Algebra I

Christian Becker[1] Patrick Hagemann[2]

5. November 2000

[1]eMail: mail@chr-becker.de
[2]eMail: mail@phagemann.de

Dieses Dokument basiert auf der Mitschrift der Vorlesung *Algebra I* von Herrn Prof. Dr. Klaus Hulek an der Universität Hannover im Wintersemester 1999/2000.

Leider können wir die vollständige Korrektheit dieses Dokumentes nicht garantieren. Sollten Fehler entdeckt werden, wären wir dankbar, wenn man einem der Autoren eine entsprechende Nachricht zukommen ließe.

Inhaltsverzeichnis

Kapitel 1

Einführung

Konstruktionen mit Zirkel und Lineal

Delisches Problem Verdopple einen gegebenen Würfel mit Zirkel und Lineal.

Dreiteilung des Winkels Dreiteilung eines gegebenen Winkels mit Zirkel und Lineal.

Konstruktion des regulären n-Ecks Mit Zirkel und Lineal

Quadratur des Kreises Konstruiere mit Zirkel und Lineal zu einem gegebenen Kreis ein Quadrat mit demselben Flächeninhalt.

(Unmöglich, da π transzendent ist, d. h. π ist nicht Nullstelle eines Polynoms mit rationalen Koeffizienten. Lindemann (1882) (1852-1939))

- *Descartes* (1596-1650): Einführung von Koordinaten.
- *Gauß* (1777-1855): Gibt ein Kriterium an, wann ein reguläres n-Eck konstruierbar ist (z. B. für $n = 3, 4, 5, 6, 8, 10, \ldots$ lösbar; $n = 7, 9, \ldots$ nicht lösbar).
- *Hermite* (1822-1902)

Auflösung von Gleichungen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x_1 + a_0 = 0 \quad (a_0, \ldots, a_n \in \mathbb{C})$$

(i) $ax^2 + bx + c = 0 \quad (a \neq 0)$

$$x_{1,2} = -\frac{b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$b^2 - 4ac \begin{cases} > 0 & \Leftrightarrow 2 \text{ reelle Lösungen,} \\ = 0 & \Leftrightarrow 1 \text{ reelle Lösung,} \\ < 0 & \Leftrightarrow 2 \text{ komplexe Lösungen.} \end{cases}$$

(ii) $x^3 + bx^2 + cx + d = 0$

$$y := x + \frac{b}{3} \tag{1.1.a}$$

Einsetzen ergibt:

$$y^3 + py + q = 0 \tag{1.1.b}$$

mit

$$2q = \frac{2b^3}{27} - \frac{bc}{3} + d, \quad 3p = \frac{3c - b^2}{3}$$

Man setze

$$u := \sqrt[3]{-q + \sqrt{q^2 + p^3}}, \quad v := \sqrt[3]{-q - \sqrt{q^2 + p^3}} \quad \text{mit} \quad uv = -p.$$

$$\varepsilon_1 := -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \varepsilon_2 := -\frac{1}{2} - i\frac{\sqrt{3}}{2} \quad (\varepsilon_i^3 = 1)$$

Lösungen von (1.1.b):

$$y_1 = u + v, \quad y_2 = \varepsilon_1 u + \varepsilon_2 v, \quad y_3 = \varepsilon_2 u + \varepsilon_1 v.$$

$p, q \in \mathbb{R}$: $\quad D = p^2 + q^3$

1	reelle Lösung		D	$>$	0
2	reelle Lösungen	$\Leftrightarrow$	D	$=$	0
3	reelle Lösungen		D	$<$	0

Formeln von Cardano (1501-1576)

(iii) Gleichungen 4-ten Grades: *Ferrari*

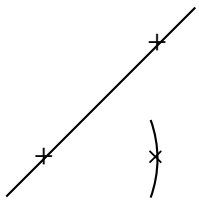
(iv) Gleichungen vom Grad $n \geq 5$:

Abel (1802-1829): die allgemeine Gleichung vom Grad $n \geq 5$ ist nicht explizit auflösbar.

Galois (1811-1832) : Hat die Bedeutung der Gruppentheorie erkannt (Galoistheorie).

1.1 Mathematisierung des Problems

$\mathcal{M}$: Menge von Punkten in der Ebene ($\mathbb{R}^2$)



$G(\mathcal{M}) :=$ Menge der Geraden, die durch 2 Punkte von $\mathcal{M}$ bestimmt sind.

$K(\mathcal{M}) :=$ Menge der Kreise, deren Mittelpunkt ein Punkt von $\mathcal{M}$ ist,und deren Radius der Abstand zweier Punkte von $\mathcal{M}$ ist.

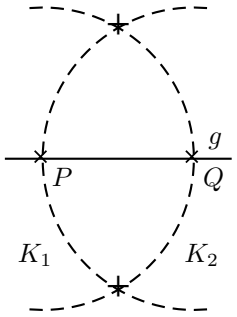
Operationen:

(O1) Schnitt von Geraden in $G(\mathcal{M})$

(O2) Schnitt einer Geraden in $G(\mathcal{M})$ mit einem Kreis in $K(\mathcal{M})$

(O3) Schnitt zweier Kreise in $K(\mathcal{M})$

$$\mathcal{M} = \{P, Q\}, \quad G(\mathcal{M}) = \{g\}, \quad K(\mathcal{M}) = \{K_1, K_2\}$$



$\mathcal{M}'$:= Menge aller Punkte, die man aus $\mathcal{M}$ durch die Operationen (O1) - (O3) erhält.

$\mathcal{M} \subset \mathcal{M}'$**.**

Wir definieren induktiv die folgenden Mengen

$$\begin{aligned} \mathcal{M}_0 &:= \mathcal{M} \\ \mathcal{M}_{n+1} &:= (\mathcal{M}_n)' \end{aligned}$$

Dies ergibt eine Inklusionskette:

$$\mathcal{M}_0 \subset \mathcal{M}_1 \subset \mathcal{M}_2 \subset \cdots \subset \mathcal{M}_n \subset \cdots \quad (\mathcal{M}_i \subset \mathbb{R}^2, i \in \mathbb{N}_0)$$

$$\boxed{\hat{\mathcal{M}} := \bigcup_{n \geq 0} \mathcal{M}_n}, \quad (\hat{\mathcal{M}} \subset \mathbb{R}^2)$$

Definition 1.1
$\hat{\mathcal{M}}$ heißt die Menge der Punkte, die sich aus $\mathcal{M}$ mit Hilfe von Zirkel und Lineal konstruieren lassen.

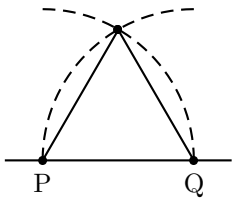
Bemerkung 1.2

(i) Jeder Punkt aus $\hat{\mathcal{M}}$ ist in endlich vielen Schritten konstruierbar.

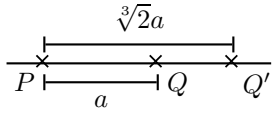
(ii) $(\hat{\mathcal{M}})' = \hat{\mathcal{M}}$

Beispiel 1.3

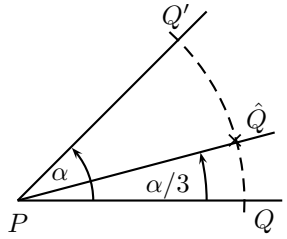
(i) **Konstruktion des gleichseitigen Dreiecks:** $\mathcal{M} = \{P; Q\}$



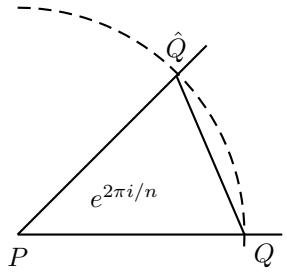
(ii) **Delisches Problem:** $\mathcal{M} = \{P, Q\}, |PQ| = a. \quad Q' \in \hat{\mathcal{M}}$?



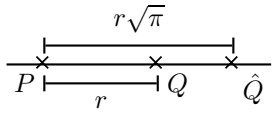
(iii) **Dreiteilung des Winkels:** $\mathcal{M} = \{P, Q, Q'\}$. Können annehmen, dass $|PQ| = |PQ'|$. $\hat{Q} \in \hat{\mathcal{M}}$?



(iv) **Konstruktion des regulären n-Ecks:** $\hat{Q} \in \hat{\mathcal{M}}$?



(v) **Quadratur des Kreises:** $\mathcal{M} = \{P, Q\}, |PQ| = r$. $\hat{Q} \in \hat{\mathcal{M}}$?



1.2 Algebraisierung des Problems

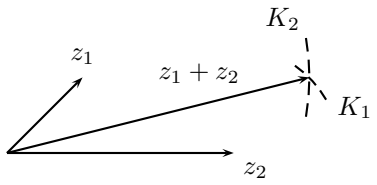
$\mathcal{M} \subset \mathbb{R}^2 = \mathbb{C}$ mit $z = (x, y) = x + iy$ für $z \in \mathbb{C}$, $x, y \in \mathbb{R}$
Können annehmen, dass $P, Q \in \mathcal{M}$ mit

$$P = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad bzw. \quad P, Q = 0, 1 \in \mathbb{C}$$

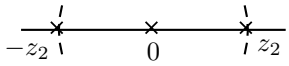
Satz 1.4
Es sei $\mathcal{M}$ eine Teilmenge von $\mathbb{R}^2 = \mathbb{C}$ mit $0, 1 \in \mathcal{M}$. Dann ist $\hat{\mathcal{M}}$ ein Unterkörper von $\mathbb{C}$.

Beweis. $z_1, z_2 \in \hat{\mathcal{M}}$. Zu zeigen: $z_1 + z_2, z_1 - z_2, z_1 z_2, \frac{z_1}{z_2}$ $(z_2 \neq 0)$ $\in \hat{\mathcal{M}}$

(i) $\underline{z_1 + z_2}$: K_1 : Mittelpunkt z_2, Radius $|z_1|$ K_2 : Mittelpunkt z_1, Radius $|z_2|$



(ii) $\underline{z_1 - z_2}$: genügt zu zeigen, dass $-z_2 \in \hat{\mathcal{M}}$.



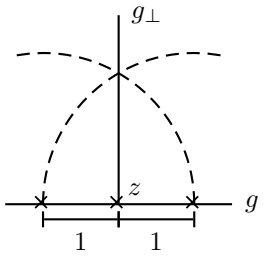
(iii) $\underline{z_1 z_2}$: $r \geq 0, \varphi \in [0, 2\pi)$

$$\left.\begin{array}{rcl} z_1 & = & r_1 e^{i\varphi_1} \\ z_2 & = & r_2 e^{i\varphi_2} \end{array}\right\} \Rightarrow z_1 z_2 = r_1 r_2 e^{i(\varphi_1 + \varphi_2)}$$

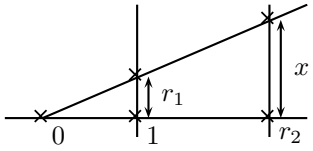
Bemerkung 1.5
$z_1, z_2 \in \hat{\mathcal{M}} \Rightarrow r_1, r_2 \in \hat{\mathcal{M}}$

(a) $\underline{r_1 r_2 \in \hat{\mathcal{M}}}$:

Hilfsüberlegung: Man kann für einen Punkt z auf der Geraden g die Senkrechte zu g durch z konstruieren.



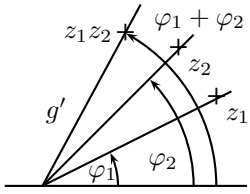
$r_2 > 1, \quad x \in \hat{\mathcal{M}}$



Nach dem Strahlensatz gilt

$$\frac{x}{r_1} = \frac{r_2}{1} \Rightarrow x = r_1 r_2$$

Betrachten nun



Trage auf der Geraden g' die Länge $r_1 r_2$ auf.

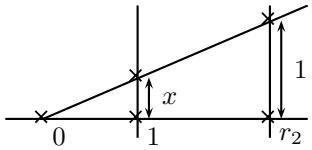
$\Rightarrow z_1 z_2 \in \hat{\mathcal{M}}$

(iv) $\frac{z_1}{z_2}$: Es genügt zu zeigen, dass $\frac{1}{z_2} \in \hat{\mathcal{M}}$.

Es gilt

$$\frac{1}{z_2} = \frac{1}{r_2} e^{-i\varphi_2}.$$

Da man die Spiegelung eines Winkels an einer Achse leicht mit Zirkel und Lineal durchführen kann, soll hier nur gezeigt werden, dass $\frac{1}{r_2} \in \hat{\mathcal{M}}$. Dies ergibt sich mit folgender Konstruktion ($r_2 > 1$):



Strahlensatz $\Rightarrow x = \frac{1}{r_2}$

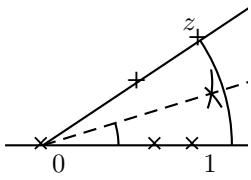
□

Satz 1.6
$z \in \hat{\mathcal{M}} \Rightarrow \pm\sqrt{z} \in \hat{\mathcal{M}}$.

Definition 1.7
Ein Körper $K \in \mathbb{C}$ heißt *quadratisch abgeschlossen*, falls mit $z \in K$ auch $\pm\sqrt{z} \in K$.

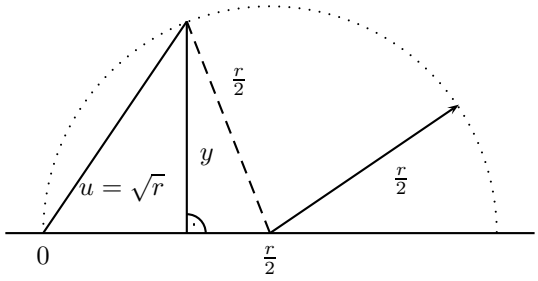
Folgerung 1.8
Der Körper $\hat{\mathcal{M}}$ ist quadratisch abgeschlossen.

Beweis. (i) Winkel können in $\hat{\mathcal{M}}$ halbiert werden. $z = re^{i\varphi} \in \hat{\mathcal{M}}$.



(ii) $z \in \hat{\mathcal{M}} \Rightarrow r \in \hat{\mathcal{M}}$

Annahme: $\frac{r}{2} > 1$



Pythagoras:

$$u^2 = 1^2 + y^2 \Rightarrow u = \sqrt{1+y^2}$$

$$\frac{r^2}{4} = y^2 + \left(\frac{r}{2} - 1\right)^2 = y^2 + \frac{r^2}{4} - r + 1 \Rightarrow r = 1 + y^2$$

Daraus folgt

$$\sqrt{r} = \sqrt{1+y^2} = u \in \hat{\mathcal{M}}.$$

Annahme: $\frac{r}{2} \leq 1$

Wähle dann ein $N \in \mathbb{N}$ mit $N^2 \frac{r}{2} > 1$. Es ist dann $N^2 r \in \hat{\mathcal{M}} \overset{\text{obiges Argument}}{\Rightarrow}$ $\sqrt{N^2 r} = N\sqrt{r} \in \hat{\mathcal{M}} \overset{N \in \hat{\mathcal{M}}}{\Rightarrow} \sqrt{r} \in \hat{\mathcal{M}}$.

□

Adjunktion

Lemma 1.9
Es sei K ein Körper, $K_i \subset K$, $i \in I$ Unterkörper. Dann ist der Durchschnitt $\bigcap_{i\in I} K_i$ wieder ein Unterkörper von K.

Beweis. $x, y \in \bigcap_{i\in I} K_i \Rightarrow x, y \in K_i$ für alle i

$$\begin{aligned} &\Rightarrow \quad x \pm y, xy, \tfrac{x}{y}\ (y \neq 0) \quad \in K_i \text{ für alle } i \\ &\Rightarrow \quad x \pm y, xy, \tfrac{x}{y}\ (y \neq 0) \quad \in \bigcap_{i\in I} K_i. \end{aligned}$$

□

Definition 1.10
Es sei $X \neq 0$, $X \subset K$ eine Teilmenge eines Körpers K.

$$(X) := \bigcap_{\substack{K' \subset K \text{ ist Körper} \\ K' \supset X}} K'.$$

Dann heißt (X) der von der Menge X erzeugte Unterkörper von K.

Bemerkung 1.11
(X) ist der kleinste Unterkörper von K, der die Menge X enthält.

Definition 1.12
$K_0(X) := (K_0 \cup X)$.
Man sagt, dass $K_0(X)$ aus K_0 durch *Adjunktion* der Menge X entsteht.

Beispiel 1.13

(i) $K = \mathbb{C}$, $K_0 = \mathbb{R}$, $X = \{i\}$; $\quad K_0(X) = \mathbb{R}(i) = \mathbb{C}$

(ii) $K = \mathbb{C}$, $K_0 = \mathbb{Q}$, $X = \{i\}$; $\quad K_0(X) \subsetneq \mathbb{C}$ (Körper der algebraischen Zahlen)

Schreibweise: $X = \{x_1, \ldots, x_n\}$, $\quad K_0(X) := K_0(x_1, \ldots, x_n)$

Bemerkung 1.14
$K_0(x_1, \ldots, x_n) = (((K_0(x_1))(x_2))(x_3)\ldots)(x_n)$

Bemerkung 1.15
Jeder Unterkörper von $\mathbb{C}$ enthält $\mathbb{Q}$.

Beweis. Denn: $K \subset \mathbb{C}$ Unterkörper $\Rightarrow 0, 1 \in K \Rightarrow n \in K$ für alle $n \in \mathbb{Z} \Rightarrow \frac{n}{m} \in K \quad n, m \in \mathbb{Z}, m \neq 0 \Rightarrow \mathbb{Q} \subset K$. □

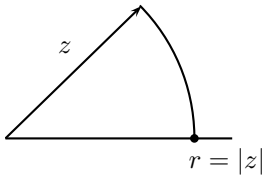
Damit: $X \subset \mathbb{C} \Rightarrow (X) = \mathbb{Q}(X)$

Zurück zu $\mathcal{M} \subset \mathbb{C}$, $0, 1 \in \mathcal{M}$.

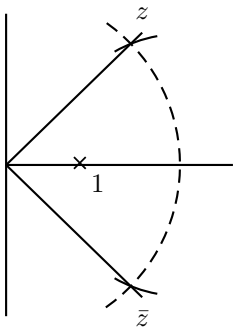
$$\bar{\mathcal{M}} := \{\bar{z}; z \in \mathcal{M}\} \quad \text{mit } z = re^{i\varphi}, \bar{z} = re^{-i\varphi}$$

Lemma 1.16
Es sei $z \in \mathcal{M}, z = x + iy$. Dann ist $\bar{z}, x, y, |z| \in \hat{\mathcal{M}}$.

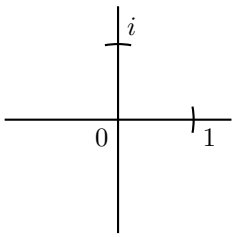
Beweis. (i) $z \in \mathcal{M} \Rightarrow |z| = r \in \hat{\mathcal{M}}$



(ii) $\bar{z} \in \hat{\mathcal{M}}$



(iii) $i \in \hat{\mathcal{M}}$



(iv) $x = \frac{1}{2}(z + \bar{z}) \in \hat{\mathcal{M}}, \quad y = \frac{1}{2i}(z - \bar{z}) \in \hat{\mathcal{M}}$

□

Definition 1.17

$$K_0 := \left(\mathcal{M} \cup \bar{\mathcal{M}}\right) = \mathbb{Q}\left(\mathcal{M} \cup \bar{\mathcal{M}}\right) \subset \hat{\mathcal{M}}, \quad \text{da } \mathcal{M}, \bar{\mathcal{M}} \subset \hat{\mathcal{M}}$$

Lemma 1.18

$$\bar{K_0} = K_0$$

Beweis. $\bar{K}_0 = \{\bar{z}; z \in K_0\} \subset \mathbb{C}$ ist ein Unterkörper, da mit $\bar{z}_1, \bar{z}_2 \in \bar{K}_0$ ist auch

$$\bar{z}_1 \pm \bar{z}_2 = \overline{z_1 \pm z_2} \in \bar{K}_0, \quad \bar{z}_1 \cdot \bar{z}_2 = \overline{z_1 \cdot z_2} \in \bar{K}_0, \quad \frac{\bar{z}_1}{\bar{z}_2} = \overline{\left(\frac{z_1}{z_2}\right)} \in \bar{K}_0.$$

Da K_0 der kleinste Körper ist, der $\mathcal{M} \cup \bar{\mathcal{M}}$ enthält, und auch $\bar{K}_0$ diese Eigenschaft hat, folgt:

$$\left.\begin{array}{c} K_0 \subset \bar{K}_0 \\ \bar{K}_0 \subset \bar{\bar{K}}_0 = K_0 \end{array}\right\} \Rightarrow K_0 = \bar{K}_0$$

□

Sei $L \subset \mathbb{C}$ ein Unterkörper mit $L = \bar{L}$ (später $L := K_0 = \mathbb{Q}\left(\mathcal{M} \cup \bar{\mathcal{M}}\right)$)

$G(L) :=$ Menge der Geraden durch Punkte von L

$K(L) :=$ Menge der Kreise, deren Mittelpunkt ein Punkt von L ist und deren Radius der Abstand zweier Punkte in L ist.

Lemma 1.19
Es seien $g, g' \in G(L), z = g \cap g'$. Dann ist $z \in L$.

Beweis.

$$\begin{array}{rrcl} g: & z' & = & z_0 + \lambda_1 \underbrace{(z_2 - z_0)}_{=:z_1 \in L}, \quad \lambda_1 \in \mathbb{R} \\ g: & z' & = & z_0 + \lambda_1 z_1; \quad z_0, z_1 \in L, \lambda_1 \in \mathbb{R} \\ g': & z' & = & z_0' + \lambda_2 z_1'; \quad z_0', z_1' \in L, \lambda_2 \in \mathbb{R} \end{array}$$

$$z = g \cap g': \qquad z_0 + \lambda_1 z_1 = z_0' + \lambda_2 z_1' \tag{1.1.c}$$

Zerlegung von (1.1.c) in Real- und Imaginärteil ergibt

$$\begin{array}{rcl} x_0 + \lambda_1 x_1 & = & x_0' + \lambda_2 x_1' \\ iy_0 + \lambda_1 iy_1 & = & iy_0' + \lambda_2 iy_1' \end{array} \tag{1.1.d}$$

$$\begin{array}{rcl} x_0 & = & \frac{1}{2}(z_0 + \bar{z}_0) \in L \text{ (da } z_0 \in L, \bar{z}_0 \in \bar{L} = L) \\ iy_0 & = & \frac{1}{2}(z_0 - \bar{z}_0) \in L \end{array}$$

Auf gleiche Art erkennt man, dass gilt $x_1, x_1', iy_1, iy_1', iy_0' \in L$.

(1.1.d) ist ein lineares Gleichungssystem für λ_1, λ_2. Da alle Koeffizienten in L sind, ist auch $\lambda_1, \lambda_2 \in L$.

$$\Rightarrow z = z_0 + \lambda z_1 \in L$$

□

Lemma 1.20
Es sei z der Schnittpunkt einer Geraden aus $G(L)$ mit einem Kreis aus $K(L)$. Dann gibt es ein $\omega \in L$ mit $z \in L(\sqrt{\omega})$.

Beweis. $z \in g \cap K . g \in G(L), K \in K(L)$

$$g: \qquad z_0 + \lambda z_1, \quad z_0, z_1 \in L, \lambda \in \mathbb{R}$$

K: Kreis mit Mittelpunkt $z_2 \in L$, mit Radius $r = |z_3 - z_4|; z_3, z_4 \in L$

$$r^2 = (z_3 - z_4)(\bar{z}_3 - \bar{z}_4) \in L \quad (\text{da } L = \bar{L})$$

Sei $z = x + iy \in K$. $z_2 = x_2 + iy_2$. Dann gilt:

$$\begin{aligned} &(x - x_2)^2 + (y - y_2)^2 = r^2 \\ \Leftrightarrow &(x - x_2)^2 - (iy - iy_2)^2 = r^2 \quad (x_2, y_2, iy_2, r^2 \in L) \end{aligned}$$

Sei $z \in g: \quad z = z_0 + \lambda z_1, \quad z_0, z_1 \in L, \lambda \in \mathbb{R}$

$$z \in g \cap K: \qquad \big((x_0 + \lambda x_1) - x_2\big)^2 - \big((iy_0 + \lambda i y_1) - iy_2\big)^2 = r^2 \tag{1.1.e}$$

mit $x_0, x_1, x_2, iy_0, iy_1, iy_2, r^2 \in L$.

(1.1.e) ist eine quadratische Gleichung für λ mit Koeffizienten in L. Falls der Koeffizient von λ^2 verschwindet, ist dies eine lineare Gleichung und $\lambda \in L$. Ansonsten:

$$\begin{aligned} \lambda^2 + \alpha_1 \lambda + \alpha_2 = 0 \quad \alpha_1, \alpha 2 \in L \\ \lambda_{1,2} = -\frac{\alpha_1}{2} \pm \sqrt{\Big(\frac{\alpha_1}{2}\Big)^2 - \alpha_2} \end{aligned}$$

Setze: $\omega := \big(\frac{\alpha_1}{2}\big)^2 - \alpha_2 \in L \Rightarrow \lambda_{1,2} \in L(\sqrt{\omega}) \quad (\text{da } \lambda_{1,2} = -\frac{\alpha_1}{2} \pm \sqrt{\omega}, \quad \alpha_1 \in L)$. □

Lemma 1.21
Es seien $K_0, K_1 \in K(L)$. Es sei $z \in K_0 \cap K_1 (K_0 \neq K_1)$. Dann gibt es ein $\omega \in L$ mit $z \in L(\sqrt{\omega})$.

Beweis.

$$K_0: \qquad (x - x_0)^2 - (iy - iy_0)^2 = r_0^2 \qquad x_0, iy_0, r_0^2 \in L \tag{1.1.f}$$
$$K_1: \qquad (x - x_1)^2 - (iy - iy_1)^2 = r_1^2 \qquad x_1, iy_1, r_1^2 \in L \tag{1.1.g}$$

(1.1.f) und (1.1.g) ergeben

$$a_1 x + a_2 (iy) = b \quad a_1, a_2 \in L \tag{1.1.h}$$

Es ist $(a_1, a_2) \neq (0, 0)$ sonst ist $K_0 = K_1$ oder $K_0 \cap K_1 = \emptyset$.

$\underline{a_1 \neq 0}$: (1.1.h) $\Rightarrow x = -\frac{a_2}{a_1}(iy) + \frac{b}{a_1}$;
Einsetzen in (1.1.f) ergibt quadratische Gleichung für iy mit Koeffizienten in L.

$$\left.\begin{array}{rl} \Rightarrow & iy \in L(\sqrt{\omega}) \text{ für ein } \omega \in L \\ \text{Mit (1.1.h):} & x \in L(\sqrt{\omega}) \end{array}\right\} \Rightarrow z = x + iy \quad \in L(\sqrt{\omega}).$$

□

Definition 1.22
Es sei K ein Unterkörper von L. Man sagt, dass L durch *Adjunktion* von Quadratwurzeln aus K hervorgeht, falls es Elemente $\omega_1, \ldots, \omega_n \in L$ gibt mit:

$$L = K(\omega_1, \ldots, \omega_n),$$

sodass:

(i) $\omega_1^2 \in K$

(ii) $\omega_{i+1}^2 \in K(\omega_1, \ldots, \omega_i) \quad (i \geq 2)$

Satz 1.23
Es sind äquivalent:

(i) $z \in \hat{\mathcal{M}}$

(ii) *z ist in einem Unterkörper L von $\hat{\mathcal{M}}$ enthalten, der aus $K_0 = \mathbb{Q}\left(\mathcal{M} \cup \bar{\mathcal{M}}\right)$ durch Adjunktion von Quadratwurzeln entstanden ist.*

Beweis. (ii)⇒(i) Wir wissen $K_0 \subset \hat{\mathcal{M}}$. Da $\hat{\mathcal{M}}$ quadratisch abgeschlossen ist, folgt $L \subset \hat{\mathcal{M}}$.

(i)⇒(ii) $z \in \mathbb{C}$ entstehe aus K_0 durch Operationen (O1-O3)

$$\begin{aligned} &\overset{(1.19)-(1.21)}{\Rightarrow} && z \in K_0(\sqrt{\omega}) \text{ für ein } \omega \in K_0 \\ &\Rightarrow && z \in \underbrace{K_0\left(\sqrt{\omega}, \sqrt{\bar{\omega}}\right)}_{=:K_1}. \text{ Es ist } \hat{\omega} \in K_0 \quad (\text{da } K_0 = \bar{K}_0) \end{aligned}$$

Jetzt argumentiere man induktiv. □

Setze

$$\begin{aligned} \sqrt{K_0} &:= \{\pm\omega; \omega^2 \in K_0\} \\ K_1 &:= K_0(\sqrt{K_0}) \end{aligned}$$

Induktiv:

$$\begin{aligned} K_{n+1} &:= K_0(\sqrt{K_n}) \\ K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots & \end{aligned}$$

Satz 1.24

$$\hat{\mathcal{M}} = \bigcup_{n \geq 0} K_n$$

Beweis. „⊃“: Gilt, da $\hat{\mathcal{M}}$ quadratisch abgeschlossen ist.

„⊂“: Sei $t \in \hat{\mathcal{M}} \overset{(1.24)}{\Longrightarrow} z \in L$ mit $L = K_0(\omega_1, \ldots, \omega_n)$ mit $\omega_1^2 \in K_0, \omega_i^2 \in K_0(\omega_1, \ldots, \omega_{i-1}) \Rightarrow z \in K_n$. □

Korollar 1.25
$\hat{\mathcal{M}}$ ist der Durchschnitt aller quadratisch abgeschlossenen Unterkörper von $\mathbb{C}$, die K_0 enthalten.

Beweis. „⊂“: $\hat{\mathcal{M}} = \bigcup_{n \geq 0} K_n \Rightarrow \hat{\mathcal{M}}$ ist in jedem Körper enthalten, der K_0 umfasst und quadratisch abgeschlossen ist.

„⊃“: Folgt, da $\hat{\mathcal{M}}$ selbst K_0 enthält und quadratisch abgeschlossen ist. □

(i) **Delisches Problem** (s. a. Seite 7)
Ist $\sqrt[3]{2}$ in einem Körper enthalten, der aus $\mathbb{Q}$ durch Adjunktion von Quadratwurzeln entsteht?

(ii) **Winkeldreiteilung** (s. a. Seite 7)
Ist $e^{i\frac{\varphi}{3}}$ in einem Körper enthalten, der aus $\mathbb{Q}\left(e^{i\varphi}\right)$ durch Adjunktion von Quadratwurzeln entsteht?

Im Allgemeinen nein, in manchen Fällen ja.

Beispiel 1.26
$\varphi = \frac{3}{2}\pi, \quad \varphi/3 = \frac{\pi}{2}$
$e^{i\varphi/3} = e^{i\frac{\pi}{2}} = i$. Es ist stets $i \in \hat{\mathcal{M}}$.

(iii) **Kreisquadratur** (s. a. Seite 7)
Ist $\sqrt{\pi}$ in einem Körper enthalten, der aus $\mathbb{Q}$ durch Adjunktion von Quadratwurzeln hervorgeht? (Nein)

Kapitel 2

Körpererweiterungen (Teil 1)

$K \subset L$; K, L seien Körper, K sei ein Unterkörper von L. Man spricht auch davon, dass L eine *Körpererweiterung* von K ist.

Schreibweise: L/K

$K[X] :=$ Polynomring der Polynome mit der Unbestimmten X und Koeffizienten in K.

$$K[X] \ni f = f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_0, \ldots, a_n \in K$$

Definition 2.1
Ein Element $x \in L$ heißt *algebraisch über* K, wenn es ein Polynom $f \in K[X], f \neq 0$, gibt, sodass $f(x) = 0$. Ansonsten heißt x *transzendent über* K.

Beispiel 2.2

(i) $K = \mathbb{Q}, L = \mathbb{C}; x = \sqrt[3]{2}$.
x ist algebraisch über $\mathbb{Q}$: $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Dann ist $f(\sqrt[3]{2}) = 0$.

(ii) $K = \mathbb{Q}, L = \mathbb{C}; x = \pi$
π ist transzendent über $\mathbb{Q}$ (schwierig zu beweisen)

Spezialfall: $K = \mathbb{Q}, L = \mathbb{C}$
Man nennt dann die über $\mathbb{Q}$ algebraischen (transzendenten) Zahlen einfach die *algebraischen* (*transzendenten*) Zahlen.

Satz 2.3
Die Menge der algebraischen Zahlen ist abzählbar.

Beweis. $\mathbb{Q}_n[X] = \{P \in \mathbb{Q}[X], \deg P \leq n\}$

$$\begin{aligned}
& \mathbb{Q}_n[X] = \{a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0; a_0, \ldots, a_n \in \mathbb{Q}\} \\
\Rightarrow \quad & \mathbb{Q}_n[X] \cong \mathbb{Q}^{n+1} \\
\Rightarrow \quad & \mathbb{Q}_n[X] \text{ ist abzählbar} \\
\Rightarrow \quad & \mathbb{Q}[X] = \textstyle\bigcup_{n \geq 0} \mathbb{Q}_n[X] \text{ ist abzählbar} \\
\Rightarrow \quad & \text{(da jedes Polynom endlich viele Nullstellen hat)} \\
& \text{Die algebraischen Zahlen sind abzählbar.}
\end{aligned}$$

□

Folgerung 2.4
Jedes Intervall $[a,b], a<b$ enthält überabzählbar viele transzendente Zahlen.

Definition 2.5
Ein Polynom heißt *normiert*, falls der Leitkoeffizient 1 ist, d. h. falls

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

Lemma 2.6
L/K sei eine Körpererweiterung. $x \in L$ sei algebraisch über K. Dann gibt es genau ein normiertes Polynom f minimalen Grades mit $f(x) = 0$.

Definition 2.7
Dieses Polynom f heißt das *Minimalpolynom* von x.

Beweis. Es sei $g(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, a_n \neq 0$ ein Polynom minimalen Grades mit $g(x) = 0$.

$$f(X) = \frac{1}{a_n}g(X) = X^n + \cdots + \frac{a_1}{a_n}X + \frac{a_0}{a_n}$$

Es gilt $f(x) = 0$. Es sei $h(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ ein weiteres normiertes Polynom mit $h(x) = 0$.

$$\Rightarrow \underbrace{(f-h)}_{\neq 0}(x) = f(x) - h(x) = 0 - 0 = 0$$

Aber $\deg(f-h) < n$. Dies ist ein Widerspruch zur Wahl von g als Polynom minimalen Grades mit der Eigenschaft $g(x) = 0$. □

Definition 2.8
Der *Grad* von x über K wird wie folgt definiert:

$$[x:K] := \begin{cases} \deg f & \text{, falls } x \text{ algebraisch über } K \text{ und } f \text{ das Minimalpolynom ist} \\ \infty & \text{, sonst} \end{cases}$$

Beispiel 2.9

(i) $K = \mathbb{Q}; x = \sqrt[3]{2}, [x:\mathbb{Q}] \leq 3$
Denn: $f(X) = X^3 - 2, f(\sqrt[3]{2}) = 0$

(ii) $[x:K] = 1 \Leftrightarrow x \in K$
$f(X) = X + a_0, a_0 \in K, \quad 0 = f(x) \Rightarrow x = -a_0 \in K$

Definition 2.10
Eine Körpererweiterung L/K heißt *algebraisch*, falls jedes Element $x \in L$ algebraisch ist über K. Ansonsten heißt die Körpererweiterung *transzendent*.

Beispiel 2.11

(i) $\mathbb{R}\,/\,\mathbb{Q}, \mathbb{C}\,/\,\mathbb{Q}$ sind transzendent, da sie überabzählbar sind.

(ii) $\mathbb{C}\,/\,\mathbb{R}$ ist algebraisch.
$z = a + ib, \quad a, b \in \mathbb{R}$

$$\begin{aligned} f(X) &= \big(X - (a+ib))(X - (a-ib)\big) \\ &= X^2 - (a+ib)X - (a-ib)X + (a+ib)(a-ib) \\ &\Rightarrow f(X) = X^2 - 2aX + (a^2+b^2) \quad \in \mathbb{R}[X] \end{aligned}$$

mit $f(z) = 0$.
Sogar:

$$[z : \mathbb{R}] = \begin{cases} 1 & \text{falls } z \in \mathbb{R} \\ 2 & \text{falls } z \notin \mathbb{R} \end{cases}$$

$K \subset L$: Körpererweiterung
Man kann L auffassen als *Vektorraum* über K.

$$\begin{aligned} + &: L \times L \to L, \quad (x, y) \mapsto x + y \\ \cdot &: K \times L \to L, \quad (\alpha, y) \mapsto \alpha \cdot y \quad (\cdot = \cdot \text{ in } L) \end{aligned}$$

Definition 2.12
Der *Grad* der Körpererweiterung L/K ist definiert als

$$[L : K] := \dim_K L$$

Beispiel 2.13

(i) $\mathbb{C} \,/\, \mathbb{R}$: $[\mathbb{C} : \mathbb{R}] = 2$. Basis: $1, i$.

(ii) $[\mathbb{R} : \mathbb{Q}] = \infty, \quad [\mathbb{C} : \mathbb{Q}] = \infty$

Satz 2.14
Es sei L ein Erweiterungskörper von K. Es gebe ein Element $x \in L$ mit $L = K(x)$. Dann gilt:

$$[K(x) : K] = [x : K].$$

Beispiel 2.15
$\mathbb{C} = \mathbb{R}(i); \quad [\mathbb{C} : \mathbb{R}] = 2 = [i : \mathbb{R}] \quad (f(X) = X^2 + 1)$

Beweis. Sei x transzendent über K. Dann ist $[x : K] = \infty$. Andererseits sind $1, x, x^2, \ldots, x^n, \ldots$ linear unabhängig über K (sonst $a_0 + a_1 X + \cdots + a_n X^n = 0, \quad a_0, \ldots, a_n \in K$).
Damit ist

$$[K(x) : K] = \dim_K K(x) = \infty$$

Es sei also x algebraisch über K. Es sei

$$n := [x : K] = \text{ Grad des Minimalpolynoms } f \text{ von } x$$

Setze

$$\tilde{K} := K + Kx + Kx^2 + \cdots + Kx^{n-1} \quad \subset \quad L.$$

Es genügt zu zeigen: $\tilde{K}$ ist ein Körper.
Dann sind wir fertig, da:

$$\dim_K \tilde{K} = n \quad \text{und} \quad \tilde{K} = K(x)$$

Letzteres gilt, da:

(i) $\tilde{K} \subset K(x)$

(ii) Ist $\tilde{K}$ ein Körper, so ist $K(x) \subset \tilde{K}$, da $K(x)$ der kleinste Körper ist, der K und x enthält.

- $y, z \in \tilde{K} \Rightarrow y \pm z \in \tilde{K}$ (klar)
- $y, z \in \tilde{K} \Rightarrow yz, \frac{y}{z} \in \tilde{K}$ $(z \neq 0)$

  (i) $\underline{yz \in \tilde{K}}$: Da

$$\begin{aligned} y &= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \quad a_i \in K \\ z &= b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}, \quad b_i \in K \end{aligned}$$

  genügt es zu zeigen: $x^i x^j \in \tilde{K}$ für alle i, j
  $\underline{i + j \leq n - 1}$: $x^i x^j = x^{i+j} \in \tilde{K}$ klar
  $\underline{i + j \geq n}$: Es sei f das Minimalpolynom von x über K. Polynomdivision mit Rest ergibt

$$x^{i+j} = g \cdot f + r \text{ mit } g, r \in K[X], \deg r \leq n - 1$$

  Einsetzen von x:

$$\begin{aligned} x^{i+j} &= \overbrace{g(x)f(x)}^{=0} + r(x) \\ \Rightarrow x^{i+j} &= r(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \tilde{K}, c_i \in K \end{aligned}$$

  (ii) Genügt: $y \neq 0, y \in \tilde{K} \overset{!}{\Rightarrow} \frac{1}{y} \in \tilde{K}$.
  y ist *algebraisch* über K:

$$1, y, y^2, \ldots, y^n \in \tilde{K} \text{ siehe (i), linear unabhängig}$$

  $\Rightarrow$ Es gibt $c_0, \ldots, c_n \in K$: $\quad c_0 + c_1 y + \cdots + c_n y^n = 0$.
  Es sei $g(X)$ das Minimalpolynom von y:

$$g(X) = d_m X^m + d_{m-1} X^{m-1} + \cdots + d_1 X + d_0$$

  Es ist $d_0 \neq 0$, sonst $g(X) = Xh(X)$ mit $h(y) = 0$ und $\deg h < \deg g$.
  Damit gilt:

$$\begin{aligned} \frac{1}{y} &= \frac{y^{m-1} + \overbrace{d_{m-2} y^{m-2} + \cdots + d_1}^{\neq 0}}{\underbrace{y(y^{m-1} + d_{m-2} y^{m-2} + \cdots + d_1)}_{= -d_0 \neq 0}} \\ \Rightarrow \frac{1}{y} &= \underbrace{-\frac{1}{d_0}}_{\in K} \underbrace{(y^{m-1} + d_{m-2} y^{m-2} + \cdots + d_1)}_{\in \tilde{K}} \\ \Rightarrow \frac{1}{y} &\in \tilde{K} \end{aligned}$$

□

Folgerung 2.16
$[x : K] = n \Rightarrow K(x) = K + Kx + \cdots + Kx^{n-1}$.

Folgerung 2.17
Ist $[x : K] < \infty \Rightarrow K(x)/K$ *ist algebraisch.*
Denn*: Sei* $n = [x : K] < \infty$*; sei* $z \in K(x)$

$$\Rightarrow 1, z, z^2, \ldots, z^n \text{ sind linear abhängig}$$
$$\Rightarrow a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = 0, a_i \in K$$
$$\Rightarrow z \text{ ist algebraisch über } K$$

Bemerkung 2.18

(i) $K \subset \mathbb{C}$ sei ein Unterkörper, $a \in K$

$$x = \sqrt{a} \Rightarrow [x : K] = \begin{cases} 1 & \text{falls } x \in K \\ 2 & \text{falls } x \notin K \end{cases}$$

$[x \notin K \Rightarrow [x : K] \geq 2$. Andererseits ist $f(X) = X^2 - a \in K[X]$ mit $f(x) = 0 \Rightarrow [x : K] \leq 2$. Also $[x : K] = 2$.]

(ii) $K \subset L \subset \mathbb{C}; [L : K] = 2$. Dann entsteht L aus K durch Adjunktion einer Quadratwurzel, d.h. $L = K(\omega)$ mit $\omega^2 \in K$.
[Sei $x \in L, x \notin K$. Wegen $[L : K] = 2$ hat das Minimalpolynom F von x Grad 2,d.h.

$$f(X) = X^2 + a_1 X + a_0, \quad a_0, a_1 \in K$$
$$\Rightarrow \quad x = -\frac{a_0}{2} \pm \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}.$$

Setze $\omega := \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$. Dann ist $\omega^2 \in K$. Es ist $\omega \notin K$ (sonst $x \in K$). Also ist $K(\omega) \supsetneq K$ und damit $\dim_K K(\omega) \geq 2$. Es ist $K(\omega) \subset L$ und $\dim_K L = 2$. Also ist $L = K(\omega)$.]

$K \subset L \subset M$ Körpererweiterungen

Satz 2.19 (Gradformel)

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

Beweis. (i) $[M : L] = \infty \Rightarrow [M : K] = \infty$

(ii) $[L : K] = \infty \Rightarrow [M : K] = \infty$

(iii) Sei $[M : L], [L : K] < \infty$. $w_1, \ldots, w_r$ sei eine Basis von M über L. $v_1, \ldots, v_s$ sei eine Basis von L über K.

Behauptung: $w_i v_j, 1 \leq i \leq r, 1 \leq j \leq s$ ist eine Basis von M über K.

Erzeugendensystem: Sei $m \in M$. Da $w_1, \ldots, w_r$ Basis von M über L ist, gibt es eine Darstellung

$$m = \lambda_1 w_1 + \cdots + \lambda_r w_r \quad \text{mit } \lambda_j \in L. \tag{2.2.a}$$

Da $v_1, \ldots, v_s$ eine Basis von L über K ist, gibt es Darstellungen

$$\lambda_j = \alpha_{1j} v_1 + \cdots + \alpha_{sj} v_s \quad \alpha_{ij} \in K; j = 1, \ldots, r \tag{2.2.b}$$

Einsetzen von (2.2.b) in (2.2.a) ergibt

$$m = \sum_{\substack{i=1,\ldots,s \\ j=1,\ldots,r}} \alpha_{ij} w_j v_i \quad , \alpha_{ij} \in K$$

Lineare Unabhängigkeit:

$$\sum_{\substack{i=1,\dots,s\\ j=1,\dots,r}} \alpha_{ij} v_i w_j = 0 \qquad \text{(zu zeigen: } \alpha_{ij} = 0\text{)}$$

$$\Rightarrow \sum_{j=1}^{r} \underbrace{\left(\sum_{i=1}^{s} \alpha_{ij} v_i \right)}_{\in L} w_j = 0.$$

Da $w_1, \dots, w_r$ linear unabhängig über L, folgt

$$\sum_{i=1}^{s} \alpha_{ij} v_i = 0 \quad j = 1, \dots, r.$$

Da $v_1, \dots, v_s$ linear unabhängig sind über K, folgt $\alpha_{ij} = 0$.

□

Korollar 2.20
Es sei L eine Körpererweiterung über $K, x \in L$. Dann teilt $[x : K]$ den Grad $[L : K]$ der Körpererweiterung L/K.

Beweis.

$$K \subset K(x) \subset L \overset{\text{Grad-}}{\underset{\text{formel}}{\Longrightarrow}} [L : K] = [L : K(x)] \cdot \underbrace{[K(x) : K]}_{=[x:K]}$$

$$\Rightarrow [x : K] \text{ teilt } [L : K].$$

□

Definition 2.21
Eine Körpererweiterung L/K heißt *endlich* (von *endlichem Typ*), falls $[L : K] < \infty$.

Satz 2.22
Für eine Körpererweiterung L/K sind äquivalent:

(i) $[L : K] < \infty$

(ii) *L/K ist algebraisch und es gibt algebraische Elemente $a_1, \dots, a_n$ von L über K mit $L = K(a_1, \dots, a_n)$.*

(iii) *Es gibt Elemente $a_1, \dots, a_n$ aus L, die algebraisch über K sind mit $L = K(a_1, \dots, a_n)$.*

Beweis. (i) $\Rightarrow$ (ii) L/K algebraisch, denn: Sei $x \in L$. Dann teilt $[x : K]$ den Grad $[L : K] < \infty \Rightarrow [x : K] < \infty \Rightarrow x$ ist algebraisch über K.

(ii) $\Rightarrow$ (iii) klar

(iii) $\Rightarrow$ (i) Betrachte:

$$K_0 := K; K_1 := K_0(a_1), \dots, K_i := K_{i-1}(a_i) = K_0(a_1, \dots, a_i)$$
$$K_0 \subset K_1 = K_0(a_1) \subset K_2 = K_1(a_2) \subset \cdots$$
$$\cdots \subset K_{i+1} = K_i(a_{i+1}) \subset \cdots \subset K_n = K(a_1, \dots, a_n) = L$$

Es ist

$$[K_{i+1} : K_i] = [K_i(a_{i+1}) : K_i] = [a_{i+1} : K_i]$$
(da a_{i+1} algebraisch ist über K und damit auch über K_i)

Satz (2.19):

$$[L : K] = \prod_{i=0}^{n-1} [K_{i+1} : K_i] = \prod_{i=0}^{n-1} \underbrace{[a_{i+1} : K_i]}_{<\infty} < \infty$$

□

Korollar 2.23
Es sei L/K eine Körperweiterung. Ist $\bar{K}$ die Menge der Elemente in L, die algebraisch sind über K, so ist $\bar{K}$ ein Unterkörper von L.

Beweis. Zu zeigen: $\bar{x}, \bar{y} \in \bar{K} \overset{!}{\Rightarrow} \bar{x} \pm \bar{y}, \bar{x}\bar{y}, \frac{\bar{x}}{\bar{y}} (\bar{y} \neq 0) \in \bar{K}$.
Betrachte $K(\bar{x}, \bar{y})$.

$$K \subset K(\bar{x}, \bar{y}) \subset L.$$

Damit ist $\bar{x} \pm \bar{y}, \bar{x}\bar{y}, \frac{\bar{x}}{\bar{y}} \in K(\bar{x}, \bar{y})$. Es genügt zu zeigen: $K(\bar{x}, \bar{y})$ ist algebraisch über K ($\Rightarrow \bar{x} \pm \bar{y}, \bar{x}\bar{y}, \frac{\bar{x}}{\bar{y}} \in \bar{K}$). Aus Satz (2.22) folgt genau dies ((iii) $\Rightarrow$ (ii)). □

Definition 2.24
$\bar{K}$ heißt der *algebraische Abschluss* von K in L.

Beispiel 2.25
$\mathbb{Q} \subsetneq \bar{\mathbb{Q}} \subsetneq \mathbb{R}$ ($\bar{\mathbb{Q}}$: algebraischen Zahlen; abzählbar).
$\bar{\mathbb{Q}}/\mathbb{Q}$ ist algebraisch, aber nicht endlich.

Korollar 2.26
Es sei $K \subset L \subset M$. Ist M/L algebraisch und L/K algebraisch, so ist auch M/K algebraisch.

Beweis. Sei $x \in M$. Da x algebraisch ist über L, gibt es eine Gleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in L).$$

Setze:

$$L' := K(a_0, \ldots, a_{n-1}) \subset L$$

Nach Konstruktion von L' ist x algebraisch über L'. Außerdem sind, da L/K algebraisch ist, $a_0, \ldots, a_{n-1}$ algebraisch über K. Damit ist nach Satz (2.22) auch L' algebraisch über K und endlich,

$$[L'(x) : K] = \underbrace{[L'(x) : L']}_{<\infty} \cdot \underbrace{[L' : K]}_{<\infty} < \infty$$

Da $K(x) \subset L'(x)$, ist $\underbrace{[K(x) : K]}_{=[x:K]} \leq [L'(x) : K] < \infty$. Also ist x algebraisch über K. □

Anwendungen auf Konstruktionen mit Zirkel und Lineal

$0, 1 \in \mathcal{M} \subset \mathbb{R}^2 = \mathbb{C} \rightsquigarrow \hat{\mathcal{M}} \subset \mathbb{C}$ (konstruierbare Elemente)

$$K_0 := (\mathcal{M} \cup \bar{\mathcal{M}}) = \mathbb{Q}(\mathcal{M} \cup \bar{\mathcal{M}})$$

Satz 2.27
z sei aus $\mathcal{M}$ konstruierbar, d.h. $z \in \hat{\mathcal{M}}$. Dann ist $K_0(z)$ eine algebraische Körpererweiterung von K_0 und es gilt

$$[z_0 : K_0] = [K(z_0) : K] = 2^m.$$

Beweis. $z_0 \in \mathcal{M} \Rightarrow z_0 \in L$ wobei $L = K_0(w_1, \ldots, w_n)$ mit $w_1^2 \in K_0, w_{i+1}^2 \in K_0(w_1, \ldots, w_i)$. Betrachte:

$$K_i := K_0(w_1, \ldots, w_i) \qquad K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset \cdots \subset L = K_n.$$

Dann ist

$$[K_{i+1} : K_i] = \begin{cases} 1 & \text{, falls } w_{i+1} \in K_i \\ 2 & \text{sonst} \end{cases}$$

Aus der Satz (2.19) (Gradformel) folgt

$$[L : K_0] = \prod_{i=0}^{n-1} [K_{i+1} : K_i] = 2^{m'}.$$

Es ist $K_0 \subset K_0(z) \subset L$

$$\begin{aligned} &\Rightarrow [K_0(z) : K_0] | [L : K_0] \\ &\Rightarrow [K_0(z) : K] = 2^m \qquad\qquad \text{mit } m \leq m'. \end{aligned}$$

□

Korollar 2.28
Das Delische Problem (Würfelverdopplung) ist nicht lösbar.

Lemma 2.29

$$\sqrt[3]{2} \notin \mathbb{Q}\,.$$

Beweis. Annahme $\sqrt[3]{2} = \frac{s}{t}$; s, t teilerfremd

$$\Rightarrow 2 = \frac{s^3}{t^3} \Rightarrow s^3 = 2t^3 \Rightarrow s = 2s'$$

und damit

$$s'^3 = 2t^3 \Rightarrow 4s'^3 = t^3 \Rightarrow t = 2t' \Rightarrow \lightning \text{ zur Teilerfremdheit von } (s, t).$$

□

Delisches Problem

Notwendige Bedingung für die Lösbarkeit: $[\sqrt[3]{2} : \mathbb{Q}] = 2^m$. Wir wollen zeigen, dass dies nicht der Fall ist, genauer: $[\sqrt[3]{2} : \mathbb{Q}] = 3$. Es ist $[\sqrt[3]{2} : \mathbb{Q}] \leq 3$, da $f(\sqrt[3]{2}) = 0$ für $f = X^3 - 2 \in \mathbb{Q}[X]$.

Auszugrenzen ist, dass $[\sqrt[3]{2} : \mathbb{Q}] = 1$ oder 2 ist.

(i) $[\sqrt[3]{2} : \mathbb{Q}] = 1 \Rightarrow \sqrt[3]{2} \in \mathbb{Q} \Rightarrow \lightning$

(ii) $[\sqrt[3]{2} : \mathbb{Q}] = 2$. Sei $g(X)$ das Minimalpolynom von $\sqrt[3]{2}$

$$g(X) = X^2 + aX + b, \quad a, b \in \mathbb{Q}\,.$$

Division von f durch g mit Rest:

$$f(X) = g(X) \cdot \underbrace{h(X)}_{\deg h = 1} + r(X) \qquad \text{mit } \deg r \leq 1$$

1. Fall: $r \not\equiv 0$. $f(\sqrt[3]{2}) = \underbrace{g(\sqrt[3]{2})}_{=0} h(\sqrt[3]{2}) + r(\sqrt[3]{2}) \Rightarrow r(\sqrt[3]{2}) = 0$. Sei

$$r(X) = \alpha X + \beta, \quad \alpha, \beta \in \mathbb{Q} \overset{r(\sqrt[3]{2})=0}{\Longrightarrow} \sqrt[3]{2} = -\frac{\beta}{\alpha} \in \mathbb{Q} \quad \lightning$$

2. Fall: $r \equiv 0$.

$$f(X) = g(X)h(X), \quad h(X) = cX + d; c, d \in \mathbb{Q}, c \neq 0$$

$x_0 := -\frac{d}{c} \in \mathbb{Q}$ mit $h(x_0) = 0$.

$$\Rightarrow f(x_0) = g(x_0) \underbrace{h(x_0)}_{=0} = 0$$

$\Rightarrow x_0$ ist eine reelle Nullstelle von $X^3 - 2$.

Da $X^3 - 2$ echt monoton steigend ist, besitzt $X^3 - 2$ nur eine Nullstelle, nämlich $\sqrt[3]{2}$.

$$\Rightarrow \sqrt[3]{2} = x_0 = -\frac{d}{c} \in \mathbb{Q} \quad \lightning$$
$$\Rightarrow [\sqrt[3]{2} : \mathbb{Q}] = 3 \neq 2^m.$$

Quadratur des Kreises

$\mathcal{M} = \{0, 1\}, \quad K_0 = \mathbb{Q}$

Frage: Ist $\sqrt{\pi} \in \hat{\mathcal{M}}$? Falls ja: $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = [\sqrt{\pi} : \mathbb{Q}] = 2^m$

Theorem 2.30 (Lindemann)

$$\pi \notin \bar{\mathbb{Q}}.$$

Korollar 2.31
Der Kreis ist nicht quadratierbar.

