Mitschrieb zur Vorlesung: Algebra I

Prof. Dr. Herrlich

Vorlesung Wintersemester 2005/2006

Letzte Aktualisierung und Verbesserung: 26. April 2008

Mitschrieb der Vorlesung Algebra I
von Herrn Prof. Dr. Herrlich im Wintersemester 2005/2006
von Marco Schreck.

Kommentare, Fehler und Vorschläge und konstruktive Kritik bitte an Marco.Schreck@gmx.de.

Inhaltsverzeichnis

Kapitel 1

Einführung/Wiederholung

Sei G eine Gruppe. Für $g \in G$ sei τ_g: $G \mapsto G$, $x \mapsto g \cdot x$ („Linksmultiplikation“). Wegen $\tau_g(e) = g$ ist dies kein Gruppenhomomorphismus. $\tau_e = \mathrm{id}$ ist jedoch einer.

Bemerkung:

Für jede Gruppe G ist die Abbildung τ: $G \mapsto \mathrm{Perm}(G)$, $g \mapsto \tau_g$ ein bijektiver Gruppenhomomorphismus (Satz von Cayley).

Beweis:

i.) $\tau_g \in \mathrm{Perm}(G)$: τ_g ist bijektiv mit Umkehrabbildung $\tau_{g^{-1}}$.

ii.) τ ist ein Gruppenhomomorphismus:

$\tau(g_1 g_2) \stackrel{?}{=} \tau(g_1) \circ \tau(g_2)$

Denn $\tau(g_1 \cdot g_2)(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \tau_{g_1}(\tau_{g_2}(x)) = (\tau_{g_1} \circ \tau_{g_2})(x)$ für alle $x \in G$.

iii.) Es ist $\mathrm{Kern}(\tau) = \{e\}$, denn ist $\tau(g) = \mathrm{id}_G$, so ist $\tau_g(x) = g \cdot x = x$ für alle $x \in G$, also $g = e$.

Definition und Bemerkung 1.11:

Sei G eine Gruppe und $g \in G$.

a.) Die Abbildung c_g: $G \mapsto G$, $x \mapsto gxg^{-1}$ ist ein Automorphismus und heißt **Konjugation** mit g.

b.) Die Abbildung c: $G \mapsto \mathrm{Aut}(G)$, $g \mapsto c_g$ ist ein Gruppenhomomorphismus.

c.) $Z(G) := \mathrm{Kern}(c)$ heißt **Zentrum** von G. Es ist $Z(G) = \{g \in G : gx = xg \text{ für alle } x \in G\}$.

d.) Die Elemente von $\mathrm{Bild}(c) =: \mathrm{Aut}_i(G)$ heißen **innere Automorphismen** von G.

e.) Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** von G, wenn $c_g(N) \subseteq N$ für jedes $g \in G$ (stabil unter allen Konjugationen). Äquivalent ist: $gxg^{-1} \in N$ für alle $g \in G$ und $x \in N$

f.) Ist f: $G \mapsto G'$ ein Gruppenhomomorphismus, so ist $\mathrm{Kern}(f)$ Normalteiler in G.

g.) $\mathrm{Aut}_i(G)$ ist Normalteiler in $\mathrm{Aut}(G)$.

a.) c_g ist ein Homomorphismus.

$c_g(x_1 x_2) = g(x_1 x_2)g^{-1}$

$c_g(x_1) \cdot c_g(x_2) = (gx_1g^{-1})(gx_2g^{-1}) = gx_1x_2g^{-1} = g(x_1x_2)g^{-1}$

c_g ist außerdem bijektiv, denn es existiert eine Umkehrabbildung $c_{g^{-1}}$. Damit handelt es sich um einen Automorphismus.

b.) $c(g_1g_2)(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1(g_2 \cdot x \cdot g_2^{-1})g_1^{-1} = c_{g_1}(c_{g_2}(x)) = (c_{g_1}) \circ c(g_2)(x)$ für alle $x \in G$

c.) klar

f.) Sei $x \in \text{Kern}(f)$ und $g \in G$. Dann ist $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = e'$.

g.) Sei $g \in \text{Aut}(G)$ und $g \in G$. Zu zeigen ist $\varphi c_g \varphi^{-1} \in \text{Aut}_i(G)$.

$$(\varphi \circ c_g \circ g^{-1})(x) = \varphi(c_g(\varphi^{-1}(x))) = \varphi(g \cdot \varphi^{-1}(x) \cdot g^{-1}) = \varphi(g) \cdot \varphi(\varphi^{-1}(x)) \cdot \varphi(g^{-1}) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = \\ = g_{\varphi(g)}(x) \, \forall \, x \in G$$

Hieraus folgt dann $\varphi \circ c_g \circ \varphi^{-1} = c_{\varphi(g)} \in \text{Aut}_i(G)$.

Definition und Bemerkung 1.12:

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe.

a.) Für $g \in G$ heißt $g \cdot H := \{g \cdot h : h \in H\} = \tau_g(H)$ **Linksnebenklasse** und $H \cdot g = \{h \cdot g : h \in H\}$ heißt **Rechtsnebenklasse** von g bezüglich H.

b.) Für $g_1, g_2 \in G$ gilt $g_1H \cap g_2H \neq \varnothing \Leftrightarrow g_1H = g_2H$ (Nebenklassen zerlegen die Gruppe in disjunkte Teilmengen.)

c.) H ist genau dann Normalteiler, wenn $gH = Hg$ für alle $g \in G$ gilt.

d.) Alle Nebenklassen von G bezüglich H sind gleichmächtig.

e.) Die Anzahl der Linksnebenklassen bezüglich H ist gleich der Anzahl der Rechtsnebenklassen. Sie heißt **Index** $[G : H]$ von H in G.

f.) Ist G endlich, so ist $[G : H] = |G|/|H|$ (Satz von Lagrange).

Beweis:

b.) „$\Rightarrow$“: Sei $y = g_1h_1 = g_2h_2 \in g_1H \cap g_2H$ mit $h_1, h_2 \in H$. Hieraus ergibt sich $g_1 = g_2h_2h_1^{-1} \in g_2H$ und daraus folgt $g_1H \subseteq g_2H$. Aus Symmetriegründen gilt auch $g_2H \subseteq g_1H$.

c.) $g \cdot H = H \cdot g \Leftrightarrow H = gHg^{-1}$

d.) τ_g: $H \mapsto gH$, $h \mapsto gh$ ist bijektiv.

e.) Die Zuordnung {Linksnebenklasse} $\mapsto$ {Rechtsnebenklasse}, $g \cdot H \mapsto H \cdot g^{-1}$ ist wohldefiniert und bijektiv.

i.) Ist $g_1H = g_2H$, also $g_2 = g_1h$ für ein $h \in H$, so folgt $Hg_2^{-1} = H(g_1h)^{-1} = H \cdot h^{-1}g_1^{-1} = Hg_1^{-1}$.

f.) Wir zerlegen G in disjunkte Vereinigung der $[G : H]$ Linksnebenklassen bezüglich H, diese haben alle $|H|$ Elemente.

1.1 Quotientenbildung

Definition und Bemerkung 1.13:

Sei f: $M \mapsto M'$eine Abbildung von Mengen.

a.) Die Relation $\sim_f$ auf M, $x \sim_f y \Leftrightarrow f(x) = f(y)$ ist eine Äquivalenzrelation.

b.) Für $x \in M$ sei $\overline{x} := \{y \in M : y \sim_f x\}$. Es ist $\overline{x} = f^{-1}(f(x))$. Es ist darüber hinaus $\overline{M} := M/\sim_f := \{\overline{x} : x \in M\}$.

c.) Ist f: $(M, \cdot) \mapsto (M', *)$ ein Homomorphismus, so wird durch $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ eine Verknüpfung auf $\overline{M}$ definiert.

d.) Ist $(M, \cdot)$ ein Homomorphismus, so auch $(\overline{M}, \cdot)$.

Beweis:

c.) Zu zeigen ist, dass $\cdot$ wohldefiniert ist. Seienalso $x' \in \overline{x}$ und $y' \in \overline{y}$. Es muss also $\overline{x' \cdot y'} = \overline{x \cdot y}$ gelten. Es gilt $f(x') = f(x)$ und $f(y') = f(y)$, womit folgt:

$$f(x' \cdot y') = f(x') * f(y') = f(x) * f(y) = f(x \cdot y)$$

Definition und Bemerkung 1.14:

Sei $f\colon G \mapsto G'$ ein Gruppenhomomorphismus.

a.) $\overline{G} = G/\sim_f$ ist die Menge der Linksnebenklassen bezüglich Kern(f).

b.) $\overline{G} =: G/\text{Kern}(f)$ heißt **Faktorgruppe** von G bezüglich Kern(f).

Beweis:

Seien x, $y \in G$. Dann gilt $\overline{x} = \overline{y} \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x) \cdot f(y^{-1}) = e' \Leftrightarrow xy^{-1} \in \text{Kern}(f) \Leftrightarrow y = (xy^{-1})^{-1}x \in \text{Kern}(f) \cdot x \Leftrightarrow x^{-1}y \in \text{Kern}(f) \Leftrightarrow y = x(\cdot x^{-1}y) \in x \cdot \text{Kern}(f)$

Definition und Bemerkung 1.18:

Sei $(A, +)$ eine abelsche Gruppe, $X \subseteq A$.

a.) A heißt **freie abelsche Gruppe** mit Basis X, wenn jedes $a \in A$ eine eindeutige Darstellung

$$a = \sum_{x \in X} n_x \cdot x$$

besitzt mit $n_x \in \mathbb{Z}$ und $n_x \neq 0$ nur für endlich viele $x \in X$. Ist in dieser Situation $|X| = n$, so heißt n der **Rang** von A. A ist isomorph zu $\mathbb{Z}^\times := \bigoplus_{x \in X} \mathbb{Z}$.

b.) Universelle Abbildungseigenschaft der freien abelschen Gruppe:

Zu jeder abelschen Gruppe A und jeder Abbildung $f\colon X \mapsto A$ gibt es genau einen Homomorphismus φ: $\mathbb{Z}^\times \mapsto A$ mit $\varphi(x) = f(x)\ \forall\ x \in X$.

Beweis:

a.) $A \mapsto \mathbb{Z}^\times\colon \sum n_x x \mapsto (n_x)_{x \in X}$ ist Isomorphismus, weil die Darstellung laut Forderung eindeutig sein soll.

b.) Setze $\varphi\left(\sum_{x \in X} n_x x\right) := \sum_{x \in X} n_x f(x)$.

Wichtigstes Beispiel:

Sei X endlich, $X = \{x_1, \ldots, x_n\}$. Dann ist $\mathbb{Z}^\times \simeq \mathbb{Z}^n$. $\mathbb{Z}^n$ ist so etwas ähnliches wie ein Vektorraum; man bezeichnet $\mathbb{Z}^n$ als „freier Modul“. Insbesondere lassen sich die Gruppenhomomorphismen $\mathbb{Z}^n \mapsto \mathbb{Z}^n$ durch eine $m \times n$-Matrix mit Einträgen in $\mathbb{Z}$ beschreiben.

Satz 2 (Elementarteilersatz):

Sei H eine Untergruppe von $\mathbb{Z}^n$ (mit $n \in \mathbb{N} \setminus \{0\}$). Dann gibt es eine Basis $\{x_1, \ldots, x_n\}$ von $\mathbb{Z}^n$, ein $r \in \mathbb{N}$ mit $0 \leq r \leq n$ und $a_1, \ldots, a_r \in \mathbb{N} \setminus \{0\}$ mit a_i / a_{i+1} für $i = 1, \ldots, r-1$, so dass $a_1 x_1, \ldots, a_r x_r$ eine Basis von H ist. Insbesondere ist H auch eine freie abelsche Gruppe.

Beweis:

Der 1.Schritt ist, dass H endlich erzeugt ist. Dies zeigen wir durch vollständige Induktion über n. Für $n = 1$ ist die Aussage erfüllt. Für $n > 1$ sei $e_1, \ldots, e_n$ eine Basis von $\mathbb{Z}^n$. Wir definieren eine Abbildung $\Pi\colon \mathbb{Z}^n \mapsto \mathbb{Z}$ der Form $\sum_{i=1}^n a_i e_i \mapsto a_n$ („Projektion auf letzte Komponente“).

- 1.Fall: $\Pi(H) = \{0\} \Rightarrow H \subseteq \mathbb{Z}^{n-1}$, aber endlich erzeugt nach Induktionsvoraussetzung
- 2.Fall: $\Pi(H) = l \cdot \mathbb{Z}$ für ein $l \in \mathbb{N} \setminus \{0\}$. Sei $y \in H$ mit $\Pi(y) = e$. Behauptung: $H \simeq \langle y \rangle \bigoplus (H \cap \text{Kern}(\Pi))$. Dann folgt die Behauptung von Schritt 1, da $\text{Kern}(\Pi) \simeq \mathbb{Z}^{n-1}$. Dann ist $H \cap \text{Kern}(\Pi)$ Untergruppe von $\mathbb{Z}^{n-1}$, also endlich erzeugt nach Induktionsvoraussetzung. Also ist auch H endlich erzeugt. Wollen wir also diese Behauptung beweisen:

  Es gilt $\langle y \rangle \cap\ (H \cap \text{Kern}(\Pi)) = \{0\}$ nach Definition von y. Also ist die Summe direkt. Sei $z \in H$ mit $\Pi(z) = k \cdot l$ für ein $k \in \mathbb{Z}$. Also ist $z - k \cdot g \in H \cap \text{Kern}(\Pi)$, woraus die Behaupung folgt.

2.Schritt: Sei $y_1, \ldots, y_r$ ein Erzeugendensystem von H. Nach Schritt 1 kann $r \leq n$ erreicht werden. Schreibe $y_j = \sum_{i=1}^{n} a_{ij} e_i$. Dann ist $A := (a_{ij}) \in \mathbb{Z}^{n \times r}$ eine Darstellungmatrix der Abbildung $H \mapsto \mathbb{Z}^n$ bezüglich der Basen $\{y_1, \ldots, y_r\}$ von H und $\{e_1, \ldots, e_n\}$ von $\mathbb{Z}^n$. Zeilen- und Spaltenumformungen entsprechen Basiswechsel in H bzw. $\mathbb{Z}^\times$. Vorsicht: Dabei dürfen nur **ganzzahlige** Basiswechselmatrizen benutzt werden, deren inverse Matrix ebenfalls ganzzahlige Einträge hat!

Das Ziel ist nun, A durch elementare Zeilen- und Spaltenumformungen auf Diagonalgesalt zu bringen.

$$\widetilde{A} := \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{pmatrix} \text{ mit } a_i \in \mathbb{Z} \text{ und } a_i / a_{i+1} \, \forall \, i = 1, \ldots, r-1$$

Kommen wir zum dritten Schritt. Wir werden sehen, dass dies mit dem ganzzahligen Gauss-Algorithmus möglich ist!

i.) Suche den betragsmäßig kleinsten Matrixeintrag $\neq 0$ und bringe diesen nach a_{11}. Dazu brauche ich höchstens eine Zeilen- und eine Spaltenvertauschung.

ii.) Stelle fest, ob alle a_{i1} $(i = 2, \ldots, n)$ durch a_{11} teilbar sind. Falls nicht, teile a_{i1} mit Rest durch a_{11}. Dann kann ich a_{i1} schreiben als $a_{i1} = q a_{11} + r$ mit $0 < r < |a_{11}|$. Dann ziehe von der i-ten Zeile das q-fache der ersten ab. Die neue i-te Zeile beginnt jetzt mit $\widetilde{a}_{i1} = r$. Dann gehe ich wieder zurück zu i.)

iii.) Sind schließlich alle a_{i1} durch a_{11} teilbar, so wird die erste Spalte zu $(a_{11}, 0, \ldots, 0)^\intercal$ gemacht, indem man von der i-ten Zeile das a_{i1}/a_{11}-fache der ersten Zeile abzieht.

iv.) Genauso wird die erste Zeile zu $(a_{11}, 0, \ldots, 0)$.

v.) Gibt es jetzt noch einen Matrixeintrag a_{ij} $(i, j \geq 2)$, der nicht durch a_{11} teilbar ist, schreibe $a_{ij} = q a_{11} + r$ mit $0 < r < |a_{11}$. Ziehe von der i-ten Zeile das q-fache der ersten ab. Die neue i-te Zeile lautet dann $(-q a_{11}, a_{i2}, \ldots, a_{ij}, \ldots, a_{ir})$, da $a_{i1} = 0$, $a_{1k} = 0$ für $1 < k \leq r$. Addiert man nun zur j-ten Spalte die erste hinzu, so ist das neue Element $\widetilde{a}_{ij} = a_{ij} - q a_{11} = r$. Dann geht man zurück zu i.)

vi.) Nach endlich vielen Schritten erhält man eine Matrix, die folgendermaßen aussieht:

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

in der alle Einträge von A' durch a_{11} teilbar sind. Wende Schritte i.) bis v.) auf A' an.

Ergänzung:

1.) In der Situation von Satz 2 heißen die a_{ii} $(i = 1, \ldots, r)$ heißen **Elementarteiler** von H.

2.) Ist $A = (h_1, \ldots, h_r) \in \mathbb{Z}^{n \times r}$, so erzeugen die Spalten $h_1, \ldots, h_r$ die Untergruppe von $\mathbb{Z}^n$. A ist die Darstellungsmatrix der Einbettung $H \mapsto \mathbb{Z}^n$. Die Elementarteiler von H heißen dann auch die Elementarteiler der Matrix A.

Satz 3 (für endlich erzeugte abelsche Gruppen):

Jede endlich erzeugbare abelsche Gruppe A ist isomorph zu einer direkten Summe von zyklischen Gruppen. Genauer: Es gibt r, $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathbb{N}$, $a_i \geq 2 \; \forall \; i$, a_i / a_{i+1} für $i = 1, \ldots, n-1$, so dass gilt:

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$$

r, m und die a_i sind durch A eindeutig bestimmt.

Beweis:

1.) Sei $x_1, \ldots, x_n$ ein Erzeugendensystem von A. Nach 1.18 gibt es einen surjektiven Gruppenhomomorphismus $\varphi\colon \mathbb{Z}^n \mapsto A$ mit $\varphi(e_i) = x_i$ für $i = 1, \ldots, n$. Nach dem Homomorphiesatz ist dann $A \simeq \mathbb{Z}^n/\mathrm{Kern}(\varphi)$. Nach Satz 2 gibt es $m \in \mathbb{N}$, $m \leq n$, die Basis $z_1, \ldots, z_n$ von $\mathbb{Z}^n$ und Elementarteiler $a_1, \ldots, a_m$ mit $a_i | a_{i+1}$, mit $i = 1, \ldots, m-1$, so dass $a_1 z_1, \ldots, a_m z_m$ Basis von $\mathrm{Kern}(\varphi)$ ist. Dann ist

$$A \simeq \mathbb{Z}^n/\mathrm{Kern}(\varphi) \simeq \left(\bigoplus_{i=1}^{n} z_i\mathbb{Z}\right) / \left(\sum_{i=1}^{n} a_i z_i \mathbb{Z}\right) \simeq \bigoplus_{i=1}^{m} (a_i\mathbb{Z}/a_i z_i \mathbb{Z}) \bigoplus_{i=m+1}^{n} z_i\mathbb{Z} \simeq \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z} \bigoplus \mathbb{Z}^{n-m}$$

Es bleibt nun noch die Eindeutigkeit zu beweisen. Fangen wir mit r, dem freien Anteil, an. r ist die maximale Anzahl linear unabhängiger Elemente in A. r ist also eindeutig durch die Gruppe A festgelegt. Sei also

$$T := \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z} \simeq \bigoplus_{j=1}^{m'} \mathbb{Z}/b_j\mathbb{Z} := T' \text{ mit } b_j | b_{j+1} \text{ für } j = 1, \ldots, m-1$$

Zu zeigen ist, dass diese beiden Zerlegungen die gleiche Anzahl von direkten Summanden haben, dass also $m' = m$ gilt, und dass alle Summanden gleich sind: $a_i = b_i$ für $i = 1, \ldots, m$. Behauptung: Für jedes $x \in T$ ist $\mathrm{ord}(x)$ Teiler von a_m. Genauso ist für jedes $y \in T'$ $\mathrm{ord}(y)$ Teiler von $b_{m'}$. T enthält auf alle Fälle ein Element von Ordnung a_m, nämlich $(\overline{0}, \ldots, \overline{0}, \overline{1})$. Hieraus folgt, dass auch T' ein Element von Ordnung a_m enthält. Hieraus folgt $a_m | b_{m'}$. Umgekehrt ist auch $b_{m'}$ ein Teiler von a_m, woraus $a_m = b_{m'}$ folgt. Sei

$$\widetilde{T} := T/(\mathbb{Z}/b_m\mathbb{Z}) \simeq \bigoplus_{i=1}^{m-1} \mathbb{Z}/a_i\mathbb{Z}$$

und

$$\widetilde{T}' = T/(\mathbb{Z}/b_{m'}\mathbb{Z}) \simeq \bigoplus_{j=1}^{m'-1} \mathbb{Z}/b_j\mathbb{Z}$$

Aus der vollständigen Induktion über m folgt die Eindeutigkeit für $\widetilde{T}$ und hieraus der Satz. q.e.d.

Jetzt müssen wir noch die Behauptung beweisen. Sei $x = (x_1, \ldots, x_m) \in T$ mit $x_i \in \mathbb{Z}/a_i\mathbb{Z}$. Hieraus folgt $a_m x = (a_m \cdot x_1, \ldots, a_m \cdot x_m)$. Damit ist $\mathrm{ord}(x)$ Teiler vom a_m.

