechnung für $\alpha_i \cdot \alpha_j$ und falls $\alpha_i \neq 0$ auch für $\frac{\alpha_j}{\alpha_i}$ folgt Behauptung 1. △

Da sowohl N als auch M alle Nullstellen von f enthalten gilt, dass $M = N$ ist.

Behauptung 2 *M hat p^m Elemente.*

Beweis. Die Nullstellen des Polynoms $g = X^{p^m-1} - 1 = \frac{f}{X}$ bilden eine zyklische Gruppe $p^m - 1$-ter Ordnung[5]. Inbesondere hat g also $p^m - 1$ verschiedene Nullstellen. Damit hat dann $f(X) = X \cdot g$ genau p^m verschiedene Nullstellen, denn 0 ist keine Nullstelle von $g(X)$. △

Da M ein Zerfällungskörper von f ist folgt, dass $M/\mathbb{F}_{p^m}$ normal und separabel ist.
Zur Eindeutigkeit bis auf Isomorphie:
Sei L ein Körper mit p^m Elementen, dann gilt: $\mathrm{Card}(L^\times) = \mathrm{Card}(L\backslash\{0\}) = p^m - 1$
Nach Satz 3.10 gilt dann für alle $x \in L^\times$ die Gleichung $x^{p^m-1} = 1$ und es folgt, dass $X^{p^m} - X = 0$ ist. Also ist L ein Zerfällungskörper von f. Nach Folgerung 13.5 gibt es dann einen Isomorphismus zwischen L und M. □

Folgerung 15.3 *Endliche Körper sind vollkommen.*

Beweis. Seien K ein endlicher Körper und L/K eine algebraische Körpererweiterung.
Angenommen L/K ist nicht separabel, dann gäbe es ein inseparables Element $\alpha \in L$ und eine endliche Körpererweiterung $K(\alpha)/K$. Da $K(\alpha)/K$ und K endlich sind ist $K(\alpha)$ ein endlicher Körper. Nach Satz 15.2 ist $K(\alpha)/K$ separabel. Dies ist ein Wiederspruch zur Inseparabilität von α. □

[5] Nach Aufgabe 5 des 9. Übungsblattes

Kapitel IV

Galois Theorie

16 Galois Erweiterungen

Definition 16.1 *(Galois Erweiterungen und Galoisgruppen)*
Sei L/K eine algebraische Körpererweiterung. Diese heißt galoisch bzw. Galois-Erweiterung, falls sie normal und separabel ist. Die Galois-Gruppe einer Galois-Erweiterung L/K ist:

$$\mathrm{Gal}(L/K) := G(L/K) := \mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L)$$

Anmerkung In der vorangegangenen Definition haben wir algebraische Körpererweiterungen, die gleichzeitig normal und separabel sind, als Galois-Erweieterungen bezeichnet. Beide Eigenschaften spielen für die nun folgenden Sätze und Bemerkungen eine wichtige Rolle

Die Rolle der Normalität:
Bei einer normalen Erweieterung L/K ist jeder K-Homomorphismus $\sigma : L \to \bar{L}$ sogar ein K-Homomorphismus von L nach L, das heißt

$$\mathrm{Hom}_K(L, \bar{L} \;=\; \mathrm{Hom}_k(L, L) \;=\; \mathrm{Aut}_K(L)$$

Die Rolle der Separabilität:
Ist L/K eine separable Körpererweiterung, dann werden die K-Homomorphismen $\sigma : K(\alpha) \to L$ für $\alpha \in L$ durch die Nullstellen des Minimalpolynoms $f_\alpha \in K[X]$ von α beschrieben, die alle einfach auftreten.

Beispiel 39 *(Bekannte Galoiserweiterungen)*

- $\mathbb{C}/\mathbb{R}$ *ist galoisch, und* $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, c\}$ *mit* $c(z) = c(a + ib) := a - ib = \bar{z}$
- *Die Erweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist galoisch.*
- *Sei K ein Körper und $f \in K[X]$ ein separabels Polynom, dann ist jeder Zerfällungskörper N von f über K ein Galois-Erweiterungskörper von K.*
  Denn N/K ist normal, da N ein Zerfällungskörper ist und separabel, da N über K von separablen Elementen (den Nullstellen von f) erzeugt wird.

Bemerkung 16.2 *Sei L/K eine normale Körpererweiterung, dann gelten:*
(i) $\mathrm{Card}\left(\mathrm{Aut}_K(L)\right) \leq [L:K]$
(ii) Sei L/K endlich. Genau dann ist L/K galoisch, wenn $\mathrm{Card}\left(\mathrm{Aut}_K(L)\right) = [L:K]$ *ist.*

Beweis. zu (i):
Sei $\bar{L}/L$ ein algebraischer Abschluss. Da L/K normal ist, sind $\mathrm{Aut}_K(L)$ und $\mathrm{Hom}_K(L,\bar{L})$ gleich. Es gilt also

$$\mathrm{Card}\left(\mathrm{Aut}_K(L)\right) = \mathrm{Card}\left(\mathrm{Hom}_K(L,\bar{L})\right) = [L:K]_S \leq [L:K]$$

Zu (ii):
Da L/K endlich ist, sind der Erweiterungsgrad und der Separabilitätsgrad genau dann gleich, wenn L/K separabel ist. □

Beispiel 40 *Wir betrachten* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$
Wegen $\mathbb{F}_{p^n} = \mathbb{F}_p^n$ kennen wir bereits den Erweiterungsgrad $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Weiter wissen wir, dass $\mathbb{F}_{p^n}/\mathbb{F}_p$ galoisch ist. Es ist ausserdem klar, dass Frob_p *in* $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^n) = \mathrm{Gal}(\mathbb{F}_p^n/\mathbb{F}_p)$ *enthalten ist.*
Es lässt sich leicht zeigen, dass der Forbeniusautomorphismus Frob_p^i *für alle $i = 1, \ldots, n$ in* $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^n)$ *enthalten ist. Hierbei ist* $\mathrm{Frob}_p^n = id$*. Dies heißt jedoch, dass* $\mathrm{Card}\left(\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^n)\right) = n$ *ist.*

Bemerkung 16.3 *Seien L/K eine Galois-Erweiterung und E ein Zwischenkörper. Dann gilt:*
(a) L/E ist galoisch und $\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/K)$.
Genauer: $\mathrm{Gal}(L/E) = \{\, \sigma \in Aut_K(L) \,|\, \sigma_{|_E} = id_E \,\}$.
(b) Ist E/K galoisch (dies gilt im Allgemeinen nicht!), dann ist

$$\begin{array}{rcl} \pi : \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \\ \sigma & \mapsto & \sigma_{|_E} \end{array}$$

ein surjektiver Gruppen-Homomorphismus und $\mathrm{Ker}(\pi) = \mathrm{Gal}(L/E)$

Beweis. Die vorhergegangenen Kapitel haben gezeigt, dass L/E und E/K separabel sind und dass L/E normal ist. Zu (a) ist nicht zu zeigen, denn $\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L) \leq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$
Zu (b):
Wir müssen zunächst nachweisen, dass π wohldefiniert ist. Nach Voraussetzung ist E/K normal, es ist also klar, dass für alle Automorphismen $\sigma \in \mathrm{Gal}(L/K)$ die Gleichung $\sigma(E) = E$ erfüllt ist.
Die Abbildung π ist offensichtlich ein Gruppen-Homomorphismus. Es bleibt die Surjektivität zu zeigen. Seien hierzu $\sigma \in \mathrm{Aut}_K(E)$ und $\bar{L}/L$ ein algebraischer Abschluss. Betrachte

$$\tau : E \xrightarrow{\sigma} E \hookrightarrow \bar{L}$$

Nach Definition 12.9 existiert ein $\tau' \in \mathrm{Hom}_K(L,\bar{L})$. Da L/K nach Voraussetzung normal ist, ist $\tau' \in \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$ mit $\tau'_{|_E} = \sigma = \pi(\tau)$.
Den Kern von π können wir direkt angeben: $\mathrm{Ker}(\pi) = \{\, \sigma \in Gal(L/K) \,|\, \pi(\sigma) = \sigma_{|_E} = id_E \,\}$ □

Definition und Satz 16.4 *(Fixkörper)*
Seien L ein Körper, und $G \leq \mathrm{Aut}(L)$ eine Untergruppe. Wir definieren den Fixkörper von L unter G durch:

$$L^G := \{\, x \in L \mid \sigma(x) = x \;\forall\, \sigma \in G \,\}$$

Es gelten:
(a) Ist G endlich oder L/L^G algebraisch, dann ist L/L^G galoisch
(b) Ist G endlich, dann ist $\mathrm{Gal}(L/L^G) = G$
(c) Ist L/L^G algebraisch und $\mathrm{Card}(G) = \infty$, dann ist $[L : L^G] = \infty$ und $G \leq \mathrm{Gal}(L/L^G)$

Beweis. L^G ist ein Körper, denn es gilt: $\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y$
Analog zeigen wir dies für $x \cdot y$ und mit $y \neq 0$ für $\frac{x}{y}$.
(a) Sei $\alpha \in L$ beliebig aber fest gewählt, dann betrachte die folgende Menge M

$$\{\, \sigma(\alpha) \mid \sigma \in G \,\} = \{\, \alpha =: \alpha_1, \ldots, \alpha_n \} =: M$$

Behauptung *Die Menge M hat nur endlich viele Elemente, also $\mathrm{Card}(M) = n < \infty$.*

Beweis. Wir betrachten zwei Fälle:
I (G endlich) Es gilt: $\mathrm{Card}(M) \leq \mathrm{Card}(G)$
II (L/L^G algebraisch) Jedes $\alpha_i \in M$ ist eine Nullstelle vom Minimalpolynom f_α über L^G. △
Per definition permutiert G die Menge M lediglich, also gilt $\tau(M) = M$ für jedes $\tau \in G$. Setze

$$g_\alpha(X) := \prod_{i=1}^{n} (X - \alpha_i) \in L[X]$$

Dann ist $\tau\big(g_\alpha(X)\big) = g_\alpha(X)$ und g_α bereits ein Element in $L^G[X]$. α ist separabel über L^G, denn $g_\alpha(X)$ ist separabel nach Konstruktion. Weiter ist L/L^G normal, denn für jedes $\alpha \in L$ ist die Nullstellenmenge von g_α eine Untermenge von L, also ist L ein Zerfällungskörper der Familie $(g_\alpha)_{\alpha \in L}$ und somit ist L/L^G galoisch.
Zu (c):
Wir haben Vorausgesetzt, dass L/L^G eine algebraische Erweiterung ist und dass $\mathrm{Card}(G) = \infty$ ist.
Es gilt $G \leq \mathrm{Aut}_{L^G}(L) := \mathrm{Gal}(L/L^G)$ also folgt

$$\infty = \mathrm{Card}(G) \leq \mathrm{Card}\left(\mathrm{Aut}_{L^G}(L)\right) = \mathrm{Card}\left(\mathrm{Gal}(L/L^G)\right) \leq [L : L^G]$$

Zu (b):
Es ist zu zeigen, dass aus der Endlichkeit von L/L^G folgt, dass $\mathrm{Gal}(L/L^G) = G$ ist.
Nach dem Satz vom primitiven Element 14.20 gilt: $L = L^G(\alpha)$ wie in (c)
$G \leq Gal(L/L^G)$, zeige also $[L : L^G] \leq \mathrm{Card}(G)$
Betrachte dazu die Menge $\{\alpha = \alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha) \mid \sigma \in G\,\}$ und das Polynom
$g_\alpha(X) = \prod_{i=1}^{n} (X - \alpha_i) \in L^G[X]$ aus (a). Wegen $g_\alpha(\alpha) = 0$ folgt, dass das Minimalpolynom zu α $f_\alpha \in L^G[X]$ das Polynom g_α teilt.
Es gilt: $[L : L^G] = \deg(f_\alpha) \leq \deg(g_\alpha) = n \leq \mathrm{Card}(G)$ □

Folgerung 16.5 *Sei L/K eine normale Körpererweiterung, und $G := \mathrm{Aut}_K(L)$. Es gelten:*
(a) L/L^G ist galoisch mit $\mathrm{Gal}(L/L^G) = G$
(b) $[L^G/K]$ ist rein inseparabel.
(c) Ist L/K separabel (also galoisch), dann ist $L^G = K$

Beweis. Zu (a)
Da L/K normal, also insbesondere algebraisch, ist, folgt, dass L/L^G algebraisch ist. Mit Satz 16.4 ist L/L^G dann auch galoisch. Betrachte nun die folgenden Inklusionen:

$$G \subseteq \mathrm{Aut}_{L^G}(L) \hookrightarrow \mathrm{Aut}_K(L) = G$$

Zu (b)
Fixiere einen algebraischen Abschluss $\bar{K}$ zu K. Sei $\sigma \in \mathrm{Hom}_K(L^G, \bar{K})$, dann gibt es nach Satz 12.9 eine Fortsetzung $\sigma' \in \mathrm{Hom}_K(L, \bar{K})$. Da L/K eine normale Körpererweiterung ist, ist σ' ein K-Automorphismus von L. Nach (a) wissen wir, dass $\mathrm{Aut}_{L^G}(L)$ und $\mathrm{Aut}_K(L)$ gleich sind, daher ist σ' auch ein L^G-Automorphismus von L, also $\sigma'_{|L^G} = \sigma = id_{L^G}$ und damit ist der Separabilitätsgrad von L^G/K gleich eins.
zu (c)
Aus der Separabilität von L/K folgt die Separabilität von L^G/K und nach (b), dass $[L^G : K]_S = 1$ ist. Somit folgt die Gleichheit von L^G und K. □

Satz 16.6 *(Hauptsatz der Galois-Theorie)*
Sei L/K eine endliche Galois-Erweiterung, und bezeichne $G := \mathrm{Gal}(L/K)$. es gelten

(a) *Die Abbildungen*

$$\begin{array}{rcl} \{\, H \mid H \leq G \,\} & \leftrightarrows & \{\, E \mid E \text{ Körper } \wedge K \subseteq E \subseteq L \,\} \\ H & \mapsto & \Phi(H) := L^H \\ \Psi(E) := \mathrm{Gal}(L/E) & \hookleftarrow & E \end{array}$$

sind bijektiv und zu einander invers.

(b) *$\mathrm{Gal}(L/E)$ ist genau dann ein Normalteiler von G, wenn E/K galoisch ist.*
Ebenso ist H genau dann ein Normalteiler von G, wenn L^H/K galoisch ist.

(c) *Sei $H \trianglelefteq G$ ein Normalteiler, dann induziert*

$$\begin{array}{rcl} \pi : G & \to & Gal(L^H/K) \\ \sigma & \mapsto & \sigma_{|_{L^H}} \end{array}$$

einen Gruppen-Isomorphismus derart, dass $G/\mathrm{Gal}(L/L^H) \cong \mathrm{Gal}(L^H/K)$ gilt.

Beweis. zu (a) ist zu zeigen, dass $\Phi \circ \Psi = id = \Psi \circ \Phi$ gelten. Wegen Folgerung 16.5 Teil (c) gilt

$$\Phi \circ \Psi(E) \;=\; \Phi(\mathrm{Gal}(L/E)) = L^{\mathrm{Gal}(L/E)} = E$$

Und mit Satz 16.4 Teil (b) ist

$$\Psi \circ \Phi(H) \;=\; \Psi(L^H) = \mathrm{Gal}(L/L^H) = H$$

Zu (b):
Sei $H \leq G$ eine Untergruppe. Die Körpererweiterung L^H/K ist genau dann eine normale Erweiterung, wenn für alle $\sigma \in G$ gilt, dass $\sigma(L^H) = L^H$ ist, denn nach Satz 13.6 ist L^H/K genau dann

normal, wenn für alle $\tau \in \mathrm{Hom}_K(L^H, \bar{K})$ mit einem algebraischen Abschluss $\bar{K}$ zu K gilt, dass $\tau(L^H) = L^H$ ist. Die Abbildung

$$G := \mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \bar{K}) \xrightarrow{(12.9)} \mathrm{Hom}_K(L^H, \bar{K})$$

ist surjektiv. Für alle $\sigma \in G$ gilt, dass $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$ ist, denn

$$\begin{aligned} a \in \sigma(L^H) &\Leftrightarrow \sigma^{-1}(a) \in L^H \\ &\Leftrightarrow h\sigma^{-1}(a) = \sigma^{-1}(a) \qquad \forall\, h \in H \\ &\Leftrightarrow \sigma \circ h \circ \sigma^{-1}(a) = a \qquad \forall\, h \in H \\ &\Leftrightarrow a \in L^{\sigma H \sigma^{-1}} \end{aligned}$$

Also ist L^H/K genau dann normal, wenn für alle $\sigma \in G$ gilt, dass $\sigma(L^H) = L^H$ ist. Für alle $\sigma \in G$ gilt

$$\begin{aligned} \sigma(L^H) = L^H &\Leftrightarrow L^{\sigma H \sigma^{-1}} = L^H \\ &\overset{(a)}{\Leftrightarrow} \Psi(L^{\sigma H \sigma^{-1}}) = \Psi(L^H) \\ &\Leftrightarrow \sigma H \sigma^{-1} = H \Leftrightarrow H \trianglelefteq G \end{aligned}$$

Teil (c) folgt aus Bemerkung 16.3 b), denn es gilt: $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/K)$ für ein E mit $K \subseteq E \subseteq L$. Nimm also $E := L^H$ □

Anmerkung Der Hauptsatz der Galois-Theorie (16.6) in Worten:
Die Untergruppen von $\mathrm{Gal}(L/K)$ klassifizieren die Zwischenkörper von L/K.