Beweis.

$$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] \cdot [\mathbb{Q}(\pi) : \mathbb{Q}] \overset{\text{Satz(2.19)}}{=} \underbrace{[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]}_{=2^m \text{ falls } \sqrt{\pi} \in \hat{\mathcal{M}}} \leq 2,$$

da $\sqrt{\pi}$ Nullstelle von $X^2 - \pi \in \mathbb{Q}(\pi)[X]$ ist.

Also:

$$\sqrt{\pi} \in \hat{\mathcal{M}} \Rightarrow [\mathbb{Q}(\pi) : \mathbb{Q}] \leq 2^m < \infty \Rightarrow \pi \in \bar{\mathbb{Q}} \quad \lightning$$

□

Winkeldreiteilung

$\mathcal{M} = \{0, 1, e^{i\varphi}\}, \quad K_0 = \mathbb{Q}(\mathcal{M}) = \mathbb{Q}(e^{i\varphi})$
Frage: $e^{i\frac{\varphi}{3}} \in \hat{\mathcal{M}}$? Falls ja: $[K_0(e^{i\frac{\varphi}{3}}) : K_0] = 2^m$. Es ist

$$[K_0(e^{i\frac{\varphi}{3}}) : K_0] \leq 3,$$

da $X^3 - e^{i\varphi} \in K_0[X]$ das Element $e^{i\frac{\varphi}{3}}$ annuliert.

$$[K_0(e^{i\frac{\varphi}{3}}) : K_0] = \begin{cases} 1 & \text{, falls } e^{i\frac{\varphi}{3}} \in \mathbb{Q}(e^{i\varphi}) \\ 2 & \longleftrightarrow \text{ hier ist die Aufgabe lösbar} \\ 3 & \longleftrightarrow \text{ hier ist die Aufgabe nicht lösbar.} \end{cases}$$

Konstruktion des n–Ecks

$\mathcal{M} = \{0, 1\}, \quad K_0 = \mathbb{Q}, \quad e^{i\frac{2\pi}{n}}?$
Frage: $\left[e^{i\frac{2\pi}{n}} : \mathbb{Q}\right] = 2^m?$

$$f(X) := X^n - 1 \in \mathbb{Q}[X], \quad f\left(e^{i\frac{2\pi}{n}}\right) = 0$$
$$\Rightarrow \left[e^{i\frac{2\pi}{n}} : \mathbb{Q}\right] \leq n$$

Es ist $\left[e^{i\frac{2\pi}{n}} : \mathbb{Q}\right] < n$, da

$$(X^n - 1) = (X - 1)\underbrace{\left(X^{n-1} + X^{n-2} + \cdots + X + 1\right)}_{=:g(X)}$$
$$\Rightarrow g\left(e^{i\frac{2\pi}{n}}\right) = 0$$
$$\Rightarrow 1 < \left[e^{i\frac{2\pi}{n}} : \mathbb{Q}\right] \leq n - 1 \qquad (n \geq 3)$$

Frage: Wie erkennt man einem Polynom f mit $f(x) = 0$ an, dass es das Minimalpolynom von x ist?

Auflösung von Polynomialgleichungen

$$f(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 = 0 \qquad (c_i \in K) \qquad (*)$$

Gibt es explizite Lösungsformeln?

Definition 2.32
Eine Körpererweiterung L/K heißt eine *Radikalerweiterung*, falls es Elemente $a_1, \ldots, a_r \in L$ und Zahlen $n_1, \ldots, n_r \in \mathbb{N}$ gibt mit

(i) $L = K(a_1, \ldots, a_r)$

(ii) $a_1^{n_1} \in K, \quad a_i^{n_i} \in K(a_1, \ldots, a_{i-1})$

Definition 2.33
Man sagt, dass $(*)$ durch Radikale aufgelöst werden kann, wenn es eine Radikalerweiterung L/K gibt, sodass $(*)$ in L eine Nullstelle hat.

Kapitel 3

Teilbarkeitstheorie in Ringen

Motivation

Lemma 3.1
L/K sei eine Körpererweiterung, $x \in L$ sei algebraisch über K. Es sei f das Minimalpolynom von x und g ein weiteres Polynom mit $g(x) = 0$. Dann gilt $g = f \cdot h$ (für ein $h \in K[x]$); "f teilt g".

Beweis. Division von g durch f mit Rest ergibt $g = f \cdot h + r$ mit $r \in K[x]$, $\deg r < \deg f$

$$\Rightarrow 0 = g(x) = \underbrace{f(x)}_{=0} \cdot h(x) + r(x) \Rightarrow g(x) = 0.$$

Falls $r \not\equiv 0$ ist, erhalten wir einen Widerspruch dazu, dass f Minimalpolynom ist. Also: $g = f \cdot g$. □

Definition 3.2
Ein *Ring (mit Eins)* ist ein Tripel $(R, +, \cdot)$ mit:

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

(ii) $(R, \cdot)$ ist abelsch (d.h. $a \cdot b = b \cdot a$) und es gilt:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(iii) Es gibt $1 \in R$, $1 \neq 0$ mit $1 \cdot a = a$ für alle $a \in R$.

Beispiel 3.3

(i) $(\mathbb{Z}, +, \cdot)$

(ii) $\mathbb{Q}[X]$

3.1 Die Einheitengruppe

Bezeichnung: $E(R) := r \in R$, r ist eine Einheit in R

Definition 3.4
Ein Element $r \in R$ heißt eine *Einheit*, falls es ein $r' \in R$ gibt mit $rr' = 1$.

Schreibweise: $r' = \frac{1}{r}$

Bemerkung 3.5
Ist r eine Einheit $\Rightarrow r \neq 0$

Lemma 3.6
$(E(R), \cdot)$ *ist eine abelsche Gruppe.*

Beweis. Zu zeigen: $r_1, r_2 \in E(R) \overset{!}{\Rightarrow} r_1 \cdot r_2 \in E(R)$

$$r_1 \in E(R) \Rightarrow \text{Es gibt } r_1' \text{ mit } r_1 \cdot r_1' = 1$$

$$r_2 \in E(R) \Rightarrow \text{Es gibt } r_2' \text{ mit } r_2 \cdot r_2' = 1$$

$$\Rightarrow (r_1 \cdot r_2)(r_1' \cdot r_2') = (r_1 \cdot r_1')(r_2 \cdot r_2') = 1 \cdot 1 = 1$$

□

Definition 3.7
$E(R)$ heißt die *Einheitengruppe* des Rings R

Beispiel 3.8

(i) $R = \mathbb{Z}$, $E(R) = \{\pm 1\}$

(ii) K sei ein Körper: $E(K) = K^* := K \backslash \{0\}$

Beispiel 3.9
Die Ringe $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$.

Sei $n > 1$ gewählt.

Definition 3.10
$a \sim b :\Leftrightarrow$ Es gibt $k \in \mathbb{Z}$ mit $a - b = k \cdot n$.

Dies ist eine Äquivalenzrelation:

(i) $a \sim a$

(ii) $a \sim b \Rightarrow b \sim a$

(iii) $a \sim b$, $b \sim c \Rightarrow a \sim c$
Denn:

$$\left.\begin{array}{l} a \sim b \Rightarrow a - b = k_1 n \\ b \sim c \Rightarrow b - c = k_2 n \end{array}\right\} a - c = (k_1 + k_2)n \Rightarrow a \sim c$$

Definition 3.11
$\mathbb{Z}/n := \mathbb{Z}/n\mathbb{Z} := \{[a]; a \in \mathbb{Z}\}$ Auf $\mathbb{Z}/n$ führen wir eine Addition und Multiplikation wie folgt ein:

$$[a] + [b] := [a + b]$$

$$[a] \cdot [b] := [a \cdot b]$$

Dies ist wohldefiniert, etwa:

$$a \sim a', b \sim b' \overset{!}{\Rightarrow} ab \sim a'b'$$

$$\left.\begin{array}{r} a \sim a' \Rightarrow a - a' = k_1 n \Rightarrow a = a' + k_1 n \\ b \sim b' \Rightarrow b - b' = k_2 n \Rightarrow b = b' + k_2 n \end{array}\right\} \Rightarrow ab = (a' + k_1 n)(b' + k_2 n)$$
$$= ab' + k_1 n b' + k_2 n a' + k_1 k_2 n^2$$
$$= a'b' + n(k_1 b' + k_2 a' + k_1 k_2 n)$$
$$\Rightarrow ab \sim a'b'$$

Beispiel 3.12
Sei $n = 15 = 3 \cdot 5$.
$\overline{3} \neq \overline{0}$, $\overline{5} \neq \overline{0} \in \mathbb{Z}_{15}$, aber $\overline{3} \cdot \overline{5} = \overline{3 \cdot 5} = \overline{15} = \overline{0}$

Definition 3.13
Ein Element $r \in R$ heißt ein *Nullteiler*, falls es ein Element $s \neq 0$ mit $rs = 0$ gibt.

Definition 3.14
Ein Ring R heißt *nullteilerfrei* oder ein *Integritätsring*, falls es in R keine Nullteiler $\neq 0$ gibt.

Beispiel 3.15

(i) $\mathbb{Z}$ ist ein Integritätsring.

(ii) Sei K ein Körper. Dann ist K ein Integritätsring.

$$\text{Sei } r \neq 0, r \cdot s = 0 \underset{r \neq 0}{\Longrightarrow} \frac{1}{r} \underbrace{(r \cdot s)}_{=0} = (\frac{1}{r} \cdot r)s = 1 \cdot s = s$$

(iii) n sei keine Primzahl $\Rightarrow \mathbb{Z}_n$ ist kein Integritätsring.

$$n = n_1 n_2,\ n_1, n_2 \neq \pm 1 \Rightarrow \overline{n_1}, \overline{n_2} \neq \overline{0}, \text{ aber } \overline{n_1} \cdot \overline{n_2} = \overline{n_1 \cdot n_2} = \overline{n} = \overline{0}.$$

(iv) $\mathcal{M}$ sei eine Menge. $R^{\mathcal{M}} := \text{Abb}(\mathcal{M}, R)$
$R^{\mathcal{M}}$ kann man wie folgt zu einem Ring machen, $f, g \in R^{\mathcal{M}}$, $m \in R^{\mathcal{M}}$:

$$(f + g)(m) := f(m) + g(m)$$

$$(f \cdot g)(m) := f(m) \cdot g(m)$$

Falls $|\mathcal{M}| \geq 2$, dann ist $R^{\mathcal{M}}$ kein Integritätsring, denn:
Sei $m_1 \neq m_2, m_1, m_2 \in \mathcal{M}$.

$$f : \mathcal{M} \to R, \qquad f(m) := \begin{cases} 1 & \text{, falls } m = m_1, \\ 0 & \text{, falls } m \neq m_1. \end{cases}$$

$$g : \mathcal{M} \to R, \qquad g(m) := \begin{cases} 1 & \text{, falls } m = m_2, \\ 0 & \text{, falls } m \neq m_2. \end{cases}$$

$$0 \neq f, g \in R^{\mathcal{M}}, \text{ aber } (f \cdot g)(m) = f(m) \cdot g(m) = 0 \Rightarrow f \cdot g \in R^{\mathcal{M}} \quad \square$$

Polynomring

$$R[X] := \left\{ \sum_{\nu=0}^{n} a_\nu X^\nu;\ a_\nu \in R \right\}$$

Alternativ:

$$R[X] = \mathrm{Abb}[\mathbb{N}, R] = \{a :\ \mathbb{N} \to R \text{ mit } a_\nu := a(\nu) = 0 \text{ für fast alle } \nu\}$$

Addition:

$$\sum_{\nu=0}^{n} a_\nu X^\nu + \sum_{\nu=0}^{n} b_\nu X^\nu := \sum_{\nu=0}^{n} (a_\nu + b_\nu) X^\nu$$

Multiplikation:

$$\left(\sum_{\nu=0}^{n_1} a_\nu X^\nu \right) \left(\sum_{\nu=0}^{n_2} b_\nu X^\nu \right) := \sum_{\nu=0}^{n_1+n_2} c_\nu X^\nu \text{ mit } c_k := \sum_{i=0}^{k} a_i b_{k-i}$$

Definition 3.16
Ist $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ mit $a_n \neq 0$, so heißt n der *Grad* von f.

Bezeichnung: $n = \deg f$ (falls $f \neq 0$)

Konvention: $\deg(0) := -\infty$

Definition 3.17
Wir definieren den Polynomring $R[X_1, \ldots, X_n]$ in n Variablen induktiv durch:

$$R[X_1, \ldots, X_n] := \Big(R[X_1, \ldots, X_{n-1}] \Big)[X_n]$$

Satz 3.18
R sei ein Integritätsring. Dann gilt für $f, g \in R[X]$: $\deg(f \cdot g) = \deg f + \deg g$.

Beweis. Klar, falls $f = 0$ oder $g = 0$. Sei also $f, g \neq 0$.

$$f = a_n X^n + \ldots + a_1 X + a_0,\ a_n \neq 0$$

$$g = b_m X^m + \ldots + b_1 X + a_0,\ b_m \neq 0$$

$$\Rightarrow f \cdot g = \underbrace{a_n b_m}_{\neq 0} X^{n+m} + \ldots + a_0 b_0 \text{ (da } R \text{ ein Integritätsring ist)}$$

$$\Rightarrow \deg(f \cdot g) = n + m = \deg f + \deg g$$

□

Achtung: $R = \mathbb{Z}/4$, $f(X) = \overline{2}X + 1$, $g(X) = \overline{2}X + \overline{2}$

$$\begin{aligned} (f \cdot g)(X) &= \overline{2} \cdot \overline{2} X^2 + \overline{2} \cdot \overline{3} X + \overline{1} \cdot \overline{2} X + \overline{1} \cdot \overline{3} \\ &= \overline{4} X^2 + \overline{8} X + \overline{3} \\ &= \overline{3} \end{aligned}$$

Korollar 3.19
Ist R ein Integritätsring, dann auch $R[X_1, \dots, X_n]$.

Beweis. Genügt für $n = 1$, dann Induktion.

$$f, g \neq 0,\ f, g \in R[X] \Rightarrow \deg f,\ \deg g \geq 0$$

$$\Rightarrow \deg(f \cdot g) = \deg f + \deg g \geq 0 \Rightarrow f \cdot g \neq 0.$$

□

Korollar 3.20
$E\Big(R[X_1, \dots, X_n]\Big) = E(R)$

Beweis. Genügt für $n = 1$, dann Induktion.
$f \in R[X]$ sei eine Einheit $\Rightarrow$ Es gibt $g \in R[X]$ mit $f \cdot g = 1$. Es ist $f,\ g \neq 0$.

$$\begin{aligned}
&\Rightarrow \underbrace{\deg(f \cdot g)}_{=\deg f + \deg g} = \deg 1 = 0 \\
&\Rightarrow \deg f = \deg g = 0 \\
&\Rightarrow f = r_1 \in R,\ g = r_2 \in R \text{ mit } f \cdot g = r_1 \cdot r_2 \\
&\Rightarrow r_1 f \in E(R)
\end{aligned}$$

□

Beispiel 3.21

(i) $E\Big(\mathbb{Z}[X_1, \dots, X_n]\Big) = E(\mathbb{Z}) = \{\pm 1\}$

(ii) Sei K ein Körper: $E\Big(K[X_1, \dots, X_n]\Big) = E(K) = K^* = K \backslash \{0\}$

$R \subset R[X_1, \dots, X_n]$ ($a_0 \in R \mapsto a_0$: konstantes Polynom)

3.2 Teilbarkeitstheorie

R: kommutativer Ring mit 1

Definition 3.22
Sei $s \in R$. Ein Element $r \in R$ heißt *Teiler* von s ($s|r$), falls es ein $q \in R$ gibt, mit $s = rq$.

Beispiel 3.23
$15 \in \mathbb{Z}$. Teiler: ± 1, ± 3, ± 5, ± 15.

Bemerkung 3.24

(i) $r|r$

(ii) $r|s$ und $s|t \Rightarrow r|t$

(iii) $r|s_1$ und $r|s_2 \Rightarrow r|(s_1 + s_2)$

(iv) $r|s_1$ und $r|(s_1 + s_2) \Rightarrow r|s_2$

$$\left.\begin{aligned} r|s_1 &\Rightarrow s_1 = q_1 r \\ r|(s_1 + s_2) &\Rightarrow s_1 + s_2 = q_2 r \end{aligned}\right\} \Rightarrow s_2 = q_2 r - q_1 r = (q_1 - q_2) r \Rightarrow r|s_2$$

(v) $r|s$ und $u|v \Rightarrow ru|sv$

Definition 3.25
Die Elemente $r, s \in R$ heißen *assoziert*, falls $r|s$ und $s|r$.

Schreibweise: $r \sim s$.

Beispiel 3.26
$R = \mathbb{Z}$; $+n$, $-n$ sind assoziert

Bemerkung 3.27
$\sim$ ist eine Äquivalenzrelation: $r \sim r$ klar, $r \sim s \Rightarrow s \sim r$ klar.

$$r \sim s,\ s \sim t \Rightarrow \left.\begin{array}{c} r|s \text{ und } s|r \\ s|t \text{ und } t|s \end{array}\right\} \Rightarrow r|t \text{ und } t|r \Rightarrow r \sim t.$$

Satz 3.28
R sei ein Integritätsring. Dann sind äquivalent:

(i) $r \sim s$

(ii) Es gibt eine Einheit $\epsilon \in E(R)$ *mit* $s = r\epsilon$.

Beweis. $r = 0$. Dann ist in (i) und (ii) auch $s = 0$. Dann sind (i) und (ii) trivialerweise äquivalent. Analog mit $s = 0$. Sei also $r,\ s \neq 0$.

(ii) $\Rightarrow$ (i): $s = r\epsilon \Rightarrow r|s$. Andererseits, da $\epsilon \in E(R)$: $s\epsilon^{-1} = r \Rightarrow s|r \Rightarrow r \sim s$

(i) $\Rightarrow$ (ii): $r \sim s \Rightarrow r|s$ und $s|r \Rightarrow s = q_1 r$ und $r = q_2 s$ für geeignete $q_1,\ q_2 \in R$.

$$\begin{aligned} &\Rightarrow s = (q_1q_2)s \Rightarrow s(1 - q_1q_2) = 0 \underset{\text{R Integritätsring}}{\overset{s\neq 0}{\Longrightarrow}} 1 - q_1q_2 = 0 \\ &\Rightarrow 1 = q_1q_2 \Rightarrow q_1, q_2 \in E(R) \\ &\Rightarrow s = rq_1, \qquad q_1 \in E(R). \end{aligned}$$

□

Voraussetzung (für den Rest des Kapitels): R sei ein Integritätsring.

Definition 3.29
Ein Element r heißt ein *echter Teiler* von s ($r \parallel s$), falls

(i) $r|s$

(ii) $r \notin E(R)$

(iii) $r \nsim s$

Beispiel 3.30
Echte Teiler von 15: ± 3, ± 5.

Definition 3.31
Ein Element r heißt *irreduzibel*, falls r keine echten Teiler besitzt, sowie $r \neq 0$, $r \notin E(R)$.

Beispiel 3.32
Irreduzible Elemente in $\mathbb{Z}$: $\pm p$, $p \geq 2$ Primzahl.

Bemerkung 3.33

(i) $r \parallel s$, $s|t \Rightarrow r \parallel t$
Denn: Klar ist, dass $r \notin E(R)$, $r|t$. Zu zeigen: $r \nsim t$. Falls $r \sim t \Rightarrow t|r$. Zusammen mit $r|s$ folgt $t|s$. Damit ist $s \sim t$. Also ist $r \sim t$, $s \sim t$ und damit auch $r \sim s$. Dies ist ein Widerspruch zu $r \parallel s$. $\lightning$

(ii) $r \parallel s$, $u|v \Rightarrow ru \parallel sv$.

Zurück zu unserer Motivation:

Lemma 3.34
$x \in L$ sei algebraisch über K. Dann ist das Minimalpolynom $d \in K[X]$ von x irreduzibel.

Beweis. Zunächst ist $f \neq 0$, $f \in E(K[X]) = K^*$. Bleibt: f hat keine echten Teiler. Sei $f = g \cdot h$. Da $f(x) = 0$ ist, ist $g(x) = 0$ oder $h(x) = 0$.

$\underline{g(x) = 0}$ Da $\deg f = \deg g + \deg h$ ist und da f das Minimalpolynom ist, muss $\deg g = \deg f$ sein. Also ist $\deg h = 0$ und daher $h \in K$. Da $f \neq 0$ ist, ist $h \neq 0$, also $h \in K^* = E(K[X])$.

$\underline{h(x) = 0}$ Analog.

□

Bemerkung 3.35

(i) $r \in R$ irreduzibel, $r \sim s \Rightarrow s$ ist irreduzibel.

(ii) r, s irreduzibel, $r|s \Rightarrow r \sim s$

Denn:

zu (i): Sei s nicht irreduzibel. Sei $t \parallel s$. Dann ist $t \notin E(R)$. Nun ist $r \sim s$, also gibt es $\epsilon \in E(R)$ mit $r = s\epsilon$. Damit ist $t|r$. Da r irreduzieble ist, geht dies nur, wenn $r \sim t$. Da $r \sim s$, folgt $t \sim s$. Dies ist ein Widerspruch zu $t \parallel s$.

zu (ii): zu zeigen: $s \sim r$.

$\underline{q \in E(R)}$: $\Rightarrow r \sim s$ (fertig)

$\underline{q \notin E(R)}$ Falls $q \nsim s$ ist $q \parallel s$, im Widerspruch zur Irreduzibilität von s. Falls $\underbrace{q \sim s}_{\Rightarrow q|s \text{ und } s|q}$ folgt $rq = s$, dass $r \in E(R)$, sonst wäre r ein echter Teiler von s, im Widerspruch zur Irreduzibilität von s.

Definition 3.36
Eine *Teilerkette* ist eine Folge $(r_n)_{n\in\mathbb{N}}$, $r_n \in R$ mit $r_{n+1}|r_n$ für $n \geq 0$.

Definition 3.37
Man sagt, dass in R der *Teilerkettensatz* gilt, falls es für jede Teilerkette $(r_n)_{n\in\mathbb{N}}$ ein n_0 gibt, mit $r_n \sim r_{n+1}$ für $n \geq n_0$.

Beispiel 3.38
In $\mathbb{Z}$ gilt der Teilerkettensatz, da wenn $r_{n+1} \parallel r_n$, so folgt $|r_{n+1}| < |r_n|$. Dies geht nur endlich oft.

Bemerkung 3.39

(i) Man fordert, dass $r_{n+1} \parallel r_n$ in einer Teilerkette nur endlich oft vorkommt.

(ii) Es gibt Integritätsringe, für die der Teilerkettensatz nicht gilt.

Satz 3.40
R sei ein Ring, in dem der Teilerkettensatz gilt. Dann gilt der Teilerkettensatz auch in $R[X_1, \ldots, X_n]$.

Beispiel 3.41
Etwa $R = K$ ein Körper.

Beweis. Genügt n = 1, dann Induktion. Sei

$$P = a_n X^n + \ldots + a_1 X + a_0, \quad a_i \in R, \quad a_n \neq 0$$

$$Q = b_m X^m + \ldots + b_1 X + b_0, \quad b_j \in R, \quad b_n \neq 0$$

Feststellung: $Q|P \Rightarrow \deg Q \leq \deg P$ und $b_m|a_n$. Denn: $Q|P \Rightarrow P = QR$ mit etwa $R = c_k X^k + \ldots + c_0$, $c_i \in R$, $c_k \neq 0$.

$$QR = b_n c_k X^{m+k} + \cdots + b_0 c_0 = P$$

$$\deg P = \deg Q + \underbrace{\deg R}_{\geq 0} \text{ (vgl. früher)} \Rightarrow \deg Q \leq \deg P \text{ und } b_m c_k = a_n$$

$$\Rightarrow b_m | a_n$$

Es seien $R_n \in K[X]$ Polynome mit $R_{n+1}|R_n$. $\Rightarrow \deg R_1 \geq \deg R_2 \geq \ldots \Rightarrow$ es gibt ein n_0 mit $\deg R_n = \deg R_{n+1}$, falls $n \geq n_0$. Es sei nun r_n der Leitkoeffizient von R_n. Dann gilt $r_{n+1}|r_n$. Da in R der Teilerkettensatz gilt, gibt es ein n_1 mit: $r_{n+1} \sim r_n$ für $n \geq n_1$.
Sei $N := \max(n_0, n_1)$. Behauptung: $n \geq N \Rightarrow R_{n+1} \sim R_n$
Denn: Zunächst ist für $n \geq N$: $\deg R_{n+1} = \deg R_n$. D.h. , aus $R_{n+1}|R_n$ folgt:

$$R_n = R_{n+1} \cdot \epsilon, \ \epsilon \in R, \ \epsilon \neq 0$$

Vergleich der Leitkoeffizienten liefert

$$r_n = r_{n+1} \cdot \epsilon$$

Es genügt zu zeigen, dass $\epsilon \in E(R) = E(R[X])(\Rightarrow R_{n+1} \sim R_n)$. Dies gilt, da $r_{n+1} \sim r_n$, d.h. $r_{n+1} = \epsilon' r_n$ mit $\epsilon' \in E(R)$.

$$\Rightarrow r_n = \epsilon' \epsilon r_n \underset{R \text{ ist Integritätsring}}{\overset{r_n \neq 0}{\Longrightarrow}} 1 = \epsilon' \epsilon \Rightarrow \epsilon \in E(R).$$

□

Satz 3.42 (Euklid)
In R gelte der Teilerkettensatz. Es sei $r \in R$, $r \neq 0$, $r \notin E(R)$. Dann gibt es eine Darstellung

$$r = p_1 \ldots p_s \quad \textit{mit } p_1, \ldots, p_s \textit{ irreduzibel} \tag{3.3.a}$$

Beweis. (i) Es sei $M \subset R$ eine Teilmenge, $M \neq \emptyset$. Dann gibt es ein $r \in M$, sodass kein Element von M ein echter Teiler von r ist. (Ansonsten gibt es eine unendliche Kette mit $r_{n+1} \parallel r_n$.)

(ii) Wende dies an auf die Menge

$$M := \{r \in R, \ r \neq 0, \ r \notin E(R), \ r \text{ hat keine Darstellung wie in ((3.3.a))}\}$$

Ziel: $M = \emptyset$.
Annahme $M \neq 0$. Dann wähle man $r_0 \in M$ wie in (i). r_0 ist nicht irreduzibel, da sonst $r_0 = r_0$ eine Darstellung wie (3.3.a) wäre. Also gibt es r_1 mit $r_1 \parallel r_0$. Es ist außerdem $r_1 \notin M$. Es ist auch $r_1 \neq 0, \ r_1 \neq E(R)$.

$$\text{Schreibe} \qquad r_0 = r_1 r_2 \tag{3.3.b}$$

Behauptung: $r_2 \parallel r_0$
Dann sind wir fertig, da $r_2 \in M$ $r_1 \notin M$ besitzen sie eine Darstellung

$$r_1 = p_1 \cdots p_n, \quad r_2 = q_1 \cdots q_m; \qquad p_i,\ p_j \text{ irreduzibel}$$

$\Rightarrow r = p_1 \cdots p_n \cdot q_1 \cdots q_m$ hat eine Darstellung von Typ (3.3.a). $\lightning$
Zur Behauptung: $r_2 \parallel r_0$.
Klar ist $r_2 | r_0,\ r_2 \neq 0$. Bleibt: $r_2 \nsim r_0$.
Falls $r_2 \sim r_0$, dann ist $r_2 = \epsilon r_0$ mit $\epsilon \in E(R)$. Dann gilt mit (3.3.b)

$$r_0 = r_1 \epsilon r_0 \Rightarrow r_1 \epsilon \in E(R) \Rightarrow r_1 \in E(R)$$

Dies ist ein Widerspruch zu $r_1 \parallel r_0$. $\lightning$

□

Beispiel 3.43

$$R_n := \left\{a + b\sqrt{n};\ a,\ b \in \mathbb{Z}\right\} \subset \mathbb{C}, \quad n \in \mathbb{Z} \text{ fest gewählt.}$$

$n = -7$:

$$R_7 = \left\{a + b\sqrt{-7};\ a,\ b \in \mathbb{Z}\right\}$$
$$8 = 2 \cdot 2 \cdot 2 = \left(1 + \sqrt{-7}\right)\left(1 - \sqrt{-7}\right)$$

$2,\ 1 \pm \sqrt{-7}$ sind irreduzibel (betrachte die Beträge)

$$\left(|a + b\sqrt{-7}|^2 = a^2 + 7b^2\right)$$

Moral: Man kann in Allgemeinen nicht erwarten, dass eine Zerlegung in irreduzible Komponenten eindeutig ist.

Definition 3.44
Zwei Darstellungen

$$r = p_1 \cdots p_m = q_1 \cdots q_n; \qquad p_i,\ q_j \text{ prim.}$$

heißen *äquivalent*, falls:

(i) $n = m$

(ii) Es gibt eine Permutation $\sigma \in S_n$ mit $p_i \sim q_{\sigma(i)}$ $\qquad (\sim \textit{assoziert})$

Beispiel 3.45

(i) $R = \mathbb{Z}$

$$15 = 5 \cdot 3 = 3 \cdot 5 = (-3)(-5) = (-5)(-3)$$

Alle äquivalent $(3 \sim -3,\ 5 \sim -5)$

(ii) $R = \left\{a + b\sqrt{-7};\ a,\ b \in \mathbb{Z}\right\} \subset \mathbb{C}$

$$8 = 2 \cdot 2 \cdot 2 = \left(1 + \sqrt{-7}\right)\left(1 - \sqrt{-7}\right)$$

nicht äquivalent.

Definition 3.46
Ein Element $p \in R,\ p \neq 0,\ p \notin E(R)$ heißt ein *Primelement*, falls gilt:

$$p|(a \cdot b) \Rightarrow p|a \text{ oder } p|b.$$

Bemerkung 3.47

(i) p prim $\Rightarrow$ p irreduzibel.

(ii) p irreduzibel $\underset{\text{i. A.}}{\not\Rightarrow}$ p prim.

zu (i): Sei $p = ab$. Da p prim ist, folgt $p|a$ oder $p|b$. Sei $p|a$, d. h. es gibt ein h mit $ph = a$.

$$\Rightarrow p = phb \Rightarrow p(1 - bh) = 0 \overset{p\neq 0}{\Rightarrow} 1 - bh = 0 \Rightarrow 1 = bh \Rightarrow b \in E(R)$$
$\Rightarrow p$ hat keine echten Teiler.

zu (ii): $R = \left\{a + b\sqrt{-7};\ a,\ b \in \mathbb{Z}\right\}$

$$8 = 2 \cdot 2 \cdot 2 = \left(1 + \sqrt{-7}\right)\left(1 - \sqrt{-7}\right)$$

2 ist irreduzibel, aber nicht prim, da

$$2 | \left(1 + \sqrt{-7}\right)\left(1 - \sqrt{-7}\right), \text{ aber } 2 \nmid \left(1 \pm \sqrt{-7}\right).$$

Denn:

$$2\left(a + b\sqrt{-7}\right) = 1 \pm \sqrt{-7} \Rightarrow a = \frac{1}{2},\ b = \pm\frac{1}{2} \Rightarrow \left(\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}\right) \notin R$$

Satz 3.48
Es sei $p \in \mathbb{Z}$ eine Primzahl ($p \geq 2$). Dann ist p ein Primelement.

Beweis. Annahme, es gibt eine Primzahl p, die kein Primelement ist. D. h. es gibt $a,\ b \in \mathbb{Z}$ mit:

$$p|ab, \text{ aber } p \nmid a,\ p \nmid b.$$

Es sein nun p mit dieser Eigenschaft minimal gewählt. Division von $a,\ b$ durch p ergibt:

$$\begin{aligned} a &= pa' + a_1 \quad (0 < a_1 < p) \\ b &= pb' + b_1 \quad (0 < b_1 < p) \end{aligned}$$

Es gilt

$$ab = p^2a'b' + pa'b_1 + pa'b_1 + pb'a_1 + a_1b_1.$$

Da $p|ab$, folgt hieraus, dass $p|a_1b_1$. D. h wir können a, b durch a_1, b_1 ersetzen und annehmen, dass $a,\ b < p$. Wir wählen nun $a,\ b$ so, dass ab minimal wird und noch ein Gegenbeispiel vorliegt.

$$p|ab \Rightarrow \text{ Es gibt } h \text{ mit } ph = ab.$$

Es sei p' ein Primteiler von h. Dann gilt, da $ph = ab < p^2$ ist, dass $p' < p$. Wir haben dann folgendes:

$$p'|h \text{ und } h|ab \Rightarrow p'ab.$$

Da $p' < p$ und p als Gegenbeispiel minimal gewählt ist, folgt:

$$p'|a \text{ oder } p'|b.$$

Es sei $p'|a$, d. h es gibt ein a' mit $p'a' = a$.

$$\Rightarrow ph = pp'h' = ab = p'a'b \Rightarrow ph' = a'b < ab.$$

Wegen der Minimalität von ab folgt:

$$p|a' \text{ oder } p|b \qquad \lightning$$

$$\Rightarrow a'|a \qquad p|a \qquad \lightning$$

□

Bemerkung 3.49

(i) p sei prim, $p|a_1 \cdots a_s$. Dann gibt es ein i mit $p|a_i$.

(ii) p prim, , $p \sim s \Rightarrow s$ ist prim.

(iii) $p,\ q$ prim, $p|q \Rightarrow p \sim q$

zu (i): Sofort durch Induktion aus der Definition.

zu (ii): Sei $s|ab$. Zu zeigen: $s|a$ oder $s|b$

$p \sim s \Rightarrow$ Es gibt $\epsilon \in E(R)$ mit $p = s\epsilon,\ s = p\epsilon^{-1}$
$s|ab \Rightarrow sh = ab \Rightarrow p\epsilon^{-1}h = a \Rightarrow ph = (\epsilon a)b \overset{p \text{ prim}}{\Longrightarrow} p|\epsilon a$ oder $p|b$
(a) $p|\epsilon a \Rightarrow ph' = \epsilon a \Rightarrow p\epsilon^{-1}h' = a \Rightarrow sh' = a \Rightarrow s|a$
(b) $p|b \Rightarrow ph'' = b \Rightarrow s(\epsilon h'') = b \Rightarrow s|b.$

$p|q \Rightarrow$ Es gibt a mit $pa = q$.
(a) $q|b \overset{p|q}{\Rightarrow} p \sim q$
(b) $q|a \Rightarrow$ Es gibt ein h mit $qh = a \Rightarrow q = pa = pqh \overset{R \text{ Integritätsring}}{\Longrightarrow} 1 = ph$
$\Rightarrow p \in E(R)$ $\lightning$ dazu, dass p prim ist.

Satz 3.50
Es sei $r \in R$. Es seien $r = p_1 \cdots p_m$, $r = q_1 \cdots q_n$ zwei Darstellungen mit $p_i,\ q_j$ prim. Dann sind diese Darstellungen äquivalent.

Folgerung 3.51
Eindeutige Primzahlzerlegung in $\mathbb{Z}$.

Satz 3.52
Sei $r \in R$ und

$$r = p_1 \cdots p_m = q_1 \cdots q_n \qquad p_i,\ q_j \text{ prim.}$$

Dann sind diese Darstellungen äquivalent.

Beweis. Sei $l := \min(m, n)$. Induktion nach l. Sei $p_1|q_1$. Dann folgt aus Bemerkung (iii), dass $p_1 \sim q_1$, d. h. $q_1 = \epsilon p_1$ für eine Einheit $\epsilon \in E(R)$.

$$\Rightarrow p_1 = p_1(\epsilon q_2 \cdots q_n) \Rightarrow 1 = \epsilon q_2 \cdots q_2 \overset{q_0 \text{ prim}}{\Longrightarrow} n = 1 \text{ und damit } p_1 = q_1.$$

l-1 $\mapsto$ l:

$$p_1 \cdots p_m = q_1 \cdots q_n \overset{\text{wie oben}}{\Longrightarrow} p_1|q_i, \text{ etwa } p_1|q_1, \text{ also } q_1 = \epsilon p_1 \text{ für ein } \epsilon \in E(R).$$

$$p_1(p_2 \cdots p_m) = p_1(\epsilon q_2 \cdots q_n) \Rightarrow p_2 \cdots p_m = (\epsilon q_2)q_3 \cdots q_n$$

Mit q_2 ist auch ϵq_2 prim (Bemerkung ii). Nach IV folgt $m = n$ und $p_i \sim q_{\sigma(i)}$ für eine Permutation $\sigma \in S_{n-1}$. □

3.3 Faktorielle Ringe

Definition 3.53
Ein Integritätsring R heißt *faktorieller Ring* (oder *ZPE-Ring* (**Z**erlegung in **P**rimfaktoren **E**indeutig), falls jedes Element $r \in R$, $r \neq 0$, $r \notin E(R)$ eine Darstellung $r = p_1 \dots p_n$, p_i prim besitzt.

Bemerkung 3.54
Solche Darstellungen sind eindeutig bis auf Äquivalenz.

Beispiel 3.55

(i) $R = \mathbb{Z}$

(ii) K Körper (trivial)

(iii) $K[x_1, \dots, x_n]$ vgl. *Satz von Gauß* (3.57)

Satz 3.56
Es sind für einen Ring äquivalent:

(i) *R ist faktoriell.*

(ii) *In R gilt der Teilerkettensatz und jedes irreduzible Element ist prim.*

(iii) *In R gilt der Teilerkettensatz und je zwei Darstellungen $r = p_1 \cdots p_m = q_1 \cdots q_n$ mit irreduziblen p_i, q_j sind äquivalent.*

Beweis. (i) $\Rightarrow$ (ii): Vorrede:

$$r = p_1 \cdots p_m,\ s = q_1 \cdots 1_n; \quad p_i,\ q_j \text{ prim.}$$

$$r|s \Rightarrow m \leq n \quad (s = r \cdot h = q_1 \cdots q_n = p_1 \cdots p_m h_1 \cdots h_l)$$

$$r \parallel s \Rightarrow m < n.$$

Aus (i) folgt, dass der Teilerkettensatz gilt: Sei $(r_n)_{n\in\mathbb{Z}}$ eine Teilerkette, d. h. $r_{n+1}|r_n$. Sei $r_0 = p_1 \cdots p_m$ (die) Primzerlegung von r_0. Wenn immer $r_{n+1}|r_n$, dann nimmt die Anzahl der Primfaktoren ab. Dies kann nur endlich oft eintreten. Bleibt: p irreduzibel $\Rightarrow$ p prim. Sei $p = p_1 \cdots p_n$ mit $p_i prim.$ $p_1, \dots, p_n$ sind echte Teiler, ansonsten etwa $p \sim p_1$, d. h $p_1 = \epsilon p$ mit $\epsilon \in E(R)$.

$$\Rightarrow p = \epsilon p p_2 \cdots p_n \Rightarrow 1 = \epsilon p_2 \cdots p_n \qquad \lightning \text{ zu } p_i \text{ prim, falls } n \geq 2.$$

Da p irreduzibel, folgt $n = 1$ und $p = p_1$, also ist p prim.

(ii) $\Rightarrow$ (i): Teilerkettensatz $\overset{\text{Satz (3.42)}}{\Longrightarrow}$ jedes Element ist Produkt von irreduziblen Elementen $\overset{\text{irred.} = \text{prim}}{\Longrightarrow}$ jedes Element ist Produkt von Primelementen.

(ii) $\Rightarrow$ (iii): Vorherige Eindeutigkeitsaussage.

(iii) $\Rightarrow$ (ii): Müssen zeigen: Jedes irreduzible Element ist ein Primelement.
Sei $p \in R$. Sei $p|ab \Rightarrow p|a$ oder $p|b$ irreduzibel. Können annehmen, dass $a,\ b \neq 0$. Ebenso $a,\ b \notin E(R)$. [Etwa $a \in E(R) \Rightarrow$ aus $ph = ab$ folgt dann $pha^{-1} = b \Rightarrow p|b$.]

$$p|ab \Rightarrow \text{ Es gibt } h \text{ mit } ph = ab$$

$$h \in E(R): \qquad p = (h^{-1}a)b \text{ und } p|a \Leftrightarrow p|h^{-1}a \tag{3.3.c}$$

D. h. in diesem Fall können wir $h = 1$ annehmen.

$$h \notin E(R): \qquad \text{Wir schreiben } h = h_1 \cdots h_r \text{ mit } h_i \text{ irreduzibel.} \tag{3.3.d}$$

$$\overset{(3.3.c),(3.3.d)}{\Longrightarrow} \underbrace{ph_1 \cdots h_r}_{\text{irreduzibel}} = ab = \underbrace{(p_1 \cdots p_m)}_{a}\underbrace{(q_1 \cdots q_m)}_{b} \text{ mit } p_i,\ q_j \text{ irreduzibel.}$$

Aus den Eindeutigkeitsaussagen folgt $p \sim p_i \Rightarrow p|a$ oder $p \sim q_j \Rightarrow p|b$.

□

Satz 3.57 (Gauß)
Ist R ein faktorieller Ring, dann ist auch $R[x_1, \ldots, x_n]$ ein faktorieller Ring.

Folgerung 3.58

$$\left.\begin{array}{l} \mathbb{Z}[X];\ \mathbb{Z}[x_1, \ldots, x_n] \\ K[X]; K[x_1 \ldots x_n] \end{array}\right\} \textit{ faktorielle Ringe.}$$

Lemma 3.59
$p \in R$ sei prim. Dann ist auch p als Element in $R[x]$ prim.

Beweis. Seien $g,\ h \in R[x]$. Zu zeigen: $p \nmid g,\ p \nmid h \Rightarrow p \nmid gh$.

$$\begin{array}{l} g(x) = a_0 + a_1 x + \ldots + a_n x^n \\ h(x) = b_0 + b_1 x + \ldots + b_n x^m \end{array}$$

$$\begin{array}{lll} p \nmid g & \Rightarrow & \text{Es gibt ein } i \text{ mit } p \nmid a_i. \\ p \nmid h & \Rightarrow & \text{Es gibt ein } j \text{ mit } p \nmid b_j. \end{array}$$

$$\begin{array}{ll} \textit{Sei} & p|a_0,\ p|a_1, \ldots, p|a_{i-1},\ p \nmid a_i \\ & p|b_0,\ p|b_1, \ldots, p|b_{j-1},\ p \nmid b_j \end{array}$$

Annahme: Es gibt $f \in R[X]$ mit

$$pf = gh \tag{3.3.e}$$

Sei

$$f = c_0 + c_1 X + \ldots + c_{n+m} X^{n+m}, \qquad n = \deg g,\ m = \deg h$$

Vergleiche die Koeffizienten beider Seiten von (3.3.e) von X^{i+j}.

$$\begin{array}{rl} \text{Linke Seite} & p \cdot p \cdot c_{i+j} \\ \text{Rechte Seite} & \displaystyle\sum_{k+l=i+j} a_k b_l \end{array}$$

$$pc_{i+j} = \sum_{k+l=i+j} a_k b_l$$

Nach Wahl von $i,\ j$ teilt p alle Summanden der rechten Seite bis auf möglicherweise $a_i b_j$.

$$\Rightarrow p|a_i b_j \overset{\text{p prim}}{\Longrightarrow} p|a_i \text{ oder } p|b_j. \qquad \lightning$$

□

Lemma 3.60
$p \in R$ prim, dann ist auch $p \in R[X]$ prim.

Beweis. (vom Satz von Gauß (3.57))
Genuügt für $R[X]$. Dann Induktion.
In $R[X]$ gilt der Teilerkettensatz (früher gezeigt). Genügt also: Zerlegung in irreduzible Faktoren ist eindeutig.
Annahme:

$$r(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x) \quad p,\, q \text{ irreduzibel.} \tag{3.3.f}$$

Sei $\deg r$ minimal, sodass es zwei nicht-äquivalente Zerlegungen gibt. Es gilt $r,\ s > 1$.
Können annehmen:

$$\begin{aligned} &m := \deg p_1 \geq \ldots \geq \deg p_r \\ &n := \deg q_1 \geq \ldots \geq \deg q_s \quad n,\ m > 0, \text{ da } R \text{ faktoriell ist.} \end{aligned}$$

$$\begin{aligned} p_1(X) &= a_m X^m + \cdots + a_0 \quad , a_m \neq 0 \\ q_1(X) &= b_n X^n + \cdots + b_0 \quad , b_n \neq 0. \end{aligned}$$

Wir betrachten:

$$s(x) := a_m r(x) - b_n p_1(x) X^{n-m} q_2(x) \cdots q_s(x)$$

Es gilt $\deg s < \deg r$. Es gilt außerdem:

$$\begin{aligned} s(x) &= a_m p_1(x) \cdots p_n(x) - b_n p_1(x) X^{n-m} q_2(x) \cdots q_s(x) \\ s(x) &= p_1(x)(a_m p_2(x) \cdots p_r(x) - b_n X^{n-m} q_2(x) \cdots q_s(x)) \end{aligned} \tag{3.3.g}$$

Ebenso gilt auch:

$$\begin{aligned} s(x) &= a_m q_1(x) \cdots q_n(x) - b_s p_1(x) X^{n-m} q_2(x) \cdots q_s(x) \\ s(x) &= (a_m q_1(x) - b_n p_1(x) X^{n-m}) q_2(x) \cdots q_s(x) \end{aligned} \tag{3.3.h}$$

Behauptung: $p_1 | a_m q_1$.

$\underline{s(x) = 0}$: (2) $\Rightarrow a_m q_1 - b_n p_1 X^{n-m} = 0 \Rightarrow p_1 | a_m q_1$

$\underline{s(x) \neq 0}$: Da $\deg s < \deg r$, besitzt s eine eindeutige Zerlegung irreduzibler Faktoren. Vergleich von (3.3.g) und (3.3.h) ergibt dann:

- $q_1 \sim q_j$ mit $j \in \{2, \ldots, s\}$. D. h. $p_1 = \epsilon q_j$, $\epsilon \in E(R)$ und wir können Gleichung (3.3.f) durch p_1 teilen. $\lightning$ zur Minimalität von r.
- $p_1 \sim (a_n q_1 - b_n X^{n-m} p_1) \Rightarrow p_1 | a_n q_1 - b_n p_1 X^{n-m} \Rightarrow p_1 | a_m q_1$.

Wir haben damit folgendes gesehen:

$$p_1 h = a_m q_1 \text{ für ein } h \in R[X]. \tag{3.3.i}$$

Betrachte $a_m = c_1 \cdot c_d$, $c_i \in R$ prim (R ist faktoriell).

$$\Rightarrow c_i | p_1 h \underset{c_i \in R[X] \text{ prim}}{\overset{\text{Lemma}}{\Rightarrow}} c_i | p_1 \text{ oder } c_i | h \qquad \lightning, \text{ da } p_1 \text{ prim, } \deg p_1 > 0$$

$$\Rightarrow c_1, \ldots, c_d | h \Rightarrow c_m | h (, \text{ da } R \text{ faktoriell})$$

Also folgt: $h = a_m h'$ mit $h' \in R[X]$.
Einsetzen in (3):

$$p_1 a_m h' = a_m q_1 \overset{\text{Integritätsring}}{\Rightarrow} p_1 h' = q_1 \Rightarrow q_1 | p_1 \overset{p_1, q_1 \text{ prim}}{\Rightarrow} p_1 \sim q_1$$

$\Rightarrow$ Man kann in (3.3.f) kürzen. $\lightning$ zur Minimalität von r. $\square$

Folgerung 3.61

(i) $\mathbb{Z}[X_1, \ldots, X_n]$

(ii) $K[X, \ldots, X_n]$; *K Körper*

sind faktorielle Ringe.

Die Relation $\sim$ ist ein Äquivalenzrelation auf der Menge der Primelemente von R. Diese zerfällt also in Äquivalenzklassen.

- $\mathbb{Z}: \ \{p, -p\}, \ p \geq 2$ prim.
- $K[X] : \{\lambda f; f \in K[X] \textit{irreduzibel}\}$ $(\lambda \in K^*)$

Es sei $P \subset R$ eine Menge von Repräsentanten dieser Äquivalenzklassen (z. B. $R = \mathbb{Z}; \ P = \{p; \ p \geq 2 \text{ prim}\}$.)

Lemma 3.62
R sei faktoriell, P ein Repräsentantensystem von Primelementen. Dann besitzt jedes Element $R \ni r \neq 0$ *eine eindeutige Darstellung.*

$$r = \epsilon \prod_{p \in P} p^{\nu(p)} \qquad (\epsilon \in E(R)); \ v(p) \geq 0 \textit{ und } v(p) > 0 \textit{ für nur endlich viele } p. \tag{3.3.j}$$

Beispiel 3.63

$$-54 = (-1) \cdot 2^1 \cdot 3^3 \cdot 5^0 \cdot 7^0 \cdots$$

Beweis. Wenn $r \in E(R)$, dann klar. Falls $r \notin E(R)$, haben wir $r = p_1' \cdots p_n'$, p_i' prim. Es gilt

$p_i' = \epsilon_i p_i \in P \Rightarrow r = (\epsilon_1 \cdots \epsilon_n) p_1 \cdots p_n$; mit $p_i \in P$. Eindeutigkeit klar.

Darstellung (3.3.j) heißt die *normierte Primfaktorzerlegung* von r bezüglich des Repräsentantensystems P.

$$r = \epsilon \prod_{p \in P} p^{\nu(p)}, \qquad s = \epsilon' \prod_{p \in P} p^{\mu(p)}$$

(a) $r | s \Leftrightarrow \nu(p) \leq \mu(p)$ für alle $p \in P$.

(b) $r \parallel s \Leftrightarrow \nu(p) \leq \mu(p)$ für alle $p \in P$ und $\nu(p_0) < \mu(p_0)$ für zumindest ein $p_0 \in P$.

(c) $r \sim s \Leftrightarrow \nu(p) = \mu(p)$ für alle $p \in P$.

□

Definition 3.64
$\nu(p)$ heißt die *Bewertung* von r bezüglich p.

Beispiel 3.65
$R = K[X], \ P =$ { normierte irreduzible Polynome}

Definition 3.66
Seien $r, \ s \in R \backslash \{0\}$. Ein Element $g \in R$ heißt *größter gemeinsamer Teiler (*ggT*)* von r und s, wenn gilt:

(i) $g | r$, $g | s$

(ii) Ist $t | r$ und $t | s$, so gilt $t | g$.

Schreibweise: $(r, s) = \mathrm{ggT}(r,\ s)$

Definition 3.67
$r, s \in R\backslash\{0\}$. Ein Element $v \in E(R)$ heißt *kleinstes gemeinsames Vielfaches (*kgV*)* von r und s, falls gilt:

(i) $r|v$, $s|v$

(ii) Ist w ein Element mit $r|w$ und $s|w$, so folgt $v|w$.

Schreibweise: $\mathrm{kgV}(r,\ s)$

Bemerkung 3.68

(i) In beliebigen Ringen existieren ggT und kgV nicht immer.

(ii) Ist g ggT von r und s; $\epsilon \in E(R)$, so ist auch ϵg ggT von r und s. Analog mit kgV.

Definition 3.69
r, s heißen *teilerfremd*, falls $1 = (r, s)$ ist. (Falls 1 ein ggT von r und s ist). R faktorieller Ring; $P =$ Repräsentantensystem von Primelementen.

$$r = \epsilon \prod_{p \in P} p^{\nu(p)}, \qquad s = \epsilon' \prod_{p \in P} p^{\mu(p)}$$

$$\mathrm{ggT}(r,\ s) = \prod_{p \in P} p^{\min(\nu(p), \mu(p))}$$
$$\mathrm{kgV}(r,\ s) = \prod_{p \in P} p^{\max(\nu(p), \mu(p))}$$

Berechnung des ggT in $\mathbb{Z}$ oder $K[X]$ geschieht mit Hilfe des euklidischen Algorithmus (im Skript nicht aufgeführt).

Kapitel 4

Irreduzibilitätskriterien

Frage: Wie sieht man einem Polynom an, dass es irreduzibel ist?

4.1 Eisensteinkriterium

Sei R ein faktorieller Ring, $R[X]$, $h \in R[X]$.

- $\deg(h) = 0$: $h = r_0 \in R$ ist irreduzibel in $R[X]$ genau dann, wenn r_0 irreduzibel in R ist.
- $\deg(h) = 1$, $h(X) = r_1X + r_0$; $r_0, r_1 \in R$

  $\underline{r_0 = 0:}$ $h(X) = r_1X$ ist irreduzibel $\Leftrightarrow r_1 \in E(R)$

  $\underline{r_0 \neq 0:}$ $h(X) = r_1X + r_0$ ist irreduzibel $\Leftrightarrow \text{ggT}(r_0,\ r_1) = 1$.

Satz 4.1 (Eisensteinkriterium)
Sei R ein faktorieller Ring. Sei

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X] \text{ mit } a_n \neq 0.$$

Es gelte:

(i) $\text{ggT}(a_0, \ldots, a_n) = 1$

(ii) Es gibt ein Primelement $p \in R$ mit: $p|a_i$ für $0 \leq i \leq n-1$, aber $p^2 \nmid a_0$.

Dann ist f irreduzibel. Solche Polynome nennt man Eisensteinpolynome.

Beispiel 4.2

(i) $f(X) = X^3 - 2 \in \mathbb{Z}[X]$; $p = 2 | a_0$, $(a_0 = 2)$, $p^2 \nmid a_0$. $\text{ggT}(a_0,\ a_1) = \text{ggT}(2,\ 1) = 1$. f ist irreduzibel über $\mathbb{Z}$.

(ii) p sei ein Primelement. $X^n - p \in R[X]$ ist irreduzibel.

(iii) $g \in R[y]$ sei irreduzibel. $f(X, y) = X^n - g(y) \in R[X, y] = (R[y])[X]$ ist irreduzibel.

Beweis. (von Satz 4.1) Annahme: f sei reduzibel, d. h. $f = g \cdot h$, $g, h \in R[X]$

$$g(X) = b_0 + b_1X + \cdots + b_rX^r$$
$$h(X) = c_0 + c_1X + \cdots + c_sX^s \quad r, s > 0 \text{ wegen } \text{ggT}(a_0, \ldots, a_n) = 1)$$

Es gilt $a_0 = b_0c_0$. Da $p|a_0$ aber $p^2|a_0$. D.h. p teilt eines der Elemente b_0, c_0, aber nicht beide. Sei $p|b_0$, $p \nmid c_0$. Sei i so gewählt, dass gilt: $p|b_0, p|b_1, \ldots, p|b_{i-1}$, aber $p \nmid b_i$. Es ist $i \leq r$, da sonst p alle a_i teilt. ($\lightning$ zu ggT$(a_0, \ldots, a_n) = 1$). Es gilt:

$$\underbrace{a_i}_{\text{enthält } p} = \underbrace{b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1}_{\text{enthält } p} + b_ic_0 \quad (p|a_i)\ (i \leq n-1)$$

$$\Rightarrow p|b_ic_0 \overset{p \text{ prim}}{\Rightarrow} p|b_i \lightning \text{ oder } p|c_0 \lightning$$

□

Bemerkung 4.3
Praktische Anwendung: In welchen Fällen kann man f so "transformieren", dass f in ein Eisensteinpolynom übergeht?

Definition 4.4
R, S seien Ringe. Eine Abbildung $\phi : R \to S$ heißt ein *Ringhomomorphismus* , falls

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

(ii) $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$

(iii) $\phi(1) = 1$

Definition 4.5
Ein Ringhomomorphismus $\phi : R \to S$ heißt ein *Ringisomorphismus*, falls es einen Ringhomomorphismus $\psi : S \to R$ mit $\psi \circ \phi = \mathrm{id}_R$, $\phi \circ \psi = \mathrm{id}_S$ gibt.