1.2 Freie Gruppen

Definition und Bemerkung 1.20:

Sei F eine Gruppe und $X \subseteq F$.

a.) F heißt **freie Gruppe mit Basis X**, wenn jedes $y \in F$ eine eindeutige Darstellung $y = x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n}$ hat, in der $n \geq 0$ ($n = 0$ ist das „leere Wort“, es ist das neutrale Element in F.) und $x_i \in X$ für $i = 1, \ldots, n$. Weiterhin ist $\varepsilon_i \in \{+1, -1\}$ für $i = 1, \ldots, n$, $x_{n+1}^{\varepsilon_{i+1}} \neq x_i^{-\varepsilon}$ für $i = 1, \ldots, n-1$.

b.) Ist F frei mit Basis X, so gilt für jedes $x \in X$: $x^{-1} \notin X$ und $\mathrm{ord}(x) = \infty$.

c.) $\mathbb{Z}$ ist frei mit Basis $\{1\}$ (oder $\{-1\}$). (einzige kommutative freie Gruppe)

d.) Ist F frei mit Basis X und $|X| \geq 2$, os ist F nicht abelsch.

Beweis: Seien $x_1, x_2 \in X$ mit $x_1 \neq x_2$. Der Kommutator $x_1 x_2 x_1^{-1} x_2^{-1}$ ist $\neq e$, da wir schon die Darstellung von e in Form des „leeren Wortes“ haben. Daraus folgt $x_1 x_2 \neq x_2 x_1$.

Satz 4:

a.) Zu jeder Menge X gibt es eine freie Gruppe $F(X)$ mit Basis X.

b.) Zu jeder Gruppe G und jeder Abbildung $f\colon X \mapsto G$ gibt es genau einen Gruppenhomomorphismus $\varphi\colon F(X) \mapsto G$ mit $\varphi(x) = f(x)$ für alle $x \in X$.

c.) Jede Gruppe ist Faktorgruppe einer freien Gruppe.

d.) Es gilt $F(x) \simeq F(y)$ genau dann, wenn $|X| = |Y|$.

Beweis:

a.) Sei $X^{\pm} = X \times \{\pm 1\}$ und i: $X^{\pm} \mapsto X^{\pm}$ die Abbildung $i(x, \epsilon) = x(-\epsilon)$. i ist bijektiv und $i^2 = \mathrm{id}$. Schreibweise: $(x, 1) =: x$ und $x(-1) =: x^{-1}$. So ist $i(x) = x^{-1}$ und $i(x^{-1}) = x$. Ein Element $y = (x_1, \ldots, x_n) \in F^{\epsilon}(X^{\pm})$ (freie Worthalbgruppe) heißt **reduziert**, wenn $x_{\nu+1} + i(x_\nu)$ für $\nu = 1, \ldots, n_1$. Sei $F(X)$ die Menge der reduzierten Wörter in $F^a(X^{\pm})$.

Definition:

Zwei Wörter in $F^a(X^{\pm})$ heißen **äquivalent**, wenn sie durch endliches Einfügen oder Streichen von Wörtern der Form $(x, i(x))$ mit $x \in X^{\pm}$ auseinander hervorgehen.

Beispiel:

Es ist $x_1 \sim x_1 x_2 x_2^{-1} \sim x_1 x_2 x_3^{-1} x_3 x_2^{-1}$.

Behauptung:

In jeder Äquivalenzklasse gibt es genau ein reduziertes Wort.

Dann definiere das Produkt auf $F(X)$: $(x_1, \ldots, x_n) * (y_1, \ldots, y_m)$ sei **das** reduzierte Wort in der Äquivalenzklasse von $(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Dieses Produkt ist assoziativ. Für x, y, $z \in F(X)$ ist $(x*y)*z$ das eindeutig bestimmte reduzierte Wort in der Klasse von $(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_l)$. Das gleiche gilt für $x*(y*z)$. Das neutrale Element ist $e = ()$ und das inverse zu $(x_1, \ldots, x_n)$ ist $(i(x_n), i(x_{n-1}), \ldots, i(x_1))$. $F(X)$ ist damit frei mit Basis X nach Konstruktion.

Beweis:

In jeder Klasse gibt es ein reduziertes Wort. Nun noch zur Eindeutigkeit: Seien x, y reduziert und äquivalent. Dann gibt es ein Wort w, aus dem sowohl x als auch y durch Streichen hervorgeht. Zu zeigen ist also, dass jede Reihenfolge von Streichungen in w zum selben reduzierten Wort führt. Induktion über die Länge $l(w)$: $l(w) = 0$, $l(w) = 1$ (klar)

Sei $l(w) \geq 2$: Enthält w genau ein Paar $(x_\nu, i(x_\nu))$, so muss das als erstes gestrichen werden. Es entsteht w' mit $l(w') = l(w) - 2$. Aus der Induktionvoraussetzung folgt die Behauptung. Enthält w Paare $(x_\nu, i(x_\nu))$ und $(x_\mu, i(x_\mu))$, so gibt es zwei Fälle, nämlich erstens $\mu = \nu + 1$, $(x_\nu, i(x_\nu), x_\nu)$. Dann führen beide Streichungen zum selben Wort. Sei zweitens $\mu \geq \nu + 2$. Streiche beide Paare und erhalte w'' mit $l(w'') = l(w) - 4$. Die Behauptung folgt dann wieder aus der Induktionsvoraussetzung.

b.) Wir gehen aus von:

$$\varphi(x_1, \ldots, x_n) := \widetilde{f}(x_1) \cdot \widetilde{f}(x_2) \cdot \ldots \cdot \widetilde{f}(x_n) \text{ mit } \widetilde{f}(x_i) = \begin{cases} f(x_i) & \text{für} \quad x_i \in X \\ f(x_i^{-1})^{-1} & \text{für} \quad x_i \in X^- = \{(x_i^{-1}) \in X^{\pm}\} \end{cases}$$

Damit ist Existenz und Eindeutigkeit bewiesen.

c.) Sei $S \subseteq G$ ein Erzeugendensystem. (Das heißt, die einzige Untergruppe H von G mit $S \subseteq H$ ist G selbst.) Sei $F(S)$ die freie Gruppe mit Basis S und f: $S \mapsto G$ die Identität und φ: $F(S) \mapsto G$ der Homomorphismus aus b.) φ ist surjektiv, weil $\varphi(F(S))$ Untergruppe ist, die S enthält. Also ist nach dem Homomorphiesatz $G \simeq F(s)/\mathrm{Kern}(\varphi)$.

d.) „$\Leftarrow$“: Sei f: $X \mapsto Y$ eine bijektive Abbildung. Dazu gibt es einen Gruppenhomomorphismus φ_f: $F(X) \mapsto F(Y)$ und $\varphi_{f^{-1}}$: $F(Y) \mapsto F(X)$. Wenn man die Abbildungen einschränkt auf die Basen X bzw Y, so gilt $\varphi_f \circ \varphi_{f^{-1}}|_Y = \mathrm{id}_Y$ und $\varphi_{f^{-1}} \circ \varphi_f|_X = \mathrm{id}_X$. Mit der Eindeutigkeit aus b.) folgt $\varphi_f \circ \varphi_{f^{-1}} = \mathrm{id}_{F(Y)}$ und ebenso $\varphi_{f^{-1}} \circ \varphi_f = \mathrm{id}_{F(X)}$.

$\varphi_f \circ \varphi_{f^{-1}}|_Y : Y \mapsto Y \hookrightarrow F(Y)$

d.) „$\Rightarrow$“: Sei $|X| \neq |Y|$. Die Anzahl der Gruppenhomomorphismen von $F(X)$ in $\mathbb{Z}/2\mathbb{Z}$ ist gleich der Anzahl der Abbildungen von X nach $\mathbb{Z}/2\mathbb{Z}$ (wegen b). Diese ist $|(\mathbb{Z}/2\mathbb{Z})^X| = 2^{|X|}$.

1.3 Kategorien und Funktoren

Definition 1.21:

Eine **Kategorie** $\mathcal{C}$ besteht aus einer Klasse $\mathrm{Ob}(\mathcal{C})$ von Objekten und für je zwei Objekte A, $B \in \mathrm{Ob}(\mathcal{C})$ aus einer Menge von **Morphismen** $\mathrm{Mor}_{\mathcal{C}}(A,B)$ von A nach B, für die folgende Eigenschaften erfüllt sind:

i.) Für jedes $A \in \mathrm{Ob}(\mathcal{C})$ gibt es ein Element $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$.

ii.) Für je drei Objekte A, B und C gibt es eine Abbildung $\circ\, \mathrm{Mor}(B,C) \times \mathrm{Mor}(A,B) \mapsto \mathrm{Mor}(A,C)$, $(g, f) \mapsto g \circ f$ mit $g \circ \mathrm{id}_A = g$ für alle $g \in \mathrm{Mor}(A,B)$, $\mathrm{id}_B \circ f = f$ für alle $f \in \mathrm{Mor}(A, B)$ und $(h \circ g) \circ f = h \circ (g \circ f)$ für alle f, g und h.

Beispiele:

1.) Mengen mit Abbildungen

2.) Mengen mit bijektiven Abbildungen

3.) K-Vektorräume mit K-linearen Abbildungen

4.) Halbgruppen mit Homomorphismen

5.) Monoide mit Homomorphismen

6.) Mengen mit Homomorphismen

7.) Gruppen mit Homomorphismen

8.) abelsche Gruppen mit Homomorphismen

9.) topologische Räume mit stetigen Abbildungen

Definition 1.22:

Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien.

a.) Ein **kovarianter Funktor** F: $\mathcal{A} \mapsto \mathcal{B}$ besteht aus einer Abbildung F: $\mathrm{Ob}(\mathcal{A}) \mapsto \mathrm{Ob}(\mathcal{B}$ sowie für je zwei Objekte X, $Y \in \mathrm{Ob}(\mathcal{A}$ aus einer Abbildung F: $\mathrm{Mor}_{\mathcal{A}}(X,Y) \mapsto \mathrm{Mor}_{\mathcal{B}}(F(X), F(Y))$, so dass gilt:

i.) $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$ für alle $x \in \mathrm{Ob}(\mathcal{A})$

ii.) $F(g \circ f) = F(g) \circ F(f)$ für alle g, $f \in \mathcal{A}$

[b.)] Ein **kontravarianter Funktor** F: $\mathcal{A} \mapsto \mathcal{B}$ besteht aus einer Abbildung F: $\mathrm{Ob}(\mathcal{A}) \mapsto \mathrm{Ob}(\mathcal{B}$ sowie für je zwei Objekte X, $Y \in \mathrm{Ob}(\mathcal{A}$ aus einer Abbildung F: $\mathrm{Mor}_{\mathcal{A}}(X,Y) \mapsto \mathrm{Mor}_{\mathcal{B}}(F(Y), F(X))$, so dass gilt:

i.) $X \xrightarrow{f} Y \xrightarrow{g} Z$, $F(X) \xleftarrow{F(f)} F(Y) \xleftarrow{F(g)} F(Z)$

ii.) $F(g \circ f) = F(f) \circ F(g)$

Beispiele:

1.) Gruppen $\mapsto$ Mengen: $(G, \bullet) \mapsto G$ („Vergissfunktor“)

2.) $\mathcal{P}$: Mengen $\mapsto$ Mengen, $X \mapsto \mathcal{P}(X)$ (Potenzmenge)
Für f: $X \mapsto Y$ sei $\mathcal{P}(f)$: $\mathcal{P}(X) \mapsto \mathcal{P}(Y)$, $U \mapsto f(U)$.

3.) Sei $\mathcal{C}$ Kategorie und X ein Objekt in $\mathcal{C}$. Definiere Funktoren $\mathcal{C} \mapsto$ Mengen durch $\mathrm{Hom}(X,\bullet)$: $Y \mapsto \mathrm{Mor}_{\mathcal{C}}(X,Y)$ bzw. $\mathrm{Hom}(\bullet,X)$: $Y \mapsto \mathrm{Mor}_{\mathcal{C}}(Y,X)$. Für f: $Y \mapsto Z$ ist $\mathrm{Hom}(X,\bullet)(f)$: $\mathrm{Hom}(X,Y) \mapsto \mathrm{Hom}(X,Z)$, $g \mapsto f \circ g$ und $\mathrm{Hom}(\bullet,X)(f)$: $\mathrm{Mor}(Z,X) \mapsto \mathrm{Mor}(Y,X)$, $g \mapsto g \circ f$. Der erste Funktor is ko- und der zweite kontravariant.

4.) Sei X Menge und F_X: Gruppen $\mapsto$ Mengen, $G \mapsto \mathrm{Abbildung}(X,G) = \mathrm{Mor}_{\mathrm{Menge}}(X,G)$. Für jedes f: $X \mapsto G$ gibt es ein φ: $F(X) \mapsto G$ (Satz 4), also die Bijektion α_G: $F_X(G) \mapsto \mathrm{Hom}_{\mathrm{Gruppe}}(F(X), G)$.

Satz 5:

Sei G eine endliche Gruppe mit $|G| = p^k \cdot m$.

a.) G enthält eine Untergruppe S von der Ordnung p^k („p-SYLOWgruppe“)

b.) Alle p-SYLOWgruppen in G sind konjugiert.

c.) Die Anzahl s_p der p-SYLOWgruppen in G erfüllt: $s_p|m$, $s_p \equiv 1 \mod p$.

Beweis:

b.) Sei $S \subset G$ eine p-SYLOWgruppe.

S $:= \{S' \subset G : S' = gSg^{-1}$ für ein $g \in G\}$

Behauptung 2: $p \nmid |\mathcal{S}|$ Wir wollen die Behauptung 2 beweisen: G operiert auf $\mathcal{S}$ durch Konjugation. Diese Aktion ist transitiv, das heißt, es gibt nur eine Bahn. Die Fixgruppe von S unter dieser Aktion ist $N_{S'} := \{g \in G : gS'g^{-1} = S'\}$. $N_{S'}$ heißt der **Normalisator** von S' in G. (S' ist Normalteiler in $N_{S'}$ nach Konstruktion und ist maximal mit dieser Eigenschaft.) Hieraus folgt $|\mathcal{S}| = [G : N_S] = |G|/|N_S| = (p^k \cdot m)/|N_S|$. S ist Untergruppe von N_S. Damit ergibt sich $p^k||N_S|$ und dass $|\mathcal{S}|$ Teiler ist von m. Sei $\widetilde{S}$ eine p-SYLOWgruppe in G. Zu zeigen ist, dass $\widetilde{S} \in \mathcal{S}$. $\widetilde{S}$ operiert auch auf $\mathcal{S}$ (da $\widetilde{S} \subset G$). Sei $S_1, \ldots, S_r$ ein Vertretersystem der Bahnen:

$$|\mathcal{S}| = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S}_{S_i}] = \sum_{i=1}^{r} \frac{p^k}{|\widetilde{S}_{S_i}|}$$

Aus Behauptung 2 folgt, dass es ein i mit $\widetilde{S} = \widetilde{S}_i$ gibt. Dann ist $\widetilde{S} \subseteq N_{S_i}$.

Behauptung 3: Dann ist $\widetilde{S} \subseteq S_i$. (Also ist $\widetilde{S} = S_i$, da beide p^k Elemente haben.) Es bleibt also noch Behauptung 3 zu beweisen. S_i ist Normalteiler in N_{S_i}, $\widetilde{S}$ ist Untergruppe in N_{S_i}. Damit ist $\widetilde{S} \cdot S_i$ Untergruppe von N_{S_i} (siehe Übung 4, Aufgabe 1). Wäre $\widetilde{S} \not\subseteq S_i$, dann wäre $\widetilde{S} \cdot S_i \supsetneq S_i$, also $|\widetilde{S} \cdot S_i| = p^k \cdot d$ mit $d > 1$ (und $p \nmid d$).

$\widetilde{S} \cdot S_i / S_i \simeq \widetilde{S}/(\widetilde{S} \cap S_i)$ (nach Übung 4, Aufgabe 1)

Hieraus ergibt sich:

$$p^k \cdot d = |\widetilde{S} \cdot S_i| = \frac{|S_i||\widetilde{S}|}{|\widetilde{S} \cap S_i|} = \frac{p^{2k}}{|\widetilde{S} \cap S_i|} = p^l \text{ für ein } l$$

Nach Voraussetzung ist $d \neq 1$, womit dies ein Widerspruch darstellt.

c.) Aus $s_p = |\mathcal{S}|$ folgt, dass $s_p|m$ und

$$|\mathcal{S}| = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S}_{S_i}]$$

Es ist $[\widetilde{S} : \widetilde{S}_{S_i}] = 1$ genau dann, wenn $\widetilde{S} = \widetilde{S}_{S_i}$ und nach Behauptung 3 ist dies genau dann der Fall, wenn $\widetilde{S} = S_i$, also genau **einmal**. Alle anderen Summanden sind durch p teilbar.

1.4 Kompositionsreihen

Beginnen wir mit einer Vorüberlegung. Angenommen, wir haben eine Gruppe G, $N \trianglelefteq G$ sei Normalteiler und G/N die Faktorgruppe. Kann man die Gruppe G aus dem Normalteiler N und der Faktorgruppe G/N rekonstruieren, ist also G durch N und G/N eindeutig bestimmt? Schreibweise: $1 \mapsto N \mapsto G \mapsto G/N \mapsto 1$ ist exakt.

Definition (1.26):

Sei $(*) \ldots \mapsto G_{i-1} \xrightarrow{\alpha_{i-1}} G_i \xrightarrow{\alpha_1} G_{i+1} \mapsto \ldots$ eine Sequenz von Gruppen und Gruppenhomomorphismen. Diese Sequenz heißt exakt an der Stelle i, wenn $\text{Kern}(\alpha_i) = \text{Bild}(\alpha_{i-1})$.

Beispiel:

Die beiden Sequenzen

$0 \mapsto \mathbb{Z}/2\mathbb{Z} \mapsto \mathbb{Z}/4\mathbb{Z} \mapsto \mathbb{Z}/2\mathbb{Z} \mapsto 0$ und $0 \mapsto \mathbb{Z}/2\mathbb{Z} \mapsto \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \mapsto 0$

sind exakt.
Die Aufgabe, Gruppen zu klassifizieren, zerlegt sich damit in zwei Teilaufgaben.

1.) Gegeben sind N und G/N. Welche Möglichkeiten gibt es für G?

2.) Welche „unzerlegbaren“ Gruppen gibt es?

Definition 1.27:

Sei G eine Gruppe:

a.) G heißt **einfach**, wenn G nur die trivialen Normalteiler G und $\{e\}$ besitzt.

b.) Eine Reihe der Form $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{e\}$ (für ein $n \in \mathbb{N}$) heißt **Normalreihe**, wenn G_{i+1} „Normalteiler“ in G_i ist und $G_{i+1} \neq G_i$ für $i = 0, \ldots, n-1$.

c.) Eine Normalreihe heißt **Kompositionsreihe**, wenn sie sich nicht verfeinern lässt, das heißt, wenn G_i/G_{i+1} einfach ist für $i = 0, \ldots, n-1$, also keine echten Normalteiler enthält.

Bemerkung 1.28:

a.) $\mathbb{Z}/n\mathbb{Z}$ ist genau dann einfach, wenn n eine Primzahl ist.

b.) $\mathbb{Z}$ besitzt keine Kompositionsreihe.

c.) Eine abelsche Gruppe G ist genau dann einfach, wenn $G \simeq \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p

d.) Jede endliche Gruppe besitzt eine Kompositionsreihe.

e.) Sei G endlich und $(*)$ eine Normalreihe. So gilt:

$$|G| = \prod_{i=1}^{n-1} |G_i/G_{i+1}|$$

Satz 1.29:

Für $n \neq 4$ ist A_n einfach.

Beweis:

Es gilt $|A_4| = 12$. A_4 enthält acht Dreizykel und drei Doppelzweier. A_4 ist auch die Symmetriegruppe des Tetraeders.

i.) Behauptung 1: Jedes $\sigma \in A_n$ ist als Produkt von 3-Zyklen darstellbar, denn $(12)(23) = (123)$ und $(12)(34) = (123)(234)$.

ii.) Behauptung 2: Je zwei 3-Zyklen in A_n sind konjugiert in A_n. Zu zeigen ist, dass (ijk) zu (123) konjugiert ist.

a.) 1.Fall: $(ijk) = (132)$
Sei $\widetilde{p} = (23) = \widetilde{p}^{-1}$. Hieraus folgt $\widetilde{p}^{-1}(132)\widetilde{p} = (123)$. Aber $p \notin A_n$. Rettung: $p = (23)(45)$ und hieraus folgt $p^{-1}(123)p = (123)$.

iii.) Behauptung 3: Enthält N einen „Doppelzweier“, so ist $N = A_n$ (N Normalteiler zu A_n).
Sei $\sigma = (12)(34) \in N$ und $\tau = (12)(35)$. Dann ist $\sigma(\tau\sigma\tau^{-1}) = (345) \in N$, weil $\sigma \in N$ und $\tau\sigma\tau^{-1} \in N$.

iv.) Behauptung 4: N enthält einen 3-Zyklus oder einen Doppelzweier.
Es genügt zu zeigen, dass N ein $\sigma \neq \mathrm{id}$ enthält mit $\sigma(i) \neq i$ für höchstens vier verschiedene $i \in \{1, \ldots, n\}$. Für jedes $\sigma \in A_n$ sei $k_\sigma := \{i \in \{1, \ldots, n\}; \sigma(i) \neq i\}$. Sei $\sigma \in N \setminus \{\mathrm{id}\}$ mit minimalem k_σ. Wir nehmen $k_\sigma \geq 5$ an.

a.) 1.Fall:
σ enthält einen Zyklus der Länge ≥ 3. Sei o.B.d.A. $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(4) \neq 4$, $\sigma(5) \neq 5$. Sei $\alpha := \sigma^{-1}(345)\sigma(354)$. Für alle i mit $\sigma(i) = i$ ist $\alpha(i) = i$ und damit gilt $k_\alpha \leq k_\sigma$. Außerdem ist $\alpha(1) = 1$, woraus $k_\alpha < k_\sigma$ folgt, was ein Widerspruch zu Annahme darstellt.

b.) 2.Fall:
σ ist ein Produkt von disjunkten Transpositionen (mindestens 4). O.B.d.A sei $\sigma = (12)(34)(56)(78)\widetilde{\sigma}$ mit $\widetilde{\sigma} \in A_n$, $\widetilde{\sigma}(i) = i$ für $i = 1, \ldots, 8$. $\alpha = \sigma^{-1}(345)\sigma(354)$ erfüllt $\alpha(i) = i$ und $\alpha(1) = 1$, woraus auch $k_\alpha < k_\sigma$ folgt, was wieder ein Widerspruch darstellt.