Folgerung 16.7 *Sei L/K eine endlich, separable Körpererweiterung, dann gibt es nur endlich viele Zwischenkörper.*

Beweis. Wir dürfen ohne Einschränkung annehmen, dass L/K galoisch ist, da wir sonst mit der normalen Hülle N/K weiter machen und diese nach Satz 13.10 endlich ist. Die Zwischenkörper von L/K entsprechen nach dem Hauptsatz der Galois-Theorie 16.6 genau den Untergruppen der endlichen Gruppe $\mathrm{Gal}(L/K)$. □

Anmerkung Die Aufgabe 6 vom 10. Übungsblatt zeigt, dass die Separabilität in Folgerung 16.7 notwendig ist.

Definition 16.8 *(zyklische und abelsche Körpererweiterungen)*
Sei L/K endliche Galois-Erweiterung.
Die Erweiterung L/K heißt genau dann zyklisch, wenn $\mathrm{Gal}(L/K)$ zyklisch ist.
Die Erweiterung L/K heißt genau dann abelsch, wenn $\mathrm{Gal}(L/K)$ abelsch ist.

Folgerung 16.9 *Sei L/K eine endliche abelsche [bzw. zyklische] Galois-Erweiterung, dann sind für jeden Zwischenkörper $K \subseteq E \subseteq L$ die Erweiterungen L/E und E/K auch abelsch [bzw. zyklisch].* □

Definition 16.10 *(Das Kompositum)*
Es sei L ein Körper und seien E, E' Unterkörper von L. Das Kompositum $EE' := E(E') := E'(E)$ ist der kleinste Teilkörper von L, der die Körper E und E' enthält.

Beispiel 41 *(Komposita)*
- $L := \mathbb{R}$, $E := \mathbb{Q}(\sqrt{2})$, $E' := \mathbb{Q}(\sqrt{3})$: $EE' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
- $L := \mathbb{C}$, $E := \mathbb{Q}(i)$, $E' := \mathbb{R}$: $EE' = \mathbb{C}$

Bemerkung 16.11 *Seien L/K eine endliche Galois-Erweiterung und E, E' Zwischenkörper mit $K \subseteq E, E' \subseteq L$. Wir definieren $H := \mathrm{Gal}(L/E)$, $H' := \mathrm{Gal}(L/E')$. Dann gelten:*
(a) E ist genau dann in E' enthalten, wenn H' eine Untergruppe von H ist.
(b) Das Kompositum lässt sich schreiben als $EE' = L^{H \cap H'}$
(c) $E \cap E' = L^{<H,H'>}$

Beweis. Zu (a)
Sei E ein Teilkörper von E' dann gilt $H = \mathrm{Gal}(L/E) \supseteq \mathrm{Gal}(L/E') = H'$. Für die Gegenrichtung sei $H' \leq H$. Nach dem Hauptsatz der Galois-Theorie 16.6 gelten die Gleichungen $E = L^H$ und $E' = L^{H'}$ und somit folgt $E = L^H \subseteq L^{H'} = E'$
Zu (b)
Es ist klar, dass das Kompositum EE' im Fixkörper $L^{H \cap H'}$ enthalten ist, also dass

$$\mathrm{Gal}(L/EE') \supseteq H \cap H'$$

gilt. Wir zeigen also nur die andere Inklusion. Sei hierzu $\sigma \in \mathrm{Gal}(L/EE')$. Da $\sigma_{|E} = id_E$ und $\sigma_{|E'} = id_{E'}$ gelten folgt, dass $\sigma \in \mathrm{Gal}[L(E)$ und $\sigma \in \mathrm{Gal}(L/E')$ ist. Daher ist $\mathrm{Gal}(L/EE')$ in $H \cap H'$ enthalten und wir haben Gleicheit gezeigt.
Zu (c)
Nach dem Hauptsatz der Galois-Theorie folgt, dass $E \cap E' = L^H \cap L^{H'}$ ist. Wir müssen also die Gleicheit von $L^H \cap L^{H'}$ und $L^{<H,H'>}$ zeigen. Auch hierbei ist eine Inklusion trivial, da sowohl H als auch H' in $< H, H' >$ enthalten sind. Betrachte nun ein $x \in L^{H \cup H}$, das heißt $\sigma(x) = x$ für alle $\sigma \in H \cup H$, dann ist die Gleichung $\sigma(x) = x$ aber auch für alle $\sigma \in < H, H' >$ erfüllt. □

Satz 16.12 *(Translationssatz der Galois-Theorie)*
Es seien L/K eine endliche Galois-Erweiterung sowie $K/E/L$ und $K/E'/L$ Zwischenkörper. Weiter seien E/K und E'/K galoisch. Es gelten:
(a) EE'/K ist galoisch und die Abbildung

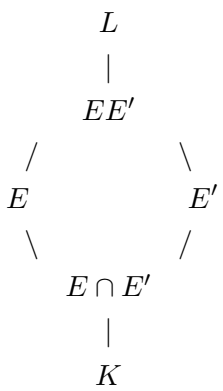
$$\begin{array}{rcl} \varphi : \mathrm{Gal}(EE'/E) & \to & \mathrm{Gal}(E'/E \cap E') \\ \sigma & \mapsto & \sigma_{|_{E'}} \end{array}$$

ist ein Gruppen-Isomorphismus.
(b) Die Abbildung

$$\begin{array}{rcl} \psi : Gal(EE'/K) & \hookrightarrow & Gal(E/K) \times Gal(E'/K) \\ \sigma & \mapsto & (\sigma_{|_E}, \sigma_{|_{E'}}) \end{array}$$

ist ein injektiver Gruppen-Homomorphismus.
Gilt zusätzlich $K = E \cap E'$, so ist ψ auch surjektiv.

Inklusionstafel



Beweis. Zu (a)
Zuerst zeigen wir, dass EE'/K normal und separabel ist. Hierbei ist klar, dass EE'/K endlich und separabel ist, da L/K endlich und separabel ist. EE'/K ist normal, denn sei $\sigma \in \mathrm{Gal}(L/K)$ dann gelten $\sigma(E) = E$ und $\sigma(E') = E'$, da E/K und E'/K normal sind. Hieraus folgt sofort, dass

$\sigma(EE') = EE'$ ist. EE'/K ist also eine endliche Galois-Erweiterung.
Es ist klar, dass φ Gruppen-Homomorphismus ist. Schnell sehen wir ein, dass φ injektiv ist, denn für $\sigma \in \mathrm{Ker}(\varphi)$ gilt $\sigma_{|_{E'}} = id_{E'}$ und $\sigma_{|_E} = id_E$, also ist jedes σ im Kern von φ die Identität auf EE'.
φ ist surjektiv, denn

$$(E')^{\mathrm{Im}(\varphi)} = E' \cap (EE')^{\mathrm{Gal}(EE'/E)}$$

Diese Gleichheit lässt sich leicht nachrechnen:
„$\subseteq$“: $x \in E' \wedge \sigma(x) = x \ \ \forall \sigma \in \mathrm{Gal}(EE'/E) \Rightarrow x \in E' \cap (EE')^{\mathrm{Gal}(EE'/E)}$
„$\supseteq$“: $x \in E' \cap (EE')^{\mathrm{Gal}(EE'/E)} \Rightarrow x \in (E')^{\mathrm{Im}(\varphi)}$
Nach dem Hauptsatz der Galois-Theorie 16.6 lässt sich diese Gleichung fortsetzen zu:

$$(E')^{\mathrm{Im}(\varphi)} = E' \cap (EE')^{\mathrm{Gal}(EE'/E)} = E' \cap E = (E')^{\mathrm{Gal}(E'/E \cap E')}$$

Da E' unter zwei Gruppen fixiert ist folgt wiederum mit Satz 16.6 und der Abbildung Ψ

$$\mathrm{Im}(\varphi) = \mathrm{Gal}(E'/E \cap E')$$

Zu (b)
Auch hier ist klar, dass ψ ein Gruppen-Homomorphismus ist. Die Injektivität zeigen wir analog zu (a). Setzen wir also nun Voraus, dass $K = E \cap E'$ gilt. Nach Teil (a) gelten die Isomorphien

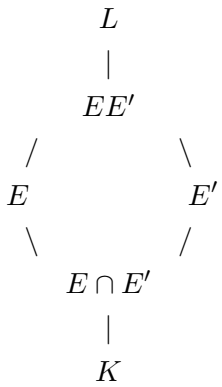
$$\mathrm{Gal}(E/K) \cong \mathrm{Gal}(EE'/E')$$

durch $\sigma \mapsto \tilde{\sigma}$ mit $\tilde{\sigma}_{|_E} = \sigma$ und

$$\mathrm{Gal}(E'/K) \cong \mathrm{Gal}(EE'/E)$$

durch $\sigma' \mapsto \tilde{\sigma}'$ mit $\tilde{\sigma}'_{|_{E'}} = \sigma'$
Setze: $\tau := \tilde{\sigma} \circ \tilde{\sigma}' \in \mathrm{Gal}(EE'/K)$, dann gilt: $\psi(\tau) = (\tau_{|_E}\,,\, \tau_{|_{E'}}) = (\,\tilde{\sigma} \circ \tilde{\sigma}'_{|_E}\,,\, \tilde{\sigma} \circ \tilde{\sigma}'_{|_{E'}}) = (\sigma, \sigma')$
Das heißt, dass ψ surjektiv ist. □

Anmerkung Der translationssatz der Galois-Theorie in Worten:
Teil (a) von Satz 16.12 besagt, dass die Galois-Gruppen der sich im nebenstehenden Diagramm diagonal gegenüberstehenden Körpererweiterungen isomorph zueinander sind.
Nach Teil (b) ist die Galois-Gruppe von EE'/K im Produkt der Galois-Gruppen von E/K und E'/K enthalten. Sie ist sogar gleich diesem Produkt, wenn $E \cap E' = K$ ist.
Wir können damit Beobachtungen, die wir an den Galois-Gruppen von EE'/E, EE'/E' oder EE'/K gemacht haben auf einfache Weise auf die Galois-Gruppen von E/K bzw. E'/K übertragen und umgekehrt. Ein beispiel dafür liefert die nächste



Folgerung 16.13 *Seien L/K eine endliche Galois-Erweiterung und E, E' Zwischenkörper mit E/K und E'/K abelsch, dann ist auch $\mathrm{Gal}(EE'/K)$ abelsch.*

Beweis. Via ψ aus Satz 16.12 kann $\mathrm{Gal}(EE'/K)$ als Untergruppe von $\mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$ aufgefasst werden. □

17 Auflösbare Gleichungen und Radikalkörper

Motivation: Gesucht ist eine Lösungsformel für $f(X) := X^2 + pX + q$ mit $f(X) = 0$ Dazu setzen wir eine Körpercharakteristik ungleich 2 voraus.Wir kennen die Lösung als pq-Formel:

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

Komplizierter ist die Lösungsformel für $f(X) = X^3 + pX + q$ mit $f(X) = 0$, hierfür setzen wir eine Körpercharakteristik ungleich 2 und 3 voraus. Sei nun $\zeta := \zeta_3 := e^{\frac{2i\pi}{3}}$ eine primitive dritte Einheitswurzel, weiter seien

$$u := \sqrt[3]{-\frac{p}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{p}{2}\right)^2}} \quad \text{und} \quad v := \sqrt[3]{-\frac{p}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{p}{2}\right)^2}}$$

dann erhalten wir als Lösung für X:

$$X = u + v \text{ oder } X = \zeta^2 u + \zeta v \text{ oder } X = \zeta u + \zeta^2 v$$

Wir wollen für den Fall, dass die Lösungen von $f(X) = 0$ Wurzeln oder genauer „Radikale“ sind, eine Sprechweise festhalten:

Definition 17.1 *(durch Radikale auflösbar)*
Sei K ein vollkommener Körper
(a) Eine endliche Körpererweiterung L/K heißt durch Radikale auflösbar, falls Zerfällungskörper E_i existieren, die die Eigenschaft $K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_r = L$ besitzen wobei $E_i = E_{i-1}(\alpha_i)$, für eine Nullstelle α_i von $X^n - a_i \in E_{i-1}[X]$, ist. Also gilt $\alpha_i = \sqrt[n_i]{a_i}$ für $i = 1, \ldots, r$.
Bei dieser Definition ist insbesondere $X^n - 1$ erlaubt.
(b) Sei $f \in K[X]$ ein Polynom, dann heißt f (genauer: Die Gleichung $f(X) = 0$) durch Radikale auflösbar, falls die Körpererweiterung N/K, mit einem Zerfällungskörper N von f, durch Radikale auflösbar ist.

Anmerkung zu (b) f ist durch Radikale auflösbar, wenn sich die Nullstellen von f in $\bar{K}$ durch n-te Wurzeln ausdrücken lassen. Insbesondere ist nach der Motivation jedes Polynom f mit $\deg(f) \leq 3$ durch Radikale auflösbar.

Bemerkung 17.2 *Sei $n \geq 1$ eine natürliche Zahl und $a \in \mathbb{Z}$. Dann sind äquivalent:*
(i) $< \bar{a} >= \mathbb{Z}/n\mathbb{Z}$ ***(ii)*** $\bar{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ ***(iii)*** $\mathrm{ggT}(a, n) = 1$ ***(iv)*** $\exists\, u \in \mathbb{Z}/n\mathbb{Z} : \bar{1} = \bar{a}\bar{u}$

Beweis. $< \bar{a} >= \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists\, \bar{u} \in \mathbb{Z}/n\mathbb{Z} : \bar{1} = \bar{u}\bar{a} \Leftrightarrow \exists\, u, r \in \mathbb{Z} : 1 = au + nr \Leftrightarrow \mathrm{ggT}(a, n) = 1$ □

Definition 17.3 *(Eulersche φ-Funktion)*
Für eine natürliche Zahl $n \geq 1$ setze $\varphi(n) := \mathrm{Card}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right)$

Bemerkung 17.4 *(Eigenschaften der Eulerschen φ-Funktion)*
(a) Für je zwei natürliche Zahlen $n, m \geq 1$ deren größter gemeinsame Teiler $\mathrm{ggT}(m, n) = 1$ ist gilt $\varphi(n, m) = \varphi(n) \cdot \varphi(m)$
(b) Für eine Primzahl p und eine natürliche Zahl $r \geq 1$ gilt $\varphi(p^r) = p^{r-1}(p - 1)$

Beweis. Die Behauptung in (a) ist eine direkte Folgerung aus dem chinesischen Restsatz. Bei (b) betrachte die Menge der nicht Einheiten in $\mathbb{Z}/p^r\mathbb{Z} = \{0, 1, \ldots, p^r - 1\}$ diese ist

$$\{0 \cdot p, 1 \cdot p, \ldots, (p^{r-1} - 1) \cdot p\} =: N$$

Es gilt:

$$\mathrm{Card}(N) = p^{r-1} \Rightarrow \mathrm{Card}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right) = p^r - p^{r-1} = p^{r-1}(p-1)$$

□

Definition und Bemerkung 17.5 *(Gruppe der n-ten Einheitswurzenl)*
Sei L/K eine Körpererweiterung und $\bar{K}$ ein algebraischer Abschluss von K. Wir betrachten das Polynom $f(X) := X^n - 1 \in K[X]$ und definieren $\mu_n(\bar{K})$ als die Menge der Nullstellen von $X^n - 1$ in $\bar{K}$. $(\mu_n(\bar{K}), \cdot)$ bildet eine zyklische Gruppe der Ordnung m mit:

$$m = \begin{cases} n & \text{falls } \mathrm{Char}(K) \nmid n \\ a & \text{falls } \mathrm{Char}(K) = p \mid n \text{ also } n = p^r \cdot a \text{ mit } \mathrm{ggT}(p, a) = 1 \end{cases}$$

$\mu_n(\bar{K})$ heißt die Gruppe der n-ten Einheitswurzeln von $\bar{K}$.

Beweis. : 9. Übungsblatt Aufgabe 5

Definition 17.6 *(Kreisteilungskörper)*
Sei $\mu_n(\bar{K})$ wie in Definition 17.5 und $\zeta \in \mu_n(\bar{K})$. Weiter sei r die Ordnung von ζ in $\mu_n(\bar{K})$. Dann nennen wir ζ eine primitive r-te Einheitswurzel.
Ist die Charakteristik von K gleich Null oder teilt diese nicht n, dann nennen wir den Körper $K(\mu_n(\bar{K}))$, der durch Adjunktion der n-ten Einheitswurzeln entsteht, den n-ten Kreisteilungskörper über K.