Lemma 4.6
Es sei $\phi : R \to S$ ein Ringhomomorphismus. Für $r \in R \backslash E(R)$ sei stets $\phi(r) \neq E(R)$. Dann gilt folgendes: Ist $a \in R$ und $\phi(a)$ in S irreduzibel, dann ist auch $a \in R$ irreduzibel.

Beweis. Sei $a = a_1a_2$ mit $a_1,\ a_2 \neq E(R)$. $\Rightarrow \phi(a) = \phi(a_1 \cdot a_2) = \phi(a_1) \cdot \phi(a_2)$ mit $\phi(a_1), \phi(a_2) \neq E(R)$. $\Rightarrow \phi(a)$ ist reduzibel. Aus der logischen Behauptung folgt die Umkehrung. □

Beispiel 4.7
Sei $p \geq 2$ prim.

$$X^p - 1 = (X-1)\underbrace{(X^{p-1} + X^{p-2} + \cdots + X +)}_{=:f(X)}$$

Frage: Ist $f \in \mathbb{Z}[X]$ irreduzibel?

$$\begin{aligned} \phi : \mathbb{Z}[X] &\to \mathbb{Z}[X] \\ \phi\left(\sum_{\nu=0}^{n} a_\nu X^\nu\right) &:= \sum_{\nu=0}^{n} a_\nu (X+1)^\nu \end{aligned}$$

ϕ ist ein Ringhomomorphismus, der Nichteinheiten auf Nichteinheiten abbildet. Es genügt zu zeigen, dass $\phi(f)$ irreduzibel ist:

$$\begin{aligned} &\phi(X^p - 1) = \phi(X-1)\phi(X^{p-1} + \cdots + X + 1) \\ &\Rightarrow (X+1)^p - 1 = X\phi(f)(X) \\ &\Rightarrow \sum_{\nu=1}^{p} \binom{p}{\nu} X^\nu = X\phi(f)(X) \\ &\Rightarrow \phi(f)(X) = \sum_{\nu=1}^{p} \binom{p}{\nu} X^{\nu-1} \end{aligned}$$

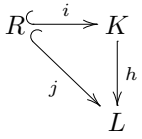
$a_{\nu-1} = \binom{p}{\nu}$. Dann gilt: $a_0 = \binom{p}{1} = p$, d. h. $p|a_0$, aber $p^2|a_0$. Ebenso gilt: $p|\binom{p}{\nu}$ für $\nu \leq p-1$. Und es ist $\binom{p}{p} = 1 \overset{\text{Satz (4.1)}}{\Longrightarrow} \phi(f)(X)$ ist irreduzibel $\Rightarrow f(X)$ ist irreduzibel.

4.2 Quotientenkörper eines Integritätsrings

R: Integritätsring

Definition 4.8
Ein Körper K heißt *Quotientenkörper* des Integritätsrings R, wenn es einen injektiven Ringhomomorphismus $i : R \to K$ mit folgender Eigenschaft gibt:

Ist L ein weiterer Körper und $j : R \to L$ ein injektiver Ringhomomorphismus, so gibt es genau einen Ringhomomorphismus $h : K \to L$ mit $j = h \circ i$, d. h. das Diagramm



kommutiert.

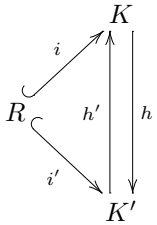
Bemerkung 4.9
K, L Körper, $h : K \to L$ ist ein Ringhomomorphismus, $h \not\equiv 0$, dann ist h injektiv.

Denn: Sei $x \neq 0$ mit $h(x) = 0$

$$\Rightarrow h(1) = h(xx^{-1}) = \underbrace{h(x)}_{=0} h(x^{-1}) = 0 \Rightarrow h \equiv 0 \quad \lightning$$

Satz 4.10
Zu jedem Integritätsring R gibt es einen Quotientenkörper K und dieser ist bis auf Isomorphie eindeutig bestimmt.

Beweis. Eindeutigkeit: Seien $i : R \to K$ und $i' : R \to K'$ Inklusionen und K, K' Quotientenkörper von R.



Da K, K' Quotienkörper sind, gibt es $h : K \to K'$ und $h' : K' \to K$ mit $i' = h \circ i$, $i = h' \circ i'$.

$$\left.\begin{matrix} i'=(h\circ h')\circ i' \\ i=(h'\circ h)\circ i \end{matrix}\right\}$$ Eindeutigkeit liefert:

$$h \circ h' = \mathrm{id}_K, \; h' \circ h = \mathrm{id}_{K'}$$

$\Rightarrow K \cong K'$.

Existenz: Betrachte die Menge $M := \{(r,s) : \ r, s \in R, s \neq 0\}$.
Schreibweise: $\frac{r}{s} := (r,s)$

Führe auf M die folgende Relation ein:

$$\frac{r}{s} \sim \frac{r'}{s'} :\Leftrightarrow rs' = r's$$

Feststellung: $\sim$ ist eine Äquivalenzrelation:

(i) $\frac{r}{s} \sim \frac{r}{s}$. Klar.

(ii) $\frac{r}{s} \sim \frac{r'}{s'} \Rightarrow \frac{r'}{s'} \sim \frac{r}{s}$. Klar.

(iii) $\frac{r}{s} \sim \frac{r'}{s'}$; $\frac{r'}{s'} \sim \frac{r''}{s''} \overset{!}{\Rightarrow} \frac{r}{s} \sim \frac{r''}{s''}$

$$\left.\begin{array}{l} \frac{r}{s} \sim \frac{r'}{s'} \Rightarrow rs' = r's \\ \frac{r'}{s'} \sim \frac{r''}{s''} \Rightarrow r's'' = s'r'' \end{array}\right\} \Rightarrow rs's'' = r'ss'' = ss'r''$$

$$\overset{s' \neq 0}{\Longrightarrow} rs'' = sr''$$

$$\Rightarrow \frac{r}{s} \sim \frac{r''}{s''}$$

—

Setze $K := {}^{M}\!/\!_{\sim}$. Wir müssen K zu einem Körper machen. Dies geschieht wie folgt:

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}$$
$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

Dies ist verträglich mit der Äquivalenzrelation, d. h.

$$\frac{r}{s} \sim \frac{\tilde{r}}{\tilde{s}}; \ \frac{r'}{s'} \sim \frac{\tilde{r}'}{\tilde{s}'} \Rightarrow \quad \frac{r}{s} + \frac{r'}{s'} \sim \frac{\tilde{r}}{\tilde{s}} + \frac{\tilde{r}'}{\tilde{s}'}$$
$$\frac{r}{s} \cdot \frac{r'}{s'} \sim \frac{\tilde{r}}{\tilde{s}} \cdot \frac{\tilde{r}'}{\tilde{s}'}$$

Wir erhalten damit also eine Addition und eine Multiplikation auf K. Damit wird K zu einem Körper.

- Additives neutrales Element: $\frac{0}{1}$

$$\frac{0}{1} + \frac{r}{s} = \frac{0 + r}{1 \cdot s} = \frac{r}{s}$$

- Zu $\frac{r}{s}$ negatives Element: $\frac{-r}{s}$
- Multiplikatives neutrales Element: $\frac{1}{1}$
- Multiplikatives inverses Element: $\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$

Bemerkung:

$$\frac{r}{s} \sim \frac{0}{1} \quad \Leftrightarrow r = 0.$$
$$\frac{r}{s} \nsim \frac{0}{1} \quad \Leftrightarrow r \neq 0. \quad \text{Dann ist } \frac{s}{r} \in M.$$

Wir bezeichnen jetzt auch die Elemente in K mit $\frac{r}{s}$. Abbildung: $i : R \hookrightarrow K$. Dies definieren wir durch $i(r) := \frac{r}{1}$. i ist injektiv: $\frac{r}{1} = 0 = \frac{0}{1} \Leftrightarrow r = 0$.

Bleibt: Gibt es einen Körper L und $j : R \hookrightarrow L$, injektiver Ringhomomorphismus, dann gibt es genau einen Körperhomomorphismus $h : K \to L$ mit $j = h \circ i$.

Existenz von h: $h(\frac{r}{s}) := j(r) \cdot j(s)^{-1}$. $(s \neq 0)$. Dann gilt $h \circ i = j.$, da $r \in R$:

$$(h \circ i)(r) = h(\frac{r}{1}) = j(r)\underbrace{j(1)}_{=1}^{-1} = j(r).$$

Eindeutigkeit von h: Sei $h' : K \to L$ mit $j = h' \circ i$. Dann gilt:

$$\begin{aligned} h'\left(\tfrac{r}{s}\right) &= h'(r)h'\left(\frac{1}{s}\right) \\ &= h'\left(\frac{r}{1}\right) h'\Big(\frac{s}{1}\Big)^{-1} \\ &= (h' \circ i)(r) \cdot (h' \circ i)(s)^{-1} \\ &= j(r)j(s)^{-1} \\ &= h\left(\frac{r}{s}\right) \end{aligned}$$

□

Bezeichnung: K= Q(R)

Beispiel 4.11

(i) $Q(\mathbb{Z}) = \mathbb{Q}$

(ii) $Q(K) = K$, K: Körper

(iii) $Q(Q[X_1, \ldots, X_n]) = \mathbb{Q}(X_1, \ldots, X_n)$

$\mathbb{Q}(X_1, \ldots, X_n) =$ Körper der rationalen Funktionen in n Variablen über $\mathbb{Q}$.

$$\mathbb{Q}(X_1, \ldots, X_n) = \left\{ \frac{R(X_1, \ldots, X_n)}{S(X_1, \ldots, X_n)};\ R, S \in \mathbb{Q}[X_1, \ldots, X_n] \right\}$$

4.3 Satz von Gauß

Motivation: Wir wissen, dass etwa $X^3 - 2 \in \mathbb{Z}[X]$ irreduzibel ist. Wir wollen nun wissen: Ist $X^3 - 2 \in \mathbb{Q}[X]$ irreduzibel?

Satz 4.12 (Gauß)
R sei ein faktorieller Ring mit Quotientenkörper $K = Q(R)$. Ist $f \in R[X]$, $\deg f > 0$, irreduzibel, dann ist auch $f \in K[X]$ irreduzibel.

Lemma 4.13
Es sei $g \in K[X]$. Dann gibt es ein $a \in K$ mit:

(i) $ag \in R[X]$

(ii) Der ggT *der Koeffizienten von ag ist* 1.

Beweis. Sei

$$\begin{aligned} g(X) &= a_0 + a_1 X + \cdots + a_n X^n \\ a_i &= \frac{r_i}{s_i} = \epsilon \prod_{p \in P} p^{\nu_{p,i}} \end{aligned}$$

, wobei P ein Repräsentantensystem von Primelementen und $\epsilon \in E(R)$ ist.

$$n := \max\{-\nu_{p,0}, \ldots, -\nu_{p,n}\}$$
$$a := \prod_{p \in P} p^n$$

Dann ist $aa_i \in R$ und $\mathrm{ggT}(aa_0, \ldots, aa_n) = 1$, da es für jedes p ein i gibt, sodass in aa_i der Faktor p mit Potenz 0 vorkommt. □

Beweis. (von Satz (4.12)) Annahme: $f = g \cdot h$; $g, h \in K[X]$, $\deg g > 0$, $\deg h > 0$.

Wählen $a, b \in K$ wie in Lemma (4.13), sodass $ag, bh \in R[X]$, und die Koeffizienten von ag, bzw bh den ggT 1 haben. $\Rightarrow (ab)f = \underbrace{(ag)}_{\in R[X]} \cdot \underbrace{(bh)}_{\in R[X]}$.

$\underline{ab \in R}$: Ansonsten gibt es (Primfaktorzerlegung beachten) ein Primelement p, das alle Koeffizienten von f teilt. Dies wäre ein Widerspruch zur Irreduzibilität von f in $R[X]$. ↯

$\underline{ab \in E(R)}$: Ansonsten gibt es ein Primelement p mit $p|ab$.

$$\Rightarrow p|(ag)(bh) \overset{p \text{ prim in } R[X]}{\Rightarrow} p|ag \text{ oder } p|bh.$$

Das ist ein Widerspruch dazu, dass die Koeffizienten von ag, bzw. bh teilerfremd sind. Da $ab \in E(R)$:

$$\begin{aligned} & (ab)f = (ag)(bh) \\ \Rightarrow \quad & f = (ab)^{-1}(ag)(bh) \\ \Rightarrow \quad & f \in R[X] \text{ ist reduzibel } \lightning \end{aligned}$$

□

4.4 Anwendung auf Konstruktionen mit Zirkel und Lineal

4.4.1 Verdopplung des Würfels

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \overset{?}{=} 3$ ($\Rightarrow$ Würfel ist nicht verdoppelbar.) Zu zeigen: $X^3 - 2 \in \mathbb{Q}[X]$ ist Minimalpolynom von $\sqrt[3]{2}$. Dies ist der Fall, da:

- $X^3 - 2 \in \mathbb{Z}[X]$ ist irreduzibel nach Satz (4.1) (Eisenstein) ($p = 2$)
- $X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel nach Satz (4.12) (Gauß).

4.4.2 Dreiteilung des Winkels

Vorbereitung:

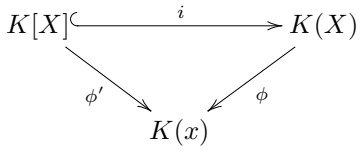
Satz 4.14
K sei ein Körper, x sei transzendent über K. Dann ist der Körper $K(X)$ der rationalen Funktionen isomorph zu $K(x) \subset L$ ($x \in L$).

Bemerkung 4.15
Dies zeigt, dass $K(X)$ nicht von dem Körper abhängt. Genauer: Es gibt einen Isomorphismus $\phi : K(X) \to K(x)$ mit $\phi_{|K} = \mathrm{id}_K$.

Beweis. Definiere

$$\begin{aligned} \phi' : K(X) &\to K(x) \\ \phi'\left(\sum_{\nu=0}^{n} a_\nu X^\nu\right) &:= \sum_{\nu=0}^{n} a_\nu X^\nu \end{aligned}$$

Wir nennen ϕ' den *Einsetzungshomomorphismus*. Nach der universellen Eigenschaft gibt es ein kommutatives Diagramm



($\phi' = \phi \circ i$). Behauptung: ϕ ist ein Isomorphismus.

- ϕ ist injektiv, da $\phi \not\equiv 0$.
- ϕ ist surjektiv: $\Im(\phi) = \phi(K(x))$ ist ein Körper mit $K(x) \supset \Im(\phi)$. Da $K(x)$ der kleinste Körper ist, der K und x enthält, folgt $\Im(\phi) = K(x)$, d. h. ϕ ist surjektiv.

Nachtrag: ϕ' ist injektiv, da x transzendent ist. $\Rightarrow \phi : K(X) \cong K(x)$ und nach Konstruktion ist $\phi_{|K} = \mathrm{id}_K$. □

Satz 4.16

(i) $S^1 = \{e^{i\varphi}; \varphi \in \mathbb{R}\}$

(ii) Ist $e^{i\varphi}$ transzendent, so ist dieser Winkel nicht mit Zirkel und Lineal durch 3 *teilbar.*

Beweis. (i) Wir haben eine Bijektion

$$\begin{aligned} [0, 2\pi[&\to S^1 \\ t &\mapsto e^{it} \end{aligned}$$

$[0, 2\pi[$ ist überabzählbar $\Rightarrow S^1$ ist überabzählbar $\Rightarrow S^1 \backslash (1^1 \cap \bar{Q})$ ist ebenfalls überzahlbar.

(ii) Betrachte $X^3 - t \in (\underbrace{\mathbb{Q}[t]}_{R})[X]$. Das Element t ist prim in R. Wende Eisenstein (Satz (4.1)) an mit $p = t$: $(a_3 = 1,\ a_0 = -t,\ t|a_0,\ t^2|a_0,\ (a_0, a_3) = 1)$. $\Rightarrow X^3 - t \in R[X]$ ist irreduzibel.

$$\overset{\text{Satz (4.12)}}{\Rightarrow} X^3 - t \in Q(R)[X] \text{ ist irreduzibel.}$$

Es gilt:

$$\begin{aligned} &\phi : \mathbb{Q}(t) \xrightarrow{\cong} \mathbb{Q}(e^{i\varphi}), \text{ falls } e^{i\varphi} \text{ transzendent} \\ &\phi_{|\,\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}},\ \phi(t) = e^{i\varphi} \end{aligned}$$

$$\begin{aligned} \Rightarrow (\mathbb{Q}(t))[X] &\xrightarrow{\cong} (\mathbb{Q}(e^{i\varphi}))[X] \\ X^3 - t &\mapsto X^3 - e^{i\varphi} = f(X) \end{aligned}$$

$\Rightarrow f(X)$ ist irreduzibel.

□

4.4.3 Konstruktion des regulären n-Ecks

$\left[\mathbb{Q}\left(e^{\frac{2\pi}{p}}\right):\mathbb{Q}\right] = 2^m$?

$$(X^p - 1) = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1);\ f\left(e^{\frac{2\pi}{p}}\right) = 0$$

$f(X) \in \mathbb{Z}[X]$ ist irreduzibel $\overset{\text{Satz (4.12)}}{\Rightarrow}$ $f(X) \in \mathbb{Q}[X]$ ist irreduzibel.

$$\Rightarrow \left[\mathbb{Q}\left(e^{\frac{2\pi}{p}}\right):\mathbb{Q}\right] = p - 1 \overset{?}{=} 2^m$$

Satz 4.17
Ist p eine Primzahl, sodass $p-1$ keine Potenz von 2 ist, dann ist das reguläre p-Eck nicht konstruierbar.

Bemerkung 4.18
Später: $p = 2^m + 1 \Rightarrow$ das reguläre p-Eck ist konstruierbar.

Kapitel 5

Restklassenringe

R, S Ringe, **kommutativ** mit 1
$\phi : R \to S$ Ringhomomorphismus

$$I = \ker \phi = \{r \in R; \phi(r) = 0\}$$

Es gilt:

(i) $(I, +)$ ist eine Gruppe
$(r, s \in I \Rightarrow r + s \in I, -r \in I; \quad \phi(r + s) = \phi(r) + \phi(s) = 0 + 0 = 0)$

(ii) $R \cdot I \subset I$
$(r \in R, s \in I \colon \phi(rs) = \phi(r) \underbrace{\phi(s)}_{=0} = 0 \Rightarrow rs \in I)$.

Definition 5.1
Ein *Ideal* in R ist eine Teilmenge $I \subset R$, sodass gilt:

(i) $(I, +)$ ist abgeschlossen

(ii) $RI \subset I$

Beispiel 5.2

(i) $(a_\lambda)_{\lambda \in \Lambda}, a_\lambda \in R$

$$I := \langle (a_\lambda)_{\lambda \in \Lambda} \rangle := \left\{ \sum_{\text{endlich}} r_\lambda a_\lambda, r_\lambda \in R \right\}$$

I heißt das von der Familie $(a_\lambda)_{\lambda \in \Lambda}$ erzeugte Ideal.

(ii) Spezialfall: $a \in R$. $\langle a \rangle = Ra = \{ra; r \in R\}$
Z.B.: $n \in \mathbb{Z}; \langle n \rangle = \{nk; k \in \mathbb{Z}\}$

(iii) K: Körper. Die einzigen Ideale sind: $\{0\}; I = K$.
$[x \in I, x \neq 0 \Rightarrow x^{-1} \cdot x = 1 \in I$; $y \in K$ beliebig $y = y \cdot \underbrace{1}_{\in I} \in I \Rightarrow I = K]$.

Definition 5.3
Ein Ideal I heißt ein *Hauptideal*, falls es von einem Element erzeugt wird, d.h. es gibt $a \in R$ mit $I = \langle a \rangle$.

Definition 5.4
R heißt ein *Hauptidealring*, falls jedes Ideal ein Hauptideal ist.

Satz 5.5
$\mathbb{Z}$ ist ein Hauptidealring.

Beweis. $I \neq 0$ Ideal. Mit $z \in I$ ist auch $-z \in I$.

$$n := \min\{k \in I; k > 0\} > 0$$

Behauptung: $I = \langle n \rangle$ $\quad (\langle n \rangle \subset I$ klar)
Sei $l \in I$, kann annehmen $l > 0$. Dann ist $l = n$ oder $l > n$. Sei $l > n$. Division von l durch n mit Rest:

$$\underbrace{l}_{\in I} = \underbrace{m \cdot n}_{\in I} + r \qquad \text{mit } 0 \leq r < n$$
$$\Rightarrow r \in I \underset{\text{von } n}{\overset{\text{Wahl}}{\Longrightarrow}} r = 0 \Rightarrow l = m \cdot n \Rightarrow l \in \langle n \rangle$$

□

Satz 5.6
K Körper. Dann ist $K[X]$ ein Hauptidealring.

Beispiel 5.7
$K[X, Y]$ ist *kein* Hauptidealring.
$m := (X, Y)$ ist *kein* Hauptidealring.

Beweis. Sei $0 \neq I \subset K[X]$ ein Ideal.

$$n := \min\{\deg f; f \in I, f \neq c \in K\} > 0.$$

Sei f ein Polynom mit $\deg f = n, f \in I$. Kann annehmen, dass f normiert ist.

Behauptung: $I = \langle f \rangle$.
Sei $g \in I$ mit $\deg g \geq \deg f$::

$$g = hf + r, \qquad \deg r < \deg f \quad \text{(Division mit Rest)}$$
$$\Rightarrow r \in I \underset{\text{von } f}{\overset{\text{Wahl}}{\Longrightarrow}} r = 0 \Rightarrow g = hf \Rightarrow g \in \langle f \rangle.$$

□

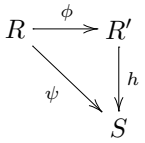
5.1 Restklassenringe

R: Ring, **kommutativ** mit 1, $I \subset R$ Ideal.

Definition 5.8
R' heißt *Restklassenring* von R nach I, falls gilt:

(i) Es gibt einen Homomorphismus $\phi\colon R \to R'$ mit $\ker \phi = I$.

(ii) Ist $\psi\colon R \to S$ ein Homomorphismus mit $I \subset \ker \psi$, dann gibt es genau einen Homomorphismus $h\colon R' \to S$, sodass das Diagramm

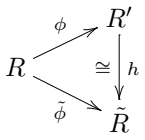


kommutiert, d.h. $h \circ \phi = \psi$.

Satz 5.9

(i) Es gibt stets einen Restklassenring R'.

(ii) Das Paar (R', ψ) ist bis auf Isomorphie eindeutig bestimmt, d.h. ist $(\tilde{R}, \tilde{\psi})$ ein weiteres solches Paar, so gibt es einen Isomorphismus $h\colon R' \to R$, sodass



kommutativ ist, d.h. $\tilde{\phi} = h \circ \phi$.

Beweis. (i) Wir führen auf R die folgende Relation ein:

$$r \sim s :\Leftrightarrow r - s \in I \qquad (\rightsquigarrow \text{Äquivalenzrelation})$$
$$R' := {}^{R}\!/\!_{\sim}\,, \quad [r] = r + I \in R'.$$

R' erhält eine Ringstruktur wie folgt:

$$[r] + [s] := [r + s]; \quad [r] \cdot [s] := [r \cdot s].$$

Unabhängigkeit von der Wahl der Repräsentanten, etwa bei der Multiplikation:

$$r \sim r', s \sim s' \overset{!}{\Rightarrow} rs \sim r's'$$
$$rs - r's' = rs - rs' + rs' + r's' = r\underbrace{(s - s')}_{=:i\in I} + s'\underbrace{(r - r')}_{=:j\in I}$$
$$\Rightarrow ri + s'j \in I$$

R' wird dadurch kommutativer Ring mit [1] als Einselement.

Brauchen:

$$\phi\colon R \to R'$$

Definiere:

$$\phi(r) := [r].$$

ϕ ist ein Ringhomomorphismus, da:

$$\phi(r + s) = [r + s] = [r] + [s] = \phi(r) + \phi(s)$$
$$\phi(r \cdot s) = [r] \cdot [s] = \phi(r) \cdot \phi(s).$$

Es gilt:

$$\ker \phi = \{r \in R; \phi(r) = 0\} = \{r \in R; [r] = [0]\}$$
$$= \{r \in R, r \in I\} = I$$

Dies zeigt (i) der Definition (5.8).
Zu (ii) der Definition: Sei $\psi\colon R \to S$, mit $I \subset \ker \psi$. Brauchen: $h\colon R' \to S$ mit $h \circ \phi = \psi$. Falls h existiert, gilt:

$$h\big([r]\big) = h(\phi(r)) = \psi(r) \quad (\Rightarrow \text{Eindeutigkeit von } h)$$

Setze also:

$$h([r]) := \psi(r).$$

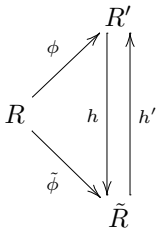
Dies ist wohldefiniert, da

$$\begin{aligned}[r] = [r'] \Rightarrow r - r' \in I &\overset{I \subset \ker \psi}{\Rightarrow} \psi(r - r') = 0 \\ &\Rightarrow \psi(r) - \psi(r') = 0 \Rightarrow \psi(r) = \psi(r')\end{aligned}$$

Nach Konstruktion ist $h \circ \phi = \psi$. Die Abbildung h ist auch ein Ringhomomorphismus:

$$\begin{aligned}h([r] + [s]) = h([r + s]) = \psi(r + s) = \psi(r) + \psi(s) = h([r]) + h([s]) \\ h([r] \cdot [s]) = h([r \cdot s]) = \psi(r \cdot s) = \psi(r)\psi(s) = h([r])h([s]).\end{aligned}$$

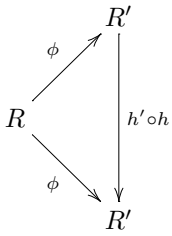
(ii) Übliches Argument



h, h' aus der universellen Eigenschaft. Eindeutigkeit:

$$h \circ h' = \mathrm{id}_{\tilde{R}}, h' \circ h = \mathrm{id}_{R'}$$

Dazu:



$$\Rightarrow \mathrm{id}_{R'} = h' \circ h.$$

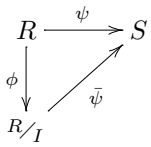
□

Bezeichnung:

(i) ${}^{R}\!/_{I} := R'$ (Restklassenring)

(ii) $\phi\colon R \to R' = {}^{R}\!/_{I}$ ist surjektiv mit $\ker \phi = \psi$. ϕ heißt die kanonische Abbildung (Projektion).

(iii) Ist $\psi\colon R \to S$ mit $I \subset \ker \psi$, so hat man ein kommutatives Diagramm

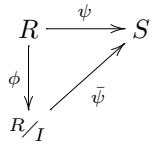


$\bar{\psi}$ heißt die durch ψ induzierte Abbildung.

Beispiel 5.10
$R = \mathbb{Z}; I = \langle n \rangle$; ${}^{R}\!/_{I} = {}^{\mathbb{Z}}\!/_{\langle n \rangle} = \mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n}$

Satz 5.11 (Homomorphiesatz)
Es sei $\psi\colon R \to S$ ein surjektiver Ringhomomorphismus mit $\ker \psi = I$. Dann liefert die induzierte Abbildung einen Isomorphismus $\bar{\psi}\colon {}^{R}\!/_{I} \xrightarrow{\cong} S$.

Beweis.



ψ surjektiv $\Rightarrow \bar{\psi}$ surjektiv. $\bar{\psi}$ ist auch injektiv, da

$$\bar{\psi}([r]) = 0 \Leftrightarrow \psi(r) = 0 \Leftrightarrow r \in I \Leftrightarrow [r] = 0$$

$\Rightarrow \bar{\psi}$ ist bijektiv $\Rightarrow \bar{\psi}$ ist ein Isomorphismus. □

Anwendung:

$$f(X) = a_0 + a_1 X + \cdots + a_k X^k \in \mathbb{Z}[X] \quad \text{irreduzibel?}$$

Idee: Reduziere mod n.

$$\begin{aligned} \mathbb{Z} &\to {}^{\mathbb{Z}}\!/_{n} = {}^{\mathbb{Z}}\!/_{\langle n \rangle} \\ \mathbb{Z}[X] &\to \mathbb{Z}_n[X] \\ \sum a_k X^k \mapsto \bar{f} := \sum \bar{a}_k X^k;& \quad \bar{a}_k = a_k \pmod{\langle n \rangle} \in \mathbb{Z}_n\,. \end{aligned}$$

Untersuche $\bar{f}$ auf Irreduzibilität.

$$\begin{aligned} f \text{ reduzibel} &\Rightarrow \bar{f} \text{ reduzibel} \\ f \text{ irreduzibel} &\Leftarrow \bar{f} \text{ irreduzibel} \end{aligned}$$

Beispiel 5.12
$f(X) = fX^4 + 3X^3 + X^2 - 6X + 5$

<u>$n = 2$:</u> $\bar{f}(X) = X^4 + X^3 + X^2 + \bar{1} = (X + \bar{1}) \underbrace{(X^3 + X + \bar{1})}_{\bar{g}(X)}$ $\bar{g}(X)$ irreduzibel, da $g(\bar{0}) = \bar{1} \neq \bar{0}, g(\bar{1}) = \bar{1} \neq \bar{0} \Rightarrow$ falls f reduzibel, dann zerfällt f in eine Linearform und einen kubischen Teil.

<u>$n = 3$:</u> $\bar{f}(X) = \bar{2}X^4 + X^2 + \bar{2}$

Falls f reduzibel $\Rightarrow \bar{f}$ spaltet Linearfaktor ab $\Rightarrow \bar{f}$ hat eine Nullstelle.

Aber:

$$\begin{aligned} \bar{f}(\bar{0}) &= \bar{2} \neq 0 & \bar{f}(\bar{1}) &= \bar{2} + \bar{1} + \bar{2} = \bar{2} \neq \bar{0} \\ \bar{f}(\bar{2}) &= \bar{f}(-\bar{1}) = \bar{f}(\bar{1}) = \bar{2} \neq \bar{0} \end{aligned}$$

$\Rightarrow f$ irreduzibel.

Beispiel 5.13
$f(X) = X^4 - X^2 + 1 \in \mathbb{Z}[X]$ ist irreduzibel
Aber: $\bar{f}(X) \in \mathbb{Z}_p[X]; p \geq 2$ prim ist immer reduzibel.
Hier liefert dieses Verfahren zumindest für Primzahlen kein Ergebnis.

Bemerkung 5.14
Es gibt (deterministische) Algorithmen, die in polynomialer Zeit entscheiden, ob ein gegebenes Polynom $f \in \mathbb{Z}[X]$ irreduzibel ist.

5.2 Der Primring eines Rings

R, S : Ringe (mit $1 \neq 0$)

Definition 5.15
Ein *Ringhomomorphismus* ist eine Abbildung $\psi\colon R \to S$ mit

(i) $\psi(r_1 + r_2) = \psi(r_1) + \psi(r_2)$

(ii) $\psi(r_1 \cdot r_2) = \psi(r_1) \cdot \psi(r_2)$

(iii) $\psi(1) = 1$

Satz 5.16
Es gibt genau einen Ringhomomorphismus $\varrho\colon \mathbb{Z} \to R$.

Beweis. Es ist $\varrho(1) = 1$. Damit muss gelten

$$(k > 0) \quad \varrho(k) = \varrho(\underbrace{1 + \cdots + 1}_{k-\text{mal}}) = \underbrace{\varrho(1) + \cdots + \varrho(1)}_{k-\text{mal}} = \underbrace{1 + \cdots + 1}_{k-\text{mal}}$$

$\Rightarrow$ Eindeutigkeit

Existenz:

$$\varrho(k) := \begin{cases} \underbrace{1 + \cdots + 1}_{k} & (k > 0) \\ 0 & (k = 0) \\ -(1 + \cdots + 1) & (k < 0) \end{cases}$$

Damit ist $\varrho(1) = 1$ und ϱ ist ein Ringhomomorphismus:

$$\varrho(k_1 + k_2) = (\underbrace{k_1 + k_2}_{=\pm(\underbrace{1 + \cdots + 1}_{|k_1+k_2|-\text{mal}})}) \cdot 1 = k_1 \cdot 1 + k_2 \cdot 1 = \varrho(k_1) + \varrho(k_2)$$

$$\varrho(k_1 \cdot k_2) = \varrho(k_1) \cdot \varrho(k_2) \quad \text{analog.}$$

□

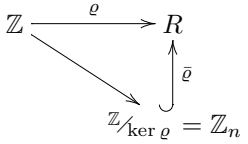
Definition 5.17
$\varrho(\mathbb{Z}) := \operatorname{im}(\varrho\colon \mathbb{Z} \to R)$ heißt der *Primring* von R. Die Abbildung ϱ heißt der *kanonische Homomorphismus*.

(i) ϱ sei injektiv. Dann ist $\varrho(\mathbb{Z}) \cong \mathbb{Z} \subset R$. [z.B. $R = \mathbb{Q}, \varrho(\mathbb{Z}) = \mathbb{Z} \subset \mathbb{Q}$]

(ii) ϱ sei nicht injektiv.

$$I := \ker \varrho \subset \mathbb{Z} \quad \text{(Ideal)}$$

$\Rightarrow I = \langle n \rangle$ für ein $n \geq 2$ ($n = 1$ unmöglich, da sonst $\varrho \equiv 0$)



$\bar{\varrho}$: induzierter Homomorphismus, $\bar{\varrho}$ ist injektiv

$\Rightarrow \varrho$ induziert also einen Isomorphismus

$$\bar{\varrho}\colon \mathbb{Z}_n \xrightarrow{\cong} \varrho(\mathbb{Z}) \quad \text{(Primring)}$$

Also haben wir gesehen

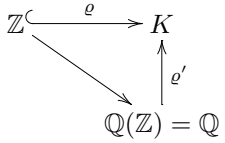
$$\text{Primring: } \varrho(\mathbb{Z}) \cong \begin{cases} \mathbb{Z} & \text{oder} \\ \mathbb{Z}_n \end{cases}$$

Definition 5.18
Es sei R ein Ring. Dann definiert man die *Charakteristik* von R durch:

$$\operatorname{char} R = \begin{cases} 0 & \text{, falls } \varrho(\mathbb{Z}) \cong \mathbb{Z} \\ n & \text{, falls } \varrho(\mathbb{Z}) \cong \mathbb{Z}_n \end{cases}$$

Beispiel 5.19
$\operatorname{char}(\mathbb{Z}_n[X]) = n$.

Bemerkung 5.20
Es sei K ein Körper, der als Ring die Charakteristik 0 hat. Dann hat man:



ϱ' definiert eine Inlusion von $\mathbb{Q}$ nach K, d.h. man kann jeden Körper der Charakteristik 0 als Körpererweiterung von $\mathbb{Q}$ auffassen.

5.3 Erzeugendensysteme von Ringerweiterungen

S Ring (kommutativ mit 1), $R \subset S$ Unterring, Familie: $(x_\lambda)_{\lambda\in\Lambda}; x_\lambda \in \varrho$.

Definition 5.21

$$R[(x_\lambda)_{\lambda\in\Lambda}] := \bigcap_{\substack{R' \text{ ist ein Unterring, der } R \\ \text{und alle Elemente } x_\lambda \text{ enthält.}}} R'$$

Bemerkung 5.22
$R[(x_\lambda)_{\lambda\in\Lambda}]$ ist der *kleinste* Unterring von S, der R und alle Elemente $x_\lambda, \lambda \in \Lambda$ enthält.

Definition 5.23

(i) $R[(x_\lambda)_{\lambda\in\Lambda}]$ heißt der *Ring, der aus R durch Adjunktion* der Elemente $x_\lambda, \lambda \in \Lambda$ entsteht.

(ii) Ist $S = R[(x_\lambda)_{\lambda\in\Lambda}]$, so sagt man, dass die Familie $(x_\lambda)_{\lambda\in\Lambda}$ ein *Erzeugendensystem* von S über R ist.

Beispiel 5.24

(i) $S = \mathbb{C}, R = \mathbb{R} \quad S = R[i]$
$z \in \mathbb{C}\colon z = a \pm ib, \quad a, b \in \mathbb{R}$

(ii) $R = \mathbb{Z}, S = \mathbb{Z}[X_1, \ldots, X_n]$ Polynomring
Dann sind $X_1, \ldots, X_n$ Erzeugende von S über R. Dies rechtfertigt auch die doppellte Verwendung des Symbols $R[\ldots]$.

5.3.1 Der Polynomring in beliebig vielen Variablen

R: kommutativer Ring mit 1
$(X_\lambda)_{\lambda\in\Lambda}$: Variablen, paarweise verschieden

$$R[(X_\lambda)_{\lambda\in\Lambda}] := \big\{f; f = f(X_{\lambda_1},\dots,X_{\lambda_n}) \text{ ist ein Polynom in } X_{\lambda_1},\dots,X_{\lambda_n} \text{ mit } \{\lambda_1,\dots,\lambda_n\}\subset\Lambda\big\}$$

Ringstruktur:

$$f = f(X_{\lambda_1},\dots,X_{\lambda_n}) \qquad g = g(X_{\mu_1},\dots,X_{\mu_k})$$

$\{\lambda_1,:,\lambda_n\},\{\mu_1,\dots,\mu_k\}\subset\Lambda$
Setze

$$\Lambda' := \{\lambda_1,\dots,\lambda_n\}\cup\{\mu_1,\dots,\mu_k\}\subset\Lambda$$

Dann gilt:

$$f,g\in R[X_\lambda;\lambda\in\Lambda']$$

Dann definieren wir $f+g, f\cdot g$ wie früher.

Einsetzungshomomorphismus

$R\subset S; (x_\lambda), x_\lambda\in S, \lambda\in\Lambda$
Wir erhalten einen Ringhomomorphismus

$$\sigma\colon R[(X_\lambda)_{\lambda\in\Lambda}]\to S$$

wie folgt: Ist

$$f = f(X_{\lambda_1},\dots,X_{\lambda_n}) = \sum_{\text{endlich}} r_{\nu_1\dots\nu_n} X_{\lambda_1}^{\nu_1}\dots X_{\lambda_n}^{\nu_n}$$

so setzen wir

$$\sigma(f) := \sum_{\text{endlich}} r_{\nu_1\dots\nu_n} x_{\lambda_1}^{\nu_1}\dots x_{\lambda_n}^{\nu_n}$$

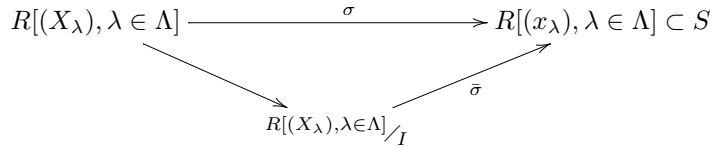
Dies ist ein Ringhomomorphismus mit $\sigma|_R = \mathrm{id}_R$. σ heißt dann *Einsetzungshomomorphismus*. Sei

$$I := \ker\sigma.$$

Satz 5.25
Dann gibt es einen natürlichen Isomorphismus

$$\bar\sigma : {}^{R[(X_\lambda);\lambda\in\Lambda]}\!/_I \cong R[(x_\lambda);\lambda\in\Lambda]$$

Beweis. Die universelle Eigenschaft des Quotienten liefert uns:



Dabei ist $\bar{\sigma}$ injektiv und $\operatorname{im}\bar{\sigma} \subset R[(x_\lambda), \lambda \in \Lambda]$. Wir brauchen nur zu sehen, dass $\operatorname{im}\bar{\sigma} = R[(x_\lambda), \lambda \in \Lambda]$ (dann Homomorphisatz anwenden: ${}^{R}\!/_{\ker\psi} \cong \operatorname{im}\psi$). Die Surjektivität folgt, da $\operatorname{im}\bar{\sigma}$ ein Ring ist, der R und die Elemente x_λ umfasst und $R[(x_\lambda), \lambda \in \Lambda]$ der kleinste Ring ist mit dieser Eigenschaft. □

L/K: Körpererweiterung $(K \subset L)$,$(x_\lambda)_{\lambda\in\Lambda}; x_\lambda \in L$
Haben:

$$K((x_\lambda)_{\lambda\in\Lambda}) \subset L \quad \text{Körperadjunktion}$$
$$K[(x_\lambda)_{\lambda\in\Lambda}] \subset L \quad \text{Ringadjunktion}$$

($K[(x_\lambda)_{\lambda\in\Lambda}]$ ist im Allgemeinen ein Ring, aber kein Körper). Klar ist

$$K[(x_\lambda)_{\lambda\in\Lambda}] \subset K((x_\lambda)_{\lambda\in\Lambda})$$

$K[(x_\lambda)_{\lambda\in\Lambda}] \subset L$ ist ein Integritätsring und besitzt damit einen Quotientenkörper.

Satz 5.26

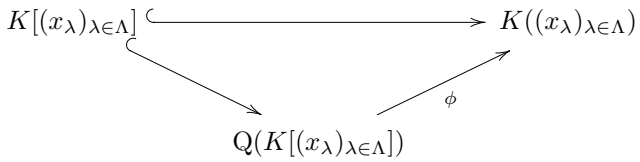
(i) $Q(K[(x_\lambda)_{\lambda\in\Lambda}]) = K((x_\lambda)_{\lambda\in\Lambda})$.

(ii) Jedes Element $y \in K((x_\lambda)_{\lambda\in\Lambda})$ *ist von der folgenden Form:*

$$y = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \quad \textit{mit } x_1, \ldots, x_n \in (x_\lambda); f, g \textit{ Polynome}$$

Beweis. (ii) sofort aus (i), da der Einsetzungshomomorphismus surjektiv ist.

(i): Universelle Eigenschaft des Quotientenkörpers



Behauptung: ϕ ist ein Isomorphismus

(i) ϕ injektiv, da $\phi|_K = \mathrm{id}_K$; also $\phi \neq 0$.

(ii) ϕ surjektiv: $\operatorname{im}\phi$ ist ein Unterkörper, der K und die $x_\lambda, \lambda \in \Lambda$ enthält. Da $K((x_\lambda)_{\lambda\in\Lambda})$ der minimale Körper mit dieser Eigenschaft ist, ist ϕ auch surjektiv.

□

Bemerkung 5.27

(i) $x \in L$ sei algebraisch über K. Dann ist:

$$K[x] = K(x)$$

Denn: $K[x] \subset K(x)$ klar. Sei n der *Grad* von x über K. Hatten gesehen

$$K(x) = K + Kx + Kx^2 + \cdots + Kx^{n-1} \subset K[x]$$

$\Rightarrow K[x] = K(x)$.
Aber: $\mathbb{Q}[X] \subsetneq \mathbb{Q}(X)$.

(ii) Sei L/K algebraisch und $L = K((x_\lambda)_{\lambda\in\Lambda})$. Dann ist $L = K[(x_\lambda)_{\lambda\in\Lambda}]$.
Denn: $K[(x_\lambda)_{\lambda\in\Lambda}] \subset L$ ist klar. Sei $x \in L$. Nach Satz (5.26) gilt:

$$x = \frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)} \quad \{x_1,\dots,x_n\} \subset \{x_\lambda; \lambda\in\Lambda\}$$

$$\Rightarrow x \in K(x_1,\dots,x_n) = \big(K(x_1,\dots,x_n)\big)(x_n) \overset{x_n \text{ algebraisch}}{=} \big(K(x_1,\dots,x_n)\big)[x_n] = \dots = K[x_1,\dots,x_n] \subset K[(x_\lambda)_{\lambda\in\Lambda}].$$

5.4 Ideale und Homomorphismen

$\phi\colon R \to S$ Ringhomomorphismus

Satz 5.28

(i) Ist $J \subset S$ ein Ideal, dann ist auch $\phi^{-1}(J) \subset R$ ein Ideal.

(ii) Ist ϕ surjektiv und $I \subset R$ ein Ideal, dann ist auch $\phi(I) \subset S$ ein Ideal.

Beweis. (i) $\phi^{-1}(J) \subset R$ ist abelsche Untergruppe (wurde früher gezeigt).

Zu zeigen: $R \cdot \phi^{-1}(J) \subset \phi^{-1}(J)$.
Hierzu: $r \in R, s \in \phi^{-1}(J)$

$$\phi(rs) = \phi(r)\underbrace{\phi(s)}_{\in J} \in J \Rightarrow rs \in \phi^{-1}(J).$$

(ii) $\phi(I) \subset S$ ist eine abelsche Untergruppe (wurde früher gezeigt).

Zu zeigen: $S \cdot \phi(I) \subset \phi(I)$
Sei $s \in S, y = \phi(x) \in \phi(I)$. Da ϕ surjektiv ist, gibt es $r \in R$ mit $\phi(r) = s$.

$$\Rightarrow sy = \phi(r)\phi(x) = \phi\underbrace{(rx)}\ r \in R, x \in I \Rightarrow rx \in I \in \phi(I).$$

□

Satz 5.29
Es gibt eine Bijektion:

$$\{\hat{J}; \hat{J} \text{ ist Ideal in } R, I \subset \hat{J}\} \overset{1:1}{\longleftrightarrow} \{J; J \text{ ist Ideal in } {}^{R}\!/_{I}\}$$

$$\hat{J} \mapsto \phi(\hat{J}) \tag{5.5.a}$$

$$\phi^{-1}(J) \hookleftarrow J \tag{5.5.b}$$

Beweis. Die Abbildungen (5.5.a) und (5.5.b) sind zueinander invers.

(i) $\phi(\phi^{-1}(J)) = J$, da ϕ surjektiv ist.

(ii) Zu zeigen: $\phi^{-1}(\phi(\hat{J})) = \hat{J}$.

„$\subset$“: ist klar.

„$\supset$“: Sei $x \in \phi^{-1}(\phi(\hat{J})) \Rightarrow \phi(x) \in \phi(\hat{J}) \Rightarrow$ Es gibt $y \in \hat{J}$ mit $\phi(x) = \phi(y) \Rightarrow$ $\phi(x) - \phi(y) = 0 \Rightarrow \phi(x - y) = 0 \Rightarrow x - y \in I$, d.h. $x - y = i$ mit $i \in I$ $\Rightarrow x = \underbrace{y}_{\in \hat{J}} + \underbrace{i}_{\in I \in \hat{J}} \in \hat{J}$.

□

Bemerkung 5.30
Falls $J = \phi(\hat{J})$ ist, so ist $J = \{\bar{l}; l \in \hat{J}\} = \{l + I; l \in \hat{J}\}$. Dies rechtfertigt die Schreibweise $J = {}^{\hat{J}}\!/_{I}$.

Noetherscher Isomorphiesatz

$$I \subset L \subset R, R\text{: Ring}; I, L\text{: Ideale in } R$$
$$\rightsquigarrow {}^{L}\!/_{I} \subset {}^{R}\!/_{I} \text{ ist ein Ideal (siehe Satz (5.29))}$$

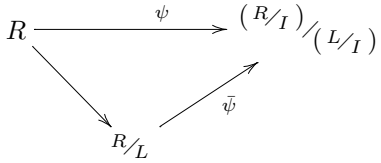
Satz 5.31 (Noetherscher Isomorphiesatz)
Es gibt einen natürlichen Isomorphismus

$${}^{R}\!/_{L} \cong {}^{\left({}^{R}\!/_{I}\right)}\!/_{\left({}^{L}\!/_{I}\right)}.$$

Beweis. Wir betrachten die folgenden Projektionen:

$$R \to {}^{R}\!/_{I} \to {}^{\left({}^{R}\!/_{I}\right)}\!/_{\left({}^{L}\!/_{I}\right)}.$$

Damit ist $L \subset \ker \psi$. Damit liefert uns die universelle Eigenschaft:



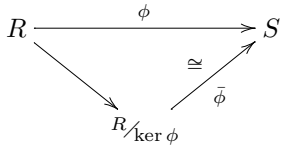
Behauptung: $\bar{\psi}$ ist ein Isomorphismus

- $\bar{\psi}$ surjektiv, da ψ surjektiv ist.
- $\bar{\psi}$ injektiv: Sei $r \in R$ mit $\bar{\psi}(\bar{r}) = 0$.

$$\Rightarrow \psi_1(r) \in {}^{L}\!/_{I}$$
$$\Rightarrow r \in \psi_1^{-1}\left({}^{L}\!/_{I}\right) = L$$
$$\Rightarrow \bar{0} = \bar{r} \in {}^{R}\!/_{L}.$$

□

Es sei $\phi\colon R \to S$ eine Surjektion. Nach früherem liefert uns dies:



d.h. $\bar{\phi}\colon {}^{R}\!/_{\ker \phi} \cong S$. (Satz (5.11)).

Sei $i \subset S$ ein Ideal. Dann ist:

$$\ker \phi \subset \phi^{-1}(I) \subset R$$

Wir betrachten:

$$\psi\colon R \to {}^{R}\!/_{\ker\phi} \cong S \to {}^{S}\!/_{I}$$

Korollar 5.32
ψ induziert einen Isomorphismus

$$\bar{\psi}\colon {}^{R}\!/_{\phi^{-1}(I)} \cong {}^{S}\!/_{I}$$

Beweis. Der Noethersche Isomorphiesatz (5.31) liefert

$${}^{R}\!/_{\phi^{-1}(I)} \cong {}^{\left({}^{R}\!/_{\ker\phi}\right)}\!/_{\left({}^{\phi^{-1}(I)}\!/_{\ker\phi}\right)} = {}^{S}\!/_{I}\,.$$

□

5.5 Primideale und maximale Ideale

Definition 5.33
Ein Ideal $p \subset R, p \neq R$ heißt *Primideal*, falls gilt: $rs \in p \Rightarrow r \in p$ oder $s \in p$.

Beispiel 5.34

(i) Es gilt

$$\{0\} \text{ ist Primideal } \Leftrightarrow R \text{ ist ein Integritätsring}$$

$[rs = 0 \Rightarrow r = 0 \text{ oder } s = 0]$.

(ii) R sei faktorieller Ring und $p \in R$ sei ein Primelement. Dann ist (p) ein Primideal.

Satz 5.35
$p \subset R$ ist Primideal $\Leftrightarrow$ ${}^{R}\!/_{P}$ ist ein Integritätsring.

Beweis. „$\Rightarrow$“ ${}^{R}\!/_{P}$ sei kein Integritätsring. Dann gibt es $\bar{r}, \bar{s} \in {}^{R}\!/_{P}\,.\ \bar{r} \neq 0, \bar{s} \neq 0$ mit $\bar{r}\bar{s} = 0 \Rightarrow r \notin p, s \notin p$ aber $rs \in p \Rightarrow p$ ist kein Primideal.

„$\Leftarrow$“ $rs \in p \Rightarrow 0 = \bar{r}\bar{s} \in {}^{R}\!/_{P} \Rightarrow \bar{r}\bar{s} = \bar{0} \overset{{}^{R}\!/_{P}\text{ Integritätsring}}{\Longrightarrow} \bar{r} = 0$ oder $\bar{s} = 0 \Rightarrow r \in p$ oder $s \in p$.

□

Definition 5.36
Ein Ideal $m \subset R$ heißt *maximales Ideal*, falls gilt:

(i) $m \neq R$.

(ii) Ist I ein Ideal mit $m \subsetneq I$, dann ist $i = R$.

Satz 5.37
$m \subset R$ ist maximales Ideal $\Leftrightarrow$ ${}^{R}\!/_{m}$ ist ein Körper.

Folgerung 5.38

$$\begin{array}{l} m \text{ maximales Ideal} \Rightarrow m \text{ ist Primideal.} \\ \qquad\qquad \Downarrow \\ {}^{R}\!/_{m} \text{ ist Körper} \\ \Rightarrow {}^{R}\!/_{m} \text{ ist Integritätsring} \end{array}$$

Beweis. „⇒“ Zu zeigen: Ist $\bar{r} \in {}^{R}\!/\!_{m}\,, \bar{r} \neq 0$, so hat $\bar{r}$ ein multiplikatives Inverses.

Definiere:

$$I := m + Rr = \{s + r'r, s \in m, r' \in R\} \subset R \text{ Ideal}$$

Da $r \notin m$ ist $I \supsetneq m$. Da m maximal ist, folgt $I = R$. Also ist $1 \in I$, d.h. es gibt $s \in m, r' \in R$: $s + r'r = 1 \Rightarrow \bar{r}'\bar{r} = \bar{1}$.

„⇐“ Sei $I \supsetneq m, I \subset R$ Ideal. Zu zeigen: $I = R$.

Betrachte:

$$\phi\colon R \to {}^{R}\!/\!_{m}\,.$$

$\phi(I) = {}^{I}\!/\!_{m}$ ist dann ein Ideal, $\neq \{0\}$ in ${}^{R}\!/\!_{m}$. Da ${}^{R}\!/\!_{m}$ ein Körper ist, folgt ${}^{I}\!/\!_{m} = {}^{R}\!/\!_{m}$. Es gilt:

$$I = \phi^{-1}(\phi(I)) = \phi^{-1}({}^{I}\!/\!_{m}) = \phi^{-1}({}^{R}\!/\!_{m}) = R.$$

□

Satz 5.39

(i) Die Primideale in $\mathbb{Z}$ sind (0) und die Ideale (p) mit $p \geq 2$ prim. Die maximalen Ideale sind (p) mit $p \geq 2$ prim.

(ii) Im Ring $R = K[X]$ sind die Primideale die Ideale (0) und (f) wobei $f \in K[X]$ irreduzibel ist mit $\deg f > 0$. Die maximalen Ideale sind die Ideale (f) mit $f \in K[X]$ irreduzibel, $\deg f > 0$.

Beweis. $R = \mathbb{Z}$ ($R = K[X]$ völlig analog)

(0) ist Primideal, da $\mathbb{Z}$ Integritätsring ist. (0) ist nicht maximal, etwa $(0) \subsetneq (7) \subsetneq \mathbb{Z}$. $\mathbb{Z}$ ist kein maximales Ideal.

Sei $I = (n), n \geq 2$. n sei *nicht prim*: $n = p \geq 2$. Zu zeigen: (p) ist maximales Ideal: ($\Rightarrow$ Primideal)

Sei $I \subset \mathbb{Z}$ Ideal, $I \supsetneq (p)$. Es ist $I = (k)$. Da $(p) \subset I$ folgt $p \in (k) \Rightarrow p = k \cdot l \Rightarrow k | p \overset{p \text{ prim}}{\Longrightarrow} k = 1$ oder $k = p \Rightarrow (k) = (1) = \mathbb{Z}$ oder $(k) = (p)$, d.h. $I = (p)$ ↯. □

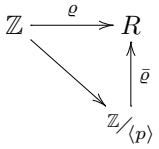
Korollar 5.40

(i) Für jedes Primideal $p \geq 2$ ist $\mathbb{Z}_p = {}^{\mathbb{Z}}\!/\!_{\langle p \rangle}$ ein Körper mit p Elementen.

(ii) Ist R ein Integritätsring der Charakteristik p, so ist der Primring von R isomorph zum Körper $\mathbb{Z}_p$.

Beweis. (i) klar

(ii)



$\varrho(1) = 1, \ker \varrho = \langle p \rangle$. Primring $= \varrho(\mathbb{Z}) \cong \bar{\varrho}({}^{\mathbb{Z}}\!/\!_{\langle p \rangle}) \cong \bar{\varrho}(\mathbb{Z}_p)$. Da $\bar{\varrho}$ injektiv ist, ist der Primring isomorph zu $\mathbb{Z}_p$.

□

Anwendung: (später wichtig für die Galoistheorie)
K: Körper, $f \in K[X]$ irreduzibel, $\deg f > 0 \Rightarrow \langle f \rangle$ maximal $\Rightarrow {}^{K[X]}\!/_{\langle f \rangle}$ ist ein Körper.

Satz 5.41
$f \in K[X]$ sei irreduzibel, $\deg f > 0$. Dann ist ${}^{K[X]}\!/_{\langle f \rangle}$ eine endliche Körpererweiterung vom Grad $n = \deg f$ über K.

Wiederholung: $L \supset K; [L : K] = \dim_K L$ Grad der Körpererweiterung.