Damit ist der Satz bewiesen. □

Satz 6 (Jordan-Hölder):

Sei G eine Gruppe und $G = G_0 \rhd G_1 \rhd \ldots \rhd G_m = \{1\}$, $G = H_0 \rhd H_1 \rhd \ldots \rhd H_l = \{1\}$ Kompositionsreihen für G. Dann ist $m = l$ und es gibt Permutationen $\sigma \in S_m$ mit $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$, wobei $i = 0, \ldots, m-1$.

Beweis:

Wir führen eine vollständige Induktion über m durch.

- $m = 1$: Dann ist G einfach, also auch $l = 1$.
- $m > 1$: Sei $\overline{G} := G/G_1$ und π: $G \mapsto \overline{G}$ die Restklassenabbildung. Hieraus folgt, dass $\overline{H}_i = \pi(H_i)$ Normalteiler in $\overline{H}_{i-1}$ ist. (Sei $\overline{h}_i \in \overline{H}$, $\overline{g} \in \overline{H}_{i-1}$, woraus $\overline{g}\overline{h}_i\overline{g}^{-1} = \pi(gh_ig^{-1}) \in \overline{H}_i$ folgt, da $gh_ig^{-1} \in H_i$ ist. Nach Voraussetzung ist $\overline{G}$ einfach. Damit gibt es ein $j \in \{0, \ldots, l-1\}$ mit $\overline{H}_0 = \ldots = \overline{H}_j = \overline{G}$, $\overline{H}_{j+1} = \ldots = \overline{H}_l = \{1\}$. Sei $G := H_i \cap G_1$. Behauptung:

  $G_1 = C_0 \rhd C_1 \rhd \ldots \rhd C_j \rhd C_{j+2} \rhd \ldots \rhd C_l = \{1\}$

  ist Kompositionsreihe für G_1. Daraus folgt, dass auch

  $G_1 \rhd G_2 \rhd \ldots \rhd G_m = \{1\}$

  Kompositionsreihe ist. Nach Induktionsvoraussetzung folgt dann $m - 1 = l - 1$ und dass es eine Permutation $\sigma := \{1, \ldots, m\} \mapsto \{0, \ldots, j, j+2, \ldots, l\}$ gibt mit $C_{i-1}/C_i \simeq G_{\sigma(i)-1}/G_{\sigma(i)}$ für $i \neq j+1$ und $C_j/C_{j+2} \simeq G_{\sigma(j=)}/G_{\sigma(j)+1}$. Behauptung 2:

  a.) $C_j = C_{j+1}$
  b.) $C_{i-1}/C_i \simeq H_{i-1}/H_i$ für $i \neq j+1$
  c.) $H_j/H_{j+1} \simeq G/G_1 = \overline{G}$

  Die erste Behauptung folgt aus der zweiten: C_i ist Normalteiler in C_{i-1} für $i = 1, \ldots, l$. Aus $x \in C_i = H_i \cap G_1$ und $y \in H_r \cap G_1$ folgt, dass $y \times y^{-1} \in H_1 \cap G_1$. C_{j+2} ist Normalteiler in C_j wegen Behauptung 2a). C_{i+1}/C_i ist wegen 2b) einfach und $\neq \{1\}$ für $i \neq j+1$. Zu zeigen bleibt nun noch Behauptung 2.

  a.) $\overline{H}_{j+1} = \{1\}$ nach Definition von H_j
  Das heißt, dass $H_{j+1} \subseteq G_1$, woraus $C_{j+1} = H_{j+1}$ folgt. Nach Definition ist $C_j = H_j \cap G_1$ Normalteiler in H_j (weil G_1 Normalteiler von G ist). Da $\overline{H}_j \neq \{1\}$, ist $C_j \neq H_j$, also ist $H_{j+1} \trianglelefteq C_j \not\trianglelefteq H_j$. Da H_j/H_{j+1} einfach ist, ist $C_j = H_{j+1} = C_{j+1}$.
  b.) Für $i \geq j+1$ ist $\overline{H}_i = \{1\}$, also $H_i \subseteq G_1$ und damit $C_i = H_i$. Für $i \leq j$ ist $\overline{H}_i = \overline{G} = G/G_1$. Hieraus folgt $H_i \cdot G_1 = G_1 \cdot H_i = G$. Nach dem Isomorphiesatz gilt:

  $C_{i-1}/C_i = C_{i-1}/(H_i \cap C_{i-1}) \simeq C_{i-1} \cdot H_i/H_i$

  Zu zeigen ist also nun, dass $C_{i-1}H_i = H_{i-1}$ ist. Dass das Produkt enthalten ist, ist klar, weil $H_i \subseteq H_{i-1}$. Da $G_i \cdot H_i = G$ ist, gibt es zu $x \in H_{i-1}$ ein $h \in H_i$ und ein $g \in G_1$ mit $x = g \cdot h$ und damit $g = xh^{-1} \in H_{i-1} \cap G_1 = C_{i-1}$.
  c.) Aus $H_{j+1} \subseteq G_1$ folgt, dass

  $H_j/H_{j+1} = H_j/C_{j+1} \underset{a.)}{=} H_j/C_j = H_j/H_j \cap G_1 \simeq H_j \cdot G_1/G_1 = G/G_1$

Definition und Bemerkung 1.30:

a.) Eine Gruppe G heißt **auflösbar**, wenn sie eine Normalreihe mit abelschen Faktorgruppen besitzt.

b.) Eine endliche Gruppe ist genau dann auflösbar, wenn die Faktoren in ihrer Kompositionsreihe zyklisch von Primzahlordnung sind.

c.) Sei $1 \mapsto G' \mapsto G \mapsto G'' \mapsto 1$ kurze exakte Sequenz von Gruppen. Dann ist G genau dann auflösbar, wenn G' und G'' auflösbar sind.

Kapitel 2

Ringe

2.1 Grundlegende Definitionen und Eigenschaften

Definition und Bemerkung 2.1:

a.) Ein **Ring** ist eine Menge R mit Verknüpfung $+$ und $\cdot$, so dass folgendes gilt:

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

ii.) $(R, \cdot)$ ist eine Halbgruppe (nur Assoziativität).

iii.) Die Distributivgesetze gelten:

$x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y\, z \in R$

b.) R heißt **Ring mit Eins**, wenn $(R, \cdot)$ Monoid ist, wenn also ein neutrales Element bezüglich der Multiplikation existiert. (Beispielsweise bilden die durch sieben teilbaren Zahlen einen Ring ohne Eins.)

c.) R heißt **kommutativer Ring**, wenn $(R, \cdot)$ kommutativ ist.

d.) R heißt **Schiefkörper**, wenn $R^\times = R \setminus \{0\}$; das heißt, wenn jedes $x \in R \setminus \{0\}$ invertierbar ist bezüglich der Multiplikation.

e.) Ein kommutativer Schiefkörper heißt **Körper**.

f.) In jedem Ring gilt $x \cdot 0 = 0 = 0 \cdot x$, $x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$ und $(-x) \cdot (-y) = x \cdot y$ für alle $x, y \in R$.

Beweis:

f.) Wir verwenden die geforderten Rechengesetze:

$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 \Leftrightarrow 0 = x \cdot 0$ durch Subtraktion von $x \cdot 0$ auf beiden Seiten

Analog funktioniert dies für $0 \cdot x$. Darüberhinaus gilt:

$x \cdot (-y) + x \cdot y = x \cdot (-y + y) = x \cdot 0 = 0 \Leftrightarrow x \cdot (-y) = -(x \cdot y)$

$(-x) \cdot (-y) = -((-x) \cdot y) = -(-(x \cdot y)) = x \cdot y$

Dies folgt also zwangsläufig aus dem Distributivgesetz. □

g.) Ist R ein Ring mit Eins und $R \neq \{0\}$, so ist $0 \neq 1$ in R.

g.) Wäre $0 = 1$, so gilt für jedes $x \in R$: $x = x \cdot 1 = x \cdot 0 = 0$. Damit wäre jedes Ringelement x das Nullement, also wäre R der Nullring $R = \{0\}$. □

Beispiel:

Betrachten wir den Schiefkörper der HAMILTON-Quaternionen:

$H = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : \ a, b, c, d \in \mathbb{R}\}$

mit komponentenweiser Addition und folgender Multiplikation $\mathbf{i}^2 = -1 = \mathbf{j}^2 = \mathbf{k}^2$ mit $\mathbf{ij} = k = -\mathbf{ji}$. Außerdem sollen $\mathbf{i}$, $\mathbf{j}$ und $\mathbf{k}$ mit den reellen Zahlen a, b, c und d kommutieren. Beispielsweise ist dann

$\mathbf{i} \cdot \mathbf{k} = \mathbf{i} \cdot \mathbf{i} \cdot \mathbf{j} = -\mathbf{j}$ bzw. $\mathbf{k} \cdot \mathbf{j} = \mathbf{i} \cdot \mathbf{j} \cdot \mathbf{j} = -\mathbf{i}$

Wie lautet das inverse Element? Dies erhalten wir durch folgenden Ansatz:

$$\begin{aligned}(a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}) \cdot (a - b \cdot \mathbf{i} - c \cdot \mathbf{j} - d \cdot \mathbf{k}) = \\ = a^2 - ab \cdot \mathbf{i} - ac \cdot \mathbf{j} - ad \cdot \mathbf{k} + ba \cdot \mathbf{i} - b^2\mathbf{i}^2 - bc \cdot \mathbf{ij} - bd \cdot \mathbf{ik} - cb \cdot \mathbf{ji} - c^2 \cdot \mathbf{j}^2 + \ldots = \\ = a^2 + b^2 + c^2 + d^2\end{aligned}$$

Damit ist das inverse Element gegeben durch:

$$\boxed{(a + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k})^{-1} = \frac{a - b \cdot \mathbf{i} - c \cdot \mathbf{j} - d \cdot \mathbf{k}}{a^2 + b^2 + c^2 + d^2} \text{ falls nicht } a = b = c = d = 0}$$

Wegen $\mathbf{ij} = -\mathbf{ji}$ bilden die HAMILTON-Quaternionen jedoch keinen Körper.

Definition 2.2:

Sei $(R, +, \cdot)$ ein Ring.

a.) $R' \subseteq R$ heißt **Unterring**, wenn $(R', +, \cdot)$ selbst Ring ist. Umgekehrt heißt R dann **Ringerweiterung** (oder Erweiterungsring) von R'.

b.) $I \subseteq R$ heißt zweiseitiges **Ideal**, wenn $(I, +)$ Untergruppe von $(R, +)$ ist und $r \cdot x \in I$ und ebenso $x \cdot r \in I$ für alle $x \in I$, $r \in R$. (Beispiel: Damit sind Unterrringe von $\mathbb{Z}$, beispielsweise durch sieben teilbare Zahlen, Ideale von $\mathbb{Z}$.)

c.) $x \in R$ heißt Links- (bzw. Rechts-)Nullteiler, wenn es ein $y \in R \setminus \{0\}$ gibt mit $x \cdot y = 0$ (bzw. $y \cdot x = 0$). (Nach dieser Definition ist 0 selbst Nullteiler. In machen Büchern wird jedoch die 0 als Nullteiler von vorn herein ausgeschlossen.)

d.) R heißt **nullteilerfrei**, wenn 0 der einzige Nullteiler in R ist. (Das heißt, aus $x \cdot y = 0$ folgt $x = 0$ oder $y = 0$.)

e.) R heißt **Integritätsbereich** (integral [domain]), wenn er nullteilerfrei, kommutativ ist und eine Eins besitzt.

Beispiele:

i.) Quaternionen bilden keinen Integritätsbereich, weil sie nicht kommutativ sind.

ii.) $\mathbb{Z}/6\mathbb{Z}$ ist kein Integrationsbereich, weil nicht nullteilerfrei.

iii.) Der Ring der geraden ganzen Zahlen ist kein Integrationsbereich, weil er kein Einselement besitzt.

Definition und Bemerkung 2.3:

a.) Eine Abbildung φ: $R \mapsto R'$ (wobei R und R' Ringe seien) heißt **Ringhomomorphismus**, wenn φ: $(R, +) \mapsto (R', +)$ Gruppenhomomorphismus und $\varphi(R, \cdot) \mapsto (R', \cdot)$ Halbgruppenhomomorphismus ist. (Gilt $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ und $\varphi(x + y) = \varphi(x) + \varphi(y)$, so gilt auch automatisch das Distributivgesetz.)

b.) Sind R, R' Ringe mit Eins, so heißt ein Ringhomomorphismus φ: $R \mapsto R'$ im Sinne von a.) ein **Homomorphismus von Ringen mit Eins**, wenn $\varphi(1_R) = 1_{R'}$ gilt.

c.) Die Ringe bilden mit Ringhomomorphismen eine Kategorie.

Beispiel: Die Multiplikation mit 2 ist kein Ringhomomorphismus. Es gilt zwar $2(x + y) = 2x + 2y$, aber $2(xy) = 2xy \neq (2x)(2y)$.

d.) Die Ringe mit Eins bilden mit Homomorphismen von Ringen mit Eins eine Kategorie (eine echte Unterkategorie der Ringe.)

e.) $(R,+,\cdot) \mapsto (R,+)$ ist kovarianter Funktor „Ringe $\mapsto$ abelsche Gruppen“.

$$\begin{array}{ccc} (R,+,\cdot) & \longrightarrow & (R,+) \\ \varphi\downarrow & & \downarrow\varphi \\ (R',+,\cdot) & \longrightarrow & (R',+) \end{array}$$

$(R,+,\cdot) \mapsto (R^\times,\cdot)$ ist kovarianter Funktor „Ringe mit Eins $\mapsto$ Gruppen“.

Bemerkung 2.4:

Sei φ: $R \mapsto R'$ ein Ringhomomorphismus. Dann gilt:

a.) Bild(φ) ist Unterring von R'.

b.) Kern(φ) ist Ideal in R. (Es ist Kern(φ) $= \varphi^{-1}(0)$.)

c.) Ist R Schiefkörper und φ Homomorphismus von Ringen mit 1, so ist φ injektiv (oder $R' = \{0\}$).

Beweis 2.24:

b.) Sei $x \in$ Kern(φ) und $r \in R$ beliebig. Hieraus ergibt sich $\varphi(r \cdot x) = \varphi(r) \cdot \varphi(x) = \varphi(r) \cdot 0 = 0$. Damit ist $r \cdot x \in$ Kern(φ).

c.) Sei $x \in R \setminus \{0\}$. Damit gilt $\varphi(x) \cdot \varphi(x^{-1}) = \varphi(1_R) = 1_{R'} \neq 0$ (wenn $R' \neq \{0\}$). Somit ist $\varphi(x) \neq 0$ und Kern(φ) $= \{0\}$, womit φ injektiv ist.

Definition und Bemerkung 2.5:

Sei R ein Ring mit 1.

a.) $\varphi_R : \mathbb{Z} \mapsto R$, $n \mapsto \begin{cases} n \cdot 1 = 1 + \ldots + 1 & \text{für} \quad n \geq 0 \\ -(-n) \cdot 1 & \text{für} \quad n < 0 \end{cases}$ ist Homomorphismus von Ringen mit Eins.

b.) Ist Kern(φ_R) $= n \cdot \mathbb{Z}$ ($n \geq 0$), so heißt n die **Charakteristik** von R: $n = \text{char}(R)$.
Beispiel: Von $\mathbb{Z}/n\mathbb{Z}$ ist $n\mathbb{Z}$ der Kern und damit n Charakteristik.

c.) Ist R nullteilerfrei, so ist char(R) $= 0$ oder char(R) $= p$ für eine Primzahl p.

d.) Bild(φ_R) $\simeq \mathbb{Z}/n\mathbb{Z}$
Ist K (Schief)körper der Charakteristik $p > 0$, so ist Bild(φ_k) $\simeq \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ der kleinste Teilkörper von K. Er heißt **Primkörper**. Ist char(K) $= 0$, so ist der kleinste Teilkörper von K isomorph zu $\mathbb{Q}$.

2.2 Verallgemeinerung des Polynomrings

Definition und Bemerkung 2.13:

Sei R ein kommutativer Ring mit Eins und $(H,\cdot)$ eine Halbgruppe.

a.) $R[H] := \{(a_h)_{h\in H}, a_h \neq 0$ nur für endlich viele $h \in H\}$ ist mit den Verknüpfungen $(a_h)+(b_h) := (a_h+b_h)$ und $(a_h) \cdot (b_h)$ mit $\sum_{h_1 \cdot h_2 = h} a_{h_1} \cdot b_{h_1} = 2$ ein Ring. $R[H]$ heißt Halbgruppenring zu H über R. Schreibe auch $\sum_{h\in H} a_h \cdot h$ für (a_h).

b.) Es ist $R[(\mathbb{N},+)]$ isomorph zu $R[x]$ und $R[(\mathbb{N}^n,+)]$ isomorph zu $R[x_1,\ldots,x_n]$.

c.) $R[H]$ ist kommutativ und hat ein Einselement genau dann, wenn J kommutativ ist und ein Einselement hat.

d.) $(H,\cdot) \mapsto (R[H],\cdot)$, $h \mapsto I_R \cdot h$ ist ein injektiver Halbgruppenisomorphismus.

e.) Ist $(H,\cdot)$ Monoid, dann ist $R \mapsto R[H]$, $r \mapsto r \cdot I_H$ ein injektiver Ringhomomorphismus.

Wir wollen uns nun universelle Eigenschaften des Monoidrings anschauen.

Satz 7:

Sei R ein kommutativer Ring mit Eins und $(H, \dot{})$ ein Monoid. Dann gibt es zu jedem φ: $R \mapsto R'$ von Ringen mit Eins und jedem Monoidhomomorphismus σ: $H \mapsto (R', \cdot)$ genau einem Ringhomomorphismus Φ: $R[H] \mapsto R'$ mit $\Phi|_R = \varphi$ und $\Phi|_H = 0$. Dabei werden R und H wie in 2.)/3d.) bzw e.) in $R[H]$ eingebettet.

Beweis:

Es muss gelten:

$$\Phi\left(\sum_h a_h \cdot h\right) = \sum_k \varphi(a_h) \cdot \sigma(h)$$

Das zeigt die Eindeutigkeit, taugt aber auch als Definition von Φ, was die Existenz zeigt.

Definition und Bemerkung 2.14:

a.) $R[x] := \{(a_i)_{i\in\mathbb{N}} : a_i \in R\}$ ist mit $+$ und $\cdot$ wie ein Polynomring ein kommutativer Ring mit Eins. $R[x]$ heißt **Ring der (formalen) Potenzreihen** über R. Schreibweise:

$$f = \sum_{i=0}^{\infty} a_i x^i \text{ für } f = (a_i)_{i\in\mathbb{N}}$$

b.) Sei $0 \neq f = \sum_{i=0}^{\infty} a_i x^i \in R[x]$. Dann heißt $o(f) := \min\{i \in \mathbb{N} : a_i \neq 0\}$ der Untergrad von f. Es gilt für alle $f, g \in R[x] \setminus \{0\}$:

$o(f+g) \geq \min\{o(f), o(g)\}$ und $o(f \cdot g) \geq o(f) + o(g)$

c.) Ist R Integritätsbereich, so ist $o(f \cdot g) = o(f) \cdot o(g)$ $\forall$ $f, g \in R[x] \setminus \{0\}$ und es gilt:

$$R[x]^\times = \left\{ f = \sum_{i=0}^{\infty} a_i x^i \in R[x] : a_0 \in R^\times \right\}$$

d.) Ist $R = K$ ein Körper, so ist

$$\mathfrak{m} := K[x] \setminus K[x]^\times = \left\{ \sum_i a_i x^i : a_0 = 0 \right\}$$

Ideal in $K[x]$.

Beweis:

c.) „$\subseteq$“: Sei $f = \sum_i a_i x^i \in R[x]^\times$. Dann gibt es $g = \sum_i b_i x^i \in R[x]$ mit $1 = f \cdot g = a_0 \cdot b_0 + (a_1 \cdot b_0 + a_0 \cdot b_1) \cdot x + \ldots$ Hieraus ergibt sich $a_0 b_0 = 1$ und damit $a_0 \in R^\times$.

„$\supseteq$“: Definiere $g = \sum_i b_i x^i$ rekursiv durch $b_0 = a_0^{-1}$ (existiert, da a_0 Einheit ist) und

$$b_i := a_0^{-1} \sum_{k=1}^{i} (-1)^k a_k b_{i-k} \text{ für } i \geq 1$$

Behauptung: Dann ist $f \cdot g = 1$ (Beispiel für $i = 1$: $b_1 = a_0^{-1}(a_1 \cdot b_0)$). □

2.3 Quotienten

Sei R ein kommutativer Ring mit Eins.

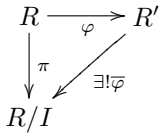
Definition und Satz 2.15:

a.) Sei I Ideal von R. Durch die Verknüpfung $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ wird die Faktorgruppe $(R,+)/(I,+)$ zu einem kommutativen Ring mit Eins. R/I heißt **Faktorring** oder **Quotientenring** von R nach I.

b.) Die Restklassenabbildung $\pi\colon R \mapsto R/I$, $x \mapsto \overline{x}$ ist ein surjektiver Ringhomomorphismus mit $\mathrm{Kern}(\pi) = I$.

c.) Universelle Abbildungseigenschaft des Faktorrings:

Sei $\varphi\colon R \mapsto R'$ ein Ringhomomorphismus. Dann gibt es zu jedem Ideal $I \subseteq R$ mit $I \subseteq \mathrm{Kern}(\varphi)$ einen eindeutig bestimmen Ringhomomorphismus $\overline{\varphi}\colon R/I \mapsto R'$ mit $\varphi = \overline{\varphi} \circ \pi$.



d.) Homomorphiesatz für Ringe:

Ist $\varphi\colon \mapsto R'$ ein surjektiver Ringhomomorphismus, dann ist R' isomorph zu $R/\mathrm{Kern}(\varphi)$.