Definition und Satz 17.7 *(Kreisteilungs Charakter)*
Seien K ein Körper, $n \in \mathbb{N}_{>0}$ eine natürliche Zahl und gelte $\mathrm{Char}(K) = 0$ oder $\mathrm{Char}(K) \nmid n$. Weiter sei $\zeta \in \bar{K}$ eine primitive n-te Einheitswurzel, dann gelten:
(a) $K(\zeta) = K(\mu_n(\bar{K}))$ und $K(\zeta)/K$ ist abelsch galoisch.
(b) $[K(\zeta) : K]$ teilt $\varphi(n)$ mit $\varphi(n)$ aus Definition 17.3
(c) Die Abbildung:

$$\chi : \mathrm{Gal}(K(\zeta)/K) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

die durch $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, für $\sigma \in \mathrm{Gal}(K(\zeta)/K)$, bestimmt ist, ist ein injektiver Gruppen-Homomorphismus. χ heißt n-ter zyklotomischer (bzw. kreisteilungs) Charakter.

Beweis. Zu (a):

$$X^n - 1 = \prod_{i=1}^{n} (X - \zeta^i) \in \bar{K}[X]$$

Damit ist $K(\zeta) = K(\mu_n(\bar{K}))$ Zerfällungskörper von $X^n - 1$ über K. Wegen der Voraussetzung an die Charakteristik von K ist $X^n - 1$ separabel.
Wir wissen jetzt, dass $K(\mu_n(\bar{K}))/K$ galoisch ist und können nun (c) Beweisen, da uns dies den Beweis von (a) und (b) erleichtert:
χ ist wohldefiniert, denn sei $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ dann betrachte: $\sigma(\zeta) = \zeta^i$ für $i \in \{1, \ldots, n\}$,

außerdem ist die Ordnung von $\sigma(\zeta))$ gleich n, da σ bijektiv ist.
Wir betrachten den Gruppen-Isomorphismus

$$\begin{array}{rccc} \phi : & \mathbb{Z}/n\mathbb{Z} & \tilde{\to} & \mu_n(\bar{K}) \\ & r & \mapsto & \zeta^r \end{array}$$

Sei nun j ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$. Nach Bemerkung 17.2 ist j dann eine Einheit von $\mathbb{Z}/n\mathbb{Z}$ und genau dann ist ζ^j ein Erzeuger von $\mu_n(\bar{K})$. ζ ist als primitive n-te Einheitswurzel ein Erzeuger von $\mu_n(\bar{K})$ und jedes $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ ist bijektiv, also ist auch $\sigma(\zeta) = \zeta^i$ ein Erzeuger von $\mu_n(\bar{K})$. Mit ϕ ist dann auch i ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$. Damit i eine Einheit in $\mathbb{Z}/n\mathbb{Z}$ und $\chi(\sigma) = i \Rightarrow \chi$ ist wohldefiniert.
χ ist Gruppen-Homomorphismus, denn seinen $\sigma, \tau \in \mathrm{Gal}(K(\zeta)/K)$, dann gilt:

$$\begin{array}{rcl} \zeta^{\chi(\sigma\tau)} & = & \sigma \circ \tau(\zeta) = \sigma(\zeta^{\chi(\tau)}) = (\zeta^{\chi(\sigma)})^{\chi(\tau)} = \zeta^{\chi(\sigma)\cdot\chi(\tau)} \\ & \Rightarrow & \chi(\sigma \circ \tau) = \chi(\sigma) \cdot \chi(\tau) \end{array}$$

χ ist injektiv, denn sei $\sigma \in \mathrm{Ker}(\chi) \Rightarrow \sigma(\zeta) = \zeta^1 = \zeta \Rightarrow \sigma = id_{K(\zeta)} = id$
Nun beweisen wir den Rest von (a) und (b):
Mittels χ können wir $\mathrm{Gal}(K(\zeta)/K)$ als Untergruppe von $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ auffassen. Da Untergruppen abelscher Gruppen abelsch sind, ist $\mathrm{Gal}(K(\zeta)/K)$ abelsch.
Weiterhin gilt:

$$[K(\zeta) : K] = [K(\zeta) : K]_S = \mathrm{Card}\left(\mathrm{Gal}(K(\zeta)/K)\right) \;\Big|\; \mathrm{Card}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right) = \varphi(n)$$

□

Definition und Bemerkung 17.8 *(n-tes Kreisteilungspolynom.)*
Sei $n \in \mathbb{N}_{>0}$ eine natürliche Zahl, dann fixiere $\bar{\mathbb{Q}}/\mathbb{Q}$ einen algebraischen Abschluss. Weiter definiere die Menge $EW_n := \{\, \zeta \in \bar{\mathbb{Q}} \,|\, \zeta$ ist primitive n-te Einheitswurzel $\}$. Das n-te Kreisteilungspolynom ist definiert als

$$\Phi_n(X) = \prod_{\zeta \in EW_n} (X - \zeta) \quad \in \bar{\mathbb{Q}}[X]$$

Es gelten:
(i) $\Phi_n(X) \in \mathbb{Q}[X]$
(ii) $\deg(\Phi_n) = \varphi(n)$
(iii) Sei p prim, dann ist $\Phi_p(X) = X^{p-1} + \cdots + x + 1$

Beweis. zu (i):
Zur besseren Lesbarkeit definiere $G := \mathrm{Gal}(\mathbb{Q}(\mu(\bar{\mathbb{Q}}))/\mathbb{Q})$. Die Elemente von G permutieren die Menge der primitiven n-ten Einheitswurzeln nur, das heißt:

$$\sigma \in G \Rightarrow \sigma(\Phi_n) = \Phi_n$$

Also ist Φ_n invariant unter G und damit liegen nach dem Hauptsatz der Galoistheorie 16.6 die Koeffizienten von Φ_n im Fixkörper $[\mathbb{Q}(\mu(\bar{\mathbb{Q}}))]^G = \mathbb{Q}$ also ist $\Phi_n(X) \in \mathbb{Q}[X]$
Teil (ii) ist sofort klar mit Satz 17.7 und zu (iii) gilt:
Jedes $\zeta \in \mu_p(\bar{\mathbb{Q}})$ mit $\zeta \neq 1$ ist eine primitive p-te Einheitswurzel und somit gilt

$$X^p - 1 = (X - 1) \cdot (X^{p-1} + \cdots + X + 1)$$

□

Satz 17.9 *Für alle natürlichen Zahlen n hat das n-te Kreisteilungspolynom $\Phi_n(X)$ ganzzahlige Koeffizienten und ist irreduzibel.*

Beweis. Wir zeigen im ersten Schritt induktiv, dass $\Phi_n(X) \in \mathbb{Z}[X]$ ist. Hierbei ist der Induktionsanfang trivial, denn für n = 1 gilt: $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$ und für den Schritt von $n-1$ auf n gilt:

$$\begin{aligned} X^n - 1 &= \prod_{\substack{d|n \\ d>0}} \Phi_d(X) \\ &= \Phi_n(X) \cdot \prod_{\substack{d|n \\ 0<d<n}} \Phi_d(X) \end{aligned}$$

Da sowohl das Produkt der Φ_d als auch $X^n - 1$ Elemente in $\mathbb{Z}[X]$ sind, muss auch Φ_n in $\mathbb{Z}[X]$ liegen. Nun werden wir im zweiten Schritt die Irreduzibilität zeigen. Für den Fall, dass n eine Primzal ist, haben wir dies bereits im Beispiel 17 (c) auf Seite 35 dieser Mitschrift gezeigt, nun zeigen wir dies auch für nicht Primzahlen n.
Im zweiten Schritt nehmen wir uns eine Zerlegung von Φ_n her. Sei $\Phi_n = f \cdot g \in \mathbb{Z}[X]$ eine Darstellung von Φ_n mit einem irreduziblen Polynom $f \in \mathbb{Z}[X]$ und sei ζ eine primitive n-te Einheitswurzel, die eine Nullstelle von f ist.

Behauptung 1 *Für alle Primzahlen p, die n nicht teilen ist $f(\zeta^p) = 0$*

Beweis. Wir nehmen an, dass $f(\zeta^p) \neq 0$ sei. Da ζ^p eine primitive n-te Einheitswurzel ist, muss $g(\zeta^p) = 0$ gelten. Da nach Voraussetzung der größte gemeinsame Teiler von n und p Eins ist folgt mit Bemerkung 17.2, dass p eine Einheit von $\mathbb{Z}/n\mathbb{Z}$ ist.
Damit ist ζ eine Nullstelle von $g(X^p)$ und das Minimalpolynom von ζ ist f daher muss f das Polynom $g(X^p)$ teilen. Wir können also ein $h \in \mathbb{Z}[X]$ finden, so dass $g(X^p) = f \cdot h$ gilt. Nun reduzieren wir die Polynome modulo p und betrachten die Polynome in $\mathbb{F}_p[X]$. In diesem Polynomring können wir den Frobenius-Automorphismus anwenden, daher gilt:

$$\bar{g}(X^p) = (\bar{g}(X))^p = \bar{f}\bar{h} \Rightarrow \mathrm{ggT}(\bar{f}, \bar{g}) \neq 1$$

Dies ist ein Widerspruch, da $\bar{f} \cdot \bar{g} = \overline{\Phi_n} \mid \overline{X^n - 1}$ und $\overline{X^n - 1}$ in $\mathbb{F}_p[X]$ separabel ist, weil es keine mehrfachen Faktoren enthalten darf und da p nicht n teilt. △

Behauptung 2 *Jede primitive n-te Einheitswurzel η ist eine Nullstelle von f.*

Beweis. Es gilt $\eta = \zeta^r$ für $r \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

$$r = \prod_{i=1}^{s} p_i$$

Sei die Primfaktorzerlegung von r, dann gilt für alle i, dass die p_i nicht n teilen. Deshalb gilt nach Behauptung 1

$$0 = f(\zeta) = f((\zeta^{p_1})^{p_2}) = \ldots = f(\zeta^r) = f(\eta)$$

△

Mit den Behauptungen 1 und 2 folgt nun $g = 1$ und somit $f = \Phi_n$ □

Folgerung 17.10 *Sei $\zeta_n \in \bar{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Es gelten:*
(a) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$
(b) Der Kreisteilungscharakter

$$\chi : \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \;\to\; \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$$

aus Satz 17.7 ist ein Gruppen-Isomorphismus.

Beweis. Φ_n ist irreduzibel und hat den Grad $\varphi(n)$ daher gilt (a) und Teil (b) folgt sofort aus (a). □

Bemerkung 17.11 *(Radikalkörper)*
Seien K ein Körper, $a \in K$ ein Element und $n \in \mathbb{N}_{>0}$ eine natürliche Zahl. Weiter sei die Charakteristik von K gleich Null oder teile nicht n. Der Zerfällungskörper des Polynoms

$$f(X) \;:=\; X^n - a \;\in K[X]$$

ist $K(\sqrt[n]{a}, \mu_n)$ wobei $\mu_n := \mu_n(\bar{K})$ die Gruppe der n-ten Einheitswurzeln ist.

Beweis. Durch Faktorisieren von f in $\bar{K}[X]$ erhalten wir

$$f(X) = \prod_{i=1}^{n}(X - \sqrt[n]{a} \cdot \zeta^i)$$

mit $<\zeta>=\mu_n$ Also ist $L = K(\zeta, \zeta^2, \ldots, \sqrt[n]{a}) = K(\zeta, \sqrt[n]{a}) = K(\mu_n, \sqrt[n]{a})$ □

Bemerkung 17.12 *In der Situation von Bemerkung 17.11 mit der zusätzlichen Voraussetzung, dass μ_n eine Teilmenge von K ist, gilt:*
(a) $K(\sqrt[n]{a})/K$ ist eine ablesche Galois-Erweiterung.
(b) Die Abbildung

$$\phi : G := \mathrm{Gal}(K(\sqrt[n]{a})/K) \;\to\; \mathbb{Z}/n\mathbb{Z}$$

welche durch $\sigma(\sqrt[n]{a}) = \sqrt[n]{a} \cdot \zeta^{\phi(\sigma)}$ beschrieben ist, ist ein injektiver Gruppen Homomorphismus. Hierbei ist $\mu_n =<\zeta>$ zyklisch.

Beweis. Wir zeigen für Teil (a) zunächst nur, dass $K(\sqrt[n]{a})/K$ galoisch ist.
Nach Bemerkung 17.11 und der Voraussetzung $\mu_n \subseteq K$ gilt, dass $K(\sqrt[n]{a}, \zeta) = K(\sqrt[n]{a})$ ist.
Hieraus folgt, dass $K(\sqrt[n]{a})$ ein Zerfällungskörper von $f(X) := X^n - a \in K[X]$ und somit normal über K ist. Die Separabilität von $K(\sqrt[n]{a})$ ist auch klar, da wir eine Körpercharakteristik von Null vorausgesetzt haben.
Für (b) zeige nun, dass ϕ wohldefiniert ist. Jedes $\sigma \in G := \mathrm{Gal}(K(\sqrt[n]{a})/K)$ sendet die Nullstelle $\sqrt[n]{a}$ notwendig auf eine Nullstelle von $X^n - a$, also auf ein Element der Form: $\sqrt[n]{a} \cdot \zeta^i$ für ein $i = 0, \ldots, n$. Benenne nun $i = \phi(\sigma)$. Weiter ist ϕ ein Gruppen-Homomorphismus, denn seien $\sigma, \tau \in G$ dann betrachte:

$$\begin{aligned}
\sqrt[n]{a}\,\zeta^{\phi(\sigma\circ\tau)} &= \sigma(\tau(\sqrt[n]{a})) = \sigma(\sqrt[n]{a}\,\zeta^{\phi(\tau)}) \\
&= \zeta^{\phi(\tau)}\,\zeta^{\phi(\sigma)}\,\sqrt[n]{a} = \zeta^{\phi(\sigma)+\phi(\tau)}\,\sqrt[n]{a} \\
&\Rightarrow \quad \phi(\sigma \circ \tau) = \phi(\sigma) + \phi(\tau)
\end{aligned}$$

Nun zeigen wir die Injektivität: Für $\sigma \in \mathrm{Ker}(\phi)$ gilt: $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\zeta^0 = \sqrt[n]{a}$
Also $\sigma = id_{K(\sqrt[n]{a})}$und damit ist σ das neutrale Element in G.
Damit folgt auch der Rest von (a), denn wir können G nun als Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ auffassen, daher ist G abelsch. □

Definition und Satz 17.13 *(Galois-Hülle)*
Seien E/K eine endliche Galois-Erweiterung und $n \in \mathbb{N}_{>0}$ Weiter sei die Charakteristik von K gleich Null oder teile nicht n und $\zeta \in E$ sei eine primitive n-te Einheitswurzel sowie $a \in E$ ein Element. Sei N der kleinste Galois-Erweiterungskörper über K, der $E(\sqrt[n]{a})$ enthält, dann heißt N die Galois-Hülle von $E(\sqrt[n]{a})$ über K. Es gelten:
(a) $N = E(\sqrt[n]{\sigma(a)}) \,|\, \sigma \in G)$ mit $G := \mathrm{Gal}(E/K)$
(b) $H := \mathrm{Gal}(N/E)$ ist abelsch

Beweis. Zu (a)
Wir führen zunächst die Bezeichnungen $\{\, \sigma(a) | \sigma \in G \,\} =: \{a = a_1, \ldots, a_r\,\}$ ein und definieren damit das Polynom

$$F(X) = \prod_{j=1}^{r} (X^n - a_j) \in E[X]$$

Für $\sigma \in G$ gilt dann

$$\sigma(F(X)) = \prod (X^n - \sigma(a_j)) = \prod (X^n - a_j) = F(X)$$

Also liegen die Koeffizienten von $F(X)$ im Fixkörper $E^G = K$ also $F(X) \in K[X]$.
Seien M ein Zerfällungskörper von F über K, also $M = K(\sqrt[n]{a_i} | i = 1, \ldots, r)$ und $\tau \in \mathrm{Gal}(N/K)$ mit $\tau_{|_E} = \sigma$.
Es gilt $[\tau(\sqrt[n]{a})]^n = \tau([\sqrt[n]{a}]^n) = \tau(a) = \sigma(a)$ also ist $\tau(\sqrt[n]{a})$ eine n-te Wurzel von $\sigma(a)$ und somit ist $\tau(\sqrt[n]{a})$ ein Element in $E(\sqrt[n]{\sigma(a)})$. Damit haben wir die Inklusion $M \subseteq N$ gezeigt, da aber N/K die kleinste Erweiterung ist, die $E(\sqrt[n]{a})$ enthält, folgt, dass $N = M$ sein muss.
Zu (b)
Wir schreiben N als Kompositum[1] der $E(\sqrt[n]{a_i})$, also:

$$N = E(\sqrt[n]{a}) E(\sqrt[n]{a_2}) \ldots E(\sqrt[n]{a_r})$$

nach Bemerkung 17.12 sind alle $E(\sqrt[n]{a_i})/K$ abelsch und Folgerung 16.13 besagt, dass das Kompositum abelscher Gruppen abelsch ist. □

[1] Zur Definition des Kompusitum siehe 16.10

18 Durch Radikale auflösbare Körpererweiterungen

Satz 18.1 *Seien K ein vollkommener Körper (also ist insbesondere jedes irreduzible Polynom separabel) und L/K eine durch Radikale auflösbare Körpererweiterung, das heißt es existieren Körper E_i für $i = 1, ..., r$ mit $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = L$ mit der Eigenschaft, dass für Nullstellen α von $X^{n_i} - a_i \in E_{i-1}[X]$ die Identität $E_i = E_{i-1}(\alpha)$ gilt. Dann gibt es Körper $F_0, \ldots, F_{2r}$ mit:*

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{2r} \quad \text{und} \quad L \subseteq F_{2r}$$

wobei F_{2r}/K galoisch ist. Weiter gilt, dass jede Erweiterung F_{i+1}/F_i abelsch und galoisch ist.