Beweis. Wir betrachten $K \subset K[X] \to {}^{K[X]}\!/_{\langle f \rangle}$. Diese Abbildung ist injektiv, d.h. ${}^{K[X]}\!/_{\langle f \rangle}$ ist Körpererweiterung von K.
Diese Körpererweiterung wird erzeugt von $\bar{X}$ ($\bar{X} = X + \langle f \rangle$).
Genügt: $\bar{X}$ ist algebraisch über K vom Grad n. In ${}^{K[X]}\!/_{\langle f \rangle}$: $f(\bar{X}) = 0$.
Also ist $\bar{X}$ algebraisch vom Grad $\leq n$. Sei g das Minimalpolynom von $\bar{X} \Rightarrow g | f \overset{f \text{ irreduz.}}{\Longrightarrow} g = c \cdot f, c \in K^* \Rightarrow \deg \bar{X} = \deg g = \deg f = n$. □

Beispiel 5.42

(i) In $K[X, Y]$ ist etwa $\langle X \rangle$ ein Primideal, aber nicht maximal.

(ii) $\langle X, Y \rangle$ ist ein maximales Ideal.

Satz 5.43 (Krull)
Sei $I \subsetneq R$ ein Ideal. Dann gibt es ein maximales Ideal $m \subset R$ mit $I \subset m$.

Zornsches Lemma $\mathcal{M}$: System von Mengen, $K \subset \mathcal{M}$

Definition 5.44

(i) K heißt eine *Kette*, falls gilt: $K_1, K_2 \in K \Rightarrow K_1 \subset K_2$ oder $K_2 \subset K_1$.

(ii) Ein Element $M \in$
$mathcal M$ heißt *maximal*, falls gilt: Ist $N \in \mathcal{M}, M \subset N$ so folgt $M = N$.

Lemma 5.45 (Zornsches Lemma (Axiom), 1. Fassung)
$\mathcal{M}$ sei ein nicht-leeres Mengensystem. Für jede Kette $\mathcal{K} \subset \mathcal{M}$ gelte

$$\bigcup_{K \in \mathcal{K}} K \in \mathcal{M}.$$

Dann gibt es ein maximales Element in $\mathcal{M}$.

Beweis. (Satz von Krull (5.43)) Betrachte

$$\mathcal{M} := \{J; J \neq R \text{ ist Ideal und } J \supset I\}$$

$\mathcal{M}$ ist nicht-leer, da $I \in \mathcal{M}$. *Ziel*: Finde maximales Element in $\mathcal{M}$. Dies folgt mit Hilfe des Zornschen Lemmas (5.45).
$\mathcal{K} \subset \mathcal{M}$ Kette. Sei

$$\hat{\mathcal{K}} := \bigcup_{K \in \mathcal{K}} K.$$

Zu zeigen: $\hat{\mathcal{K}} \in \mathcal{M}$. $\hat{\mathcal{K}}$ ist *Ideal*:

(i) $x, y \in \hat{\mathcal{K}} \Rightarrow x \in K_1, y \in K_2 \overset{\substack{\mathcal{K} \text{ Kette} \\ K_1, K_2 \in \mathcal{K}}}{\Longrightarrow} K_1 \subset K_2$ oder $K_2 \subset K_1 \overset{\text{etwa } K_1 \subset K_2}{\Longrightarrow}$
$x, y \in K_2 \Rightarrow x + y \in K_2 \Rightarrow x + y \in \hat{\mathcal{K}}$.

(ii) $R \cdot \hat{\mathcal{K}} \subset \hat{\mathcal{K}}$ völlig analog

(iii) $\hat{\mathcal{K}} \supset I$ (trivial)

(iv) Bleibt: $\hat{\mathcal{K}} \neq R$. Sei $\hat{\mathcal{K}} = R \Rightarrow 1 \in \hat{\mathcal{K}} \Rightarrow$ Es gibt i mit $1 \in K_i \overset{K_i \text{ Ideal}}{\Longrightarrow} K_i = R \Rightarrow K_i \notin \mathcal{M}$ $\lightning$

□

Kapitel 6

Algebraische Körpererweiterungen (Teil 2)

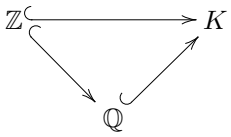
6.1 Einfache algebraische Körpererweiterungen

K: Körper

Definition 6.1
Der *Primkörper* von K ist der Durchschnitt aller Unterkörper von K.

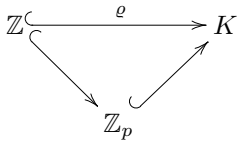
Bemerkung 6.2
Der Primkörper ist der von 1 erzeugte Unterkörper von K.

$\underline{\operatorname{char} K = 0:}$



$$n \mapsto n \cdot 1 = \underbrace{1 + \cdots + 1}_{n}$$

$\underline{\operatorname{char} K = p > 0:}$



Satz 6.3

(i) Ist die Charakteristik $\operatorname{char} K = 0$*, so ist der Primkörper isomorph zu* $\mathbb{Q}$*.*

(ii) Ist $\operatorname{char} K = p > 0$*, so ist der Primkörper isomorph zu* $\mathbb{Z}_p$*.*

Beweis. Siehe oben. □

Satz 6.4
Ist K ein endlicher Körper, so ist die $\operatorname{char} K = p > 0$*. K enthält p^m ($m \in \mathbb{N}$) Elemente.*

Beweis. $\operatorname{char} K = 0 \Rightarrow \mathbb{Q} \hookrightarrow K \Rightarrow |K| = \infty$. Also ist $\operatorname{char} K = p > 0$, der Primkörper ist isomorph zu $\mathbb{Z}_p$. D.h. K ist eine Körpererweiterung von $\mathbb{Z}_p$, also ist K ein $\mathbb{Z}_p$–Vektorraum der Dimension

$$m := [K : \mathbb{Z}_p] < \infty.$$

$\Rightarrow K \cong \mathbb{Z}_p^m$ (als Vektorraum!) $\Rightarrow |K| = p^m$. □

Bemerkung 6.5
Es gibt zu jedem p, m genau einen (bis auf Isomorphie) Körper mit p^m Elementen ($GF(p; m)$).

Definition 6.6
Eine Körpererweiterung L/K heißt *einfach*, falls es ein Element $x \in L$ gibt mit $L = K(x)$.

Beispiel 6.7

(i) $\mathbb{C} = \mathbb{R}(i)$

(ii) $L = K(X)$ (Körper der rationalen Funktionen über K in X)

(iii) $f \in K[X]$ irreduzibel $\deg f > 0$.

$$L := {}^{K[X]}\!/_{\langle f \rangle} \supset K$$

$L = K(x)$ mit $x = X \bmod \langle f \rangle$.

(iv) $K(X, Y)$ ist keine einfache Körpererweiterung von K.

Satz 6.8
Es sei $L = K(x)$ eine einfache, algebraische Körpererweiterung. Es sei $f(X)$ das Minimalpolynom von x. Dann induziert der Einsetzungshomomorphismus

$$\phi\colon K[X] \to K(x) \qquad (\phi|_K = \mathrm{id}_K; \phi(X) = x)$$

einen Isomorphismus

$$\bar{\phi}\colon {}^{K[X]}\!/_{\langle f \rangle} \cong K(x) = L.$$

Beweis. Es gilt $\langle f \rangle \subset \ker \phi$. $[f(x) = 0]$. Da $\langle f \rangle$ ein maximales Ideal ist, folgt $\langle f \rangle = \ker \phi$.

$$\Rightarrow \bar{\phi}\colon {}^{K[X]}\!/_{\langle f \rangle} \hookrightarrow L = K(x).$$

Da $\operatorname{im} \bar{\phi}$ ein Körper ist, der K und x enthält, ist $\bar{\phi}$ surjektiv, also ein Isomoprhismus. □

$K \subset R, S$ $\qquad (R, S\colon$ Ringe)

Definition 6.9
Ein Ringhomomorphismus $f\colon R \to S$ heißt ein K–Homomorphismus, falls $f|_K = \mathrm{id}_K$ ist.

Damit: Bis auf K–Isomorphie ist jede einfache algebraische Körpererweiterung von der Form ${}^{K[X]}\!/_{\langle f\rangle}$ für ein irreduzibles Polynom $f \in K[X]$ mit $\deg f > 0$.

Bemerkung 6.10

$$ {}^{K[X]}\!/_{\langle f\rangle} \cong {}^{K[X]}\!/_{\langle g\rangle} \underset{\text{i.a.}}{\not\Rightarrow} f \sim g. $$

Satz 6.11
Es sei $f \in K[X]$. Dann gibt es eine einfache algebraische Körpererweiterung L von K, sodass f in L eine Nullstelle hat. ($\deg f > 0$)

Beweis. Es sei g ein irreduzibler Faktor von f, $\deg g > 0$. Betrachte:

$$ L := {}^{K[X]}\!/_{\langle g\rangle} \supset K \qquad \text{(einfach algebraisch)}. $$

Es sei $x := X \bmod g$. ($L = K(x)$). Dann ist nach Konstruktion $g(x) = 0$. □

Satz 6.12
Es seien $f_1, \ldots, f_n \in K[X]$, $\deg f_i > 0$ Polynome. Dann gibt es eine endliche Körpererweiterung L, sodass $f_1, \ldots, f_n$ in L eine Nullstelle besitzen.

Beweis. n–fache Anwendung des Satzes (6.11). □

6.2 Der algebraische Abschluss eines Körpers

$K \subset L$

Früher:

$$ \bar{K}_L := \{x \in L; x \text{ ist algebraisch über } K\} $$
$$ K \subset \bar{K}_L \subset L \qquad \text{„algebraischer Abschluss von } K \text{ in } L\text{“} $$

Wir wollen nun den algebraischen Abschluss ohne Vorgabe eines Oberkörpers L betrachten.

Definition 6.13
Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes Polynom $f \in K[X]$, $\deg f > 0$ in K eine Nullstelle besitzt.

Satz 6.14 (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis. Funktionentheorie, bzw. später im Abschnitt (A.4). □

Beispiel 6.15
$\mathbb{R}, \mathbb{Q}$ sind nicht algebraisch abgeschlossen. ($f(X) = X^2 + 1$).

Satz 6.16
Es sind äquivalent:

(i) K ist algebraisch abgeschlossen.

(ii) Jedes Polynom f zerfällt in Linearfaktoren ($\deg f > 0$).

(iii) Die irreduziblen Polynome positiven Grades sind Linearformen.

(iv) Ist L/K algebraisch, so ist $L = K$.

Lemma 6.17

(i) Es sei $f \in K[X]$ und es sei $f(c) = 0$. Dann gilt $f = (X - c)g$ mit $g \in K[X]$.

(ii) Ein Polynom vom Grad n hat höchstens n verschiedene Nullstellen.

Beweis. (i) Division mit Rest:

$$f = (X - c)g + c' \qquad \text{mit } c' \in K.$$

Aus $f(c) = 0$ folgt dann $c' = 0$.

(ii) sofort aus (i).

□

Beweis. (von Satz (6.16))

(i) ⇒ (ii): Sofort aus Lemma (6.17).

(ii) ⇒ (iii): Klar.

(iii) ⇒ (iv): Sei $x \in L$. Es sei f das Minimalpolynom von x. Wegen (iii) ist f eine Linearform, d.h.

$$f(X) = X - a, \qquad a \in K.$$

$f(x) = 0 \Rightarrow x = a \in K \Rightarrow L = K$.

(iv) ⇒ (i): Es sei $f \in K[X]$, $\deg f > 0$. Kann annehmen, dass f irreduzibel ist. Setze:

$$L = {}^{K[X]}\!/_{\langle f \rangle} \supset K \qquad \text{algebraisch, einfach.}$$

Es ist $f(x) = 0$ mit $x = X \bmod \langle f \rangle \in L$. L/K algebraisch $\overset{\text{(iv)}}{\Rightarrow} K = L$. Dann hat f bereits in K die Nullstelle x.

□

Korollar 6.18
Der algebraische Abschluss $\bar{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis. $f(X) \in \bar{\mathbb{Q}}[X]$; $\deg f > 0$. Da $\bar{\mathbb{Q}} \subset \mathbb{C}$ hat f in $\mathbb{C}$ eine Nullstelle x. Dann ist $\bar{\mathbb{Q}}(x)/\bar{\mathbb{Q}}$ algebraisch und $\bar{Q}/\,\mathbb{Q}$ ist algebraisch $\Rightarrow x$ ist algebraisch über $\mathbb{Q} \Rightarrow x \in \bar{\mathbb{Q}}$. □

Definition 6.19
K sei ein Körper. Ein Körper $\bar{K}$ heißt ein algebraischer Abschluss von K, falls gilt:

(i) $\bar{K}$ ist algebraisch abgeschlossen.

(ii) $\bar{K}/K$ ist algebraisch.

Beispiel 6.20
$\mathbb{C}\,/\,\mathbb{R}$, $\quad \bar{\mathbb{Q}}/\,\mathbb{Q}$

Ziel: Existenz und „Eindeutigkeit“ von $\bar{K}$.

—

Zornsches Lemma (2. Fassung)

M: Menge, $M \neq \emptyset$.

Definition 6.21
Eine *Relation* R ist eine Teilmenge $R \subset M \times M$.

Schreibweise: $a\mathrm{R}b :\Leftrightarrow (a,b) \in R \subset M \times M$

Definition 6.22
Eine *Teilordnung* auf M ist eine Relation R mit folgenden Eigenschaften:

(i) $a\mathrm{R}b$ und $b\mathrm{R}c \Rightarrow a\mathrm{R}c$.

(ii) $a\mathrm{R}b$ und $b\mathrm{R}a \Rightarrow a = b$.

(iii) $a\mathrm{R}a$.

Schreibweise: $a\mathrm{R}b \Leftrightarrow: a \leq b$

Definition 6.23
Eine Teilordnung heißt eine *Ordnung* auf M, falls für je 2 Elemente $a, b \in M$ $a \leq b$ oder $b \leq a$ gilt.

Beispiel 6.24

(i) M' = Menge, $M = \mathfrak{P}(M')$ Potenzmenge von M'

$$U_1 \leq U_2 :\Leftrightarrow U_1 \subset U_2$$

Teilordnung, aber *keine* Ordnung.

(ii) $M = \mathbb{R}$, $a \leq b$ im üblichen Sinn (Ordnung).

Definition 6.25

(i) Ein Element $m \in M$ heißt *maximal* bezüglich der Teilordnung $\leq$, falls gilt: $m \leq m' \Rightarrow m = m'$.

(ii) Es sei N eine Teilmenge von M. Dann heißt ein Element $m \in M$ eine *obere Schranke* von N, falls gilt:

$$n \in N \Rightarrow n \leq m.$$

Lemma 6.26 (Zornsches Lemma, 2. Fassung)
Es sei M eine Menge mit einer Teilordnung $\leq$. Falls jede total geordnete Teilmenge $N \subset M$ eine obere Schranke besitzt, dann gibt es in M ein maximales Element.

Beispiel 6.27
M sei die Potenzmenge einer Menge M': $\leq$ sei durch $\subset$ definiert. Dann ist eine total geordnete Teilmenge dasselbe wie eine Kette. Dann erhält man die 1. Fassung des Zornschen Lemmas (5.45) als Spezialfall zurück.

—

Satz 6.28
Es sei K ein Körper und $\bar{K}$ ein algebraischer Abschluss. Es sei L eine algebraische Körpererweiterug von K und L_0 ein Zwischenkörper von L/K. Es sei $\phi_0 \colon L_0 \to \bar{K}$ ein K–Homomorphismus. Dann gibt es einen K–Homomorphismus $\phi \colon L \to \bar{K}$ mit $\phi|_{L_0} = \phi_0$.

Korollar 6.29
L/K sei algebraisch. Dann gibt es stets eine Inklusion $\phi\colon L \to \bar{K}$ mit $\phi|_K = \mathrm{id}_K$.

Beweis. $L_0 = K, \phi_0 = \mathrm{id}_K$. Dann Satz (6.28). □

$\rightsquigarrow$ Eindeutigkeit von $\bar{K}$ (bis auf K–Isomorphie).

Beweis. (von Satz (6.28)). Betrachte

$$M := \{(L', \phi'); L_0 \subset L' \subset L, \phi'\colon L' \to \bar{K} \text{ mit } \phi'|_{L_0} = \phi_0\}.$$

Es ist $M \neq \emptyset$, da $(L_0, \phi_0) \in M$. Teilordnung auf M:

$$(L_1, \phi_1) \leq (L_2, \phi_2) :\Leftrightarrow L_1 \subset L_2 \text{ und } \phi_2|_{L_1} = \phi_0.$$

Wir wollen hierauf das Zornsche Lemma (6.26) anwenden. Es sei $(L_\lambda, \phi_\lambda)_{\lambda\in\Lambda}$ eine total geordnete Teilmenge von M. Wir benötigen hierfür eine obere Schranke. Hierzu:

$$\tilde{L} := \bigcup_{\lambda\in\Lambda} L_\lambda, \qquad \tilde{\phi}\colon \tilde{L} \to \bar{K} \text{ durch: } x \in L_\lambda, \text{ so setze } \tilde{\phi}(x) := \phi_\lambda(x).$$

(i) $\tilde{L}$ ist ein Körper. (Genau wie beim Satz von Krull (5.43)).
$[x, y \in \tilde{L}$, d.h. $x \in L_{\lambda_1}, y \in L_{\lambda_2}$. Es gilt $L_{\lambda_1} \subset L_{\lambda_2}$ oder $L_{\lambda_2} \subset L_{\lambda_1}$. Sei $L_{\lambda_1} \subset L_{\lambda_2}$, dann ist $x, y \in L_{\lambda_2} \Rightarrow x \pm y, x \cdot y, \frac{x}{y} \in L_{\lambda_2} \subset \tilde{L}]$.

(ii) $\tilde{\phi}$ ist wohldefiniert: $x \in L_\lambda, x \in L_{\lambda'}$. Dann ist $L_\lambda \subset L_{\lambda'}$ oder $L_{\lambda'} \subset L_\lambda$. Sei $L_\lambda \subset L_{\lambda'}$. Da $(L_\lambda, \phi_\lambda) \leq (L_{\lambda'}, \phi_{\lambda'})$ ist $\phi_{\lambda'}|_{L_\lambda} = \phi_\lambda$, also $\phi_\lambda(x) = \phi_{\lambda'}(x)$.

(iii) $\tilde{\phi}$ ist ein Homomorphismus.

(iv) $\tilde{\phi}|_{L_0} = \phi_0$. Dies folgt, da $\phi_\lambda|_{L_0} = \phi_0$ für alle $\lambda \in L$.

$\Rightarrow (\tilde{L}, \tilde{\phi}) \in M$. Nach Konstruktion ist $(\tilde{L}, \tilde{\phi})$ Schranke von $(L_\lambda, \phi_\lambda)_{\lambda\in\Lambda}$.
Zornsches Lemma (6.26) $\Rightarrow M$ besitzt ein maximales Element

$$(L^*, \phi^*).$$

Ziel: $L^* = L$. Dann kann man $\phi := \phi^*$ wählen.

Annahme: $L^* \neq L$. Sei $x \in L \setminus L^*$.

Ziel: Setze ϕ^* zu einem Homomorphismus auf $L^*(x)$ fort. Dann erhalten wir einen Widerspruch zur Maximalität von (L^*, ϕ^*).

Es sei f das Minimalpolynom von x über L^*.

$$\Rightarrow {}^{L^*[X]}\!/_{\langle f\rangle} \cong L^*(x).$$

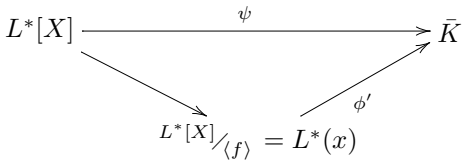
Betrachten:

$$\tilde{\phi}^*\colon L^*[X] \to \bar{K}[X], \quad \sum_i a_i X^i \mapsto \sum_i \phi^*(a_i) X^i.$$

Dann ist $\tilde{\phi}^*(f) \in \bar{K}[X]$. Es sei y eine Nullstelle von $\tilde{\phi}^*(f)$.
Betrachten:

$$\psi\colon L^*[X] \xrightarrow{\tilde{\phi}^*} \bar{K}[X] \xrightarrow{\text{y einsetzen}} \bar{K}.$$

Dann ist $\psi(f) = 0$. $\Rightarrow \langle f \rangle \subset \ker \psi \overset{f \text{ irreduzibel}}{\Longrightarrow} \langle f \rangle = \ker \psi \Rightarrow$



Nach Konstruktion ist $L^*(x) \supsetneqq L^*$ und $\phi'|_{L^*} = \phi^*$ $\lightning$. □

Korollar 6.30
Sind $\bar{K}, \bar{\bar{K}}$ zwei algebraische Abschlüsse von K, so gibt es einen K–Homomorphismus $\bar{K} \cong \bar{\bar{K}}$.

Beweis. Aus Satz (6.28): Es gibt einen K–Homomorphismus $\phi\colon \bar{\bar{K}} \to \bar{K}$. Sei $\tilde{K} := \phi(\bar{\bar{K}}) \subset \bar{K}$. Dann ist $\tilde{K}$ algebraisch abgeschlossen, da $\bar{\bar{K}}$ dies ist.

Da $\bar{K}$ algebraisch ist über K, ist $\bar{K}$ auch algebraisch über $\tilde{K}$. $\Rightarrow \bar{K} = \tilde{K} \Rightarrow$ $\phi\colon \bar{\bar{K}} \xrightarrow{\cong} \bar{K}$ und nach Konstruktion ein K–Homomorphismus. □

Satz 6.31 (Steinitz)
Zu jedem Körper K gibt es einen algebraischen Abschluss.

Beweis. Wir betrachten die folgende Familie von Unbestimmten

$$\{X_f\}_{f \in K[X]}.$$

Dazu gehört der Polynomring in unendlich vielen Variablen:

$$K[\{X_f\}].$$

Wir betrachten hierin folgendes Ideal:

$$I := \text{ Ideal erzeugt von den Polynomen } f(X_f)$$
$$I \subset K[\{X_f\}]$$

1. Schritt: $I \neq K[\{X_f\}]$. Ansonsten

$$1 = \sum_{i=1}^{m} g_i f_i(X_{f_i}); \qquad g_i \in K[\{X_f\}]. \tag{$*$}$$

In dieser Relation kommen endlich viele Unbestimmte $X_{f_1}, \ldots, X_{f_n}$, $n \geq m$ vor. Es sei L eine algebraische Körpererweiterung von K, in der die Polynome $f_1, \ldots, f_m$ eine Nullstelle $x_1, \ldots, x_m$ haben. Wir betrachten:

$$\begin{aligned} K[X_{f_1}, \ldots, X_{f_n}] &\to L \qquad (K\text{–Homomorphismus}) \\ X_{f_i} &\mapsto x_i \qquad i = 1, \ldots, m \\ X_{f_j} &\mapsto 0 \qquad j \geq m+1. \end{aligned}$$

Dann geht $(*)$ über in

$$1 = \sum_{i=1}^{m} g_i \underbrace{f_i(x_i)}_{=0} = 0 \quad \lightning.$$

2. Schritt: Nach dem Satz von Krull (5.43) gibt es ein maximales Ideal m mit

$$I \subset m.$$

Setze

$$E_1 := {}^{K[\{X_f\}]}\!/_{m} \quad (E_1 \text{ ist ein Körper}).$$

Da $K \cap m = \{0\}$ ist $K \hookrightarrow E_1$, d.h. E_1 ist eine Körpererweiterung von K.

E_1 ist *algebraische* Körpererweiterung von K:
Setze $x_f := X_f \bmod m$.

Da E_1 von diesen Elementen erzeugt wird, genügt es zu zeigen, dass die x_f algebraisch sind. Dies folgt, da $f(X_f) \in I \subset m$, d.h. $f(x_f) = 0$.

3. Schritt: Iteration dieser Konstruktion.

Wir konstruieren eine Kette

$$K = E_0 \subset E_1 \subset E_2 \subset \cdots$$

wobei E_i aus E_{i-1} durch die Konstruktion in Schritt 2 entsteht.

$$E_{n+1}/E_n \text{ ist algebraisch}, E_n/E_{n-1} \text{ ist algebraisch}$$
$$\cdots \Rightarrow E_n/K \text{ ist algebraisch für alle } n \geq 1.$$

4. Schritt:

$$\bar{K} := \bigcup_{n \geq 0} E_n.$$

$\bar{K}$ ist ein Körper, $K \subset \bar{K}$, und $\bar{K}/K$ ist algebraisch.

Zu zeigen bleibt: $\bar{K}$ ist algebraisch abgeschlossen.
Sei $F \in \bar{K}[X]$. Zu zeigen: $\bar{F}$ hat in $\bar{K}$ eine Nullstelle. Es gibt ein n mit $F \in E_n[X]$. Nach Konstruktion hat F dann eine Nullstelle in E_{n+1} und damit auch in $\bar{K}$.

□

Zerfällungskörper

K: Körper; $f \in K[X]$

Definition 6.32
L heißt *Zerfällungskörper* von f, falls:

(i) f zerfällt über L in Linearformen.

(ii) $L = K[x_1, \ldots, x_n]$, wobei die x_i die Nullstellen von f in L sind.

Bemerkung 6.33
In der Definition (6.32) gilt: $K[x_1, \ldots, x_n] = K(x_1, \ldots, x_n)$.

Satz 6.34
Sei $f \in K[X]$, $\deg f > 0$. Dann gilt:

(i) Es gibt einen Zerfällungskörper L von f.

(ii) Je zwei Zerfällungskörper sind K–isomorph.

Beweis. (i) Sei $\bar{K}$ ein algebraischer Abschluss von K. Dann hat f in $\bar{K}$ die Nullstellen $x_1, \ldots, x_n$. Setze

$$L := K[x_1, \ldots, x_n] \quad (= K(x_1, \ldots, x_n)).$$

Dieses L ist ein Zerfällungskörper.

(ii) Es sei L' ein weiterer Zerfällungskörper. Da L' algebraisch ist über K, gibt es einen K–Homomorphismus $\phi\colon L' \to \bar{K}$. Dann ist $L'' := \phi(L') \cong L'$ ebenfalls Zerfällungskörper.

Da ϕ Nullstellen von f auf Nullstellen abbildet, folgt

$$L'' \subset L. \tag{6.6.a}$$

Umgekehrt zerfällt f über L'', d.h. $x_1, \ldots, x_n \in L''$, damit

$$L \subset L'' \tag{6.6.b}$$
$$(6.6.a), (6.6.b) \Rightarrow L = L'' \Rightarrow L \cong_K L'.$$

□

6.3 Separabilität

$f \in K[X]$; $\bar{K}$ algebraischer Abschluss
Dann zerfällt f über $\bar{K}$:

$$f(X) = \kappa \prod_{i=1}^{n} (X - x_i)^{\nu_i}; \qquad x_1, \ldots, x_n \text{ Nullstellen von } f.\ \kappa \in K.$$

Definition 6.35
Ein Polynom $f \in K[X]$ heißt *separabel*, falls f irreduzibel ist und in $\bar{K}$ keine mehrfachen Nullstellen besitzt. Ansonsten heißt das Polynom *inseparabel*.

Ableitung:

$$f \in R[X]; \qquad R\colon \text{ Ring}$$
$$f(X) := \sum_{\nu=0}^{n} r_\nu X^\nu, \qquad r_\nu \in R.$$

Definition 6.36
Die *Ableitung* (formale Ableitung) von f ist definiert durch

$$f'(X) := \sum_{\nu=0}^{n} \nu r_\nu X^{\nu-1}.$$

Achtung: $f' = 0 \not\Rightarrow f = c \in R$.

Beispiel 6.37

(i) $f(X) = 4X^3 \in \mathbb{Z}_{12}[X]; \quad f'(X) = \underbrace{3 \cdot 4}_{=12} X^2 = 0 \in \mathbb{Z}_{12}[X].$

(ii) $f(X) = X^p - 1 \in \mathbb{Z}_p[X] \Rightarrow f'(X) = pX^{p-1} = 0 \in \mathbb{Z}_p[X].$

Satz 6.38
Für $f, g \in R[X]$ gilt:

(i) $\deg f' < \deg f$.

(ii) $f = r \in R \Rightarrow f' = 0$.

(iii) $(f+g)' = f' + g'$.

(iv) $(rf)' = rf' \quad (r \in R)$.

(v) $(fg)' = f'g + fg'$.

Beweis. (v) Wegen (iii) und (iv) genügt es, dies für $g = X^m$ zu zeigen.

$$f(X) = \sum_{\nu=0}^{n} r_\nu X^\nu \Rightarrow gf = \sum_{\nu=0}^{n} r_\nu X^{\nu+m} \Rightarrow (gf)' = \sum_{\nu=1}^{n} (\nu+m) r_\nu X^{\nu+m-1}$$
$$= \Big(\sum_{\nu=1}^{n} \underbrace{\nu r_\nu X^{\nu-1}}_{f'}\Big) \underbrace{X^m}_{g} + \Big(\sum_{\nu=1}^{n} r_\nu X^\nu\Big) \underbrace{X^{m-1} m}_{g'}.$$

□

Korollar 6.39
Ist $f(X) = r(X-a)^m; r, a \in R$. Dann ist

$$f'(X) = m \cdot r \cdot (X-a)^{m-1}.$$

Beweis. Induktion

$\underline{m = 1:}$ $f(X) = r(X-a) = rX - ra \Rightarrow f'(X) = r = r \cdot 1 (X-a)^0$.

$\underline{m \mapsto m+1:}$

$$f(X) = r(X-a)^{m+1} = \underbrace{r(X-a)^m}_{g} \underbrace{(X-a)}_{h}$$
$$\overset{(v)}{\Rightarrow} f'(X) = g'h + gh'$$
$$\overset{IV}{=} mr(X-a)^{m-1}(X-a) + r(X-a)^m \cdot 1$$
$$= (mr + r)(X-a)^m$$
$$= (m+1) r (X-a)^m.$$

□

R: Integritätsring, $\operatorname{char} R = p > 0 \qquad (\underbrace{1 + \cdots + 1}_{p} = 0)$ $(p \geq 2$ prim$)$

$$F\colon R \to R \qquad \textit{Frobeniushomomorphismus}$$
$$r \mapsto r^p$$

F ist ein Homomorphismus, d.h.

$$F(r_1 + r_2) = f(r_1) + F(r_2) \quad \leftarrow (r_1 + r_2)^p \overset{!}{=} r_1^p + r_2^p$$
$$F(r_1 \cdot r_2) = F(r_1) \cdot F(r_2)$$
$$F(1) = 1$$

Beispiel 6.40
$R = \mathbb{Z}_3$

$$\begin{aligned}(r_1+r_2)^3 &= r_1^3 + 3r_1^2r_2 + 3r_1r_2^2 + r_2^3 \\ &= r_1^3 + \varrho(3)r_1^2r_2 + \varrho(3)r_1r_2^2 + r_2^3 \\ &= r_1^3 + \bar{0}\cdot r_1^2r_2 + \bar{0}\cdot r_1r_2^2 + r_2^3 \\ &= r_1^3 + r_2^3\end{aligned} \qquad \begin{aligned}&\varrho\colon \mathbb{Z}\to\mathbb{Z}_3 \\ &1\mapsto\bar{1} \\ &2\mapsto\bar{2} \\ &3\mapsto\bar{3}=\bar{0}\end{aligned}$$

6.3.1 Frobenius Homomorphismus

R: Ring, $\operatorname{char} R = p; p$ prim
$F\colon R\to R, \quad r\mapsto r^p$

Satz 6.41

(i) *F ist ein Ringhomomorphismus*

(ii) *R Integritätsring $\Rightarrow$ F ist injektiv*

(iii) $\operatorname{im}(F) =: R^p = \{r^p; r\in R\} \subset R$ *ist ein Unterring*

(iv) *Ist R ein Körper, dann auch R^p.*

F heißt der Frobeniushomomorphismus.

Beweis. (i)

$$F(rr') = (rr')^p = r^p(r')^p = F(r)F(r')$$

$$F(r+r') = (r+r')^p \overset{\text{binom. Lehrsatz}}{=} \sum_{i=0}^{p} \underbrace{\binom{p}{i}}_{\text{eigentlich } \varrho\binom{p}{i}} r^{p-i}(r')^i$$

(wobei $\varrho\colon \mathbb{Z}\to R,\ \varrho(n) = \underbrace{1+\cdots+1}_{n}$)

Es gilt:

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

Also gilt: $i\neq 0$, $p\colon p\mid\binom{p}{i} \Rightarrow \varrho\binom{p}{i} = 0$.

$$\Rightarrow (r+r')^p = \underbrace{\binom{p}{0}}_{=1} r^p + \underbrace{\binom{p}{p}}_{=1} r'^p = r^p + r'^p = F(r) + F(r').$$

(ii) Sei $r\neq 0$ mit $F(r)=0$, d.h. $r^p = 0$. Wähle $n\leq p$ minimal mit $r^p = 0$ $(n\geq 2)$
$\Rightarrow \underbrace{r}_{\neq 0}\underbrace{(r^{n-1})}_{\neq 0} = r^n = 0 \Rightarrow R$ hat Nullteiler.

(iii) Klar, da $(r+r')^p = r^p + (r')^p$, $(rr')^p = r^p\cdot r'^p$.

(iv) Klar, da $r\neq 0$. $(r^p)\cdot(\frac{1}{r})^p = 1^p = 1$.

□

6.3.2 Separable / inseparable Körpererweiterungen

Erinnerung: $f \in K[X]$ sei irreduzibel. Dann heißt f *separabel*, falls f in $\bar{K}$ keine mehrfachen Nullstellen besitzt, ansonsten heißt f *inseparabel*.

Satz 6.42
Es sei $f \in K[X]$, $\deg f > 0$ irreduzibel. Dann sind äquivalent:

(i) f *ist inseparabel.*

(ii) $f' = 0$.

(iii) $f = g(X^{p^e})$ *wobei* $p = \operatorname{char} K > 0$, $e \geq 1$ *und* g *separabel ist.*

Bemerkung 6.43
Inseparabilität tritt nur in positiver Charakteristik auf.

Beispiel 6.44

$$f(X) := X^p - t \in (\underbrace{\mathbb{Z}_p[t]}_{R})[X]$$

$f(X)$ ist irreduzibel in $R[X]$ nach Eisenstein (Primelement: t). Nach Gauß (4.12) ist $f(X)$ auch irreduzibel in

$$f(X) \in (\underbrace{\mathbb{Z}_p(t)}_{K})[X].$$

Es ist

$$f'(X) = pX^{p-1} = 0.$$

Beweis. (i)⇒(ii): f inseparabel ⇒ f hat in $\bar{K}$ eine mehrfache Nullstelle $a \in \bar{K}$.

$$\begin{aligned} &\Rightarrow f(X) = (X-a)^m h(X) \qquad (\text{über } \bar{K}) \\ &\Rightarrow f'(X) = m(X-a)^{m-1}h(X) + (X-a)^m h'(X) \\ &\Rightarrow f'(a) = 0 \end{aligned}$$

Betrachte den Auswertungshomomorphismus

$$\phi\colon K[X] \to \bar{K},\ g \mapsto g(a)$$

$\Rightarrow f \in \ker\phi \overset{f \text{ irred.}}{\Rightarrow} \langle f\rangle = \ker\phi$.
Andererseits ist

$$f'(a) = 0 \Rightarrow f' \in \langle f\rangle.$$

Da

$$\deg f' < \deg f \Rightarrow f' = 0.$$

(ii)⇒(iii) $f(X) = a_0 + a_1X + \cdots + a_nX^n \Rightarrow 0 = f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1} \Rightarrow i\cdot a_i = 0$ für $i = 1,\ldots,n \Rightarrow i = 0$ oder $a_i = 0$ für $i = 1,\ldots,n$.
Alle $a_i = 0$ für $i = 1,\ldots,n$ bedeutet, dass $f = a_0$ $(\lightning)$

$$\begin{aligned} &\Rightarrow \text{ mindestens ein } i = 0, i \geq 1, \text{ d.h. } \operatorname{char} K = p > 0 \\ &\Rightarrow f(X) = \sum_{i=0} a_{i\cdot p}X^{i\cdot p} = \sum_{i=0} a_{i\cdot p}(X^p)^i =: f_1(X^p). \end{aligned}$$

Da $f(X)$ irreduzibel ist, gilt dies auch für $f_1(X)$. Falls f_1 separabel ist, ist man fertig. Ansonsten liefert die Fortsetzung des Verfahrens, dass

$$f(X) = g(X^{p^l}).$$

Dies muss abbrechen und g ist schließlich separabel.

(iii)⇒(i): Sei

$$f(X) = g(X^{p^l}) = \sum_{i=0}^{m} a_i (X^{p^l})^i.$$

In $\bar{K}$ hat die Gleichung

$$X^{p^l} - a_i = 0$$

eine Nullstelle, d.h. es gibt ein $b_i \in \bar{K}$ mit $a_i = (b_i)^{p^l}$

$$\Rightarrow f(X) = \sum_{i=0}^{m} (b_i)^{p^l} (X^{p^l})^i = \sum_{i=0}^{m} (b_i)^{p^l} (X^i)^{p^l}$$

$$\overset{\text{Frobenius}}{=} (\sum_{i=0}^{m} b_i X^i)^{p^l}$$

$$\Rightarrow f \text{ hat in } \bar{K} \text{ mehrfache Nullstellen}$$

$$\Rightarrow f \text{ ist inseparabel.}$$

□

Definition 6.45
L/K sei eine algebraische Körpererweiterung

(i) $x \in L$ heißt *separabel* über K, falls das Minimalpolynom von $f(X)$ separabel ist.

(ii) L/K heißt *separabel*, falls jedes Element $x \in L$ separabel über K ist.

Satz 6.46
$[L : K]$ sei $n < \infty$. Dann sind äquivalent:

(i) L/K ist eine separable Körpererweiterung.

(ii) Es gibt genau n verschiedene K–Homomorphismen von $L \to \bar{K}$.

Beispiel 6.47
$L = \mathbb{C} = \bar{K}, K = \bar{K}$ ist separabel, da $\operatorname{char} K = 0$.
Frage: Wie viele $\mathbb{R}$–Homomorphismen von $\mathbb{C}$ nach $\mathbb{C}$ gibt es?

$$\{\phi \colon \phi \colon \mathbb{C} \to \mathbb{C}, \phi|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}\} = \{\mathrm{id}_{\mathbb{C}}, {}^{-}\}$$

ϕ Homomorphismus, $z \mapsto \bar{z}$ komplexe Konjugation

Vorbereitungen (zum Beweis von Satz (6.46))
L, N Körper, $0 \neq \sigma \colon L \to N$ Körperhomomorphismus
Dies induziert einen Homomorphismus

$$L[X] \to N[X]$$
$$f = \sum a_i X^i \mapsto f^\sigma := \sum \sigma(a_i) X^i.$$

Satz 6.48
Es sei $0 \neq \sigma\colon L \to N$. Es sei $M = L[x]$ eine einfache algebraische Körpererweiterung von L. Es sei f das Minimalpolynom von x. Ferner habe f^σ in N genau m verschiedene Nullstellen. Dann kann man $\sigma\colon L \to N$ auf genau m verschiedene Weisen nach $M = L[x]$ fortsetzen.

Beweis. Es sei $n = [M : L]$. Dann ist

$$M = L[x] = L + Lx + Lx^2 + \cdots + Lx^{n-1}.$$

D.h. ein Homomorphismus $\bar{\sigma}$, der σ fortsetzt ist bereits durch $\bar{\sigma}(x)$ festgesetzt. Es gilt:

$$f(x) = 0 \Rightarrow f^\sigma(\sigma(x)) = \sigma(0) = 0$$

$\Rightarrow \sigma(x)$ muss eine Nullstelle von f^σ sein!

(i) Falls f^σ m Nullstellen hat, gibt es also höchstens m Möglichkeiten für $\bar{\sigma}$.

(ii) Es gibt tatsächlich m Fortsetzungen $\bar{\sigma}$ von σ:
Sei z eine Nullstelle von f^σ. Betrachte:

$$L[x] \to N[x] \to N;\ g \mapsto g^\sigma \mapsto g^\sigma(z).$$

$$\overset{\text{Standardargument}}{\Longrightarrow} \langle f \rangle = \ker \sigma$$
$$\Rightarrow \bar{\phi}\colon \underbrace{{}^{L[x]}\!/_{\langle f \rangle}}_{\cong L[x]=M} \to N.$$

Nach Konstruktion ist

$$\bar{\sigma}(x) = \sigma(x) = z.$$

□

Beweis. (von Satz (6.46))
Es seien $x_1, \ldots, x_t$ gegeben mit

$$L = K[x_1, \ldots, x_t] \qquad \text{(geht, da } [L : K] < \infty\text{)}.$$

Setze:

$$L_0 := K$$
$$L_i := K[x_1, \ldots, x_i]; \qquad n_i := [L_i : L_{i-1}].$$

Dann ist

$$[L : K] = n = \prod_{i=1}^{t} n_i.$$

(i) L/K sei *separabel*:

Dann gibt es nach Satz (6.48) genau n_1 K–Homomorphismen $K[x_1] \to \bar{K}$ (da x_1 separabel ist, d.h. das Minimalpolynom genau n_1 verschiedene Nullstellen hat). Fortsetzung des Verfahrens:
x_2 ist separabel über $K[x_1]$ (da es schon über K separabel ist).

Dann kann man jeden Homomorphismus $K[x_1] \to \bar{K}$ auf genau n_2 Weisen auf $K[x_1, x_2]$ fortsetzen. D.h. wir haben $n_1 \cdot n_2$ K–Homomorphismen von $K[x_1, x_2]$ nach $\bar{K}$.

Nach t Schritten ergeben sich genau $n_1 \cdot \ldots \cdot n_t = n$ K–Homomorphismen von L nach $\bar{K}$.

(ii) L/K sei *inseparabel*:

Dann kann man annehmen, bzw. das Erzeugendensystem so wählen, dass x_1 inseparabel ist über K. Dann erhält man im 1. Schritt $< n_1$ Fortsetzungen und damit insgesamt $< n$ K–Homomorphismen von L nach $\bar{K}$.

□

Korollar 6.49
Es sei $[L : K] = n < \infty$. Es sei M algebraisch über K. Dann gibt es höchstens n K–Homomorphismen von L nach M.

Beweis. Man kann M in $\bar{K}$ einbetten, dann sofort aus Satz (6.48). □

Korollar 6.50
L/K sei algebraisch. Es sei $L = K[x_1, \ldots, x_t]$. Es sei $L_i := K[x_1, \ldots, x_i]$ und x_i sei separabel über L_{i-1}. Dann ist L separabel über K.

Beweis. Sei $n_i := [L_i : L_{i-1}]$. Dann ist

$$n := [L : K] = \prod n_i.$$

In jedem Schritt gibt es n_i Fortsetzungen von $L_{i-1} \to \bar{K}$ nach L_i (Argument des Beweises des Satzes (6.46)).

$$\Rightarrow \text{ Es gibt } n = \prod n_i \text{ } K\text{–Homomorphismen } L \to \bar{K}.$$
$$\overset{\text{Satz (6.46)}}{\Longrightarrow} L/K \text{ ist separabel.}$$

□

6.3.3 Separable Hülle

L/K sei eine Körpererweiterung

Definition 6.51
$L_{sep} := \{x \in L; x \text{ ist separabel über } K\}$. L_{sep} heißt die *separable Hülle* von K in L.

$$K \subset L_{sep} \subset L.$$

Korollar 6.52
L_{sep} ist ein Zwischenkörper von L/K.

Beweis.

$$x, y \in L_{sep} \overset{!}{\Longrightarrow} x \pm y, xy, \frac{x}{y}\,(y \neq 0) \quad \in L_{sep}.$$
$$y \in L_{sep} \overset{(6.50)}{\Longrightarrow} K[y] \text{ ist separabel über } K.$$
$$x \in L_{sep} \overset{\text{insbesondere}}{\Longrightarrow} x \text{ ist separabel über } K[y].$$
$$\overset{(6.50)}{\Longrightarrow} K[x, y] \text{ separabel über } K$$
$$\Longrightarrow K[x, y] \subset L_{sep}$$
$$\Longrightarrow x \pm y, xy, \frac{x}{y} \quad \in L_{sep}.$$

□

Definition 6.53
Der *Separabilitätsgrad* von L/K ist definiert durch $[L_{sep} : K]$.

Korollar 6.54 (Transitivität der Separabilität)
L/N separabel und N/K separabel $\Rightarrow$ L/K ist eine separable Körpererweiterung.

Beweis. Sei $x \in L$; sei $f \in N[X]$ das Minimalpolynom von x über N. Sei

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n; \qquad a_i \in N.$$

Da N separabel ist über K, sind die a_i separabel über K. Es gilt, dass f ein separables Polynom ist, da x separabel ist über N.

$$\begin{aligned} &\Longrightarrow x \text{ ist separabel über } K[a_0, \ldots, a_n]. \\ &\overset{(6.50)}{\Longrightarrow} x \text{ ist separabel über } K. \\ &\Longrightarrow L \text{ ist separabel über } K. \end{aligned}$$

□

Satz 6.55
Sei $[L : K] < \infty$. Dann gilt:

$$[L_{sep} : K] = \#\{\phi; \phi \colon L \to \bar{K} \textit{ ist ein } K\textit{–Homomorphismus}\}.$$

Beweis. Haben bereits gesehen

$$[L_{sep} : K] = \#\{\phi; \phi \colon L_{sep} \to \bar{K} \text{ ist ein } K\text{–Homomoprhismus}\}.$$

Zu zeigen: Jeder Homomorphismus $\phi \colon L_{sep} \to \bar{K}$ kann nur auf eine Weise auf L fortgesetzt werden.
Sei dazu $y \in L \setminus L_{sep}$.
genügt: Das Minimalpolynom von y über L_{sep} hat in $\bar{K}$ nur eine Nullstelle.
Sei $f \in K[X]$ das Minimalpolynom von y über K. Da y nicht separabel ist, hat f folgende Gestalt

$$f(X) = g(y^{p^e}); \qquad e \geq 1,\ g \text{ separabel}$$

$$\Rightarrow 0 = f(y) = g(y^{p^e}) \overset{g \text{ sep.}}{\Longrightarrow} y^{p^e} \in L_{sep} \qquad (p = \operatorname{char} K > 0).$$

Über L_{sep} gilt: y ist Nullstelle von

$$X^{p^e} - y^{p^e} \in L_{sep}[X].$$

Über $\bar{K}$ gilt

$$(X^{p^e} - y^{p^e}) = (X - y)^{p^e} \qquad \text{(Frobenius)}$$

$\Rightarrow$ das Minimalpolynom von y über L_{sep} hat in $\bar{K}$ nur eine Nullstelle. □

6.4 Normale und galoische Körpererweiterungen

L/K Körpererweiterung

Definition 6.56
L/K heißt *normal*, falls

(i) L/K ist algebraisch

(ii) Hat $f \in K[X]$ in L eine Nullstelle, so zerfällt es bereits über L.

Beispiel 6.57

(i) $\bar{K}/K$ ist normal

(ii) $[L:K]=2 \Rightarrow L/K$ ist normal
$(f(a)=0 \Rightarrow f(X)=(X-a)g(X), \deg g(X)=1)$

(iii) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist *nicht* normal
$[X^4-2$ hat in $\mathbb{Q}(\sqrt[4]{2})$ eine Nullstelle, nämlich $\pm\sqrt[4]{2}$, zerfällt aber nicht, da $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})]$.

Satz 6.58
L/K sei algebraisch. Dann sind äquivalent:

(i) L/K ist normal

(ii) Für jeden K–Homomorphismus $\sigma\colon L \to \bar{L}$ gilt $\sigma(L)=L$.

Bemerkung 6.59
$\bar{L}=\bar{K}$ (da $\bar{L}/K$ algebraisch und $\bar{L}$ algebraisch abgeschlossen ist)

Beweis.

(i)⇒(ii): $\sigma(L) \subset L$.

Sei $x \in L$. Es sei $f \in K[X]$ das Minimalpolynom von x über K. Nach Voraussetzung zerfällt f über L, d.h. L enthält alle Nullstellen von f.

$$f(x)=0 \Rightarrow \underbrace{f^{\sigma}(\sigma(x))}_{\substack{= \\ f|_K=\mathrm{id}_K}} = \sigma(0)=0 \overset{\substack{\text{obiges} \\ \text{Argument}}}{\Longrightarrow} \sigma(x) \in L.$$

$L \subset \sigma(L)$.

x wie oben, $x \in L$. Es seien $x=x_1,\dots,x_r$ die Nullstellen von f. Die Abbildung σ definiert eine Permutation

$$\sigma\colon \{x_1,\dots,x_r\} \to \{x_1,\dots,x_r\}.$$

Also gibt es ein i mit $x_1=\sigma(x_i)$. D.h. $x_1=x \in \sigma(L)$.

(ii)⇒(i): Es sei $f \in K[X]$ ein Polynom, das in L eine Nullstelle $x \in L$ besitzt. Es sei y eine weitere Nullstelle von f in $\bar{L}$. Zu zeigen: $y \in L$.

Behauptung:
Es gibt einen K–Homomorphismus $\sigma\colon L \to \bar{\sigma}$ mit $\sigma(x)=y$. Dies genügt, da dann $y \in \sigma(L) \overset{\text{(ii)}}{=} L$.

zur Behauptung: Es gibt einen K–Homomorphismus (Standardargument)

$$\phi\colon K[X] \to \bar{L} \qquad \text{mit } \phi(x)=y.$$

Setze diesen auf L fort, um σ zu erhalten.

□

Definition 6.60
Sei L/K algebraisch, $\sigma\colon L \to \bar{\sigma}$ ein K–Homomorphismus, $x \in L$.

(i) Die Elemente

$$\sigma(x) \in \bar{L}; \sigma\colon L \to \bar{L} \text{ wie oben}$$

heißen die zu x über K *konjugierten Elemente*.

(ii) Die Körper $\sigma(L)$ heißen die zu L *konjugierten Körper*.

Bemerkung 6.61
L/K normal $\Leftrightarrow$ Jeder zu L über K konjugierte Körper ist gleich L.

Beispiel 6.62
$L = \mathbb{C},\ K = \mathbb{R}$

$$\{\sigma\colon \mathbb{C} \to \mathbb{C}; \sigma|_{\mathbb{R}} = id_{\mathbb{R}}\} = \{id_{\mathbb{C}}, \tau\}$$

mit

$$\tau(a + ib) = \overline{a + ib} = a - ib.$$

D.h. die zu x konjugierten Elemente sind: $x, \bar{x}$.

Satz 6.63
Es sei $f \in K[X]$ und L der Zerfällungskörper von f. Dann ist L/K normal.

Beweis. Es seien $x_1, \ldots, x_n$ die Nullstellen von f in $\bar{K} = \bar{L}$. Dann ist

$$L = K[x_1, \ldots, x_n]$$

$\Rightarrow \sigma(L) = K[\sigma(x_1), \ldots, \sigma(x_n)] = K[x_1, \ldots, x_n] = L.$ □

Satz 6.64
Es sei $[L : K] < \infty$ und L/K normal. Dann gibt es ein Polynom $f \in K[X]$, sodass L der Zerfällungskörper von f über K ist.

Beweis. Da $[L : K] < \infty$ gibt es $x_1, \ldots, x_n$ mit

$$L = K[x_1, \ldots, x_n].$$

Es sei f_i das Minimalpolynom von x_i. Setze

$$f := \prod_{i=1}^{n} f_i \quad \in K[X].$$

Es seien $x_1, \ldots, x_n$ $(m \geq n)$ die Nullstellen von f. Da L/K normal ist, gilt:

$$K[x_1, \ldots, x_m] \subset L = K[x_1, \ldots, x_n] \overset{n \leq m}{\subset} K[x_1, \ldots, x_m]$$
$$\Rightarrow L = K[x_1, \ldots, x_m] \quad (= \text{Zerfällungskörper von } f).$$

□

Satz 6.65
Es sind äquivalent:

(i) L/K ist normal

(ii) Es gibt eine Familie $f_\lambda \in K[X]$ von Polynomen $(f_\lambda)_{\lambda \in \Lambda}$, sodass L aus K durch Adjunktion der Nullstellen von f_λ entsteht.

Beweis. (i)⇒(ii): Es sei $(x_\lambda)_{\lambda\in\Lambda}$ eine Familie mit $L = K[(x_\lambda)_{\lambda\in\Lambda}]$. Es sei f_λ das Minimalpolynom von x_λ. Die Nullstellen von f_λ liegen wegen der Normalität von L in L. Diese Nullstellen erzeugen L über K.

(ii)⇒(i): Es sei $f \in K[X]$ und sei $x \in L$ mit $f(x) = 0$. Zu zeigen ist, dass dann f über L zerfällt. Es gibt endlich viele Polynome $f_{\lambda_1}, \ldots, f_{\lambda_m}$, sodass x in dem Körper $L' = K[x_1, \ldots, x_n]$ liegt, wobei $x_1, \ldots, x_n$ die Nullstellen von $\underbrace{f_{\lambda_1} \cdot \ldots \cdot f_{\lambda_m}}_{=:g}$ sind.

Also: x liegt in dem Zerfällungskörper L' von g. L' ist normal (siehe oben) $\Rightarrow$ f zerfällt über $L \supset L'$.

□

Korollar 6.66
L/K sei normale Körpererweiterung und L' ein Zwischenkörper von L/K. Dann ist L/L' normal.

Beweis. f_λ wie oben, $f_\lambda \in K[X]$. da $L' \supset K$ ist auch $f_\lambda \in L'[X]$. L entsteht auch aus L' durch Adjunktion der Nullstellen der f_λ, d.h. also, dass nach Satz (6.65) L/L' normal ist. □

6.4.1 Normale Hülle

Ziel: $K \subset L \overset{!}{\subset} L_{norm}$, L_{norm}/K normal und L_{norm} möglichst klein.

Definition 6.67
Es sei L/K eine algebraische Körpererweiterung. Ein Oberkörper N von L heißt *normale Hülle* von L/K, falls gilt:

(i) N/K ist normal

(ii) Ist N' ein Zwischenkörper von N/L, der über K normal ist, dann ist $N' = N$.

Satz 6.68
Zu jeder algebraischen Körpererweiterung L/K gibt es eine normale Hülle N. Diese ist bis auf L–Isomorphie eindeutig bestimmt.

Beweis. Wähle $(x_\lambda)_{\lambda\in\Lambda}$ mit $L = K[(x_\lambda)]$. Es sei f_λ das Minimalpolynom von x_λ über K.

$$N := \text{Körper, der aus } K \text{ durch Adjunktion der Nullstellen der } x_\lambda \text{ in } \bar{L} \text{ entsteht.}$$

Dann ist N/K algebraisch und nach Satz (6.65) normal. Da jede normale Körpererweiterung von K, die L umfasst, diese Nullstellen enthalten muss, ist auch (ii) in der Definition (6.67) der normalen Hülle erfüllt ($\Rightarrow$ *Existenz*).

Eindeutigkeit: Es sei $\tilde{N}$ eine weitere normale Hülle von L/K. Da $\tilde{N}/K$ algebraisch ist, gibt es eine Einbettung $\tilde{N} \hookrightarrow \bar{L} = \bar{K}$ (L–Homomorphismus). Nach Konstruktion von N ist $\tilde{N} \subset \tilde{N}$. Wendet man (ii) von (6.67) auf $\tilde{N}$ an, so folgt $N = \tilde{N}$. □

Definition 6.69
Eine Körpererweiterung L/K heißt *galoisch*, falls sie endlich, normal und separabel ist.

Satz 6.70
L/K ist genau dann galoisch, wenn L der Zerfällungskörper eines Polynoms $f \in K[X]$ ist, dessen Primfaktoren alle separabel sind.