Beweis:

a.) Wir müssen nachrechnen, dass das Produkt wohldefiniert ist. Es soll also unabhängig von den Vertretern der Klasse sein. Seien x' und $y' \in R$ mit $\overline{x'} = \overline{x}$, $\overline{y'} = \overline{y}$. Dann gibt es $a, b \in I$ mit $x' = x + a$ mit $y' = y + b$. Hieraus folgt $x' \cdot y' = (x+a) \cdot (y+b) = xy + ay + xb + ab$. Da a und $b \in I$, ist auch $ay + xb + ab \in I$. Hieraus folgt $\overline{x'} \cdot \overline{y'} = \overline{x} \cdot \overline{y}$. Die restlichen Eigenschaften vererben sich dann in R.

b.) π ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = I$ nach Satz 1a). Dann ist $\pi(x \cdot y) = \pi(x) \cdot \pi(y)$ nach Definition der Verknüpfung.

c.) Nach Satz 1b) gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\overline{\varphi}\colon R/I \mapsto R'$ mit $\varphi = \overline{\varphi} \circ \pi$. Zeige aber, dass $\overline{\varphi}$ Ringhomomorphismus ist. Für $x, y \in R$ ist $\overline{\varphi}(\overline{x} \cdot \overline{y}) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y})$.

d.) Folgt aus c.) und Satz 1a).

Definition und Bemerkung 2.16:

a.) Ein Ideal $I \subsetneq R$ heißt **maximal**, wenn es kein Ideal I in R gibt mit $I \subsetneq I' \subsetneq R$.

b.) Ein Ideal $I \subsetneq R$ heißt **Primideal**, wenn für $x, y \in R$ mit $x \cdot y \in I$ gilt: $x \in I$ oder $y \in I$.

c.) R ist nullteilerfrei genau dann, wenn (0) Primzahl ist.

d.) Jedes maximale Ideal I ist Primideal.

Beweis:

c.) R ist nicht nullteilerfrei genau dann, wenn $a, b \in R \setminus \{0\}$ existieren, so dass $a \cdot b = 0$. Hieraus folgt, dass (0) kein Primideal ist.

d.) Seien $x, y \in R$ mit $x \cdot y \in I$ und $x \notin I$. Dann ist $(x) + I \supsetneq I$. Da I maximal ist, folgt $(x) + O = R$ und hieraus $I \in (x) + I$. Das heißt, es gibt $r \in R$ und $a \in I$ mit $1 = r \cdot x + a$. Hieraus folgt $y = rxy + ay \in I$ (da $rxy \in I$ und $ay \in I$), womit I ein Primideal ist.

Beispiel:

1.) p ist eine Primzahl genau dann, wenn $p \cdot \mathbb{Z}$ Primideal in $\mathbb{Z}$ (sogar maximal) ist.

2.) (x) ist Primideal in $R[x]$ genau dann wenn R ein Körper ist.

Bemerkung 2.17:

Sei $I \subsetneq R$ ein Ideal. Dann gilt:

a.) I ist Primideal genau dann, wenn R/I nullteilerfrei ist.

b.) I ist maximales Ideal genau dann, wenn R/I Körper ist.

Beweis:

a.) R/I ist nicht nullteilerfrei genau dann, wenn es $\overline{x} \neq \overline{0} \neq \overline{y} \in R/I$ gibt mit $\overline{x} \cdot \overline{y} = \overline{0} = \overline{x \cdot y}$. Dies ist äquivalent dazu, dass $x \cdot y \in I$ für $x, y \notin I$, was auch wieder äquivalent dazu ist, dass I kein Primideal ist.

b.) Nach 2.6d) ist R/I genau dann Körper, wenn (0) und R/I die einzigen Ideale in R/I sind. Nach Blatt 7, A3 entsprechen die Ideale in R/I bijektiv den Idealen in R, die I enthalten.

Beispiel:

Sei $C = \{(a_n)_{n\in\mathbb{N}} : (a_n)$ CAUCHY-Folge$\}$ mit $a_n \in \mathbb{Q}$. (Das heißt, für $k \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$, so dass $|a_i - a_j| < 1/k$ für $i, j \geq n$. C ist Ring mit komponentenweier Addition und Multiplikation (siehe Analysis I).

$$C \subseteq \prod_{n\in\mathbb{N}} \mathbb{Q}$$

$N := \{(a_n) \in C : (a_n)$ Nullfolge$\}$ (das heißt, für $k \in \mathbb{N}$ existiert ein $n \in \mathbb{N}$, so dass $|a_i| < 1/k$ für alle $i \geq n$). N ist Ideal in C.

Behauptung:

C/N ist ein Körper (bzw. N ist maximal).

Beweis:

Sei $a \in C - N$, wobei $a = (a_n)_{n\in\mathbb{N}}$. Zu zeigen ist, dass $1 \in N + (a) = \langle N \cup \{a\}\rangle$. Aus $(a_n) \notin N$ folgt, dass $a_n = 0$ ist nur für endlich viele n. Das heißt, $a_i \neq 0$ für $i > n_0$.

$$b_n := \begin{cases} 0 & \text{für} \quad i < n_0 \\ 1/a_i & \text{für} \quad i \geq n_0 \end{cases} \quad \text{mit } b = (b_n) \in C$$

$$a \cdot b = (c_n) \text{ mit } c_n = \begin{cases} 0 & \text{für} \quad n < n_0 \\ 1 & \text{für} \quad n \geq n_0 \end{cases}$$

Hieraus folgt, dass

$$1 - a \cdot b = (d_n) \text{ mit } d_n = \begin{cases} 1 & \text{für} \quad n < n_0 \\ 0 & \text{für} \quad n \geq n_0 \end{cases} \Rightarrow (d_n) \in N$$

eine Nullfolge ist. Wir haben also die Eins geschrieben als Nullfolge und Vielfaches der Folge a. Somit ist N maximal. $C/N = \mathbb{R}$! (In der Analysis benötigt man zur Konstruktion der reellen Zahlen den Begriff der CAUCHY-Folgen.)

2.3.1 Chinesischer Rest(e)satz

Diesen Satz war chinesischen Astronomen schon vor Jahrtausenden bekannt, woher der Name rührt.

Satz 8:

Sei R ein kommutativer Ring mit Eins und $I_1, \ldots, I_n$ seien Ideale in R mit $I_\nu + I_\mu = R$ für alle $\nu \neq \mu$. (Solche Ideale heißen relativ prim oder auch koprim. Man kann dann die Eins aus ihnen linearkombinieren.) Für $\nu = 1, \ldots, n$ sei p_ν: $R \mapsto R/I_\nu$ die Restklassenabbildung. Dann gilt:

a.) Der Ringhomomorphismus φ: $R \mapsto R/I_1 \times \ldots \times R/I_n$, $x \mapsto (p_1(x), \ldots, p_n(x))$ ist surjektiv.

b.) $R/I_1 \times \ldots \times R/I_n \simeq R/\bigcap_{\nu=1}^{m} I_\nu$

c.) Für paarweise teilerfremde Zahlen $m_1, \ldots, m_n \in \mathbb{Z}$ und beliebige $r_1, \ldots, r_n \in \mathbb{Z}$ gibt es ein $x \in \mathbb{Z}$ mit $x \equiv r_\nu \bmod m_\nu$ für $\nu = 1, \ldots, n$. (Spezialfall von a.) für $R = \mathbb{Z}$)

Beweis:

a.) Es genügt zu zeigen, dass $(0, \ldots, 0, 1, 0, \ldots, 0) \in \text{Bild}(\varphi)$ (mit der 1 an der ν-ten Stelle) ist für jedes ν, also dass es $e_\nu \in R$ ($\nu = 1, \ldots, n$) gibt mit $e_\nu \in I_\mu$ für $\mu \neq \nu$ und $1 - e_\nu = a_\nu \in I_\nu$. (Denn für $x = (\overline{r}_1, \ldots, \overline{r}_n) \in R/I_1 \times \ldots \times R/I_n$ sei $e := \sum_{\nu=1}^{n} r_\nu e_\nu$ mit $r_\nu \in p_\nu^{-1}(\overline{r}_\nu)$. Hieraus folgt $\varphi(e) = \sum_\nu p_\nu(r_\nu e_\nu) = x$.) Nach Voraussetzung gibt es für jedes $\mu \neq \nu$ ein $a_\mu \in I_\nu$ und $b_\mu \in I_\mu$ mit $a_\mu + b_\mu = 1$. Wir multiplizieren alle Einsen:

$$1 = \prod_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} (a_\mu + b_\mu) = \prod_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} b_\mu + a_\nu$$

Dies funktioniert, weil alle anderen Summanden immer ein $a_\nu \in I_\nu$ beinhalten. Da I_ν ein Ideal ist, folgt also $a_\nu \in I_\nu$. Für das Produkt der b_μ gilt:

$$e_\nu := \prod_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} b_\mu \in \bigcap_{\substack{\mu=1 \\ \mu\neq\nu}}^{n} I_\mu$$

Damit ist $1 = e_\nu + a_\nu$ wie gewünscht.

2.3.2 Teilbarkeit

Sei R ein kommutativer Ring mit Eins.

Definition und Bemerkung 2.18:

Seien a, $b \in R$ und $a \neq 0$.

a.) a **teilt** b (Schreibweise: $a|b$) genau dann wenn $b \in (a)$, also in dem von a erzeugten Hauptideal drin ist (Vielfaches von a). (Es existiert ein $x \in R$, so dass $b = a \cdot x$.)

b.) $d \in R$ heißt **größter gemeinsamer Teiler** von a mod b (Schreibweise: $\text{ggT}(a, b)$), wenn gilt:

i.) $d|a$ und $d|b$

ii.) Ist $d' \in R$ auch Teiler von a und b, so gilt $d'|d$ (auch $d \in (d')$).

c.) Ist $d \in R$ ein ggT von a und b und $e \in R^\times$, so ist auch $e \cdot d$ ein ggT. Ist R nullteilerfrei und sind d, d' beide ggT von a und b, so gibt es ein $e \in R^\times$ mit $d' = e \cdot d$.

Beweis:

c.) Nach Definition gibt es x, $y \in R$ mit $d' = x \cdot d$ und $d = y \cdot d'$. Hieraus ergibt sich $d' = x \cdot y \cdot d'$, woraus $d' \cdot (1 - x \cdot y) = 0$ folgt. Aus der Tatsache, dass $d \neq 0$ ist (R nullteilerfrei) ergibt sich $1 = x \cdot y$, also x, $y \in R^\times$.

Definition und Satz 2.19:

a.) Ein Integritätsbereich R heißt **euklidisch**, wenn es eine Abbildung δ: $R \setminus \{0\} \mapsto \mathbb{N}$ gibt mit folgender Eigenschaft: Zu f, $g \in R$ und $g \neq 0$ gibt es a, $r \in R$ mit $f = q \cdot g + r$, wobei $r = 0$ oder $\delta(r) < \delta(g)$.

b.) Sei R euklidisch und a, $b \in R \setminus \{0\}$. Dann gilt:

i.) In R gibt es einen ggT von a und b.

ii.) Es ist $d \in (a, b)$ (Das heißt, es existieren x, $y \in R$ mit $d = x \cdot a + y \cdot b$.)

iii.) $(d) = (a, b)$

c.) Jeder euklidische Ring ist ein Hauptidealring.

Beispiel:

$\mathbb{Z}$ mit $\delta(a) = (a)$, $k[X]$ mit $\delta(f) = \text{grad}(f)$

Beweis:

b.) Ohne Einschränkung sei $\delta(a) \geq \delta(b)$. Nach Voraussetzung gibt es q_1, $r_1 \in R$ mit $a = q_1 \cdot b + r_1$ und $\delta(r_1) < \delta(b)$ oder $r_1 = 0$. Ist $r_1 = 0$, so ist $a \in (b) = (a, b)$ und $\mathrm{ggT}(a, b) = b$. Sonst gibt es q_2, $r_2 \in R$ mit $b = q_2 \cdot r_1 + r_2 R$ mit $r_2 = 0$ oder $\delta(r_2) < \delta(r_1)$. Dies kann man endlich oft fortsetzen, bis man zu $r_i = q_{i+2} r_{i+1} + r_{i+2}$ mit $r_{n-2} = q_n r_{n-1}$ (da $\delta(r_{i+2}) < \delta(r_{i+1})$) kommt. Behauptung: $d = r_{n-1}$ ist ggT von a und b, denn $d | r_{n-2}$. In der vorletzten Zeile steht $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$, woraus $d | r_{n-3}$ folgt. Nach Induktion ist $b | r_i$ für alle i, woraus $d | b$ und $d | a$ folgt. Umgekehrt: Sei d' Teiler von a und b. So folgt $d' | r_1$ und nach Induktion $d' | r_i$ für alle i, also $d' | d$.

ii.) Noch zu zeigen: $d \in (a, b)$. Nach Konstruktion ist $r_{i+2} \in (r_i, r_{i+1}) \subset \ldots \subset (a, b)$ für alle i.

iii.) Es gilt auch die Umkehrung $(d) = (a, b)$. „$\subseteq$“ ist (ii), „$\supseteq$“ $a \in (d)$, $b \in (d)$ nach Definition

c.) Sei $I \subset R$ Ideal und $I \neq \{0\}$. Wähle $a \in I$ mit $\delta(a)$ minimal. Dann gilt für jedes $b \in I$, dass es ein Vielfaches von a sein muss, also $b = q \cdot a + r$ mit $r \in I$ und $\delta(r) < \delta(a)$. Dies stellt ein Widerspruch dar, womit $r = 0$ ist. Damit folgt $I = (a)$.

Definition und Bemerkung 2.20:

Sei R kommutativer Ring mit Eins.

a.) $x, y \in R$ heißen **assoziiert**, wenn es ein $e \in R^\times$ gibt mit $y = x \cdot e$. „assoziiert“ ist eine Äquivalenzrelation.

b.) $x \in R \setminus R^\times$ heißt **irreduzibel**, wenn aus $x = y_1 \cdot y_2$ mit y_1, $y_2 \in R$ folgt, dass $y_1 \in R^\times$ oder $y_2 \in R^\times$.

c.) $x \in R \setminus R^\times$ heißt **prim** (oder **Primelement**), wenn (x) ein Primideal ist. Das heißt: Aus $x | y_1 \cdot y_2$ folgt $x | y_1$ oder $x | y_2$.

d.) Sind $x, y \in R \setminus R^\times$ assoziiert, so ist x genau dann irreduzibel (bzw. prim), wenn y irreduzibel (prim) ist.

e.) Ist R nullteilerfrei, so ist jedes Primelement $\neq 0$ irreduzibel.

Beweis:

e.) Sei (x) Primideal und $x = y_1 \cdot y_2$ mit y_1, $y_2 \in R$. Ohne Einschränkung ist $y_1 \in (x)$, also $y_1 = x \cdot a$ für ein $a \in R$. Damit ergibt sich $x = x \cdot a \cdot y_2$, also $x(1 - a y_2) = 0$. Daraus folgt, weil R nullteilerfrei ist und mit $x \neq 0$, dass $a y_2 = 1$ ist. □

Beispiel:

Die Umkehrung stimmt nicht! Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\}$.

$2 \cdot 3 = 6 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right) \subset \mathbb{C}$

Dabei ist die Multiplikation folgendermaßen definiert:

$\left(a + b\sqrt{-5}\right) \cdot \left(c + d\sqrt{-5}\right) = ac - 5bd + (ad + bc)\sqrt{-5}$

In R ist 2 kein Primelement, denn weder $1 + \sqrt{-5}$ noch $1 - \sqrt{-5}$ ist durch 2 teilbar. Aber 2 ist irreduzibel. Dies überprüfen wir damit, ob sich 2 als Produkt wie folgt darstellen lässt: $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$.

$4 = |2|^2 = (a + b\sqrt{-5}) \cdot (a - b\sqrt{-5}) \cdot (c + d\sqrt{-5}) \cdot (c - d\sqrt{-5}) = (a^2 + 5b^2) \cdot (c^2 + 5d^2) = a^2 \cdot c^2 + 5P$ mit $P \geq 0$

Hieraus ergibt sich $P = 0$, was nur mit $b = d = 0$ zu erfüllen ist. Somit ist nur die Wahl $a^2 = 1$ und $c^2 = 4$ möglich. 2 ist also irreduzibel aber kein Primelement in diesem Ring!

Proposition und Definition 2.21:

Sei R ein Integritätsbereich.

a.) Folgende Eigenschaften sind äquivalent.

i.) Jedes $x \in R \setminus \{0\}$ lässt sich eindeutig als Produkt von Primidealen schreiben.

ii.) Jedes $x \in R \setminus \{0\}$ lässt sich irgendwie als Produkt von Primidealen schreiben.

iii.) Jedes $x \in R \setminus \{0\}$ lässt sich eindeutig als Produkt von irreduziblen Elementen schreiben.

b.) Sind die drei Eigenschaften aus a.) für R erfüllt, so heißt R **faktorieller** Ring (oder ZPE-Ring, englisch UFD (unique factorization domain)).

Dabei ist in a.) „eindeutig“ gemeint bis auf Reihenfolge und Multiplikation mit Einheiten. Präziser: Sei $\mathfrak{P}$ ein System der Primelemente ($\neq 0$) bezüglich „assoziiert“. Dann heißt i.): Für alle $x \in R \setminus \{0\}$ $\exists!$ $e \in R^\times$ und für jedes $p \in \mathfrak{P}$ ein $\nu_p(x) \geq 0$:

$$x = e \cdot \prod_{p \in \mathfrak{P}} p^{\nu_p(x)}$$

(Beachte: Es ist $\nu_p(x) \neq 0$ nur für endlich viele p.)

Beweis:

Aus i.) folgt ii.), denn wenn die Zerlegung eindeutig ist, dann ist jedes $x \in R \setminus \{0\}$ auf jeden Fall irgendwie zerlegbar. Wir zeigen, dass ii.) aus iii.) folgt. Sei $x \neq 0$, $x = e \cdot p_1 \cdot \ldots \cdot p_r$ mit $p_i \in \mathfrak{P}$ und $e \in R^\times$. Sei weiter $x = q_1 \cdot \ldots \cdot q_s$ mit irreduziblen Elementen q_j. Es ist x insbesondere ein Vielfaches von p_1 also im von p_1 erzeugten Hauptideal drin: $x \in (p_1)$. Hieraus folgt, dass ein j existiert mit $q_j \in (p_1)$. Ohne Einschränkung nehmen wir $j = 1$ an. Das heißt, wir können schreiben $q_1 = \varepsilon_1 q_1$ mit $\varepsilon_1 \in R^\times$ (da q_1 irreduzibel ist). Analog zu vorher folgt daraus, dass R nullteilerfrei ist:

$$\varepsilon_1 \cdot q_2 \cdot \ldots \cdot q_s = e \cdot p_2 \cdot \ldots \cdot p_r$$

Mit Induktion über r folgt die Behauptung. Aus iii.) folgt dann i.). Noch zu zeigen ist, dass jedes irreduzible Element in R prim ist. Sei $p \in R \setminus R^\times$ irreduzibel. Sei $x, y \in R$ mit $x \cdot y \in (p)$, also $x \cdot y = p \cdot a$ für ein $a \in R$. Schreibe $x = p_1 \cdot \ldots \cdot q_m$ und $y = s_1 \cdot \ldots \cdot s_m$ und $a = p_1 \cdot \ldots \cdot p_l$ mit irreduziblen Elementen q_i, s_j und p_k. Setzen wir diese Zerlegungen ein, so folgt:

$$x \cdot y = q_1 \cdot \ldots \cdot q_m \cdot s_1 \cdot \ldots \cdot s_n = p \cdot a = p \cdot p_1 \cdot \ldots \cdot p_l$$

Wegen der Eindeutigkeit folgt $p \in \{q_1, \ldots, q_m, s_1, \ldots, s_n\}$ (bis auf Einheit). Somit ist $x \in (p)$ oder $y \in (p)$. □

Bemerkung 2.22:

Ist R ein faktorieller Ring, so gibt es zu allen a, $b \in R \setminus \{0\}$ einen ggT(a,b).

Beweis:

Sei $\mathfrak{P}$ wie in 2.21 ein Vertretersystem der Primelemente

$$a = e_1 \cdot \prod_{p \in \mathfrak{P}} p^{\nu_p(a)} \text{ und } b = e_2 \cdot \prod_{p \in \mathfrak{P}} p^{\nu_p(b)}$$

Es ist

$$d := \prod_{p \in \mathfrak{P}} p^{\nu_p(d)} \text{ mit } \nu_p(d) = \min(\nu_p(a), \nu_p(b))$$

der ggT von a und b (Primfaktorzerlegung!).

Satz 9:

Jeder nullteilerfreie Hauptidealring ist faktoriell.

Beweis:

a.) 1.Schritt: Jedes $x \in R \setminus \{0\}$ lässt sich als Produkt von irreduziblen Elementen schreiben.

$x \in R \setminus \{0\}$ heiße Störenfried, wenn x nicht als Produkt von irreduziblen Elementen darstellbar ist. Sei x Störenfried. Dann ist $x \notin R^\times$ und x nicht irreduzibel, also $x = x_1 \cdot y_1$ mit x_1, $y_1 \in R^\times$. Ohne Einschränkung ist x_1 Störenfried (sonst ist x doch Produkt von irreduziblen). Also ist $x_1 = x_2 \cdot y_2$ mit x_2, $y_2 \in R^\times$. Sei ohne Einschränkung x_2 Störenfried. Induktiv erhalten wir x, x_1, x_2, ... Dies sind alle Störenfriede mit $(x) \subsetneqq (x_1) \subsetneqq (x_2) \subsetneqq \ldots \subsetneqq (x_i) \subsetneqq (x_{i+1})$. Sei nun $I = \bigcup_{i \geq 1}(x_i)$. I ist ein Ideal. Damit gibt es ein $a \in R$ mit $I = (a)$. Damit existiert ein i mit $a \in (x_i)$ und somit $x_j \in (x_i)$ für alle $j \geq i$, was ein Widerspruch darstellt, denn die Ideale sollten nach Annahme echt wachsen. □

b.) 2.Schritt: Jedes irreduzible $x \in R \setminus \{0\}$ erzeugt ein maximales Ideal.