Beweis. Konstruktiv:
Wir setzen $F_0 := E_0 = K$ unf für $i > 0$ setzen wir:

$$F_{2i-1} := F_{2i-2}(\mu_{n_i}) \text{ und } F_{2i} := F_{2i-1}(\, \sqrt[n_i]{\sigma(a_i)} \,|\, \sigma \in \mathrm{Gal}(F_{2i-1}/K)\,)$$

Nach Satz 17.7 ist F_{2i-1}/F_{2i-2} abelsch und F_{2i-1} ist das Kompositum von $K(\mu_{n_i})F_{2i-2}$. Da nach Satz 16.12 das Kompositum von Galois-Erweiterungen galoisch ist, ist auch F_{2i-2}/K eine Galois-Erweiterung.
Nach Satz 17.13 sind F_{2i}/F_{2i-1} sowie F_{2i}/K galoisch. □

Anmerkung: Wir formulieren Satz 18.1 in Termen von Galois-Gruppen:

$$\mathrm{Gal}(F_{2r}/K) \trianglerighteq \mathrm{Gal}(F_{2r}/F_1) \trianglerighteq \cdots \trianglerighteq \{id\}$$

mit der Eigenschaft:

$$\mathrm{Gal}(F_{2r}/F_i)\big/\mathrm{Gal}(F_{2r}/F_{i+1}) \overset{\text{(16.6 c)}}{\cong} \mathrm{Gal}(F_{i+1}/F_i) \text{ abelsch}$$

Da diese Anmerkung so wichtig ist erheben wir sie zur nächsten

Definition 18.2 *(Normalreihe, auflösbare Gruppen)*
Sei G eine endliche Gruppe.

(a) Eine Folge von Untergruppen mit $G =: G_0 \geq G_1 \geq \cdots \geq G_r \geq \{e\}$ heißt Normalreihe von G, falls für alle $i = 0, \ldots, r-1$ gilt, dass G_{i+1} ein Normalteiler von G_i ist.
(b) Die Quotienten G_i/G_{i+1} heißen Faktoren der Normalreihe.
(c) G heißt auflösbar, falls sie eine Normalreihe mit abelschen Faktoren besitzt.

Folgerung 18.3 *die Galois-Gruppe $\mathrm{Gal}(F_{2r}/K)$ aus Satz 18.1 ist auflösbar.* □

Definition 18.4 *(Kommutatorgruppe)*
Es sei G eine Gruppe mit Untergruppen $H_1, H_2 \leq G$ sowie Elementen $a, b \in G$. Wir definieren $[a, b] := a\,b\,a^{-1}b^{-1}$ den Kommutator von a und b, sowie $[H_1, H_2] := < [a, b] \,|\, a \in H_1 \wedge b \in H_2 >$ die Kommutatorgruppe von H_1 und H_2. Weiter ist $G' := [G, G]$ die Kommutatorgruppe (bzw. Abgeleitete Gruppe) von G.

Anmerkung Ist G eine abelsche Gruppe, so gilt $[a, b] = aba^{-1}b^{-1} = abb^{-1}a^{-1} = e$ für alle $a, b \in G$.

Bemerkung 18.5 *Ist G eine Gruppe, so gelten:*
(a) G' besteht aus allen Produkten von allen möglichen Kommutatoren in G
(b) G' ist Normalteiler von G
(c) G/G' ist abelsch und
(d) Wenn es einen Normalteiler $N \trianglelefteq G$ gibt, so dass G/N abelsch ist, dann ist $G' \subseteq N$

Beweis. Zu (a)

$$[a,b] \circ [b,a] = a\,b\,a^{-1}b^{-1}\ b\,a\,b^{-1}a^{-1} = e \Rightarrow [a,b]^{-1} = [b,a]$$

Zu (b)
Sei $g \in G$ ein Element, dann betrachte:

$$\begin{aligned} g[a,b]g^{-1} &= g\,a\,b\,a^{-1}b^{-1}g^{-1} \\ &= g\,a\,g^{-1}g\,b\,g^{-1}\ g\,a^{-1}g^{-1}g\,b^{-1}g^{-1} \quad \text{durch Einfügen von: } e = g^{-1}g \\ &= [gag^{-1}, gbg^{-1}] \in G' \end{aligned}$$

Zu (c)
Es gilt: $ab = [a,b]\,ba$, denn $[a,b]\,ba = a\,b\,a^{-1}b^{-1}b\,a = ab$. Wir betrachten diese Formel in G/G'

$$\overline{ab} = \overline{[a,b]\,ba} = \overline{e}\,\overline{ba} = \overline{ba}$$

Damit ist G/G' abelsch.
Zu (d)
Es existiere ein N wie beschrieben, dann gilt

$$\overline{[a,b]} = \overline{a\,b\,a^{-1}b^{-1}} = \overline{e} \in G/N$$

also ist $[a,b] \in N$ für alle $a, b \in G$. Hieraus folgt die Behauptung. □

Erinnerung (Symmetrische - / alternierende Gruppe)
Sei N eine Menge mit $n \in \mathbb{N}_{>1}$ Elementen, dann heißt

$$S_n \ := \ \left\{ \tau : N \to N \,\middle|\, \tau \text{ ist bijektiv} \right\}$$

die Symmetrische Gruppe der Ordnung n. Die Alternierende Gruppe $A_n \subseteq S_n$ der Ordnung n ist die Gruppe der geraden Permutationen in S_n.

Satz 18.6 *Es sei $n \in \mathbb{N}_{>1}$ eine natürliche Zahl.*
(a) In der symmetrischen Gruppe S_n für $a_i = \{1, \ldots, n\}$ und $r \leq n$ gilt

$$(a_1\,a_2\,\ldots a_r) = (a_1\,a_2) \circ (a_3\,a_4) \circ \ldots \circ (a_{r-1}\,a_r)$$

(b) Die symmetrische Gruppe S_n wird von Transpositionen (2-Zykeln) erzeugt.
(c) Die alternierende Gruppe A_n wird von 3-Zykeln erzeugt.
(d) Die alternierende Gruppe ist von der symmetrischen abgeleitet, also $S_n' = A_n = [S_n, S_n]$
(e) Die von der alternierenden Gruppe abgeleitete Gruppe ist

$$A_n' = \begin{cases} \{e\} & \text{für } 1 < n \leq 3 \\ V_4 := \{e, (12)(34), (13)(24), (14)(23)\} & \text{für } n = 4 \\ A_n & \text{sonst} \end{cases}$$

Beweis. Teil (a) lässt sich leicht nachrechnen und (b) folgt direkt aus (a). Für den Beweis von Teil (c) genügt es die möglichen Ergebnise von zwei verknüpften Transpositionen zu betrachten. Seien dazu $a_1, a_2, a_3, a_4 \in \{1, \ldots, n\}$ mit $a_i \neq a_j$ für $i \neq j$. Betrachte:
$(a_1\, a_2) \circ (a_2\, a_1) = e$
$(a_1\, a_2) \circ (a_2\, a_3) = (a_1\, a_2\, a_3)$
$(a_1\, a_2) \circ (a_3\, a_4) = (a_1\, a_2\, a_3) \circ (a_1\, a_3\, a_4)$
Zu (d)
$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ (für $n \geq 2$) mit Bemerkung 18.5 d) ist dann S_n' eine Untergruppe von A_n. Es bleibt zu zeigen, dass $A_n \leq S_n'$ ist, also müssen wir zeigen, dass jeder 3-Zykel ein Kommutator ist:

$$(a_1\, a_2\, a_3) = (a_1\, a_3) \circ (a_2\, a_3) \circ (a_1\, a_3)^{-1} \circ (a_2\, a_3)^{-1} = [(a_1\, a_3), (a_2\, a_3)]$$

Zu (e)
$A_2' = \{e\}$ ist klar, es gilt $A_3 =< (1\,2\,3) > \cong \mathbb{Z}/3\mathbb{Z}$ damit ist A_3 abelsch, also muss $A_3' = \{e\}$ gelten.
zu ($n = 4$): $V_4 := \{e, (12)(34), (13)(24), (14)(23)\}$ ist Untergruppe von S_4,
zeige: $V_4 \trianglelefteq S_4$. Sei also $g \in S_4$, dann gilt: $g(12)(34)g^{-1} = (g(1)\, g(3))(g(3)\, g(4))$
$\mathrm{Card}\left(\left(S_4/V_4\right)\right) = \frac{12}{4} = 3$ also ist $S_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ und damit folgt mit Bemerkung 18.5 d), dass A_4' eine Untergruppe von V_4 ist.
Zu $V_4 \leq A_4$ betrachte: $(a_1\, a_2)(a_2\, a_4) = [(a_1\, a_2\, a_3), (a_1\, a_2\, a_4)] \in A_4'$
Zu ($n \geq 5$): Es ist per Definition klar, dass $A_n' \leq A_n$ gilt.
Zu $A_n \leq A_n'$ sei $(a_1\, a_2\, a_3) \in A_n$ und wähle hierzu a_4, a_5 mit $a_i \neq a_j$ für $i \neq j$. Dann gilt:

$$(a_1\, a_2\, a_3) = [(a_1\, a_2\, a_4), (a_1\, a_3\, a_5)] \in A_n'$$

□

Definition 18.7 *(höhere Kommutatorgruppen)*
Sei G eine Gruppe. Schreibe $G =: D^0(G)$, $G' =: D^1(G)$.
Induktiv definieren wir $D^{i+1}(G) := [D^i(G), D^i(G)]$, die höheren Kommutatorgruppen.

Satz 18.8 *Sei G eine Gruppe, dann gelten:*
(a) $D^{i+1}(G)$ ist ein Normalteiler von $D^i(G)$ und $D^i(G)/D^{i+1}(G)$ ist abelsch.
(b) G ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ derart, dass $D^n(G) = \{e\}$ ist, gibt-

Beweis. Teil (a) ist eine Folgerung aus Bemerkung 18.5. Zu (b) „⇐“:

$$G := D^0(G) \trianglerighteq D^1(G) \trianglerighteq \ldots \trianglerighteq D^{n-1}(G) \trianglerighteq D^n(G) = \{e\}$$

Also ist G auflösbar.
zu „⇒“:
Nach Voraussetzung ist G auflösbar, mit $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{e\}$.
Nach Bemerkung 18.5 ist $D^1(G_i)$ dann eine Untergruppe von G_{i+1}.

Behauptung 1 *$D^i(G)$ ist eine Untergruppe von G_i*

Beweis. Induktiv: $(i = 1):\ D^1(G) = G \leq G$ ist klar.
$(i \curvearrowright i+1):\ D^{i+1}(G) = [D^i(G), D^i(G)] \leq [G_i, G_i] = D^1(G_i) \leq G_{i+1}$ △
Betrachte nun:

$$D^n(G) \leq G_n = \{e\} \Rightarrow D^n(G) = \{e\}$$

□

Folgerung 18.9 *Die Gruppen A_n und S_n sind genau dann auflösbar, wenn $n \leq 4$ ist.*

Beweis. Wir gehen die Fälle, die von Satz 18.6 (e) vorgegeben werden, durch:

$n \geq 5$ Betrachte $S_n' = [S_n, S_n] = DS_n = A_n$ nach Satz 18.6 und weiter sind $D^2S_n = [A_n, A_n] = A_n$ und $D^3S_n = A_n$ und so weiter. Die Folge wird also stationär.

$n = 2$ Es gilt $S_2 \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ und somit abelsch.

$n = 3$ Die Kette $\{e\} \trianglelefteq A_3 \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \trianglelefteq S_3$ hat die Eigenschaft, dass alle Faktoren abelsch sind.

$n = 4$ Die Kette $\{e\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ hat abelsche Faktoren.

□

Folgerung 18.10 *Sei G eine endliche Gruppe.*
(a) Sei $H \leq G$ eine Untergruppe. Ist G auflösbar, dann ist auch H auflösbar.
(b) Sei $N \trianglelefteq G$ ein Normalteiler. G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. Teil (a) ist trivial. Wir zeigen (b):
Sei zunächst G auflösbar, dann ist N auflösbar nach (a) und G besitzt eine Normalreihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = \{e\}$$

Es gibt ein $n \in 1, \ldots, r$ mit $N \subseteq G_n$. Damit ist

$${}^{G}\!/_{N} \trianglerighteq {}^{G}\!/_{G_n} \trianglerighteq {}^{G}\!/_{G_{n-1}} \trianglerighteq \ldots \trianglerighteq {}^{G}\!/_{G} = \{e\}$$

eine Normalreihe des Quotienten G/N.
Seien nun N und G/N auflösbar, dann konstruiere aus der Normalreihe des Quotienten eine Fortsetzung der Normalreihe von N zu einer Normalreihe von G. □

Anmerkung Sei $f \in K[X]$ ein Polynom und N/K ein Zerfällungskörper von f. Dann folgt aus der nicht Auflösbarkeit der Galoisgruppe $\mathrm{Gal}(N/K)$, dass die Gleichung $f(X) = 0$ nicht durch Radikale auflösbar ist.

Beweis. Die Gleichung $f(X) = 0$ ist genau dann durch Radikale auflösbar, wenn N/K durch Radikale auflösbar ist.
Nach Satz 18.1 ist die Galois-Gruppe einer durch Radikale auflösbaren Körpererweiterung N/K Normalteiler einer auflösbaren Gruppe G und der Quotiente

$${}^{G}\!/_{\mathrm{Gal}(N/K)}$$

ist abelsch. Also ist N/K auflösbar, wenn N/K durch Radikale auflösbar ist. □

Anmerkung Wir werden sehr bald sehen, dass wir die in der Anmerkung formulierte Aussage zu einer „genau dann, wenn“ Aussage erweitern können.

Folgerung 18.11 *Sei G eine auflösbare Gruppe, das heißt es gibt eine Kette*

$$G = G_0 \trianglerighteq \ldots \trianglerighteq G_r = \{e\}$$

mit abelschen Quotienten. Dann gibt es eine Verfeinerung dieser Normalreihe mit zyklischen Faktoren. Das heißt

$$G = G_0 = G_{0,0} \trianglerighteq G_{0,1} \trianglerighteq \ldots \trianglerighteq G_{0,s_0} = G_1 \trianglerighteq G_{1,1} \trianglerighteq \ldots \trianglerighteq G_{r-1,s_{r-1}} = G_r$$

derart, dass der Quotient zweier aufeinanderfolgenden Gruppen zyklisch ist.

Beweis. In zwei Schritten. Sei H eine abelsche Gruppen, dann ist nach dem Hauptsatz über endlich erzeugte abelsche Gruppen 3.12 H darstellbar als

$$H = \prod_{j=1}^{s} C_j \qquad \text{mit zyklischen Gruppen } C_j$$

Setze nun

$$H_i = \prod_{j=1}^{s-i} C_j$$

dann ist

$$H_i / H_{i+1} \cong C_{j-1}$$

Im zweiten Schritt verfeinern wir nun die Normalreihe $G_0 \trianglerighteq \ldots \trianglerighteq G_r$ wie folgt. Für $i = 1, \ldots, r$ betrachte die natürliche Projektion

$$\pi_i : G_i \to G_i / G_i + 1 =: H_i$$

Da die H_i nach Voraussetzung abelsch sind zerlegen wir diese nach Schritt eins in zyklische Gruppen und erhalten

$$G_0 = H_{0,0} \trianglerighteq H_{0,1} \trianglerighteq \ldots \trianglerighteq H_{0,s_0} = G_1 = H_{1,0} \trianglerighteq \ldots \trianglerighteq G_r$$

□

19 Galois-Gruppen von Polynomen

Wir haben weiter oben schon einmal das allgemeine Polynom zweiten Gerades

$$f(X) \;=\; X^2 + pX + q \;\in K(p,q)[X]$$

und die zugehörige Lösung $x = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$ von $f(x) = 0$ betrachtet. Wir haben festgehalten, dass damit diese Gleichung „durch Radikale auflösbar“ ist. Wir wollen nun in diesem Abschnitt das allgemeine Polynom n-ten Gerades definieren und betrachten welche dieser Polynome durch Radikale auflösbar sind. Mit der Anmerkung nach Folgerung 18.10 im vorhergegangenen Abschnitt und dem Satz von Cayley 1.20 vermuten wir aber bereits, dass kein Polynom g mit $\deg(g) \geq 5$ auflösbar ist.

Definition 19.1 *(Operation einer Gruppe auf einer Menge)*
Sei G eine Gruppe und X eine Menge. Eine (Links-)Operation von G auf X ist eine Abbildung:

$$\begin{aligned} \omega : G \times X &\to X \\ (g, x) &\mapsto g.x \end{aligned}$$

mit den Eigenschaften:
(i) $e.x = x \qquad \forall\, x \in X$
(ii) $g.(h.x) = (g \circ h).x \quad \forall\, x \in X\ \forall\, g, h \in G$
Die Menge der Operationen von G auf X bezeichnen wir mit $\mathrm{Op}(G, X)$.