Beweis. Folgt aus dem bisher bewiesenen. □

Satz 6.71
L/K sei galoisch und L' ein Zwischenkörper von L/K. Dann ist auch L/L' galoisch.

Beweis. Nach Korollar (6.66) ist L/L' normal und natürlich auch endlich. Da das Minimalpolynom eines Elementes $x \in L$ über L' das Minimalpolynom über K teilt, folgt auch die Separabilität. □

6.4.2 Galoische Hülle

Satz 6.72
Es sei L/K endlich und separabel. Dann gibt es einen Oberkörper N von L mit:

(i) N/K ist galoisch

(ii) Ist N' Zwischenkörper von N/L, sodass N'/K galoisch ist, dann ist $N' = N$. N liegt bis auf L–Isomorphie fest.

Definition 6.73
N heißt die *galoische Hülle* von L/K.

Beweis. Falls das N existiert, muss es die normale Hülle sein. Zu zeigen ist, dass die normale Hülle separabel ist. Es sei

$$L = K[x_1, \ldots, x_n].$$

Die x_i sind nach Voraussetzung separabel, d.h. die Minimalpolynome f_i sind separabel. Dann ist die normale Hülle der Zerfällungskörper von $f = f_1 \cdot \ldots \cdot f_n$. Nach Satz (6.71) ist dieser Zerfällungskörper galoisch über K. □

—

Definition 6.74
Die *Automorphismengruppe* von L/K ist definiert durch

$$G(L/K) := \{\sigma; \sigma \colon L \to L \text{ ist ein } K\text{–Automorphismus}\}$$

(d.h. $\sigma|_K = \mathrm{id}_K$).

Definition 6.75
Ist L/K eine galoische Körpererweiterung, so nennt man $G(L/K)$ die *Galoisgruppe* von L/K.

Bemerkung 6.76
$[L : K] = n \Rightarrow |G(L/K)| \leq n$.

Satz 6.77
Es sei $[L : K] = n$. Dann sind äquivalent:

(i) L/K ist galoisch

(ii) $|G(L/K)| = n$.

Beweis. (i)⇒(ii): L/K ist galoisch ⇒ L/K ist insbesondere separabel ⇒ Es gibt n verschiedene K–Homomorphismen $\sigma_1, \ldots, \sigma_n \colon L \to \bar{L}$. Da L/K normal ist, folgt $\sigma_i(L) = L \Rightarrow \sigma_1, \ldots, \sigma_n \in G(L/K) \Rightarrow |G(L/K)| = n$.

(ii)⇒(i): $|G(L/K)| = n \Rightarrow$ Es gibt insbesondere n verschiedene K–Homomorphismen $\sigma_i \colon L \to \bar{L}$, $i = 1, \ldots, n$. D.h. L/K ist separabel. Da bereits $|G(L/K)| = n$ ist, gilt für jeden der n möglichen Homomorphismen $\sigma \colon L \to \bar{L}$, dass $\sigma(L) = L$ ist. D.h. dass L/K normal ist.

□

6.5 Hauptsatz der Galoistheorie

G: Gruppe, K: Körper

Definition 6.78
Ein *Charakter* von G in K ist ein Homomorphismus $\sigma\colon G \to K^*$. ($(K^*, \cdot)$ wird hierbei als multiplikative Gruppe aufgefasst).

Beispiel 6.79

(i) $G = (\mathbb{C}, +),\ K = \mathbb{C}$

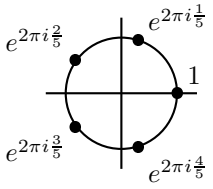
$$\sigma\colon G = \mathbb{C} \to \mathbb{C}^*, \qquad \sigma(z) := e^{2\pi i z}$$

$[\sigma(z+w) = e^{2\pi i(z+w)} = e^{2\pi i z} + e^{2\pi i w} = \sigma(z) + \sigma(w)]$

(ii) $G = \mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{\langle n \rangle},\ K = \mathbb{C}$

$$\sigma\colon \mathbb{Z}_n \to \mathbb{C}^*, \qquad \bar{k} \mapsto e^{2\pi i \frac{k}{n}}$$

[wohldefiniert: $\bar{k} = \bar{l} \Rightarrow k - l = a \cdot n; a \in \mathbb{Z} \Rightarrow e^{2\pi i \frac{k-l}{n}} = e^{2\pi i \frac{an}{n}} = e^{2\pi i a} = 1$ $(a \in \mathbb{Z})$]. Damit: $\mathbb{Z}_n \subset S^1 = \{z \in \mathbb{C}; |z| = 1\}$



$(n = 5)$

(iii) $\sigma\colon L \to N,\ \sigma \neq 0$ Körperhomomorphismus

$$\sigma^*\colon \underset{\substack{\| \\ G}}{L^*} \to \underset{K=N}{N^*} \qquad (\sigma^* = \sigma|_{L^*} = \sigma|_{L \setminus \{0\}})$$

σ^* ist Charakter der multiplikativen Gruppe L^* in dem Körper N.

Satz 6.80 („Lineare Unabhängigkeit von Charakteren“)
Es seien $\sigma_1, \ldots, \sigma_n$ verschiedene Charaktere von G in K. Gilt:

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \quad \textit{für alle } x \in G; (a_1, \ldots, a_n \in K).$$

Dann gilt $a_1 = \cdots = a_n = 0$.

Beweis. Induktion nach n.

$\underline{n = 1:}$ $a_1\sigma_1(x) = 0$ Für alle $x \in G \Rightarrow a_1 = 0$.

$\underline{n - 1 \mapsto n:}$ Die Voraussetzung ist

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \quad \text{für alle } x \in G. \tag{$*$}$$

Zu zeigen: $a_1 = \cdots = a_n = 0$.

Da $\sigma_1 \neq \sigma_n$ können wir ein $y \in G$ wählen mit $\sigma_1(y) \neq \sigma_n(y)$.

$$(*) \cdot \sigma_n(y) \Rightarrow a_1\sigma_1(x)\sigma_n(y) + \cdots + a_n\sigma_n(x)\sigma_n(y) = 0 \tag{1}$$

$$x \mapsto x \cdot y \text{ in } (*) \Rightarrow a_1\sigma_1(xy) + \cdots + a_n\sigma_n(xy) = 0 \tag{2}$$

$$\Rightarrow a_1\sigma_1(x)\sigma_1(y) + \cdots + a_n\sigma_n(x)\sigma_n(y) = 0. \tag{3}$$

(1)-(3) ergibt dann:

$$a_1(\underbrace{\sigma_n(y)-\sigma_1(y)}_{\neq 0})\sigma_1(x)+\cdots+a_{n-1}(\sigma_n(y)-\sigma_{n-1}(y))\sigma_{n-1}(x)=0$$

$$\text{IV } \Rightarrow a_1(\underbrace{\sigma_n(y)-\sigma_1(y)}_{\neq 0})=0 \Rightarrow a_1=0.$$

Damit wird $(*)$ zu:

$$a_2\sigma_2(x)+\cdots+a_n\sigma_n(x)=0 \qquad \text{für alle } x\in G$$
$$\overset{\text{IV}}{\Longrightarrow} a_2=\cdots=a_n=0.$$

□

L/K Körpererweiterung; $G(L/K)$ Automorphismengruppe

(i) $K\subset L'\subset L$; L' sei Zwischenkörper. Dann definieren wir

$$G_L:=\{g\in G(L/K); g|_{L'}=\mathrm{id}_{L'}\}=G(L/L') \qquad \text{„}\textit{Fixgruppe} \text{ von } L\text{“}$$

(ii) Sei umgekehrt $H\subset G(L/K)$ eine Untergruppe. Dann definieren wir

$$L_H:=\{x\in L; h(x)=x \text{ für alle } h\in H\} \qquad \text{„}\textit{Fixkörper} \text{ von } H\text{“}$$

Dann gilt: $K\subset L_H\subset L$.

(*Fixgruppe = Isotropiegruppe*)

L_H ist ein Körper, denn: $h(x)=x,\ h(y)=y$ für alle $h\in H \Rightarrow h(x\pm y)=x\pm y,\ h(xy)=xy,\ h(\frac{x}{y})=\frac{x}{y}$ $(y\neq 0)$.
D.h. also $x\pm y, xy, \frac{x}{y}\in L_H$.

Satz 6.81 (E. Artin)
Es sei $G\subset Aut(L)$ eine endliche Gruppe bestehend aus n Elementen und

$$K:=\{x\in L; g(x)=x \textit{ für alle } g\in G\}$$

der zugehörige Fixkörper. Dann gilt:

$$[L:K]=n=|G|.$$

Beweis. Sei $G=\{\sigma_1,\ldots,\sigma_n\}$.

<u>1. Schritt:</u> $[L:K]\geq n$.

Annahme: $[L:K]=:r<n$.

Es sei $w_1,\ldots,w_r$ eine K–Basis von L. Das lineare Gleichungssystem

$$\sum_{i=1}^{n}\sigma_i(w_k)x_k=0 \qquad (k=1,\ldots,r)$$

hat r Gleichungen und $n>r$ Unbekannte, besitzt also eine nicht-triviale Lösung $a_1,\ldots,a_n$.

$$\sum_{i=1}^{n}\sigma_i(w_k)a_i=0 \qquad (k=1,\ldots,r). \tag{1}$$

Sei nun $x \in L$ beliebig. Da $w_1, \ldots, w_r$ eine Basis ist, gibt es eine Darstellung:

$$x = \sum_{j=1}^{r} c_j w_j$$

$$\begin{aligned}\sum_{i=1}^{n} \sigma_i(x) a_i &= \sum_{i=1}^{n} \sigma_i\Big(\sum_{j=1}^{r} c_j w_j\Big) a_i \\ &= \sum_{j=1}^{r} c_j \underbrace{\left(\sum_{i=1}^{n} \sigma_i(w_j) a_i\right)}_{\overset{(1)}{=} 0} = 0\end{aligned}$$

$$\Rightarrow a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \qquad \text{für alle } x \in L, \text{ ein } a_j \neq 0$$

Andererseits induziert $\sigma\colon L \to L$ einen Charakter $\sigma^* = \sigma|_{L^*}\colon L^* \to L^* \Rightarrow \lightning$ (zur linearen Unabhängigkeit der Charaktere $\sigma_1^*, \ldots, \sigma_n^*$).

2. Schritt: $[L : K] \leq n$.

Vorbereitung: Wir betrachten folgende Abbildung

$$\begin{aligned} S&\colon L \to L \\ S(x) &:= \sigma_1(x) + \cdots + \sigma_n(x) \qquad \text{„Spur von } L/K\text{“}\end{aligned}$$

$S(x)$ ist ein Homomorphismus.

Behauptung: $S(x) \in K$.

Denn:

$$\begin{aligned}\sigma_i(S(x)) &= \sigma_i\big(\sigma_1(x) + \cdots + \sigma_n(x)\big) \\ &= \big(\sigma_i \circ \sigma_1\big)(x) + \cdots + \big(\sigma_i \circ \sigma_n\big)(x)\end{aligned}$$

Die Abbildung $G \to G; \sigma \mapsto \sigma_i\sigma$ ist eine Bijektion.

$$\begin{aligned}&\Rightarrow \sigma_i(S(x)) = \sigma_1(x) + \cdots + \sigma_n(x) = S(x) \qquad (i = 1, \ldots, n) \\ &\Rightarrow S(x) \in K.\end{aligned}$$

Wir haben also einen Homomorphismus

$$S\colon L \to K.$$

Wegen der Unabhängigkeit der Charaktere gibt es ein $x \in L$ mit $S(x) \neq 0$.

Gegeben seien Elemente $y_1, \ldots, y_{n+1} \in L$.
Zu zeigen: $y_1, \ldots, y_{n+1}$ sind linear abhängig über K.
Wir betrachten das folgende lineare Gleichungssystem

$$\sum_{k=1}^{n+1} \sigma_i^{-1}(y_k) x_k = 0 \qquad (i = 1, \ldots, n).$$

Haben $n+1$ Unbekannte x_k und n Gleichungen und damit eine nicht-triviale Lösung $a_1, \ldots, a_{n+1}$.

$$\sum_{k=1}^{n+1} \sigma_i^{-1}(y_k) a_k = 0. \qquad (i = 1, \ldots, n) \tag{1}$$

Anwendung von σ_i ergibt:

$$\sum_{k=1}^{n+1} y_k \sigma_i(a_k) = 0 \qquad (i = 1, \ldots, n) \tag{2}$$

$a_1, \ldots, a_{n+1}$ ist eine nicht-triviale Lösung. Sei $a_1 \neq 0$. Da es ein x gibt mit $S(x) \neq 0$ gibt es ein z mit $S(a_1 z) \neq 0$. Nun ist auch $za_1, \ldots, za_{n+1}$ eine nicht-triviale Lösung von (1). Nach eventuellem Ersetzen von a_1 durch $a_1 z$ können wir $S(a_1) \neq 0$ annehmen. Aufsummieren von (2) über alle i liefert:

$$\begin{aligned} & y_1 \underbrace{S(a_1)}_{\neq 0} + \cdots + y_{n+1} S(a_{n+1}) = 0 \\ \Rightarrow & y_1, \ldots, y_{n+1} \text{ sind linear abhängig} \\ \Rightarrow & [L : K] \leq n. \end{aligned}$$

□

L/K sei eine Körpererweiterung.

$$\begin{aligned} \mathcal{Z} &:= \{L'; L' \text{ ist Zwischenkörper von } L/K\} \\ \mathcal{G} &:= \{H; H \text{ ist Untergruppe von } G(L/K)\}. \end{aligned}$$

$$\phi \colon \mathcal{Z} \to \mathcal{G}, \qquad \psi \colon \mathcal{G} \to \mathcal{Z}.$$

Die Abbildungen ϕ und ψ sind wie folgt definiert:

(i) $\phi(L') := H_{L'} := \{h \in G(L/K); h|_{L'} = \mathrm{id}_{L'}\}$ „*Fixgruppe*“

(ii) $\psi(H) := L_H := \{x \in L; h(x) = x \text{ für alle } h \in H\}$ „*Fixkörper*“

Theorem 6.82 (Hauptsatz der Galoistheorie)
Ist L/K galoisch, so sind ϕ und ψ bijektive Abbildungen, die zueinander invers sind.

Leitfaden: Jeder Zwischenkörper entspricht also einer Untergruppe und umgekehrt. Mann kann also Fragen über die Existenz von Zwischenkörpern auf Fragen über die Existenz von Untergruppen zurückführen. ($\rightsquigarrow$ *auflösbare Gruppen*)

Beweis. (i) $\psi \circ \phi = \mathrm{id}_{\mathcal{Z}}$:

Starten mit $L' \in \mathcal{Z}$:

$$\phi(L') = \{g \in G(L/K); g|_{L'} = \mathrm{id}_{L'}\} = G(L/L').$$

L/K galoisch $\Rightarrow$ L/L' ist galoisch

$$\Rightarrow |\phi(L')| = |G(L/L')| = [L : L']. \tag{6.6.c}$$

Bilde nun

$$L'' = \psi(\phi(L')) = L_{\phi(L')}.$$

Nach Artin:

$$[L : L''] = |\phi(L')| = [L : L']. \qquad (**)$$

Nach Konstruktion ist $L'' \supset L'$. $\underset{\text{Gradformel}}{\overset{(**)}{\Longrightarrow}} L' = L''$.

(ii) $\phi \circ \psi = \mathrm{id}_{\mathcal{G}}$:

Starte mit einer Untergruppe $H \subset G(L/K)$.

$$\psi(H) = L_H = \{x \in L; h(x) = x \text{ für alle } h \in H\}.$$

Nach Artin:

$$[L : L_H] = |H|.$$

Bilde nun die Fixgruppe $\phi(\psi(H))$ von L_H. Nach Konstruktion ist $H \subset \phi(\psi(H))$. Da L/L_H galoisch ist, folgt

$$|\phi(\psi(H))| = [L : L_H] = |H|$$
$$\overset{H \subset \phi(\psi(H))}{\Longrightarrow} \phi(\psi(H)) = H.$$

□

Bemerkung 6.83

(i) $H \subset H' \Rightarrow L_H \supset L_{H'}$

(ii) $L' \subset L'' \Rightarrow G_{L'} \supset G_{L''}$

Satz 6.84
Es sei L/K eine endliche, separable Körpererweiterung. Dann gibt es nur endlich viele Zwischenkörper von L/K.

Beweis. Es sei $N \supset L$ die galoische Hülle von L/K

$$\underset{\text{d. Galoistheorie}}{\overset{\text{Hauptsatz}}{\Longrightarrow}} N/K \text{ hat nur endlich viele Zwischenkörper}$$

$$\Rightarrow L/K \text{ hat nur endlich viele Zwischenkörper.}$$

□

Kapitel 7

Gruppentheorie

$G = (G, \cdot)$ Gruppe; M: Menge

Definition 7.1
Eine *Operation* der Gruppe G auf der Menge M ist eine Abbildung

$$\begin{array}{rcl} G \times M & \to & M \\ (g, m) & \mapsto & g(m), \end{array}$$

sodass folgendes gilt:

(i) $1(m) = m$ für alle $m \in M$

(ii) $g'(g(m)) = (g'g)(m)$.

Bemerkung 7.2
Sei $g \in G$ fest gewählt. Dann liefert uns dies eine Abbildung:

$$\begin{array}{rcl} \bar{g}: M & \to & M \\ m & \mapsto & g(m) \end{array}$$

$\bar{g}$ ist bijektiv, da

$$\bar{g}^{-1}(g(m)) = g^{-1}(g(m)) \overset{\text{(ii)}}{=} (g^{-1}g)(m) = 1(m) \overset{\text{(i)}}{=} m$$

D.h. $(\bar{g})^{-1} = \overline{(g^{-1})}$. Wir haben also eine Abbildung, sogar einen Homomorphismus

$$\begin{array}{rcl} G & \to & \mathrm{Bij}(M) = \{f;\ f: M \to M \text{ ist bijektiv}\} \\ g & \mapsto & \bar{g} \end{array}$$

Beispiel 7.3

(i) $M = \{1, \ldots, n\}$. $S_n := \mathrm{Bij}(M)$

$$\begin{array}{rcl} S_n \times M & \to & M \\ (\sigma, i) & \mapsto & \sigma(i) \end{array}$$

(ii) L/K Körpererweiterung; $G = G(L/K)$. G operiert auf L:

$$\begin{array}{rcl} G \times L & \to & L \\ (g, x) & \mapsto & g(x) \end{array}$$

(iii) $G = \mathbb{R}^*$, $M := \mathbb{R}^{n+1} \setminus \{0\}$

$$\begin{array}{rcl} G \times M & \to & M \\ (\lambda, (x_1, \ldots, x_{n+1})) & \mapsto & (\lambda x_1, \ldots, \lambda x_{n+1}) \end{array}$$

(iv) $M := G$

- Die *Linkstranslation* von $g \in G$ ist definiert durch

$$\begin{array}{rcl} L_g \colon G & \to & G \\ g' & \mapsto & g \cdot g' \end{array}$$

Dies liefert eine Operation von G auf sich selbst.

$$\begin{array}{rcl} G \times \underbrace{G}_{=M} & \to & \underbrace{G}_{=M} \\ (g, g') & \mapsto & g \cdot g' = L_g(g') \end{array}$$

(a) $(1, g) \mapsto 1 \cdot g = g$

(b) $g''(g'(g)) = g''(g' \cdot g) = g'' \cdot (g' \cdot g) = (g'' \cdot g') \cdot g = (g'' \cdot g')(g)$.

- *Rechtstranslation:*

$$\begin{array}{rcl} R_g \colon G & \to & G \\ g' & \mapsto & g'g \end{array}$$

Achtung:

$$\begin{array}{rcl} G \times \underbrace{G}_{=M} & \to & \underbrace{G}_{=M} \\ (g, g') & \mapsto & g' \cdot g = R_g(g') \end{array}$$

ist im Allgemeinen <u>keine</u> Gruppenoperation.

$$\begin{array}{l} g''(g'(g)) = g''(g \cdot g') = (g \cdot g') \cdot g'' = g \cdot (g' \cdot g'') \\ (g'' \cdot g')(g) = g(g'' \cdot g') \underset{i.\,A.}{\neq} g \cdot (g' \cdot g'') \text{ (falls } g' \cdot g'' \neq g'' \cdot g') \end{array}$$

Dagegen erhält man eine Gruppenoperation durch:

$$\begin{array}{rcl} G \times \underbrace{G}_{=M} & \to & \underbrace{G}_{=M} \\ (g, x) & \mapsto & g' \cdot x \cdot g^{-1} =: g(x). \end{array}$$

(v) *Konjugation*

$$\begin{array}{rcl} G \times \underbrace{G}_{=M} & \to & \underbrace{G}_{=M} \\ (g, x) & \mapsto & g \cdot x \cdot g^{-1} =: g(x). \end{array}$$

Dies ist eine Gruppenoperation von G auf sich selbst, denn:

(a) $1(x) = 1 \cdot x \cdot 1^{-1} = x$

(b) $(g'g)(x) = (g'g) \cdot x \cdot (g'g)^{-1} = (g'g) \cdot x \cdot (g^{-1} \cdot g'^{-1}) = g' \cdot \underbrace{(gxg^{-1})}_{g(x)} \cdot g'^{-1} =$

$g'(g(x))$.

(vi) $G = \mathrm{GL}(n, K)$; $M := \mathrm{Mat}(n \times n; K)$

$$\begin{array}{rcl} G \times M & \to & M \\ (A, M) & \to & AMA^{-1} \text{ („Ahnlichkeit von Matrizen“)} \end{array}$$

zu (v) Sei $g \in G$ fest:

$$\begin{array}{rcl} \sigma_g \colon G & \to & G \\ x & \mapsto & gxg^{-1} \end{array}$$

σ_g ist ein Gruppenhomomorphismus

$$\sigma_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \sigma_g(x) \cdot \sigma_g(y)$$

Definition 7.4
σ_g heißt der durch g definierte *innere Automorphismus* der Gruppe G.

—

G operiere auf einer Menge M.

Definition 7.5
Die Menge

$$M_G := \{m \in M;\ g(m) = m \text{ für alle } g \in G\}$$

heißt die *Fixpunktmenge* der Operation von G auf M.

Beispiel 7.6

$$\begin{array}{l} H \subset G(L/K) \\ L_H = \{x \in L;\ h(x) = x \text{ für alle } h \in H\} \end{array}$$

Sei $M' \subset M$ eine Teilmenge.

Definition 7.7
Die *Fixgruppe (Isotropiegruppe)* von M' in G ist

$$G_{M'} := \{g \in G;\ g(m') = m' \text{ für alle } m' \in M'\}$$

Bemerkung 7.8
$G_{M'}$ ist Untergruppe von G.

$$g \in G_{M'}: \quad g(m') = m' \Rightarrow \underbrace{g^{-1}(g(m'))}_{=(g^{-1}g)(m')=1(m')=m} = g^{-1}(m') \Rightarrow g^{-1} \in G_{M'}$$

$$g, h \in G_{M'}: \quad \underbrace{g(h(m'))}_{=(gh)(m')} = g(m') = m'$$

$$\Rightarrow gh \in G_{M'}$$

Beispiel 7.9

(i) Galoistheorie: L' Zwischenkörper von L/K.

$$G_{L'} := \{g \in G(L/K);\ g(x) = x \text{ für alle } x \in L'\}$$

(ii) G operiere auf G durch

$$\begin{array}{rcl} G \times G & \to & G \\ (g, x) & \mapsto & gxg^{-1} \end{array}$$

Definition 7.10
Der *Zentralisator* von M' ist die folgende Menge:

$$Z(M') = \{g \in G; gm'g^{-1} = m' \text{ für alle } m' \in M\}$$

Speziell: $M' = G$

Definition 7.11
Der *Zentralisator* von G ist die Menge (Untergruppe):

$$Z(G) = \{g \in G; gxg^{-1} = x \text{ für alle } x \in G\}$$

„Zentrum von G“

$$Z(G) = \{g \in G; gx = xg \text{ für alle } x \in G\}$$

Bemerkung 7.12
G abelsch $\Leftrightarrow Z(G) = G$

Beispiel 7.13

$$Z(\mathrm{GL}(n, K)) = \{\lambda \cdot E_n;\ \lambda \in K\}$$

—

G: Gruppe, M: Menge . G operiere auf M.

$$G \times M \to M.$$

Definition 7.14
Die *Bahn* von $m \in M$ ist definiert durch

$$Gm := \{g(m);\ g \in G\} \subset M.$$

Beispiel 7.15

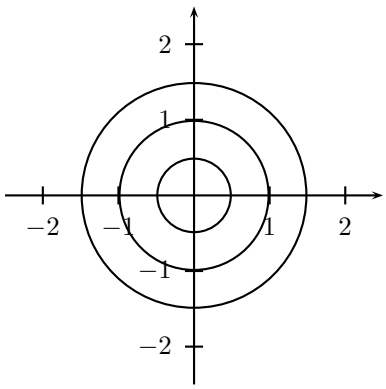
(i) $M = G$, $M \subset G$ Untergruppe. M operiere auf G durch Linkstranslation.

$$Hg := \{hg;\ h \in H\}$$

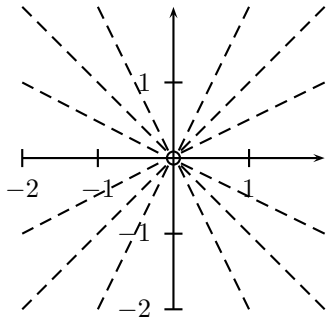
Hg heißt *Rechtsnebenklasse* von g bezüglich M. Analog ist die *Linksnebenklasse* definiert durch

$$gH := \{gh;\ h \in H\}$$

(ii) $G = S^1 := \{z \in \mathbb{C};\ |z| = 1\} = \{e^{i\varphi};\ \varphi \in \mathbb{R}\}$ S^1 operiert auf $\mathbb{C}$ durch $(z, w) \mapsto z \cdot w$



(iii) $G = (R^*, \cdot)$; $M = \mathbb{R}^2 \setminus \{(0,0)\}$



(iv) $G = \mathrm{GL}(n, K)$; $M = \mathrm{Mat}(n \times n, K)$; $M \mapsto AMA^{-1}$.

Bahnen = Ähnlichkeitsklassen von Matrizen

Definition 7.16
$m \sim m' :\Leftrightarrow$ es gibt $g \in G$ mit $m' = g(m)$ (d.h. m, m' liegen in derselben Bahn).

Lemma 7.17
$\sim$ ist eine Äquivalenzrelation.

Beweis. (i) $m \sim m$, da $m = 1(m)$

(ii) $m \sim m' \Rightarrow m' = g(m)$ für ein $g \in G \Rightarrow g^{-1}(m') = g^{-1}(g(m)) = m \Rightarrow m' \sim m$.

(iii) $m \sim m', m' \sim m'' \Rightarrow m' = g(m)$; $m'' = g'(m') = g'(g(m)) = (g' \cdot g)(m)$ $\Rightarrow m \sim m''$

□

Bemerkung 7.18
Die Äquivalenzklassen sind genau die Bahnen. Insbesondere $Gm = Gm'$ oder $Gm \cap Gm' = \emptyset$.

Definition 7.19
Die *Ordnung* einer Gruppe ist definiert durch:

$$|G| := \begin{cases} \#\text{Elemente von } G & \text{falls } G \text{ endlich ist} \\ \infty & \text{sonst.} \end{cases}$$

Satz 7.20
Es sei G eine endliche Gruppe, die auf einer endlichen Menge G operiert. Sei $m \in M$. Dann gilt:

$$|G| = |G_m| \cdot |Gm|$$

Beweis. Es seien $g_1, \ldots, , g_r \in G$ so gewählt, dass

$$Gm = \{g_1(m), \ldots, g_r(m)\} (\text{d.h. } |Gm| = r)$$

$\underline{|G| \geq |G_m||Gm|}$: Dies folgt aus folgender Behauptung: Durchläuft h die verschiedenen Elemente von G_m, so sind die Gruppenelemente $g_1h, \dots g_rh$ alle verschieden. Denn:

$$\begin{aligned} g_ih = g_jh' \Rightarrow \quad & (g_ih)(m) = (g_jh')(m) \\ \Leftrightarrow \quad & g_i(h(m)) = g_j(h'(m)) \\ \Leftrightarrow \quad & g_i(m) = g_j(m) \Rightarrow j = i \end{aligned}$$

$\Rightarrow g_ih = g_ih' \Rightarrow h = h'$

$\underline{|G| \leq |G_m||Gm|}$: Sei $g \in G$. Dann gibt es ein $i \in \{1, \dots, r\}$ mit $g(m) = g_i(m)$ $\Rightarrow (g_i)^{-1}g(m) = m \Rightarrow {g_i}^{-1}g = h \in G_m \Rightarrow g = g_ih$ mit $h \in G_m$.

—

□

G operiere auf M. $\mathfrak{P}(M)$ = *Potenzmenge* von M (= Familie der Teilmengen von M). Dann operiert G auch auf $\mathfrak{P}(M)$:

$$\begin{aligned} G \times \mathfrak{P}(M) \quad &\rightarrow \quad \mathfrak{P}(M) \\ (g, M) \quad &\mapsto \quad gM = \{gh;\ h \in M\} \end{aligned}$$

Beispiel 7.21
$M = G$ ist eine Untergruppe. G operiert auf G durch Linkstranslation. Dann operiert G auch auf der Potenzmenge und gH ist genau die Linksnebenklasse von g bezüglich H.

Bemerkung 7.22

(i) $gH = g'H$ oder $gH \cap g'H = \emptyset$.

(ii) $Hg = Hg'$ oder $Hg \cap Hg' = \emptyset$ (folgt, da Gruppenoperationen Äquivalenzrelationen definieren.)

$\underline{\text{zu (i):}}$ Nehme die Operation

$$\begin{aligned} G \times G \quad &\rightarrow \quad G \\ (g, x) \quad &\mapsto \quad xg^{-1} \end{aligned}$$

und argumentiere wie in (ii) oder elementar.

$$\begin{aligned} gH \cap g'H = \emptyset \Rightarrow \ &\text{Es gibt } h, h' \in M \text{ mit } gh = g'h \\ \Rightarrow g' = ghh'^{-1} \Rightarrow g'H \subset gH. &\text{ Analog } gH \subset g'H \end{aligned}$$

Bemerkung 7.23
Ist $M \subset G$ Untergruppe, so ist

$$G_{\{H\}} = M \quad (G_{\{H\}} = \{g \in G;\ gH = H\})$$

Denn:

(i) $g \in M \Rightarrow gH = H$

(ii) $gH = H \Rightarrow g \cdot 1 \in H \Rightarrow g \in H$

Definition 7.24
Es sei G eine Gruppe und H eine Untergruppe von G. Dann wird der *Index* von H in G definiert durch

$$(G : H) = \#\text{ Linksnebenklassen von } H \text{ in } G.$$

Korollar 7.25
Es sei G eine endliche Gruppe und H eine Untergruppe. Dann gilt:

$$|G| = |H| \cdot (G : H)$$

Beweis. Dies ist ein Spezialfall des obigen Satzes, da H die Fixgruppe von $\{H\} \in \mathfrak{P}(G)$ ist und $(G : H)$ die Anzahl der Elemente in der Bahn $G \cdot H$ ist. □

Bemerkung 7.26
Insbesondere: Die Ordnung einer Untergruppe teilt die Ordnung der Gruppe selbst.

—

L/K galoisch. $K \subset L' \subset L$ Zwischenkörper $\Leftrightarrow$ Untergruppe $H \subset G(L : K)$, $|H|$ teilt $|G(L/K)|$.

Nächstes Ziel: G Gruppe, $H \subset G$ Untergruppe. Wir möchten G/H definieren (Faktorgruppe). Idee:

$$G/H := \{\text{ Linksnebenklassen } gH,\ g \in G\}$$

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

Problem: Dies ist im Allgemeinen nicht wohldefiniert (falls G nicht abelsch) $\rightsquigarrow$ normale Untergruppen.

7.1 Quotientengruppen

G: Gruppen, H Untergruppe

Ziel: Wir wollen auf der Menge der Linksnebenklassen $\{gH;\ g \in G\}$, $gH = \{gh;\ h \in H\} \subset G$ eine Gruppenstruktur einführen. Sei $\varphi\colon G \to G'$ ein Gruppenhomomorphismus und sei

$$H = \ker \varphi = \{g \in G;\ \varphi(g) = 1\}$$

Lemma 7.27

(i) H ist Untergruppe.

(ii) Es gilt, dass $gH = Hg$ ist, für alle $g \in G$.

Beweis. (i) $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$, denn $\varphi(h_1h_2) = \underbrace{\varphi(h_1)}_{=1} \cdot \underbrace{\varphi(h_2)}_{=1} = 1$. Ebenso: $h \in H \Rightarrow h^{-1} \in H$, denn: $\varphi(h^{-1}) = \varphi(h)^{-1} = 1^{-1} = 1$.

(ii) Es gilt: $gH = Hg \Leftrightarrow gHg^{-1} = H$:

$\underline{gHg^{-1} \subset H}$: Sei dazu $h \in H$. Dann gilt

$$\varphi(ghg^{-1}) = \varphi(g)\underbrace{\varphi(h)}_{=1}\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = 1 \Rightarrow ghg^{-1} \in H.$$

$\underline{H \subset gHg^{-1}}$: Nach obigem (ersetze g durch g^{-1}) gilt:

$$g^{-1}Hg \subset H \Rightarrow H \subset gHg^{-1}$$

□

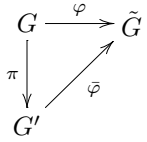
Definition 7.28
Eine Gruppe H heißt ein *Normalteiler* von G, falls gilt: $gH = Hg$ für alle $g \in G$.

Schreibweise: $H \lhd G$

Definition 7.29
Es sei H ein Normalteiler von G. Eine Gruppe G' heißt *Restklassengruppe* (*Faktor-, Quotientengruppe*) von G bzgl. H, falls gilt:

(i) Es gibt einen Homomorphismus $\pi\colon G \to G'$ mit $\ker \pi = H$.

(ii) Ist $\varphi\colon G \to \tilde{G}$ ein Homomorphismus von Gruppen mit $H \subset \ker \varphi$, so gibt es genau einen Homomorphismus $\bar{\varphi}\colon G' \to \tilde{G}$, so dass

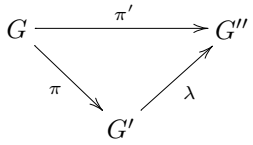


kommutiert, d. h. $\varphi = \bar{\varphi} \circ \pi$.

Satz 7.30

(i) Ist $H \lhd G$, so gibt es eine Faktorgruppe $\pi\colon G \to G'$ von G bzgl. H.

(ii) Ist $\pi'\colon G \to G''$ eine weitere Faktorgruppe, so gibt es genau einen Isomorphismus $\lambda\colon G' \to G''$, sodass



kommutiert.

Schreibweise: $G' =: {}^{G}\!/_{H}$

Beweis. (i) Setze

$$\begin{aligned} G' &:= \text{Menge der Linksnebenklassen von } H \text{ in } G \\ G' &:= \{gH;\ g \in G\} \end{aligned}$$

Gruppenoperation auf G': $(g_1H) \cdot (g_2H) := (g_1g_2)H$

Wohldefiniertheit:

$$\left.\begin{array}{rcl} g_1H &=& g_1'H \\ g_2H &=& g_2'H \end{array}\right\} (g_1g_2)H = (g_1'g_2')H. \qquad (7.7.a)$$

$$\left.\begin{array}{l} \Rightarrow \text{ Es gibt } h_1 \text{ mit } g_1 = g_1'h_1 \\ \Rightarrow \text{ Es gibt } h_2 \text{ mit } g_2 = g_2'h_2 \end{array}\right\} g_1g_2 = g_1'h_1g_2'h_2. \qquad (7.7.b)$$

Es gilt, da H ein Normalteiler ist, folgendes:

$$h_1 g_2' \in H g_2' = g_2' H$$

$\Rightarrow$ Es gibt h_1' mit $h_1 g_2' = g_2' h_1'$. In (7.7.b):

$$g_1 g_2 = g_1' g_2' h_1' h_2 \in g_1' g_2' H \Rightarrow g_1 g_2 H \subset g_1' g_2' H.$$

Analog: $g_1' g_2' H \subset g_1 g_2 H$.

G' ist eine Gruppe: (a) Neutrales Element:

$$\begin{aligned} (gH)(1H) &= (g1)H = gH \\ (1H)(gH) &= (1g)H = gH \quad (1H: \text{ neutrales Element}) \end{aligned}$$

(b) Inverses Element:

$$\begin{aligned} (gH)(g^{-1}) &= (gg^{-1})H = 1 \cdot H \\ (g^{-1}H)(gH) &= 1 \cdot H \end{aligned}$$

Die Abbildung

$$\begin{aligned} \pi\colon G &\to G' \\ \pi(g) &:= gH \end{aligned}$$

π ist ein *Homomorphismus*:

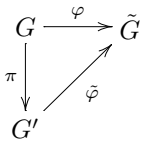
$$\pi(g_1 g_2) = (g_1 g_2)H = (g_1 H)(g_2 H) = \pi(g_1) \cdot \pi(g_2) :$$

Der *Kern* von π:

$$\begin{aligned} g \in \ker \pi &\Leftrightarrow \pi(g) = 1H \\ &\Leftrightarrow gH = 1H \\ &\Leftrightarrow g \in H. \end{aligned}$$

D.h. $\ker \varphi = H$

Universelle Eigenschaft Sei $\varphi\colon G \to \tilde{G}$ Homomorphismus mit $\ker \varphi \supset H$.
Aufgabe: Es gibt genau ein $\tilde{\varphi}\colon G' \to \tilde{G}$, sodass



kommutiert.

Eindeutigkeit ist klar, wegen: $\underbrace{\tilde{\varphi}(\pi(g))}_{=\tilde{\varphi}(gH)} = \varphi(g)$. Setze also: $\tilde{\varphi}(gH) := \varphi(g)$.

$\tilde{\varphi}$ ist wohldefiniert: Sei $g_1 H = g_2 H$. $\Rightarrow$ Es gibt $h \in H$ mit $g_1 = g_2 h \Rightarrow \varphi(g_1) = \varphi(g_2 h) = \varphi(g_2) \underbrace{\varphi(h)}_{=1, \text{ da } H \subset \ker \varphi} = \varphi(g_2)$.

$\tilde{\varphi}$ ist ein Homomorphismus:

$$\tilde{\varphi}((g_1 H)(g_2 H)) = \tilde{\varphi}(g_1 g_2 H) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \tilde{\varphi}(g_1 H)\tilde{\varphi}(g_2 H)$$

(ii) wie gehabt.

□

Bemerkung 7.31
Ist G eine abelsche Gruppe, so gilt stets $gH = Hg$, d. h. dass jede Untergruppe einer *abelschen* Gruppe ein Normalteiler ist.

Beispiel 7.32

(i) $G = (\mathbb{Z}, +);\ H = n\,\mathbb{Z}$

$$G/H = \mathbb{Z}/n\,\mathbb{Z} = \mathbb{Z}_n$$

(ii) $G = S_n = \mathrm{Bij}\{1, \ldots, n\}$

$$H := A_n = \{\sigma \in S_n; \mathrm{sign}\ \sigma = 1\}$$

$$\begin{aligned} A_n \lhd S_n: \quad & \tau \in S_n,\ \sigma \in A_n \overset{!}{\Rightarrow} \tau\sigma\tau^{-1} \in A_n \\ & \mathrm{sign}(\tau\sigma\tau^{-1}) = \mathrm{sign}\ \tau \cdot \underbrace{\mathrm{sign}\ \sigma}_{=1} \cdot \mathrm{sign}\ \tau^{-1} = 1 \\ & 1 \to A_n \to S_n \overset{\mathrm{sign}}{\longrightarrow} \mathbb{Z}_2 = \{\pm 1\} \\ & S_n/A_n \cong \mathbb{Z}_2\,. \end{aligned}$$

(iii)

$$G := \mathrm{SL}(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{Z};\ ad - bc = 1 \right\}$$

$$H = G_0 := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\ \mathbb{Z});\ c = 0 \right\}$$

H ist eine Untergruppe:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \in H$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \in H$$

H ist kein Normalteiler:

$$\begin{aligned} & \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{g} \underbrace{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}}_{\in H} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{g^{-1}} \overset{?}{\in} H \\ = \quad & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} b & -a \\ d & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ -b & a \end{pmatrix} \quad \notin H \text{ für } b \neq 0 \end{aligned}$$

Bemerkung 7.33
Ist G endlich, so ist

$$|\,G/H\,| = (G : H)$$

Definition 7.34
Eine Gruppe heißt *einfach*, falls sie außer $\{1\}$, G keine Nullteiler (d.h. normalen Untergruppen) besitzt.

Theorem 7.35
Die endlichen einfachen Gruppen sind klassifiziert. (Bewiesen: ca. 1980/85)

(ohne Beweis)

Satz 7.36
Es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus.

(i) Ist U eine Untergruppe (Normalteiler) von H, dann gilt dies auch für $\varphi^{-1}(U)$.

(ii) Ist U Untergruppe von G, dann ist auch $\varphi(U)$ eine Untergruppe von H.

(iii) Ist φ surjektiv und U Normalteiler von G, dann ist $\varphi(U)$ ein Normalteiler von H.

(iv) Ist φ surjektiv, so gibt es eine Bijektion

$$\left\{ \begin{array}{l} U \subset G \text{ ist Untergruppe} \\ \text{(Normalteiler) mit } U \supset \ker\varphi \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{l} V \subset H \text{ ist Untergruppe} \\ \text{(Normalteiler)} \end{array} \right\}$$

Beweis. (i)

$$g, h \in \varphi^{-1}(U) \Rightarrow \varphi(g) \in U,\ \varphi(h) \in U \Rightarrow \underbrace{\varphi(g)\varphi(h)}_{=\varphi(gh)} \in U$$

$$\Rightarrow \quad gh \in \varphi^{-1}(U)$$

$$g \in \varphi^{-1}(U) \Rightarrow \varphi(g) \in U \Rightarrow \underbrace{\varphi(g)^{-1}}_{\varphi(g^{-1})} \in U$$

$$\Rightarrow \quad g^{-1} \in \varphi^{-1}(U)$$

Sei nun $U \lhd H$; $g \in G$.
$g\varphi^{-1}(U)g^{-1} \subset (U)$:]
$\underline{g\varphi^{-1}(U)g^{-1} \subset (U)}$: Sei $u \in \varphi^{-1}(U)$

$$\Rightarrow \quad \varphi(gug^{-1}) = \varphi(g)\underbrace{\underbrace{\varphi(u)}_{\in U}\varphi(g)^{-1}}_{\in U}$$

$$\Rightarrow \quad gug^{-1} \in \varphi^{-1}(U)$$

Ersetze $g \mapsto g^{-1}$. Dann folgt:

$$g^{-1}\varphi^{-1}(U)g \subset \varphi^{-1}(U) \Rightarrow \underline{\varphi^{-1}(U) \subset g\varphi^{-1}(U)g^{-1}}$$

$$\Rightarrow \quad g\varphi^{-1}(U)g^{-1} = \varphi^{-1}(U) \Rightarrow \varphi^{-1}(U) \lhd G.$$

(ii) •

$$g, h \in \varphi(U) \Rightarrow \text{ Es gibt } g', h' \in H \text{ mit } g = f(g'),\ h = \varphi(h')$$
$$\Rightarrow gh = \varphi(g')\varphi(h') = \varphi(\underbrace{g'h'}_{\in U}) \in \varphi(U)$$

- $$g \in \varphi(U) \Rightarrow g = \varphi(g') \text{ mit } g' \in U$$
$$\Rightarrow g^{-1} = (\varphi(g'))^{-1} = \varphi(g'^{-1})$$
$$\Rightarrow g^{-1} \in \varphi(U).$$

(iii) Sei $U \lhd G$. Zu zeigen: $\varphi(U) \lhd H$. Sei $h \in H$. Zu zeigen: $h\varphi(U)h^{-1} = \varphi(U)$. Da φ surjektiv ist, gibt es ein $g \in G$ mit $h = \varphi(g)$. Damit:

$$h\varphi(U)h^{-1} = \varphi(g)\varphi(U)\varphi(g^{-1}) = \varphi(gUg^{-1}) \overset{U \lhd G}{=} \varphi(U).$$

(iv) Dies folgt, da $\varphi^{-1}(\varphi(U)) = U$, $\varphi(\varphi^{-1}(V)) = V$, da φ surjektiv ist.

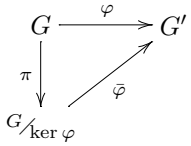
□

Folgerungen:

Korollar 7.37 (Homomorphiesatz für Gruppen)
Es sei $\varphi\colon G \to G'$ ein surjektiver Gruppenhomomorphismus. Dann induziert φ einen Isomorphismus

$$\bar{\varphi}\colon \ {}^{G}\!/_{\ker\varphi} \xrightarrow{\cong} G'$$

Beweis. $\ker\varphi \lhd G$: d. h. wir erhalten ein kommutatives Diagramm



Da φ surjektiv ist, gilt dies auch für $\bar{\varphi}$. Der Homomorphismus $\bar{\varphi}$ ist auch injektiv, da:

$$\bar{\varphi}(\bar{g}) = 1 \Leftrightarrow \varphi(g) = 1 \Leftrightarrow g \in \ker\varphi \Leftrightarrow \bar{g} = \bar{1} \quad (\bar{g} = g\ker\varphi)$$

□

$N_1,\ N_2 \subset G$ seien Untergruppen. Es seien $N_1,\ N_2$ sogar Normalteiler von G. Es sei $N_2 \subset N_1$.
Bemerkung: $N_2 \lhd N_1$.
Betrachten die Projektion:

$$\pi\colon G \to {}^{G}\!/_{N_2}.$$

Dann gilt $\pi(N_1) = {}^{N_1}\!/_{N_2}$.
Da $N_2 \lhd N_1$, folgt aus obigem Satz, dass $\pi(N_1) = {}^{N_1}\!/_{N_2}$.

Korollar 7.38 (2. Noetherscher Isomorphiesatz)
Die Abbildung

$$\tilde{\pi}\colon g \xrightarrow{\pi} {}^{G}\!/_{N_2} \longrightarrow {}^{({}^{G}\!/_{N_2})}\!/_{({}^{N_1}\!/_{N_2})}$$

induziert einen Isomorphismus

$${}^{G}\!/_{N_1} \cong {}^{({}^{G}\!/_{N_2})}\!/_{({}^{N_1}\!/_{N_2})}$$

Beweis. π ist surjektiv und damit auch $\tilde{\pi}$. Der Kern von $\tilde{\pi}$ ist $\pi^{-1}\left({}^{N_1}\!/_{N_2}\right) = N_1$. Nach Korollar (7.37) folgt:

$$ {}^{G}\!/_{N_1} \;=\; {}^{G}\!/_{\ker\tilde{\pi}} \;\cong\; {}^{\left({}^{G}\!/_{N_2}\right)}\!/_{\left({}^{N_1}\!/_{N_2}\right)} $$

□

Bemerkung 7.39
Sei $N \lhd G$, $U \subset G$ sei eine Untergruppe. $\pi\colon G \to {}^{G}\!/_{N}$. Dann ist

$$\pi^{-1}(\pi(U)) = UN = \{un;\ u \in U,\ n \in N\}.$$

Nach dem Satz (7.36) ist dies eine Untergruppe von G. Da $N \subset UN$ und $N \lhd G$, gilt auch $N \lhd UN$.

Bemerkung 7.40

$$U \cap N \lhd U.$$

Beweis.

$$\begin{aligned} u \in U,\ x \in U \cap N \quad &\Rightarrow \quad uxu^{-1} \in U \quad (\text{da } x \in U) \\ &\qquad\quad uxu^{-1} \in N \quad (\text{da } N \subset G). \\ &\Rightarrow \qquad uxu^{-1} \in U \cap N \\ &\Rightarrow \qquad u(U \cap N)u^{-1} \subset U \cap N \\ \text{wie gehabt:} \ &\Rightarrow \qquad u(U \cap N)u^{-1} = U \cap N. \end{aligned}$$

□

Korollar 7.41 (1. Noetherscher Isomorphiesatz)
Die Abbildung

$$\pi' := \pi_{|U}\colon U \to {}^{G}\!/_{N}$$

induziert einen Isomorphismus

$$ {}^{U}\!/_{U\cap N} \cong {}^{UN}\!/_{N}\,.$$

Beweis. Folgt aus dem Korollar (7.37), da

$$\begin{aligned} \operatorname{im}\pi' &= {}^{UN}\!/_{N} \\ \ker\pi' &= U \cap N \end{aligned}$$

□

7.2 Zyklische Gruppen

Lemma 7.42
Jede Untergruppe von $\mathbb{Z}$ ist von der Form $n\,\mathbb{Z}$.

Beweis. Ist bekannt für Ideale in $\mathbb{Z}$. Ist $U \subset \mathbb{Z}$ eine Untergruppe, dann ist U auch ein Ideal, denn für $u \in U$, $z \in \mathbb{Z}$ gilt

$$zu = \pm\underbrace{(u + \cdots + u)}_{|z|} \in U$$

□

Lemma 7.43
Sei G eine Gruppe, $g \in G$. Dann gibt es genau einen Homomorphismus

$$\delta\colon \mathbb{Z} \to G \text{ mit } \delta(1) = g$$

Beweis. Falls δ existiert, muss gelten

$$\delta(n) = \begin{cases} g^n & \text{, falls } n \geq 0, \\ \left(g^{-1}\right)^{|n|} & \text{, falls } n < 0. \end{cases}$$

Da dies ein Homomorphismus ist, ist die Aussage bewiesen. □

Definition 7.44
$\langle g \rangle := \delta(\mathbb{Z}) \subset G$. Dies heißt die von g *erzeugte Untergruppe* von G.

Definition 7.45
Eine Gruppe G heißt *zyklisch*, falls es ein $g \in G$ gibt, mit $G = \langle g \rangle$.

Bemerkung 7.46
$\delta\colon \mathbb{Z} \to G,\ \delta(1) = g$.

(i) δ ist injektiv $\Rightarrow G \cong \mathbb{Z}$.

(ii) $\ker \delta = n\,\mathbb{Z} \Rightarrow \bar{\delta}\colon {}^{\mathbb{Z}}\!/_{n\,\mathbb{Z}} = \mathbb{Z}_n \cong G$ (Korollar (7.37))

zu (i) $G = \{g^n;\ n \in \mathbb{Z}\}$

zu (ii) $G = \{g^0 = 1, g, g^2, \ldots, g^{n-1}\}$

Satz 7.47

(i) Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.

(ii) Ist $|G| = n < \infty$, G zyklisch, dann gibt es zu jedem Teiler m von n genau eine Untergruppe der Ordnung m.

Beweis. (i)
- $G = \mathbb{Z}$, $U \subset G$ Untergruppe $\overset{\text{Lemma (7.42)}}{\Rightarrow}$ $U = n\,\mathbb{Z} = \langle n \rangle$, also zyklisch.
- $G \cong \mathbb{Z}_n$. Betrachte $\delta\colon \mathbb{Z} \to \mathbb{Z}_n$, $U \subset \mathbb{Z}_n$ sei Untergruppe. $\Rightarrow \delta^{-1}(U) \subset \mathbb{Z}$ ist eine Untergruppe mit $n\,\mathbb{Z} \subset \delta^{-1}(U) =: U'$. $\Rightarrow U' = k\,\mathbb{Z}$ mit $k|n$. Sei $n = k \cdot m$. Dann gilt $U \cong {}^{\delta^{-1}(U)}\!/_{n\,\mathbb{Z}} = {}^{k\,\mathbb{Z}}\!/_{n\,\mathbb{Z}} = {}^{k\,\mathbb{Z}}\!/_{mk\,\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{m\,\mathbb{Z}} = \mathbb{Z}_m$, also zyklisch von Ordnung m mit $m|n$.

(ii) Folgt sofort aus obigen Überlegungen.

□

Bemerkung 7.48
Sei $G = \{1, g, \ldots, g^{n-1}\}$, $n = mk$. Dann ist die eindeutig bestimmte zyklische Untergruppe der Ordnung m von G die Gruppe $G' = \{1, g^k, g^{2k}, \ldots, g^{k(m-1)}\}$.

Definition 7.49
Ein Element h einer zyklischen Gruppe G heißt ein *primitives* Element, falls $G = \langle h \rangle$.

Definition 7.50
Die *Ordnung eines Elements* g einer (beliebigen) Gruppe ist die Ordnung der von g erzeugten zyklischen Untergruppe $\langle g \rangle$. (= minimales $n > 0$ mit $g^n = 1$, bzw. ∞, falls stets $g^n \neq 1$ für alle $n > 0$.)

Beispiel 7.51
$G = \mathbb{Z}_6$, (Achtung: additive Gruppe):

Primitive Elemente:	$\bar{1},\ \bar{5}$
Nicht-primitive Elemente:	$\bar{1},\ \bar{2},\ \bar{3}, \bar{4}$
Elemente der Ordnung 1:	$\bar{0}$
Elemente der Ordnung 2:	$\bar{3}$,
Elemente der Ordnung 3:	$\bar{2},\ \bar{4}$
Elemente der Ordnung 6:	$\bar{1},\ \bar{5}$

Bemerkung 7.52
G sei zyklisch von Ordnung n. Dann gilt:

$$h \in G \text{ ist primitiv} \Leftrightarrow \text{ord } k = n.$$

Lemma 7.53
Es sei $G = \langle g \rangle$ von Ordnung $n < \infty$. Dann gilt:

$$g^m \textit{ ist primitiv} \Leftrightarrow (m, n) = 1$$

Beweis. "$\Rightarrow$" Sei $d = \text{ggT}(m,\ n) > 1$. D.h. $m = \mu d$, $n = \nu d$ mit $\mu, \nu < n$.

$$(g^m)^\nu = g^{m\nu} = g^{\mu d \nu} = g^{\mu n} = (g^n)^\mu = 1^\mu = 1$$

$\Rightarrow$ ord$(g^m) < n$.

"$\Leftarrow$" Es sei $(g^m)^k = 1 \Rightarrow km \equiv 0 \mod n \overset{(m,n)=1}{\Rightarrow} k = \nu n$. $\Rightarrow$ Die folgenden Elemente: $g^m, g^{2m}, \ldots, g^{(n-1)m} \neq 1$. Damit müssen diese Elemente auch alle verschieden sein. $\Rightarrow$ (ord g^m) $= n = |G| \Rightarrow g^m$ ist primitiv.

□

Definition 7.54
Die *Eulersche φ-Funktion* ist definiert durch

$$\begin{aligned} \varphi\colon \mathbb{N}_{>0} &\to \mathbb{N} \\ \varphi(n) &:= \#\{m;\ 1 \le m \le n \text{ mit } (m,n) = 1\} \end{aligned}$$

Beispiel 7.55

(i) $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

(ii) p prim $\Rightarrow \varphi(p) = p - 1$

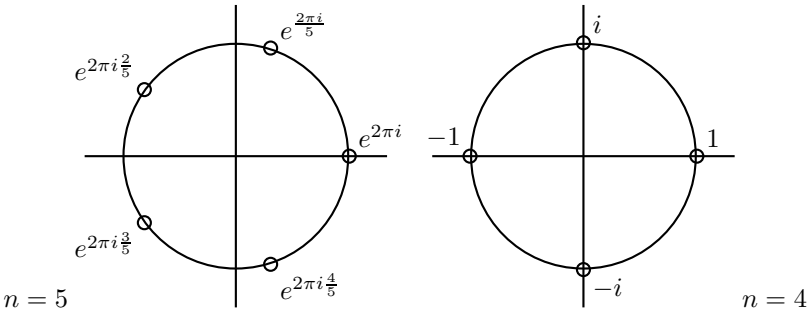
Korollar 7.56
Ist $\tilde{G} = \mathbb{Z}_n$, dann besitzt G genau $\varphi(n)$ primitive Elemente.