Sei $p \in R \setminus \{0\}$ irreduzibel und I Ideal in R mit $(p) \subseteq I \subsetneq R$. Nach Voraussetzung gibt es $a \in R$ mit $I = (a)$, wobei $a \notin \mathbb{R}^x$, da $I \neq R$. Da $p \in (p) \subseteq I = (a)$, gibt es ein $\varepsilon \in R$ mit $p = a \cdot \varepsilon$. Da p irreduzibel ist, folgt $\varepsilon \in R^\times$. Damit ist $(p) = (a) = I$.

Mit 2.21 a (ii) folgt dann die Behauptung.
Erinnerung: EISTENSTEINkriterium

$$f = \sum_{i=0}^{n} a_i X^i \in R[x]$$

Sei R faktoriell und $a_n \neq 0$. Sei $p \in R$ Primelement mit $p \nmid a_n$, $p | a_i$ für $i = 0, \ldots, n-1$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

Beispiel 2.27:

Sei $f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X]$ und p eine Primzahl. Behauptung: f ist irreduzibel. Laut Beobachtung ist $f(X) = (X^p - 1)/(X - 1)$. f heißt „p-tes Kreisteilungspolynom“. Wir machen nun folgenden Trick und zwar betrachten wir das Polynom $g(X) := f(X + 1)$. $g(X)$ ist genau dann irreduzibel, wenn $f(X)$ irreduzibel ist.

$$g(X) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$$

Der Polynomgrad ist $n = p - 1$. Wir lesen ab:

$$a_{p-1} = \binom{p}{p} = 1 \text{ und } a_0 = \binom{p}{1} = p$$

Es ist nun noch zu überlegen, dass $\binom{p}{k}$ durch p teilbar ist für $k = 2, \ldots, p-1$. Bekannt ist:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Dies ist auf jeden Fall durch p teilbar! Mit dem EISENSTEIN-Kriterium folgt damit die Behauptung.

Proposition 2.28:

Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $\overline{R} := R/(p)$.

a.) Wir können auf zweierlei Arten Polynome reduzieren: $\overline{R}[X] \simeq R[X]/p \cdot R[X]$

b.) Sei $f \in R[X]$ primitiv und $p \nmid a_n$.

$$f = \sum_{i=1}^{n} a_i X^i \text{ für } a_n \neq 0$$

Ist $\overline{f} \in \overline{R}[X]$ irreduzibel, so ist f irreduzibel in $R[X]$.

Beweis:

a.) $R \mapsto \overline{R}$ induziert den Homomorphismus φ: $R[X] \mapsto \overline{R}[X]$. Offensichtlich ist φ surjektiv.

$$\text{Kern}(\varphi) = \left\{ f \in \sum_{i=0}^{n} a_i X^i : p | a_i \text{ für } i = 0, \ldots, n \right\} = p \cdot R[X]$$

Mit dem Homomorphiesatz folgt die Behauptung.

b.) Sei $f = g \cdot h$ und hieraus folgt $\overline{f} = \overline{g} \cdot \overline{h}$. Schreibe h in der Form $h = \sum_{i=0}^{s} c_i X^i$. Also ist ohne Einschränkung $\overline{h} \in (\overline{R}[X])^\times = R^\times$ und damit gilt $p | c_i$ für $i = 1, \ldots, s$. Für $s \geq 1$ wäre c_s durch p teilbar, also auch $b_r c_s = a_n$. Dies stellt ein Widerspruch dar.

Beispiel:

Wir betrachten $f = X^2 - 5 \in \mathbb{Z}[X]$.

- $p = 2$: $\overline{f} = X^2 - 1 = (X-1)^2$
- $p = 5$: $\overline{f} = X^2$
- $p = 3$: $\overline{f} = X^2 + 1 \in \mathbb{F}_3[X]$ ist irreduzibel.

Satz 11 (Gauß):

Ist R ein faktorieller Ring, so ist $R[X]$ faktoriell.

Beweis:

Sei $K := \mathrm{Quot}(R)$. Dann ist $K[X]$ faktoriell (weil Hauptidealring). Sei $R[X] \subseteq K[X]$ Unterring. $0 \neq f \in R[X]$ lässt sich als Produkt von Primelementen in $K[X]$ schreiben. Zu zeigen ist also, dass die Faktoren in $R[X]$ liegen und dort prim sind. Dazu müssen wir zuerst Vorarbeit leisten:

Bemerkung 2.29:

Für jedes Primelement $p \in R$ und alle $f, g \in K[X]$ gilt $\nu_p(fg) = \nu_p(f) + \nu_p(g)$. Wähle dabei ein System $\mathcal{P}$ von Vertretern der Primelemente. Zerlege $x \in R$ als $x = e \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$. Beachte, dass $\nu_p(x \cdot y) = \nu_p(x) + \nu_p(y)$ gilt. Für $f = \sum_{i=1}^n a_i X^i$ ist $\nu_p(f) = \min_{i=0,\ldots,n} \nu_p(a_i)$. Für $x = a/b \in K$ sei $\nu_p(x) = \nu_p(a) - \nu_p(b) \in \mathbb{Z}$.

Beweis der Bemerkung 2.29:

a.) 1.Schritt: Sei $\mathrm{Grad}(f) = 0$, also $f = a_0 \in K$ und $g = \sum_{i=0}^n b_i X^i$. Hieraus folgt:

$$f \cdot g = \sum_{i=0}^{n} a_0 b_i \cdot X^i \Rightarrow \nu_p(f \cdot g) = \min_{i=0,\ldots,n} \nu_p(a_0 b_i) = \min_{i=0,\ldots,n} (\nu_p(a_0) + \nu_p(b_i)) =$$
$$= \nu_p(a_0) + \min_{i=0,\ldots,n} \nu_p(b_i) = \nu_p(f) + \nu_p(g)$$

b.) 2.Schritt: Wir dürfen annehmen, dass $f, g \in R[X]$ primitiv sind. Denn wähle $a \in R$ mit $a \cdot f \in R[X]$ („Hauptnenner“). Sei d ein ggT der Koeffizienten von $a \cdot f$. Damit ist $a \cdot f = a/d \cdot f \in R[X]$ primitiv. Seien also $a \cdot f$ und $b \cdot g$ primitiv ($a, b \in K \setminus \{0\}$ geeignet). Es gelte $\nu_p(a \cdot f \cdot b \cdot g) = \nu_p(af) + \nu_p(bg)$. Dann ist nach Schritt 1:

$$\nu_p(a \cdot f \cdot b \cdot g) = \nu_p(a \cdot b) + \nu_p(f \cdot g) = \nu_p(a \cdot f) + \nu_p(b \cdot g) = \nu_p(a) + \nu_p(f) + \nu_p(b) + \nu_p(g)$$

Also folgt $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$.

c.) 3.Schritt: Für primitive $f, g \in R[X]$ gilt $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$. (Sei $f = \sum_i a_i X^i$, $g = \sum_j b_j X^j$ und $f \cdot g = \sum_k c_k X^k$.) Sei weiterhin $p \in \mathcal{P}$, $\overline{R} = R/(p)$. Hieraus folgt $\overline{f} \neq 0 \neq \overline{g}$ in $\overline{R}[X]$, weil f und g primitiv sind. Hieraus folgt $\overline{f} \cdot \overline{g} \neq 0$, da $\overline{R}[X]$ nullteilerfrei ist und außerdem $\nu_p(f \cdot g) = 0$. Aus der Tatsache, dass f und g primitiv sind, ergibt sich $\nu_p(f) = \nu_p(g) = 0$.

Sei $\widetilde{\mathcal{P}}$ Vertretersystem der Primelemente in $K[X]$. Alle $f \in \widetilde{\mathcal{P}}$ seien in $R[X]$ und primitiv. Sei nun $f \in R[X]$ und $f \neq 0$. Schreibe $f = c \cdot f_1 \cdot \ldots \cdot f_n$ mit $f_i \in \widetilde{P}$ (und $c \in K^\times$). Beobachtung: Es ist $c \in R$, denn für $p \in \mathcal{P}$ ist $0 \leq \nu_p(f) = \nu_p(c) + \sum_{i=1}^n \nu_p(f_i) = \nu_p(c)$. Somit ist $c \in R$. Schreibe also $c = e \cdot p_1 \cdot \ldots \cdot p_m$ mit $e \in R^\times$ und $p_i \in \mathcal{P}$. Es bleibt nun noch zu zeigen, dass

1.) $p_i \in R[X]$ prim ist und

2.) dass f_i prim in $R[X]$ ist.

Beweisen wir zuerst (1). Zeige, dass $R[X]/(p_i)$ nullteilerfrei ist. Dies folgt daraus, dass $R[X] = R[X]/p_i \cdot R[X] \simeq (R/p_i \cdot R)[X]$ gilt und $R/p_i \cdot R$ selbst nullteilerfrei ist. Kommen wir nun zu Punkt (2). Sei $g, h \in R[X]$ mit $g, h \in f_i \cdot R[X] = (f_i)$. Da f_i Primelement in $K[X]$ ist, muss einer der Faktoren, also zum Beispiel g in $f_i \cdot K[X]$ liegen, also $g = f_i \cdot \widetilde{g}$ für ein $\widetilde{g} \in K[X]$. Für jedes $p \in \mathcal{P}$ ist dann $0 \leq \nu_p(g) = \nu_p(f_i) + \nu_p(\widetilde{g}) = \nu_p(\widetilde{g})$, da $\nu_p(f_i) = 0$. Somit ist $\widetilde{g} \in R[X]$ und f_i prim in $R[X]$.

2.3.3 Moduln

Sei R ein kommutativer Ring mit Eins.

Definition und Bemerkung 2.30:

a.) Eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung $\cdot: R \times M \mapsto M$ heißt **R-Modul**, wenn gilt:

i.) $a \cdot (x+y) = a \cdot x + a \cdot y$

ii.) $(a+b) \cdot x = a \cdot x + b \cdot x$

iii.) $(a \cdot b) \cdot x = a \cdot (b \cdot x)$

iv.) $1 \cdot x = x$

b.) Eine Abbildung φ: $M \mapsto M'$ von R-Moduln heißt **R-Modulhomomorphismus** (oder R-linear), wenn φ Gruppenhomomorphismus ist für alle $x \in M$, $a \in R$ gilt: $\varphi(a \cdot x) = a \cdot \varphi(x)$.

c.) Lineare Abbildung kann man punktweise addieren und skalar multiplizieren. $\mathrm{Hom}_R(M, M') := \{\varphi : M \mapsto M' | \varphi \ R\text{-linear}\}$ ist R-Modul durch $(\varphi_1 + \varphi_2)(x) := \varphi_1(x) + \varphi_2(x)$ und $(a \cdot \varphi)(x) := a \cdot \varphi(x)$.

d.) Die R-Moduln bilden mit den R-linearen Abbildungen eine Kategorie **R-Mod**. (Identität linear und Komposition von linearen Abbildungen wieder linear.)

e.) Die Kategorien **$\mathbb{Z}$-Mod** und **abelsche Gruppen** sind isomorph. Denn ein $\mathbb{Z}$-Modul-Homomorphismus ist nach Definition auch ein Gruppenhomomorphismus. Die Umkehrung gilt auch, denn $\varphi(n \cdot x) = \varphi(x + \ldots + x) = \varphi(x) + \ldots + \varphi(x) = n \cdot \varphi(x)$ für φ: $A \mapsto A'$ Gruppenhomomorphismus, $x \in A$ und $n \in \mathbb{N}$. Damit ist jeder Gruppenhomomorphismus von abelschen Gruppen $\mathbb{Z}$-linear.

Beispiele:

1.) Man kann jeden Ring als Modul über sich selbst auffassen, so wie man jeden Körper als eindimensionalen Vektorraum über sich selbst auffassen kann. R ist also R-Modul (mit $\cdot$ als Ringmultiplikation).

2.) Ist R ein Körper, so ist der R-Modul gleich dem R-Vektorraum.

3.) Für $R = \mathbb{Z}$ kann man $M = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ als $\mathbb{Z}$-Modul auffassen durch $n \cdot \overline{0} = \overline{0}$, $n \cdot \overline{1} = \overline{n}$. Jede abelsche Gruppe A ist $\mathbb{Z}$-Modul durch $n \cdot x = x + \ldots + x$ (n mal) für $n \in \mathbb{N}$, $x \in A$.

4.) Jedes Ideal in R ist ein R-Modul (aber nicht jeder Unterring).

Definition und Bemerkung 2.31:

Sei M ein R-Modul.

a.) Eine Untergruppe U von $(M,+)$ heißt Untermodul von M, wenn $R \cdot U \subseteq U$ ist. (Das heißt, U ist selbst R-Modul.)

b.) Ist φ: $M \mapsto M'$ R-linear, so sind Kern(φ) und Bild(φ) Untermoduln von M bzw. M'. (Denn aus $\varphi(x) = 0$ folgt $\varphi(a \cdot x) = 0$, da $\varphi(a \cdot x) = a\varphi(x)$ ist. Außerdem folgt aus $a \cdot \varphi(x) = \varphi(a \cdot x)$.)

c.) Sei $U \subseteq M$ Untermodul. Dann wird M/U zu einem R-Modul durch $a \cdot \overline{x} := \overline{a \cdot x}$ mit $\overline{x} = M/U$ und $a \in R$. (Wir müssen uns überlegen, dass dies wohldefiniert ist. Ist $x' \in \overline{x}$, also $x - x' \in U$, so ist $a \cdot x' - a \cdot x = a \cdot (x' - x) \in U$. Damit definieren $a \cdot x'$ und $a \cdot x$ dasselbe Element in M/U.) Die Restklassenabbildung p: $M \mapsto M/U$, $x \mapsto \overline{x}$ ist dann R-linear. (Denn es gilt $p(a \cdot x) = \overline{a \cdot x} = a \cdot \overline{x} = a \cdot p(x)$.) Dies ist nur eine andere Formulierung der Eigenschaft, dass die Faktorgruppe zum R-Modul wird.

Definition und Bemerkung 2.32:

Sei M ein R-Modul.

a.) Für $X \subseteq M$ heißt $\langle X \rangle := \bigcap_{\substack{U \text{ Untermodul von } M \\ x \subseteq U}} U$ der von X erzeugte Untermodul.

b.) $\langle X \rangle = \left\{ \sum_{i=0}^{n} a_i x_i | a_i \in R, x_i \in X, n \in \mathbb{N} \right\}$ (analog zur linearen Algebra: Linearkombination der erzeugenden Vektoren)

c.) $B \subseteq M$ heißt **linear unabhängig**, wenn $0 = \sum_{i=0}^{n} a_i b_i$ mit $a_i \in R$, $b_i \in B$, $n \in \mathbb{N}$ nur möglich ist mit $a_i = 0$ für alle i.

d.) $B \subseteq M$ heißt **Basis**, wenn jedes $x \in M$ eindeutig als Linearkombination $x = \sum_{i=0}^{n} a_i b_i$ mit $a_i \in R$, $b_i \in B$ und $n \in \mathbb{N}$ darstellbar ist. Äquivalent: B ist linear unabhängig und $\langle B \rangle = M$.

e.) M heißt **freier** R-Modul, wenn M eine Basis besitzt.

Beispiele:

1.) R ist freier R-Modul mit Basis 1 (oder einer anderen Einheit).

2.) Für jedes $n \in \mathbb{N}$ ist $R^n = R \oplus R \oplus \ldots \oplus R$ freier R-Modul mit Basis $e_1, \ldots, e_n$, wobei $e_i = (0, \ldots, 1, \ldots, 0)$.

3.) Ist $I \subseteq R$ Ideal, so ist $M := R/I = \langle \{\overline{1}\} \rangle$. Für $I \neq \{0\}$ ist R/I **nicht** frei! Denn sei $\overline{x} \in M$, $a \in I \setminus \{0\}$, so folgt $a \cdot \overline{x} = \overline{a \cdot x} = \overline{0}$. Damit gibt es in M keine linear unabhängigen Elemente.

Kapitel 3

Algebraische Körpererweiterungen

3.1 Grundbegriffe

Definition 3.1:

Sei L ein Körper und $K \subset L$ ein Teilkörper.

a.) Dann heißt L Körpererweiterung von K. Schreibweise: L/K Körpererweiterung

b.) $[L : K] := \dim_k L$ heißt **Grad** von L über K.

c.) L/K heißt **endlich**, wenn $[L : K] < \infty$.

d.) $\alpha \in L$ heißt algebraisch über K, wenn es ein $f \neq 0 \in K[X]$ gibt mit $f(\alpha) = 0$.

e.) $\alpha \in L$ heißt **transzendent** über K, wenn α nicht algebraisch über K ist.

f.) L/K heißt **algebraische Körpererweiterung**, wenn jedes $\alpha \in L$ algebraisch über K ist.

Beispiel:

1.) Für $a \in \mathbb{Q}$ und $n \geq 2$ ist $\sqrt[n]{a}$ algebraisch über $\mathbb{Q}$, da es sich um eine Nullstelle des Polynoms $X^n - a$ handelt. Summen und Produkte von solchen Wurzeln sind auch algebraisch über $\mathbb{Q}$. Betrachten wir als Beispiel $\sqrt{2} + \sqrt{3}$. Dies ist Nullstelle von...

2.) Sei $L = K(X) = \text{Quot}(K[X])$. Dann ist X transzendent über K. Das gleiche gilt für jedes $f \in K(X) - K$.

3.) In $\mathbb{R}$ gibt es sehr viele über $\mathbb{Q}$ transzendente Elemente. $\mathbb{Q}$ ist abzählbar ($\mathbb{R}$ nicht), also auch $\mathbb{Q}[X]$. Jedes $f \in \mathbb{Q}[X]$ hat endlich viele Nullstellen. Damit gibt es nur abzählbar viele Elemente in $\mathbb{R}$, die algebraisch über $\mathbb{Q}$ sind.

Bemerkung und Definition 3.2:

Sei L/K Körpererweiterung mit $\alpha \in L$ und φ_α: $K[X] \mapsto L$, $f \mapsto f(\alpha)$ der Einsetzungshomomorphismus.

a.) $\text{Kern}(\varphi_\alpha)$ ist Primideal in $K[X]$.

b.) α ist algebraisch genau dann, wenn $\text{Kern}(\varphi_\alpha) \neq \{0\}$ ist.

c.) Ist α algebraisch über K, so gibt es ein eindeutig bestimmtes irreduzibles normiertes Polynom $f_\alpha \in K[X]$ mit $f_\alpha(a) = 0$ und $\text{Kern}(\varphi_\alpha) = (f_\alpha)$. f_α heißt **Minimalpolynom** von α.

d.) $K[\alpha] := \text{Bild}(\varphi_\alpha) = \{f(\alpha) : f \in K[X]\} \subset L$ ist der kleinste Unterring von L, der K und α enthält.

e.) α ist transzendent. $\Leftrightarrow K[\alpha] \simeq K[X]$

f.) Ist α algebraisch über K, so ist $K[\alpha]$ ein Körper und $[K[\alpha] : K] = \text{Grad}(f_\alpha)$.

Beweis:

a.) Kern(φ_α) ist Ideal, da φ_α Homomorphismus ist. Seien f, $g \in K[X]$ mit f, $g \in$ Kern(φ_α). Mit $0 = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$ muss $f(\alpha) = 0$ oder $g(\alpha) = 0$ sein (aufgrund der Nullteilerfreiheit).

c.) $K[X]$ ist Hauptidealring. Damit existiert ein $\widetilde{f_\alpha}$ mit Kern(φ_α) = $(\widetilde{f_\alpha})$. Wegen a.) ist $\widetilde{f_\alpha}$ irreduzibel und eindeutig bis auf eine Einheit in $K[X]$, also ein Element von $K^\times$. Somit existiert genau ein $\lambda \in K^\times$, so dass $\lambda\widetilde{f_\alpha} =: f_\alpha$ normiert ist.

e.) Dies folgt aus b.)

f.) Nach dem Homomorphiesatz ist $K[\alpha] \simeq K[X]/\text{Kern}(\varphi_\alpha)$. Wir müssen uns klar machen, dass das Ideal Kern(φ) ein maximales Ideal ist. Dies ist so, da es sich um ein Primideal $\neq (0)$ in $K[X]$ handelt (siehe Beweis von Satz 9, Behauptung 2). Dann ist $K[\alpha]$ ein Körper.

Alternativer Beweis von f.)

Es ist $f_\alpha(\alpha) = 0$, also $\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0$ mit $c_i \in K$ und $c_0 \neq 0$, da f_α irreduzibel ist. $(\alpha(\alpha^{n-1} + \ldots + c_1) = -c_0)$ Genauso ist 1, α, α^2, …, α^{n-1} eine K-Basis von $K[\alpha]$.

Definition 5.3:

Sei L/K eine Körperweiterung.

a.) Für $A \subseteq L$ sei $K(A)$ der kleinste Teilkörper von L, der A und K umfasst. $K(A)$ heißt der **von** A **erzeugte** Teilkörper. Es ist $K(A) = \{f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$: $n \geq 1$, $\alpha_i \in A$, f, $g \in K[X_1, \ldots, X_n]$, $g \neq 0\}$.

b.) L/K heißt **einfach**, wenn es $\alpha \in L$ gibt mit $L = K(\alpha)$.

c.) L/K heißt **endlich erzeugt**, wenn es eine endliche Menge $\{x_1, \ldots, x_n\} \subset L$ gibt mit $L = K(\alpha_1, \ldots, \alpha_n)$.