Beispiel 42 *für Operationen:*
$G \times G \to G,\ (g, h) \mapsto gh$ *ist eine Operation von G auf G.*
Sei L/K Galois-Erweiterung mit der Galois-Gruppe $G = \mathrm{Gal}(L/K)$. Die Abbildungen:

$$\begin{aligned} G \times L &\to L \text{ und} \\ G \times L^\times &\to L^\times \\ \text{je mit: } (\sigma, x) &\mapsto \sigma(x) \end{aligned}$$

sind Operationen.
Sei G eine Gruppe. Die Konjugationsabbildung:
$G \times G \to G,\ (g, a) \mapsto gag^{-1}$ *ist eine Operation.*

Bemerkung 19.2 *Es seien G eine Gruppe, X eine Menge und S_X die symmetrische Gruppe auf X (Also $S_X := \{\, \tau \,|\, \tau : X \to X$ bijektiv $\}$). Dann sind die folgenden Zuordnungen bijektiv und zueinander invers:*

$$\{\, \tau \in \mathrm{Hom}(G, S_X) \,\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\omega \in \mathrm{Op}(G, X) \,\}$$

wobei Φ einen Homomorphismus $\tau \in \mathrm{Hom}(G, S_X)$ auf die Operation

$$G \times X \to X \quad \text{mit} \quad g.x \mapsto (\tau(g))(x)$$

abbildet und Ψ eine Operation $G \times X \to X,\ (g, x) \mapsto g.x$ auf den Gruppen-Homomorphismus

$$G \to S_X,\ \ g \mapsto \sigma_g \quad \text{mit} \quad \sigma_g : X \to X,\ x \mapsto g.x$$

abbildet.

Beweis. Zunächst zeigen wir die Wohldefiniertheit von Ψ, Φ:
Sei ein Gruppen-Homomorphismus $\varphi : G \to S_X$ gegeben. Dann ist $g.x := (\varphi(g))(x)$ eine Operation, denn die Eigenschaft (i) aus Definition 19.1 ist erfüllt, da $e.x = \varphi(e)(x) = x$ und da für alle $g, h \in G$ sowie für alle $x \in X$ gilt, dass $g.(h.x) = g.(\varphi(h))(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(gh)(x) = gh.x$ ist, ist auch Bedingung (ii) erfüllt.
Sei $G \times X \to X,\ (g, x) \mapsto g.x$ eine Gruppen-Operation. Dann ist $\varphi \in \mathrm{Hom}(G, S_X)$, mit $\varphi(g) = \sigma_g$, denn

$$\varphi(gh)(x) = \sigma_{gh}(x) = (gh)x = g.(h.x) = \sigma_g \circ \sigma_h(x) = (\varphi(g) \circ \varphi(g))(x)$$

Weiter ist $\sigma_g \in S_X$, denn σ_g ist injektiv, da $\sigma_g(x) = \sigma_g(y) \Leftrightarrow g^{-1}g(x) = g^{-1}g(y)$ und auch surjektiv, da für $y \in X$ gegeben nimm das Elemet $g^{-1}y$ als Urbild. Die Inversität von Φ und Ψ ist leich nachzurechnen. □

Definition 19.3 *(Bahn, Stabilisator, transitiv und treu)*
Sei G Gruppe, X Menge und $\omega \in \mathrm{Op}(G, X)$. Die Bahn von G unter $x \in X$ ist definiert als

$$G(x) := \{\, \omega(g, x) \,|\, g \in G \,\}$$

Sei $x \in X$, der Stabilisator von x unter G ist definiert als

$$G_x := \{\, g \in G \,|\, \omega(g, x) = x \,\}$$

Die Operation heißt transitiv, falls es ein $x \in X$ mit der Eigenschaft $G(x) = X$ gibt.
Die Operation heißt treu, falls der Homomorphismus $\varphi : G \to S_X$ mit $g \mapsto \omega(g, \cdot)$ aus Bemerkung 19.2 injektiv ist.

Bemerkung 19.4 *In der Situation aus Definition 19.3 gilt:*
(a) Sei $x \in X$ ein Element. Der Stabilisator G_x ist eine Untergruppe von G.
(b) Seien $x \in X$ und $g \in G$ Elemente, dann ist $G_{g.x} = g\, G_x\, g^{-1}$
(c) Durch $x \sim y :\Leftrightarrow G(x) = G(y)$ wird eine Äquivalenzrelation auf X definiert, die zugehörigen Äquivalenzklassen sind die Bahnen.
(d) X ist die disjunkte Vereinigung der Bahnen.
(e) Sei $x \in X$ ein Element. Die Abbildung: ${}^{G}\!/_{G_x} \to G(X),\ gG_x \mapsto g.x$ ist bijektiv. Daher gilt die folgende Identität: $\mathrm{Card}\left(G(X)\right) = (G : G_x)$

Beweis. Nachrechnen. □

Folgerung 19.5 *(Bahnengleichung)*
Sei G eine Gruppe und X endliche Menge sowie $\omega \in \mathrm{Op}(G, X)$, dann gilt:

$$\mathrm{Card}(X) = \sum_{i=1}^{n} \mathrm{Card}\left(G(x_i)\right) = \sum_{i=1}^{n} (G : G_{x_i})$$

wobei die $x_1, \ldots, x_n \in X$, mit $x_i \nsim x_j$ für $i \neq j$ und $X = \bigcup_{i=1}^{n} G(x_i)$. □

Satz 19.6 *Sei K ein Körper und $f \in K[X]$ ein separables Polynom. Seien weiter L der Zerfällungskörper von f über K und $N := \{\alpha_1, \ldots, \alpha_n\} \subseteq L$ die Nullstellen von f sowie $G := \mathrm{Gal}(L/K)$. Dann gelten::*
(a) Die Abbildung

$$\begin{array}{rcl} \omega : G \times N & \to & N \\ (g, x) & \mapsto & g(x) \end{array}$$

definiert eine Operation von G auf N.
(b) $\mathrm{Card}(G)$ *teilt* $n! = \mathrm{Card}(S_n)$
(c) die Operation ω ist genau dann transitiv, wenn f irreduzibel über $K[X]$ ist.

Beweis. Wir beweisen die Punkte der Reihe nach. Bei (a) ist klar, dass ω wohldefiniert und eine Operation ist. ω ist treu, denn betrachte die Abbildung $\varphi : G \ni g \mapsto \omega(g, \cdot) \in S_n$. Per Definition ist ω genau dann treu, wenn φ injektiv ist. Es gilt

$$\mathrm{Ker}(\varphi) \;=\; \left\{ g \in G \,\middle|\, \omega(g,\cdot) = id_N \right\} \;=\; \left\{ g \in G \,\middle|\, g = id_N \right\} \;=\; \left\{ e \right\}$$

Wir benutzen die Abbildung φ auch im Nachweis von (b), denn φ gibt eine Injektion von G in S_n. G kann also als Untergruppe von S_n aufgefasst werden, daher gilt, dass die Elementanzahl von G die Elementanzahl von S_n (das ist $n!$) teilt.
bei (c) ist eine Äquivalenz zu zeigen, wir betrachten zunächst „⇒“:
Sei ω transitiv und f reduzibel, also $f = g \cdot h$ mit zwei nicht konstanten Polynomen $g, h \in K[X]$, das heißt $\mathrm{Grad}(h) \geq 1 \leq \mathrm{Grad}(g)$. Da wir f als separabel vorausgesetzt haben, gilt: $\mathrm{ggT}(g, h) = 1$. Schreibe nun X als disjunkte Vereinigung $N = N_g \cup N_h$ wobei N_g, N_h die Nullstellenmengen von g bzw h sind. Die Mengen N_g und N_h werden unter G wieder auf N_g bzw. N_h abgebildet. Damit gibt es mindestens zwei Bahnen, also ist ω nicht transitiv. Dies ist ein direkter Wiederspruch, also muss f irreduzibel sein. Wir wollen nun „⇐“ betrachten:
Nach Vorraussetzung ist f irreduzibel. Seien uns $i, j \in \{1, \ldots, n\}$ gegeben. Da f irreduzibel ist, gibt es $\tilde{g} \in \mathrm{Hom}_K(K(\alpha_i), K(\alpha_j))$ derart, dass $\tilde{g}(\alpha_i) = \alpha_j$ ist. Betrachte $\hat{g}$ von $K(\alpha_i)$ nach L mit

$$\hat{g} : K(\alpha_i) \xrightarrow{\tilde{g}} K(\alpha_j) \hookrightarrow L$$

Setze nach Satz 12.9 $\hat{g}$ fort zu $g : L \to L$ mit $g(\alpha_i) = \alpha_j$. Es folgt sofort die Transitivität von ω. □

Um das allgemeine Polynom n-ten Grades zu definieren brauchen wir noch etwas mehr Wissen über Körper. Der nun folgende kurze Ausflug in die Körpertheorie, bestehend aus der nächsten Definition und dem nächsten Satz, soll uns dieses Wissen erschließen.
Wir haben bisher nur über algebraische Körpererweiterungen gesprochen. Nun wollen wir uns den nicht algebraischen, das heißt den transzendenten, Elementen widmen:

Definition 19.7 *(Transzendenzbasis)*
Sei L/K eine Körpererweiterung. Eine Menge $\mathfrak{B} \subseteq L$ heißt Transzendezbasis (TB) von L über K, falls die folgenden Bedingungen erfüllt sind:

(i) *$\mathfrak{B}$ ist transzendent über K*

(ii) *$L/K(\mathfrak{B})$ ist algebraisch.*

Konvention: Ist L/K algebraisch, so setze $\mathfrak{B} = \varnothing$.

Satz 19.8 *Sei L/K eine Körpererweiterung, dann gelten:*
(a) Es gibt eine Transzendenzbasis $\mathfrak{B}$ von L über K
(b) Existiere eine endliche Transzendenzbasis, dann haben je zwei Transzendenzbasenen die gleiche Elementanzahl.

Beweis. zu (a):
Im Sonderfall, dass L/K eine algebraische Körpererweiterung ist, existiert eine Transzendenzbasis mit $\mathfrak{B} = \varnothing$. Im Hauptfall bilde die Menge der transzendenten Teilmengen von L über K. Jede Teilmenge dieser Menge hat eine obere Schranke, wende also nun *Zorns Lemma* an[2].

[2](Vgl. Beweis zu Satz 5.5 oder Bosch: Algebra I - Seite 293, Satz 3)

Teil (b) beweisen wir induktiv über die Länge der kürzesten Transzendenzbasis.
Seien $\mathfrak{B} := \{x_1, \ldots, x_n\}$ und $\mathfrak{C} := \{y_1, \ldots, y_m\}$ mit $m \geq n$ zwei Transzendenzbasen. Wir benötigen nun zwei Induktionsanfänge:
(n = 0): Es gilt, dass $\mathfrak{B} = \varnothing$ und somit L/K algebraisch ist. Nach Konvention ist dann $\mathfrak{C} = \varnothing$
(n = 1): $\mathfrak{B} = \{x_1\}$ und $\mathfrak{C} = \{y_1, \ldots, y_m\}$. Jedes y_i ist algebraisch über $K(x_1)$, da $L/K(x_1)$ algebraisch ist nach Definition 19.7. Es gibt also Polynome $f_i \in K[T_1, T_2]$ mit $f_i(x_1, y_i) = 0$. Das heißt aber, dass x_1 für alle i algebraisch über $K[y_i]$ ist. Insbesondere also auch über $K[y_1]$.
Daher gilt: y_2 ist algebraisch über $K(x_1)$ und $K(x_1)/K(y_1)$ ist eine algebraische Körpererweiterung. Also ist y_2 algebraisch über $K(y_1)$, dann ist $\mathfrak{C}$ aber keine Transzendenzbasis.
Nun führen wir den Induktions-Schluss von $n-1$ nach n aus:
Nach der Induktionsvoraussetzung hat jede Transzendenzbasis von $L/K(x_1)$ genau $n-1$ Elemente. Wähle also aus $\mathfrak{C}$ $n-1$ Elemente aus, diese seien in $\tilde{\mathfrak{C}} \subseteq \mathfrak{C}$, so dass $\tilde{\mathfrak{C}}$ eine Transzendenzbasis von $L/K(x_1)$ ist. Schreibe $\mathfrak{C}$ als disjunkte Vereinigung

$$\mathfrak{C} = \tilde{\mathfrak{C}} \cup \mathfrak{R}$$

Dann ist $\mathfrak{R}$ algebraisch über $K(x_1, \tilde{\mathfrak{C}})$. Benutze nun den Induktionsanfang für $n = 1$, denn sowohl $\{x_1\}$ als auch $\mathfrak{R}$ sind Transzendenzbasen von $L/K(\tilde{\mathfrak{C}})$.
Also ist $\mathrm{Card}(\mathfrak{R}) = 1$ und somit $\mathrm{Card}(\mathfrak{C}) = n$ □

Beispiel 43 *für Transzendenzbasen*
Sei K ein Körper und $K[X]$ sein Polynomring. Weiter sei $K(X) := \mathrm{Quot}(K[X])$ der zugehörige Funktionenkörper. Es gelten: Die Menge $\{X\}$ ist Transzendenzbasis von $K(X)/K$ und entsprechend ist $\{X_1, \ldots, X_n\}$ eine Transzendenzbasis von $K(X_1, \ldots, X_n)/K$.

Definition 19.9 *(elementarsymmetrische Polynome)*
Es sei K ein Körper mit Funktionskörper $K(T_1, \ldots, T_n)$.
Wir definieren Polynome $s_j(T_1, \ldots, T_n) \in K[T_1, \ldots, T_n]$ für $j = 1, \ldots, n$ durch

$$\prod_{i=1}^{n}(X + T_i) \;=\; \sum_{j=0}^{n} s_j(T_1, \ldots, T_n) \cdot X^{n-j} \;\in K[T_1, \ldots, T_n, X]$$

Die s_j heißen die elementarsymmetrischen Polynome.

Beispiel 44 *(elementarsymmetrische Polynome)*
Für $n = 3$

$$\prod_{i=1}^{3}(X + T_i) = X^3 + X^2(T_1 + T_2 + T_3) + X(T_1T_2 + T_2T_3 + T_1T_3) + T_1T_2T_3$$

Die n elementarsymmetrischen Polynome sind:
$s_0(T_1, \ldots, T_n) = 1$
$s_1(T_1, \ldots, T_n) = \sum_{i=1}^{n} T_i$
$s_2(T_1, \ldots, T_n) = T_1T_2 + \ldots$ *„Summe über alle Zweierkombinationen“*
$s_3(T_1, \ldots, T_n) = T_1T_2T_3 + \ldots$ *„Summe über alle Dreierkombinationen“*
$\vdots$
$s_n(T_1, \ldots, T_n) = \prod_{i=0}^{n} T_i$

Definition 19.10 *(Das Allgemeine Polynom n-ten Grades)*
Sei K ein Körper und $K[S_1, \ldots, S_n]$ sein Polynomring in n Variablen. Das allgemeine Polynom n-ten Grades über K ist:

$$f(X) \;=\; X^n + \sum_{j=1}^{n} S_j X^{n-j} \;\in K[S_1, \ldots, S_n][X]$$

Definition 19.11 *(Galois-Gruppen von Polynomen)*
Seien L ein Körper und $f(X) \in L[X]$ ein separables Polynom. Weiter sei N ein Zerfällungskörper von f über L. Die Galois-Gruppe von f über L ist definiert als:

$$\mathrm{Gal}(f) := \mathrm{Gal}(N/L)$$

Der nun folgende Satz über die Galois-Gruppe des allgemeinen Polynoms ist das Kernstück zur Beantwortung der Frage: Wann ist die Gleichung $f(X) = 0$ durch radikale auflösbar:

Satz 19.12 *(Galoisgruppe des allgemeinen Polynoms)*
Es sei K ein Körper und $L := \mathrm{Quot}(K[S_1, \ldots, S_n])$ sein Funktionskörper in n Variablen. Weiter sei $f(X) \in L[X]$ das allgemeine Polynom n-ten Grades und N sein Zerfällungskörper über L. Es bezeichne $M := \mathrm{Quot}(K[T_1, \ldots, T_n])$ einen weitereren Funktionskörper über K. Die symmetrische Gruppe S_n operiert auf M mittels der Körperautomorphismen von M, die wie folgt gegeben sind: Für $\pi \in S_n$ und $\frac{g(T_1,\ldots,T_n)}{h(T_1,\ldots,T_n)} =: \tilde{g} \in M$ betrachte

$$\pi(\tilde{g}) = \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})}$$

Sei $\{t_1, \ldots, t_n\} \subseteq N$ die Nullstellenmenge von $f(X)$, dann induziert die Abbildung

$$\begin{aligned} \Psi : M &\;\to\; N \\ T_i &\;\mapsto\; -t_i \end{aligned}$$

wie folgt einen Körper-Isomorphismus auf den Fixkörpern:

$$\begin{aligned} \Psi|_{M^{S_n}} : \qquad M^{S_n} &\;\to\; N^{\mathrm{Gal}(N/L)} = L \\ s_j(T_1, \ldots, T_n) &\;\mapsto\; S_j \end{aligned}$$

Hierbei sind die s_j die elementarsymmetrischen Polynome nach Definition 19.9. Weiter ist die folgende Abbildung ein Gruppen-Isomorphismus.

$$\begin{aligned} \alpha : S_n &\;\to\; \mathrm{Gal}(N/L) = \mathrm{Gal}(f) \\ \pi &\;\mapsto\; \Psi \circ \pi \circ \Psi^{-1} \end{aligned}$$

Anmerkung Satz 19.12 in Worten:
Die Galois-Gruppe des allgemeinen Polynoms n-ten Grades ist die symmetrische Gruppe S_n.