Beispiel 7.57

$$\begin{aligned} G &= \mathbb{Z}_n \subset \mathbb{C}^* \\ \bar{k} &\mapsto e^{2\pi i \frac{k}{n}} \end{aligned}$$

$\boxed{\mu_n := i(\mathbb{Z}_n)}$ (Gruppe der n-ten Einheitswurzel)

Dann entsprechen die primitiven Elementen gerade den *primitiven Einheitswurzeln.*



7.2.1 Einheitengruppe von $\mathbb{Z}_n$

$$E(R) = \{r \in R;\ \text{ es gibt } r' \text{ mit } rr' = 1\}$$
$$E(\mathbb{Z}_n) = \text{ Einheitengruppe von } \mathbb{Z}_n\,.$$

Satz 7.58
$|E(\mathbb{Z}_n)| = \varphi(n)$.

Beweis. Es genügt folgendes zu zeigen:

$$\bar{m} \in E(\mathbb{Z}_n) \Leftrightarrow (m,n) = 1 \text{ (d. h. } \bar{m} \text{ ist primitives Element)}$$

„⇐“

$$(m,n) = 1 \Rightarrow (m,n) = \langle 1\rangle = \mathbb{Z} \Rightarrow \text{Es gibt } k,l \text{ mit } mk + ln = 1$$
$$\Rightarrow \bar{m}\bar{k} = \bar{1} \Rightarrow \bar{m} \in E(\mathbb{Z}_n).$$

„⇒“

$$\bar{m} \in E(\mathbb{Z}_k) \Rightarrow \text{ Es gibt } \bar{k} \text{ mit } \bar{m}\bar{k} = \bar{1} \Rightarrow mk \equiv 1 \mod n,$$
$$\text{d.h. } mk = 1 + rn \text{ für ein } R \in \mathbb{Z} \Rightarrow mk + (-r)n = 1 \Rightarrow (m,n) = 1.$$

□

Frage: Explizite Formel für $\varphi(n)$?

Satz 7.59
Sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ mit verschiedenen Primzahlen $p_1, \dots, p_r$. Dann gilt

$$\varphi(n) = p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1)$$

.

Beispiel 7.60

$$6 = 2 \cdot 3,\ \varphi(6) = 2^0 \cdot 3^0(2-1)(3-1) = 2$$

Lemma 7.61
Für $n = p^\alpha$ gilt $\varphi(n) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Lemma 7.62
Sei $(n_1, n_2) = 1$, sei $n = n_1 \cdot n_2$. Dann gilt:

$$\varphi(n) = \varphi(n_1)\varphi(n_2)$$

Bemerkung 7.63
Lemma (7.61) + Lemma (7.62) ⇒ Satz (Primzahlzerlegung von n)

Beweis. (von Lemma (7.61))
Die nicht-primitiven Elemente in $\mathbb{Z}_{p^\alpha}$ sind die folgenden:

$$\{\bar{p}, 2\bar{p}, 3\bar{p}, \dots, p^{\alpha-1}\bar{p}\}$$

Diese $p^{\alpha-1}$ Elemente haben Repräsentanten, die durch p teilbar sind. □

Beweis. (von Lemma (7.62))
Dies folgt aus der folgenden Behauptung: Die Abbildung

$$\begin{aligned} \psi\colon E(\mathbb{Z}_n) &\to E(\mathbb{Z}_{n_1}) \times E(\mathbb{Z}_{n_2}) \\ \nu + \langle n\rangle &\mapsto (\nu + \langle n_1\rangle, \nu + \langle n_2\rangle) \end{aligned}$$

ist eine Bijektion.

Wohldefiniertheit Ist ν eine Einheit in $\mathbb{Z}_n \Rightarrow (\nu, n) = 1 \Rightarrow (\nu, n_1) = 1$ und $(\nu, n_2) = 1 \Rightarrow \nu + \langle n_1\rangle \in E(\mathbb{Z}_{n_1})$, $\nu + \langle n_2\rangle \in E(\mathbb{Z}_{n_2})$.

ψ ist injektiv $\psi(\nu) = \psi(\nu') \Rightarrow \nu - \nu' \in \langle n_1\rangle$ und $\nu - \nu' \in \langle n_2\rangle \Rightarrow \nu - \nu' \in \langle n_1\rangle \cap \langle n_2\rangle = \langle n_1 n_2\rangle = n. \Rightarrow \nu + \langle n\rangle = \nu' + \langle n\rangle$

ψ ist surjektiv (vgl. chinesischer Restsatz)

$$\nu_1 + \langle n_1\rangle \in E(\mathbb{Z}_{n_1}),\ \nu_2 + \langle n_2\rangle \in E(\mathbb{Z}_{n_2})$$

Da $(n_1, n_2) = 1$ gibt es μ_1, μ_2 mit

$$\mu_1 n_1 + \mu_2 n_2 = 1. \tag{7.7.c}$$

Setze $\nu := \mu_2 n_2 \nu_1 + \mu_1 n_1 \nu_2$.
ν definiert eine *Einheit* in $\mathbb{Z}_n$: Hätten ν und n einen gemeinsamen Teiler, so hätten auch ν und n_1 oder ν und n_2 einen gemeinsamen Teiler. D. h. ν definiert in $\mathbb{Z}_{n_1}$ keine Einheit. Aber: $\nu + \langle n_1\rangle \overset{!}{=} \nu_1 + \langle n_1\rangle \Rightarrow \nu_1$ ist keine Einheit in $E(\mathbb{Z}_{n_1})$. $\lightning$
Bleibt: $\psi(\nu + \langle n\rangle) = (\nu_1 + \langle n_1\rangle, \nu_2 + \langle n_2\rangle)$. Es gilt:

$$\begin{aligned} &\nu + \langle n_1\rangle = \mu_2 n_2 \nu_1 + \mu_1 n_1 \nu_2 + \langle n_1\rangle = \mu_2 n_2 \nu_1 + \langle n_1\rangle \\ &\overset{(7.7.c)}{=} (1 - \mu_1 n_1)\nu_1 + \langle n_1\rangle = \nu_1 + \langle n_1\rangle \end{aligned}$$

Analoge Rechnung: $\nu + \langle n_2\rangle = \nu_2 + \langle n_2\rangle$. □

Bemerkung 7.64
Der Beweis dieses Lemmas liefert auch folgendes:

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

falls $(n_1, n_2) = 1$.

Beispiel 7.65
$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

7.3 Endlich erzeugte abelsche Gruppen

$(G, +)$ sei eine abelsche Gruppe.

Definition 7.66

(i) Eine Menge $\{g_1, \ldots, g_s\}$ heißt ein *Erzeugendensystem* von G, falls jedes Element $g \in G$ eine Darstellung

$$g = n_1 g_1 + \cdots + n_s g_s \quad (n_i \in \mathbb{Z})$$

besitzt.

(ii) Ein Erzeugendensystem $\{g_1, \ldots, g_s\}$ heißt ein *minimales* Erzeugendensystem, falls es kein Erzeugendensystem bestehend aus $s-1$ Elementen gibt.

(iii) Ein Erzeugendensystem heißt eine *Basis* von G, wenn jedes Element g eine eindeutige Darstellung

$$g = n_1 g_1 + \cdots + n_s g_s$$

besitzt.

Bemerkung 7.67
$\{g_1, \ldots, g_s\}$ ist eine Basis, falls es ein Erzeugendensystem ist und falls gilt

$$n_1 g_1 + \cdots + n_s g_s = 0 \Rightarrow n_1 = \cdots = n_s = 0.$$

Beispiel 7.68
$\mathbb{Z}_n$: $\bar{1}$ ist minimales Erzeugendensystem, aber keine Basis, da $n \cdot \bar{1} = 0 \cdot \bar{1} = \bar{0}$.

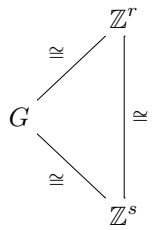
Bemerkung 7.69
Ist $\{g_1, \ldots, g_s\}$ eine Basis von G, so definiert

$$\begin{array}{rcl} G & \to & \mathbb{Z}^s \\ g = n_1 g_1 + \cdots + n_s g_s & \mapsto & (n_1, \ldots, n_s) \end{array}$$

einen Isomorphismus $G \cong \mathbb{Z}^s$ (*freie Abelsche Gruppe vom Rang s*).

Lemma 7.70
Sind $\{g_1, \ldots, g_r\}$ und $\{g'_1, \ldots, g'_s\}$ Basen der Gruppe G, so folgt $r = s$.

Beweis. Es ist $G \cong \mathbb{Z}^r$, $G \cong \mathbb{Z}^s$. Betrachten



$$G^{(p)} := \{pg;\ g \in G\} \subset G \text{ Untergruppe.}$$

Dies induziert

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^r \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^s.$$

Dies sind endlich dimensionale Vektorräume der Dimension r, bzw. s über dem Körper $\mathbb{Z}_p \Rightarrow r = s$. □

Definition 7.71
Es seien $G_1, \ldots, G_s$ Untergruppen von G. Man sagt, G ist die *direkte Summe* der Untergruppen G_i, falls jedes $g \in G$ eine eindeutige Darstellung

$$g = g_1 + \cdots + g_s \quad \text{mit } g_i \in G_i;\ i = 1, \ldots, s$$

besitzt.

Schreibweise: $G = G_1 \oplus \cdots \oplus G_s$

Bemerkung 7.72
$G_1 \oplus \cdots \oplus G_s \cong G_1 \times \cdots \times G_s$

Satz 7.73 (Hauptsatz für endlich erzeugte abelsche Gruppen)
Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es Zahlen $r, n_1, \ldots, n_s$, sodass $n_i | n_{i-1}$ und es gilt

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}\,.$$

Die Zahl $r + s$ ist dabei die minimale Länge eines Erzeugendensystems.

Bemerkung 7.74
(ohne Beweis) Die Zahlen $r, n_1, \ldots, n_s$ sind durch G festgelegt. Man nennt r den *Rang* der Gruppe G.

Beweis. Es sei

$$t := \text{minimale Länge eines Erzeugendensystems.}$$

Induktion nach t:

$\underline{t = 1}$ Es gibt einen Erzeugenden, d. h. $G = \langle g_1 \rangle$. Damit ist G zyklisch, also $G \cong \mathbb{Z}$ oder $G = \mathbb{Z}_n$.

$\underline{t - 1 \mapsto t}$ Falls es eine Basis $g_1, \ldots, g_t$ gibt, dann gilt:

$$G \cong \mathbb{Z}^t\,.$$

Also ist man fertig, d. h. für jedes minimale Erzeugendensystem $g_1, \ldots, g_t$ gibt es nicht-triviale Relationen

$$n_1 g_1 + \cdots + n_t g_t = 0. \tag{7.7.d}$$

Definiere

$$n := \min\{|n_i|;\ \text{Es gibt eine Relation (7.7.d) mit } n_i \neq 0\}.$$

Betrachte eine Relation mit $n_i = n$ für ein i. Kann dann annehmen, dass $n_1 = n$. Sei dies:

$$n_1 g_1 + \cdots + n_t g_t = 0; \quad n_1 = n \tag{7.7.e}$$

$\underline{\text{Behauptung:}}$ Für jede Relation $n_1' g_1 + \cdots + n_t' g_t = 0$ gilt $n_1 | n_1'$.

$\underline{\text{Beweis:}}$ Da $m = n_1$ minimal ist, gilt $|n_1| \leq |n_1'|$ (falls $n_1' \neq 0$). Wir können schreiben:

$$n_1' = a_1 n_2 + r_1 \quad \text{mit } a_1 \in \mathbb{Z}; 0 \leq r_1 \leq n_1 - 1.$$

Bilde $q_1 \cdot$ (7.7.d) $-$ (7.7.e):

$$\underbrace{(q_1 n_1 - n_1')}_{|\ | = r_1 < n_1} g_1 + (q_1 n_2 - n_2') g_2 + \cdots + (q_1 n_t - n_t') g_t = 0$$

Nach Wahl von $n_1 = n$ folgt: $r_1 = 0 \Rightarrow n_1 | n_1'$.

Behauptung: Es sei $g_1', \ldots, g_t'$ ein weiteres Erzeugendensystem und

$$m_1 g_1' + \cdots + m_t g_t' > 0$$

eine Relation mit $m_i = n_1$ für ein i. Dann gilt $n_1 | m_j$ für alle j.

Beweis: Wir können $m_1 = n_1$ annehmen. Schreibe

$$m_i = q_i n_1 + r_i \quad \text{mit } 0 \leq r_i < n_1.$$

Mit $g_1', \ldots, g_t'$ ist auch $g_1' + q_i g_i', g_2', \ldots, g_t'$ ein Erzeugendensystem von G.

$$\underbrace{m_1}_{=n_1} g_1' + \cdots + \underbrace{m_i}_{=q_i n_1 + r_i} g_i' + \cdots + m_t g_t' = 0 \qquad (7.7.\text{f})$$

$$\Rightarrow n_1(g_1' + q_i g_i') + m_2 g_2' + \cdots + r_i g_i' + \cdots + m_t g_t' = 0 \quad (0 \neq r_i < n_1)$$

Aus der Minimalität von n_1 folgt $r_1 = 0 \Rightarrow m_i = q_i n_1 \Rightarrow n_1 | m_i$.

Wende dies nun auf die Relation (7.7.e) an:

$$n_1 g_1 + \cdots + n_t g_t = 0$$

Dann folgt $n_1 | n_i$ für alle i. D.h.

$$n_i = q_i n_1, \quad i = 2, \ldots, t$$

Setze

$$g_1' := g_1 + q_2 g_2 + \cdots + q_t g_t.$$

Dann ist $g_1', g_2, \ldots, g_t$ ein Erzeugendensystem von G. Es gilt

$$n_1 g_1' = n_1 g_1 + \underbrace{n_1 q_2 g_2}_{=n_2} + \cdots + \underbrace{n_1 q_t g_t}_{=n_t} = 0$$

Andererseits ist $r g_1' \neq 0$ für $0 < r < n_1$ (Minimalität von n_1).

$$\Rightarrow \langle g_1' \rangle \cong \mathbb{Z}_{n_1}\,.$$

Setze $G_1 := \langle g_1' \rangle$; $G' := \langle g_2, \ldots, g_t \rangle$ (d. h. die von $g_2, \ldots, g_t$ erzeugte Untergruppe). D.h.

$$G' := \left\{ \sum_{i=2}^{t} m_i g_i;\ m_i \in \mathbb{Z} \right\} \subset G$$

Behauptung: $G = G_1 \oplus G'$.

Beweis: Klar ist, da $g_1', g_2, \ldots, g_t$ ein Erzeugendensystem von G ist, dass jedes Element in G von der Form $g = g^1 + g'$ mit $g^1 \in G_1,\ g' \in G'$ ist.

Annahme: Eine solche Dartstellung ist nicht eindeutig.

Daraus folgt: Es gibt eine Darstellung $g^1 + g' = 0$ mit $g^1 \neq 0$, $g^1 \in G^1,\ g' \in G'$

$$\Rightarrow \underbrace{r_1 g_1'}_{\neq 0} + r_2 g_2 + \cdots + r_t g_t \text{ mit } 0 < r_1 < n_1$$

Dies ist ein Widerspruch zur Minimalität von n_1. $\lightning$

—

Induktionsvoraussetzung auf G' angewandt ($g_2, \ldots, g_t$ ist ein Erzeugendensystem minimaler Länge) liefert uns:

$$G' \cong \mathbb{Z}^r \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}$$

mit $n_i | n_{i+1}$ und $t = r + (s-1)$.

$$\Rightarrow G = G_1 \oplus G' \cong \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}$$

mit $n_i | n_{i+1}$, falls $i \geq 2$.

Bleibt:

Behauptung: $n_1 | n_2$

Beweis: Es sei g_i' ein primitives Element von $\mathbb{Z}_{n_i}$ $(i = 2, \ldots, s)$. Es sei $g'_{s+1}, \ldots, g'_{s+r=t}$ eine Basis von $\mathbb{Z}^r$. Dann ist

$$g_1', g_2', \ldots, g_t'$$

ein Erzeugendensystem von G von minimaler Länge. Es gilt dann:

$$n_1 g_1' + n_2 g_2' = 0$$

Aus der zweiten Behauptung folgt nun $n_1 | n_2$.

□

Lemma 7.75 (2. Version des Hauptsatzes)
Es sei n eine natürliche Zahl mit Primzahlzerlegung:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$

Dann gilt

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\alpha_i}} .$$

Korollar 7.76
Ist G eine endlich erzeugte abelsche Gruppe, so gilt

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{\beta_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{\beta_l}}$$

mit (nicht notwendig verschiedenen) Primzahlen $p_1, \ldots, p_l$.

Beweis. Wende das Lemma auf den Hauptsatz für jeden Summanden $\mathbb{Z}_{n_i}$ an. □

Beweis. (von Lemma (7.75)) Sei $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. ($p_i \neq p_j$ für $i \neq j$). Betrachte den Homomorphismus

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \mathbb{Z}_n \\ 1 &\mapsto \overline{\left(\frac{n}{p_i^{\alpha_i}}\right)} = \overline{p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_s^{\alpha_s}} \end{aligned}$$

Es gilt $\ker \varphi_i = \langle p_i^{\alpha_i} \rangle$. $\Rightarrow \varphi_i$ induziert also einen Homomorphismus:

$$\overline{\varphi_i}\colon {}^{\mathbb{Z}}\!/_{\langle p_i^{\alpha_i} \rangle} = \mathbb{Z}_{p_i^{\alpha_i}} \hookrightarrow \mathbb{Z}_n$$

Wir erhalten damit einen Homomorphismus

$$\begin{aligned}\overline{\varphi} = (\overline{\varphi_1}, \ldots, \overline{\varphi_s})\colon \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} &\to \mathbb{Z}_n \\ \bar{\varphi}(\overline{m_1}, \ldots, \overline{m_s}) &= \varphi_1(\overline{m_1}) + \cdots + \varphi_s(\overline{m_s}).\end{aligned}$$

Da beide Gruppen dieselbe Anzahl von Elementen besitzen, genügt zu zeigen, dass $\overline{\varphi}$ surjektiv ist, bzw. $\bar{1} \in \mathrm{im}(\overline{\varphi})$.

Die Zahlen

$$\frac{n}{p_1^{\alpha_1}}, \ldots, \frac{n}{p_s^{\alpha_s}}$$

sind teilerfremd.

$$\begin{aligned}\Rightarrow \quad & < \frac{n}{p_1^{\alpha_1}}, \ldots, \frac{n}{p_s^{\alpha_s}} >= \mathbb{Z} \\ \Rightarrow \quad & \text{Es gibt } m_1, \ldots, m_s \text{ mit } m_1 \frac{n}{p_1^{\alpha_1}} + \cdots + m_s \frac{n}{p_s^{\alpha_s}} = 1 \\ \Rightarrow \quad & \overline{\varphi}(\overline{m_1}, \ldots, \overline{m_s}) = \bar{1}.\end{aligned}$$

□

Satz 7.77
Es sei G eine endliche abelsche Gruppe, $n = |G|$. Es sei m eine Zahl mit $m|n$. Dann besitzt G eine Untergruppe H mit $|H| = m$.

Beweis. Satz (7.73): $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ mit $n = n_1 \cdots n_s$ mit $n_i | n_{i+1}$. Da $m|n$ gibt es eine Darstellung $m = m_1 \cdots m_s$ mit $m_i | n_i$. In $\mathbb{Z}_{n_i}$ gibt es (genau eine) Untergruppe $\mathbb{Z}_{m_i}$. Setze

$$H := \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s} \subset G.$$

□

Satz 7.78 (kleiner Fermat)
Es sei G eine endliche Gruppe der Ordnung n. Dann gilt $g^n = 1$ für jedes Element $g \in G$.

Beweis. $G' := \langle g \rangle \subset G$. Dann gilt

$$\begin{aligned}n = |G| &= \underbrace{|G'|}_{\mathrm{ord} g} \underbrace{[G : G']}_{=:k} = (\mathrm{ord}\ g) \cdot k. \\ \Rightarrow g^n &= g^{\mathrm{ord}\ g \cdot k} = \left(g^{\mathrm{ord}\ g}\right)^k = 1^k = 1.\end{aligned}$$

□

Satz 7.79
Es sei R ein Integritätsring mit Quotientenkörper K und Einheitengruppe $E(R)$. Es sei $G \subset E(R)$ eine endliche Untergruppe. Dann ist G zyklisch.

Beweis. G ist eine endliche abelsche Gruppe. G sei nicht zyklisch. Satz (7.73) liefert uns

$$G = G_1 \oplus G_2,\ n_1 = \mathrm{ord}\ G_1,\ n_2 = \mathrm{ord}\ G_2,\ n_1 | n_2 \tag{7.7.g}$$

Satz (7.78):

$$\begin{aligned}x \in G_2 \quad &\Rightarrow \quad x^{n_2} = 1 \Rightarrow x^{n_2} - 1 = 0 \\ x \in G_1 \quad &\Rightarrow \quad x^{n_1} = 1 \overset{n_1 | n_2}{\Rightarrow} x^{n_2} - 1 = 0.\end{aligned}$$

Die Gleichung $x^{n_2} - 1$ hat in k höchstens n_2 Nullstellen

$$\Rightarrow G_1 \subset G_2 \quad \lightning \text{ zu (7.7.g)}$$

□

7.4 p-Gruppen und der Satz von Sylow

G: Gruppe. Jetzt nicht mehr notwendig abelsch.

Definition 7.80
G heißt eine *p-Gruppe*, falls es eine Primzahl p gibt, mit

$$|G| = p^\alpha.$$

Satz 7.81
Es sei G eine p-Gruppe, $G \neq \{1\}$. Dann gilt $Z(G) \neq \{1\}$.
[Erinnerung: $Z(G) = \{g \in G;\ gx = xg$ für alle $x \in G\}$ Zentrum von G]

Beweis. Wir betrachten die folgende Operation von G auf sich selbst:

$$\begin{array}{rcl} G \times \underbrace{G}_{=M} & \to & \underbrace{G}_{=M} \\ (g, x) & \mapsto & gxg^{-1}. \end{array}$$

(Operation durch Konjugation mit Elementen von G). Diese Operation zerlegt G in Bahnen (Äquivalenzklassen)

$$G = B_1 \cup \cdots \cup B_r \text{ mit } B_i \cap B_j = \emptyset \text{ für } i \neq j.$$

Sei B_1 die Bahn der 1, d.h.

$$B_1 = \{g \cdot 1 \cdot g^{-1}; g \in G\} = \{1\}$$

Sei $b_i := |B_i|$ (# Elemente in der Bahn B_i).

$$\Rightarrow p^\alpha = |G| = b_1 + b_2 + \cdots + b_r = 1 + b_2 + \cdots + b_r.$$

Für $x \in B_i$ gilt:

$$p^\alpha = |G| = |G_x||B_i|,$$

wobei G_x der Stabilisator von x ist, d.h.

$$G_x = \{g \in G; gxg^{-1} = x\}.$$

$$\begin{array}{rcl} \Rightarrow b_i & = & |B_i| = p_{\beta_i} \\ \Rightarrow p^\alpha & = & 1 + p^{\beta_1} + \cdots + p^{\beta_r} \end{array}$$

$\Rightarrow$ Es gibt ein β_i, $i \geq 2$ mit $\beta_i = 0$ (sonst $1 \equiv 0 \bmod p$ $\lightning$) Sei etwa $\beta_2 = v$, d.h. $|B_2| = 1$. Sei $x_2 \in B_2$.

$$\begin{array}{rcl} \Rightarrow & & g \cdot x_2 = x_2 \cdot g \text{ für alle } g \in G. \\ \Rightarrow & & \underbrace{x_2}_{\neq 1} \in Z(G) \Rightarrow Z(G) \neq \{1\} \end{array}$$

□

Definition 7.82
Für $n \in \mathbb{N}_+$ und eine feste Primzahl p setzen wir

$$\nu_p(n) := \max\{\alpha;\ p^\alpha | n\}$$

Beispiel 7.83

$$\begin{aligned} n = 54,\ p = 2: \quad & \nu_2(54) = 1 \\ 54 = 2 \cdot 27 = 2 \cdot 3^3 \quad & \nu_3(54) = 3 \\ & \nu_p(54) = 0 \text{ für alle } p \geq 5. \end{aligned}$$

„p-adische Bewertung“

Bemerkung 7.84

(i) $\nu_p(n \cdot n') = \nu_p(n) + \nu_p(n')$

(ii) $\nu_p(n + n') \geq \min\{\nu_p(n), \nu_p(n')\}$

(iii) $\nu_p(n) < \nu_p(n') \Rightarrow \nu_p(n + n') = \nu_p(n)$
Folgt sofort aus der Primzahlzerlegung von n, n'.

—

Sei G eine endliche Gruppe, $n = \text{ord } G$.

Satz 7.85 (Sylow)
Es sei $p^\alpha | n$, $n = ord\ G$. Dann gibt es eine Untergruppe $H \subset G$ mit $|H| = p^\alpha$.

Beweis. Es sei

$$M := \text{Menge der Teilmengen von } G \text{ der Mächtigkeit } p^\alpha$$

$$|M| = \binom{n}{p^\alpha};$$

Da $p^\alpha | n$ gibt es ein m mit $n = mp^\alpha$.

$$\Rightarrow |M| = \binom{n}{p^\alpha} = \frac{p^\alpha n(p^\alpha m - 1) \cdots (p^\alpha m - (p^\alpha - 1))}{p^\alpha \cdot 1 \cdot 2 \cdot 3 \cdots (p^\alpha - 1)}$$

Es gilt nach Bemerkung (7.84) (iii):

$$\begin{aligned} & \nu_p(k) = \nu_p(p^\alpha m - k) \text{ für } 0 < k < p^\alpha - 1 \\ \Rightarrow \quad & \nu_p(|M|) = \nu_p\binom{n}{p^\alpha} = \nu_p(m). \end{aligned}$$

—

Die Gruppe operiert auf M wie folgt:

$$g \cdot \{g_1, \ldots, g_{p^\alpha}\} := \{gg_1, \ldots, gg_\alpha\}.$$

Diese Operation zerlegt M in disjunkte Bahnen

$$M = B_1 \cup \cdots \cup B_r;\ b_i := |B_i|$$

Dann gilt:

$$|M| = \binom{n}{p^\alpha} = b_1 + \cdots + b_r$$

Da $\nu_p\binom{n}{p^\alpha} = \nu_p(m)$ gibt es ein b_i mit

$$\nu_p(b_i) \leq \nu_p(m). \quad \text{(aus Bemerkung (7.84) (ii))}$$

Sei $x \in B_i$ und H der Stabilisator von x, d.h.

$$H = \{g \in G;\ gx = x\}$$

H ist eine Untergruppe von G.
Behauptung: $|H| = p^\alpha$

$\underline{|H| \leq p^\alpha}$ Sei $x = \{g_1, \ldots, g_{p^\alpha}\}$, $h \in H$.

$$\begin{aligned} &\Rightarrow && x = hx = \{hg_1, \ldots, hg_{p^\alpha}\} = \{g_1, \ldots, g_{p^\alpha}\} \\ &\Rightarrow && \text{Es ist stets } hg_1 \in \{g_1, \ldots, g_{p^\alpha}\} \\ &\Rightarrow && |H| \leq p^\alpha. \end{aligned}$$

$\underline{|H| \geq p^\alpha}$: Es gilt:

$$\begin{aligned} && mp^\alpha = |G| = |H||B_i| = |H|b_i \\ \Rightarrow \quad && \underbrace{\nu_p(mp^\alpha)}_{=\nu_p(m)+\alpha} = \nu_p(|H|) + \nu_p(b_i) \end{aligned}$$

Da $\nu_p(b_i) \leq \nu_p(m)$ ist, folgt $\nu_p(b_i) \leq \nu_p(m)$ ist, folgt $\nu_p(|H|) \geq \alpha$, also $p^\alpha \mid |H|$. Damit $|H| \geq p^\alpha$.

□

Definition 7.86
Es sei $n = |G|$, $\alpha = \nu_p(n)$. Dann heißt eine Untergruppe H von G mit $|H| = p^\alpha$ eine *p-Sylow Untergruppe* von G.

Bemerkung 7.87
(ohne Beweis) Je zwei p-Sylowgruppen H_1, H_2 von G sind konjugiert, d.h. es gibt $g \in G$ mit $gH_1g^{-1} = H_2$.

7.5 Auflösbare Gruppen

Definition 7.88
Eine Gruppe G heißt *auflösbar*, falls es eine Kette von Untergruppen gibt:

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_l = \{1\}$$

mit

(i) $N_i \lhd N_{i-1}$

(ii) ${}^{N_{i-1}}\!/_{N_i}$ ist abelsch.

Beispiel 7.89

(i) S_2, S_3, S_4 sind auflösbar, z.B. $S_3 \rhd A_3 \rhd 1$, ${}^{S_3}\!/_{A_3} = \mathbb{Z}_2$, $A_3 \cong \mathbb{Z}_3$

(ii) S_5 ist *nicht* auflösbar (Beweis später)

—

G sei eine Gruppe.

Definition 7.90
Die *Kommutatoruntergruppe* $G^{(1)}$ von G ist die Gruppe:

$$G^{(1)} := \langle aba^{-1}b^{-1};\ a, b \in G\rangle.$$

Bemerkung 7.91
G abelsch $\Leftrightarrow G^{(1)} = \{1\}$.

Definition 7.92
$[a, b] := aba^{-1}b^{-1}$ heißt der *Kommutator* von a und b.

Lemma 7.93

(i) $G^{(1)}$ *ist ein Normalteiler von* G *und* ${}^{G}\!/_{G^{(1)}}$ *ist abelsch.*
$[1 = [a, b] = aba^{-1}b^{-1} \Leftrightarrow ba = ba]$

(ii) Ist H *ein Normalteiler von* G *mit* ${}^{G}\!/_{H}$ *abelsch, dann ist* $H \supset G^{(1)}$.

Beweis. (i)

$$\begin{aligned} g(aba^{-1}b^{-1})g^{-1} &= \underbrace{gag^{-1}}_{:=a'}\underbrace{gbg^{-1}}_{:=b'}ga^{-1}g^{-1}gb^{-1}g^{-1} \\ &= a'b'a'^{-1}b'^{-1} \end{aligned}$$

$$\begin{aligned} &\Rightarrow \quad gG^{(1)}g^{-1} \subset G^{(1)}. \quad \text{Analog } g^{-1}G^{(1)}g \subset G^{(1)} \\ &\Rightarrow \quad G^{(1)} \subset gG^{(1)}g^{-1} \\ &\Rightarrow \quad gG^{(1)}g^{-1} = G^{(1)} \end{aligned}$$

${}^{G}\!/_{G^{(1)}}$ ist *abelsch*, da: $\pi(a)\pi(b)\pi(a^{-1})\pi(b^{-1}) \stackrel{!}{=} \pi(1)$, wobei $\pi\colon G \to {}^{G}\!/_{G^{(1)}}$ die kanonische Projektion ist. Es gilt:

$$\begin{aligned} \pi(a)\pi(b)\pi(a^{-1})\pi(b^{-1}) &= \pi(\underbrace{aba^{-1}b^{-1}}_{\in G^{(1)}}) \\ &= \pi(1) \end{aligned}$$

(ii) Es sei ${}^{G}\!/_{H}$ abelsch:

$$\begin{aligned} &\Rightarrow \quad \bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{1} \\ &\Rightarrow \quad \overline{aba^{-1}b^{-1}} = \bar{1} \\ &\Rightarrow \quad aba^{-1}b^{-1} \in H \\ &\Rightarrow \quad G^{(1)} \subset H. \end{aligned}$$

□

—

Wir definieren uns induktiv:

$$G^{(1)} := \text{Kommutatoruntergruppe von } G$$

Ist $G^{(i-1)}$ definiert, so setzen wir

$$G^{(i)} := \left(G^{(i-1)}\right)^{(1)},$$

d.h. $G^{(i)}$ ist die Kommutatoruntergruppe von $G^{(i-1)}$. Wir erhalten dann eine Kette

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd G^{(3)} \rhd \cdots \rhd G^{(i)} \rhd \cdots$$

mit ${}^{G^{(i)}}\!/_{G^{(i+1)}}$ ist abelsch.

Lemma 7.94
Es sind äquivalent:

(i) G ist auflösbar.

(ii) Es gibt ein l mit $G^{(l)} = \{1\}$.

Beweis. (ii) $\Rightarrow$ (i) klar.

(i) $\Rightarrow$ (ii) Behauptung: Ist $G = N_0 \rhd N_1 \rhd \cdots \rhd N_l = \{1\}$ eine Kompositionsreihe, dann gilt $N_i \supset G^{(0)}$.
$[\Rightarrow N_l = \{1\} \supset G^{(1)} \Rightarrow G^{(l)} = \{1\}]$.
Induktion nach i:

$i = 1$: Lemma (7.93): $N_1 \supset G^{(1)}$, da ${}^{G}\!/_{N_1}$ abelsch ist.
$i - 1 \mapsto i$: Induktionsvoraussetzung $N_{i-1} \supset G^{(i-1)}$.

$${}^{N_{i-1}}\!/_{N_i} \text{ abelsch} \overset{Lemma\ (7.93)}{\Rightarrow} N_1 \supset \left(G^{(i-1)}\right)^{(1)} = G^{(i)}$$

□

Lemma 7.95
Es sei A eine endliche abelsche Gruppe. Dann gibt es eine Kette $A = U_0 \rhd U_1 \rhd \cdots \rhd U_n$ mit ${}^{U_i}\!/_{U_{i+1}}$ zyklisch von Primzahlordnung.

Beweis. Lemma (7.75):

$$A \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\alpha_i}}; \quad p_1, \ldots, p_i \text{ Primzahlen}$$

Es genügt, die Aussage für ein $\mathbb{Z}_{p^\alpha}$ so zu beweisen. Hier kann man eine solche Kette konkret angeben:

$$\mathbb{Z}_{p^\alpha} \supset \mathbb{Z}_{p^{\alpha-1}} \supset \mathbb{Z}_{p^{\alpha-2}} \supset \cdots \supset \mathbb{Z}_p \supset \{0\}$$

$$\bar{p} \leftarrow\!\shortmid \bar{1}$$

Es gilt:

$${}^{\mathbb{Z}_{p^k}}\!/_{\mathbb{Z}_{p^{k-1}}} \overset{\text{Kor. (7.37)}}{\cong} {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} = \mathbb{Z}_p$$

□

Satz 7.96
Es sei G auflösbar. Dann gibt es eine Kette

$$G = N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_l = \{1\},$$

sodass ${}^{N_{i-1}}\!/_{N_i}$ zyklisch von Primzahlordnung ist.

Beweis. Die Idee besteht darin, eine gegebene Kette, die G auflöst zu verfeinern. Es genügt: $H \lhd G,\ {}^{G}\!/_{H}$ ist abelsch. $\Rightarrow$ Dann gibt es eine Kette

$$G = M_0 \rhd M_1 \rhd \dots M_l = H,$$

sodass ${}^{M_{i-1}}\!/_{M}$ zyklisch von Primzahlordnung ist. Betrachte $\pi\colon G \to {}^{G}\!/_{H} =: A$ und wende Lemma (7.95) auf A an:

$$A = M_0' \rhd M_1' \rhd \cdots \rhd M_k' = \{0\}$$

mit ${}^{M_{i-1}'}\!/_{M_i'} \cong \mathbb{Z}_{p_i}$. Setze

$$M_i := \pi^{-1}(M_i') \quad (H \subset M_i' \subset G).$$

Es gilt:

$$G = M_0 \rhd M_1 \rhd \cdots \rhd M_k = H,$$

$${}^{M_{i-1}}\!/_{M_i} \cong {}^{M_{i-1}'}\!/_{M_i'} \cong \mathbb{Z}_{p_i}.$$

□

Satz 7.97
Es sei G eine auflösbare Gruppe. Dann gilt:

(i) Jede Untergruppe von G ist auflösbar.

(ii) Ist $\varphi\colon G \to G'$ ein Homomorphismus, so ist $H := \varphi(G)$ wieder auflösbar.

Beweis. (i) Betrachte:

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_l = \{1\}$$

mit ${}^{N_{i-1}}\!/_{N_i}$ abelsch. Betrachte:

$$U = U \cap N_0 \supset U \cap N_1 \supset U \cap N_2 \supset \cdots \supset U \cap N_l = \{1\}$$

Dann gilt:

$$U \cap N_i \lhd U \cap N_{i-1}$$

Klar: $g \in U \cap N_i,\ x \in U \cap N_{i-1} \Rightarrow$

$$\left.\begin{matrix} gxg^{-1} \in U \\ gxg^{-1} \in N_{i-1} \end{matrix}\right\} \Rightarrow gxg^{-1} \in U \cap N_{i-1}$$

Ferner gilt:

$$U \cap {}^{N_{i-1}}\!/_{U\cap N_i} = {}^{U\cap N_{i-1}}\!/_{(U\cap N_{i-1})\cap N_i} \cong {}^{(U\cap N_{i-1})N_i}\!/_{N_i} \subset {}^{N_{i-1}}\!/_{N_i}$$

$\Rightarrow {}^{U\cap N_{i-1}}\!/_{U\cap N_i}$ ist ebenfalls abelsch.

(ii) Betrachte

$$G' = \varphi(G) = \varphi(N_0) \rhd \varphi(N_1) \rhd \varphi(N_2) \rhd \cdots \rhd \varphi(N_l) = \{1\}.$$

Wir haben eine Surjektion

$${}^{N_{i-1}}\!/_{N_i} \to {}^{\varphi(N_{i-1})}\!/_{\varphi(N_i)}$$

Da ${}^{N_{i-1}}\!/_{N_i}$ abelsch ist, gilt dies auch für ${}^{\varphi(N_{i-1})}\!/_{\varphi(N_i)}$.

□

Satz 7.98
Es sei G auflösbar, $N \lhd G$. Dann gibt es eine Kette

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_I \rhd \cdots \rhd N_l = \{1\}$$

mit

(i) ${}^{N_{i-1}}\!/_{N_i}$ *ist zyklisch von Primzahlordnung.*

(ii) Es gibt ein i mit $N_i = N$.

Beweis. Nach obigem Satz sind N und ${}^{G}\!/_{N}$ auflösbare Gruppen. D.h. wir haben Ketten

$${}^{G}\!/_{N} = N_0' \rhd N_1' \rhd \cdots \rhd N_r' = \{1\} \text{ mit } {}^{N_{i-1}'}\!/_{N_i'} \cong \mathbb{Z}_{p_i} \tag{7.7.h}$$

und

$$N := N_r \rhd N_{r+1} \rhd \cdots \rhd N_s = \{1\} \text{ mit } {}^{N_{j-1}}\!/_{N_s} = \mathbb{Z}_{p_j} \tag{7.7.i}$$

Setze:

$$N_i := \pi^{-1}(N_i') \quad (\pi \colon G \to G(N))$$

$$\Rightarrow G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = N \text{ mit } {}^{N_{i-1}}\!/_{N_i} \cong {}^{N_{i-1}'}\!/_{N_i'} \cong \mathbb{Z}_{p_i} \tag{7.7.j}$$

Kombiniere nun Kette (7.7.j) mit Kette (7.7.i). □

Satz 7.99
Jede p-Gruppe ist auflösbar.

Beweis. G sei p-Gruppe. Damit ist $Z(G) \neq \{1\}$.

$$N^1 := Z(G) \rhd N^0 := \{1\}$$

$${}^{N^1}\!/_{N^0} = Z(G) \text{ ist abelsch.}$$

Betrachte: $G^1 := {}^{G}\!/_{N^1}$; G^1 ist wieder eine p-Gruppe, also gilt

$$Z(G^1) \neq \{1\}$$

Betrachte $\pi^1 \colon G \to G^1$ und definiere

$$N^2 := (\pi^1)^{-1}(Z(G^1)).$$

Dies liefert uns

$$N^l \rhd \cdots \rhd N^2 \rhd N^1 \rhd N^0 = \{1\}$$

mit ${}^{N^i}\!/_{N^{i-1}}$ abelsch, da isomorph zu einem Zentrum

$${}^{N^2}\!/_{N^1} \cong Z(G^1)$$

Da G endlich ist, kommt man nach endlich vielen Schritten zu $N^l = G$. □

Satz 7.100
Die symmetrische Gruppe S_n ist für $n \geq 5$ nicht auflösbar.

Definition 7.101
Ein *Dreierzykel* in S_n ist ein Element, das genau $n-3$ Elemente fest lässt.

Schreibweise: $(a\ b\ c) \quad (a \to b \to c \to a)$

Lemma 7.102
Sei $n \geq 5$ und sei U eine Untergruppe von S_n, die alle Dreierzykeln enthält. Sei $N \lhd U$ mit ${}^{U}\!/_{N}$ abelsch. Dann enthält auch N alle Dreierzykel.

Beweis. Sei $(a\ b\ c) \in S_n$: Wähle d, e mit $d \neq e$; $d, e \notin \{a, b, c\}$.

$$\begin{aligned} x &:= (d\ b\ a) \\ y &:= (a\ e\ c) \quad x, y \in U \end{aligned}$$

$$\Rightarrow x^{-1}y^{-1}xy = (a\ b\ d)(c\ e\ a)(d\ b\ a)(a\ e\ c) = (a\ b\ c) \in U$$

Da ${}^{U}\!/_{N}$ abelsch ist, folgt $x^{-1}y^{-1}xy \in N$, d.h. aber $(a\ b\ c) \in U$. □

Beweis. (von Satz (7.100))
Angenommen S_n sei auflösbar:

$$S_n = N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_l = \{1\} \text{ mit } {}^{N_{i-1}}\!/_{N_i} \text{ abelsch.}$$

$\overset{\text{Lemma (7.102)}}{\Rightarrow}$ N_1 enthält alle Dreierzykel. $\overset{\text{Lemma (7.102)}}{\Rightarrow}$ N_2 enthält alle Dreierzykel. $\Rightarrow \cdots \Rightarrow N_l$ enthält alle Dreierzykel. Widerspruch dazu, dass $N_l = \{1\}$ ist. □

Kapitel 8

Galoistheorie

8.1 Ergänzungen zur Galoistheorie

L/K sei galoisch, d.h. endlich, normal, separabel.

$$\mathcal{Z} := \{L'; K \subset L' \subset L \text{ ist ein Zwischenkörper von } L/K\}$$
$$G := G(L/K) = \{g; g\colon L \to L \text{ mit } g|_K = \mathrm{id}_K,\ g \text{ Automorphismus}\}$$

(Galoisgruppe)

$$\mathcal{G} := \{H; H \subset G \text{ Untergruppe}\}$$

Hauptsatz (6.82)

$$\begin{aligned} \mathcal{G} &\overset{1:1}{\longleftrightarrow} \mathcal{Z} \\ H &\longmapsto L_H := \{x \in L; h(x) = x \text{ für alle } h \in H\} \end{aligned}$$

(„Fixkörper“)

$$G_{L'} := \{g \in G; g|_{L'} = \mathrm{id}_{L'}\} \longleftarrow\!\shortmid L'$$

(„Isotropiegruppe“)

Die *Konjugierten* zu einem Zwischenkörper L' sind die Körper $g(L')$ mit $g \in G = G(L/K)$.

Konjugation Sei $g \in G$

$$\begin{aligned} \sigma g\colon G &\to G \\ x &\mapsto gxg^{-1}. \end{aligned}$$

Die *konjugierten Untergruppen* von $H \subset G$ sind die Gruppen gHg^{-1} $(g \in G)$.

Erinnerung: $\underset{\text{(normal)}}{H \lhd G} \Leftrightarrow gHg^{-1} = H \qquad (g \in G)$

Lemma 8.1
Unter der Galoiskorrespondenz entsprechen die konjugierten Körper von L' genau den konjugierten Untergruppen von $G_{L'}$, genauer:

$$G_{g(L')} = gG_{L'}g^{-1}.$$

Beweis. $gG_{L'}g^{-1} \subset G_{g(L')}$: Sei hierzu $x \in L'$, $h \in G_{L'}$. Dann gilt:

$$(ghg^{-1})(g(x)) = (gh)(\underbrace{g^{-1}g(x)}_{=x}) = g(x)$$

genügt nun: $|gG_{L'}g^{-1}| = |G_{g(L')}|$.
Dies gilt, da:

$$|G_{g(L')}| = [L : g(L')] = [L : L'] = |G_{L'}| = |gG_{L'}g^{-1}|.$$

□

Definition 8.2
Eine Galoiserweiterung L/K heißt *abelsch* (*zyklisch, auflösbar*), falls die Galoisgruppe $G = G(L/K)$ abelsch (zyklisch, auflösbar) ist.

Satz 8.3
L/K sei galoisch, L' sei ein Zwischenkörper. Dann gilt:

(i) *L'/K ist galoisch $\Leftrightarrow G_{L'} \lhd G$*

(ii) *Ist L'/K galoisch, so gilt*

$$G(L'/K) = {}^{G}\!/_{G_{L'}}.$$

Beweis. (i) L'/K ist galoisch $\Leftrightarrow$ L'/K ist normal $\overset{\text{Lemma (8.1)}}{\Longleftrightarrow}$ $G_{L'} \lhd G$. (Endlichkeit und Separabilität ergeben sich automatisch)

(ii) Wir wissen, dass L/L' normal ist, d.h. für $g \in G = G(L/K)$ ist $g(L') = L'$. D.h. wir können betrachten

$$\begin{aligned} \varphi\colon G &\to G(L'/K) \qquad \text{(surjektiv)} \\ g &\mapsto g|_{L'} \qquad \text{(da } g(L') = L') \end{aligned}$$

Es gilt

$$\ker\varphi = \{g; g|_{L'} = \mathrm{id}_{L'}\} = G_{L'}.$$

Es gilt

$$G(L'/K) \cong {}^{G}\!/_{\ker\varphi} = {}^{G}\!/_{G_{L'}}.$$

□

Folgerung 8.4

(i) *L/K sei zyklisch von Ordnung n. Dann gibt es zu jedem $m|n$ genau einen Zwischenkörper L' mit $[L' : K] = m$.*

(ii) *L/K sei abelsch. L' sei ein Zwischenkörper. Dann sind L/L' und L'/K abelsch. Ist $n = [L : K]$ und $m|n$, so gibt es mindestens einen Zwischenkörper L' mit $[L' : K] = m$.*

(iii) *L/K sei auflösbar. Dann ist auch L/L' auflösbar. Ist L'/K galoisch, so ist auch L'/K auflösbar.*

Beweis. (i) $G \cong \mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{n\,\mathbb{Z}}$. Es sei $mk = n$. Es gibt dann genau eine Untergruppe H von G mit $|H| = k$. Setze

$$L' := L_H.$$

Dann gilt:

$$[L : L'] = |H| = k.$$

Andererseits:

$$n = [L : K] = \underbrace{[L : L']}_{=k} \cdot [L' : K]$$

$\Rightarrow [L' : K] = \frac{n}{k} = m.$

(ii) L/L' ist automatisch galoisch. Es gilt

$$G(L/L') = G_{L'} \subset G.$$

Da G abelsch ist, gilt dies auch für $G_{L'}$.

L'/K ist galoisch, da $G_{L'}$ als Untergruppe einer abelschen Gruppe normal ist. Nach obigem gilt

$$G(L'/K) = {}^{G}\!/_{G_{L'}}$$

und ist damit als Quotient einer abelschen Gruppe abelsch.

(iii) Hier gilt

$$G(L/L') = G_{L'} \subset G \qquad\qquad G(L'/K) = {}^{G}\!/_{G_{L'}}$$

Die Aussage folgt, da Untergruppen und Quotientengruppen auflösbarer Gruppen wieder auflösbar sind.

□

Satz 8.5
Es sei $L = K[x]/K$ galoisch. Es sei $f \in K[X]$ das Minimalpolynom von x. Dann ist die Galoisgruppe $G = G(L/K)$ isomorph zu einer Untergruppe der Permutationsgruppe von $\{x_1, \ldots, x_n\}$, wobei $x_1, \ldots, x_n$ die Nullstellen von f sind.

Beweis. Es sei $f \in K[X]$ das Minimalpolynom von x. Für $f \in G$ gilt $f^g = f$. Also operiert g auf den Wurzeln von f, d.h. auf $\{x_1 = x, \ldots, x_n\}$ (Denn: $f(g(x_i)) = a_0 + a_1 g(x_i) + \cdots + g(x_i)^n \overset{f^g = f}{=} g(a_0) + g(a_1 x_i) + \cdots + g(x_i)^n = g(\underbrace{a_0 + a_1 x_i + \ldots a_n x_i^n}_{=0}) =$ $g(0) = 0 \Rightarrow g(x_i)$ ist auch Nullstelle). D.h.

$$G \to \mathrm{Perm}\{(x_1, \ldots, x_n)\} \cong S_n.$$

Bleibt: Diese Abbildung ist injektiv. Folgt aus der folgenden Aussage:

Behauptung: g ist durch $g(x)$ festgelegt.

Denn: Sei $y \in L$. Dann gibt es eine Darstellung

$$y = \sum_{i=0}^{n-1} a_i x^i; \qquad a_i \in K$$
$$\Rightarrow g(y) = \sum_{i=0}^{n-1} g(a_i x^i) = \sum_{i=0}^{n-1} a_i g(x^i) = \sum_{i=0}^{n-1} a_i g(x)^i.$$

□

8.2 Konstruktionen mit Zirkel und Lineal

$\mathcal{M} \subset \mathbb{C} = \mathbb{R}^2; 0, 1 \in \mathcal{M}$.
$\bar{\mathcal{M}} := \{\bar{m}; m \in \mathcal{M}\}$
$K_0 := (\mathcal{M} \cup \bar{\mathcal{M}}) = \mathbb{Q}(\mathcal{M} \cup \bar{\mathcal{M}})$
Hatten gesehen:

Satz 8.6
Ist $x \in \mathbb{C}$ aus der Menge $\mathcal{M}$ mit Zirkel und Lineal konstruierbar, so gilt:

$$[K_0(x) : K_0] = 2^m.$$

Satz 8.7
Es sind äquivalent

(i) *$z \in \mathcal{M}$ konstruierbar*

(ii) *z ist in einem Zwischenkörper L von $\mathbb{C}/K_0$ enthalten, der aus K_0 durch sukzessive Adjunktion von Quadratwurzeln entsteht.*

Ziel: Charakterisierung mit Hilfe des Zerfällungskörpers von z.
Vorbereitungen hierzu:

Lemma 8.8
Es sei K ein Körper, $\operatorname{char} K \neq 2$. *Es sei $[L : K] = 2$. Dann entsteht L aus K durch Adjunktion einer Quadratwurzel.*

Bemerkung 8.9
Hatten dies bereits für $K \subset L \subset \mathbb{C}$ gesehen.

Beweis. Sei $x \in L \setminus K$, Dann gilt $L = K[x]$ (da: $[L : K] = 2$). Das Minimalpolynom von x hat Grad 2. Dies sei etwa

$$f(X) = X^2 + \lambda_1 X + \lambda_0 \qquad (\lambda_0, \lambda_1 \in K)$$

Setze

$$y := x + \frac{\lambda_1}{2} \in L \setminus K \qquad (\Rightarrow L = K[y]).$$

Bleibt: $y^2 \in K$. Dies gilt, da

$$y^2 = \left(x + \frac{\lambda_1}{2}\right)^2 = x^2 + \lambda_1 x + \frac{\lambda_1^2}{4}$$
$$= \underbrace{(x^2 + \lambda_1 x + \lambda_0)}_{=0} - \underbrace{\lambda_0 + \frac{\lambda_1^2}{4}}_{\in K} \Rightarrow y^2 \in K.$$

□

Satz 8.10
Es sei $\operatorname{char} K \neq 2$. *Es sei* $\bar{K}$ *der algebraische Abschluss von* K *und* $x \in \bar{K}$ *sei separabel über* K *mit Minimalpolynom* $f(X) \in K[X]$. *Es sei* Z *der Zerfällungskörper von* f. *Dann sind äquivalent:*

(i) x *ist in einem Zwischenkörper* $\bar{K}/K$ *enthalten, der aus* K *durch sukzessive Adjunktion von Quadratwurzeln entsteht.*

(ii) $[Z : K] = 2^m$

Anwendung:

Korollar 8.11
Es sind äquivalent:

(i) $x \in \mathbb{C}$ *ist aus* $\mathcal{M}$ *konstruierbar mit Zirkel und Lineal.*

(ii) x *ist algebraisch über* K_0 *und der Grad der Körpererweiterung des Zerfällungskörpers* Z *von* x *über* K_0 *ist eine* 2*-er Potenz (d.h.* $[Z : K_0] = 2^m$*).*

Bemerkung 8.12
Wegen $\operatorname{char} K_0 = 0$ ist x automatisch separabel.

Bemerkung 8.13
Da $K(x_0) \subset Z$ ist, finden wir auch wieder, dass $[K_0(x) : K_0] = 2^k$.

Lemma 8.14
Es sei $L = K[x_1, \ldots, x_n]$ *mit* $x_1^2 \in K$ *und* $x_i^2 \in K[x_1, \ldots, x_{i-1}]$. *Es sei* N *die normale Hülle von* L. *Dann gilt* $[N : K] = 2^k$.

Beweis. Induktion nach n.

$\underline{n = 1}$: $L = K[x_1]; x_1^2 \in K$. Entweder $L = K$ oder $[L : K] = 2$. Dann ist $N = L$ und daher $[N : K] = 2$.

$\underline{n - 1 \mapsto n}$: Sei $L' = [x_1, \ldots, x_{n-1}]$ und N' die normale Hülle.

$$IV \Rightarrow [N' : K] = 2^m.$$

Es seien $y_1, \ldots, y_r$ die Konjugierten von x_n über K, d.h. die Elemente $\sigma_i(x_n)$ mit $\sigma_i \in G(\bar{K}/K)$. Es gilt

$$x_n^2 \in L'$$
$$\Rightarrow y_i^2 = \sigma_i(x_n^2) \in \sigma(L') \subset \sigma(N') = N'$$

da N' normal ist. Es gilt

$$N = N'[y_1, \ldots, y_r]$$

(vgl. die Konstruktion der normalen Hülle).

$\Rightarrow N$ entsteht aus N' durch sukzessive Adjunktion von Quadratwurzeln.
$\Rightarrow [N : N'] = 2^l \Rightarrow [N : K] = [\underbrace{N : N'}_{=2^l}][\underbrace{N' : K}_{=2^m}] = 2^{l+m}$.

□

Beweis. (von Satz (8.10))

(i)⇒(ii): Wir haben $K \subset L \subset N$. Es ist auch $Z \subset N$

$$\Rightarrow [Z:K] \mid [N:K] = 2^m \overset{Lemma}{\Rightarrow} [Z:K] = 2^k.$$

(ii)⇒(i): Da Z/K Zerfällungskörper eines separablen Polynoms ist, ist Z/K galoisch. Da $[Z:K] = |G|$ (G=Galoisgruppe) ist $|G| = 2^m$, d.h. G ist eine 2-Gruppe.

$$\Rightarrow \text{ Es gibt eine Folge von Untergruppen:}$$
$$G = N_0 \underset{\neq}{\rhd} N_1 \underset{\neq}{\rhd} N_2 \underset{\neq}{\rhd} \dots \underset{\neq}{\rhd} N_l = \{1\},$$

sodass N_i/N_{i+1} zyklisch von Ordnung 2 ist.

$$\Rightarrow N_i/M_{i+1} = \mathbb{Z}_2 \Rightarrow [N_i : N_{i+1}] = 2.$$

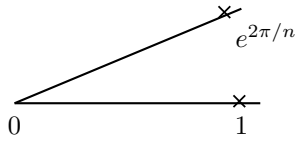
Hauptsatz der Galoistheorie liefert dann:

$$K = L_0 \subset L_1 \subset \cdots \subset L_l = Z$$

mit $[L_i : L_{i-1}] = 2$. $\overset{\text{Lemma (8.8)}}{\Longrightarrow}$ L_i entsteht aus L_{i-1} durch Adjunktion einer Quadratwurzel $\Rightarrow$ Z entsteht aus K durch sukzessive Adjunktion von Quadratwurzeln $\overset{x\in\mathbb{Z}}{\Longrightarrow}$ (i).