Bemerkung 3.4:

Für eine Körperwerweiterung L/K sind folgende Aussagen äquivalent:

i.) L/K ist endlich.

ii.) L/K ist endlich erzeugt und algebraisch.

iii.) L wird von endlich vielen über K algebraischen Elementen erzeugt.

Beweis:

Aus (i) folgt (ii). Sei $[L : K] = n$ und $\alpha \in L$. Damit sind 1, α, α^2, …, α^n K-linear abhängig, womit es $c_i \in K$ gibt, die nicht alle Null sind, mit $\sum_{i=1}^m c_i\alpha^i = 0$. Hieraus ergibt sich $f(\alpha) = 0$ für $f = \sum_{i=0}^n c_iX^i \in K[X]$. Aus (ii) folgt (iii) und aus (iii) wieder (i). Dies zeigen wir mit Induktion über die Anzahl n der Erzeuger. ($n = 1$: 3.2f), $n > 1$ folgt auch aus 3.2f)

Bemerkung 3.5:

Seien $K \subset L \subset M$ Körper.

a.) Sind M/L und L/K algebraisch, so auch M/K.

b.) Sind M/L und L/K endlich, so auch M/K und es gilt: $[M : K] = [M : L] \cdot [L : K]$.

Beweis:

b.) Sei $k_1, \ldots, k_m$ K-Basis von L und $e_1, \ldots, e_n$ L-Basis von M. Hieraus folgt, dass $B = \{e_ib_j{:}i = 1, \ldots, n, j = 1, \ldots, m\}$ eine K-Basis von M ist, weil B M erzeugt. Sei $\alpha \in M$, $\alpha = \sum_{i=1}^n \lambda_ie_i$ mit $\lambda_i \in L$. Durch Einsetzen von $\lambda_i = \sum_{j=1}^m \mu_{ij}b_j$ folgt die Behauptung. Ist $\sum \mu_{ij}e_ib_j = 0$, so ist für jedes feste i $\sum_{j=1}^n \mu_{ij}b_j = 0$, da die e_i über L linear unabhängig sind. Da die b_j linear unabhängig sind, verschwinden die μ_{ij}.

3.2 Kronecker-Konstruktion

Sei $f \in K[X]$ irreduzibel und nicht konstant. Dann hat f eine Nullstelle im Körper $K[X]/(f)$, nämlich die Restklasse von X.

Satz 12:

Jeder Körper K besitzt einen algebraischen Abschluss, also eine Körpererweiterung, die algebraisch abgeschlossen ist.

Beweis:

Der Hauptschritt war, dass es eine algebraische Körpererweiterung K'/K gibt, so dass jedes $f \in K[X]$ eine Nullstelle in K' hat. Zuerst wollen wir jedoch beweisen, dass dies auch gilt. Für jedes $f \in K[X] - K$ sei X_f ein Symbol. und $\Upsilon := \{X_f : f \in K[X] - K\}$ mit $R := K[\Upsilon]$. Nun verwenden wir die zuvor diskutierte KRONECKER-Konstruktion. I sei das von allen $f(X_f)$ in R erzeugte Ideal. Sei $\mathfrak{m} \subset R$ ein maximales Ideal mit $I \subseteq \mathfrak{m}$ und $K' := R/\mathfrak{m}$. K' ist ein Körper und $K'|K$ ist algebraisch, denn K' wird über K erzeugt von den $X_f \in \Upsilon$ und $f(X_f) = 0$ in K', weil $f(X_f) \in I \subseteq \mathfrak{m}$ ist. f hat in K' die Nullstelle (Klasse von) X_f. Es bleibt nun noch folgendes zu zeigen:

1.) $I \neq R$

Angenommen, es ist $I = R$, also $1 \in I$. Dann gibt es ein $n \geq 1$ mit $f_1, \ldots, f_n \in K[X] - f$ und $g_1, \ldots, g_n \in R$ mit $1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$. Sei L/K Körpererweiterung, in der jedes f_i für $i = 1, \ldots, n$ Nullstelle α_i hat (beispielsweise der Zerfällungskörper von $f_1 \cdot \ldots \cdot f_n$). Setzen wir nun für X_{f_i} die Nullstelle α_i ($i = 1, \ldots, n$) ein (und 42 für alle anderen X_f). Dann ist:

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, \ldots, \alpha_n, 42, \ldots) \cdot \underbrace{f_i(\alpha_i)}_{=0} = 0$$

Dies widerspricht natürlich der Annahme, dass das Polynom das konstante Polynom 1 ist.

2.) Es gibt ein maximales Ideal $\mathfrak{m}$ mit $i \subseteq \mathfrak{m}$.

Proposition: Sei R ein kommutativer Ring mit 1, $I \subset R$ echtes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$ in R mit $I \subseteq \mathfrak{m}$. Wir benötigen nun das Lemma von ZORN: Sei $M \neq \varnothing$, geordnet. Hat jede total geordnete Teilmenge von M eine obere Schranke, so hat M ein maximales Element (das heißt, es gibt ein $x \in M$, so dass aus $y \in M$, $x \leq y$ folgt $x = y$).

Sei M die Menge der echten Ideale in R, die I enthalten. Es ist $I \subseteq M$, also $M \neq \varnothing$. Sei $N \subseteq M$ total geordnete Teilmenge. Behauptung: $\widetilde{J} := \bigcup_{J \in N} J$ ist Element von M (un dann auch obere Schranke für N), denn es gilt $I \subseteq \widetilde{J}$. $\widetilde{J}$ ist Ideal, weil aus $x_1, x_2 \in \widetilde{J}$ folgt, dass $x_1 \in J_1$, $x_2 \in J_2$ ist. Ohne Einschränkung ist $J_2 \subseteq J_1$ und daraus folgt $x_2 \in J_1$ und damit $x_1 + x_2 \in J_1 \subset J$. Genauso gilt $r \cdot x_n \in J_1$ für $r \in R$. Es ist $1 \notin \widetilde{J}$, da sonst $1 \in J$ für ein $J \in N$ ist.

3.3 Fortsetzung von Körperhomomorphismen

Proposition 3.8:

Sei $L = K(\alpha)$ und K ein Körper (also einfache Körpererweiterung). Außerdem sei α algebraisch über K und $f = f_\alpha \in K[X]$ das Minimalpolynom. Sei K' Körper und σ: $K \mapsto K'$ ein Körperhomomorphismus. Sei f^σ das Bild von f in $K'[X]$ unter dem Homomorphismus $K[X] \mapsto K'[X]$, $\sum_i a_i X^i \mapsto \sum_i \sigma(a_i) X^i$. Dann gilt:

a.) Zu jeder Nullstelle β von f^σ in K' gibt es genau einen Körperhomomorphismus $\widetilde{\sigma}$: $L \mapsto K'$ mit $\widetilde{\sigma}(\alpha) = \beta$ und $\widetilde{\sigma}|k = \sigma$.

b.) Ist $\widetilde{\sigma}$: $L \mapsto K'$ Fortsetzung von σ (das heißt, $\widetilde{\sigma}|K = \sigma$), so ist $\widetilde{\sigma}(\alpha)$ Nullstelle von f^σ.

Beweis:

a.) Die Eindeutigkeit ergibt sich daraus, dass $\widetilde{\sigma}$ auf den Erzeugenden von L festgelegt ist. Nun noch zur Existenz: $K[X] \mapsto K'$, $X \mapsto \beta$

$$\varphi(f) = f^\sigma(\beta), \sum_i a_i X^i \mapsto \sum_i \sigma(a_i)\beta^i = g^\sigma(\beta) \text{ mit } a_i = g$$

Nach Voraussetzung ist $f^\sigma(\beta) = 0$, also induziert φ nach dem Homomorphiesatz ein $\widetilde{\sigma}$: $K[X]/(f) \mapsto K'$ mit $K[X] = L$.

b.) $f^\sigma(\widetilde{\sigma}(\alpha)) = f^{\widetilde{\sigma}}(\widetilde{\sigma}(\alpha)) = \widetilde{\sigma}(f(\alpha)) = 0$ □.

Folgerung 3.9:

Sei $f \in K[X] - K$ ein konstantes Polynom. Dann ist der Zerfällungskörper $Z(f)$ bis auf Isomorphie eindeutig bestimmt.

Beweis:

Seien L und L' Zerfällungskörper, $L = K(\alpha_1, \ldots, \alpha_n)$, wobei α_i Nullstellen von f sind. Sei weiter $\beta_1 \in L'$ Nullstelle von f. Nach 3.8 gibt es σ: $K(\alpha_1) \mapsto L'$ mit $\sigma|K = \mathrm{id}_K$ und $\sigma(\alpha_1) = \beta_1$ und τ: $K(\beta_1) \mapsto L$ mit $\tau(\beta_1) = \alpha_1$, $\tau(k) = l_k$.

$\tau \circ \sigma = \mathrm{id}_{K(\alpha_1)}$ und $\sigma \circ \tau = \mathrm{id}_{K(\beta_1)} \Rightarrow K(\alpha_1) \simeq K(\beta_1)$

Mit Induktion über n folgt die Behauptung. □.

Bemerkung 3.10:

Sei L/K eine algebraische Körpererweiterung, $\overline{K}$ ein algebraisch abgeschlossener Körper und σ: $L \mapsto \overline{K}$ ein Homomorphismus. Dann gibt es eine Fortsetzung $\widetilde{\sigma}$: $L \mapsto \overline{K}$.

Beweis:

Ist L/K endlich, so folgt die Aussage aus 3.8. Für den allgemeinen Fall sei $\mathcal{M} := \{(L', \tau)$: L'/K Körpererweiterung, $L' \subseteq L$, τ: $L' \mapsto \overline{K}$ Fortsetzung von $\sigma\}$. Da $\mathcal{M} \neq \varnothing$, ist $(k\sigma) \in \mathcal{M}$. $\mathcal{M}$ ist geordnet durch $(L_1, \tau_1) \leq (L_2, \tau_2) \Leftrightarrow L_1 \subseteq L_2$ und τ_2 Fortsetzung von τ_1. Sei $\mathcal{N} \subset \mathcal{M}$ total geordnet. $\widetilde{L} := \bigcup_{(L', \tau) \in \mathcal{N}} L'$ ist ein Körper und $\widetilde{L} \subseteq L$, $\widetilde{\tau}$: $\widetilde{L} \mapsto \overline{K}$. Es ist $\widetilde{\tau}(x) = \tau(x)$, falls $x \in L'$ und $(L', \tau) \in \mathcal{N}$. Wohldefiniertheit: Ist $x \in L''$, so ist ohne Einschränkung $(L', \tau) \subseteq (L'', \tau'')$ und damit $\tau''(x) = \tau(x)$. Hieraus folgt, dass $(\widetilde{L}, \widetilde{\tau})$ eine obere Schranke ist. Also können wir das Zornsche Lemma anwenden. $\mathcal{M}$ hat maximales Element $(\widetilde{L}, \widetilde{\sigma})$. Es bleibt nun noch zu zeigen, dass $\widetilde{L} = L$ ist. Sonst sei $\alpha \in L \setminus \widetilde{L}$ und σ' Fortsetzung von $\widetilde{\sigma}$ auf $\widetilde{L}(x)$ (nach 3.8). Also gilt $(\widetilde{L}(\alpha), \sigma') \in \mathcal{M}$ und $(\widetilde{L}, \sigma) \lneqq (\widetilde{L}, \widetilde{\sigma})$, was ein Widerspruch darstellt.

Folgerung 3.11:

Für jeden Körper K ist der algebraische Abschluss $\overline{K}$ bis auf Isomorphie eindeutig bestimmt.

Beweis:

Seien $\overline{K}$ und C algebraische Abschlüsse von K.

$$\begin{array}{ccc} \overline{K} & \longrightarrow & C \\ \subset\downarrow & & \downarrow\subset \\ K & \xrightarrow[id]{} & K \end{array}$$

Nach Proposition 3.10 gibt es einen Körperhomomorphismus σ: $\overline{K} \mapsto C$, der id_K fortsetzt. Ein Körperhomomorphismus ist immer injektiv, es bleibt also noch die Surjektivität zu zeigen. Dann ist $\sigma(\overline{K}) \subset C$ auch algebraisch abgeschlossen. Ist $f \in \sigma(\overline{K})[X]$, so hat $f^{\sigma^{-1}} \in \overline{K}[X]$ Nullstelle $\alpha \in \overline{K}$. Damit ist $\sigma(a)$ Nullstelle von f.

$$f = \sum_i a_i X^i \Rightarrow f^{\sigma^{-1}} = \sum_i \sigma^{-1}(a_i) X^i$$

$$\sum_i \sigma^{-1}(a_i)\alpha^i = 0 \Rightarrow \sigma\left(\sum_i \sigma^{-1}(a_i)\alpha^i\right) = \sum_i a_i \sigma(a)^i$$

C ist algebraisch über K, also erst recht über $\sigma(\overline{K})$. Nach Satz 3.7 ist $\sigma(\overline{K}) = C$.

Definition und Bemerkung 3.12:

Seien L/K, L'/K zwei Körpererweiterungen von K.

a.) $\mathrm{Hom}_K(L, L') = \{\sigma : L \mapsto L' \text{ Körperhomomorphismus, } \sigma|_K = \mathrm{id}_K\}$

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

b.) Ist L/K endlich und $\overline{K}$ algebraischer Abschluss von K, so ist $|\mathrm{Hom}_K(L, \overline{K})| \leq [L : K]$. Es gibt also höchstens so viele Homomorphismen, wie der Körpergrad ist.

Beweis:

b.) Sei $L = K(\alpha_1, \ldots, \alpha_n)$, wobei die α_i algebraisch über K sind. Induktion über n liefert:

- $n = 1$: Sei $f \in K[X]$ das Minimalpolynom von α_1.
  Für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ Nullstelle von $f^\sigma \in \overline{K}[X]$. Durch $\sigma|_K = \mathrm{id}_K$ und $\sigma(\alpha)$ ist σ eindeutig bestimmt. Damit ist $|\mathrm{Hom}_K(L, \overline{K})|$ gleich der Anzahl der Nullstellen von f^σ. Die Anzahl der Nullstellen ist jedoch höchstens der Grad des Polynoms. Also gilt $|\mathrm{Hom}_K(L, \overline{K})| \leq \mathrm{Grad}(f^\sigma) = [L : K]$.
- $n > 1$: Sei $L_1 = K(\alpha_1, \ldots, \alpha_{n-1})$ und $f \in L_1[X]$ das Minimalpolynom von α_n über L_1. Für $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ Nullstelle von $f^{\sigma_1} \in \overline{K}[X]$ mit $\sigma_1 = \sigma|_{L_1}$. Daraus folgt:

  $$|\mathrm{Hom}_L(L, \overline{K})| \leq |\mathrm{Hom}_K(L_1, \overline{K})| \cdot \mathrm{Grad}(f) \underset{\text{I.V.}}{\leq} [L_1 : K] \cdot [L : L_1] \underset{3.5b.)}{=} [L : K]$$

3.4 Separable Körpererweiterungen

Definition und Bemerkung 3.13:

Sei L/K algebraische Körpererweiterung und $\overline{K}$ der algebraische Abschluss.

a.) $f \in K[X] - K$ heißt **separabel**, wenn f in $\overline{K}$ keine mehrfache Nullstelle hat (also $\mathrm{Grad}(f)$ verschiedene Nullstellen).

b.) $\alpha \in L$ heißt **separabel**, wenn das Minimalpolynom von α über K separabel ist.

c.) L/K heißt **separabel**, wenn jedes $\alpha \in L$ separabel ist.

d.) $f \in K[X] - K$ ist genau dann separabel, wenn $\mathrm{ggT}(f, f') = 1$ ist. Dabei ist:

$$f = \sum_{i=0}^{n} a_i X^i \text{ und } f' = \sum_{i=1}^{n} i a_i X^{i-1}$$

e.) Ist $f \in K[X]$ irreduzibel, so ist f separabel genau dann, wenn $f' \neq 0$ ist.

Beweis:

d.) Wir zerlegen das Polynom in Linearfaktoren. Sei $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ für $\alpha_i \in \overline{K}$. Damit ergibt sich die Ableitung als:

$$f'(X) = \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j)$$

Nach Definition ist f genau dann separabel, wenn $\alpha_i \neq \alpha_j$ für $i \neq j$. Behauptung: Es ist $\alpha_1 = \alpha_i$ für ein $i \geq 2$ genau dann, wenn $(X - \alpha_1) | f'$. Aus der Behauptung folgt, dass f separabel ist genau dann, wenn f und f' teilerfremd in $\overline{K}[X]$ sind. Ist das so, dann ist $\mathrm{ggT}(f, f') = 1$ (teilerfremd in $K[X]$). Ist umgekehrt $\mathrm{ggT}(f, f') = 1$, so gibt es Polynome $g, h \in K[X]$ mit $1 = g \cdot f + h f'$ (nach euklidischem Algorithmus). Das stimmt dann auch in $\overline{K}[X]$, also sind f und f' auch in $\overline{K}[X]$ teilerfremd.

Es bleibt nun noch die Behauptung zu beweisen. $(X - \alpha_1)$ teil $\prod_{i \neq j}(X - \alpha_j)$, falls $i \neq 1$ ist. Also teilt $(X - \alpha_1)$ f' genau dann, wenn $(X - \alpha_1)$ Teiler von $\prod_{j \neq 1}(X - \alpha_j)$ ist. Dies ist genau dann der Fall, wenn $\alpha_1 = \alpha_j$ für ein $j \neq 1$.

e.) Ist $f' = 0$, so ist $\mathrm{ggT}(f, f') = f \neq 1$. Ist $f' \neq 0$, so ist $\mathrm{Grad}(f') < \mathrm{Grad}(f)$. Ist außerdem f irreduzibel und $\alpha \in \overline{K}$ Nullstelle von f, so ist f das Minimalpolynom von α. Aus $f' \neq 0$ folgt, dass α nicht Nullstelle von f' ist. Somit ist $\mathrm{ggT}(f, f') = 1$.

Folgerung 3.14:

Ist $\text{char}(K) = 0$, so ist jede algebraische Körperweiterung von K separabel.

Beispiel 3.15:

Sei p eine Primzahl und $K = \mathbb{F}_p(t) = \text{Quot}(\mathbb{F}_p[t])$. $f(X) = X^p - t \in K[X]$ ist ein Beispiel für ein irreduzibles aber nicht separables Polynom. Es gilt $f'(X) = pX^{p-1} = 0$ wegen $\text{char}(p)$. $t \in \mathbb{F}_p[t]$ ist Primelement. Nach dem EISENSTEIN-Kriterium ist f irreduzibel in $(\mathbb{F}_p[t])[X]$ und nach Folgerung 2.29 ist f auch irreduzibel in $K[X]$.
Aus $f(X) = X^p - a \in \mathbb{F}_p[X]$ folgt $f' = 0$. Frage: Ist f irreduzibel? Nein, denn f hat Nullstelle in $\mathbb{F}_p$, das heißt, es gibt ein $b \in \mathbb{F}_p$ mit $b^p = a$. Die Abbildung φ: $\mathbb{F}_p \mapsto \mathbb{F}_p$, $b \mapsto b^p$ ist surjektiv. Die Abbildung einer endlichen Menge in sich selbst ist genau dann surjektiv, wenn sie injektiv ist. Injektiv ist sie aber, weil sie ein Körperhomomorphismus ist, denn $(a+b)^p = a^p + b^p$.

Definition:

φ heißt FROBENIUS-Automorphismus.

Bemerkung 3.16:

Sei $\text{char}(k) = p > 0$, $f \in K[X]$ irreduzibel.

a.) Es gibt ein separables irreduzibles Polynom $y \in K[X]$, so dass $f(X) = g(X^{p^r})$ für ein $r \geq 0$.

b.) Jede Nullstelle von f in $\overline{K}$ hat die Vielfachheit p^r.

Beweis:

Sei f nicht separabel.

$$f = \sum_i a_i X^i \text{ und } f' = \sum_i i a_i X^{i-1} = 0$$

Hieraus folgt $ia_i = 0$ für $i = 1, \ldots, n$. Damit ist $a_i = 0$, falls i nicht durch p teilbar ist und damit ist f ein Polynom in X^p, also $f = g_1(X^p)$. Durch Induktion über k folgt die Behauptung.

Satz 13:

Sei L/K endliche Körpererweiterung und $\overline{K}$ algebraischer Abschluss von L.

a.) $[L:K]_s := |\text{Hom}_K(L, \overline{K})|$ heißt **Separabilitätsgrad** von L über K. ($\overline{K}$ ist bis auf Isomorphie eindeutig bestimmt, womit der Separabilitätsgrad wohldefiniert ist.)

b.) Ist L' Zwischenkörper von L/K, so ist von L über K: $[L:K]_s = [L:L']_s \cdot [L':K]_s$.

c.) L/K ist separabel genau dann, wenn $[L:K] = [L:K]_s$.

d.) Ist $\text{char}(k) = p > 0$, so gibt es ein $r \in \mathbb{N}$ mit $[L:K] = p^r \cdot [L:K]_s$.

Beweis:

b.) Sei $\text{Hom}_K(L', \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ und $\text{Hom}_{L'}(L, \overline{K}) = \{\tau_1, \ldots, \tau_m\}$. Sei $\overline{\sigma}_i$: $\overline{K} \mapsto \overline{K}$ Fortsetzung von σ_i für $i = 1, \ldots, n$. Dann ist $\overline{\sigma}_i \in \text{Aut}_K(\overline{K}, \overline{K})$. Behauptung:

1.) $\text{Hom}_K(L, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \text{—} i = 1, \ldots, n; j = 1, \ldots, m\}$

2.) $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_i \circ \tau_{j'}$ genau dann. wenn $i = i'$ und $j = j'$

Aus 1.) und 2.) folgt als die Aussage b). Beweisen wir also nun noch die Behauptung:

1.) „$\supseteq$“ ist klar. „$\subseteq$“: Sei $\sigma \in \text{Hom}_K(L, \overline{K})$. Dann gibt es ein i mit $\sigma|_{L'} = \sigma_i$. Hieraus folgt $\overline{\sigma}_i^{-1} \circ \sigma|_{L'} = \text{id}_{L'}$. Damit existiert ein j mit $\overline{\sigma}_i^{-1} \circ \sigma = \tau_j$ und es folgt $\sigma = \overline{\sigma}_i \circ \tau_j$.