Beweiskizze Da N ein Zerfällungskörper von f ist, wird N über L von den Nullstellen $t_1, \ldots, t_n$ von f erzeugt. Zeige zuerst, dass N auch über K von den t_i erzeugt wird. Insbesondere sind die Mengen $\mathfrak{B}_1 := \{S_1, \ldots, S_n\}$ und $\mathfrak{B}_2 := \{t_1, \ldots, t_n\}$ Transzendenzbasen von N über K. Damit können wir nun die Eigenschaften der gegebenen Abbildungen Ψ und α nachrechnen und erhalten die Behauptung.

Beweis. Es gilt:

$$N = L(T_1, \ldots, T_n) = K(S_1, \ldots, S_n, t_1, \ldots, t_n) = K(t_1, \ldots, t_n)$$

denn:

$$f(X) = X^n + \sum_{j=1}^{n} S_j X^{n-j} = \prod_{i=1}^{n} (X - t_i) = X^n + \sum_{j=1}^{n} s_j(-t_1, \ldots, -t_n) \cdot X^{n-j}$$

Und somit gilt für alle j, dass $S_j = s_j(-t_1, \ldots, -t_n)$ ist. Wir können N/K nun in eine algebraische, nämlich $N = K(t_1, \ldots, t_n)/L$, und eine transzendente, nämlich $L = K(S_1, \ldots, S_n)/K$, Körpererweiterung aufteilen. Der Transzendenzgrad von N/K ist also n, denn $\{t_1, \ldots, t_n\}$ ist eine Transzendenzbasis von N/K. Da die Elemente einer Transzendenzbasis transzendent sind, ist die folgende Abbildung per Definition injektiv.

$$\begin{array}{rcl} \psi : K[T_1, \ldots, T_n] & \to & N \\ T_i & \mapsto & -t_i \end{array}$$

Durch den Übergang zum Funktions- oder Quotientenkörper M erhalten wir Ψ. Dieser ist Körper-Isomorphismus, da er surjektiv ist, weil N von den t_i erzeugt wird.
Betrachte nun die Abbildung α. Es ist zu zeigen, dass $\Psi \circ \pi \circ \Psi^{-1}$ für alle $\pi \in S_n$ ein Element von $\mathrm{Gal}(f)$ ist.

$$\begin{array}{rcll} \Psi \circ \pi \circ \Psi^{-1}(S_j) & = & \Psi \circ \pi \circ \Psi^{-1}(s_j(-t_1, \ldots, -t_n)) & \\ & = & \Psi \circ \pi(s_j(T_1, \ldots, T_n)) & \\ & = & \Psi(s_j(T_{\pi(1)}, \ldots, T_{\pi(n)})) & \\ & = & \Psi(s_j(T_1, \ldots, T_n)) & \text{da die } s_j \text{ symmetrisch sind} \\ & = & s_j(-t_1, \ldots, -t_n) = S_j & \end{array}$$

Also ist $\Psi \circ \pi \circ \Psi^{-1}$ die Identitätsabbildung auf L. Es ist klar, dass α ein Gruppen-Homomorphismus ist, da α nichts weiter als die Hintereinanderausführung von Gruppen-Homomorphismen ist.
α ist injektiv, denn $\Psi \circ \pi \circ \Psi^{-1} = id_L$ und damit ist $\pi = \Psi \circ \Psi^{-1} = id_L$. Wir wollen nun zeigen, dass die Einschränkung von Ψ auf die Fixkörper M^{S_n} und $N^{\mathrm{Gal}(N/L)}$ ein Isomorphismus ist:

$$\begin{array}{rcll} m \in M^{S_n} & \Leftrightarrow & \pi(m) = m & \forall\, \pi \in S_n \\ & \Leftrightarrow & \Psi \circ \pi \circ \Psi^{-1} \circ \Psi(m) = \Psi(m) & \forall\, \pi \in S_n \\ & \Leftrightarrow & \alpha(\pi) \circ \Psi(m) = \Psi(m) & \forall\, \pi \in S_n \\ & \Leftrightarrow & \Psi(m) \in N^{\alpha(S_n)} & \\ & \Rightarrow & \Psi|_{M^{S_n}} M^{S_n} \to N^{\alpha(S_n)} & \text{ist bijektiv.} \end{array}$$

Wir wissen, dass $n! = [M : M^{S_n}] = [M : N^{\alpha(S_n)}] = \mathrm{Card}\,\big(\alpha(S_n)\big)$ und $\alpha(S_n) \leq \mathrm{Gal}(f)$ ist und mit Satz 19.6 (b) gilt, dass $n!$ von $\mathrm{Card}\,\big(\mathrm{Gal}(f)\big)$ geteilt wird. Damit folgt aber $\mathrm{Card}\,\big(\mathrm{Gal}(f)\big) = n!$ Wir haben damit gezeigt, dass α Gruppen-Isomorphismus ist. □

Folgerung 19.13 *(Auflösbarkeit des allgemeinen Polynoms)*
Sei K ein Körper mit $\mathrm{Char}(K) = 0$ und $n \geq 5$, dann ist das allgemeine Polynom n-ten Grades nicht (durch Radikale) auflösbar. Das heißt es gibt keine Formel in Termen von K und den Variablen $S_1, \ldots, S_n$, die nur Radikale und die Verknüpfungen $\cdot, \div, +, -$ benutzt um die Nullstellen des allgemeinen Polynoms auszudrücken.

Beweis. Im vorangegangenen Abschnitt haben wir gezeigt, dass die symmetrische Gruppe der Ordnung n für $n \geq 5$ nicht auflösbar ist. Mit Satz 19.12 ist S_n die Galois-Gruppe des allgemeinen Polynoms n-ten Grades, also folgt die Behauptung. □

Beispiel 45 *(Galois-Gruppen allgemeiner Polynome)*
Betrachte das allgemeine Polynom 2-ten Grades $f(X) = X^2 + pX + q \in \mathbb{Q}(p,q)[X]$
Wir haben soeben in Satz 19.12 gezeigt, dass $\mathrm{Gal}(f) \cong S_2 \cong \mathbb{Z}/2\mathbb{Z}$ ist.
Setzen wir $p = 0$ und $q = 2$ ein, so gilt:

$$f(X) = X^2 + 2 \in \mathbb{Q}[X] \text{ mit } \mathrm{Gal}(f) \cong \mathbb{Z}/2\mathbb{Z}$$

Setzen wir hingegen $p = 0$ und $q = -1$ ein, so gilt:

$$f(X) = X^2 - 1 \in \mathbb{Q}[X] \text{ mit } \mathrm{Gal}(f) = \{id\}$$

denn $\mathbb{Q}$ ist bereits der Zerfällungskörper von f. Nach dem Einsetzen von bestimmten Zahlen kann mit Satz 19.12 also keine Aussage mehr über die Galois-Gruppe von f getroffen werden.

Dieses Beispiel zeigt, dass wir das wissen über das allgemeine Polynom n-ten Grades nicht auf triviale Weise auf konkret gegebene Polynome vom Grad n übertragen können. Damit wir auch über die Galois-Gruppe von konkreten Polynomen mehr aussagen können benötigen wir nich den Begriff der Diskriminante:

Definition und Bemerkung 19.14 *(Diskriminante)*
Sei K ein Körper mit algebraischem Abschluss $\bar{K}$ und $f \in K[X]$ ein Polynom. Weiter seien $\alpha_1, \ldots, \alpha_n \in \bar{K}$ die Nullstellen von f in $\bar{K}$. Wir definieren die Diskriminante von f durch:

$$\Delta_f \ := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

Es gelten:
(a) Δ_f ist genau dann ungleich Null, wenn f separabel ist.
(b) $\Delta_f \in K$

Beweis. Teil (a) ist nach Definition klar, denn Separable Polynome haben keine vielfachen Nullstellen. Für den Beweis von (b) sei ohne Beschränkung der Allgemeinheit f separabel (Andernfalls wäre die Diskriminiante von f Null also in K). Sei L ein Zerfällungskörker von f über K und bezeichne $G := \mathrm{Gal}(L/K)$ die Galois-Gruppe von L/K, dann gilt für alle $\sigma \in G$

$$\sigma(\Delta_f) = \prod_{i<j} \sigma((\alpha_i - \alpha_j)^2) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta_f$$

Und mit dem Hauptsatz der Galois-Theorie 16.6 folgt die Behauptung, dass$\Delta_f \in K$ ist. □

Bemerkung 19.15 *Sei K Körper und $f \in K[X]$ ein separables Polynom. Hierzu sei L ein Zerfällungskörper von f über K und $N := \{\alpha_1, \dots \alpha_n\} \subseteq L$ die Nullstellenmenge von f. Weiter sei $\varphi : \mathrm{Gal}(L/K) \to S_n$, gegeben durch $\sigma(\alpha_i) := \alpha_{\varphi(\sigma)(i)}$[3], ein Gruppen-Homomorphismus. Dann sind äquivalent:*
(a) Δ_f hat eine Quadratwurzel in K.
(b) $\mathrm{Im}(\varphi) \leq A_n$.

Beweis. Setze

$$\delta_j \ := \ \prod_{i=1}^{n} (\alpha_i - \alpha_j)$$

Teil a der Bemerkung ist äquivalent damit, dass alle δ_j bereits in K liegen, denn Quadratwurzeln sind bis auf das Vorzeichen eindeutig bestimmt. Sei nun $\sigma \in \mathrm{Gal}(L/K)$, dann gilt

$$\begin{aligned} \sigma(\delta_j) &= \sigma\left(\prod_{i=1}^{n}(\alpha_i - \alpha_j)\right) = \prod_{i=1}^{n}\big(\sigma(\alpha_i) - \sigma(\alpha_j)\big) \\ &= \prod_{i=1}^{n}(\alpha_{\varphi(\sigma)(i)} - \alpha_{\varphi(\sigma)(j)}) = \mathrm{sgn}(\varphi(\sigma)) \cdot \delta_j \end{aligned}$$

Mit dieser Rechnung und dem Hauptsatz der Galois-Theorie 16.6 ist die Aussage $\delta_j \in K$ äquivalent damit, dass $\mathrm{sgn}(\varphi(\sigma)) = 1$ für alle $\sigma \in \mathrm{Gal}(L/K)$ ist, also dass jedes $\varphi(\sigma)$ eine gerade Permutation ist. Das heißt aber nichts anderes, als dass jedes $\varphi(\sigma)$ bereits in A_n liegt. □

Bemerkung 19.16 *Das Polynom $X^2 + pX + q$ hat die Diskriminante $p^2 - 4q$ und das Polynom $X^3 + aX + b$ hat die Diskriminante $-4a^3 - 27b^2$* □

Folgerung 19.17 *Sei K ein Körper mit $\mathrm{Char}(K) \notin \{2, 3\}$ und $f(X) = X^3 + aX + b \in K[X]$ ein irreduzibles Polynom. Dann gilt:*

$$Gal(f) \ \cong \ \begin{cases} A_3 & \text{falls } -4a^3 - 27b^2 \text{ ein Quadrat in } K \text{ ist} \\ S_3 & \text{sonst} \end{cases}$$

□

Beispiel 46 *(Dikriminanten und Galoisgruppen)*
Das Polynom $f(X) = X^3 - X - 1 \in \mathbb{Q}[X]$ hat die Diskriminante

$$\Delta_f = -4(-1)^3 - 27(19)^2 = -23$$

Da $\sqrt{-23}$ keine rationale Zahl ist, folgt $\mathrm{Gal}(f) \cong S_3$.
Das Polynom $g(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ hat die Diskriminante

$$\Delta_g = -4(-3)^3 - 27 = 3 \cdot 27 = 9^2$$

Da $\sqrt{9^2} = 9$ ein Element in $\mathbb{Q}$ ist, folgt $\mathrm{Gal}(g) \cong A_3$.

[3]Die Abbildung φ kennen wir schon aus Bemerkung 19.2 mit $\varphi : \mathrm{Gal}(L/K) \ni \sigma \mapsto \omega(\sigma, \cdot) \in S_n$ wobei ω eine Operation von $\mathrm{Gal}(L/K)$ auf N ist.

20 Kummer-Theorie

Wir haben in den vorangegangenen Abschnitten gezeigt, dass ein Polynom f genau dann durch Radikale auflösbar ist, wenn N/K, für einen Zerfällungskörper N von f, eine auflösbare Galois-Erweiterung ist. Wir wollen nun zeigen, dass eine Körpererweiterung N/K durch Radikale auflösbar ist, vergleiche Definition 17.1, wenn N/K eine auflösbare Galois-Erweiterung ist.

Definition 20.1 *(Spur und Norm)*
Sei L/K eine endliche Körpererweiterung mit Separabilitätsgrad $[L:K]_S = n$ und $a \in L$. Fixiere einen algebraischen Abschluss $\bar{K}$ zu K. Wir wissen:

$$[L:K] \;=\; [L:K]_S \cdot q \quad \text{und} \quad \mathrm{Hom}_K(L, \bar{K}) \;=\; \{\sigma_1, \ldots, \sigma_n\}$$

Die Spur von a ist definiert als

$$\mathrm{SP}_{L/K}(a) := q \cdot \sum_{i=1}^{n} \sigma_i(a)$$

Die Norm von a ist definiert als

$$\mathrm{N}_{L/K}(a) := \left(\prod_{i=1}^{n} \sigma_i(a) \right)^q$$

Anmerkung Ist L/K galoisch, so ist $q = 1$.
Sei $a \in L$ ein Element und B eine Basis von L als K-Vektorraum. Gibt es eine K-lineare Abbildung

$$\begin{array}{rccc} \varphi_a : L & \to & L \\ x & \mapsto & ax \end{array}$$

so kann φ_a als Matrix M bezüglich B beschrieben werden. Es gelten:

$$\mathrm{SP}_{L/K}(a) \;=\; \mathrm{Spur}(M) \quad \text{und} \quad \mathrm{N}_{L/K}(a) \;=\; \det(M)$$

Definition 20.2 *(Charakter von G)*
Seien G eine Gruppe und K ein Körper, dann heißt ein Gruppen-Homomorphismus

$$\chi : G \to (K^\times, \cdot)$$

Charakter von G mit Werten in K.

Satz 20.3 *Es seien G eine Gruppe, K ein Körper und $n \in \mathbb{N}$ eine natürliche Zahl. Seien weiter $\chi_1, \ldots \chi_n$ paarweise verschiedene Charaktere von G mit Werten in K.*
Wir können $\mathrm{Abb}(G, K)$ mit punktweiser Addition und skalarer multiplikation als K-Vektorraum auffassen, daher sind die Elemente $\chi_1, \ldots, \chi_n$ K-linear unabhängig in $\mathrm{Abb}(G, K)$.

Beweis. Annahme $\chi_1, \ldots, \chi_n$ sind K-linear abhängig.
Sei n das kleineste $n \in \mathbb{N}$, so dass es n K-linear-abhängige Charaktere gibt, also das es $a_i \in K$ gibt, so dass die Summe $\sum_{i=1}^{n} a_i \chi_i$ Null ist, wobei nicht alle $a_i = 0$ sind.

Es gilt $n \geq 2$, denn der triviale Charakter $G \ni g \mapsto 1 \in K$ ist nicht 0. Weiter gibt es ein $g \in G$ derart, dass $\chi_1(g)$ nicht gleich $\chi_2(g)$ ist und damit

$$\forall\, h \in G: \qquad 0 \;=\; \sum_{i=1}^{n} a_i \chi_i(gh) = \sum_{i=1}^{n} (a_i \chi_i(g)) \chi_i(h)$$

Insbesondere sind die $(a_i(\chi_i(g)) \cdot \chi_i$ keine triviale Linearkombination der Null. Es folgt:

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \left[(a_i(\chi_i(g)) \cdot \chi_i\right] - 0 \\ &= \sum_{i=1}^{n} (a_i \chi_i(g)) \cdot \chi_i - \left(\sum_{i=1}^{n} a_i \chi_i \right) \chi_1(g) \\ &= \sum_{i=1}^{n} (a_i \chi_i(g) - a_i \chi_1(g)) \chi_i \\ &= \sum_{i=1}^{n} a_i (\chi_i(g) - \chi_1(g)) \chi_i \end{aligned}$$

Aus der letzten Gleichung folgt, dass $a_2 \neq 0 \neq \chi_2(g) - \chi_1(g)$ sind und damit ist auch $a_2(\chi_2(g) - \chi_1(g))$ nicht Null. Dies ist aber ein Widerspruch zu unserer Annahme, wir haben also höchstens $n-1$ linear abhängige Charaktere. □

Folgerung 20.4 *Sei L/K eine algebraische Körpererweiterung mit paarweise verschiedenen Automorphismen $\sigma_1, \ldots \sigma_n \in \mathrm{Aut}_K(L)$. Dann sind die $\sigma_1, \ldots \sigma_n \in \mathrm{Abb}(L, L)$ L-linear unabhängig.* □

Satz 20.5 *(Hilbertsatz 90)*
Sei L/K eine zyklische Galois-Erweiterung vom Grad n, und sei $b \in L$ ein Element, dann gilt: Genau dann ist $\mathrm{N}_{L/K}(b) = 1$, wenn es ein $a \in L$ mit der Eigenschaft $b = \frac{a}{\sigma(a)}$ gibt, wobei die Galois-Gruppe $\mathrm{Gal}(L/K)$ von σ erzeugt wird.