□

Konstruktion des regulären n–Ecks



$$\mathcal{M} = \{0,1\},\ K_0 = \mathbb{Q}$$

Satz 8.15
Sei $n = p$ prim. Dann ist das reguläre n–Eck genau dann konstruierbar, wenn

$$p = 2^m + 1.$$

Beweis. Z: Zerfällungskörper von $e^{2\pi i/p}$ über $\mathbb{Q}$.

$$X^p - 1 = (X-1)(\underbrace{X^{p-1} + X^{p-2} + \cdots + 1}_{\text{irreduzibel (Eisenstein)}})$$
$$\Rightarrow [Z:\mathbb{Q}] = p - 1 \overset{!}{=} 2^m \Leftrightarrow p = 2^m + 1.$$

□

Satz 8.16
Ist $p = 2^m + 1$ eine Primzahl, dann ist auch m eine Zweierpotenz, d.h. $p = 2^{(2^n)} + 1$.

Beweis. $m = 2^n \cdot r$, mit $2 \nmid r$. Dann ist r ungerade.
Annahme: $r > 1$

$$\begin{aligned} 2^m + 1 &= 2^{(2^n \cdot r)} + 1 = (2^{(2^n)})^r - (-1)^r = a^r - b^r \qquad (a = 2^{(2^n)},\ b = -1) \\ &= (a-b)(\underbrace{a^{r-1} + a^{r-2}b + \cdots + b^{r-1}}_{\neq 1 \text{ falls } r>1}) \\ &\Rightarrow 2^m + 1 \text{ ist nicht prim} \qquad \lightning \end{aligned}$$

□

$n = 0$: $p = 3$, $n = 1$: $p = 5$, $n = 2$: $p = 17$
$n = 3$: $p = 257$, $n = 4$: $p = 65537$
$n = 5, 6, 7, 8, 9$: keine Primzahl $n \geq 10$: ?

Fermatsche Primzahlen: Gibt es weitere (oder unendliche viele) Fermatsche Primzahlen?

——

Frage: Wann ist das reguläre n–Eck (n beliebig) konstruierbar?

8.3 Einheitswurzeln

K: Körper

Definition 8.17
Die n–ten *Einheitswurzeln* von K sind die Lösungen der Gleichung

$$X^n - 1 = 0.$$

Bemerkung 8.18
$W_n(K) \subset K^*$ ist eine endliche Gruppe und damit zyklisch.

Beispiel 8.19
$W_n(\mathbb{C}) = \{e^{2k\pi i/n}; 0 \leq k < n\} \cong \mathbb{Z}_n$.

Definition 8.20
Der n–te *Einheitswurzelkörper* über K ist der Zerfällungskörper des Polynoms $X^n - 1$ über K.

Bezeichnung: $E_n(K)$

Beispiel 8.21
$E_n(\mathbb{Q}) = \mathbb{Q}(e^{2\pi i/n})$

Bemerkung 8.22
$E_n(K) = K(W_n(\bar{K}))$.

Satz 8.23
Es sei $p = \operatorname{char} K$. Es sei $p = 0$ oder $p \nmid n$. Dann ist $E_n(K)/K$ galoisch.

Beweis. $E_n(K)$ ist der Zerfällungskörper von $X^n - 1$. Dieses Polynom ist separabel, falls $p = 0$ oder $p \nmid n$, da:

$$(X^n - 1)' = \underbrace{n}_{\neq 0} X^{n-1}.$$

Da 0 keine Nullstelle von $X^n - 1$ ist, ist das Polynom separabel. □

Satz 8.24
Es sei wieder $p = 0$ oder $p \nmid n$. Dann gilt

$$W_n(\bar{K}) = W_n(E_n(K)) \cong \mathbb{Z}_n \,.$$

Beweis. $X^n - 1$ hat genau n Nullstellen, da es separabel ist. Also ist $|W_n(\bar{K})| = n$. Da $W_n(\bar{K})$ zyklisch ist, folgt $W_n(\bar{K}) \cong \mathbb{Z}_n$. □

Generalvoraussetzung für diesen Abschnitt: $\boxed{p = 0 \text{ oder } p \nmid n}$

Definition 8.25
Eine n–te Einheitswurzel heißt *primitiv*, falls sie die Gruppe $W_n(E(K))$ erzeugt.

Beispiel 8.26
$K = \mathbb{Q}$, $e^{2\pi ik/n}$ ist primitiv $\Leftrightarrow (k, n) = 1$

Erinnerung: Die Anzahl der primitiven Einheitswurzeln ist gleich $\varphi(n)$ (= Eulersche φ–Funktion).

Kreisteilungspolynome

Es seien $\xi_1, \ldots, \xi_{\varphi(n)} \in E_n(K)$ die primitiven n–ten Einheitswurzeln.

$$\boxed{\phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - \xi_i)} \qquad (\deg \phi_n = \varphi(n))$$

Definition 8.27
$\phi_n(X)$ heißt das n–te Kreisteilungspolynom über dem Körper K.

Bemerkung 8.28

$$[E_n(K) : K] \leq \varphi(n) = \deg \phi_n(X).$$

Der Grad kann kleiner sein, etwa wenn K bereits die n–ten Einheitswurzeln enthält.

Lemma 8.29

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

Beweis. Beide Polynome sind normiert. Dann folgt die Aussage, da

(i) Jede n–te Einheitswurzel ist eine primitive d–te Einheitswurzel für ein $d \mid n$.

(ii) Ist $d \mid n$, dann ist jede d–te Einheitswurzel auch eine n–te Einheitswurzel.

□

Es gilt: $\phi_n \in E_n(K)[X]$.

Erinnerung: Es sei K ein Körper. Der Primkörper von K ist der kleinste Unterkörper von K.

$$\text{Primkörper } \cong \begin{cases} \mathbb{Q}, & \text{falls } \operatorname{char} K = 0 \\ \mathbb{Z}_p, & \text{falls } p = \operatorname{char} K > 0 \end{cases}$$

Satz 8.30
Die Koeffizienten von $\phi_n(X)$ liegen bereits im Primkörper von K, bzw. falls $\operatorname{char} K = 0$ *ist sogar in $\mathbb{Z}$.*

Beweis. Induktion nach n.

$\underline{n = 1:}$ $\phi_1 = X - 1$.

$\underline{n - 1 \mapsto n:}$

$$X^n - 1 = \prod_{d|n} \phi_d(X) = \phi_n(X) \cdot \underbrace{\prod_{\substack{d|n \\ d<n}} \phi_d(X)}_{\overset{\text{IV}}{=:} g(X) \in \mathbb{Z}_p[X] \text{ bzw. } \mathbb{Z}[X]} \tag{1}$$

Polynomdivision von $X^n - 1$ durch $g(X)$ in $\mathbb{Z}_p[X]$ bzw. $\mathbb{Z}[X]$:

$$X^n - 1 = g(X)h(X) + r(X), \qquad h(X), r(X) \in \mathbb{Z}_p[X], \mathbb{Z}[X] \tag{2}$$

Eindeutigkeit der Polynomdivision, (1) und (2) $\Rightarrow r(X) = 0$, $h(X) = \phi_n(X)$.

□

Satz 8.31
Es sei wieder $p = \operatorname{char} K = 0$ oder $p \nmid n$. Dann gibt es eine Inklusion

$$G(E_n(K)/K) \hookrightarrow E(\mathbb{Z}_n) \qquad \textit{(Einheitengruppe).}$$

Beweis. Sei ξ eine primitive n–te Einheitswurzel. Dann ist jedes Element $g \in G(E_n(K)/K)$ durch $g(\xi)$ bestimmt. Es ist $g(\xi) = \xi^r$ eine primitive Einheitswurzel, d.h. $(r, n) = 1$. D.h. $\bar{r}$ ist eine Einheit in $\mathbb{Z}_n$. Damit erhalten wir eine Inklusion

$$\begin{aligned} G(E_n(K)/K) &\hookrightarrow E(\mathbb{Z}_n) \\ g &\mapsto \bar{r}. \end{aligned}$$

Dies ist ein Homomorphismus: Sei g' mit $g'(\xi) = \xi^s$. Dann gilt

$$(g'g)(\xi) = g'(g(\xi)) = g'(\xi^r) = (g'(\xi))^r = (\xi^s)^r = \xi^{s \cdot r}.$$

D.h. $g'g$ wird $\bar{s}\bar{r}$ zugeordnet. □

$K = \mathbb{Q}$

Satz 8.32
Für $K = \mathbb{Q}$ gilt:

(i) $\phi_n(X)$ ist irreduzibel

(ii) $[E_n(\mathbb{Q}) : \mathbb{Q}] = \varphi(n)$

(iii) $G(E_n(\mathbb{Q})/\mathbb{Q}) \cong E(\mathbb{Z}_n)$

Beweis. (ii), (iii) sind leichte Folgerungen von (i), denn:

(ii) $[E_n(\mathbb{Q}) : \mathbb{Q}] = [\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = [e^{2\pi i/n} : \mathbb{Q}] \overset{\text{(i)}}{=} \deg \phi_n(X) = \varphi(n)$

(iii) wegen (ii) ist $|G(E_n(\mathbb{Q})/\mathbb{Q})| = \varphi(n) = |E(\mathbb{Z}_n)|$. Damit sofort aus obigem Satz.

Bleibt: $\phi_n(X)$ ist irreduzibel. □

Lemma 8.33
Es gilt stets:

$$n^p \equiv n \mod p. \qquad (n \in \mathbb{Z})$$

Beweis. $\underline{n = 0 = (k \cdot p)}$: klar

$\underline{n \neq 0}$: Betrachte $E(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$.
kleiner Fermat: $n^{p-1} \equiv 1 \mod p$ (falls $p \nmid n$)

$$\Rightarrow n^p \equiv n \mod p.$$

□

Andere Formulierung: Der Frobeniushomomorphismus

$$\begin{aligned} F\colon \mathbb{Z}_p &\to \mathbb{Z}_p \\ x &\mapsto x^p \end{aligned}$$

ist die Identität.

Zurück zur Irreduzibilität von $\phi_n(X)$:

Beweis. Es sei ξ eine primitive n–te Einheitswurzel und $f(X)$ das Minimalpolynom von ξ über $\mathbb{Q}$. Es gilt, dass $f(X)|\phi_n(X)$.

Ziel: $f(X) = \phi_n(X)$.

1**. Behauptung:** $f(X) \in \mathbb{Z}[X]$
Denn: Zerlege $X^n - 1$ über $\mathbb{Z}$ in irreduzible Faktoren. Es sei f_1 ein solcher Faktor mit $f_1(\xi) = 0$. Nach Gauß (4.12) ist $f_1(X)$ über $\mathbb{Q}$ irreduzibel (da $X^n - 1$ normiert ist, ist $\pm f_1(X)$ normiert), also $f = \pm f_1 \in \mathbb{Z}[X]$.

Es sei nun p prim mit $p \nmid n$. Dann ist auch ξ^p eine primitive n–te Einheitswurzel. Es sei $g(X)$ das Minimalpolynom von ξ^p. Dann ist $g(X) \in \mathbb{Z}[X]$.

2**. Behauptung:** $f(X) = g(X)$
Denn: Ansonsten hat man eine Gleichung

$$X^n - 1 = f(X)g(X)h(X) \qquad (h \in \mathbb{Z}[X]) \tag{8.8.a}$$

(Dies gilt, da f, g beide $X^n - 1$ teilen und keinen gemeinsamen Faktor haben). Das Polynom $g(X^p)$ hat ebenfalls die Nullstelle ξ. Also gilt

$$g(X^p) = f(X)j(X) \qquad (j \in \mathbb{Z}[X]) \tag{8.8.b}$$

Wir „reduzieren nun modulo p“, d.h. wir betrachten das Bild unter der Abbildung

$$\alpha\colon\ \mathbb{Z}[X] \to \mathbb{Z}_p[X].$$

Unter dieser Abbildung werden (8.8.a), (8.8.b) zu:

$$\alpha(X^n - 1) = \alpha(f(X))\alpha(g(X))\alpha(h(X)) \tag{8.8.c}$$
$$\alpha(g(X^p)) = \alpha(f(X))\alpha(j(X)) \tag{8.8.d}$$

In $\mathbb{Z}_p[X]$ gilt:

$$\alpha(g(X^p)) = \alpha(\sum_{i=0}^{N} a_i(X^p)^i) = \sum_{i=0}^{N} \bar{a}_i(X^p)^i \overset{\text{Lem. (8.33)}}{=} \sum_{i=0}^{N} \bar{a}_i^p(X^i)^p$$
$$= \left(\sum_{i=0}^{N} \bar{a}_i \cdot X^i\right)^p = (\alpha(g(X))^p$$

Damit wird (8.8.d) zu

$$(\alpha(g(X)))^p = \alpha(f(X))\alpha(j(X)). \tag{8.8.e}$$

Es sei $\gamma(X)$ ein Teiler von $\alpha(f(X))$ in $\mathbb{Z}_p[X]$. Nach (8.8.e) ist dies auch ein Teiler von $\alpha(g(X))$. Nach (8.8.c) ist dann $\gamma^2(X)$ ein Teiler von $\alpha(X^n - 1) \Rightarrow$ $X^n - 1$ hat über $\bar{\mathbb{Z}}_p[X]$ mindestens eine doppelte Nullstelle. Dies ist ein Widerspruch, da:

$$(X^n - 1)' = \underbrace{n}_{\neq 0} X^{n-1}.$$

$\Rightarrow$ Behauptung 2.

3. **Behauptung:** Es gilt $f(\eta) = 0$ für jede n–te Einheitswurzel ($\Rightarrow f = \phi_n$)
Denn: Es ist $\eta = \xi^r$ mit (r,n)=1.

Sei $r = p_1 \cdots p_s$ mit p_i prim (Insbesondere gilt $(p_i, n) = 1$)
Induktion nach s:

$\underline{s = 1}$: $\eta = \xi^{p_1}$. Nach obigem gilt für das Minimalpolynom g von η, dass $g = f$ ist, also gilt: $f(\eta) = 0$.

$\underline{s - 1 \mapsto s}$: $f(\eta) = f(\xi^{p_1 \cdots p_s}) = f\big((\underbrace{\xi^{p_1 \cdots p_{s-1}}}_{=:\varrho})^{p_s}\big)$. ϱ ist eine primitive Einheitswurzel mit $f(\varrho) = 0$

$$\overset{\text{obiger Schritt}}{\Longrightarrow} f(\underbrace{\varrho^{p_0}}_{\| \ f(\eta)}) = 0$$

□

8.3.1 Reguläres n–Eck

Satz 8.34
Das reguläre n–Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn:

$$n = 2^m p_1 \cdots p_r$$

wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. $e^{2\pi i/n}$. Frage: Wann ist die Körpererweiterung

$$[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = 2^k \qquad ?$$

Hatten gesehen

$$[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n) \qquad (=\text{Eulersche Phi-Funktion})$$

Es sei

$$n = p_1^{\nu_1} \cdots p_s^{\nu_s}$$

die Primzahlzerlegung der Zahl n.

$$\Rightarrow \varphi(n) = p_1^{\nu_1 - 1} \cdot \ldots \cdot p_s^{\nu_s - 1}(p_i - 1) \cdots (p_s - 1) \stackrel{?}{=} 2^k.$$

Dies ist genau dann eine 2–er Potenz, wenn jede Primzahl $\neq 2$ nur mit Potenz 1 vorkommt und zusätzlich $p_i - 1$ eine 2–er Potenz ist, d.h. p_i ist eine Fermatsche Primzahl. □

8.4 Endliche Körper

K: Körper; $|K| < \infty$.
Wissen dann: $\operatorname{char} K = p > 0; \mathbb{Z}_p \subset K$

$$[K : \mathbb{Z}_p] = m \Rightarrow |K| = p^m.$$

Beispiel 8.35
$K = \mathbb{Z}_p$.

Satz 8.36
Ist p eine Primzahl, $m \geq 1$. Dann gibt es bis auf Isomorphie genau einen Körper mit p^m Elementen.

Bezeichnung: $\mathbb{F}_{p^m}$, $(\mathbb{F}_p = \mathbb{Z}_p)$, $GF(p, m)$ $(= \mathbb{F}_{p^m})$
Galoiskörper, Galoisfelder

Beweis. **Existenz:** $K = E_{p^m - 1}(\mathbb{Z}_p)$ (Zerfällungskörper von $X^{p^m - 1} - 1 =: f(X)$)
$E_{p^m - 1}(\mathbb{Z}_p)/\mathbb{Z}_p$ ist galoisch, da $X^{p^m - 1}$ separabel ist. Dies folgt, da

$$f'(X) = \underbrace{(p^m - 1)}_{\neq 0} X^{p^m - 2}.$$

Es gibt also genau $p^m - 1$ verschiedene $(p^m - 1)$–te Einheitswurzeln.

Behauptung: Die $p^m - 1$ Einheitswurzeln $W_{p^m - 1}(\bar{\mathbb{Z}}_p)$ bilden zusammen mit der 0 einen Körper. $(\Rightarrow |K| = p^m)$

Denn: $x, y \in W_{p^m - 1}(\bar{\mathbb{Z}}_p) \stackrel{!}{\Rightarrow} x \pm y, \frac{x}{y}, xy \in W_{p^m - 1}(\bar{\mathbb{Z}}_p)$
Etwa: Sei $x \neq y$.

$$(x - y)^{(p^m)} = x^{(p^m)} - y^{(p^m)} \stackrel{x^{(p^m - 1)} = 1}{=} x - y$$
$$\Rightarrow (x - y)^{(p^m - 1)} = 1.$$

Eindeutigkeit: Sei $|K| = p^m$.

Behauptung: $K \cong E_{p^m-1}(\mathbb{Z}_p)$.

Denn: K^* ist zyklisch (früheres Ergebnis), also $K^* \cong \mathbb{Z}_{p^m-1}$. Sei $x \in K^* \overset{\text{kl. Fermat}}{\Rightarrow}$ $x^{(p^m-1)} = 1$. Da $K/\mathbb{Z}_p$ endlich ist, kann man K in $\bar{\mathbb{Z}}_p$ einbetten und es gilt

$$K^* \subset W_{p^m-1}(\bar{\mathbb{Z}}_p).$$

Da $|K^*| = p^m - 1 = |W_{p^m-1}(\bar{\mathbb{Z}}_p)|$ folgt Gleichheit und damit

$$K = E_{p^m-1}(\mathbb{Z}_p).$$

□

Frage: Was ist die Galoisgruppe von $G(\mathbb{F}_{p^m}/\mathbb{F}_p)$?
Betrachte:

$$\begin{aligned} \sigma\colon \mathbb{F}_{p^m} &\to \mathbb{F}_{p^m} \\ x &\mapsto x^p \end{aligned}$$

Hatten gesehen: $\sigma|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p} \Rightarrow \sigma \in G(\mathbb{F}_{p^m}/\mathbb{F}_p)$.

Satz 8.37
$G(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \mathbb{Z}_m$ und wird von σ erzeugt.

Beweis. $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m \Rightarrow |G(\mathbb{F}_{p^m}/\mathbb{F}_p)| = m$.
genügt: $\sigma^i \neq \sigma^j$ für $1 \leq i \neq j \leq m$.
Sei y eine primitive $(p^m - 1)$–te Wurzel.
Annahme:

$$\begin{array}{ccc} \sigma^i(y) & = & \sigma^j(y) \qquad (1 \leq i \neq j \leq m) \\ \| & & \| \\ y^{p^i} & & y^{p^j} \end{array}$$

$$\Rightarrow \frac{y^{p^i}}{y^{p^j}} = 1 \Rightarrow y^{p^i - p^j} = 1$$

Widerspruch zur Primitivität von y, da $|p^i - p^j| < p^m - 1$. □

8.5 Auflösbarkeit von Gleichungen

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0 \qquad (a_i \in K)$$

Frage: Wann ist eine solche Gleichung durch Radikale auflösbar?

Definition 8.38
Man sagt, dass f *durch Radikale auflösbar* ist, falls es einen Körper L/K gibt mit:

(i) Es gibt $a_1, \ldots, a_k \in L,\ r_1, \ldots, r_k \in \mathbb{N}$ mit

$$a_1^{r_1} \in K,\ a_i^{r_i} \in K(a_1, \ldots, a_{i-1})$$

(ii) f hat in L eine Nullstelle.

Erinnerung: f sei separabel (z.B. $\mathrm{char}\, K = 0$). Dann ist der Zerfällungskörper Z von f galoisch über K.
Galoisgruppe von f: $G(f/K) := G(Z/K)$
Im wesentlichen: f auflösbar $\underset{(\mathrm{char}\, K=0)}{\Longleftrightarrow}$ $G(f/K)$ auflösbar

Die „reine“ Gleichung

$$f(X) = X^n - a \in K[X] \qquad (a \in K)$$

Bemerkung 8.39

(i) Gleichung $X^n - a = 0$ ist durch Radikale lösbar.

(ii) $\operatorname{char} K = 0$, $\operatorname{char} K = p \nmid n \Rightarrow f(X)$ ist separabel ($f'(X) = \underbrace{n}_{\neq 0} X^{n-1}$)

Satz 8.40
Es sei $\operatorname{char} K = 0$ *oder* $\operatorname{char} K = p \nmid n$. *Dann ist die Galoisgruppe von* $X^n - a = 0$ *zyklisch.* K enthalte die n–ten Einheitswurzeln.

Beweis. $L :=$ Zerfällungskörper von f über K.
Es sei $x \in \bar{K}$ mit $x^n = a$. Es sei $\xi \in K$ eine primitive n–te Einheitswurzel.
Lösungen von $X^n - a$: $\{x, \xi x, \xi^2 x, \ldots, \xi^{n-1} x\}$.
$\Rightarrow L = K[X]$.
Sei $G = G(L/K) = G(f/K)$. Dann ist jedes Element $g \in G$ durch $g(x)$ festgelegt

$$g \in G\colon\ g(x) = \xi^r x. \qquad (0 \leq r \leq n-1; r = r(g))$$

Damit

$$\begin{aligned} G &\hookrightarrow \mathbb{Z}_n \qquad \text{(Homomorphismus)} \\ g &\mapsto \bar{r} = r \mod n. \end{aligned}$$

$\Rightarrow G$ ist zyklisch. □

Bemerkung 8.41
Ist $f(X) = X^n - a$ irreduzibel, so folgt

$$G(f/K) \cong \mathbb{Z}_n\,.$$

(Denn: $|G(f/K)| = [L : K] = n$)
Achtung: K enthält die n–ten Einheitswurzeln.

Frage: Inwieweit gilt die Umkehrung?

Satz 8.42
K enthalte die n–ten Einheitswurzeln. Es sei $\operatorname{char} K = 0$ *oder* $\operatorname{char} K = p \nmid n$. *Es sei L eine galoische Körpererweiterung mit $G(L/K) \cong \mathbb{Z}_n$. Dann gibt es ein $x \in L$ mit $L = K[x]$ und $x^n \in K$.*

Beweis. Sei $G = G(L/K) \cong \mathbb{Z}_n$. Sei $g \in G$ ein erzeugendes Element, d.h.

$$G = \{1, g, g^2, \ldots, g^{n-1}\}.$$

Nach der Unabhängigkeit der Charaktere gibt es ein $\alpha \in L$ mit

$$x := \alpha + \xi g(\alpha) + \xi^2 g^2(\alpha) + \cdots + \xi^{n-1} g^{n-1}(\alpha) \neq 0$$

(ξ: primitive n–te Einheitswurzel).
Dann gilt:

$$g(x) = g(\alpha) + \xi g^2(\alpha) + \xi^2 g^3(\alpha) + \cdots + \underset{\xi^{-1}}{\xi^{n-1}} \underset{\alpha}{g^n(\alpha)}$$

$$\Rightarrow g(x) = \xi^{-1} \cdot x \Rightarrow g^\nu(x) = \xi^{-\nu} \cdot x \qquad (\nu \geq 1)$$

Sei $L' := K[x]$.
Ziel: $L' = L$

Es gilt $L' = K[x] \subset L$. Da es $\geq n$ verschiedene Abbildungen von L' nach $\bar{K}$ gibt (verwende G), folgt

$$[L' : K] \geq n.$$

Andererseits: $[L' : K] \leq [L : K] = n \Rightarrow [L' : K] = [L : K] = n$

$$\Rightarrow L = L' = K[x].$$

Bleibt: $x^n \in K = \text{Fix } G$.
genügt: $g(x^n) = x^n$. $\quad (\Rightarrow g^i(x^n) = x^n \text{ für } 1 \leq i \leq n)$

Dies gilt, da: $g(x) = \xi^{-1}x$

$$\Rightarrow g(x^n) = (g(x))^n = (\xi^{-1}x)^n = \underbrace{\xi^{-n}}_{=1} x^n = x^n$$

□

Definition 8.43
Eine Körpererweiterung N/K heißt *metaabelsch*, falls es eine Kette gibt:

$$K = K_0 \subset K_1 \subset \cdots \subset K_l = N,$$

so dass K_i/K_{i-1} abelsch ist.

Bemerkung 8.44
N ist endlich (klar), separabel (Transitivität der Separabilität), aber N/K muss nicht automatisch galoisch sein.

Satz 8.45
N/K sei metaabelsch und $\tilde{N}$ sei die galoische Hülle von N/K. Dann ist $\tilde{N}/K$ ebenfalls metaabelsch und galoisch, also insbesondere auflösbar.

Beweis. Erfolgt später. □

Theorem 8.46
Es sei $\operatorname{char} K = 0$. *Das Polynom $f \in K[X]$ sei irreduzibel. Ist f durch Radikale auflösbar, dann ist die Galoisgruppe $G(f/K)$ auflösbar.*

Beweis. Nach Voraussetzung haben wir

$$L = K(a_1, \ldots, a_s)$$

mit

(i) Es gibt $r_1, \ldots, r_s \geq 1$ mit $a_1^{r_1} \in K,\ a_i^{r_i} \in K(a_1, \ldots, a_{i-1})$

(ii) f hat in L eine Nullstelle.

Sei $n := r_1 \cdot \ldots \cdot r_s$. Sei $K' :=$ Körper, der aus K durch Adjunktion der r_1–ten, r_2–ten, … , r_s–ten Einheitswurzeln entsteht. Damit gilt

$$K \subset K' \subset E_n(K).$$

Da $E_n(K)/K$ abelsch, ist auch K'/K abelsch.
Sei nun:

$N :=$Körper, der aus L durch Adjunktion der r_1–ten, r_2–ten, … , r_s–ten Einheitswurzeln besteht.

Damit gilt:

$$N = K'(a_1, \ldots, a_s)$$

Behauptung: N/K ist metaabelsch.

Denn:

$$K \underset{(i)}{\subset} K' \underset{(ii)}{\subset} K'(a_1) \underset{(iii)}{\subset} K'(a_1, a_2) \subset \cdots \subset K'(a_1, \ldots, a_s) = N.$$

zu (i): abelsch

zu (ii): abelsch, da Zerfällungskörper von $X^{r_1} - b_1 = 0$; $b_1 = a_1^{r_1} \in K$ (Satz (8.40))

zu (iii): abelsch (selbes Argument)

$\overset{\text{Satz (8.45)}}{\Longrightarrow}$ $\tilde{N}/K$ ist galoisch ($\tilde{N}$ = galoische Hülle von N)

Es sei Z der Zerfällungskörper von f. Dann gilt

$$K \subset Z \subset \tilde{N}$$

(da f in $L \subset N$ eine Nullstelle hat und da $\tilde{N}/K$ normal ist. D.h. f zerfällt über $\tilde{N}$)

$$\tilde{N}/K \text{ galoisch } \underset{\text{Ergebnis}}{\overset{\text{früheres}}{\Longrightarrow}} Z/K \text{ ist galoisch.}$$

□

Bemerkung 8.47
Ist $p = \operatorname{char} K > r_i$, dann ist dieses Theorem auch in positiver Charakteristik richtig.

Definition 8.48
$K_1, \ldots, K_s \subset N$. Das *Kompositum* von $K_1, \ldots, K_s$ ist der kleinste Körper in N, der $K_1, \ldots, K_s$ umfasst.

Schreibweise: $K_1 \cdot \ldots \cdot K_s$.

Lemma 8.49
$\tilde{N}/K$ sei Körpererweiterung; $K_1 \subset K_2$ seien Zwischenkörper. N_1 sei ein weiterer Zwischenkörper. K_2/K_1 sei galoisch.

(i) *N_1K_2/N_1K_1 ist wieder galoisch*

(ii) *$G(N_1K_2/N_1K_1) \subset G(K_2/K_1)$*

Beweis. (i) K_2/K_1 galoisch $\Rightarrow$ K_2 entsteht aus K_1 durch Adjunktion der Nullstellen eines separablen Polynoms. Adjunktion derselben Nullstellen an N_1K_1 liefert N_1K_2. Da die Separabilität erhalten bleibt, ist N_1K_2/N_1K_1 ebenfalls galoisch.

(ii) Haben wir eine Abbildung

$$G(N_1N_2/N_1K_1) \to G(K_2/K_1)$$
$$g \mapsto g|_{K_2}.$$

Da g bereits durch die Werte auf K_2 bestimmt ist ($g|_{N_1} = \mathrm{id}_{N_1}$) ist diese Abbildung injektiv.

□

Lemma 8.50
N_1N_2 seien Zwischenkörper von $\tilde{N}/K$. Sind N_1, N_2 metaabelsch über K, dann auch $N_1 \cdot N_2$.

Beweis. N_1, N_2 sind metaabelsch über $K \Rightarrow$

$$\begin{aligned} K = K_0 \subset K_1 \subset \cdots \subset K_s = N_1; \qquad & K_i/K_{i-1} \text{ ist abelsch} \\ K = K_0' \subset K_1' \subset \cdots \subset K_t' = N_2; \qquad & K_j'/K_{j-1}' \text{ ist abelsch} \end{aligned}$$

Betrachte:

$$K = \underbrace{K_0 \subset \cdots \subset K_s}_{\text{jeder Schritt abelsch}} = N_1 = \underbrace{N_1K_0' \subset N_1K_1' \subset \cdots \subset N_1K_t'}_{\text{jeder Schritt abelsch}} = N_1N_2.$$

Denn

$$G(N_1K_j'/N_1K_{j-1}') \subset G(K_j'/K_{j-1}') \quad \text{abelsch}$$

□

Beweis. (von Satz (8.45))
N/K sind metaabelsch. Es seien $N_1 = N, N_2, \ldots, N_s$ die konjugierten Körper von N über K. Dann ist $N_1 \cdot \ldots \cdot N_s$ normal und damit ist

$$\tilde{N} = N_1 \cdot \ldots \cdot N_s.$$

N/K ist metaabelsch und N_i/K ist K–isomorph zu N/K. Also sind alle Erweiterungen N_i/K metaabelsch.

$$\overset{\text{Lem. (8.50)}}{\Longrightarrow} \tilde{N} = N_1 \cdot \ldots \cdot N_s/K$$

ist metaabelsch. □

Theorem 8.51
Es sei $0 \neq f \in K[X]$ *irreduzibel, separabel. Die Galoisgruppe* $G(f/K)$ *sei auflösbar.* $\operatorname{char} K = 0$ *oder* $\operatorname{char} K \nmid |G|$. *Dann ist* f *durch Radikale auflösbar und jede Lösung* $f = 0$ *liegt in einer Radikalerweiterung von* K *(d.h. sind Radikale).*

Beweis. $Z =$ Zerfällungskörper von f.
Z/K auflösbar $\Rightarrow$

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = Z$$

mit

$$G(K_i/K_{i-1}) \cong \mathbb{Z}_{r_i}\,.$$

Dann gilt

$$[Z : K] = r_1 \cdot \ldots \cdot r_s =: r = |G|$$

$K' :=$ Körper, der aus K durch Adjunktion der r_1–ten, … , r_s–ten Einheitswurzeln entsteht.
$N :=$ Körper, der aus Z durch Adjunktion der r_1–ten, … , r_s–ten Einheitswurzeln entsteht.

Da $\operatorname{char} K \nmid |G| = r$. Also $\operatorname{char} K \nmid r_i$.

Betrachte folgende Kette:

$$\begin{array}{ccc} K \subset K' & = K' \cdot K_0 \subset K'K_1 \subset K'K_2 \subset \cdots \\ \uparrow & \| \\ \text{sukzessive Radikal-erweiterungen} & K \end{array}$$

$$\subset K'K_s = K'Z = N \quad (\Rightarrow Z \subset N) \quad (8.8.\text{f})$$

Ziel: N entsteht aus K durch sukzessive Adjunktion von Wurzeln. (Hieraus folgt, wegen $Z \subset N$, die Behauptung).

Nach Lemma (8.49) (ii):

$$\begin{aligned} & G(K'K_i/K'K_{i-1}) \subset G(K_i/K_{i-1}) \cong \mathbb{Z}_{r_i} \\ \Rightarrow & G(K'K_i/K'K_{i-1}) \cong \mathbb{Z}_{r_i'} \qquad \text{mit } r_i' | r_i \end{aligned}$$

Da K' die r_1–ten, $\ldots$, r_s–ten Einheitswurzeln enthält und $r_i'|r_i$, enthält K' auch die r_1'–ten, $\ldots$, r_s'–ten Einheitswurzeln. D.h. wir können Satz (8.45) anwenden.

$$\text{Satz (8.45)} \Rightarrow K'K_i = K'K_{i-1}[x_i] \qquad \text{mit } x_i^{r_i'} \in K'K_{i-1}.$$

D.h. jeder Schritt in (8.8.f) ist eine Radikalerweiterung

$$\Rightarrow N/K \text{ ist eine Radikalerweiterung.}$$

□

Beispiel 8.52
$f(X) := X^5 - 2X^4 + 2 \in \mathbb{Q}[X]$

Behauptung 1: f ist nicht auflösbar!

Zunächst ist f irreduzibel über $\mathbb{Z}$ (Eisenstein $p = 2$). Damit auch über $\mathbb{Q}$ (Gauß (4.12)).

Behauptung 2: $G(f/\mathbb{Q}) \cong S_5$

$$S_5 \text{ nicht auflösbar} \overset{\text{Theorem (8.46)}}{\Longrightarrow} f \text{ ist nicht auflösbar}$$

Zur Gruppe S_n

S_n ist die Menge der Bijektionen von $M = \{1, \ldots, n\}$ in sich.

Definition 8.53
Eine Untergruppe $G \subset S_n$ heißt *transitiv*, wenn es zu je zwei Elementen $a, b \in M$ ein Element $g \in G$ gibt mit $g(a) = b$.

Satz 8.54
Es sei p prim. Ist $G \subset S_p$ eine transitive Untergruppe, die eine Transposition enthält, dann ist $G = S_p$.

Schreibweise: (a, b) = Transposition, die a und b vertauscht.

Bemerkung 8.55
$(a, b) = (b, a) = (a, b)^{-1}$

Beweis. Wir führen auf M folgende Relation ein:

$$a \sim b :\Leftrightarrow a = b \text{ oder } (a,b) \in G$$

Dies ist eine *Äquivalenzrelation*:

$$a \sim a \quad \surd, \qquad a \sim b \Rightarrow b \sim a \quad \surd \quad ((a,b) \in G \Rightarrow (b,a) = (a,b) \in G)$$
$$a \sim b, b \sim c \overset{!}{\Rightarrow} a \sim c$$

Denn: Kann annehmen, dass $a \neq b \neq c \neq a$ (sonst trivial)

$$(a,c) = \underbrace{(b,c)}_{\in G}\underbrace{(a,b)}_{\in G}\underbrace{(b,c)}_{\in G} \in G \Rightarrow a \sim c$$

Behauptung: Alle Äquivalenzklassen haben dieselbe Anzahl von Elementen.

Seien $\{a_1, \ldots, a_m\}$ und $\{a'_1, \ldots, a'_{m'}\}$ zwei Äquivalenzklassen. Da G transitiv ist, gibt es ein $\varphi \in G$ mit $\varphi(a_1) = a'_1$.

Behauptung:

$$\left.\begin{array}{rl} \varphi\colon \{a_1, \ldots, a_m\} \to \{a'_1, \ldots, a'_{m'}\} & (\Rightarrow m \leq m') \\ \text{analog} \quad \varphi^{-1}\colon \{a'_1, \ldots, a'_{m'}\} \to \{a_1, \ldots, a_m\} & (\Rightarrow m' \leq m) \end{array}\right\} \Rightarrow m = m'$$

Es gilt:

$$\underbrace{\varphi}_{\in G}\underbrace{(a_1, a_j)}_{\in G}\underbrace{\varphi^{-1}}_{\in G} \overset{(*)}{=} (\varphi(a_1), \varphi(a_j)) \in G$$
$$\Rightarrow \varphi(a_j) \sim \varphi(a_1) = a'_1$$
$$\Rightarrow \varphi(a_j) \in \{a'_1, \ldots, a'_{m'}\},\ j = 2, \ldots, m$$

Zu $(*)$:

$$(\varphi(a_1, a_j)\varphi^{-1})(\varphi(a_1)) = (\varphi(a_1, a_j))(a_1)(a_1) = \varphi(a_j)$$
$$(\varphi(a_1, a_j)\varphi^{-1})(\varphi(a_j)) = (\varphi(a_1, a_j))(a_j) = \varphi(a_1)$$
$$(\varphi(a_1, a_j)\varphi^{-1})(x) = (\varphi(a_1, a_j))\varphi^{-1}(x) = \varphi(\varphi^{-1}(x)) = x \quad (x \neq \varphi(a_1), \varphi(a_j))$$

Es sei nun m die Anzahl der Elemente in allen Äquivalenzklassen. Es gilt $m|p$, also $m = 1$ oder $m = p$. Da G eine Transposition enthält, gilt $m \geq 2$ und damit $m = p$. D.h. alle Elemente sind äquivalent. D.h. G enthält alle Transpositionen. D.h. $G = S_p$. □

Zurück zu Beispiel (8.52)

$$f(X) = X^5 - 2X^4 + 2 \in \mathbb{Q}[X]$$

Behauptung: f hat genau 3 reelle Nullstellen.

≥ 3 reelle Nullstellen:

$$f(-1) = -1 - 2 + 2 = -1 < 0 \qquad f(0) = 2 > 0$$
$$f(\frac{3}{2}) = \frac{81}{32} \cdot 3 - \frac{81}{32} \cdot 4 + 2 = 2 - \frac{81}{32} < 0 \quad f(2) = 32 - 32 + 2 > 0$$

$\underline{\leq 3 \text{ reelle Nullstellen:}}$ Hätte $f \geq 4$ reelle Nullstellen, so hätte $f' \geq 3$ relle Nullstellen.

Aber:

$$f'(X) = 5X^4 - 8X^3 = X^3(5X - 8).$$

Nullstellen: $x_1, x_2, x_3 \in \mathbb{R},\ x_4, x_5 \in \mathbb{C} \setminus \mathbb{R}\ (x_4 = \bar{x}_5)$

$Z :=$ Zerfällungskörper von f

$G(f/\mathbb{Q}) = G(Z/\mathbb{Q}) =: G$

G operiert auf den Wurzeln $x_1, \ldots, x_5$, also $G \subset S_5$.

Wir wissen:

(i) G operiert transitiv auf $\{x_1, \ldots, x_t\}$ (Galoistheorie)

(ii) $\iota\colon \mathbb{C} \to \mathbb{C},\ z \mapsto \bar{z}$ ist in $G(Z/\mathbb{Q})$, d.h. $(x_4, x_5) \in G$ $(\iota(x_4) = \bar{x}_4 = x_5)$ $(\iota|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}})$

D.h. G enthält eine Transposition (x_4, x_5)

$$\overset{\text{Satz (8.54)}}{\Longrightarrow} G = S_5.$$

Kapitel 9

Transzendente Körpererweiterungen

$K \subset L$ Körpererweiterung, $M \subset L$ (Teilmenge), $K \subset K(M) \subset L$.

Definition 9.1
Die *algebraische Hülle* von M in L über K ist wie folgt definiert:

$$H(M) := \{x \in L; x \text{ ist algebraisch über } K(M)\}$$

Bezeichnung: $H(M) = H_{L/K}(M)$
Haben also $K(M) \subset H(M) \subset L$.

Definition 9.2
Wir sagen, dass ein Element $\alpha \in L$ von der Menge M *algebraisch abhängig* ist, falls $\alpha \in H(M)$.

Definition 9.3
Eine Menge M heißt *algebraisch unabhängig*, falls für jedes Element $\alpha \in M$ gilt:

$$\alpha \notin H(M \setminus \{\alpha\})$$

Ansonsten heißt M algebraisch abhängig.

Bemerkung 9.4

(i) Für $\alpha \in M$ gilt $\alpha \in H(M \setminus \{\alpha\}) \Leftrightarrow H(M) = H(M \setminus \{\alpha\})$.

(ii) $\alpha \notin M$. Ist α algebraisch über $K(M)$, dann ist die Menge $M \cup \{\alpha\}$ algebraisch abhängig.

(iii) Eine Menge M ist genau dann algebraisch unabhängig, wenn jede endliche Teilmenge dies ist.

Bemerkung 9.5

(i) $M \subset H(M)$.

(ii) $H \subset M' \Rightarrow H(M) \subset H(M')$.

(iii) $H(H(M)) = H(M)$ (Transitivität der Algebraizität).

Lemma 9.6
Eine Menge M ist genau dann algebraisch unabhängig, wenn folgendes gilt:
Sind $\alpha_1, \dots \alpha_n \in M$ paarweise verschieden, so ist der Einsetzungshomomorphismus

$$\begin{aligned} K[X_1, \dots, X_n] &\to K[\alpha_1, \dots, \alpha_n] \\ f(X_1, \dots, X_n) &\mapsto f(\alpha_1, \dots, \alpha_n) \end{aligned}$$

injektiv (d.h. $K(X_1, \dots, X_n) \cong K[\alpha_1, \dots, \alpha_n]$). D.h. ist $f(\alpha_1, \dots, \alpha_n) = 0$, so ist $f = 0$.

Beweis. (i) M sei algebraisch unabhängig. Seien etwa $\alpha_1, \dots, \alpha_n$ algebraisch abhängig. Wir können annehmen: α_n ist algebraisch über $K(\alpha_1, \dots, \alpha_n)$. D.h. es gibt eine nicht-triviale Gleichung

$$\sum_{i=0}^{m} \underbrace{g_i(\alpha_1, \dots, \alpha_{n-1})}_{\in K(\alpha_1, \dots, \alpha_n)} = 0 \qquad (\text{ein } g_i \neq 0)$$

mit $g_i \in K[X_1, \dots, X_{n-1}]$. Setze

$$f(X_1, \dots, X_{n-1}) := \sum_{i=0}^{m} g_i(X_1, \dots, X_{n-1}) X_n^i$$

Dann ist $f \neq 0$, und es gilt $f(\alpha_1, \dots, \alpha_n) = 0$.

(ii) Es seien nun $\{\alpha_1, \dots, \alpha_n\}$ algebraisch unabhängig. Sei $f \in K[X_1, \dots, X_n]$ mit $f(\alpha_1, \dots, \alpha_n) = 0$. Es ist $f = 0$ zu zeigen: „Entwickle f nach x_n“, d.h. wir schreiben

$$f(X_1, \dots, X_n) = \sum_{i=0}^{m} g_i(X_1, \dots, X_{n-1}) X_n^i$$

$$\Rightarrow 0 = f(\alpha_1, \dots, \alpha_n) = \sum_{i=0}^{m} \underbrace{g_i(\alpha_i, \dots, \alpha_{n-1}) \alpha_n^i}_{\in K(\alpha_1, \dots, \alpha_{n-1})}$$

Da α_n nicht algebraisch über $K(\alpha_1, \dots, \alpha_{n-1})$ ist, folgt $g_i(\alpha_1, \dots, \alpha_{n-1}) = 0$; $i = 0, \dots, m$. Durch absteigende Induktion folgt $g_i(X_1, \dots, X_{n-1}) = 0$, also $f = 0$.

□

Lemma 9.7
Es sei M Teilmenge von L, $L \notin M$.

(i) Ist M algebraisch unabhängig, aber $M \cup \{\alpha\}$ algebraisch abhängig, so folgt $\alpha \in H(M)$.

(ii) Es sei $B \subset M$ eine maximale algebraisch unabhängige Teilmenge. Dann gilt $M \subset H(B)$ (d.h. jedes Element in M ist algebraisch über $K(B)$).

Beweis. (ii) folgt sofort aus (i). Bleibt also (i) $\Rightarrow$ (ii): $M \cup \{\alpha\}$ ist algebraisch abhängig. Dann gibt es $\alpha_1, \dots, \alpha_{n-1} \in M$, sodass für $\alpha_n = \alpha$ eine nicht-triviale Gleichung besteht:

$$f(\alpha_1, \dots, \alpha_n) = 0 \quad (f \in K[X_1, \dots, X_n])$$

Wieder

$$f(X_1, \ldots, X_m) = \sum_{i=0}^{m} g_i(X_1, \ldots, X_{n-1}) X_n^i$$

$$\Rightarrow 0 = f(\alpha_1, \ldots, \alpha_n) = \sum_{i=0}^{m} g_i(\alpha_i, \ldots, \alpha_{n-1}) \alpha_n^i \tag{9.9.a}$$

Da $f \neq 0$ und $\alpha_1, \ldots, \alpha_{n-1}$ algebraisch unabhängig sind, gibt es ein i_0, sodass $g_{i_0}(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Damit folgt

$$(9.9.a) \Rightarrow \alpha_n \text{ ist algebraisch über } K(M) \Rightarrow \alpha \in H(M)$$

□

9.1 Transzendenzbasen

Definition 9.8
L/K sei eine Körpererweiterung. Eine *Transzendenzbasis* von L/K ist eine Teilmenge $B \subset L$ mit:

(i) $L = H(B)$ (d.h. L ist algebraisch über $K(B)$).

(ii) B ist algebraisch unabhängig.

Lemma 9.9
Für eine Teilmenge $B \subset L$ sind äquivalent:

(i) B ist eine Transzendenzbasis von L/K.

(ii) Ist $B \subset M$ und $H(M) = L$, dann ist B eine maximale algebraisch unabhängige Teilmenge von M.

(iii) Es gibt eine Teilmenge M von L mit $H(M) = L$, sodass B eine maximale algebraisch unabhängige Teilmenge ist.

Beweis. (i) ⇒ (ii) Sei $\alpha \in M \backslash B$. Zu zeigen: $B \cup \{\alpha\}$ ist algebraisch abhängig. Dies folgt, da $\alpha \in L = H(B)$, d. h. α ist algebraisch über $K(B)$ (bzw. $H(B) = H(B \cup \{\alpha\})$).

(ii) ⇒ (iii) Setze $M := B$ (es gilt nämlich, $H(B) = L$, sonst könnte man B zu einer algebraisch unabhängigen Menge erweitern).

(iii) ⇒ (i) Zu zeigen: $H(B) = L$. Aus Lemma (9.7) folgt:

$$M \subset H(B) \Rightarrow L = H(M) \subset H(H(B)) = H(B) \Rightarrow L = H(B)$$

□

Satz 9.10
Es sei M eine Menge mit $L = H(M)$, es sei $C \subset M$ algebraisch unabhängig. Dann gibt es eine Transzendenzbasis B von L/K mit $C \subset B \subset M$.

Beweis. Wir müssen eine algebraisch unabhängige, maximale Teilmenge B von M finden mit $C \subset B$. Falls M endlich ist, können wir C, falls C nicht schon maximal ist, durch Hinzunahme eines Elements vergrößern, sodass $C \cup \{\alpha\}$ algebraisch unabhängig ist. Man findet dann nach endlich vielen Schritten ein geeignetes B. Im Allgemeinen: wende das Zornsche Lemma auf folgendes System von Mengen an:

$$\mathcal{M} := \{X;\ C \subset X \subset M,\ X \text{ ist algebraisch unabhängig}\}$$

□

Lemma 9.11
Es sei M eine Teilmenge von L mit $L = H(M)$. Es sei C algebraisch unabhängig. Dann gibt es eine Teilmenge $B' \subset M$ mit $B' \cap C = \emptyset$, sodass $B = C \cup B'$ eine Transzendenzbasis von ${}^{L}\!/_{K}$ ist.

Beweis. Nach obigem Satz gibt es eine Transzendenzbasis B mit $C \subset B \subset B \subset M \cup C$. Setze $B' := B \setminus C$. Dann ist $B \cap C = \emptyset$, damit $B' \subset M$ und $B' \cup C = B$ ist Transzendenzbasis. □

Satz 9.12
Ist $\{\alpha_1, \ldots, \alpha_n\}$ eine Transzendenzbasis von ${}^{L}\!/_{K}$, dann hat auch jede andere Transzendenzbasis die Länge n.

Beweis. $\{\beta_1, \ldots, \beta_m\}$ sei algebraisch unabhängig. Zu zeigen: $m \leq n$ (dies genügt). Denn: Wir zeigen folgende Behauptung:

Für jedes k mit $0 \leq k \leq n$ gibt es eine Teilmenge $B_k \subset B = \{\alpha_1, \ldots, \alpha_n\}$ mit:

(i) $B_0 \supsetneqq B_1 \supsetneqq \cdots \supsetneqq B_i \supsetneqq \cdots \supsetneqq B_k$

(ii) $\{\beta_1, \ldots, \beta_k\} \cup B_k$ ist Transzendenzbasis von ${}^{L}\!/_{K}$.

(iii) $\{\beta_1, \ldots, \beta_k\} \cap B_k = \emptyset$.

Dies genügt, da:

$$\text{(i)} \underset{B_k \subset B}{\Rightarrow} |B_k| \leq n - k.$$

Also ist $B_n = \emptyset$. Wegen (ii) ist $\{\beta_1, \ldots, \beta_n\}$ eine Transzendenzbasis von ${}^{L}\!/_{K} \Rightarrow m \leq n$.

Konstruktion der B_k: Sei $B_0 = B$. Die Konstruktion geschieht dann induktiv. Seien $B_0, \ldots, B_k$ Mengen, die (i) - (iii) erfüllen. Wir definieren dann B_{k+1} wie folgt: Nach Lemma (9.11) gibt es eine Teilmenge B_{k+1} von $\{\beta_1, \ldots, \beta_k\} \cup B_k$ mit

(iv) $\{\beta_1, \ldots, \beta_{k+1}\} \cup B_{k+1}$ ist Transzendenzbasis.

(v) $\{\beta_1, \ldots, \beta_{k+1}\} \cap B_{k+1} = \emptyset$

Nach Konstruktion ist $B_{k+1} \subset B_k$. Zu zeigen: $B_{k+1} \neq B_k$. Sei $B_{k+1} = B_k$, dann hätten wir:

(iv)' $\{\beta_1, \ldots, \beta_k\} \cup \{\beta_{k+1}\}$ ist Transzendenzbasis.

(ii)' β_{k+1} ist algebraisch über $\beta_1, \ldots, \beta_k\} \cup B_k$.

(ii)' und (iv)' stehen zueinander im Widerspruch. □

Definition 9.13
Ist ${}^{L}\!/_{K}$ eine Körpererweiterung, so ist der *Transzendenzgrad* von L über K wie folgt definiert:

$$\operatorname{trdeg} {}^{L}\!/_{K} = \begin{cases} \infty & \text{, falls es keine endliche Transzendenzbasis gibt} \\ n & \text{, falls es eine Transzendenzbasis der Länge } n \text{ gibt.} \end{cases}$$

Definition 9.14
${}^{L}\!/_{K}$ heißt *rein transzendent*, falls es eine Transzendenzbasis B gibt, mit $L = K(B)$.

Bemerkung 9.15
$\operatorname{trdeg} {}^{L}\!/_{K} = n$, ${}^{L}\!/_{K}$ rein transzendent. Dann ist

$$L = \underbrace{K(X_1, \ldots, X_n)}_{\substack{\text{Körper der rationalen} \\ \text{Funktionen in } n \text{ Variablen}}} = \operatorname{Quot}(K[X_1, \ldots, X_n])$$

Bemerkung 9.16
L/K allgemein:

$$K \underset{\text{rein transzendent}}{\subset} L' \underset{\text{algebraisch}}{\subset} L$$

(L' ist nicht eindeutig bestimmt)

Satz 9.17
Sei $K \subset F \subset L$. Dann gilt

$$\operatorname{trdeg} L/K = \operatorname{trdeg} F/K + \operatorname{trdeg} L/F$$

Beweis. B sei Transzendenzbasis von F/K, B' sei Transzendenzbasis von L/F. Behauptung: $B \cap B' = \emptyset$; $B \cup B'$ ist Transzendenzbasis von L/K.

(i) $B \cap B' = \emptyset$:

Sei $\alpha \in B \cap B' \Rightarrow \alpha \in B \subset F \Rightarrow \alpha$ ist algebraisch über $F \Rightarrow B'$ ist nicht algebraisch unabhängig über F. $\lightning$

(ii) $H(B \cup B') = L$:

$F/K(B)$ ist algebraisch $\Rightarrow$ $F \cdot K(B')/K(B) \cdot K(B')$ (Körperkompositum) ist algebraisch. $\Rightarrow L = H(B')$ ist algebraisch über $K(B) \cdot K(B') = K(B \cup B')$.

(iii) $B \cup B'$ ist algebraisch unabhängig:

Nach Lemma (9.11) gibt es B'' mit $B \cap B'' = \emptyset$, $B'' \subset B \cup B'$, sodass $B \cup B''$ eine Transzendenzbasis von L/K ist. Zu zeigen: $B'' = B'$.

(a) $B'' \subset B'$ ist klar.

(b) Sei $\alpha \in B' \backslash B''$, dann folgt, da $B \cup B'$ Transzendenzbasis ist, α ist algebraisch über $K(B \cup B'') = K(B)(B'') \subset F(B'') \Rightarrow B'$ ist algebraisch abhängig. $\lightning$ (da B' Transzendenzbasis von L/F).

□

Kapitel 10

Modultheorie

R: Ring, kommutativ mit 1
$(M,+)$: abelsche Gruppe

$$\begin{aligned} R \times M &\to M \\ (r,m) &\mapsto r \cdot m \end{aligned}$$

Definition 10.1
Ein *Modul (R-Modul)* ist ein Tripel $(R, M, +)$, sodass gilt:

(i) $r \cdot (m+n) = r \cdot m + r \cdot n$.

(ii) $(r+s) \cdot m = r \cdot m + s \cdot m$.

(iii) $1 \cdot m = m$.

Beispiel 10.2

(i) $R = K$ Körper: Vektorraum

(ii) $(G,+)$ eine abelsche Gruppe; $R = \mathbb{Z}$

$$n \cdot g = \underbrace{(g + \cdots + g)}_{\text{n-mal}}$$

(iii) $M = R[X_1, \ldots, X_n]$ ist ein R-Modul

(iv) R: Ring; $a \subset R$ Ideal in R. Da $R \cdot a \subset a$ ist, ist a in natürlicherweise ein R-Modul.