2.) Sei $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_i \circ \tau_j$. Hieraus folgt $\overline{\sigma}_i|_{L'} = \overline{\sigma}_{i'}|_{L'}$ ($\sigma_i = \sigma_{i'}$) und somit resultiert $i = i'$ und $\tau_j = \tau_{j'}$, also $j = j'$.

c.) „⇒“: Sei $L = K(\alpha_1, \ldots, \alpha_n)$. Wir führen eine vollständige Induktion über n durch.

- $n = 1$: Für $L = K(\alpha)$ ist $f = f_\alpha \in K[X]$ das Minimalpolynom von α über K. Hieraus folgt:

  $$[L : K]_s \underset{3.12}{=} |\{\text{Nullstellen von } f \text{ in } \overline{K}\}| = \text{Grad}(f) = [L : K]$$

- $n > 1$: Für $L_1 := K(\alpha_1, \ldots, \alpha_{n-1})$ ist $f \in L_1[X]$ das Minimalpolynom von α_n. Zu jedem $\sigma_1 \in \text{Hom}_K(L_1, \overline{K})$ und jeder Nullstelle von f in $\overline{K}$ gibt es genau eine Fortsetzung $\widetilde{\sigma}_1$: $L \mapsto \overline{K}$. Daraus, dass f separabel ist, folgt

  $$\begin{aligned}[L : K]_s &= |\text{Hom}_K(L, \overline{K})| = \text{Grad}(f) \cdot |\text{Hom}_K(L_1, \overline{K})| = \\ &= [L : L_1] \cdot [L_1 : K]_s \underset{\text{I.V.}}{=} [L : L_1] \cdot [L_1 : K] = [L : K]\end{aligned}$$

„⇐“: Ist $\text{char}(K) = 0$, so ist L/K separabel. Sei also $\text{char}(k) = p > 0$ und $\alpha \in L$, $f \in K[X]$ das Minimalpolynom von α. Nach 3.16 gibt es ein $r \geq 0$ und separables irreduzibles $g \in K[X]$ mit $f(x) = g(X^{p^r})$.

$\Rightarrow [K(\alpha) : K]_s = |\{\text{Nullstellen von } f \text{ in } \overline{K}\}| = |\{\text{Nullstellen von } g \text{ in } \overline{K}\}| = \text{Grad}(g)$

$\Rightarrow [K(\alpha) : K] = \text{Grad}(f) = p^r \cdot \text{Grad}(g) = p^r \cdot [K(\alpha) : K]_s \, (*)$

$\Rightarrow [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] \geq [L : K(\alpha)]_s \cdot p^r [K(\alpha) : K]_s \underset{b.)}{=} [L : K]_s \cdot p^r$

Damit folgt $p^r = 1$ und also $g = f$. Also ist α separabel.

d.) Diese Aussage folgt aus $(*)$.

3.4.1 Satz vom primitiven Element

Satz 14:

Jede endliche separable Körpererweiterung L/K ist einfach.

Beweis:

Ist K endlich, so folgt aus Paragraph 5, dass $L^\times$ zyklische Gruppe ist. Ist $L^\times = \langle \alpha \rangle$, so ist $L = K[\alpha]$. Sei also K unendlich, $L = K(\alpha_1, \ldots, \alpha_r)$. Ohne Einschränkung betrachten wir $r = 2$, also $L = K(\alpha, \beta)$. Sei $\overline{K}$ algebraischer Abschluss von L mit $[L : K] = n$, $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ (Satz 13c) und

$$g(X) = \prod_{1 \leq i < j \leq n} [\sigma_i(\alpha) - \sigma_j(\alpha) + (\sigma_i(\beta) - \sigma_j(\beta)) \cdot X] \in \overline{K}[X]$$

Es ist $g \neq 0$, denn aus $\sigma_i(\alpha) = \sigma_j(\alpha)$ und $\sigma_i(\beta) = \sigma_j(\beta)$ folgt $\sigma_i = \sigma_j$. Da K unendlich ist, gibt es $\lambda \in K$ mit $g(\lambda) \neq 0$. Behauptung: $\gamma := \alpha + \lambda\beta \in L$ erzeugt L über K. Dies können wir folgendermaßen begründen. Sei $f \in K[X]$ das Minimalpolynom von γ über K. Für jedes i ist $f(\sigma_i(\gamma)) = \sigma_i(f(\gamma)) = 0$, da $\sigma_i|_K = \text{id}_K$. Angenommen, es gilt $\sigma_i(\gamma) = \sigma_j(\gamma)$ für ein $i \neq j$. Dann wäre $\sigma_i(\alpha) + \sigma_i(\beta) \cdot \lambda = \sigma_j(\alpha) + \sigma_j(\beta) \cdot \lambda$, bzw. $\sigma_i(\alpha) + \sigma_i(\beta) \cdot \lambda - \sigma_j(\alpha) + \sigma_j(\beta) \cdot \lambda = 0$, also $g(\lambda) = 0$. Dies stellt ein Widerspruch dar. Damit hat f mindestens n Nullstellen.

$\text{Grad}(f) = [K(\gamma) : K] \geq n = [L : K]$

Da $\gamma \in L$ ist, folgt $K(\gamma) = L$.

3.5 Endliche Körper

Proposition 3.17:

Ist K ein Körper, so ist jede endliche Untergruppe von $(K^\times, \cdot)$ zyklisch.

Beweis:

Sei $G \subseteq K^\times$ endliche Untergruppe und $a \in G$ ein Element maximaler Ordnung. Sei $n = \text{ord}(a)$ und $G_n := \{b \in G : \text{ord}(b) | n\}$. Es gilt $G_n = \langle a \rangle$, denn jedes $b \in G_n$ ist Nullstelle von $X^n - 1$. Diese sind 1, a, a^2, …, a^{n-1}. Hieraus folgt $|G_n| = |\langle a \rangle| = n$. Nach Satz 3 ist $G \simeq \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$ mit $a_i | a_{i+1}$. Für jedes $b \in G$ ist $\text{ord}(b)$ Teiler von a_r.

Satz 15:

Sei p Primideal mit $n \geq 1$ und $q = p^n$. Sei $\mathbb{F}_q$ der Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$. Dann gilt:

a.) $\mathbb{F}_q$ hat q Elemente.

b.) Zu jedem endlichen Körper K gibt es ein $q = p^n$ mit $K \simeq \mathbb{F}_q$.

Beweis:

a.) $f(X) = X^q - X$ ist separabel, da $f'(X) = -1$ ist. Damit ist ggT(f,f')=1. Damit ist f separabel und hat q verschiedene Nullstellen in $\mathbb{F}_q$ und somit hat $\mathbb{F}_q$ mindestens q Elemente, also ist $|\mathbb{F}_q| \geq q$. Umgekehrt ist jedes $a \in \mathbb{F}_q$ Nullstelle von f, denn $\mathbb{F}_q$ wird erzeugt von den Nullstellen von f. Sind also a, b Nullstellen von f, so ist $a^q = a$ und $b^q = b$, also auch $(ab)^q = ab$ und $(a + b)^q = a^q + b^q = a + b$.

Kapitel 4

Galois-Theorie

4.1 Der Hauptsatz

Definition und Proposition 4.1:

Sei L/K eine algebraische Körpererweiterung. (Es wird nicht vorausgesetzt, dass die Erweiterung endlich ist.)

a.) L/K heißt **normal**, wenn es eine Familie $\mathcal{F} \subset K[X]$ gibt, so dass L Zerfällungskörper von $\mathcal{F}$ ist.

b.) Ist L/K normal, so ist $\mathrm{Hom}_K(L, \overline{K})$ (wobei $\overline{K}$ algebraischer Abschluss von L sei) gleich $\mathrm{Aut}_K(L)$.

c.) L/K heißt **galoisch** (Galois-Erweiterung), wenn L/K normal und separabel ist.

d.) Ist L/K galoisch, so heißt $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ die Galois-Gruppe von L/K.

e.) Eine endliche Erweiterung L/K ist genau dann galoisch, wenn $|\mathrm{Aut}_K(L)| = [L : K]$ ist. (Diese macht natürlich nur für endliche Körpererweiterungen Sinn.)

f.) Ist L/K galoisch und E ein Zwischenkörper, so ist L/E galoisch und $\mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$.

g.) Ist in f.) zusätzlich auch E/K galoisch (was im allgemeinen nicht gilt), so ist

$$1 \mapsto \mathrm{Gal}(L/E) \mapsto \mathrm{Gal}(L/K) \underset{\beta}{\to} \mathrm{Gal}(E/K) \mapsto 1$$

exakt.

Beweis:

b.) „$\supseteq$“ gilt immer, weil L eine Teilmenge von K ist. „$\subseteq$“: Sei $L = Z(\mathcal{F})$, $f \in \mathcal{F}$ und $\alpha \in L$ Nullstelle von f. Für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ ist $\sigma(\alpha)$ auch Nullstelle von f.

$$f(X) = \sum_{i=0}^{n} a_i X^i \Rightarrow 0 = \sigma(f(\alpha)) = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = f(\sigma(\alpha))$$

Somit ist $\sigma(\alpha) \in L$. L wird von den Nullstellen der $f \in \mathcal{F}$ erzeugt. Damit folgt $\sigma(L) \subseteq L$.

e.) „$\Rightarrow$“: Die Erweiterung sei galoisch. Dann ist L/K normal und aus b.) folgt:

$$|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L, \overline{K})| = [L : K]_s \overset{\text{Satz } 13}{=} [L : K] \qquad (*)$$

„$\Leftarrow$“: In Gleichung $(*)$ gilt stets

$$|\mathrm{Aut}_K(L)| \leq |\mathrm{Hom}_K(L, \overline{K})| = [L : K]_s \leq [L : K]$$

Aus $|\mathrm{Aut}_K(L)| = [L : K]$ folgt, dass $[L : K]_s = [L : K]$ ist. Damit ist L/K separabel. Des weiteren folgt mit Satz 14, dass $L = K(\alpha)$ ist für ein $\alpha \in L$. Sei $f \in K[X]$ das Minimalpolynom von α und $\beta \in \overline{K}$ Nullstelle von f. Nach 3.8 gibt es $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ mit $\sigma(\alpha) = \beta$. Wegen $(*)$ ist $\sigma \in \mathrm{Aut}_K(L)$ und somit $\beta \in L$, womit L Zerfällungskörper von f ist.

f.) L/E ist normal, da Zerfällungskörper von $\mathcal{F} \subset K[X] \subseteq E[X]$. Ebenso ist L/E separabel, da L/K separabel ist.

g.) Für $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ ist $\sigma|_E$: $E \mapsto L$, also $\sigma \in \mathrm{Hom}_K(E, L) \subseteq \mathrm{Hom}_K(E, \overline{K}) \underset{\text{b.)}}{=} \mathrm{Aut}_K(E)$, da E/K galoisch ist. Damit ist die Abbildung β wohldefiniert. Wir müssen zeigen, dass β surjektiv ist. Sei $\sigma \in \mathrm{Gal}(E/K)$ ist. Nach 3.10 lässt sich σ fortsetzen zu $\widetilde{\sigma}$: $L \mapsto \overline{K}$, $\widetilde{\sigma} \in \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$ und $\beta(\widetilde{\sigma}) = \widetilde{\sigma}|_E = \sigma$.

Kern $= \{\sigma \in \mathrm{Gal}(L/K) : \sigma|_E = \mathrm{id}_E\} = \mathrm{Aut}_E(L) = \mathrm{Gal}(L/E)$

Satz 17 (Hauptsatz der Galois-Theorie):

Sei L/K endliche Galois-Erweiterung.

a.) Die Zuordnungen

$\{\text{Zwischenkörper von } L/K\} \underset{\Phi}{\overset{\Psi}{\rightarrow\leftarrow}} \{\text{Untergruppe von } \mathrm{Gal}(L/K)\}$

$E \mapsto \mathrm{Gal}(L/E)$ und $L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \,\forall\, \sigma \in H\} \leftarrow H$

sind bijektiv und zueinander invers.

b.) Ein Zwischenkörper E von L/K ist genau dann galoisch über K, wenn $\mathrm{Gal}(L/E)$ Normalteiler in $\mathrm{Gal}(L/K)$ ist.

Beweis:

a.) L^H ist Zwischenkörper. „$\Psi \circ \Phi = \mathrm{id}$“: Sei $H \subseteq \mathrm{Gal}(L/K)$ Untergruppe. Zu zeigen ist $\mathrm{Gal}(L/L^H) = H$. „$\supseteq$“ gilt nach Definition von L^H. „$\subseteq$“: Nach 4.1 e.) ist $|\mathrm{Gal}(L/L^H)| = [L : L^H]$. Es genügt also zu zeigen, dass $[L : L^H] \leq |H|$. Sei $\alpha \in L$ primitives Element der Körpererweiterung L/L^H, also $L = L^H(\alpha)$. Sei $f := \prod_{\sigma \in H}(X - \sigma(\alpha)) \in L[X]$, da $\alpha \in L$ und σ ein Automorphismus von L ist. Dann ist $\mathrm{Grad}(f) = |H|$. Für jedes $\tau \in H$ ist $f^\tau = f$. (Mit σ durchläuft auch $\tau \cdot \sigma$ alle Elemente von H.) Dies bedeutet $f \in L^H[X]$. Hieraus folgt, dass das Minimalpolynom g von α über L^H Teiler von f ist und damit $[L : L^H] = \mathrm{Grad}(g) \leq \mathrm{Grad}(f) = |H|$. „$\Phi \circ \Psi = \mathrm{id}$“: Sei E Zwischenkörper, $H := \mathrm{Gal}(L/E)$. Zu zeigen ist, dass $E = L^H$. „$\subseteq$“ folgt aus der Definition. „$\supseteq$“ Da L^H/E separabel ist, genügt es zu zeigen, dass der Separabilitätsgrad $[L^H : E]_s = 1$ ist. Sei $\sigma \in \mathrm{Hom}_E(L^H, \overline{K})$ und $\widetilde{\sigma} \in \mathrm{Hom}_E(L, \overline{K}) = \mathrm{Aut}_E(L) = \mathrm{Gal}(L/E) = H$ Fortsetzung. Es folgt also $\widetilde{\sigma}|_{L^H} = \sigma|_{L^H} = \mathrm{id}_{L^H}$.

b.) „$\Rightarrow$“: Dies folgt aus 4.1 (g). „$\Leftarrow$“: Sei $H := \mathrm{Gal}(L/E)$ Normalteiler in $\mathrm{Gal}(L/K)$. Wegen 4.1 (e) genügt es zu zeigen, dass für jedes $\sigma \in \mathrm{Hom}_K(E, \overline{K}$ gilt: $\sigma(E) \subseteq E$. Sei also $\sigma \in \mathrm{Hom}_K(E, \overline{K})$ und $\widetilde{\sigma} \in \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}(L/K)$ Fortsetzung und $\alpha \in E$ und $\tau \in H$. Dann ist

$\tau(\sigma(\alpha)) = (\tau \circ \widetilde{\sigma})(\alpha) = (\widetilde{\sigma} \circ \tau')(\alpha) = \widetilde{\sigma}(\alpha) = \sigma(\alpha)$

(Aufgrund der Normalteilereigenschaft $\widetilde{\sigma}^{-1} \circ \tau \circ \widetilde{\sigma} = \tau' \in H$ folgt nämlich $\tau \circ \widetilde{\sigma} = \widetilde{\sigma} \circ \tau'$.) Damit gilt $\sigma(\alpha) \in L^H = E$ nach (a). □

Folgerung 4.2:

Sei L/K endliche Galoiserweiterung. Dann gilt für Zwischenkörper E, E' (bzw. Untergruppen H, H' von $\mathrm{Gal}(L/K)$):

a.) $E \subseteq E'$ ist äquivalent zu $\mathrm{Gal}(L/E) \supseteq \mathrm{Gal}(L/E')$.

b.) $\mathrm{Gal}(L/E \cap E') = \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/E') \rangle$ (die von $\mathrm{Gal}(L/E)$ und $\mathrm{Gal}(L/E')$ erzeugte kleinste Untergruppe)

Beweis:

Dieser kann als Übung durchgeführt werden.

Folgerung 4.3:

Zu jeder endlichen **separablen** Körpererweiterung gibt es nur endlich viele Zwischenkörper.

Beweis:

Ist L/K endliche Galoiserweiterung, so entsprechen die Zwischenkörper bijektiv den Untergruppen der endlichen Gruppe $\mathrm{Gal}(L/K)$. Im allgemeinen ist $L = K(\alpha)$ (Satz 14). Sei f das Minimalpolynom von α über K. f ist separabel, da L/K separabel ist. Sei $\widetilde{L}$ der Zerfällungskörper von f über K. Damit ist $\widetilde{L}/K$ galoisch und wegen $K \subseteq L \subseteq \widetilde{L}$ hat L/K nur endliche viele Zwischenkörper.

Proposition 4.4:

Sei L ein Körper und $G \subseteq \mathrm{Aut}(L)$ eine endliche Untergruppe. Weiterhin sei $K := L^G = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G\}$. Dann ist L/K Galoiserweiterung und $\mathrm{Gal}(L/K) = G$.

Beweis:

K ist Körper, da σ Körperautomorphismen sind. Damit ist L/K eine Körpererweiterung. L/K ist außerdem algebraisch und separabel. Sei $\alpha \in L$ und $G \cdot \alpha = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$ mit $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ für $I \neq j$ und $\sigma_1 = \mathrm{id}_1$. ($\{\sigma(\alpha) : \sigma \in G\} = G \cdot \alpha$ ist endlich.) Dabei ist r ein Teiler von $n = |G|$. Sei

$$f_\alpha(X) := \prod_{i=1}^{r}(X - \sigma_i(\alpha)) \in L[X]$$

ein Polynom mit $f_\alpha(\alpha) = 0$. Zu zeigen ist, dass $f_\alpha \in K[X]$ ist. Dies gilt, weil für $\sigma \in G$ ist

$$f_\alpha^\sigma(X) = \prod_{i=1}^{r}(X - \sigma\sigma_i(\alpha))$$

$\sigma\sigma_i(\alpha)$ sind dieselben Faktoren wie $\sigma_i(\alpha)$ (eventuell in anderer Reihenfolge). Damit ist $f_\alpha = f_\alpha^\sigma$ und $f_\alpha \in K[X]$. Somit ist α algebraisch und separabel (da f_α separables Polynom ist) und $[K(\alpha) : K] \leq n$.

- Damit die Körpererweiterung L/K galoisch ist, muss sie außerdem normal sein. Der Zerfällungskörper von f_α ist in L enthalten, womit L Zerfällungskörper der Familie $\{f_\alpha : \alpha \in L\}$ ist.
- Es bleibt nun noch zu zeigen, dass L/K endlich ist. Sei $(\alpha_i)_{i \in I}$ Erzeugendensystem von L/K. Für jede endliche Teilmenge $I_0 \subseteq I$ ist $K(\{\alpha_i : i \in I_0\})$ endlich über K, also ist $K(\{\alpha_i, i \in I_0\} = K(\alpha_0)$ für ein $\alpha_0 \in L$. Wegen $[K(\alpha) : K] \leq n$ ist $[K(\{\alpha_i : i \in I_0\}) : K] \leq n$. Sei $I_1 \subseteq I$ endlich, so dass $K_1 := K(\{\alpha_i : i \in I_1\})$ maximal unter den $K(\{\alpha_j : j \in J\})$, wobei J eine endliche Teilmenge von I ist. Wir nehmen an, dass $K_1 \neq L$ ist. Dann gibt es ein $i \in I$ mit $\alpha_i \notin K_1$. Hieraus folgt, dass $K_1(\alpha_i) \supsetneqq K_1$, aber trotzdem endlich ist. Dies ist ein Widerspruch zur Wahl von K_1. Also ist L/K endlich; genauer ist $[L : K] \leq n$ wegen $[K(\alpha) : K] \leq n$.
- $\mathrm{Gal}(L/K) = G$. „$\subseteq$“ gilt nach Definition. Nach 4.1 (e) ist $n = |G| \leq |\mathrm{Gal}(L/K)| = [L : K] \leq n$. □

4.2 Die Galoisgruppe einer Gleichung

Definition und Bemerkung 4.5:

Sei K ein Körper und $f \in K[X]$ ein separables Polynom.

a.) Sei $L = L(f)$ Zerfällungskörper von f über K. Dann heißt $\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$ Galoisgruppe von f.

b.) Ist $n = \mathrm{Grad}(f)$, so gibt es einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(f) \hookrightarrow S_n$ (durch Permutation der Nullstellen von f).

c.) Ist L/K separable Körpererweiterung vom Grad n, so ist $\mathrm{Aut}_K(L)$ isomorph zu einer Untergruppe von S_n.

Beweis:

c.) Sei $L = K(\alpha)$ und $f \in K[X]$ Minimalpolynom von α. $\alpha_1, \ldots,; \alpha_d$ seien die Nullstellen von f in L. Damit permutiert jedes $\sigma \in \mathrm{Aut}_K(L)$ die Nullstellen $\alpha_1, \ldots, \alpha_d$.

Beispiel 4.6:

Die Galoisgruppe von $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist S_5.