Beweis. Wir müssen wieder eine Äquivalenz nachweisen und beginnen mit der leichten Richtung. Setze also voraus, dass es ein $a \in L$ mit der beschriebenen Eigenschaft gibt, dann gilt

$$\mathrm{N}_{L/K}(b) = \frac{\mathrm{N}_{L/K}(a)}{\mathrm{N}_{L/K}(\sigma(a))} = \frac{\mathrm{N}_{L/K}(a)}{\mathrm{N}_{L/K}(a)} = 1$$

Nun zur Gegenrichtung. Nach Voraussetzung ist $\mathrm{N}_{L/K}(b) = 1$. Wir bezeichnen die Elemente von $\mathrm{Gal}(L/K)$ mit σ^0 bis σ^{n-1} diese sind nach Folgerung 20.4 linear unabhängig. Hieraus folgt:

$$0 \neq \sigma^0 + b \cdot \sigma + b \cdot \sigma(b) \cdot \sigma^2 + \cdots + b \cdot \sigma(b) \ldots \sigma^{n-2}(b) \cdot \sigma^{n-1}$$

Also gibt es $c \in L$ mit:

$$0 \neq c + b \cdot \sigma(c) + b \cdot \sigma(b) \cdot \sigma^2(c) + \cdots + b \cdot \sigma(b) \ldots \sigma^{n-2}(b) \cdot \sigma^{n-1}(c) =: a$$

Betrachte:

$$\frac{a}{\sigma(a)} = \frac{c + b \cdot \sigma(c) + b \cdot \sigma(b) \cdot \sigma^2(c) + \cdots + b \cdot \sigma(b) \ldots \sigma^{n-2}(b) \cdot \sigma^{n-1}(c)}{\sigma(c) + \sigma(b) \cdot \sigma^2(c) + \cdots + \sigma(b) \cdot \sigma(b) \ldots \sigma^{n-1}(b) \cdot c} = b$$

denn: $\sigma(b) \cdot \sigma(b) \ldots \sigma^{n-1}(b) = \frac{\mathrm{N}_{L/K}(b)}{b} = \frac{1}{b}$. □

Satz 20.6 *(Hauptsatz der Kummer Theorie)*
Sei L/K eine zyklische Galois-Erweiterung vom Grad n und setze eine Körpercharakteristik voraus, die nicht n teilt, oder gleich Null ist. Weiter gebe es eine primitive n-te Einheitswurzel $\zeta \in K$.
Dann gibt es $a \in L$ mit Minimalpolynom $f_a = X^n - c \in K[X]$, insbesondere ist

$$L = K(a) = K(\sqrt[n]{c})$$

Beweis. Mit Hilbertsatz 90 gilt $\mathrm{N}_{L/K}(\zeta) = \zeta^n = 1$ daher gibt es wiederrum nach Satz 20.5 ein $a \in L$ derart, dass $\zeta = \frac{a}{\sigma(a)}$ ist. Weiter wird dann die Galois-Gruppe $\mathrm{Gal}(L/K)$ von σ erzeugt. Also ist $\sigma(a) = \zeta^{-i} \cdot a$ und somit gilt für alle $i = 1, \ldots, n-1$, dass $\sigma^i(a) = \zeta^{-1} \cdot a$ ist. Also muss $\mathrm{Card}\left(\mathrm{Hom}_K(K(a), L)\right)$ größer als n sein, denn die Bilder von a unter den σ^i sind paarweise verschieden. Damit ist dann auch sofort $[K(a) : K]_S \geq n$. Zusammengefasst gilt also $n \leq [K(a) : K]_S \leq [L : K] = n$ Mit dem Quetschlemma ist dann $[K(a) : K] = n$ also $K(a) = L$. Es gilt:

$$\sigma(a^n) \;=\; \sigma(a)^n \;=\; (\zeta^{-1})^n a^n \;=\; a^n \;=\; c \in K$$

□

Satz 20.7 *Sei K ein Körper der Charakteristik 0 und sei L/K eine endliche Körpererweiterung, dann sind äquivalent:*
(i) Es gibt eine endliche Körpererweiterung M/K, die L enthält und durch Radikale auflösbar ist.
(ii) Es gibt eine endliche Galois-Erweiterung N/K, die L enthält und deren Galois-Gruppe $\mathrm{Gal}(N/K)$ auflösbar ist.

Beweis. Die Implikation von (i) auf (ii) ist die Hauptaussage von Abschnitt 18, ab Seite 77, daher beweisen wir nun die Gegenrichtung „(ii) ⇒ (i)“:
Nach Voraussetzung ist $G := \mathrm{Gal}(N/K)$ auflösbar, also gibt es nach Folgerung 18.11 eine Normalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = \{e\}$ mit zyklischen Faktoren G_i/G_{i+1} für alle $i = 1, \ldots, r$
Der Hauptsatz der Galoistheorie 16.6 gibt uns mit $N_i = N^{G_i}$ eine Kette von Zwischenkörpern

$$N = N_r \supseteq \ldots \supseteq N_1 \supseteq N_0 = K \;\text{ mit zyklischen Galois-Erweiterungen } N_i/N_{i-1} \;\text{ für alle } i$$

Sei $n = [N : K]$, dann betrachte mit $\zeta_n \in \bar{K}$ primitive n-te Einheitswurzel die Kette:

$$N(\zeta_n) = N_r(\zeta_n) \supseteq \ldots \supseteq N_0(\zeta_n) \supseteq K$$

mit zyklisch Galois-Erweiterungen $N_{i+1}(\zeta_n)/N_i(\zeta_N)$ denn nach Satz 16.12 ist

$$\mathrm{Gal}(N_{i+1}(\zeta_n)/N_i(\zeta_N)) \leq \mathrm{Gal}(N_{i+1}/N_i)$$

Nach dem HauptSatz der Kummer Theorie 20.6 ist $N_{i+1}(\zeta_n)$ eine Erweiterung von $N_i(\zeta_n)$ von der Form: $N_i(\zeta_n)(\sqrt[n_i]{c})$ mit $n_i = [N_{i+1}(\zeta_n) : N_i(\zeta_n)] \,|\, n$. □

21 Die Sylow-Sätze

In diesem Abschnitt bezeichne p immer eine Primzahl.

Definition 21.1 *(p-Gruppen und p-Sylow-Gruppen)*

- *Eine endliche Gruppe G heißt p-Gruppe, falls es eine natürliche Zahl $n \in \mathbb{N}$ gibt, so dass $\mathrm{Card}(G) = p^n$ ist.*
- *Sei G eine endliche Gruppe der Ordnung $\mathrm{Card}(G) = p^n \cdot m$ mit natürliche Zahlen $n, m \in \mathbb{N}$ und $\mathrm{ggT}(p, m) = 1$.*
  Eine p-Sylow-(Unter-)Gruppe $S \leq G$ ist eine Untergruppe der Ordnung $\mathrm{Card}(S) = p^n$.

Beispiel 47 *Wir betrachten die alternierende Gruppe A_4:*
$\mathrm{Card}(A_4) = 12 = 2^2 \cdot 3$
2-Sylow-Gruppe(n): $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ *mit* $\mathrm{Card}(V_4) = 2^2$
3-Sylow-Gruppe(n): $< (123) >, < (124) >, < (134) >, < (234) >$

Beispiel 48 *Sei G endliche Gruppe und $p \neq \mathrm{Card}(G)$, dann ist $\{e\}$ eine p-Sylow-Gruppe.*

Bemerkung 21.2 *Sei G eine endliche, abelsche Gruppe mit $p \mid \mathrm{Card}(G)$, dann gibt es ein $x \in G$ mit $\mathrm{Ord}(x) = p$.*

Beweis. Die Behauptung folgt sofort aus dem Hauptsatz über endlich erzeugte abelsche Gruppen[4]. □

Wir wissen, dass die Konjugation

$$\begin{aligned} \kappa : G \times G &\to G \\ (g, x) &\mapsto gxg^{-1} \end{aligned}$$

eine Operation von G auf G ist. Wir spezialisieren nun den Begriff des Stabilisators, denn wir schon in Definition 19.3 für allgemeine Operationen eingeführt haben:

Definition 21.3 *(Normalisator und Zentralisator)*
Sei G eine Gruppe und $h \in G$. Der Stabilisator

$$\mathrm{Stab}_G(h) := \mathrm{Z}_h := \{\, g \in G \mid ghg^{-1} = h \,\}$$

heißt der Zentralisator von h. Sei $H \subseteq G$, wir definieren

$$\mathrm{Z}_H := \{\, g \in G \mid ghg^{-1} = h \ \forall\, h \in H \,\} = \bigcap_{h \in H} \mathrm{Z}_h$$

als den „Zentralisator von H“.
Sei nun $H \leq G$. Der Normalisator von H in G ist:

$$\mathrm{N}_H := \{\, g \in G \mid gHg^{-1} = H \,\}$$

Anmerkung Der Zentralisator von G, also Z_G, ist das Zentrum von G.

[4] Satz 3.12

Bemerkung 21.4 *In der Situation aus Definition 21.3 gelten:*
(a) $\mathrm{Z}_H \leq G \wedge \mathrm{Z}_h \leq G$
(b) $H \leq G \Rightarrow \mathrm{Z}_H \leq N_H$
(c) $H \trianglelefteq \mathrm{N}_H$*, und* N_H *ist die größte Untergruppe von* G *mit Normalteiler* H*.*

Beweis. Nachrechnen. □

Satz 21.5 *Sei* G *eine endliche Gruppe, dann gelten:*
(a) Sei $g \in G$*, dann liegt* g *genau dann im Zentrum* Z_G *von* G*, wenn* $\mathrm{Z}_g = G$ *gilt*
(b) Es gilt die Formel

$$\mathrm{Card}(G) \;=\; \mathrm{Card}(Z_G) + \sum_{i=1}^{n} (G : \mathrm{Z}_{x_i}) \qquad \text{mit } Z_{x_i} \neq G \;\; \forall\, i = 1, \ldots, n$$

denn

$$G = \mathrm{Z}_G \bigcup_{i=1}^{n} \{\, g x_i g^{-1} \,|\, g \in G \,\}$$

Beweis. (b) ist ein Spezialfall der Bahnengleichung 19.5.
Zu (a) betrachte

$$g \in \mathrm{Z}_G \;\Leftrightarrow\; ghg^{-1} = h \;\; \forall\, h \in G \;\Leftrightarrow\; \mathrm{Z}_g = \{\, h \in G \,|\, hgh^{-1} = g \,\} = G$$

□

Satz 21.6 *(Sylow-Sätze)*
Sei G *eine endliche Gruppe, dann gelten*

(a) *G besitzt eine p-Sylow-(Unter-)Gruppe.*

(b) *Sei $H \leq G$ mit $\mathrm{Ord}(H) = p$, dann exisitert eine p-Sylow-Gruppe S mit $H \leq S$.*

(c) *Sei S eine p-Sylow-Gruppe von G, dann ist gSg^{-1} eine p-Sylow-Gruppe von G für alle $g \in G$.*

(d) *Je zwei Sylow-Gruppen sind konjugiert, das heißt S und S' sind genau dann p-Sylow-Gruppen, wenn es ein $g \in G$ mit der Eigenschaft $gSg^{-1} = S'$ gibt.*

(e) *Sei s_p die Anzahl der p -Sylow-Gruppen, dann gelten $s_p | \,\mathrm{Card}(G)$ und $s_p \equiv 1(p)$*

Beweis. Satz (a) beweisen wir induktiv über die Ordnung q von G. Hierbei ist der Anfang für $q = 1$ klar. Nimm nun an, dass $q > 1$ ist, also dass $\mathrm{Ord}(G) = q = p^n \cdot m$ mit $n > 0$ und $\mathrm{ggT}(p, m) = 1$ gilt. Wir müssen zwei Fälle unterscheiden:
Fall I (p teilt nicht die Elementanzahl von Z_G):
In diesem Fall existiert ein $i \in \{1, \ldots, n\}$ mit $p \nmid (G : Z_{x_i})$ für Z_{x_i} aus Satz 21.5.
Es gilt: $(G : Z_{x_i}) = \frac{q}{\mathrm{Card}(\mathrm{Z}_{x_i})} \;\Rightarrow\; p^n \mid \mathrm{Card}(\mathrm{Z}_{x_i})$, da $\mathrm{Card}(\mathrm{Z}_{x_i}) \leq \mathrm{Card}(G)$ ist, folgt nach Induktionsvoraussetzung, dass Z_{x_i} eine Untergruppe S mit $\mathrm{Ord}(S) = p^n$ besitzt.
S ist p-Sylow-Gruppe von G.
Fall II (p teilt die Elementanzahl von Z_G):
Da Z_G abelsch ist existiert nach Bemerkung 21.2 $x \in \mathrm{Z}_G$ mit $\mathrm{Ord}(x) = p$.
Definiere $N :=< x > \trianglelefteq G$ dann ist $\mathrm{Card}(N) = p$. Betrachte die natürliche Projektion:

$$\pi : G \to {}^{G}\!/_{N}$$

Nach Induktionsvoraussetzung gibt es p-Sylow-Gruppe
$\bar{S}$ ist eine Untergruppe von G/N und weiter gilt, dass $\mathrm{Card}\left(G/N\right) = p^{n-1} \cdot m$ ist, also folgt $\mathrm{Card}(\bar{S}) = p^{n-1}$. Definiere nun $S := \pi^{-1}(\bar{S}) \leq G$. Beschränken wir nun die natürliche Projektion auf S so gilt: $\pi_{|S} : S \to \bar{S}$ hat den Kern N.
$\Rightarrow S/N \cong \bar{S} \;\Rightarrow\; \mathrm{Card}(S) = \mathrm{Card}(N) \cdot \mathrm{Card}(\bar{S}) = p^n$
$\Rightarrow S$ ist die gesuchte p-Sylow-Gruppe von G.
Zu (b): Definiere $\mathfrak{M}_p$ die Menge aller p-Sylow-Gruppen von G. Wir haben in (a) gesehen, dass diese nicht leer ist.
(1) Seien $g \in G$ und $S \in \mathfrak{M}_p$, dann ist $gSg^{-1} \in \mathfrak{M}_p$.
Sei $S \in \mathfrak{M}_p$. Der Stabilisator von S ist $\mathrm{N}_S = \{\, g \in G \,|\, gSg^{-1} = S \,\}$ der Normalisator. Nach Bemerkung 19.4 (e) gilt nun, dass$(G : N_S) = \mathrm{Card}(\{\, hSh^{-1} \,|\, h \in G \,\})$ die „Länge der Bahn von S unter G“ ist. Weil S eine Untergruppe von N ist gilt: $p \nmid (G : N_S)$.
(2) Sei $H \leq G$ die vorgegebene p-Gruppe.
Wir wissen, die Konjugation $\kappa : H \times \mathfrak{M}_p \to \mathfrak{M}_p$ ist eine Operation, insbesondere operiert H auf $\{\, gSg^{-1} \,|\, g \in G \,\} \subseteq \mathfrak{M}_p$. Die Bahnengleichung 19.5 liefert:

$$\{\, gSg^{-1} \,|\, g \in G \,\} = \bigcup_{i=1}^{r} \{\, hg_iSg_i^{-1}h^{-1} \,|\, h \in H \,\}$$

Nach (1) wird $\mathrm{Card}\left(\{gSg^{-1} \,|\, g \in G\,\}\right)$ nicht von p geteilt und es gilt auch

$$\mathrm{Card}\left(\{hg_iSg_i^{-1}h^{-1} \,|\, h \in H\}\right) = p^e \quad \forall\, i = 1, \ldots, r$$

Das heißt es gibt ein j mit $\mathrm{Card}\left(\{\, hg_jSg_j^{-1}h^{-1} \,|\, h \in H \,\}\right) = 1$.
(3) Setze $T := g_jSg_j^{-1}$ für j aus (2).
Wir haben bereits gezeigt, dass alle $h \in H$ die Eigenschaft $hTh^{-1} = T$ haben und daraus folgern wir nun, dass $H \leq \mathrm{N}_T$ und $T \leq \mathrm{N}_T$ gelten. Weiter ist dann $HT \leq \mathrm{N}_T$ und daher gilt nach dem Isomorphiesatz: $HT/T \cong H/T \cap H$ somit hat $H/T \cap H$ genau p^r elemente, denn $\mathrm{Card}(H) = p^t$
Damit haben wir gezeigt, dass HT in T enthalten ist und da T eine p-Sylow-Gruppe ist folgt: $H \subseteq T$.
zu (c),(d): „$\Rightarrow$“ folgt sofort aus (b).
S, S' seien p-Sylow-Gruppen. Finde Hierzu mit (b) ein g derart, dass $gSg^{-1} = S'$. Da S' p-Sylow-Gruppe ist gilt: $S' = gSg^{-1}$.
Der Beweis von (e) wurde aus Zeitmangel nicht erbracht. □

Folgerung 21.7 *Sei G eine endliche Gruppe. Es gelten:*
(a) Falls p die Elementanzahl von G teilt gibt es ein $x \in G$ mit der Ordnung p.
(b) Falls G eine p-Gruppe ist, dann gibt es für alle $x \in G$ eine Zahl $n \in \mathbb{N}$ derart, dass $\mathrm{Ord}(x) = p^n$
□

Folgerung 21.8 *Sei G eine endliche Gruppe. Wenn G nur eine einzige p-Sylow-Gruppe S hat, dann ist S normal in G.*

Beweis. Satz 21.6 Teil (c) □

Beispiel 49 *(Anwendungen der Sylow-Sätze)*
Jede Gruppe G der Ordnung $30 = 2 \cdot 3 \cdot 5$ hat einen nicht trivialen Normalteiler. (Insbesondere ist G also nicht einfach.)