Definition 10.3
Es seien M, N Moduln. Ein *R-Modulhomomorphismus* ist eine Abbildung $f : M \to N$ mit

(i) $f(m+n) = f(m) + f(n)$

(ii) $f(r \cdot m) = r \cdot f(m) \qquad r \in R,\ m, n \in M$

Beispiel 10.4

(i) Vektorraumhomomorphismen

(ii) $f : G \to G'$ Gruppenhomomorphismus abelscher Gruppen. Dann ist f auch ein $\mathbb{Z}$-Modulhomomorphismus, da

$$f(ng) = f(\underbrace{g + \cdots + g}_{\text{n-mal}}) = \underbrace{f(g) + \cdots + f(g)}_{\text{n-mal}} = nf(g)$$

Bemerkung 10.5
$f : M \to N$, $g : N \to K$ seien R-Modulhomomorphismen. Dann ist $g \circ f : M \to K$ wieder ein R-Modulhomomorphismus.

Definition 10.6

$$\mathrm{Hom}_R(M, N) := \{f; f : M \to N \text{ ist eine } R\text{-Modulhomomorphismus}\}$$

Dies ist ein R-Modul bezüglich:

(i) $(f + g)(m) := f(m) + g(m)$

(ii) $(r \cdot f)(m) := r \cdot f(m)$

Dualer Modul:

$$M^* := \mathrm{Hom}_R(M, R)$$

Definition 10.7
$M' \subset M$ heißt ein *Untermodul*, falls

(i) $(M', +) \subset (M, +)$ ist Untergruppe.

(ii) $RM' \subset M'$.

10.1 Bild und Kern

$f : M \to N$ sei R-Modulhomomorphismus

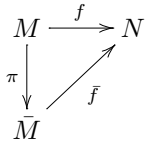
$$\begin{aligned} \mathrm{im}(f) &:= f(M) \subset N \\ \ker(f) &:= \{m \in M; f(m) = 0\} \subset M \end{aligned}$$

$\mathrm{im}(f) \subset M$, $\ker(f) \subset N$ sind Untermoduln von M und N.

Definition 10.8
Es sei $M' \subset M$ ein Untermodul. Ein *Quotient* von M nach M' ist ein Modul $\bar{M}$, sodass gilt:

(i) Es gibt einen Homomorphismus $\pi : M \to \bar{M}$ mit $\ker \pi = M'$.

(ii) Ist $f : M \to N$ ein Homomorphismus mit $h' \subset \ker f$, so gibt es genau einen Homomorphismus $\bar{f} : \bar{M} \to N$, sodass



kommutiert.

Satz 10.9
$\bar{M}$ existiert und ist bis auf Isomorphie eindeutig bestimmt.

Beweis. Sei $M' \subset M$ eine abelsche Untergruppe (also normal). $\bar{M} = {}^{M}\!/_{M'}$ (als abelsche Gruppe). Dies machen wir zu einem R-Modul durch

$$r \cdot \bar{m} := \overline{rm}$$

(Dies ist wohldefiniert, da $m' \in M' \Rightarrow rm' \in M' \Rightarrow \overline{rm'} = 0$) Rest wie mehrfach vorgeführt. □

Bezeichnung: $\bar{M} = {}^{M}\!/_{M'}$

Satz 10.10
Es sei $f : M \to N$ ein R-Modulhomomorphismus. Dann gibt es einen natürlichen Isomorphismus:

$$ {}^{M}\!/_{\ker f} \cong \mathrm{im}(f) $$

Beweis. Genau wie früher. □

$M_1, M_2 \subset M$ Untermoduln.

Definition 10.11
Die *Summe* von M_1, M_2 ist erklärt durch

$$ M_1 + M_2 := \{m;\ m = m_1 + m_2;\ m_1 \in M_1,\ m_2 \in M_2\} $$

Bemerkung 10.12
$M_1 + M_2$ ist der kleinste Untermodul von M, der M_1 und M_2 enthält.

Satz 10.13

(i) Es seien $N \subset M \subset L$ Untermoduln. Dann hat man einen natürlichen Isomorphismus

$$ \left({}^{L}\!/_{N}\right)\!/_{\left({}^{M}\!/_{N}\right)} \cong {}^{L}\!/_{M} $$

(ii) Sind $M_1, M_2 \subset M$ Untermoduln, so hat man einen natürlichen Isomorphismus

$$ {}^{(M_1+M_2)}\!/_{M_1} \cong {}^{M_2}\!/_{(M_1 \cap M_2)} $$

Beweis. (i) Wir betrachten die Abbildung

$$ \begin{array}{rccc} \varphi\colon & & \to & {}^{L}\!/_{M} \\ & x & \mapsto & \bar{x} = x + M \end{array} $$

Da $N \subset M$ ist, ist $N \subset \ker\varphi$. Also gibt es einen Homomorphismus

$$ \begin{array}{rccc} \bar{\varphi}\colon {}^{L}\!/_{N} & \to & {}^{L}\!/_{M} \\ x + N & \mapsto & x + M \end{array} $$

Es gilt:

$$ \ker\bar{\varphi} = {}^{M}\!/_{N} \overset{\text{Satz (10.13)}}{\Rightarrow} \underbrace{\left({}^{L}\!/_{N}\right)\!/_{\ker\bar{\varphi}}}_{=\left({}^{L}\!/_{N}\right)\!/_{\left({}^{M}\!/_{N}\right)}} \cong \mathrm{im}\,\bar{\varphi} = {}^{L}\!/_{M} $$

(ii) Betrachten die surjektive Abbildung: $\psi : M_2 \hookrightarrow M_1 + M_2 \to {}^{(M_1+M_2)}\!/_{M_1}$. Es gilt:

$$ \ker\psi = M_1 \cap M_2 \Rightarrow \underbrace{{}^{M_2}\!/_{\ker\psi}}_{{}^{M_2}\!/_{(M_1\cap M_2)}} \cong \mathrm{im}\,\psi = {}^{(M_1+M_2)}\!/_{M_1}. $$

□

10.2 Direkte Summe und Produkte

Definition 10.14
I: Indexmenge, $(M_i)_{i\in I}$: Familie von R-Moduln. Wir setzen:

- *Direkte Summe*:

$$\bigoplus_{i\in I} M_i := \left\{ x;\ x : I \to \bigcup_{i\in I} M_i,\ x(i) \in M_i;\ x(i) = 0 \text{ für fast alle } i \in I \right\}$$

- *Direktes Produkt*:

$$\prod_{i\in I} M_i := \left\{ x;\ x : I \to \bigcup_{i\in I} M_i,\ x(i) \in M_i \right\}$$

Bemerkung 10.15
Dies werden R-Moduln durch

$$\begin{aligned} (x+y)(i) &:= x(i) + y(i) \\ (r\cdot x)(i) &:= r \cdot x(i) \end{aligned}$$

Schreibweise:

$$\begin{aligned} x &= (x_i)_{i\in I} \\ (x+y)_i &= x_i + y_i \\ (rx)_i &= rx_i \end{aligned}$$

10.3 Erzeugendensysteme und Basen

Definition 10.16

(i) Eine Familie $(m_i)_{i\in I}$ von Elementen $m_i \in M$ heißt ein *Erzeugendensystem*, falls jedes Element $m \in M$ eine Darstellung

$$m = \sum_{\text{endlich}} r_i m_i;\ r_i \in R$$

besitzt.

(ii) M heißt *endlich erzeugt*, falls M ein endliches Erzeugendensystem besitzt.

Beispiel 10.17

(i) $M = R^n = R \oplus \cdots \oplus R$ ist endlich erzeugt.

$$e_i = (0, \ldots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0, \ldots 0)$$

$$r = (r_1, r_2, \ldots, r_n) = \sum_{i=1}^{n} r_i e_i$$

(ii) $M = R[X]$ ist nicht endlich erzeugt, da der Grad der Polynome nicht beschränkt ist.

(iii) $M := \mathbb{Q}$ als $\mathbb{Z}$-Modul. M ist nicht endlich erzeugt:

Annahme:

$$\mathbb{Q} = \mathbb{Z}\,\frac{a_1}{b_1} + \mathbb{Z}\,\frac{a_2}{b_2} + \cdots + \mathbb{Z}\,\frac{a_n}{b_n}; \quad \left(\frac{a_i}{b_i} \in \mathbb{Q}\right)$$

Jedes Element in M ist von der Form: $q = \frac{a}{b_1 \cdots b_n}$; $a \in \mathbb{Z}$. Sei p Primzahl mit $p > |b_1 \cdots b_n|$, dann ist $\frac{1}{p} \notin M$. $\lightning$

Satz 10.18

(i) M ist endlich erzeugt.

(ii) Es gibt $n \geq 1$ und einen surjektiven Homomorphismus $\varphi : R^n \to M$, d.h. M ist Quotient von R^n.

Beweis. (i) $\Rightarrow$ (ii) Es sei $m_1, \ldots, m_n$ ein Erzeugendensystem von M. Betrachte

$$\begin{aligned} \varphi\colon R^n &\to M \\ \varphi\left(\sum_{i=1}^{n} a_i e_i\right) &:= \sum_{i=1}^{n} a_i m_i \quad (\varphi(e_i) = m_i) \end{aligned}$$

Da $m_1, \ldots, m_n$ ein Erzeugendensystem ist, ist φ surjektiv.

(ii) $\Rightarrow$ (i) Es sei $\varphi\colon R^n \to M$ surjektiv. Sei $M_i := \varphi(e_i)$; $i = 1, \ldots, n$.

Behauptung: $M_1, \ldots, m_n$ ist ein Erzeugendensystem von M. Denn: $m \in M \overset{\varphi \text{ surjektiv}}{\Longrightarrow}$ Es gibt $x \in R^n$ mit $\varphi(x) = m$.

$$x = \sum_{i=1}^{n} x_i e_i; \ (x_i \in R) \Rightarrow m = f(x) = \sum_{i=1}^{n} x_i \varphi(e_i) = \sum_{i=1}^{n} x_i m_i.$$

□

Beispiel 10.19
$M = \mathbb{Z}_k = {}^{\mathbb{Z}}\!/_{k\,\mathbb{Z}}$ ($\mathbb{Z}$-Modul):

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to \mathbb{Z}_k \\ \varphi &\mapsto \bar{\varphi} \end{aligned}$$

$\bar{1} = \varphi(1)$ ist Erzeuger von $\mathbb{Z}_k$.

Definition 10.20
Eine Familie $(m_i)_{i \in I}$ von Elementen von M heißt *linear unabhängig (frei)*, wenn gilt

$$\sum_{\text{endlich}} r_i m_i = 0 \Rightarrow r_i = 0.$$

Definition 10.21
Eine *Basis* von M ist ein Erzeugendensystem $(m_i)_{i \in I}$, das frei ist.

Beispiel 10.22
$M = R^n$, $e_i = (0, \ldots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0, \ldots 0)$; $i = 1, \ldots, n$ ist eine Basis.

Bemerkung 10.23
Achtung: Nicht jeder Modul besitzt eine Basis.

Beispiel 10.24
$M := \mathbb{Z}_k = {}^{\mathbb{Z}}\!/_{k\,\mathbb{Z}} : \; k\bar{l} = \bar{0}$

Lemma 10.25
Es sind äquivalent

(i) $(m_i)_{i\in I}$ *ist eine Basis von* M*.*

(ii) Jedes Element $m \in M$ *besitzt eine eindeutige Darstellung*

$$m = \sum_{endlich} r_i m_i.$$

Beweis. Genau wie bei Vektorräumen. □

Definition 10.26
Ein Modul, der eine Basis besitzt, heißt ein *freier Modul*.

Definition 10.27
Es seien $M_i \subset M$, $i \in I$ Untermoduln von M. Man sagt, dass M die *direkte Summe* ($M = \bigoplus_{i\in I} M_i$) *der Untermoduln* von M ist, falls jedes Element $m \in M$ eine eindeutige Darstellung

$$m = \sum_{\text{endlich}} m_i$$

besitzt.

Satz 10.28
Es sind äquivalent:

(i) M *ist frei.*

(ii) Es gibt eine Familie $(m_i)_{i\in I}$, $m_i \in M$ *mit* $M = \bigoplus_{i\in I} Rm_i$.

Bemerkung 10.29
Dann gilt

$$M \cong \bigoplus_{i\in I} Rm_i = \bigoplus_{i\in I} R \quad (R \cong Rm;\; 1 \mapsto m_i)$$

Beweis. (i) ⇒ (ii) Ist $(m_i)_{i\in I}$ eine Basis, so hat jedes Element $m \in M$ eine eindeutige Darstellung

$$m = \sum_{\text{endlich}} r_i m_i. \text{ D.h. } M \cong \bigoplus_{i\in I} Rm_i.$$

(ii) ⇒ (i) $(m_i)_{i\in I}$ ist eine Basis.

□

Satz 10.30
Es sei M *ein freier* R*-Modul. Besitzt* M *eine Basis der Länge* n*, so hat jede andere Basis von* M *ebenfalls die Länge* n*.*

Definition 10.31
n heißt der *Rang* von M.

Beweis. Sei $m_1, \ldots, m_n$ eine Basis von M. $\Rightarrow M \cong R^n$. Sei $(e_i)_{i\in I}$ eine weitere Basis von M

$$\Rightarrow M \cong \bigoplus_{i\in I} R =: R^{|I|}.$$

$\Rightarrow$ Es gibt einen Isomorphismus $\varphi : R^n \to R^{|I|}$.

Behauptung: $n \geq |I|$, insbesondere ist $m = |I|$ endlich. (Dann analog: $m \geq n$.)
$m \subset R$ sei ein maximales Ideal: ${}^{R}\!/\!_{m} = K$ Körper. $\bar{\varphi} : R^n \to R^{|I|}$.

Da $\bar{\varphi}(mR^n) \subset mR^{|I|}$, induziert dies eine surjektive Abbildung

$$\tilde{\varphi}\colon \underset{\|}{({}^{R}\!/\!_{mR})^n} \to \underset{\|}{({}^{R}\!/\!_{mR})^{|I|}}$$
$$K^n \qquad\qquad K^{|I|}$$

($K = {}^{R}\!/\!_{M}$-Moduln $= K$-Vektorraum)
$\tilde{\varphi}$ ist ein K-Vektorraumhomomorphismus. $\Rightarrow |I| \leq n$. □

10.4 Noethersche Moduln

M: R-Modul

Definition 10.32
Ein R-Modul M heißt *noethersch*, wenn jeder Untermodul von M endlich erzeugt ist.

Satz 10.33
Ist R ein noetherscher Ring und M ein endlich erzeugter R-Modul, dann ist M ein noetherscher Modul.

Beweis. M endlich erzeugt:

$$M = Rm_1 + \cdots + Rm_k;\ m_i \in M,\ i = 1, \ldots, k$$

Wir haben also eine Surjektion:

$$\begin{aligned} \varphi\colon R^n &\to M \\ \varphi\left(\sum_{i=1}^{n} r_i e_i\right) &= \sum_{i=1}^{n} r_i m_i, \quad (e_i = (0, \ldots, 0, \underset{\uparrow}{1}, 0, \ldots 0)) \\ & \qquad\qquad\quad i \end{aligned}$$

Sei $U \subset M$ ein Untermodul. $\Rightarrow \varphi^{-1}(U) \subset R^n$ ist ebenfalls ein Untermodul. Ist $\varphi^{-1}(U)$ endlich erzeugt $\Rightarrow U$ ist endlich erzeugt. Es genügt also, die Aussage für R^n zu beweisen.

Induktion nach n:

$\underline{n = 1}$: $M = R$. Ein Untermodul $U \subset M$ ist dann ein Ideal in R. Da R ein noetherscher Ring ist, ist U endlich erzeugt.

$\underline{n - 1 \mapsto n}$: $U \subset M$ sei Untermodul. Sei

$$I := \{u^1 \in R;\ \text{ es gilt } u = (u^1, \ldots, u^n) \in U\} \subset R$$

(d. h. $I = \mathrm{Pr}_1(U)$, wobei Pr_1 die Projektion auf die erste Komponente ist.) I ist ein Ideal $\overset{R \text{ noethersch}}{\Rightarrow}$ $I = (u_1^1, \ldots, u_l^1)$. Wähle $u_1, \ldots, u_l \in U$, sodass die erste Komponente von u_i gleich u_1^1 ist. Sei $u \in U$. Dann gibt es $r_1, \ldots, r_l \in R$ mit

$$u - r_1 u_1 - \cdots - r_l u_l = (0, *, \ldots, *).$$

Wir identifizieren $R^{n-1} = \{0\} \times R^{n-1} \subset R^n$. Betrachte: $U' := U \cap R^{n-1} \subset R^{n-1}$ ist ein Untermodul. Aus der Induktionsvoraussetzung folgt: Es gibt $v_1, \ldots, v_k \in U'$, sodass diese Elemente U' erzeugen. $\Rightarrow$ $u_1, \ldots, u_l, v_1, \ldots, v_k$ ist ein Erzeugendensystem von U.

□

10.5 Nakayama Lemma

M: R-Modul, $a \subset M$ sei ein Ideal.

Definition 10.34

$$aM := \left\{ \sum_{\text{endlich}} a_i m_i;\ a_i \in a,\ m_i \in M \right\}$$

Satz 10.35
Es sei $\varphi : M \to M$ ein Homomorphismus mit $\varphi(M) \subset aM$. Dann gibt es $a_1, \ldots, a_n \in a$ mit

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0$$

Beweis. $x_1, \ldots, x_n$ seien Erzeugende von M. Da $\varphi(M) \subset aM$ ist, gibt es eine Relation

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_j;\ a_{ij} \in a.\ (i = 1, \ldots, n)$$

$$\Rightarrow \sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij}) x_i = 0 \tag{10.10.a}$$

Betrachte

$$B := (\delta_{ij}\varphi - a_{ij})_{i,j=1,\ldots,n}$$

Wir betrachten die adjungierte Matrix zu B: $B^\sharp = (b_{ij}^\sharp)$, wobei

$$b_{ij}^\sharp = \det \begin{pmatrix} b_{1,1} & \ldots & b_{1;i-1} & 0 & b_{1,i+1} & \ldots & b_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ b_{j-1,1} & \ldots & b_{j-1,i-1} & 0 & b_{j-1,i+1} & \ldots & b_{j-1,n} \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ b_{j+1,1} & \ldots & b_{j+1,i-1} & 0 & b_{j+1,i+1} & \ldots & b_{j+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ b_{n,1} & \ldots & b_{n,i-1} & 0 & b_{n,i+1} & \ldots & b_{n,n} \end{pmatrix}$$

Es gilt $B^\sharp B = \det B \cdot E_n$. Dies gilt auch in Ringen, also auch in unserer Situation. Setze:

$$\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$(10.10.\text{a}) \Rightarrow 0 = B^\sharp \underbrace{B\underline{x}}_{\overset{(10.10.\text{a})}{=}0} = \det B E_n \underline{x} \Rightarrow (\det B)(x_i) = 0;\ (i = 1, \ldots, n).$$

Entwickeln von B ergibt:

$$\det B = \varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n \text{ mit } a_1, \ldots, a_n \in a.$$

Da $\det Bx_i = 0;\ i = 1, \ldots, n$ und $x_1, \ldots, x_n$ ein Erzeugendensystem von M ist, folgt

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n \equiv 0.$$

□

Korollar 10.36
M sei ein endlich erzeugter Modul. Es sei $a \in R$ ein Ideal mit $aM = M$. Dann gibt es ein Element $x \in R$; $x \equiv 1 \mod a$ mit $xM = 0$.

Beweis. Wende Satz (10.35) auf $\varphi = \mathrm{id}_M$ an (geht, denn $\mathrm{id}_M = aM$).

$$\Rightarrow (1 + a_{n-1} + \cdots + a_0)\,\mathrm{id} \equiv 0 \quad (a_0, \ldots a_{n-1} \in a).$$

Setze $x := 1 + \underbrace{a_{n-1} + \cdots + a_0}_{\in a} \equiv 1 \mod n$.

$$\begin{aligned} (10.10.\text{a}) \quad &\Rightarrow \quad x \cdot m = 0 \text{ für alle } m \in M \\ &\Rightarrow \quad xM = 0. \end{aligned}$$

□

Definition 10.37
R sei ein Ring. Das *Jacobsonideal* von R ist definiert durch:

$$\mathcal{R} := \bigcap_{m \in R \text{ ist maximales Ideal}} m$$

Bemerkung 10.38
$\mathcal{R}$ ist ein Ideal in R.

Satz 10.39
$x \in \mathcal{R} \Leftrightarrow 1 - xy \in R^*$ für alle $y \in R$.

Beweis. „$\Rightarrow$“ Sei $1 - xy \notin R^*$. Dann gibt es ein maximales Ideal m mit $1 - xy \in m$. Da $x \in \mathcal{R}$, ist auch $x \in m$, d. h. aber $1 \in m$. ↯

„$\Leftarrow$“ Sei $x \notin \mathcal{R}$. Dann gibt es ein maximales Ideal m mit $x \notin m$. $\Rightarrow (m, x) = \mathcal{R}$. $\Rightarrow$ Es gibt $n \in m, y \in \mathcal{R}$ mit: $n + xy = 1$. $\Rightarrow 1 - xy = n \in m \Rightarrow 1 - xy \notin R^*$.

□

Satz 10.40 (Nakayama-Lemma, 1.Form)
M sei endlich erzeugter R-Modul; $a \subset \mathcal{R}$ sei ein Ideal. Dann gilt

$$aM = M \Rightarrow M = 0.$$

Beweis. Nach Korollar (10.36) gibt es $x \equiv 1 \mod a$ mit $xM = 0$. Da $a \subset \mathcal{R}$, gilt auch $x \equiv 1 \mod \mathcal{R}$, d.h.

$$x = 1 - y;\ y \in \mathcal{R} \Rightarrow x = 1 - y \in R^* \overset{\text{Satz (10.39)}}{\Rightarrow} M = 1 \cdot M = x^{-1} \underbrace{xM}_{=0} = 0.$$

□

Korollar 10.41
M sei endlich erzeugter R-Modul; $a \subset \mathcal{R}$ ein Ideal, $N \subset M$ ein Untermodul. dann gilt:

$$M = aM + N \Rightarrow M = N$$

Beweis. Wir betrachten den R-Modul ${}^{M}\!/_{N}$. Dann gilt

$$a \cdot {}^{M}\!/_{N} = {}^{(aM+N)}\!/_{N} = {}^{M}\!/_{N} \overset{\text{Satz (10.40)}}{\Longrightarrow} {}^{M}\!/_{N} = 0 \Rightarrow M = N.$$

□

Definition 10.42
Ein *lokaler Ring* R ist ein Ring, der genau ein maximales Ideal m besitzt.

Bemerkung 10.43
Dann gilt: $\mathcal{R} = m$.

Bemerkung 10.44
${}^{M}\!/_{mM}$ ist dann ein ${}^{\mathcal{R}}\!/_{m}$-Modul durch $\bar{r} \cdot \bar{x} = \overline{rx}$.

—

Sei $K := {}^{\mathcal{R}}\!/_{m} =$ Körper. D.h. ${}^{M}\!/_{mM}$ ist ein K-Vektorraum.

Satz 10.45 (Nakayama-Lemma, 2. Form)
Es sei R ein lokaler Ring mit maximalem Ideal m. M sei endlich erzeugt. Es seien $x_1, \ldots, x_n \in M$, sodass $\bar{x_1}, \ldots, \bar{x_n} \in {}^{M}\!/_{mM}$ sind. Dann sind $x_1, \ldots, x_n$ Erzeugende des Moduls M.

Beweis. Sei

$$N := Mx_1 + \cdots + Mx_n \subset M.$$

Betrachten: $\varphi\colon N \hookrightarrow M \to {}^{M}\!/_{mM}$. Nach Voraussetzung ist φ surjektiv.

$$N + mM = M \underset{m=\mathcal{R}}{\overset{\text{Kor. (10.41)}}{\Rightarrow}} M = N \Rightarrow x_1, \ldots, x_n \text{ erzeugen } M.$$

□

Anhang A

Die Transzendenz von π und e

A.1 Hauptergebnis

Theorem A.1
Es seien $\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}} \setminus \{0\}$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Es sei L die normale Hülle von $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Zu jedem Automorphismus $\sigma \in G(L/\mathbb{Q})$ gebe es eine Permutation $\pi \in S_n$ mit $\sigma(\alpha_i) = \alpha_{\pi(i)}$ und $a_{\pi(i)} = a_i$ für $i = 1, \ldots, n$.

Dann gilt:

$$a_1 e^{\alpha_1} + \cdots + a_n e^{\alpha_n} \notin \mathbb{Z} \setminus \{0\}$$

Anwendung: Unmöglichkeit der Kreisquadratur.

Korollar A.2 (Carl-Louis Ferdinand von Lindemann (1882))
Die Zahl π ist transzendent.

Beweis. Annahme π ist algebraisch. Dann ist auch $\beta := i\pi$ algebraisch. Es seien $\beta_1, \ldots, \beta_m$ die konjugierten von $i\pi$.

OBdA gelte $\beta_1 = \beta$. Dann ist

$$\prod_{j=1}^{m} (1 + e^{\beta_j}) = 0.$$

Ausmultiplizieren:

$$1 + \sum_{j=1}^{m} e^{\beta_j} + \sum_{1 \le j < k \le m} e^{\beta_j + \beta_k} + \cdots + e^{\beta_1 + \cdots + \beta_m} = 0.$$

Es seien $\alpha_1, \ldots, \alpha_n$ diejenigen der Exponenten $\beta_j, \beta_j + \beta_k, \ldots, \beta_1 + \cdots + \beta_m$, die $\neq 0$ sind.

Dann:

$$1 + N + e^{\alpha_1} + \cdots + e^{\alpha_n} = 0,$$

wobei N die Anzahl der Exponenten $\beta_j, \ldots, \beta_1 + \cdots + \beta_m$ ist, die $= 0$ sind.

Insbesondere ist

$$e^{\alpha_1} + \cdots + e^{\alpha_n} = \underbrace{-N - 1}_{\le -1} \in \mathbb{Z} \setminus \{0\}.$$

Die Menge $\{\alpha_1, \ldots, \alpha_n\}$ ist galois invariant. Damit können wir das Theorem anwenden (mit $a_1 = \cdots = a_n = 1$). $\Rightarrow$ Widerspruch $\lightning$. $\square$

Korollar A.3
Die Zahl e ist transzendent.

Beweis. Annahme: e algebraisch.
Dann gibt es $a_0, \ldots, a_n \in \mathbb{Z},\ a_0 \neq 0$ mit

$$a_0 + a_1 e + \cdots + a_n e^n = 0.$$

Widerspruch zum Theorem (mit $\alpha_i = i$ $(i = 1, \ldots, n)$). Die Bedingung des Theorems ist trivialerweise erfüllt, da $G(L/\mathbb{Q}) = G(\mathbb{Q}/\mathbb{Q}) = \{\mathrm{id}\}$. $\square$

A.2 Beweis des Theorems

Behauptung 1: Für alle $x \in \mathbb{C}$ unf $j = 0, 1, 2, \ldots$ gilt:

$$j! e^x = (j! + j!x + \frac{j!}{2!}x^2 + \cdots + x^j) + x^{j+1} q_j(x) e^{|x|}$$

mit $|q_j(x)| < 1$.

Beweis. Es gilt

$$\begin{aligned} j! e^x &= j!(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^j}{j!} + \frac{x^{j+1}}{(j+1)!} + \cdots) \\ &= (j! + j!x + \frac{j!}{2!}x^2 + \cdots + \frac{j!}{j!}x^j) + x^{j+1} \underbrace{(\frac{1}{j+1} + \frac{x}{(j+1)(j+2)} + \cdots)}_{=:\delta_j(x)} \end{aligned}$$

wobei

$$|\delta_j(x)| \leq 1 + \frac{|x|}{2!} + \frac{|x|^2}{3!} + \cdots < e^{|x|} \qquad \text{für } x \neq 0$$

Mit $q_j(x) := \delta_j(x) e^{-|x|}$ folgt die Behauptung. $(q_j(0) = 0)$ $\square$

Wir nehmen nun an, dass

$$\boxed{a_1 e^{\alpha_1} + \cdots + a_n e^{\alpha_n} = a \in \mathbb{Z} \setminus \{0\}}$$

Wir werden später sehen, dass diese Annahme zu einem Widerspruch führt. Damit ist dann das Theorem bewiesen.

Behauptung 2: Es gibt ein Polynom $g(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ vom Grad $\leq n$ mit $b_0 \neq 0$ und $g(\alpha_1) = \cdots = g(\alpha_n) = 0$.

Beweis. OBdA: $\alpha_1, \ldots, \alpha_n$ paarweise verschieden. (Wenn nicht, finden wir sogar ein Polynom vom Grad $< n$). Nach Voraussetzung des Theorems kommen mit jedem α_i auch alle Konjugierten von α_i in $\{\alpha_1, \ldots, \alpha_n\}$ vor.

Es seien $g_1(X), \ldots, g_k(X)$ die *verschiedenen* Minimalpolynome von $\alpha_1, \ldots, \alpha_n$ $(k \leq n)$. Dann hat $\tilde{g}(X) := g_1(X) \cdot \ldots \cdot g_k(X) \in \mathbb{Q}[X]$ Grad n und $\tilde{g}(\alpha_1) = \cdots = \tilde{g}(\alpha_n) = 0$. Wegmultiplizieren der Nenner liefert $\hat{g}(X) \in \mathbb{Z}[X]$ vom Grad n und $\hat{g}(\alpha_1) = \cdots = \hat{g}(\alpha_n) = 0$. Schreibe schließlich $\hat{g}(X) = X^l \cdot g(X)$ mit $g(0) \neq 0$. Dann erfüllt das Polynom g alle Bedingungen der Behauptung. $\square$

Bemerkung A.4
Hier benutzen wir die Bedingung $\alpha_i \neq 0$! Wir wählen nun eine Primzahl p. p beliebig aber fest. Später $p \to \infty$. Man beachte also was im Folgenden von p abhängt und was unabhängig von p ist.

Definition A.5

$$(p-1)! \cdot f(X) := 1^{p-1} \cdot g(X)^p = X^{p-1}(\sum_{i=0}^{n} b_i X^i)^p$$
$$=: \sum_{j=0}^{m} c_j X^j \in \mathbb{Z}[X]$$

wobei $m = np + p - 1$.

Das Polynom f und die Koeffizienten c_j hängen von p ab. Es gilt:

$$c_0 = \cdots = c_{p-1} = 0 \quad \text{und} \quad c_{p-1} = b_0^p \neq 0$$

Definition A.6

$$F(X) := f(X) + f'(X) + \cdots + f^{(m)}(X) \in \frac{1}{(p-1)!}\mathbb{Z}[X].$$

Es gilt:

$$(p-1)!F(X) = \sum_{j=0}^{m} c_j X^j + \sum_{j=1}^{m} j \cdot c_j \cdot X^{j-1} + \cdots + m! c_m$$
$$= \sum_{0 \leq l \leq j \leq m} \frac{j!}{(j-l)!} c_j X^{j-l} \overset{k:=j-l}{=} \sum_{0 \leq k \leq j \leq m} \frac{j!}{k!} c_j X^k$$

Insbesondere:

$$(p-1)!F(0) = \sum_{j=0}^{m} j! c_j = \sum_{j=p-1}^{m} j! c_j$$

also

$$f(0) = \sum_{j=p-1}^{m} \frac{j!}{(p-1)!} c_j = c_p + \sum_{j=p}^{m} \frac{p}{p} \cdot \frac{j!}{(p-1)!} c_j$$
$$= b_0^p + p \underbrace{\sum_{j=p}^{m} \frac{j!}{p!} c_j}_{\in \mathbb{Z}},$$

d.h. $F(0) \in \mathbb{Z}$ und $F(0) \equiv b_0^p \mod p$.

Nach Behauptung (1) gilt:

$$\begin{array}{rrcl}
(j=0) & c_0 e^x & = & (1 + q_0(x) e^{|x|} x) c_0 \\
(j=1) & c_1 e^x & = & (1 + x + q_1(x) x^2 e^{|x|}) c_1 \\
(j=2) & c_2 2! e^x & = & ((2! + 2! x + x^2) + q_2(x) x^3 e^{|x|}) c_2 \\
\vdots & & \vdots & \\
(j=m) & c_m m! e^x & = & ((m! + m! x + \cdots + x^m) + q_m(x) x^{m+1} e^{|x|}) c_m
\end{array}$$

mit $|q_j(x)| < 1$

Addieren:

$$e^x(p-1)!F(0) = \sum_{j=0}^{m} j!c_j e^x = \sum_{j=0}^{m}\sum_{k=0}^{j} c_j \frac{j!}{k!}x^k + e^{|x|}\cdot \underbrace{\sum_{j=0}^{m} c_j q_j(x)x^{j+1}}_{=:(p-1)!Q(x)}$$

$$= \sum_{0\le k\le j\le m} c_j \frac{j!}{k!}x^k + e^{|x|}\cdot(p-1)!Q(x) = (p-1)!\big[F(x)+e^{|x|}Q(x)\big]$$

also insbesondere

$$F(0)e^{\alpha_i} = F(\alpha_i) + e^{|\alpha_i|}\cdot Q(\alpha_i)$$

Multiplizieren mit a_i und Aufaddieren liefert

$$F(0)\cdot\sum_{i=1}^{n} a_i e^{\alpha_i} = \underbrace{\sum_{i=1}^{n} a_i F(\alpha_i)}_{=a} + \sum_{i=1}^{n} a_i e^{|\alpha_i|}Q(\alpha_i)$$

Also:

$$aF(0) - \sum_{i=1}^{n} a_i F(\alpha_i) = \sum_{i=1}^{n} a_i e^{|\alpha_i|}Q(\alpha_i)$$

Behauptung 3: Es gibt ein Polynom $h(X)\in\mathbb{Z}[X]$ vom Grad $< n\cdot p$ mit $F(\alpha_i) = p\cdot h(\alpha_i)$.

Beweis. Aus $(p-1)!f(X) = \sum_{j=0}^{m} c_j X^j \in \mathbb{Z}[X]$ folgt

$$(p-1)!f^{(k)}(X) = \sum_{j=k}^{m} \frac{j!}{(j-k)!}c_j X^{j-k}$$

Für $k\ge p$ gilt

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

Also

$$(p-1)!f^{(k)}(X) =: p!h_k(X) \qquad \text{mit } h_k(X)\in\mathbb{Z}[X].$$

Das Polynom $h_k(X)$ hat den Grad $\le m-k\le m-p = np-1$ für $k\ge p$.

Man beachte, dass $f(\alpha_i) = \cdots = f^{(p-1)}(\alpha_i) = 0$, weil $(p-1)!f(X) = X^{p-1}g(X)^p$ mindestens p–fach in α_i verschwindet.

Also

$$F(\alpha_i) = f^{(p)}(\alpha_i) + \cdots + f^{(m)}(\alpha_i)$$
$$= p\cdot\underbrace{(h_p(\alpha_i) + \cdots + h_m(\alpha_i))}_{=:h(\alpha_i)}$$

□

Behauptung 4: Es gibt eine *von p unabhängige* nichtnegative ganze Zahl b mit

$$b^p \cdot \sum_{i=1}^{n} a_i h(\alpha_i) \in \mathbb{Z} \qquad \text{für alle } p.$$

Zum Beweis benötigen wir den folgenden Begriff:

Definition A.7
Eine komplexe Zahl α heißt *ganzalgebraisch*, falls es ein *normales* Polynom $A(X) \in \mathbb{Z}[X]$ mit $A(\alpha) = 0$ gibt.
(ganzalgebraisch $\overset{\Rightarrow}{\not\Leftarrow}$ algebraisch).

Beispiel A.8

(i) ganzalgebraisch: $\sqrt[5]{3}, \frac{1}{2} + \frac{1}{2}\sqrt{5}, e^{2\pi i/7}, \ldots$

(ii) nicht ganzalgebraisch: $\frac{1}{2}, \frac{1}{2}\sqrt{3}, \frac{1}{2}\sqrt{5}, \ldots$

Lemma A.9
Zu jeder algebraischen Zahl α gibt es eine positive ganze Zahl m mit $m \cdot \alpha$ ganzalgebraisch.

Beweis. Sei $n := [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Sei

$$g(X) := X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}[X]$$

das Minimalpolynom von α.

Die $a_i \in \mathbb{Q}$ sind von der Form $\frac{s_i}{t_i}$, $s_i, t_i \in \mathbb{Z}$. OBdA gelte $\mathrm{ggT}(s_i,\ t_i)$=1. Definiere m als

$$m := \mathrm{kgV}(t_0, \ldots, t_{n-1}).$$

ObdA sei $m \in \mathbb{Z}_{>0}$ (sonst mit -1 multiplizieren). Sei $k := m^n \in \mathbb{Z}_{>0}$. Dann gilt:

$$\begin{aligned} 0 = g(\alpha) = k \cdot g(\alpha) &= k \cdot (\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) \\ &= (\alpha m)^n + \underbrace{a_{n-1}m}_{\in\mathbb{Z}}(\alpha m)^{n-1} + \underbrace{a_{n-2}m^2}_{\in\mathbb{Z}}(\alpha m)^{n-2} + \cdots + \underbrace{m^n a_0}_{\in\mathbb{Z}} \end{aligned}$$

da $t_i | m$ $(\Rightarrow t_i | m^j)$, $i = 0, \ldots, n-1$.

Definiere $c_i := a_i \cdot m^{n-i} \in \mathbb{Z}$. Dann ist $h(X) := X^n c_{n-1}X^{n-1} + \cdots + c_0 \in \mathbb{Z}[X]$ ein Polynom mit $g(m \cdot \alpha) = 0$, d.h. $m \in \mathbb{Z}_{>0}$ ist eine Zahl für die gilt, $m \cdot \alpha$ ist ganzalgebraisch. □

Lemma A.10
Ist $\alpha \in \mathbb{Q}$ ganzalgebraisch, so ist $\alpha \in \mathbb{Z}$.

Beweis. Schreibe $\alpha = \frac{r}{s}$ gekürzt, d.h. $r, s \in \mathbb{Z}$, $s > 0$, $\mathrm{ggT}(r,\ s) = 1$.

Annahme: α ganzalgebraisch, aber $\alpha \notin \mathbb{Z}$.

Dann $s > 1$ und $\frac{r^n}{s^n} + t_{n-1}\frac{r^{n-1}}{s^{n-1}} + \cdots + t_0 = 0$ mit $t_i \in \mathbb{Z}$

$$\Rightarrow r^n = -s(t_{n-1}r^{n-1} + \cdots + t_0 s^{n-1}) \Rightarrow s | r^n \Rightarrow \mathrm{ggT}(r,\ s) \geq s > 1 \quad \lightning$$

□

Satz A.11
Die ganzalgebraischen Zahlen bilden einen Unterring O (oder $\bar{\mathbb{Z}}$) von $\bar{\mathbb{Q}}$.

Beweis. Erfolgt in Abschnitt (A.3). □

Beweis. (von Behauptung (4))

$$h(X) =: \sum_{j=0}^{np-1} n_j X^j \qquad \text{mit } n_j \in \mathbb{Z}\,.$$

Wähle $\tilde{b} \in \mathbb{Z}_{>0}$, so dass $\tilde{b}\alpha_1, \ldots, \tilde{b}\alpha_n$ *ganzalgebraisch* sind.

Definiere:

$$b := \tilde{b}^n.$$

b hängt nicht von p ab!

Es gilt

$$b^p h(\alpha_i) = \tilde{b}^{np} \sum_{j=0}^{np-1} n_j \cdot \alpha_i^j = \sum_{j=0}^{np-1} \underbrace{(\tilde{b}^{np-j} n_j)}_{in\,\mathbb{Z}} (\underbrace{\tilde{b}}_{\in O} \alpha_i)^j \overset{O \text{ Ring}}{\in} O.$$

Damit gilt auch

$$b^p \underbrace{\sum_{i=1}^{n} a_i h(\alpha_i)}_{=:y} = \sum_{i=1}^{n} a_i \cdot b^p h(\alpha_i) \in O.$$

Wegen $O \cap \mathbb{Q} = \mathbb{Z}$ reicht es zu zeigen, dass $y \in \mathbb{Q}$. Nach dem Hauptsatz der Galoistheorie (6.82) reicht es zu zeigen, dass y $G(L/\,\mathbb{Q})$–invariant ist ($L/\,\mathbb{Q}$ ist galoisch!).

Sei also $\sigma \in G(L/\,\mathbb{Q})$. Zu zeigen: $\sigma(y) = y$.

Nach Voraussetzung des Theorems gibt es eine Permutation $\pi \in S_n$. Daraus folgt die gewünschte Invarianz von y:

$$\begin{aligned}\sigma(y) &= \sum_{i=1}^{n} a_i h(\sigma(\alpha_i)) = \sum a_i h(\alpha_{\pi(i)}) = \sum_{i=1}^{n} a_{\pi(i)} h(\alpha_{\pi(i)}) \\ &\overset{j=\pi(i)}{=} \sum_{j=1}^{n} a_j h(\alpha_j) = y\end{aligned}$$

□

Betrachte die Zahl

$$\begin{aligned}C &:= b^p \cdot \sum_{i=1}^{n} a_i Q(\alpha_i) e^{|\alpha_i|} = b^p [aF(0) - \sum_{i=1}^{n} a_i F(\alpha_i)] \\ &\overset{\text{Beh. } 3}{=} ab^p \underbrace{F(0)}_{\in\mathbb{Z}} - p \underbrace{b^p \sum_{i=1}^{n} a_i h(\alpha_i)}_{\in\mathbb{Z} \text{ Beh. } 4}\end{aligned}$$

$\Rightarrow C \in \mathbb{Z}$ und $C \equiv ab^p b_0^p \mod p$.

Wähle p so groß, dass $p \nmid a \cdot b \cdot b_0$. Solche p gibt es, weil

(i) $a \cdot b \cdot b_0 \neq 0$

(ii) $a \cdot b \cdot b_0$ hängt nicht von p ab!

$$\left.\begin{array}{rl} p \nmid abb_0,\ p \text{ prim} \quad \Rightarrow & p \nmid ab^p b_0^p \\ & C \equiv ab^p b_0^p \mod p \end{array}\right\} \Rightarrow C \not\equiv 0 \mod p$$
$$\Rightarrow C \neq 0$$

Also $C \in \mathbb{Z} \setminus \{0\}$ und damit $|C| < 1$.

Behauptung 5: Für $p \gg 0$ gilt $|C| < 1$.

Behauptung 5 liefert den gesuchten Widerspruch.

Beweis. Es gilt: $b^{-p} \cdot C = \sum_{i=1}^{n} a_i Q(\alpha_i) e^{|\alpha_i|}$.

Wegen $|q_j(x)| < 1$ gilt außerdem:

$$\begin{aligned}\forall x \in \mathbb{C}\colon (p-1)!Q(x) &= |\sum_{j=p-1}^{m} c_j q_j(x) X^{j+1}| \\ &\leq \sum_{j=p-1}^{m} |c_j||q_j(x)||X|^{j+1} \\ &< \sum_{j=p-1}^{m} |c_j||X|^{j+1} = |X| \sum_{j=p-1}^{m} |c_j||X|^{j} \\ &\overset{\text{Lemma (A.12)}}{\leq} |X|^p \big(\sum_{i=0}^{n} |b_i||X|^i\big)^p\end{aligned}$$

Also gilt für $j = 1, \ldots, n$:

$$(p-1)!|b^p Q(\alpha_j)| < \underbrace{\big(|b\alpha_j| \cdot \sum_{i=0}^{n} |b_j||\alpha_j|^i\big)^p}_{=:M_j} = M_j^p$$

M_j hängt nicht von p ab! Mit $M := \max\{M_1, \ldots, M_n\}$ gilt für $j = 1, \ldots, n$

$$|a_j b^p Q(\alpha_j) e^{|\alpha_j|}| < \frac{|a_j| M^p e^{|\alpha_j|}}{(p-1)!} \overset{p>>0}{\leq} \frac{1}{2n}$$

und daher

$$|C| \leq \sum_{j=1}^{n} |a_j b^p Q(\alpha_j) e^{|\alpha_j|}| < \frac{1}{2}.$$

□

Lemma A.12
Es gelte $X^{p-1}(\sum_{j=0}^{n} b_i X^i)^p = \sum_{j=p-1}^{m} c_j X^j$ *in* $\mathbb{Z}[X]$. *Dann gilt*

$$|\sum_{j=p-1}^{m} |c_j||\alpha|^j| \leq |\alpha|^{p-1} \big(\sum_{j=0}^{n} |b_i||\alpha|^i\big)^p \quad \forall \alpha \in \mathbb{C}\,.$$

Beweis. Es gilt

$$\begin{aligned}\sum c_j X^j &= X^{p-1} \big(\sum i = 0^n b_i X^i\big)^p \\ &= X^{p-1} \cdot \sum_{\substack{q_0+\cdots+q_n=p \\ q_0,\ldots,q_n \geq 0}} \frac{p!}{q_0! \cdots q_n!} b_0^{q_0} (b_i X)^{q_1} \cdots (b_n X^n)^{q_n} \\ &= X^{p-1} \cdot \sum_{\substack{q_0+\cdots+q_n=p \\ q_0,\ldots,q_n \geq 0}} \frac{p!}{q_0! \cdots q_n!} b_0^{q_0} - b_n^{q_n} X^{q_1+2q_2+\cdots+nq_n}\end{aligned}$$

Koeffizientenvergleich:

$$c_j = \sum_{\substack{q_0+\cdots+q_n=p \\ q_0,\ldots,q_n\geq 0 \\ q_1+2q_2+\cdots+nq_n=j-p+1}} \frac{p!}{q_0!\cdots q_n!} b_0^{q_0}\cdots b_n^{q_n}$$

es folgt

$$|c_j| \leq \underbrace{\sum_{\substack{q_0+\cdots+q_n=p \\ q_0,\ldots,q_n\geq 0 \\ q_1+2q_2+\cdots+nq_n=j-p+1}} \frac{p!}{q_0!\cdots q_n!} |b_0|^{q_0}\cdots|b_n|^{q_n}}_{\gamma_j}.$$

Es gilt

$$\sum \gamma_j X^j = X^{p-1}\Big(\sum_{i=0}^{n} |b_i| X^i\Big)^p \qquad \text{in } \mathbb{Z}[X].$$

Substituiere $x = |\alpha|$:

$$\sum \gamma_j |\alpha|^j = |\alpha|^{p-1}\Big(\sum_{i=0}^{n} |b_i||\alpha|^i\Big)^p \underset{\substack{\uparrow \\ |c_j|\leq\gamma_j}}{\geq} \sum |c_j||\alpha|^j$$

□

A.3 Ganzalgebraische Zahlen

Beweis. (von Satz (A.11))

Seien $\alpha_1, \alpha_2 \in O$. Zu zeigen $\alpha_1 \cdot \alpha_2$ und $\alpha_1 + \alpha_2 \in O$. Betrachte dazu den durch α_1 und α_2 erzeugten Unterring $\mathbb{Z}[\alpha_1, \alpha_2]$ von $\bar{\mathbb{Q}}$.

Nach Voraussetzung gibt es Relationen

$$\alpha_1^n = a_{n-1}\alpha^{n-1} + \cdots + a_0$$
$$\alpha_2^m = b_{m-1}\alpha^{m-1} + \cdots + b_0$$

mit $a_0, \ldots, a_{n-1}, b_0 \ldots, b_{m-1} \in \mathbb{Z}$.

Daraus folgt

$$\mathbb{Z}[\alpha_1, \alpha_2] = \{\sum_{i=0}^{n-1}\sum_{j=0}^{m-1} d_{ij}\alpha_1^i\alpha_2^j; d_{ij} \in \mathbb{Z}\}.$$

Wir schreiben nun $\beta_1 \ldots, \beta_N$ für die Elemente des Erzeugendensystems $\{\alpha_1^i\alpha_2^j \mid 0 \leq i \leq n, 0 \leq j \leq n\}$ (also $N = nm$).

OBdA $\beta_1 = \alpha_1^0\alpha_2^0 = 1$. Es sei α irgendein Element von $\mathbb{Z}[\alpha_1, \alpha_2]$.

Behauptung: α ist ganzalgebraisch. (Trifft insbesondere auf $\alpha_1 \cdot \alpha_2$ und $\alpha_1 + \alpha_2$ zu).

Es gilt $\alpha\beta_1, \ldots, \alpha\beta_N \in \mathbb{Z}[\alpha_1, \alpha_2]$ (Ring!)

$$\Rightarrow \exists a_{ij} \in \mathbb{Z}\colon\ \alpha_{\beta_j} = \sum_{k=1}^{N} a_{jk}\beta_k \qquad (j = 1, \ldots, N).$$

Es sei $C \in \mathbb{C}^{N\times N}$ die Matrix

$$C := (c_{jk}) := (\delta_{jk}\alpha - a_{jk}).$$

Dann gilt

$$\sum_{k=1}^{N} c_{jk}\beta_k = 0 \qquad (j = 1, \ldots, N)$$

Es sei $\tilde{C} = (\tilde{c}_{jk})$ die zu C komplementäre Matrix, d.h.

$$\tilde{c}_{jk} = \det \bar{C} \cdot (-1)^{j+k}$$

mit

$$\bar{C} := \begin{array}{c} \text{k–te Spalte} \\ \downarrow \\ \begin{pmatrix} c_{11} & \ldots & c_{1_k} & \ldots & c_{1n} \\ \vdots & & \vdots & & \vdots \\ c_{j1} & \ldots & c_{jk} & \ldots & c_{jn} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \ldots & c_{nk} & \ldots & c_{nn} \end{pmatrix} \end{array} \leftarrow j\text{–te Zeile}$$

Cramer:

$$\tilde{C} \cdot C = \det(C) \cdot E_n$$

Es folgt:

$$\begin{aligned} \det(C) &= \det(C) \cdot 1 = \det(C) \cdot \beta_1 \\ &= \sum_{k=1}^{N} \det(C)\delta_{ik}\beta_k \\ &\overset{\text{Cramer}}{=} \sum_{k+1}^{N}\sum_{j=1}^{N} \tilde{c}_{1j}c_{jk}\beta_k = \sum_{j=1}^{N} \tilde{c}_{1j} \underbrace{\sum_{k=1}^{N} c_{jk}\beta_k}_{=0\ \forall j} = 0. \end{aligned}$$

Betrachte nun das charakteristische Polynom der Matrix $(a_{ij}) \in \mathbb{Z}^{N\times N}$

$$f(X) = \det\big((X \cdot \delta_{jk} - a_{ik})\big) \in \mathbb{Z}[X].$$

f ist normiert.

Es gilt

$$f(\alpha) = \det\big(\alpha \cdot \delta_{jk} - a_{jk})\big) = \det(C) = 0.$$

Damit ist α ganzalgebraisch. □

A.4 Der Fundamentalsatz der Algebra

Theorem A.13
$\mathbb{C}$ *ist algebraisch abgeschlossen.*

$$\mathbb{R}(i) = \mathbb{C} \xleftarrow{\text{algebraischer Schritt}} \mathbb{R} \xleftarrow{\text{analytischer Schritt}} \mathbb{Q}$$

Aus der Vollständigkeit von $\mathbb{R}$ folgt:

(i) Ein Polynom $f(X) \in \mathbb{R}[X]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.

(ii) Das Bild von $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist $\{x \in \mathbb{R}; x \geq 0\}$

Eigenschaftt (ii) impliziert:

Lemma A.14
Es gibt keine Erweiterung $L \supset \mathbb{C}$ mit $[L : \mathbb{C}] = 2$.

Beweis. Betrachte eine quadratische Gleichung

$$x^2 + a_1 x + a_2 = 0$$

mit $a_1, a_2 \in \mathbb{C}$. Zu zeigen Nullstelle in $\mathbb{C}$. Nullstellen sind

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}$$

(in einem algebraischen Abschluss von $\mathbb{C}$).

Behauptung: Die Nullstellen liegen bereits in $\mathbb{C}$.
Es reicht zu zeigen, dass $\sqrt{a_1^2 - 4a_2} \in \mathbb{C}$. Schreibe dazu

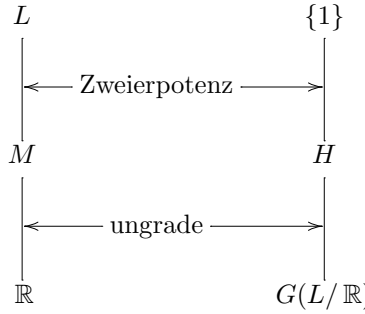
$$a_1^2 - 4a_2 = c + di \qquad c, d \in \mathbb{R}\,.$$

Dann gilt

$$\sqrt{a_1^2 - 4a_2} = \underbrace{\sqrt{\frac{c + \sqrt{c^2 + d^2}}{2}}}_{\in\mathbb{R}\,(\text{Eigensch. (ii)})} \pm i \underbrace{\sqrt{\frac{-c + \sqrt{c^2 + d^2}}{2}}}_{\in\mathbb{R}\,(\text{Eigensch. (ii)})} \in \mathbb{C}$$

□

Beweis. (von Theorem (A.13), nach E. Artin)
Es sei α algebraisch über $\mathbb{C}$. Es sei L die normale Hülle von $\mathbb{C}(\alpha)$. Werden zeigen: $L = \mathbb{C}$. ($\Rightarrow \alpha \in \mathbb{C} \Rightarrow$ Theorem)
$L/\mathbb{C}$ und $L/\mathbb{R}$ sind galoisch. Betrachte Sylow–Untergruppe $H \subset G(L/\mathbb{R})$ zu $p = 2$. Sei $M \subset L$ der Fixkörper von H.



Lemma A.15 (Satz vom primitiven Element)
Sei $M/\mathbb{R}$ galoisch. Dann gibt es ein $\alpha \in M$ mit $M = \mathbb{R}[\alpha]$.

Beweis. Nach dem Hauptsatz der Galoistheorie (6.82) gibt es endlich viele Zwischenkörper

$$\mathbb{R} \subsetneq N_i \subsetneq M \qquad (i = 1, \ldots, n).$$

Da $\dim_{\mathbb{R}} N_i < \dim_{\mathbb{R}} M$ gilt:

$$\bigcup_{i=1}^{n} N_i \neq M.$$

Wähle $\alpha \in M \setminus \bigcup_{i=1}^{n} N_i$. Dann gilt

$$M = \mathbb{R}[\alpha].$$

□

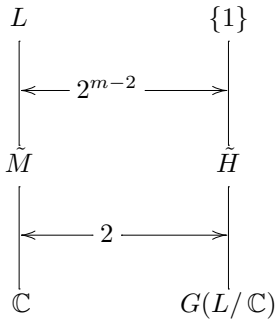
Sei $f(X) \in \mathbb{R}[X]$ das Minimalpolynom von α über $\mathbb{R}$.

$$\begin{aligned} &f \text{ irreduzibel und } \deg(f) = [M : \mathbb{R}] \text{ ist ungrade} \\ &\overset{\text{Eig. (i)}}{\Longrightarrow} \deg(f) = 1 \Rightarrow M = \mathbb{R} \\ &\Rightarrow [L : M] = 2^m \Rightarrow [L : \mathbb{C}] = 2^{m-1}. \end{aligned}$$

Betrachte nun:

Annahme: $L \neq \mathbb{C}$, also $2^{m-1} > 1$.

Untergruppe $\tilde{H} \subset G(L/\mathbb{C})$ der Ordnung 2^{m-2} (Existiert nach Satz (7.85)). Sei $\tilde{M} \subset L$ Fixkörper von $\tilde{H}$.



Es gilt $[\tilde{M} : \mathbb{C}] = \frac{|G(L/\mathbb{C})|}{|\tilde{H}|} = 2$. Dies ist ein Widerspruch zum Lemma (A.14). Damit ist der Beweis vollständig. □

Literaturverzeichnis

[1] E. Kunz: *Algebra,* Vieweg Studium

[2] Fischer, Sacher: *Algebra I-II,* Teubner

[3] Lang, *Algebra,* Addison Wesley

[4] v.d. Waerden: *Algebra I,II,* Heidelberger Taschenbuch

[5] Lorenz: *Algebra,* BI

[6] M. Artin: *Algebra,* Birkhäuser