Beweis:

- ✳ f ist irreduzibel.
- ✳ f hat drei reelle und zwei zueinander konjugierte komplexe Nullstellen. Es gilt $f(-\infty) = -\infty$, $f(0) = 2$, $f(1) = -1$ und $f(\infty) = \infty$, damit hat f also mindestens drei reelle Nullstellen.

  $$f'(X) = 5X^4 - 4 = 5\left(X^2 - \frac{2}{\sqrt{5}}\right)\left(X^2 + \frac{2}{\sqrt{5}}\right)$$

  $f'(X)$ hat genau zwei reelle Nullstellen. Hieraus folgt, dass f **genau** drei reelle Nullstellen hat. Ist $\alpha \in \mathbb{C}$ Nullstelle von f, so ist $f(\overline{\alpha}) = \overline{f(\alpha)} = f(\alpha) = 0$. (Hat ein Polynom reelle Koeffizienten, so müssen die komplexen Nullstellen zueinander konjugiert sein.)
- ✳ $G = \mathrm{Gal}(f)$ enthält die komplexe Konjugation τ. τ operiert als Transposition, da τ zwei Nullstellen (nämlich die beiden komplexen) vertauscht und die drei reellen fest lässt.
- ✳ G enthält ein Element der Ordnung 5. Ist α Nullstelle von f, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ und $\mathbb{Q}(\alpha) \leq L(f)$. Der Index von H in G muss gleich 5 sein. Nach Satz 17 teil 5 die Ordnung von G, also $|G|$ und nach Sylow folgt die Behauptung.
- ✳ Ein Element von Ordnung 5 in S_5 ist ein 5-Zyklus. G enthält also einen 5-Zyklus und eine **Transposition**. Hieraus folgt $G = S_5$. (Übungsaufgabe!)

Wir betrachten nun eine allgemeine Gleichung n-ten Grades.

Bemerkung 4.7:

Sei k ein Körper und $L = k(T_1, \ldots, T_n) = \mathrm{Quot}(k[T_1, \ldots, T_n])$.

a.) S_n operiert auf L durch $\sigma(T_i) = T_{\sigma(i)}$.

b.) Sei $K := L^{S_n}$. L/K ist Galois-Erweiterung (nach Proposition 4.4) vom Grad $n!$.

c.) L ist (über K) Zerfällungskörper von $f(X) = \prod_{i=1}^{n}(X - T_i) \in K[X]$.

d.) $\mathrm{Gal}(f) = S_n$

e.) $f(X) = \sum_{\nu=0}^{n}(-1)^\nu s_\nu(T_1, \ldots, T_n)X^{n-\nu}$ mit $s_\nu(T_1, \ldots, T_n) = \sum_{1 \leq i < \ldots, j \leq n} T_{i1} \cdot \ldots T_{i\nu}$

Beispielsweise ist $s_1(T_1, \ldots, T_n) = T_1 + \ldots + T_n$, $s_2 = T_1T_2 + T_1T_3 + \ldots$ und $s_n = T_1 \cdot \ldots \cdot T_n$

f.) $K = K(s_1, \ldots, s_n)$

4.3 Einheitswurzeln

Bemerkung und Definition 4.8:

Sei K ein Körper und $\overline{K}$ der algebraische Abschluss. Sei weiterhin $n \in \mathbb{N}$, teilerfremd zu $\mathrm{char}(K)$.

a.) Die Nullstellen von $X^n - 1$ in $\overline{K}$ heißen ***n*-te Einheitswurzeln**.

b.) $\mu_n(\overline{K}) := \{\zeta \in \overline{K} : \zeta^n = 1\}$ ist zyklische Untergruppe der multiplikativen Gruppe $\overline{K}^\times$ von Ordnung n.

c.) Eine n-te Einheitswurzel ζ heißt **primitiv**, wenn $\langle\zeta\rangle$ (die von ihr erzeugte Untergruppe) gleich $\mu_n(\overline{K})$ ist.

Beweis:

b.) $\mu_n(\overline{K})$ bilden eine Untergruppe bezüglich der Multiplikation. Eine endliche Untergruppe einer multiplikativen Gruppe ist zyklisch nach 3.17. $X^n - 1$ ist separabel, da $f'(X) = nX^{n-1}$ ($n \nmid \mathrm{char}(K)$) und $f(X)$ keine gemeinsame Nullstelle haben (Proposition 3.13).

c.) Sind $\zeta_1, \ldots, \zeta_{\varphi(n)}$ die primitiven Einheitswurzeln, so heißt

$$\Phi_n(x) := \prod_{i=1}^{\varphi(n)} (X - \zeta_i) \in \overline{K}[X]$$

das n-te **Kreisteilungspolynom**.

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

e.) Sei ζ primitive n-te Einheitswurzel. Dann ist $K(\zeta)/K$ eine GALOIS-Erweiterung.

f.) χ_n: $\mathrm{Gal}(K(\zeta)/K) \mapsto (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma \mapsto \chi_n(\sigma)$, wobei $\sigma(\zeta) = \zeta^{\chi_n(\sigma)}$ ist injektiver Gruppenhomomorphismus. (χ_n heißt auch zyklotronischer Charakter.)

g.) Es ist $\Phi_n \in K[X]$, genauer:

$$\Phi_n(X) = \begin{cases} \in \mathbb{Z}[X] \text{ primitiv} & \text{für} \quad \mathrm{char}(k) = 0 \\ \in \mathbb{F}_p[X] & \text{für} \quad \mathrm{char}(k) = p \end{cases}$$

k.) Ist $K = \mathbb{Q}$, so ist Φ_n irreduzibel und χ_n ein Isomorphismus. $\mathbb{Q}(\zeta)$ heißt n-ter **Kreisteilungskörper**.

Satz 18:

Sei K ein Körper und $\overline{K}$ der algebraische Abschluss. Sei weiterhin $n \in \mathbb{N}$, teilerfremd zu $\mathrm{char}(K)$ und außerdem $n \geq 2$.

a.) Die Anzahl der primitiven Einheitswurzeln in $\overline{K}$ ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \{m \in \{1, \ldots, n\} : \mathrm{ggT}(m, n) = 1\}$ (die Anzahl der zu n teilerfremden Zahlen $\leq n$). $n \mapsto \varphi(n)$ ist die EULERsche φ-Funktion.

b.) Nach dem chinesischen Restsatz (Satz 8) gilt:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}$$

Die Einheitenbildung funktioniert komponentenweise:

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^\times \oplus \ldots \oplus (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^\times$$

$$|(\mathbb{Z}/p^\nu\mathbb{Z})^\times| = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$$

d.) $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ \mathrm{ord}(\zeta) = d}} (X - \zeta) = \prod_{d|n} \Phi_d(X)$

e.) $K(\zeta)$ ist Zerfällungskörper von $X^n - 1$ über K, weil ζ alle Einheitswurzeln erzeugt. Also ist $K(\zeta)$ normal. $X^n - 1$ ist außerdem separabel (wegen 4.8 (b)) und damit ist $K(\zeta)/K$ GALOIS-Erweiterung.

f.) $\chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$, weil $\sigma(\zeta)$ primitive Einheitswurzel sein muss. χ_n ist Gruppenhomomorphismus, da für $\sigma_1, \sigma_2 \in \mathrm{Gal}(K(\zeta)/K)$ gilt:

$$\sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{\chi_n(\sigma_2)}) = (\sigma_1(\zeta))^{\chi_n(\sigma_2)} = \zeta^{\chi_n(\sigma_1)}\zeta^{\chi_2(\sigma_2)}$$

Es bleibt zu zeigen, dass χ_n injektiv ist. Dazu schauen wir uns den Kern an, also alle Elemente die auf 1 abgebildet werden: $\chi_n(\sigma) = 1$. Hieraus folgt $\sigma(\zeta) = \zeta$ und damit $\sigma = \mathrm{id}$.

g.) Wir führen eine vollständige Induktion über n durch. Der Fall $n = 2$ ist klar. Für $n > 2$ gilt:

$$X^n - 1 \underset{(\mathrm{d})}{=} \Phi_n(X) \cdot \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}_{\in \mathbb{F}_p[X] \text{ nach I.V.}}$$

Aus $\mathrm{char}(k) = p \in \mathbb{F}_p[X]$ folgt $\Phi_n(X) \in \mathbb{F}_p[X]$. Aus $\mathrm{char}(k) = 0 \in \mathbb{Z}[X]$ folgt $\Phi_n(X) \in \mathbb{Z}[X]$ primitiv. Nach dem Lemma von GAUSS ist $\phi_n(X) \in \mathbb{Z}[X]$ primitiv.

h.) Es genügt zu zeigen, dass Φ_n irreduzibel ist. (Dann folgt, dass χ_n Isomorphismus ist, aus (e) und (f).) Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ, wobei $f \in \mathbb{Z}[X]$ wegen (g). Behauptung: Es gilt $f(\zeta^p) = 0$ für jede Primzahl p mit $p \nmid n$. Dann ist auch $f(\zeta^m) = 0$ für jedes m mit $(m, n) = 1$. Dann folgt $f(\zeta_i) = 0$ für jede primitive Einheitswurzel ζ_i und damit $\phi_n | f$ und $\Phi_n = f$. Also ist Φ_n irreduzibel, weil f Minimalpolynom ist. Wir müssen nun noch die Behauptung beweisen. Sei $X^n - 1 = f \cdot h$. Wäre $f(\zeta^p) \neq 0$, so müsste $h(\zeta^p) = 0$ sein. Also ist ζ Nullstelle von $h(X^p)$. Hieraus ergibt sich, dass $h(X^p)$ Vielfaches von f ist, es existiert also ein $g \in \mathbb{Z}[X]$ mit $h(X^p) = f \cdot g$. Reduziert modulo p gilt $\overline{f} \cdot \overline{g} = \overline{h}^p$ in $\mathbb{F}_p[X]$. Jede Nullstelle von $\overline{f}$ ist auch Nulstelle von $\overline{h}$, also haben $\overline{f}$ und $\overline{h}$ gemeinsame Nullstellen in $\mathbb{F}_p$ und somit hat $X^n - \overline{1} = \overline{f} \cdot \overline{h}$ doppelte Nullstelle. Dies ist aber ein Widerspruch dazu, dass $X^n - 1$ separabel ist. □

Beweis:

a.) Ist ζ primitve n-te Einheitswurzel, so ist $\mu_n(\overline{K}) = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. ζ^k erzeugt $\mu_n(\overline{K})$ genau dann, wenn $\mathrm{ggT}(n, k) = 1$ ist.

b.) Ist $n = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ (Primfaktorzerlegung), so ist

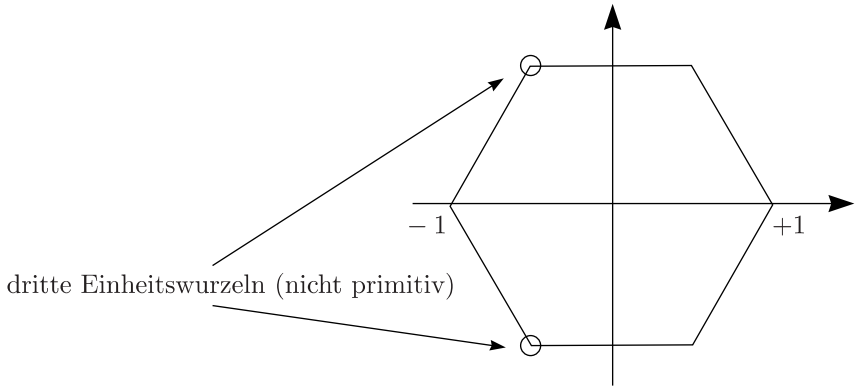
$$\varphi(n) = \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_i - 1)$$

Beispiele:

Sei $\Phi_2(X) = X + 1$, $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$.

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_2 \cdot \Phi_1} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$$

$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_3 \cdot \Phi_2 \cdot \Phi_1} = X^2 - X + 1$$



$\Phi_8(X) = X^4 + 1$

Für $n < 105$ sind alle Koeffizienten von Φ_n: 0, 1 oder -1.

Folgerung 4.9:

Das regelmäßige n-Eck ist genau dann aus 0, 1 mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.

Beweis:

Zu zeigen ist, dass ζ_n genau dann eine primitive n-te Einheitswurzel $\in K(\{0, 1\})$ ist, wenn $\varphi(n) = 2^l$ für ein $l \geq 1$. ζ_n ist primitive Einheitswurzel ist äquivalent zu $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^l$ und es gibt eine Kette $\mathbb{Q} \subset L_1 \subset \ldots \subset L_z = \mathbb{Q}(\zeta_n)$.

„⇐“: Woher kommt die Kette? Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ ist abelsch von Ordnung 2^l. Dazu gehört die Kompositionsreihe mit Faktoren $\mathbb{Z}/2\mathbb{Z}$.

Satz 19:

b.) Sei L/K zyklische Galois-Erweiterung, $\sigma \in \mathrm{Gal}(L/K)$ ein Erzeuger. Zu $\beta \in L$ mit $\mathrm{Tr}_{L/K}(\beta) = 0$ gibt es $\alpha \in L$ mit $\beta = \alpha - \sigma(\alpha)$. $(n := [L : K])$

Beweis:

b.) Sei $\gamma \in L$ mit $\mathrm{Tr}_{L/K}(\gamma) \neq 0$ und

$$\alpha := \frac{1}{\mathrm{Tr}_{L/K}(\gamma)} \left[\beta\sigma(\gamma) + (\beta + \sigma(\beta))\sigma^2(\gamma) + \ldots + (\beta + \sigma(\beta) + \ldots + \gamma^{n-1}(\beta)\sigma^{n-1}(\gamma))\right]$$

$$\Rightarrow \sigma(\alpha) = \frac{1}{\mathrm{Tr}_{L/K}(\gamma)} \left[\sigma(b)\sigma^2(\gamma) + \sigma(b) + \sigma^2(\beta)\sigma^3(\gamma) + \ldots + (\sigma(\beta) + \ldots + \sigma^{n-1}(\beta)\sigma^n(\gamma))\right]$$

$$\Rightarrow (\alpha - \sigma(\alpha)) \cdot \mathrm{Tr}_{L/K}(\gamma) = \beta\sigma(\gamma) + \beta\sigma^2(\gamma) + \ldots + \beta\sigma^{n-1}(\gamma) - \underbrace{(\sigma(\beta) + \ldots + \sigma^{n-1}(\beta))}_{=-\beta}\gamma = \beta\mathrm{Tr}_{L/K}(\gamma)$$

Folgerung 4.13:

Sei L/K zyklische Galois-Erweiterung.

a.) Ist $\mathrm{char}(K)$ kein Teiler von $n = [L : K]$ und enthält K eine primitive n-te Einheitswurzel ζ, so gibt es ein primitives Element $\alpha \in L$, so dass das Minimalpolynom von α über K die Form $X^n - \gamma$ hat für ein $\gamma \in K$ (Kummer-Erweiterung).

b.) Ist $\mathrm{char}(K) = [L : K] = p$, so gibt es ein Primelement α mit Minimalpolynom $X^p - X - \gamma$ für ein $\gamma \in K$ (Artin-Schreier-Erweiterungen).

Beweis:

a.) Es ist $N_{L/K}(\zeta) = \zeta^n = 1 = N_{L/K}(\zeta^{-1})$. Nach Satz 19 gibt es ein $\alpha \in L$ mit $\sigma(\alpha) = \zeta \cdot \alpha$. Hieraus folgt $\sigma^i(\alpha) = \zeta^i\alpha$ für $i = 0, \ldots, n-1$. Also hat das Minimalpolynom von α über K n verschiedene Nullstellen. Daraus folgt $L = K(\alpha)$. Außerdem ist $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n\zeta^n = \alpha^n$ und damit $\gamma := \alpha^n \in K$. Also ist das Minimalpolynom von α gegeben durch $X^n - \gamma$.

b.) Es gilt $\mathrm{Tr}_{L/K} = 1 + \ldots + 1 = p = 0$ wegen $\mathrm{char}(K) = p$. Nach Satz 19 (b) gibt es ein $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1$. Hieraus ergibt sich $\sigma^i(\alpha) = \alpha + i$ für $i = 0, \ldots, n-1$ und $K(\alpha) = L$.

$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha$

Also ist $\alpha^p - \alpha =: \gamma \in K$ und $X^p - X - \gamma$ ist ein Minimalpolynom von α. □

Proposition 4.14:

Sei L/K einfache Körpererweiterung, $L = K(\alpha)$.

a.) Ist α Nullstelle eines Polynoms $X^n - \gamma$ für ein $\gamma \in K$ und enthält K eine primitive n-te Einheitswurzel ζ, so ist L/K galoisch, $\mathrm{Gal}(L/K)$ zyklisch und $d := [L : K]$ ist Teiler von n mit $a^d \in K$. $X^d - \alpha^d$ ist Minimalpolynom von α.

b.) Ist $\mathrm{char}(K) = p > 0$ und $\alpha \in L \setminus K$ Nullstelle eines Polynoms $X^p - X - \gamma$ für ein $\gamma \in K$, so ist L/K galoisch und $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$.

Beweis:

a.) Die Nullstellen von $X^n - \gamma$ sind $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$. Das Polynom zerfällt vollständig und die Nullstellen erzeugen L, also ist L Zerfällungskörper von $X^n - \gamma$ und damit normal. Da das Polynom keine doppelte Nullstelle besitzt, ist L außerdem separabel, also galoisch. Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(\alpha) = \zeta^{\nu(\sigma)} \cdot \alpha$ für ein $\nu(\sigma) \in \mathbb{Z}/n\mathbb{Z}$. $\sigma \mapsto \nu(\sigma)$ ist injektiver Gruppenhomomorphismus $\mathrm{Gal}(L/K) \mapsto \mathbb{Z}/n\mathbb{Z}$, da $\mathrm{Kern}(\sigma) = \mathrm{id}$. Also ist $\mathrm{Gal}(L/K)$ zyklisch, da sie eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}$ ist. Somit ist $d = [L : K]$ Teiler von n. Für $\sigma \in \mathrm{Gal}(L/K)$ ist

$\sigma(\alpha^d) = (\zeta^{\nu(\sigma)})^d \cdot \alpha^d = \alpha^d \Rightarrow \alpha^d \in K$

$X^d - \alpha^d$ ist Minimalpolynom, da $L = K(\alpha)$ und $[K(\alpha) : K] = d$.

b.) Für $i \in \mathbb{F}_p$ ist

$(\alpha + i)^p - (\alpha + i) - \gamma = \alpha^p + i^p - \alpha - i - \gamma = \alpha^p - \alpha - \gamma = 0$ da $i^p = i$

Dies gilt nach Voraussetzung, weil α Nullstelle des Polynoms ist. $X^p - X - \gamma$ hat p verschiedene Nullstellen in L, also ist L Zerfällungskörper von $X^p - X - \gamma$ und L/K ist separabel. Außerdem folgt $\mathrm{Gal}(L/K) = \mathbb{Z}/p\mathbb{Z}$. □

Kapitel 5

Auflösung von Gleichungen durch Radikale

Definition 4.15:

Sei K ein Körper.

a.) Eine einfache Körpererweiterung $L = K(\alpha)$ heißt **elementare** (oder **einfache**) **Radikalerweiterung**. wenn entweder

i.) α ist eine Einheitswurzel.

ii.) α ist Nullstelle von $X^n - \gamma$ für ein $\gamma \in K$ und $\mathrm{char}(K) \nmid n$.

iii.) α ist Nullstelle von $X^p - X - \gamma$ für ein $\gamma \in K$ und $\mathrm{char}(K) = p$.

b.) Eine endliche Körpererweiterung L/K heißt **Radikalerweiterung**, wenn es eine Körpererweiterung L'/L gibt und eine Kette $K = L_0 \subset L_1 \subset \ldots \subset L_m = L'$ von Zwischenkörpern, so dass L_{i+1}/L_i elementare Radikalerweiterung ist für $i = 0, \ldots, n-1$.

c.) Ist $f \in K[X]$ separabel, nicht konstant, so heißt die Gleichung $f(X) = 0$ durch **Radikale auflösbar**, wenn der Zerfällungskörper von f eine Radikalerweiterung ist.

Beispiel:

Sei $K = \mathbb{Q}$ und $f(X) = X^3 - 3X + 1$. Behauptung: Ist α Nullstelle von f, so ist $O(\alpha)$ Zerfällungskörper von f, hat also Grad 3 über $\mathbb{Q}$. $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist **keine** einfache Radikalerweiterung! Die Nullstellen von f sind:

$$\alpha_1 = \exp\left(\frac{2\pi \mathrm{i}}{9}\right) + \exp\left(\frac{16\pi \mathrm{i}}{9}\right), \; \alpha_2 = \exp\left(\frac{8\pi \mathrm{i}}{9}\right) + \exp\left(\frac{10\pi \mathrm{i}}{9}\right) \text{ und } \alpha_3 = \exp\left(\frac{14\pi \mathrm{i}}{9}\right) + \exp\left(\frac{4\pi \mathrm{i}}{9}\right)$$

$$\alpha_1^2 = \exp\left(\frac{4\pi \mathrm{i}}{9}\right) + \exp\left(\frac{14\pi \mathrm{i}}{9}\right) + 2 = \alpha_3 + 2$$

Also liegt α_3 in der von α_1 erzeugten Körpererweiterung $\mathbb{Q}(\alpha_1)$ drin. Damit ist auch $\alpha_2 = -\alpha_1 - \alpha_3 \in \mathbb{Q}(\alpha_1)$.

Satz 20:

Sei K ein Körper und $f \in K[X]$ separabel, nicht konstant.

a.) Die Gleichung $f(X) = 0$ ist genau dann durch Radikale auflösbar, wenn ihre Galoisgruppe G auflösbar ist. (Also hat G Normalreihe $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$ mit G_i/G_{i+1} abelsch.)

b.) Eine endliche Körpererweiterung L/K ist genau dann Radikalerweiterung, wenn es eine endliche Galoiserweiterung L'/K gibt mit $L \subseteq L'$, so dass $\mathrm{Gal}(L'/K)$ auflösbare Gruppe ist.

Beispiel:

$X^5 - 4X + 2$ hat Galoisgruppe S_5 und ist deshalb nicht durch Radikale auflösbar. $S_5 \supset A_5 \supset \{e\}$ ist Kompositionsreihe. Nach Jordan-Möller tritt A_5 in jeder Kompositionsreihe für S_5 als Faktorgruppe auf.