Erinnerung *Nach Teil (e) ist $s_p := \mathrm{Card}\left(\{\, S \mid S \text{ } p\text{-Sylow Gruppe in } G \,\}\right)$ wobei s_p die Anzahl der Elemente in G teilt und $s_p \equiv 1\,(p)$ gilt.*

Wir erhalten als mögliche Werte $s_2 \in \{1, 3, 5, 15\}$ sowie $s_3 \in \{1, 10\}$ und $s_5 \in \{1, 6\}$ Wir wollen nun zeigen, dass immer entweder s_3 oder s_5 gleich 1 sein muss.
Wir nehmen an, dass dies nicht gilt. Seien also $s_3 \neq 1 \wedge s_5 \neq 1$ Dann müssen $s_3 = 10$ und $s_5 = 6$ gelten.
Betrachte die 3-Sylow-Gruppen: Es ist klar, dass jede 3-Sylow-Gruppe von G genau 3 Elemente hat. Seien also P, Q 3-Sylow-Gruppen, dann gilt:

$$P \cap Q = P \quad \vee \quad P \cap Q = \{e\}$$

Es gibt nach Annahme 10 3-Sylow-Gruppen, also gibt es $10 \cdot 2 = 20$ Elemente der Ordnung 3
Betrachte nun analog die 5-Sylow-Gruppen: Analog zu den 3-Sylow-Gruppen folgt, dass es $6 \cdot 4 = 24$ Elemente der Ordnung 5 gibt.
Insgesamt hat G dann 44 Elemente - Dies ist ein Widerspruch, da $\mathrm{Card}(G) = 30$.

Folgerung 21.9 *Seien $p < q$ zwei Primzahlen mit $p \nmid (q-1)$. Es gilt:*
Jede Gruppe der Ordnung $p \cdot q$ ist zyklisch.

Beweis. Es gilt: $s_p, s_q \mid pq \;\wedge\; s_p \equiv 1\,(p),\; s_q \equiv 1\,(q) \;\Rightarrow s_p \in \{1, q\} \wedge s_q \in \{1, p\}$
Annahme 1: $s_p = q \equiv 1\,(p) \;\Rightarrow\; p \mid (q-1)$ - Widerspruch!
Annahme 2: $s_q = p \equiv 1\,(q) \;\Rightarrow\; q \mid (p-1) \;\Rightarrow\; (q < p)$ - Widerspruch!
$\Longrightarrow s_p = s_q = 1$
$\Rightarrow P$ ist die einizige p-Sylow-Gruppe und Q ist die einizige q-Sylow-Gruppe. Insbesondere sind beide normal in G.
Mit dem Chinesischen Restsatz 7.16 folgt nun, dass $G = PQ$ ist, es genügt also zu zeigen, dass G abelsch ist. Sei $x \in P \wedge y \in Q$, dann betrachte: $[xy] = xyx^{-1}y^{-1} \in P \cap Q = \{e\}$
$\Rightarrow G$ ist abelsch $\;\Rightarrow\;$ $G = P \times Q \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{q\mathbb{Z}}$ □

Beispiel 50 *Jede Gruppe mit 35 Elementen ist zyklisch, denn $35 = 5 \cdot 7$.*

22 Konstruktion mit Zirkel und Lineal

Als Abschluss wollen wir einige interessante geometrische Begebenheiten mit der in dieser Vorlesung aufgebauten Theorie beweisen. Wir werden allein aus den gezeigten Eigenschaften von Körpererweiterungen und Gruppen die Konstruierbarkeit von regelmäßigen n-Ecken ableiten und die unmöglichkeit der Quadratur des Kreises zeigen.
Der Einfachheit halber wird bei der Konstruierbarkeit die genauere Beschreibung „mit Zirkel und Lineal“ weggelassen, da wir uns hier
nicht mit anderen Konstruktionsarten befasst haben.

Definition 22.1 *(Konstruierbarkeit)*
Eine Teilmenge $M \subseteq \mathbb{C}$ sei gegeben.
Ein Punkt $z \in M$ heißt aus der Menge M konstruierbar, falls die Menge M zu einer Menge M' mit $z \in M'$ durch folgende elementare Konstruktionsschritte vergrößert werden kann:

I *Seien $z_1, \ldots, z_4 \in M$, so dass die Geraden $\overline{z_1\, z_2}$, $\overline{z_3\, z_4}$ nicht parallel verlaufen. Füge den Schnittpunkt $\overline{z_1\, z_2} \cap \overline{z_3\, z_4}$ zu M hinzu.*

II *Seien $z_1, \ldots, z_5 \in M$. Bezeichne K_1 einen Kreis um z_1 mit Radius $|z_2 - z_3|$, dann füge zu M die Schnittpunkte $K_1 \cap \overline{z_4\, z_5}$ hinzu.*

III *Seien $z_1, \ldots, z_6 \in M$. Bezeichne K_1 einen Kreis um z_1 mit Radius $|z_2 - z_3|$ und K_2 einen Kreis um z_4 mit Radius $|z_5 - z_6|$. Füge zu M die Schnittpunkte von $K_1 \cap K_2$ hinzu.*

Wir definieren weiterhin die folgenden Notationen:
$\mathfrak{X}(M) := \{\, z \in \mathbb{C} \mid z \text{ ist aus } M \text{ konstruierbar} \,\}$ *und*
$M^C := \{\, \bar{z} \mid z \in M \,\}$ *hierbei ist $\bar{z}$ das komplexe Konjugat von z.*

Bemerkung 22.2 *Sei $M \subseteq \mathbb{C}$ ein Teilkörper mit $M = M^C$ der i mit $i^2 = -1$ enthält.*
Falls $z \in \mathfrak{X}(M)$, dann ist der Grad von $[M(z) : M]$ höchstens zwei.

Beweis. Nachrechnen mit analytischer Geometrie. Merke: Kreise sind durch quadratische, Geraden durch lineare Gleichungen gegeben. □

Bemerkung 22.3 *Folgende Konstruktionen sind mit Zirkel und Lineal durchführbar:*
(a) Konstruktion einer Senkrechten durch gegebenen Punkt und Grade.
(b) Konstruktion einer Parallelen durch gegebenen Punkt und Grade.
(c) Halbierung einer Strecke.
(d) Spiegelung eines Punktes an einer gegebenen Graden.
(e) Errichtung eines gleichseitigen Dreiecks auf einer gegebenen Strecke.
(f) Winkeladdition.
(g) Winkelhalbierung.
(h) Winkelnegation.

Beweis. Dieses wissen ist Elementar, und kann mit wenigen Handgriffen überprüft werden. □

Bemerkung 22.4 *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die $\{0,1\}$ enthält. Seien weiter $z,\ z_1,\ z_2 \in \mathfrak{X}(M)$ aus M konstruierbar, dann gelten:*
(a) $z_1 + z_2 \in \mathfrak{X}(M)$
(b) $-z \in \mathfrak{X}(M)$
(c) $|z| \in \mathfrak{X}(M)$
(d) $e^{\frac{i\pi}{3}} \cong 60^o \in \mathfrak{X}(M)$
(e) $|z_1| \cdot |z_2| \in \mathfrak{X}(M)$
(f) $|z|^{-1} \in \mathfrak{X}(M)$
(g) $z_1 \cdot z_2 \in \mathfrak{X}(M)$
(h) $z^{-1} \in \mathfrak{X}(M)$
(i) $\pm\sqrt{|z|} \in \mathfrak{X}(M)$
(j) $\pm\sqrt{z} \in \mathfrak{X}(M)$
Insbesondere ist $\mathfrak{X}(M)$ ein Körper, welcher abgeschlossen ist unter Bildung von Quadratwurzeln.

Beweis.

zu (a) Konstruiere eine Parallele zu $\overline{0z_2}$ durch z_1 und trage mit dem Zirkel die Länge von $\overline{0z_2}$ ab.

zu (b) Verlängere die Strecke $\overline{0z}$ bis zum zweiten Schnittpunkt mit dem Kreis vom Radius $|z|$ um 0.

zu (c) $|z|$ ist der Schnittpunkt des Kreises um 0 mit Radius $|z|$ (d.h. Zirkel bei 0 einstechen und bei z aufsetzen) mit der Geraden durch 0 und 1.

zu (d) Konstruiere ein Gleichseitiges Dreieck über $\overline{01}$. Die Spitze ist $e^{\frac{i\pi}{3}}$.

zu (e) Sei g_1 eine Gerade durch $|z_1|$ und $e^{\frac{i\pi}{3}}$. Sei s der Schnittpunkt der Geraden durch 0 und $e^{\frac{i\pi}{3}}$ mit dem Kreis um 0 mit Radius $|z_2|$. Dann konstruiere eine Parallele g_2 zu g_1 durch s. Der Schnittpunkt von g_2 mit der Geraden durch 0 und 1 ist $x = |z_1| \cdot |z_2|$.

zu (f) Analog zu (e) betrachte wieder die Gerade g_1 durch $|z|$ und $e^{\frac{i\pi}{3}}$. Konstruiere eine Parallele g_2 zu g_1 durch $|1| = 1$. Den Schnittpunkt von g_2 und der Geraden durch 0 und $e^{\frac{i\pi}{3}}$ bezeichne mit s, dann ist Der Schnittpunkt vom Kreis um 0 mit Radius $|s|$ und der Geraden durch 0 und 1 die gesuchte Lösung.

zu (g) Multipliziere die Beträge und Addiere die Winkel von z_1 und z_2.

zu (h) Konstruiere den Betrag von z^{-1} wie oben und negiere den Winkel von z.

zu (i) Ohne Einschränkung sei $z \neq 0$. Konstruiere einen oberen Halbkreis h mit den Endpunkten $-|z|$ und 1 sowie eine Senkrechte g durch 0 auf die Gerade durch 0 und 1. Bezeichne den Schnittpunkt von g und h mit q, dann ist $|q| = \sqrt{|z|}$.

zu (j) Für $\sqrt{z}$ gilt: Konstruiere den Berag wie oben und halbiere den Winkel von z. □

Satz 22.5 *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die $\{0,1\}$ enthält und $z \in \mathbb{C}$. Es gilt:*
Genau dann ist z aus M konstruierbar, wenn es eine Körperfolge $L_1, \ldots, L_n$ mit $z \in L_n$ und

$$\mathbb{Q}(M \cup M^C) = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_n$$

derart gibt, dass der Körpergrad von $[L_{i+1} : L_i]$ höchstens zwei ist.

Beweis. „⇒“: Ohne Einschränkung gelte $M = M^C \wedge i \in M$ mit $i^2 = -1$. Induktiv folgt die Behauptung nun aus Bemerkung 22.2.
„⇐“: Sei $[L_i : L_{i-1}] = 2$, dann gibt es $z_i \in L_{i-1}$ mit der Eigenschaft, dass $L_i = L_{i-1}(\sqrt{z_i})$.
Also ist $L_n \subseteq \mathfrak{X}(M)$, insbesondere gilt also $z \in L_n \subseteq \mathfrak{X}(M)$ □

Folgerung 22.6 *Sei $M \subseteq \mathbb{C}$ eine Teilmenge, die $\{0,1\}$ enthält und $z \in \mathfrak{X}(M)$, dann gelten:*
(a) $\mathfrak{X}(M)/\mathbb{Q}(M \cup M^C)$ ist eine algebraische Körpererweiterung
(b) $[\mathbb{Q}(M \cup M^C \cup \{z\}) : \mathbb{Q}(M \cup M^C)] = 2^r$ für $r \in \mathbb{N}$

Beweis. Die Behauptung ist ein Spezialfall von Satz 22.5. □

Satz 22.7 *(Konstruierbarkeit des regelmäßigen n-Ecks)*
Ohne Einschränkung sei der Mittelpunkt des n-Ecks der Nullpunkt und der Radius des Kreises um das n-Eck sei eins. Das regelmäßige n-Eck ist genau dann konstruierbar, wenn $\varphi(n) = 2^r$ ist mit $r \in \mathbb{N}$.

Beweis. Wir erinnern zunächst an die Eulersche φ-Funktion aus Definition 17.3:

$$\varphi(n) := \mathrm{Card}\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

„⇐“: Es genügt $\zeta_n := e^{\frac{2\pi i}{n}}$ zu konstruieren, denn die anderen Punkte können aus ζ_n durch Winkeladdition gewonnen werden.
Es gilt: $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist abelsch. Nach Voraussetzung ist: $\mathrm{Card}(G) = 2^r$.
Mit dem Hauptsatz über endlich erzeugte abelsche Gruppen erhalten wir:

$$G \cong \mathbb{Z}/2^{t_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/2^{t_s}\mathbb{Z}$$

Es gibt also $G_i \trianglelefteq G$ für $i = 1, \ldots, s$ mit $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_s = \{e\}$, mit $G_i/G_{i+1} \cong \mathbb{F}_2$.
Nun liefert uns der Hauptsatz der Galois-Theorie 16.6, dass es Körper L_i für $i = 1, \ldots, s$ gibt, die die Eigenschaft $\mathbb{Q}(\zeta_n) = L_s \supseteq L_{s-1} \supseteq \ldots \supseteq L_0 = \mathbb{Q}$ mit $[L_i : L_{i-1}] = 2$ haben, nämlich: $L_i = (\mathbb{Q}(\zeta_n))^{G_i}$ Mit Satz 22.5 folgt nun die Konstruierbarkeit aus $\{0,1\}$.
„⇒“: Nach Voraussetzung ist das n-Eck konstruierbar, also ist $\zeta_n \in \mathfrak{X}(\{0,1\})$ Nach Folgerung 22.6 ist dann

$$2^r = [\mathbb{Q}(\{0,1\}, \zeta_n) : \mathbb{Q}(\{0,1\})] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

Damit gilt, dass $\varphi(n) = 2^r$ ist. □

Definition 22.8 *(Fermat Primzahl)*
Eine Primzahl p heißt Fermat-Primzahl, falls es eine natürliche Zahl n mit der Eigenschaft $p = 2^{2^n} + 1$ gibt.

Beispiel 51 *(Fermat-Primzahlen bis $n = 4$)*
$n = 1 : \ p = 5$
$n = 2 : \ p = 17$
$n = 3 : \ p = 257$
$n = 4 : \ p = 65537$

Folgerung 22.9 *Das regelmäßige n-Eck ist genau dann Konstruierbar, wenn n von der Form*

$$n = 2^m \cdot p_1 \cdot \ldots \cdot p_s$$

mit verschiedenen Fermatprimzahlen $p_1, \ldots, p_s$ und $m \in \mathbb{N}$ ist.

Beweis. Aus Zeitgründen entfallen[5].

Satz 22.10 *(Würfelprobleme)*
(a) Aus einem gegebenen Würfel kann kein Würfel mit doppeltem Volumen konstruiert werden.
(b) Ein gegebener Winkel lässt sich nicht konstruktiv dreiteilen.

Beweis. Zu (a): Ohne Einschränkung sei die Kantenlänge des Würfels 1. Das doppelte Volumen ist somit 2. Die Kantenlänge des gesuchten Würfels ist $\sqrt[3]{2}$. Wäre dieser Würfel konstruierbar, dann wäre auch $\sqrt[3]{2} \in \mathfrak{X}(\{0,1\})$ enthalten. Dies ist aber eine Widerspruch zu Folgerung 22.6, da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist.
Zu (b): Ohne Einschränkung sei der Winkel 60^o. Wäre der Winkel 20^o konstruierbar, dann wäre auch das regelmäßige 18-Eck konstruierbar, aber $\varphi(18) = \varphi(9) = 2 \cdot 3 = 6$ □

Satz 22.11 *(Quadratur des Kreises)*
Es ist unmöglich zu gegebenem Kreis ein Quadrat mit dem selben FLächeninhalt zu konstruieren.

Beweis. Ohne Einschränkung sei der Kreisradius 1. Der Flächeninhalt des Kreises also π.
Nach dem Satz von Lindemann ist π transzendent über $\mathbb{Q}$. Die Kantenlänge $\sqrt{\pi}$ des gesuchten Quadrats ist demnach auch transzendent über $\mathbb{Q}$. Mit Folgerung 22.6 folgt nun die Behauptung. □

[5] Zum Beweis siehe: Bosh - Algebra, Seite 288 - Satz 5